Open source Secure Mail Gateway Software

Administrators Guide, Version 1.0.5
For use with MailScanner Version 4.45.4
rpm based installations

Developed by Julian Field, Electronics and Computer Science Department, the University of Southampton.

9.7.2005

This manual has been created and is supported free of charge by:

www.fsl.com

Author: Stephen Swaney, Fort Systems Ltd., steve.swaney@fsl.com
Contributors: Denis Beauchemin [denis.beauchemin@usherbrooke.ca]
Ugo Bellavance, [ugob@camo-route.com]
Michele Neylon, [michele@blacknightsolutions.com]
Ron Pool [amp1@nysaes.cornell.edu]

Fort Systems Ltd.
3807 Fulton Street N.W.
Washington, DC 20007-1345
202 338-1670
www.FSL.com

Contents

This Page is intentionally blank

Chapter 1

Introduction

Congratulations, your email will now be protected by the world's most widely used and respected email scanning software, MailScanner

A Brief History of MailScanner

MailScanner is a highly respected open source email security system. It is used at over 30,000 sites around the world, protecting top government departments, commercial corporations and educational institutions. This technology is becoming the standard email solution at many ISP sites for virus protection and spam filtering.

MailScanner scans all e-mail for viruses, spam and attacks against security vulnerabilities and plays a major part in the security of a network. To securely perform this role, it must be reliable and trustworthy. The only way to achieve the required level of trust is to be open source, an approach the commercial suppliers are not willing to take. By virtue of being open source, the technology in MailScanner has been reviewed many times over by some of the best and brightest in the field of computer security, from around the world.

MailScanner has been developed by Julian Field at the world-leading Electronics and Computer Science Department at the University of Southampton.

How MailScanner Works

MailScanner provides the engine used to scan incoming emails, detecting security attacks, viruses and spam.

Email is accepted and delivered to an incoming queue directory. When there are messages waiting in the incoming spool directory, MailScanner processes the waiting messages and then delivers the cleaned messages to the outgoing queue directory where they are picked up and delivered normally. Only after the messages are delivered to the outgoing queue directory are they deleted from the incoming spool directory. This ensures that no mail is lost, even in the event of unexpected power loss, as the system always has an internal copy of all messages being processed.

The MailScanner engine initiates email scanning by starting, in most configurations, two instances of the Mail Transport Agent (MTA). The first MTA instance is started in daemon mode to accept incoming email. Email is accepted and simply delivered to an incoming queue directory. The second MTA instance is also started in daemon mode and watches an outgoing queue directory for scanned and processed messages that need to be delivered.

To accomplish these scanning and processing tasks, MailScanner starts a configurable number of MailScanner child processes. Typically there are five child processes which examine the incoming queue at five second intervals and select a number of the oldest messages in the queue for batch processing. The number of child processes and the time interval between them is configurable and should be set based on the gateway system’s speed, memory, number of processors and other application loads.

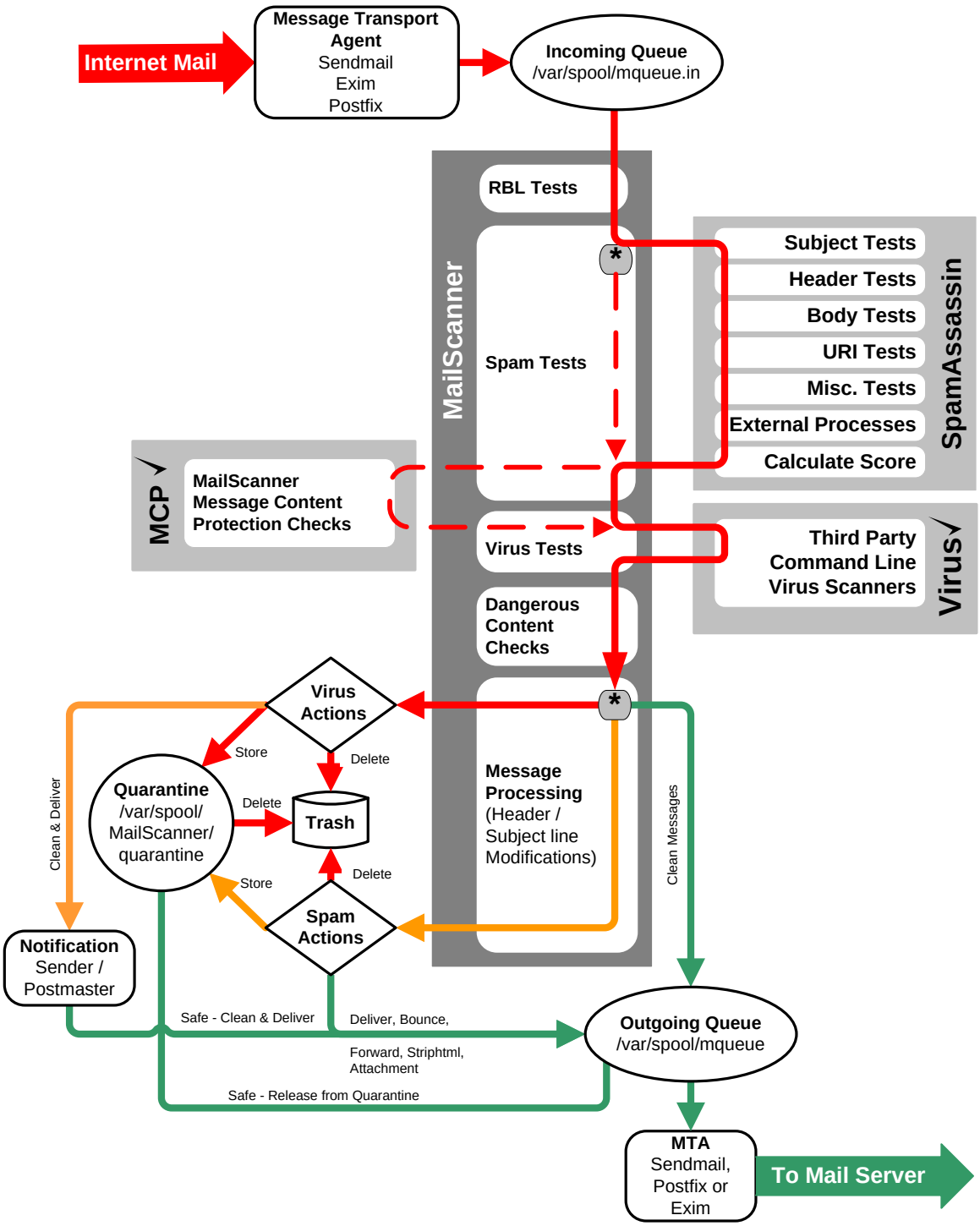

Figure. 1 MailScanner Process Flow

Typically, once a MailScanner child process has found a batch of emails in the incoming queue and MailScanner has been configured to use RBLs, it first runs a series of Real-time Black List (RBL) tests on each message. If the IP address of the sender's mail server or mail relay servers matches a definable number of RBLs, the message may by marked as definitely spam and no further tests are performed to save processing time.

If the message passes the MailScanner RBL tests it is passed to SpamAssassin which uses heuristic, Bayesian and other tests to determine the spam level of the message (see Figure 1.)

SpamAssassin assigns a numerical value to each test that is used on the message. SpamAssassin also examines the site specific whitelists (not spam) and black lists (is spam). If the sender, system or domain of the message sender is on either list, a very high (black list), or a very low (negative score) is assigned to the message. SpamAssassin calculates the final spam score for each message at the end of these tests.

MailScanner may be configured to use one or more of twenty six commercial or open source virus scanners. MailScanner may be configured to scan for viruses inside of zip files. If a virus is detected at this point, the message is marked as containing a virus.

Once virus detection is complete, Message Content Protection (MCP) rules are checked if MCP is enabled. MCP scanning checks use a 2nd copy of SpamAssassin to check text and HTML message segments for any banned text. This 2nd copy has its own entire set of rules, preferences and settings. When used together with the patches for SpamAssassin, it can also check the content of attachments such as office documents.

The MailScanner child process next examines the filename and file types of any email attachments against site configurable rulesets. Virtually any type or name of attachments can be blocked or passed depending on how MailScanner has been configured. The message is also examined to see if the body contains possibly dangerous HTML content such as:

- IFrame tags
- <Form> tags
- WebBugs
- <Object Codebase =...> tags

Configurable options allow logging, passing, deleting, blocking or disarming these HTML content tags.

After this stage of processing, MailScanner has all the information needed to modify, deliver, reject or quarantine the message. This final message processing depends on the message content and the MailScanner configuration settings.

If a virus is detected, MailScanner can send (or not send):

- A customized message to the sender of the virus (almost never desirable as the
- sending addresses of viruses are usually forged)
- A customized message to the recipient of the virus
- The disarmed and sanitized message to the recipient
- The message and the virus to quarantine
- The disinfected or cleaned message to the recipient

Every message has now received a “spam score”. MailScanner can be configured to discern between different levels spam scores:

- Not spam, i.e. spam score < 6
- Spam, i.e. spam score =>6 and <=10
- High scoring spam, i.e. spam score >10

For each of the not spam or spam levels listed above, MailScanner can perform any combination of the following options:

- Delete - delete the message
- Store - store the message in the quarantine
- Bounce - send a rejection message back to the sender (although this is almost never desirable!)
- Forward user@domain.com - forward a copy of the message to user@domain.com
- Strip HTML - convert all in-line HTML content to plain text
- Attachment - convert the original message into an attachment of the message
- Deliver - deliver the message as normal

These and most other message processing options are configurable using rulesets for any combination of To: and/or From: addresses for specific domains, senders or recipients. For example, spam and virus detection may be turned on or off for different combinations of To: and/or From: addresses of specific domains, senders or recipients. For more information on rulesets, see Chapter 5.

All mail or mail to specific recipients or domains may also be archived.

Many other alterations may be made to individual messages depending on the site’s preferences:

- Various levels and types of spam scores may be added to the header of the message
- Custom headers may be added or removed
- Customizable “X-“style messages may be added to the header of the message
- Subject: lines may be customized depending on Virus, attachment or spam score detected
- Messages may be signed with site customized footers
- Reports to administrators, senders and recipients may be customized (standard reports are available in fifteen different languages)

MailScanner also provides the additional features and functions required for ease of email gateway administration and maintenance:

- Simple, automated installation
- Sensible defaults for most sites
- Automated updating of virus definitions for all supported virus scanning engines
- Configurable cleaning options for quarantined messages
- Very simple application updating

Chapter 2

Planning the Installation

Taking a little time to plan out the installation of MailScanner will ensure that the process is straight forward and successful.

Gather the following information prior to installing:

root password: _____

IP address for MailScanner gateway: _____

Netmask for MailScanner gateway: _____

Name Server IP address: _____

Domain names for which you process email: _____

Current mail server hostname(s): _____

System Requirements

System requirements are dependent on:

- Number of email messages processed daily
- Number of virus scanners used
- Number of MailScanner features enabled
- Number of SpamAssassin features and rules enabled
- Number of related applications installed

It is important to note that the number of messages per hour that the system can process is directly dependent on the type of hardware used. Larger volume sites will need to use more powerful hardware to handle their larger volume of mail.

For example, a Pentium II with 256MB of RAM running MailScanner, SpamAssassin, DCC, Pyzor, Razor, MailWatch, Vispan and MailScanner-MRTG can process approximately 5,000 messages per day.

A System with dual 2.4 GHz Xeon processors, 2 GB of RAM and 15,000 RPM SCSI drives and running only MailScanner and SpamAssassin can process up to 1,400,000 messages per day.

Some further examples of actual system capacities may be found at:

http://wiki.mailscanner.info/doku.php?id=mag:index#setup_examples

Proper operation of the MailScanner software requires that it run on a server with a fixed IP address. This is typically a requirement of any mail server, and to the outside world, the MailScanner gateway appears as a mail server. For most email servers to accept email from your email gateway, your mail server must also have a reverse name lookup entry (PTR) record ideally, corresponding to the “ehlo or helo” string of your mail server.

Firewall and Network Requirements

The MailScanner gateway will need direct access to the Internet for ports:

- SMTP tcp port 25 (inbound and outbound)
- DNS tcp/udp port 53 (outbound. Inbound and outbound if you are also running a DNS server on the gateway)

Related applications, if installed will also need NAT access to the internet. The most common ports that may need to be enabled on the firewall are:

- Razor2 tcp ports 2703 and 7 (outbound)
- Pyzor udp port 24441 (outbound)
- DCC udp port 6277 (outbound)

Installing Red Hat Enterprise Linux

> Please note that this manual currently only covers the installation of MailScanner for Red Hat Linux (other RPM-based Linux distributions will be similar). An installation on CentOS will be almost identical.

While MailScanner can be installed on most versions of Linux and UNIX operating systems, this version of the MailScanner Manual includes only installation instructions for Red Hat Linux. Instruction for installing MailScanner on other operating systems may be found at:

http://wiki.mailscanner.info/doku.php?id=maq:indexe

Before the MailScanner may be installed, the Linux Operating system must be installed. Step by step instructions for installing Red Hat Enterprise Linux are included in Appendix A. Installation of other Linux Operating System will be similar.

> After installing Red Hat Linux you should edit the file /etc/sysconfig/i18n to change the lines:
>
> LANG="en_US.UTF-8"
>
> SUPPORTED="en_US.UTF-8:en_US:en"
>
> To:
>
> LANG="en_US"
>
> SUPPORTED="en_US.UTF-8:en_US:en"

Note the example shown above is for US English installations. You may need to make similar edits for other languages.

Failure to make these changes may result in MailScanner and SpamAssassin installation errors.

Installing the Message Transfer Agent

Before the MailScanner may be installed, your Message Transfer Agent (MTA) must be installed, configured and tested. MailScanner supports several MTAs and the choice of which one to use is up to the user. The three most popular MTA are:

- Sendmail
- Exim
- Postfix

For other information on other supported MTAs please visit:

http://wiki.mailscanner.info/doku.php?id=&idx=documentation:install_upgrade:install

Installing sendmail

Binary rpm packages are available from your Operating System Vendor. Packaged distributions are also available for other Operating Systems. Instructions for obtaining, installing and configuring Exim from source may be found at:

http://www.sendmail.org/

Installing Exim

Binary rpm packages are available from

http://rpm.pbone.net/

Packaged distributions are also available for other Operating Systems. Instructions for obtaining, installing and configuring from source. Exim may be found at:

http://www.exim.org/

Installing Postfix

Binary rpm packages are available from your Operating System Vendor. Packaged distributions are also available for other Operating Systems. Instructions for obtaining, installing and configuring Postfix from source may be found at:

http://www.postfix.org/

Installing MailScanner

Please note that this manual currently only covers the installation of MailScanner for Red Hat Linux (and other RPM-based Linux distributions)

MailScanner software may be downloaded from:

http://www.sng.ecs.soton.ac.uk/mailscanner/downloads.shtml

1. Login to your server as root.
2. This step is not really necessary but it is useful to keep your installation packages and installed software download in one location; create an installation directory, e.g.:

   `mkdir /home/install`

   cd to installation directory:

   `cd /home/install`

   Download the latest Stable version of MailScanner software for Red Hat Linux (and other RPM-based Linux distributions) from the URL listed above into the installation directory

3. Unpack the distribution:

   ```
   mkdir build
   cd build
   tar zxf ../ MailScanner-<version_number>.tar.gz
   cd MailScanner-<version_number>
   ./install.sh
   ```

4. The install.sh script should finish without major errors. This is typically all that needs to be done to install MailScanner on a Linux rpm based distribution. If you experience errors or problems at this stage, please see Chapter 7, Tuning and Troubleshooting.

5. Stop the MTA from starting at boot time:
   ```
   chkconfig --level all sendmail off
   ```

6. Setup MailScanner to start at boot time:
   ```
   chkconfig --level 345 MailScanner on
   ```

7. Start MailScanner:
   ```
   service sendmail stop
   service MailScanner start
   ```

8. Check the mail logs to ensure that MailScanner has started properly with no Errors.

Installing SpamAssassin

SpamAssassin software may be downloaded from:

http://www.spamassassin.org/downloads.html

The version that should be installed with MailScanner is:

SpamAssassin(tm) in tar.gz format.

> Do not install the rpm version available on the SpamAssassin Site. There have been many problems reported after installing SpamAssassin from this rpm.

Before beginning the installation, you should review the SpamAssassin installation documentation available at:

http://spamassassin.apache.org

Login to your server as root.

1. If you created the installation directory as recommended above:

   ```
   cd /home/install
   ```

2. Download the SpamAssassin in the tar.gz format. from the URL listed above into the `/home/install` directory
   ```
   cd build
   tar zxf ../Mail-SpamAssassin-<version_number>.tar.gz
   ```

```
cd Mail-SpamAssassin-<version_number>
perl MakeFile.PL
make
make test
make install
```

These steps should complete without errors. This is typically all that needs to be done to install SpamAssassin for use with MailScanner. If you experience errors or problems at this stage, please see Chapter 7, Tuning and Troubleshooting.

SpamAssassin may also be installed using CPAN. To install using this method:

1. Start CPAN:

   ```
   Perl –MCPAN –e shell
   ```

2. Start the installation:

   ```
   cpan> install Mail::SpamAssassin
   ```

Sometime the CPAN mirrors tale a while to update after a new release of SpamAssassin so if you use the CPAN installation method you should check that you have installed the latest version.

This page is left intentionally blank

Chapter 3

MailScanner Configuration

MailScanner ships with sensible defaults but the MailScanner default configuration should be examined in detail before placing the system into production.

MailScanner Files

MailScanner is configured and controlled by editing text files. The most important files are located in the directory `/etc/MailScanner` (Linux rpm version):

`/etc/MailScanner/MailScanner.conf` contains the MailScanner configuration. Most of your configuration work will involve changing the values in this file to match your site's need.

/`etc/MailScanner/spam.assassin.prefs.conf` contains the SpamAssassin configuration values as:

```
Parameter <value>
```

All SpamAssassin configuration values should be placed in this file. All site SpamAssassin Rulesets should be placed in `/etc/mail/spamassassin` (default location) or the locations specified by

SpamAssassin Site Rules Dir = /etc/mail/spamassassin

In the `MailScanner.conf file`.

Please note that MailScanner ships with reasonable default values for SpamAssassin but you are advised to examine other configuration options at:

http://www.spamassassin.org/doc/Mail_SpamAssassin_Conf.html

Other configurable files (Linux rpm version) are located in the

- `/etc/MailScanner/reports/<your_language>` directories. The files located here should be edited to reflect your site name and preferences.
- /etc/MailScanner/rules directories. This directory contains the default rulesets and your custom rulesets. Please see Chapter 5, Advanced Configuration via Rulesets.

Getting Started with MailScanner Configuration

The following steps should be followed in order to quickly configure MailScanner and place it in production:

1. Edit the `MailScanner.conf` file to reflect your site's preferences. Please read this documentation thoroughly before configuring `MailScanner.conf.`

2. Review and edit if necessary the SpamAssassin site preferences file `spam.assassin.prefs.conf.`

3. Edit the files in `/etc/MailScanner/reports/<your_language>` directory and correct for your site information.

Before you start

Editing the MailScanner.conf file to reflect your sites preferences involves changing values or adding rulesets. The format of this file is simply:

- `#` - Lines starting with # are comments. While you may add comments you should note that they may be lost if you automatically upgrade the `MailScanner.conf` file using the `upgrade_MailScanner_conf` script. To keep your old comments in your original file, add "`--keep-comments`" to the command line. Note that this will mean you don't get to see any new comments describing new possible values that may have been added to existing options.
- MailScanner configuration values may be:

  `Parameter = <value>`

  or

  `Parameter = <pointer to a ruleset>`

  or

  `Parameter = <space separated list>`

Before editing the MailScanner.conf file please note:

- If your directories are symlinked (soft-linked) in any way, please put their *real* location as the value, not a path that includes any links. You may get some very strange error messages from some virus scanners if you don't.
- A lot of the settings can take a ruleset as well as just simple values. These rulesets are files containing rules which are applied to the current message to calculate the value of the configuration option. The rules are checked in the order they appear in the ruleset. Please see Chapter 6 for additional information.

In addition to rulesets, you can now include your own functions as values. Please locate and look at the file `MyExample.pm` located in `/usr/lib/MailScanner/MailScanner/CustomFunctions` and create your own `MyFunctions.pm` in the same directory. In this file, you can add your own "value" function and an Initvalue function to set up any global state you need such as database connections. To use your new function, refer to it in a `MailScanner.conf` configuration setting this way:

`Configuration Option = &ValueFunction`

where ValueFunction is the name of the function you have written in `MyFunctions.pm.`

MailScanner.conf Parameters

Below we will list the all of the configurable parameters in the MailScanner.conf file in the order in which they appear in the file. The format will be:

`Parameter = default value`

A description of what the rule does.

A list of the possible options and the results of specifying the specific option

General settings

%report-dir% = /etc/MailScanner/reports/en

Sets directory containing the language for reports used at your site.

Look in /etc/MailScanner/reports for a listing of the supported languages.

An example: If you want to use French for your MailScanner reports, set:

%report-dir% = /etc/MailScanner/reports/fr

This setting may point to a ruleset.

%etc-dir% = /etc/MailScanner

Sets the top directory containing the MailScanner configuration files.

This should not be changed for the Linux rpm distribution. It will typically need to be changed for other Operating Systems, i.e. Solaris, TRU64.

%rules-dir% = /etc/MailScanner/rules

Sets the top directory containing the MailScanner rulesets. Your custom rulesets should be placed in this directory.

This should not be changed for the Linux rpm distribution. It will typically need to be changed for other Operating Systems, i.e. Solaris, TRU64

%mcp-dir% = /etc/MailScanner/mcp

Sets the top directory containing the Message Content Protection configuration files.

This should not be changed for the Linux rpm distribution. It will typically need to be changed for other Operating Systems, i.e. Solaris, TRU64.

%org-name% = yoursite

A short identifying name for your organization. This value will be used to create unique X-MailScanner headers which identify your organization.

Sites with multiple servers should use an identical value on all servers within the site. This will avoid adding multiple redundant headers where mail has passed through several servers within your organization.

This must be changed to identify your site. Using a custom %org-name% here avoids a problem where mail tagged by MailScanner could be mis-categorized as a virus be a naive third part virus scanner rule on someone else's mail server.

Note: This value MUST NOT contain any white spaces or periods.

%org-long-name% = Your Organization Name Here

Enter the full name of your organization. This value is used in the signature placed at the bottom of report messages sent by MailScanner. It can include pretty much any text you like. You can make the result span several lines by including "\n" sequences in the text. These will be replaced by line-breaks.

Sites with multiple servers should use an identical value on all servers within the site. This will avoid adding multiple redundant headers where mail has passed through several servers within your organization.

This must be changed to identify your site.

%web-site% = www.your-organisation.com

Enter the location of your organization's web site. This value is used to create the signature placed at the bottom of report messages sent by MailScanner. It should preferably be the location of a page that you have written explaining why you might have rejected the mail and what the recipient and/or sender should do about it.

Sites with multiple servers should use an identical value on all servers within the site. This will avoid adding multiple redundant headers where mail has passed through several servers within your organization.

This must be changed to identify your site.

System Settings

Max Children = 5

This is the number of MailScanner processes to run at a time. There is no point increasing this figure if your MailScanner server is happily keeping up with your mail traffic.

Each process will consume at least +20MB of RAM and using additional SpamAssassin rulesets can increase this to +40MB. If you are running on a server with more than 1 CPU, or you have a high mail load (and/or slow DNS lookups) then you should see better performance if you increase this figure. As a very rough guide you can try 5*(number of CPUs) for multiple CPU systems.

It is important to ensure that there is enough ram for all processes. Performance will suffer greatly if the Scanner Nodes run out of ram and begin to swap.

Run As User = <blank>

User to run MailScanner processes as (not normally used for sendmail). If you want to change the ownership or permissions of the quarantine or temporary files created by MailScanner, please see the "Incoming Work" settings later in this document.

Other Possible values: mail postfix and possibly others

Run As Group = <blank>

Group to run MailScanner processes as (not normally used for sendmail).

Other Possible values: mail postfix and possibly others

Queue Scan Interval = 5

The time (in seconds) between the start up of each MailScanner child process. If you have a quiet mail server, you might want to increase this value so it causes less load on your server, at the cost of slightly increasing the time taken for an average message be processed.

Other Possible values: integers

Incoming Queue Dir = /var/spool/mqueue.in

Set location of incoming mail queue. This can be any one of:

- A directory name
  Example: `/var/spool/mqueue.in`
- A wildcard giving directory names
  Example: `/var/spool/mqueue.in/*`
- The name of a file containing a list of directory names, which can in turn contain wildcards.
  Example: `/etc/MailScanner/mqueue.in.list.conf`

This should not be changed for the Linux rpm distribution. It may need to be changed for other distributions or with other prepackaged applications servers, e.g. Ensim

Quarantine Dir = /var/spool/MailScanner/quarantine

This sets where to store infected and message attachments (if they are kept).

This should not be changed for the Linux rpm distribution. It may need to be changed for other distributions.

PID file = /var/run/MailScanner.pid

This sets where to store the process id number used to stop MailScanner processes.

This should not be changed for the Linux rpm distribution. It may need to be changed for other distributions.

Restart Every = 14400

This setting determines how often (in seconds) MailScanner will restart the MailScanner processes. This is done to avoid resource leaks. When MailScanner processes are restarted, the configuration files are re-read. This restart will not restart the MTA, only MailScanner.

Typically this setting does not need to be changed.

MTA = sendmail

This should be set to the MTA used on your gateway. If you are using postfix, then see the SpamAssassin User State Dir parameter later in this documentation.

Other Possible values: postfix exim, qmail or exim.

Sendmail2 = sendmail2

This setting is provided for Exim users. It is the command used to attempt delivery of outgoing cleaned/disinfected messages. This is not usually required for sendmail. This can also be the filename of a ruleset. i.e. for Exim users:

Sendmail2 = /usr/sbin/exim -C /etc/exim/exim_send.conf

This setting typically only should be changed when using exim.

Incoming Work Dir Settings

You should not normally need to touch Incoming Work Dir Settings unless you are using ClamAV and need to be able to use the external archive un-packers instead of ClamAV's built-in ones.

Incoming Work User = <blank>

Incoming Work Group = <blank>

These settings should be changed only if you want to create the temporary working files so they are owned by a user other than the **Run As User** setting discussed earlier. Note: If the **Run As User** setting is not "root" then you cannot change the user but may still be able to change the group, if the **Run As User** is a member of both of the groups **Run As Group** and **Incoming Work Group**.

Permissible values are system usernames, i.e. root, postfix

Typically this setting does not need to be changed.

Incoming Work Permissions = 0600

Used to set the permissions (file mode) for working files. For example, if you want processes running under the same *group* as MailScanner to be able to read the working files (and list what is in the directories, of course), set to 0640. If you want *all* users to be able to read them, set to 0644. Typical use: external helper programs of virus scanners (notably ClamAV).

Permissible values are those allowed by the `chmod` command

Typically this setting does not need to be changed.

> Use with care, you may well open security holes.

Quarantine and Archive Settings

If you are using a web interface to allow users to manage their quarantined files, you might want to change the ownership and permissions of the quarantine files so that they can be read and/or deleted by the web server. Don't touch this unless you know what you are doing!

Quarantine User = <blank>

Quarantine Group = <blank>

These settings would be changed only if you want to create the quarantine/archive so the files are owned by a user other than the Run As User discussed earlier. Typically this is done to allow an application such as MailWatch to release messages from quarantine.

Typically this setting does not need to be changed but if it does, this typical changes is required if MailWatch is installed are:

Quarantine User = root and **Quarantine Group = apache**.

Quarantine Permissions = 0600

Used to set permissions (file mode) of quarantine files. For example, if you want processes running under the same group as MailScanner to be able to read the quarantined files and list what is in the directories, set this value to

0640. If you want all other users to be able to read them, set to 0644. For a detailed description, refer to `man 2 chmod`.

Typical use: let the web server have access to quarantined files so users can download them if they really want to.

Typically this setting does not need to be changed, but if it does, e.g. for MailWatch, the typical value is 0640.

Use with care, you may well open security holes.

Processing Incoming Mail

Max Unscanned Bytes Per Scan = 100000000

This setting controls the maximum total size of un-scanned messages, in bytes, that each MailScanner child process will pick up and process from the incoming mail queue. If the Scanner Nodes have substantial unused memory, increasing this value can increase message throughput, as long as the system's CPU(s) is not overloaded.

Typically this setting does not need to be changed.

Max Unsafe Bytes Per Scan = 50000000

This setting controls the maximum total size of potentially infected messages, in bytes, that each MailScanner child process will pick up and process from the incoming mail queue. On a system with plenty of unused memory, increasing this value can increase message throughput, as long as the system's CPU(s) is not overloaded.

Typically this setting does not need to be changed.

Max Unscanned Messages Per Scan = 30

This setting controls the maximum number of un-scanned messages that each MailScanner child process will pick up and process from the incoming mail queue. On Scanner Nodes with plenty of unused memory, increasing this value can increase message throughput, as long as the system's CPU(s) is not overloaded.

Typically this setting does not need to be changed.

Max Unsafe Messages Per Scan = 30

This setting controls the maximum number of potentially infected messages that each MailScanner child process will pick up and process from the incoming mail queue. On Scanner Nodes with plenty of unused memory, increasing this value can increase message throughput, as long as the system's CPU(s) is not overloaded.

Typically this setting does not need to be changed.

Max Normal Queue Size = 800

If more than this number of messages are found in the incoming queue, MailScanner will switch to an "accelerated" mode of processing messages. This will cause it to stop scanning messages in strict date order, but instead will scan in the order it finds them in the queue. If your queue is bigger than this size a lot of the time, then some messages could be greatly delayed. So treat this option as an "in emergency only" option.

Possible values = integers

Typically this setting does not need to be changed.

Scan Messages = yes

If this is set to yes, then email messages passing through MailScanner will be processed and checked, and all the other options in this file will be used to control what checks are made on the message. If this is set to no, then email messages will NOT be processed or checked *at all*, and so any viruses or other problems will be ignored.

The purpose of this option is to set it to be a ruleset, so that you can skip all scanning of mail destined for some of your users/customers and still scan all the rest. A sample ruleset would look like this:

```
To:       bad.customer.com  no
From:     ignore.domain.com no
FromOrTo: default           yes
```

That will scan all mail except mail to bad.customer.com and mail from ignore.domain.com. To set this up, put the 3 lines above into a file called /etc/MailScanner/rules/scan.messages.rules and set:

```
Scan Messages = %rules-dir%/scan.messages.rules
```

This can also be the filename of a ruleset (as illustrated above).

Maximum Attachments Per Message = 200

This setting controls the maximum number of attachments allowed in a message before it is considered to be an error. Some email systems, if bouncing a message between 2 addresses repeatedly, add information about each bounce as an attachment, creating a message with thousands of attachments in just a few minutes. This can slow down or even stop MailScanner as it uses all available memory to unpack these thousands of attachments.

Possible values = integers

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Expand TNEF = yes

This setting determines if TNEF attachments are to be expanded using an external program or a Perl module. This should be "yes" unless the scanner you are using is Sophos, McAfee or a virus scanner that has the built-in ability to expand the message. If set to no, then the filenames within the TNEF attachment will not be checked against the filename rules.

Typically this setting does not need to be changed unless you are using the Sophos or McAfee virus scanners.

Deliver Unparsable TNEF = no

Some versions of Microsoft Outlook generate un-parsable Rich Text format attachments. If you want to deliver these bad attachments anyway, then set this value to yes. This introduces a slight risk of a virus getting through, but if you have complaints from Outlook users, you may need to set this value to yes.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

TNEF Expander = /usr/bin/tnef --maxsize=100000000

This setting determines which MS-TNEF expander is used.

This is EITHER the full command (including maxsize option) that runs the external TNEF expander binary, OR the keyword **internal** which will cause MailScanner to use the Perl module that does the same job. They are both provided as we are unsure which one is faster and which one is capable of expanding more file formats (there are plenty!).

The --maxsize option limits the maximum size that any expanded attachment may be. It helps protect against Denial of Service attacks in TNEF files.

If this setting is changed, it is typically set to internal.

This cannot be the filename of a ruleset.

Typically this setting does not need to be changed.

TNEF Timeout = 120

This setting controls the length of time (in seconds) that the TNEF expander is allowed to run on a single message.

Permissible values = integers

Typically this setting does not need to be changed.

File Command = #/usr/bin/file

Where the "file" command is installed. The file command is used for checking the content type of files, regardless of their filename. The default value of `#/usr/bin/file` actually disables filename checking (note the # starts a comment).

To enable filename checking, set the value to /usr/bin/file (on most systems). The location of the file command varies with different operating systems.

This setting is often changed to force file type settings.

File Timeout = 20

This setting controls the length of time (in seconds) that the file is allowed to run on a single message.

Permissible values = integers

Typically this setting does not need to be changed.

Unrar Command = /usr/bin/unrar

This is used for unpacking rar archives so that the contents can be checked for banned filenames and filetypes, and also so that the archive can be tested to see if it is password-protected. Virus scanning the contents of rar archives is still left to the virus scanner, with one exception. If using the clavavmodule virus scanner, this adds external RAR checking to that scanner which is needed for archives which are RAR version 3.

Permissible values = blank or the location of the unrar executable file.

Typically this setting should be changed to the location of the unrar binary file.

Unrar Timeout = 50

This setting controls the length of time (in seconds) the "unrar" command is allowed to run for one RAR archive scan (in seconds).

Permissible values = integers

Typically this setting does not need to be changed.

Maximum Message Size = 0

This setting controls the maximum size, in bytes, of any message including the headers. If this is set to zero, then no size checking is done. If this is set to a value, messages exceeding this size, in bytes, will be blocked.

This can also be the filename of a ruleset, so you can have different settings for different users. You might want to set this to be small for dialup users so their email applications don't time out downloading huge messages.

Permissible values = integers

Typically this setting should not to be changed.

Maximum Attachment Size = -1

This setting controls the maximum size, in bytes, of any attachment in a message. If this is set to zero, effectively no attachments are allowed. If this is set less than zero, then no size checking is done. Attachments that exceed this value, in bytes, will be blocked.

This can also be the filename of a ruleset, so you can have different settings for different users. You might want to set this quite small for large mailing lists so they don't get deluged by large attachments.

Typically this setting does not need to be changed.

Minimum Attachment Size = -1

This setting controls the minimum size, in bytes, of any attachment in a message. If this is set less than or equal to zero, then no size checking is done. It is very useful to set this to 1 as it removes any zero-length attachments which may be created by broken viruses.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Maximum Archive Depth = 3

The maximum depth to which zip archives will be unpacked, to allow for filenames and filetype checking within zip archives. To disable this feature set this to 0.

Often this setting is changed to 0.

A common useful setting is to **Maximum Archive Depth = 0**, and set **Allow Password-Protected Archives = no**. This will block password-protected archives but does not do any filename or filetype checks on the files within the archive. This allows users to receive files that would normally be blocked by filename and filetype rules if they are compressed before sending. Virus scanning will still occur on files within the archive.

Find Archives By Content = yes

Find zip archives by filename or by file contents? Finding zip archives by content is far more reliable, but means that users cannot avoid zip file checking by renaming the file from ".zip" to "_zip.

Only set this to no (i.e. check by filename only) if you don't want to reliably check the contents of zip files. Note this does not affect virus checking, but it will affect all the other checks done on the contents of the zip file.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Virus Scanning and Vulnerability Testing

Virus Scanning = yes

This setting switches on/off the processing of all the email messages for virus checking. If you do not have a license for a commercial virus scanner you should consider installing ClamAV, an open source virus scanner.

This can also be the filename of a ruleset. If you want to be able to switch scanning on/off for different users or different domains, set this to the filename of a ruleset and create the corresponding ruleset.

Typically this setting does not need to be changed.

Virus Scanners = none

If you want to use a single virus scanner, then this should be the name of the of virus scanner. For example:

Virus Scanners = sophos

If you want to use multiple virus scanners, then this should be a space-separated list of virus scanners. For example:

Virus Scanners = sophos f-prot mcafee

Make sure that you check that the base installation directory in the 3rd column of the `virus.scanners.conf` file matches the location where you have installed each of your virus scanners. The defaults provided in the `virus.scanners.conf` file assume installation in the locations recommended by each of the virus scanner's installation instructions

Please see Appendix B, Installing Third party Virus Scanners, for instructions on configuring the many virus scanning engines supported by MailScanner.

Note for McAfee users: do not use any symlinks with McAfee at all. It is very strange, but McAfee may not detect all viruses when started from a symlink or when scanning a directory path that includes symlinks.

This setting should be changed to match the virus scanner or scanners used at your site.

Virus Scanner Timeout = 300

This setting controls the length of time, in seconds, the virus scanner is allowed to run on a single message.

Permissible values = integers

Typically this setting does not need to be changed.

Deliver Disinfected Files = no

This setting controls whether or not to disinfect infected attachments and then deliver the cleaned attachment. "Disinfection" involves removing viruses from files (such as removing macro viruses from documents). "Cleaning" is the replacement of infected attachments with "VirusWarning.txt" text attachments.

Since less than 1% of viruses in the wild can be successfully disinfected and since macro viruses are now a rare occurrence, the default is set to no as it results in a significant performance improvement.

Typically this setting does not need to be changed.

Silent Viruses = HTML-IFrame All-Viruses

Strings listed here, separated by white space, will be searched for in the output of the virus scanner(s). These strings are used to list which viruses should be handled differently from other viruses. If a virus name is given here, then

- The (probably forged) sender will not be warned that they sent the message.
- No attempt at true disinfection will take place (but it will still be "cleaned" by removing the nasty attachments from the message).
- The recipient will not receive the message, unless the **Still Deliver Silent Viruses** option is set (see below).

The only words that can be put in this list are the 5 special keywords plus virus names:

- **HTML-IFrame**: inserting this will stop senders being warned about HTML IFrame tags, when they are not allowed.
- **HTML-Codebase**: inserting this will stop senders being warned about HTML Object Codebase tags, when they are not allowed.
- **HTML-Form**: inserting this will stop senders being warned about HTML Form tags, when they are not allowed.
- **Zip-Password**: inserting this will stop senders being warned about password-protected zip files, when they are not allowed (This keyword is not needed if you include All-Viruses)
- **All-Viruses**: inserting this will stop senders being warned about any virus, while still allowing you to warn senders about HTML-based attacks. This includes Zip-Password so you don't need to include both.

The default of **All-Viruses** means that no senders of viruses will be notified (since the sender address is almost always forged), but anyone who sends a message that is blocked for other reasons will still be notified.

This setting may also be the filename of a ruleset.

Typically this setting does not need to be changed.

Still Deliver Silent Viruses = no

Still deliver (after cleaning) messages that contained viruses listed in the above option ("Silent Viruses") to the recipient?

Setting this to "yes" is good when you are testing everything, because it shows management that MailScanner is protecting them, but it is bad because they have to filter/delete all the incoming virus warnings.

Note: Once you have deployed this into "production" use, you should set this option to "no" so you don't bombard thousands of people with useless messages they don't want!

This setting may also be the filename of a ruleset.

Typically this setting does not need to be changed.

Non-Forging Viruses = Joke/ OF97/ WM97/ W97M/

Strings listed here, separated by white space, will be searched for in the output of the virus scanner(s). This works to achieve the opposite effect of the **Silent Viruses** setting above. If a string here is found in the output of the virus scanners, then the message will be treated as if it were not infected with a "Silent Virus". If a message is detected as both a silent virus and a non-forging virus, then the non-forging status will override the silent status. In simple terms, you should list virus names (or parts of them) that you know do *not* forge the From address.

A good example of this is a document macro virus or a Joke program. Another word that can be put in this list is the special keyword **Zip-Password**. Inserting this will cause senders to be warned about password-protected zip files, when they are not allowed. This will over-ride the All-Viruses setting in the list of Silent Viruses setting described above.

Typically this setting does not need to be changed.

Block Encrypted Messages = no

This setting can stop encrypted messages from being sent from your site. This is useful if you do not want users to be able to send encrypted messages.

This can be a ruleset so you can block encrypted message to certain domains or from specific users.

Typically this setting does not need to be changed.

Block Unencrypted Messages = no

This setting will allow only encrypted messages to be set sent from your site. This is useful if you need to enforce encryption for all messages sent from your domain.

This can be a ruleset so you can force encryption to specific domains.

Typically this setting does not need to be changed.

Allow Password-Protected Archives = no

This setting can stop password-protected files from being received by your site. Since password protected archives cannot be opened and checked by virus scanners, leaving this set to "no" is a good way of protecting against all the protected zip files used by viruses.

This can be a ruleset so you can block any password-protected zip files from certain domains or permit password-protected zip files to be sent to specific users.

Typically this setting does not need to be changed.

Options specific to Sophos Anti-Virus

Allowed Sophos Error Messages = <blank>

Anything on the next line that appears in brackets at the end of a line of output from Sophos will cause the error/infection to be ignored. Use of this option is dangerous, and should only be used if you are having trouble with Sophos corrupting PDF files. If you need to specify more than one string to find in the error message, then put each string in quotes and separate them with a comma. For example:

Allowed Sophos Error Messages =

Typically this setting does not need to be changed but some sites using Sophos virus scanner change this to:

```
Allowed Sophos Error Messages = "corrupt", "format not supported"
```

Sophos IDE Dir = /usr/local/Sophos/ide

This sets the directory (or a link to it) containing all the Sophos *.ide files. This is only used by the "sophossavi" virus scanner, and is irrelevant for all other scanners.

Typically this setting does not need to be changed.

Sophos Lib Dir = /usr/local/Sophos/lib

This sets the directory (or a link to it) containing all the Sophos *. so libraries. This is only used by the "sophossavi" virus scanner, and is irrelevant for all other scanners.

Typically this setting does not need to be changed.

Options specific to ClamAV Anti-Virus

Monitors for ClamAV Updates = /usr/local/share/clamav/*.cvd

This sets the directory to monitor for changes in files size to detect when a ClamAV update has occurred. This setting is only used by the "clamavmodule" virus scanner, not the "clamav" virus scanner.

Typically this setting does not need to be changed.

ClamAVmodule Maximum Recursion Level = 5

This sets the maximum recursion level of archives.

Typically this setting does not need to be changed.

This setting cannot be the filename of a ruleset, only a simple integer.

ClamAVmodule Maximum Files = 1000

This sets the maximum number of files per batch.

Typically this setting does not need to be changed.

This setting cannot be the filename of a ruleset, only a simple integer.

ClamAVmodule Maximum File Size = 10000000 # (10 Mbytes)

This sets the maximum file of each file.

Typically this setting does not need to be changed.

This setting cannot be the filename of a ruleset, only a simple integer.

ClamAVmodule Maximum Compression Ratio = 250

This sets the maximum file of each file.

Typically this setting does not need to be changed.

This setting cannot be the filename of a ruleset, only a simple integer.

Removing/Logging dangerous or potentially offensive content

Dangerous Content Scanning = yes

Do you want to scan the messages for potentially dangerous content? These checks include all of the settings below; HTML checks , webbug checks. and filename/type checks. Setting this to "no" will disable all the content-based checks except Allow Partial Messages and Allow External Message Bodies.

This setting may also be the filename of a ruleset.

Typically this setting does not need to be changed.

Allow Partial Messages = no

Do you want to allow partial messages, which only contain a part of the attachments, not the entire attachment? There is absolutely no way to scan these "partial messages" properly for viruses, since MailScanner never sees all of the attachment at the same time.

Enabling this option can allow viruses through. You have been warned.

This can also be the filename of a ruleset so you can, for example, allow them in outgoing mail but not in incoming mail.

Typically this setting does not need to be changed.

Allow External Message Bodies = no

Do you want to allow messages whose body is stored somewhere else on the internet, which is downloaded separately by the user's email package? There is no way to guarantee that the file fetched by the user's email package is free from viruses, as MailScanner never sees it. This feature is only currently supported by Netscape 6 anyway, and the organization using it is the IETF. Changing this setting can expose your end users to attacks which bypass MailScanner and desktop virus scanners.

Enabling this feature is dangerous as it can allow viruses to be fetched from other Internet sites by a user's email package. The user would think MailScanner has scanned such attachments like normal messages or attachments, but in reality MailScanner would never see or scan the external messages or attachments

This can also be the filename of a ruleset.

Typically this setting should never be changed.

Find Phishing Fraud = yes

Do you want to check for "Phishing" attacks? These are attacks that look like a genuine email message from a financial institution, which contain a link to click on to take you to the web site where you will be asked to type in personal information such as your account number or credit card details. However it is not the real financial institution’s web site; it is a very good copy of it run by thieves who want to steal your personal information or credit card details. These can be spotted because the real address of the link in the message is not the same as the text that appears to be the link.

This does cause extra load, particularly on systems receiving lots of spam such as secondary MX hosts.

This setting may also be the filename of a ruleset.

Typically this setting does not need to be changed.

Also Find Numeric Phishing = yes

While detecting "Phishing" attacks, do you also want to point out links to numeric IP addresses? Genuine links to totally numeric IP addresses are very rare, so this option is set to "yes" by default. If a numeric IP address is found in a link, the same phishing warning message is used as in the Find Phishing Fraud option above.

This setting may also be the filename of a ruleset.

Typically this setting does not need to be changed.

Highlight Phishing Fraud = yes

If a phishing fraud is detected, do you want to highlight the tag with a message stating that the link may be to a fraudulent web site.

This can also be the filename of a ruleset.

Allow IFrame Tags = no

Do you want to allow <IFrame> tags in email messages? This can be dangerous since it leaves you unprotected against various Microsoft-specific security vulnerabilities, but since many mailing lists use <IFrame> tags, you may want to allow them to avoid end user complaints.

Available setting values include:

- yes Allow <IFrame> tags in the message
- no Blocks messages containing <IFrame> tags
- disarm Allow <IFrame> tags, but stop these tags from working.

The disarm setting will stop <IFrame> tags from working but preserve the appearance of HTML messages. This is a common setting for many sites.

This can also be the filename of a ruleset, so you can allow them from known mailing lists or to be received by specific users.

This setting is often changed to suit site conditions.

Allow Form Tags = no

Do you want to allow <Form> tags in email messages? These are commonly use by Phishing attacks.

Available setting values include:

- yes Allow <Form> tags in the message
- no Blocks messages containing <IFrame> tags
- disarm Allow <Form> tags, but stop these tags from working.

The disarm setting will stop <Form> tags from working but preserve the appearance of HTML messages. This is a common setting for many sites.

This can also be the filename of a ruleset, so you can allow <Form> tags from known senders but ban them from everywhere else.

This setting is often changed to suit site conditions.

Allow Script Tags = no

Do you want to allow <Script> tags in email messages? These tags are often used to exploit vulnerabilities in email and web browsers.

Available setting values include:

- yes Allow < Script > tags in the message

- no Blocks messages containing < Script > tags
- disarm Allow < Script > tags, but stop these tags from working.

The disarm setting will stop < Script > tags from working but preserve the appearance of HTML messages. This is a common setting for many sites.

This can also be the filename of a ruleset, so you can allow < Script > tags from known senders but ban them from everywhere else.

This setting is often changed to suit site conditions.

Allow WebBugs = disarm

Do you want to allow <Img> tags with very small images in email messages? This is a bad idea as these are used as 'web bugs' to find out if a message has been read. make you give away information, for example such a web bug can allow a spammer to verify your email address as one that exists and is being actively read.

Available setting values include:

- yes Allow < Img > tags in the message
- disarm Allow < Img > tags, but stop these tags from working.

Disarming can be defeated; it is not 100% safe! Also you cannot block messages containing web bugs as their detection is very vulnerable to false alarms.

This setting may also be the filename of a ruleset.

This setting is often changed to suit site conditions.

Allow Object Codebase Tags = no

Do you want to allow <Object Codebase=...> tags in email messages? This can be dangerous since it leaves you unprotected against various Microsoft-specific security vulnerabilities, but may be necessary to avoid end user complaints.

This can also be the filename of a ruleset, so you can allow <Object Codebase=...> tags from known senders but ban them from everywhere else.

Available setting values include:

- yes Allow < Object Codebase=...> tags in the message
- no Blocks messages containing < Object Codebase=...> tags
- disarm Allow < Object Codebase=... > tags, but stop these tags from working.

The disarm setting will stop <Object Codebase=...> tags from working but preserve the appearance of HTML messages. This is a common setting for many sites.

Convert Dangerous HTML To Text = no

This setting interacts with the "Allow ... Tags" options above to produce the following results:

Allow (I-Frame | Codebase)Tags	Convert Dangerous HTML To Text	Action Taken on HTML Message containing HTML Tag
no	no	Blocked
no	yes	Blocked
disarm	no	Specified HTML tags disarmed

disarm	yes	Specified HTML tags disarmed
yes	no	Nothing, allowed to pass
yes	yes	All HTML tags stripped

Typically this setting does not need to be changed.

Convert HTML To Text = no

Do you want to convert all HTML messages into plain text? This is very useful for children or users who are offended by nasty things like pornographic spam.

This can also be the filename of a ruleset, so you can switch this feature on and off for particular users or domains.

Typically this setting does not need to be changed.

Attachment Filename Checking

Filename Rules = %etc-dir%/filename.rules.conf

This sets where to find the attachment filename ruleset. This ruleset is used to accept or reject file attachments based on their name, regardless of whether they are infected or not.

The structure of this file must be:

```
# This is a comment line
# A typical entry line is below
[allow|deny]    <regular expression>   <Log Text>   <User Report
text>
```

Since the Text fields may contain spaces, all fields must be separated by tabs. All fields must exist. Use a “-“(dash) if you want to leave either of the Text fields blank.

Outlook Express allows the second to last extension (just to the left of the rightmost extension) to be the associated application used to execute the file, so to be safe, very long filenames must be denied regardless of the final extension.

This setting can also be the filename of a ruleset but the ruleset file name must end in ".rules". Creating such a ruleset will allow you to switch this feature on and off for particular users or domains. See Appendix C, Practical Ruleset Examples, for further instructions.

This setting is often changed to allow certain domains and users to receive specific named attachments.

Filetype Rules = %etc-dir%/filetype.rules.conf

This sets where to find the attachment filetype ruleset. This ruleset is used to accept or reject file attachments based on the type of file, regardless of whether they are infected or not. To disable this feature, set Filetype Rules = to a blank string.

The structure of this file must be:

```
# This is a comment line
# A typical entry line is below
```

```
[allow|deny]    <regular expression>   <Log Text>   <User Report
text>
```

Since the Text fields may contain spaces, all fields must be separated by tabs. All fields must exist. Use a “-“(dash) if you want to leave either of the Text fields blank.

This setting can also be the filename of a ruleset but the ruleset file name must end in ".rules". Creating such a ruleset will allow you to switch this feature on and off for particular users or domains. . See Appendix C, Practical Ruleset Examples, for further instructions.

This setting is often changed to allow certain domains and users to receive specific types of attachments.

Reports and Responses

Quarantine Infections = yes

Do you want to store copies of the infected attachments and messages?

This can also be the filename of a ruleset, so you can switch this feature on and off for specific users or domains. There is no point quarantining most viruses these days as very few clean files are falsely identified as viruses..

Typically this setting does not need to be changed.

Quarantine Silent Viruses = no

These messages contain no useful content, so if you set this to "no" then no infections listed in your "Silent Viruses" setting will be quarantined, even if you have chosen to quarantine infections in general. The default is currently set to "yes" so the behavior is the same as it was in previous versions.

This can also be the filename of a ruleset.

Typically this setting is changed to “no”.

Quarantine Whole Message = yes

Do you want to quarantine the original *entire* message as well as just the infected attachments?

This can also be the filename of a ruleset.

Quarantine Whole Message = no

Do you want to quarantine the original *entire* message as well as just the infected attachments?

This can also be the filename of a ruleset, so you can switch this feature on and off for specific users or domains.

Typically this setting does not need to be changed. This should be changed to **yes** if you are using MailWatch

Quarantine Whole Messages As Queue Files = no

When you quarantine an entire message, do you want to store it as raw mail queue files (so you can easily send them onto users) or as human-readable files (header in one file, body in another file)?

Typically this setting does not need to be changed.

Keep Spam And MCP Archive Clean = no

Do you want to stop any virus-infected spam getting into the spam or MCP archives? If you have a system where users can release messages from the spam or MCP archives, then you probably want to stop them being able to release any infected messages, so set this to yes. It is set to no by default as it causes a small hit in performance, and many people don't allow users to access the spam quarantine. Set this to yes if there is a possibility that users can release infected messages from quarantine.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Language Strings = %report-dir%/languages.conf

Set where to find all the language dependent strings used so they can be translated into your local language.

This may also be the filename of a ruleset so you can produce different languages for different messages.

Typically this setting does not need to be changed.

Deleted Bad Content Message Report = %report-dir%/deleted.content.message.txt

Deleted Bad Filename Message Report = %report-dir%/deleted.filename.message.txt

Deleted Virus Message Report = %report-dir%/deleted.virus.message.txt

These should be set to the location of the message text sent to users when one of their attachments or a virus has been deleted from a message.

These can also be the filenames of rulesets.

Typically these settings do not need to be changed.

Stored Bad Content Message Report = %report-dir%/stored.content.message.txt

Stored Bad Filename Message Report = %report-dir%/stored.filename.message.txt

Stored Virus Message Report = %report-dir%/stored.virus.message.txt

These should be set to the location of the message text sent to users when one of their attachments has been deleted from a message and stored in the quarantine.

These can also be the filenames of rulesets.

Typically these settings do not need to be changed.

Disinfected Report = %report-dir%/disinfected.report.txt

This should be set to the location of the message text sent to users explaining the attached disinfected documents.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Inline HTML Signature = %report-dir%/inline.sig.html

Inline Text Signature = %report-dir%/inline.sig.txt

These should be set to the location of the HTML and text versions of the signature files that will be added to the end of all clean messages, if Sign Clean Messages is set to yes.

These can also be the filenames of rulesets.

Typically this setting does not need to be changed.

Inline HTML Warning = %report-dir%/inline.warning.html

Inline Text Warning = %report-dir%/inline.warning.txt

These should be set to the location of the HTML and text warnings that will be inserted at the top of messages that have had viruses removed from them.

These can also be the filenames of rulesets.

Typically these settings do not need to be changed.

Sender Content Report = %report-dir%/sender.content.report.txt

Sender Error Report = %report-dir%/sender.error.report.txt

Sender Bad Filename Report = %report-dir%/sender.filename.report.txt

Sender Virus Report = %report-dir%/sender.virus.report.txt

These should be set to the location of the messages that are delivered to the sender when they sent an email containing an error, banned content, a banned filename or a virus infection.

These can also be the filenames of rulesets.

Typically these settings do not need to be changed.

Hide Incoming Work Dir = yes

Hide the directory path from all virus scanner reports sent to users. The extra directory paths give away information about your setup and tend to confuse users.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Include Scanner Name In Reports = yes

Include the name of the virus scanner in each of the scanner reports. This also includes the translation of "MailScanner" in each of the report lines resulting from one of MailScanner's own checks such as filename, filetype or dangerous HTML content. To change the name "MailScanner", look in `reports/<your_language>/languages.conf`. Very useful if you use several virus scanners, but might not be desirable if you don't want to let your customers know which scanners you use.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Changes to Message Headers

Mail Header = X-%org-name%-MailScanner:

Add this extra header to all mail as it is processed.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

The value for this setting MUST include the colon ":" at the end and should have NO white space between the **X-** and the "**:**" at the end of the line.

Spam Header = X-%org-name%-MailScanner-SpamCheck:

Add this extra header to all messages found to be spam.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Spam Score Header = X-%org-name%-MailScanner-SpamScore:

Add this extra header if "Spam Score" = yes. The header will contain one character for every point of the SpamAssassin score or an integer, depending on your spam score settings.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Information Header = X-%org-name%-MailScanner-Information:

Add this extra header to all mail as it is processed. The content is set by the **Information Header Value** option and is intended for you to be able to insert a help URL for your users. If you don't want an information header at all, just comment out this setting or set it to be blank.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Add Envelope from Header = yes

Do you want to add the Envelope-From: header? This is very useful for tracking where spam came from as it contains the envelope sender address.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Add Envelope To Header = no

Do you want to add the Envelope-To: header? This can be useful for tracking spam destinations, but should be used with care due to possible privacy concerns with the use of Bcc: headers by users.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Envelope From Header = X-MailScanner-From:

This is the name of the Envelope From header controlled by the option above.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Spam Score Character = s

The sets the character to use in the "Spam Score Header". Do not use the following characters:

x Since users will think a score of 3 "xxx" is porn,

#	Since it will cause confusion with comments in procmail as well as MailScanner itself,
*	Since it will cause confusion with pattern matches in procmail,
.	Since it will cause confusion with pattern matches in procmail,
?	Since it will cause the users to think something went wrong.

Do use "s" as it is nice and safe and stands for "spam".

Typically this setting does not need to be changed.

SpamScore Number Instead Of Stars = no

If this option is set to yes, you will get a spam-score header showing only the value of the spam score, instead of the row of characters representing the score.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Minimum Stars If On Spam List = 0

This sets the minimum number of "Spam Score Characters" which will appear if a message triggered the **Spam List** option setting (see below) but received a very low SpamAssassin score. This means that people who only filter on the Spam Stars will still be able to catch messages which receive a very low SpamAssassin score. Set this value to 0 to disable it.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Infected Header Value = Found to be infected

Clean Header Value = Found to be clean

Disinfected Header Value = Disinfected

These values set the "Mail Header" to these values for clean, infected and disinfected messages.

These can also be the filenames of a rulesets.

Typically these settings do not need to be changed.

Information Header Value = Please contact the ISP for more information

This sets the "Information Header" to this value.

These can also be the filenames of a rulesets.

Typically this setting is customized for each site.

Detailed Spam Report = yes

Do you want the full spam report, or just a simple "spam / not spam" report?

This setting should be changed to reflect your site’s preferences.

Always Include Scores In SpamAssassin Report = yes

Do you want to include the numerical scores in the detailed SpamAssassin report, or just list the names of the scoring rules?

Typically this setting does not need to be changed.

Multiple Headers = append

This setting determines what happens when there are multiple MailScanner headers from multiple MailScanner servers in one message.

Available setting values include:

- append Append the new data to the existing header
- add Add a new header
- replace Replace the old headers with the new headers

Typically this setting does not need to be changed.

Hostname = the %org-name% MailScanner

This sets the name of this host, or a name like "the MailScanner" if you want to hide the real hostname. It is used in the Help Desk note contained in the virus warnings sent to users.

This can also be the filename of a ruleset.

Typically this setting should be changed to identify your site, for example:

Hostname = the %org-name% MailScanner at <site_name>

Sign Messages Already Processed = no

Add the **Inline HTML Signature** or **Inline Text Signature** (see below) to the end of uninfected messages?

This can also be the filename of a ruleset.

Often this setting is changed to publicize the use of MailScanner at your site.

Sign Clean Messages = no

If this is "no", then (as far as possible) messages which have already been processed by another MailScanner server will not have the clean signature added to the message. This prevents messages getting many copies of the signature as they flow through your site.

This can also be the filename of a ruleset.

This setting should be changed to reflect your site’s preferences.

Mark Infected Messages = yes

Add the **Inline HTML Warning** or **Inline Text Warning** (see below)to the top of messages that have had attachments removed from them?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Mark Unscanned Messages = yes

When a message is to not be virus-scanned, which may happen depending upon the setting of **Virus Scanning** option , especially if it is a ruleset, do you want to add a header advising the users to sign up to have their email virus-scanned by MailScanner.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed for ISP and ASP sites but other sites might consider changing this value to no.

Unscanned Header Value = Not scanned: please contact your Internet E-Mail Service Provider for details

This is the text used by the Mark Unscanned Messages option listed above.

This can also be the filename of a ruleset.

Typically this setting is customized for each site if Mark Unscanned Messages is set to yes.

Remove These Headers = X-Mozilla-Status: X-Mozilla-Status2:

If any of these headers are included in a message, they will be deleted. This is very useful for removing return-receipt requests and any headers which mean special things to your email client application. X-Mozilla-Status is bad as it allows spammers to make a message appear to have already been read, which is believed to bypass some naive spam filtering systems. Receipt requests are bad as they give any attacker confirmation that an account is active and being read. You don't want this sort of information to leak outside your corporation. So you might want to remove:

```
Disposition-Notification-To and Return-Receipt-To.
```

If you are having problems with duplicate message-id headers when you release spam from the quarantine and send it to an Exchange server, then add:

```
Message-Id.
```

Each header should end in a ":", but MailScanner will add it if you forget. Headers should be separated by commas or spaces.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Deliver Cleaned Messages = yes

Do you want to deliver messages once they have been cleaned of any viruses? By making this a ruleset, you can re-create the "Deliver From Local" facility of previous versions of MailScanner.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Notifications back to the senders of blocked messages

Notify Senders = yes

Do you want to notify the people who sent you messages containing viruses or badly-named filenames?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Notify Senders of Viruses = no

If **Notify Senders** option (above) is set to yes, do you want to notify people who sent you messages containing viruses? The standard default is "no" since most viruses now fake the sender addresses and therefore should be on the "Silent Viruses" list.

This can also be the filename of a ruleset.

This setting should almost never be changed.

Notify Senders Of Blocked Filenames Or File types = yes

If **Notify Senders** option (above) is set to yes, do you want to notify people who sent you messages containing attachments that are blocked due to their filename or file contents?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Notify Senders Of Other Blocked Content = yes

If **Notify Senders** option (above) is set to yes, do you want to notify people who sent you messages containing other blocked content, such as partial messages or messages with external bodies?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Never Notify Senders of Precedence = list bulk

If you supply a space-separated list of message "precedence" settings, then senders of those messages will not be warned about anything you rejected. This is particularly suitable for mailing lists, so that any MailScanner responses do not get sent to the entire list.

Typically this setting does not need to be changed.

Changes to the Subject: line

Scanned Modify Subject = no

When the message has been scanned but no other subject line changes have happened, do you want modify the subject line?

Available setting values include:

- no Do not modify the subject line
- start Add text to the start of the subject line
- end Add text to the end of the subject line

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Scanned Subject Text = {Scanned}

This is the text to add to the start/end of the subject line if the **Scanned Modify Subject** option (above) is set to yes.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Virus Modify Subject = yes

If the message contained a virus, do you want to modify the subject line? This makes filtering in Outlook very easy.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Virus Subject Text = {Virus?}

This is the text to add to the start/end of the subject line if the **Virus Modify Subject** option (above) is set to yes.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Filename Modify Subject = yes

If an attachment triggered a filename check, but there was nothing else wrong with the message, do you want to modify the subject line? This makes filtering in Outlook very easy.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Filename Subject Text = {Filename?}

This is the text added to the start of the subject if the **Filename Modify Subject** option (above) option is set to yes. You might want to change this so your users can see at a glance whether it just was just the filename that MailScanner rejected.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Content Modify Subject = yes

If an attachment triggered a content check, but there was nothing else wrong with the message, do you want to modify the subject line? This makes filtering in Outlook very easy.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Content Subject Text = {Blocked Content}

This is the text to add to the start of the subject if the **Content Modify Subject** option (above) is set to yes. You might want to change this so your users can see at a glance whether it just was just the content that MailScanner rejected.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Disarmed Modify Subject = yes

If HTML tags in the message were "disarmed" by using the HTML "Allow" options above with the "disarm" settings, do you want to modify the subject line?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Disarmed Subject Text = {Disarmed}

This is the text to add to the start of the subject if the **Disarmed Modify Subject** option is set to “yes”

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Phishing Modify Subject = no

If a potential phishing attack is found in the message, do you want to modify the subject line?

This can also be the filename of a ruleset.

Phishing Subject Text = {Fraud?}

This is the text to add to the start of the subject if the "Phishing Modify Subhect" option is set.

This can also be the filename of a ruleset.

Spam Modify Subject = yes

If the message is spam, do you want to modify the subject line? This makes filtering in Outlook very easy.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Spam Subject Text = {Spam?}

This is the text to add to the start of the subject if the "**Spam Modify Subject =**" option is set to yes. The exact string "_SCORE_" will be replaced by the numeric SpamAssassin score.

You might consider setting this value to **{Spam _SCORE_}** if you want to expose spam scores to your users.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

High Scoring Spam Modify Subject = yes

This is just like the **Spam Modify Subject** option above, except that it applies when the score from SpamAssassin is higher than the **High SpamAssassin Score** value (see below). The exact string "_SCORE_" will be replaced by the numeric SpamAssassin score.

You might consider setting this value to **{High Scoring Spam}** or **{High Scoring Spam _SCORE_}** if you deliver all spam to your users and want them to be able to spam and high scoring spam with different filters.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Changes to the Message Body

Warning Is Attachment = yes

When a virus or attachment is replaced by a plain-text warning, should the warning be in an attachment? If "**no**" then it will be placed in-line.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Attachment Warning Filename = %org-name%-Attachment-Warning.txt

When a virus or attachment is replaced by a plain-text warning, and that warning is an attachment, this is the filename of the warning text.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Attachment Encoding Charset = us-ascii

What character set do you want to use for the attachment If your site is located outside of the US or England, you will probably want **ISO-8859-1** instead.

This can also be the filename of a ruleset.

If your site is located outside of the US, you might need to change this setting.

Mail Archiving and Monitoring

Archive Mail = <blank>

This setting is used to control which messages are archived. It may be set to a space-separated list of any combination of:

- Email addresses to which mail should be forwarded
- Directory names where you want mail to be stored
- Names of local users (they must already exist!) to which mail will be appended in "mbox" format suitable for most UNIX mail systems.

If you implement archiving, you should be aware of the legal implications. In many jurisdictions it may be an illegal interception of a private, privileged message unless an appropriate authority has requested you to intercept the messages.

If you set this value to a ruleset, you can control exactly whose mail is archived or forwarded.

Typically this setting does not need to be changed.

Notices to System Administrators

Send Notices = yes

Notify the local system administrators ("Notices To") when any infections are found.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Notices Include Full Headers = yes

Include the full headers of each message in the notices sent to the local system administrators?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Notices Include Full Headers = no

Include the full headers of each message in the notices sent to the local system administrators?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Hide Incoming Work Dir in Notices = no

Hide the directory path from all the system administrator notices? The extra directory paths give away information about your setup, and tend to just confuse users but are still useful for local system administrators.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Notice Signature = \nMailScanner\nEmail Virus Scanner\nwww.mailscanner.info

The signature to add to the bottom of notices to system administrators. To insert a line-break in the signature, use the sequence "**\n**".

This can also be the filename of a ruleset.

Often this setting is customized for a site.

Notices From = MailScanner

The visible part of the email address used in the "From:" line of the notices. The <user@domain> part of the email address is set to the "Local Postmaster" setting.

This can also be the filename of a ruleset.

Often this setting is customized for a site, i.e. MailScanner at <site_name>

Notices to = postmaster

Where to send MailScanner notices to system administrators.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed, but if you are handling mails for multiple domains, you might want to set this to a ruleset.

Local Postmaster = postmaster

This setting is used as the "From" address in virus warnings sent to users.

This can also be the filename of a ruleset.

Often this setting is customized for a site, i.e. helpdesk@sitename.com

Spam Detection and Virus Scanner Definitions

Spam List Definitions = %etc-dir%/spam.lists.conf

This is the name of the file that translates the names of the Spam List values (below) to the real DNS names of the spam blacklists. The

`%etc-dir%/spam.lists.conf` file is used only by MailScanner and rarely needs to be modified. You need to modify this file only if you want to add additional RBL sites for use by the MailScanner **Spam List** or **Spam Domains** settings that are not already listed in this file.

Typically this setting should not be changed.

Virus Scanner Definitions = %etc-dir%/virus.scanners.conf

This is the name of the file that translates the names of the virus scanners into the commands that have to be run to do the actual scanning.

Typically this setting should not be changed.

Spam Detection and Spam Lists (DNS Blacklists)

Spam Checks = yes

Do you want to check messages to see if they are spam?

If you set this value to no then NO spam checks will be done at all. This includes both MailScanner's own checks and SpamAssassin. If you want to just disable MailScanner's "Spam List" feature then set **Spam List =** and **Spam Domains =** to a blank string (an empty list) in the settings below.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Spam List = # MAPS-RBL+ costs money (except .ac.uk)

This is the list of spam blacklists (RBLs) which you are using in MailScanner

This value is typically customized for each site. See the **Spam List Definitions** file (see above) for more information about what values may be used here.

RBLs may be used in any combination of three methods:

1. Blocking at the MTA level: This is an MTA configuration level option. Messages blocked at the MTA level are not accepted for delivery. Blocking at this level reduces the load on you system but you assume the risk of rejecting some amount of good, legitimate email.

2. MailScanner RBL checking: MailScanner checks to see if the sender or a relay of the message is listed in **Spam List =** or **Spam Domains =.** If found in these lists, the message is marked as spam. If the message is found in multiple RBL lists, the Spam **Lists To Reach High Score =** setting is used to determine if the message should be treated as High Scoring Spam.

3. SpamAssassin scoring: SpamAssassin by default checks various RBL and adds to the spam score each time sender or relay of the message is found in an RBL.

This can also be the filename of a ruleset.

Often this setting is changed to be <blank> to enable RBL checking only by SpamAssassin.

Spam Domain List = <blank>

This is the list of spam domain blacklists (such as the "rfc-ignorant" domains) which are used by MailScanner.

See the **Spam List Definitions file** option (see above) for more information about what values may be used here.

Often this setting left <blank> to enable RBL checking only by SpamAssassin.

Spam Lists To Be Spam = 1

If a message appears in at least this number of

If a message appears in at least this number of **Spam Lists** and/or **Spam Domain Lists** (as defined above), then the message will be treated as spam and so the "Spam Actions" will happen, unless the message reaches the levels for "High Scoring Spam". By default this is set to 1 to mimic the previous behavior, which means that appearing in any "Spam Lists" will cause the message to be treated as spam.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Spam Lists To Reach High Score = 3

If a message appears in at least this number of **Spam Lists** and/or **Spam Domain Lists** (as defined above), then the message will be treated as High Scoring Spam and the **High Scoring Spam Actions** will happen. If you use RBL checking in MailScanner you probably want to set this to 2. Setting this value to 5 is high enough that it will never happen unless you a large number of Spam Lists.

See the **Spam List Definitions file** (see above) for more information about what values may be used here.

This can also be the filename of a ruleset.

If **Spam List** and **Spam Domains** options are set to a blank string this setting is not used.

Spam List Timeout = 10

If an individual **Spam List** or **Spam Domain List** check takes longer than this value (in seconds), the check is abandoned and the timeout noted in the log.

Permissible values = integer

Typically this setting does not need to be changed.

Max Spam List Timeouts = 7

The maximum number of timeouts caused by any individual **Spam List** or **Spam Domain List** before it is marked as "unavailable". Once so marked, the marked list will be ignored until the next automatic re-start. Also see the **Restart Every** option above for the longest time it will wait.

Permissible values = integer

Typically this setting does not need to be changed.

Spam List Timeouts History = 10

The total number of Spam List attempts during which the **Max Spam List Timeouts** option will cause the spam list to be marked as "unavailable". See **Max Spam List Timeouts** above for more information.

The default values of 5 and 7 mean that 5 timeouts in any sequence of 7 attempts will cause the list to be marked as "unavailable" until the next periodic restart. Also see the **Restart Every** option above for the longest time it will wait.

Permissible values = integer

Typically this setting does not need to be changed.

Is Definitely Not Spam = %rules-dir%/spam.whitelist.rules

This option sets the location of the Spam Whitelist ruleset. Anything in this ruleset whose value is "yes" will never be marked as spam.

This is always the filename of a ruleset.

Typically this setting does not need to be changed.

Is Definitely Spam = no

If this value points to a ruleset, that ruleset will be used to determine which sites are blacklisted. See Appendix C, Practical ruleset Examples for instructions on changing the value to a ruleset.

This can also be the filename of a ruleset.

This value is typically customized for each site. A ruleset similar to `spam.whitelist.rules` is created in %rules-dir%. Sites listed in this file will be treated as defined by the Definite Spam Is High Scoring setting (see below)

Definite Spam Is High Scoring = no

Setting this option to yes results in spam found in the blacklist being treated as High Scoring Spam in the **High Spam Actions** (see below). Setting this value to no means that it will be treated as "normal" spam.

This can also be the filename of a ruleset.

Many Sites typically set this value to yes.

Ignore Spam Whitelist If Recipients Exceed = 20

Spammers have learned that they can get their message through by sending a message to many recipients, one of which chooses to whitelist everything coming to them, including the spammer. If a message arrives with more than this number of recipients, ignore the "Is Definitely Not Spam" whitelist.

Typically this setting does not need to be changed.

SpamAssassin

Use SpamAssassin = no

Do you want to find spam using the "SpamAssassin" package?

This can also be the filename of a ruleset.

Typically this setting is changed to yes to enable SpamAssassin

Hint: point this value to a ruleset to turn off SpamAssassin checking for specific users or domains. Set the configuration variables **Spam Checks** and **Dangerous Content Checks** to **no** or a ruleset to turn off all MailScanner spam checks

Max SpamAssassin Size = 30000

SpamAssassin is not very fast when scanning huge messages, so messages bigger than this value will be truncated to this length for SpamAssassin testing. The original message will not be affected by this. This value is a good compromise as very few spam messages are bigger than this (it takes too long to send out large spam messages).

Permissible values = integers

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Required SpamAssassin Score = 6

This replaces the SpamAssassin configuration value 'required_hits'. If a message achieves a SpamAssassin score higher than this value, it is spam. Also see the **High SpamAssassin Score** configuration option (below).

Permissible values = nn.nn where n = integer

This can also be the filename of a ruleset.

Typically this setting is changed at every site. The “right” value depends on the number and types (DCC, Pyzor, Razor, RBLs, etc.) of spam checking methods implemented at your site. Some general rules for setting this value:

5 Mildly Aggressive, some false positives will result

6 Normal Setting

7+ Or Above. Few false positives but a lot more spam

High SpamAssassin Score = 10

If a message achieves a SpamAssassin score higher than this value, its fate will be determined using **High Scoring Spam Actions** configuration option (below).

Permissible values = nn.nn where n = integer

This can also be the filename of a ruleset.

Typically this setting is changed at every site. Again the “right” value depends on the number and types (DCC, Pyzor, Razor, RBLs, etc.) of spam checking methods implemented at your site. Some general rules for setting this value:

8 Aggressive, but end users will see less spam

10 Normal Setting

12+ More spam will be seen by the end users

SpamAssassin Auto Whitelist = no

Setting this option to **yes** will enable the automatic SpamAssassin whitelisting functions. Since some spammer have been able to abuse this function (and poison Bayes databases as a result), this value should be left set to no.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

SpamAssassin Prefs File = %etc-dir%/spam.assassin.prefs.conf

This value sets the location of the SpamAssassin user_prefs file. See Chapter 6 for configuring SpamAssassin preferences.

Typically this setting does not need to be changed.

SpamAssassin Timeout = 75

If SpamAssassin takes longer than this value, in seconds, the SpamAssassin check is abandoned and the timeout is noted in the logs.

Permissible values = integer

Typically this setting does not need to be changed.

“SpamAssassin timeout” messages in your logs indicates a problem and correct spam detection is probably not occurring. See Chapter 7 Tips, Tuning and Troubleshooting to diagnose this problem.

Max SpamAssassin Timeouts = 10

If consecutive SpamAssassin time outs exceed this value, then SpamAssassin will be marked as "unavailable" (SpamAssassin spam detection will stop, but mail will flow) until the next MailScanner re-start.

Permissible values = integer

Typically this setting does not need to be changed.

SpamAssassin Timeouts History = 30

The total number of SpamAssassin attempts during which "Max SpamAssassin Timeouts" will cause SpamAssassin to be marked as "unavailable". The default values of 10 (**Max SpamAssassin Timeouts**) and 30 (**SpamAssassin Timeouts History**) means that 10 timeouts in any sequence of 30 attempts will trigger the behavior described above, until the next periodic restart. Also see the **Restart Every** option.

Permissible values = integer

Typically this setting does not need to be changed.

Check SpamAssassin If On Spam List = yes

If the message sender is on any of the Spam Lists, do you still want to do the SpamAssassin checks? Setting this to **no** will reduce the load on your server, but will stop SpamAssassin from scoring messages if the message triggers the MailScanner RBL checks.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Always Include SpamAssassin Report = no

Do you want to always include the Spam Report in the SpamCheck header, even if the message wasn't spam?

This can also be the filename of a ruleset.

Many sites change this setting is changed to **yes** to allow spam score checking of messages that should have been marked as spam.

Spam Score = yes

Do you want to include the "Spam Score" header? This shows 1 character (**Spam Score Character**) for every point of the SpamAssassin score. This allows users to filter their mail using whatever SpamAssassin threshold they want. For example, they just look for "sssss" for every message whose score is > 5.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Rebuild Bayes Every = 0

If you are using the Bayesian statistics engine on a busy server, you may well need to force a Bayesian database rebuild and expiry at regular intervals. The value 0 disables this function; the value of 86400 rebuilds the Bayes database once a day.

This setting is often changed. See Chapter 6, SpamAssassin Configuration.

Wait During Bayes Rebuild = no

The Bayesian database rebuilds and expiry may take a 2 or 3 minutes to complete. During this time you can either wait, or simply disable SpamAssassin checks until it has completed.

Setting this value to **yes** will disable MailScanner processing during the rebuild

Typically this setting does not need to be changed.

Custom Spam Scanner Plugin

Use Custom Spam Scanner = no

Use the Custom Spam Scanner. This is code you will have to write yourself, a function called "GenericSpamScanner" stored in the file:

`MailScanner/lib/MailScanner/CustomFunctions/GenericSpamScanner.pm`

This function will be passed:

- $IP The numeric IP address of the system on the remote end of the SMTP connections
- $From The address of the envelope sender of the message
- $To A perl reference to the envelope recipients of the message
- $Message A perl reference to the list of line of the message

A sample function is included in a file of the same name in the distribution. This sample function also includes code to show you how to make it run an external program to produce a spam score.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Max Custom Spam Scanner Size = 20000

How much of the message should be passed tot he Custom Spam Scanner. Most spam tools only need the first 20 KB of the message to determine if it is spam or not. Passing more than is unnecessary and only slows things down.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Custom Spam Scanner Timeout = 20

How long should the custom spam scanner take to run? If it takes more seconds than this, then it should be considered to have crashed and should be killed. This helps to prevent denial-of-service attacks.

This setting cannot be the filename of a ruleset. It may only be set to an integer.

Typically this setting does not need to be changed.

Max Custom Spam Scanner Timeouts = 10

How long should the custom spam scanner take to run? If it takes more seconds than this, then it should be considered to have crashed and should be killed. This stops denial-of-service attacks.

This setting cannot be the filename of a ruleset. It may only be set to an integer.

Typically this setting does not need to be changed.

Custom Spam Scanner Timeout History = 20

The total number of SpamAssassin attempts during which "Max SpamAssassin Timeouts" will cause SpamAssassin to be marked as "unavailable". The default values of 10 (**Custom Spam Scanner Timeouts**) and 20 (**Custom Spam Scanner Timeouts History**) means that 10 timeouts in any sequence of 20 attempts will trigger the behavior described above, until the next periodic restart. Also see the **Restart Every** option.

This setting cannot be the filename of a ruleset. It may only be set to an integer.

Typically this setting does not need to be changed.

What to do with spam

Spam Actions = deliver

This is a list of actions to take when a message is spam. It can be white space separated list of any combination of the following:

- deliver — Deliver the message as normal
- delete — Delete the message
- store — Store the message in the quarantine
- bounce — Send a rejection message back to the sender (not recommended)
- forward user@domain.com — Forward a copy of the message to user@domain.com
- striphtml — Convert all in-line HTML content to plain text. You need to specify "deliver" after striphtml for the message to reach the intended recipient.
- attachment — Convert the original message into an attachment of the message. This means the user has to take an extra step to open the spam, and stops "web bugs" very effectively. You need to specify "deliver" after “attachment” for the message to reach the intended recipient.
- notify — Send the recipients a short notification that spam addressed to them was not delivered. They can then take action to request retrieval of the original message if they think it was not spam.

This can also be the filename of a ruleset.

Most sites set this value to deliver or attachment deliver.

High Scoring Spam Actions = deliver

This is a list of actions to take when a message is high scoring spam. It can be white space separated list of any combination of the following:

- deliver — Deliver the message as normal
- delete — Delete the message
- store — Store the message in the quarantine
- bounce — Send a rejection message back to the sender (not recommended)

- forward user@domain.com — Forward a copy of the message to user@domain.com
- striphtml — Convert all in-line HTML content to plain text. You need to specify "deliver" after striphtml for the message to reach the intended recipient.
- attachment — Convert the original message into an attachment of the message. This means the user has to take an extra step to open the spam, and stops "web bugs" very effectively . You need to specify "deliver" after “attachment” for the message to reach the intended recipient.
- notify — Send the recipients a short notification that spam addressed to them was not delivered. They can then take action to request retrieval of the original message if they think it was not spam.

This can also be the filename of a ruleset.

Many sites set this value to store or delete.

Non Spam Actions = deliver

This operates like the **Spam Actions** option above, except it applies messages that are not spam and would normally be delivered:

- deliver — Deliver the message as normal
- delete — Delete the message
- store — Store the message in the quarantine
- forward user@domain.com — Forward a copy of the message to user@domain.com
- striphtml — Convert all in-line HTML content to plain text. You need to specify "deliver" after striphtml for the message to reach the intended recipient.

This can also be the filename of a ruleset.

Typically this value is not changed.

Sender Spam Report = %report-dir%/sender.spam.report.txt

Sender Spam List Report = %report-dir%/sender.spam.rbl.report.txt

Sender SpamAssassin Report = %report-dir%/sender.spam.sa.report.txt

There are three Spam Reports:

- Sender Spam Report — Sent when a message triggers both a Spam List and SpamAssassin
- Sender Spam List Report — Sent when a message triggers a Spam List
- Sender SpamAssassin Report — Sent when a message triggers SpamAssassin.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Inline Spam Warning = %report-dir%/inline.spam.warning.txt

If you use the 'attachment' Spam Action or High Scoring Spam Action this value is the location of inline spam report that is inserted at the top of the message.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Recipient Spam Report = %report-dir%/recipient.spam.report.txt

If you use the 'notify' Spam Action or High Scoring Spam Action this value is the location of the notification message that is sent to the original recipients of the message.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Enable Spam Bounce = %rules-dir%/bounce.rules

You can use this ruleset to enable the "bounce" Spam Action. You must ONLY enable this for mail from sites with which you have agreed to bounce possible spam. Use it on low-scoring spam only (<10) and only to your regular customers for use in the rare case that a message is tagged as spam when it shouldn't have been.

Beware that many sites will automatically delete the bounce messages created by using this option unless you have agreed this with them in advance. If you enable this, be prepared to handle the irate responses from people to whom you are essentially sending more spam!

This can also be the filename of a ruleset.

Typically this setting should never be changed.

Bounce Spam As Attachment = no

When you bounce a spam message back to the sender, do you want to encapsulate it in another message, rather like the "attachment" option when delivering spam to the original recipient?

> “If you enable this option, be sure to whitelist your local server, i.e. 127.0.0.1 or the spam bounce message will be detected as spam again, which will cause another spam bounce and so on until your mail queues fill up and your server crashes!

This can also be the filename of a ruleset.

Typically this setting should not be changed.

Logging

Syslog Facility = mail

This is the syslog "facility" name that MailScanner uses. If you don't know what a syslog facility name is, then either don't change this value or else please read `man syslog.conf`. The default value of "mail" will cause the MailScanner logs to go into the same place as all your other mail logs.

Typically this setting does not need to be changed.

Log Speed = no

Do you want to log the processing speed for each section of the code for a batch? This can be very useful for diagnosing speed problems, particularly in spam checking.

Typically this setting does not need to be changed unless you are troubleshooting speed or delivery problems. This may need to be set to **yes** if you are using mailscanner-mrtg.

Log Spam = no

Do you want all spam to be logged? This can be useful if you want to gather spam statistics from your logs, but can increase the system load substantially if you receive a lot of spam.

Typically this setting does not need to be changed unless you are troubleshooting speed or delivery problems. Many sites change this value to yes to gather spam statistics from logs.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Log Non Spam = no

Do you want all non-spam to be logged? This can be useful if you want to gather spam statistics from your logs, but can increase the system load substantially.

Typically this setting does not need to be changed unless you are troubleshooting spam detection problems. Many sites change this value to yes to gather spam statistics from logs.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Log Permitted Filenames = no

Log all the filenames that are allowed by the Filename Rules, or just the filenames that are denied?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Log Permitted Filetypes = no

Log all the filenames that are allowed by the Filetype Rules, or just the filetypes that are denied?

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Log Silent Viruses = no

Log all occurrences of "Silent Viruses" as defined above?

This cannot be the filename of a ruleset. Only a simple yes / no value is allowed

Typically this setting does not need to be changed.

Log Dangerous HTML Tags = yes

Log all occurrences of HTML tags found in messages that can be blocked. This will help you build up your whitelist of message sources for which

particular HTML tags should be allowed, such as mail from newsletters and daily cartoon strips.

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

Advanced SpamAssassin Settings

If you are using Postfix you may definitely need to use some of the settings below, since the home directory for the "postfix" user cannot be written to by the "postfix" user.
You may also need to use these settings if you have installed SpamAssassin somewhere other than the default location.

SpamAssassin User State Dir = <blank>

The per-user files (bayes, auto-whitelist, user_prefs) are looked for in this directory and in `~/.spamassassin/` (where ~ is the home directory of the user running the MailScanner processes). If this is unset (left blank) then no additional directories other than `~/.spamassassin` are searched.

If you are using Postfix, you probably want to set this value to:

```
SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin
```

And then run the following commands:

```
mkdir /var/spool/MailScanner/spamassassin
chown postfix.postfix /var/spool/MailScanner/spamassassin
```

Typically this setting does not need to be changed unless you are using Postfix.

SpamAssassin Install Prefix = <blank>

This setting is useful if SpamAssassin is installed in an unusual place, e.g. `/opt/MailScanner`. The install prefix is used to find some fallback directories if neither of the following two settings work. If this is set then it adds to the list of places that are searched; otherwise it has no effect.

Typically this setting does not need to be changed.

SpamAssassin Site Rules Dir = /etc/mail/spamassassin

The SpamAssassin site rules are searched for in this location.

Typically this setting does not need to be changed.

SpamAssassin Local Rules Dir = <blank>

The local SpamAssassin rules are searched for in this directory, and in `<prefix>/share/spamassassin`, `/usr/local/share/spamassassin`, `/usr/share/spamassassin`, and possibly other directories. If this is set it adds to the list of places that are searched; otherwise it has no effect.

Typically this setting does not need to be changed.

SpamAssassin Default Rules Dir = <blank>

The default SpamAssassin rules are searched for in this directory, and in `<prefix>/share/spamassassin`, `/usr/local/share/spamassassin`, `/usr/share/spamassassin`, and possibly other directories. If this is set it adds to the list of places that are searched; otherwise it has no effect.

Typically this setting does not need to be changed.

MCP (Message Content Protection)

This scans text and HTML messages segments for any banned text, using a 2nd copy of SpamAssassin to provide the searching abilities. This 2nd copy has its own entire set of rules, preferences and settings. When used together with the patches for SpamAssassin, it can also check the content of attachments such as office documents. For more information please see:

http://www.sng.ecs.soton.ac.uk/mailscanner/install/mcp/

MCP Checks = no

Should MCP Checks be used?

This setting can be the filename of a ruleset.

Typically this setting does not need to be changed.

First Check = mcp

Do the spam checks first or the MCP checks first?

This cannot be the filename of a ruleset, only a fixed value, **mcp** or **spam**.

Typically this setting does not need to be changed.

MCP Required SpamAssassin Score = 1

If a message achieves an MCP score higher than this value, it is MCP. Also see the **MCP High SpamAssassin Score** configuration option (below).

Permissible values = nn.nn where n = integer

This can also be the filename of a ruleset.

This value should be tailored to suit site conditions if MCP is enabled.

MCP High SpamAssassin Score = 10

If a message achieves a MCP High SpamAssassin score higher than this value, it's delivery options will be determined using **High Scoring MCP Actions** configuration option (below).

Permissible values = nn.nn where n = integer

This can also be the filename of a ruleset.

This value should be tailored to suit site conditions if MCP is enabled.

MCP Error Score = 1

This is the score given the message if the MCP checks failed. This gives you control over what you want to do in the case where the checks failed. If you set it to **0** it will fail "open", i.e. let the message through. If you set it to at least your MCP Required SpamAssassin Score then it will fail "closed", i.e. block the message as if it was caught by MCP.

Permissible values = nn.nn where n = integer

This can also be the filename of a ruleset.

This value should be tailored to suit site conditions if MCP is enabled.

MCP Header = X-%org-name%-MailScanner-MCPCheck:

Add this extra header to all messages found to be MCP.

This can also be the filename of a ruleset.

Typically this value does not need to be changed.

Non MCP Actions = deliver

This is a list of actions to take when a message is MCP. It can be white space separated list of any combination of the following:

- deliver — Deliver the message as normal
- delete — Delete the message
- store — Store the message in the quarantine
- bounce — Send a rejection message back to the sender (not recommended)
- forward user@domain.com — Forward a copy of the message to user@domain.com
- striphtml — Convert all in-line HTML content to plain text. You need to specify "deliver" after striphtml for the message to reach the intended recipient.
- attachment — Convert the original message into an attachment of the message. This means the user has to take an extra step to open the spam, and stops "web bugs" very effectively. You need to specify "deliver" after “attachment” for the message to reach the intended recipient.
- notify — Send the recipients a short notification that spam addressed to them was not delivered. They can then take action to request retrieval of the original message if they think it was not spam.

This can also be the filename of a ruleset.

This value should be tailored to suit site conditions if MCP is enabled.

High Scoring MCP Actions = deliver

This is a list of actions to take when a message is MCP. It can be white space separated list of any combination of the following:

- deliver — Deliver the message as normal
- delete — Delete the message
- store — Store the message in the quarantine
- bounce — Send a rejection message back to the sender (not recommended)
- forward user@domain.com — Forward a copy of the message to user@domain.com
- striphtml — Convert all in-line HTML content to plain text. You need to specify "deliver" after striphtml for the message to reach the intended recipient.
- attachment — Convert the original message into an attachment of the message. This means the user has to take an extra step to open the spam, and stops "web bugs" very effectively. You need to specify "deliver" after “attachment” for the message to reach the intended recipient.

- notify — Send the recipients a short notification that spam addressed to them was not delivered. They can then take action to request retrieval of the original message if they think it was not spam.

This can also be the filename of a ruleset.

This value should be tailored to suit site conditions if MCP is enabled.

MCP Actions = deliver

This is a list of actions to take when a message is MCP. It can be white space separated list of any combination of the following:

- deliver — Deliver the message as normal
- delete — Delete the message
- store — Store the message in the quarantine
- bounce — Send a rejection message back to the sender (not recommended)
- forward user@domain.com — Forward a copy of the message to user@domain.com
- striphtml — Convert all in-line HTML content to plain text. You need to specify "deliver" after striphtml for the message to reach the intended recipient.
- attachment — Convert the original message into an attachment of the message. This means the user has to take an extra step to open the spam, and stops "web bugs" very effectively. You need to specify "deliver" after “attachment” for the message to reach the intended recipient.
- notify — Send the recipients a short notification that spam addressed to them was not delivered. They can then take action to request retrieval of the original message if they think it was not spam.

This can also be the filename of a ruleset.

This value should be tailored to suit site conditions if MCP is enabled.

Bounce MCP As Attachment = no

When you bounce a MCP message back to the sender, do you want to encapsulate it in another message, rather like the "attachment" option when delivering spam to the original recipient?

“If you enable this option, be sure to whitelist your local server, i.e. 127.0.0.1 or the MCP bounce message will be detected as MCP again, which will cause another MCP bounce and so on until your mail queues fill up and your server crashes!

This can also be the filename of a ruleset.

Typically this setting should not be changed.

Is Definitely MCP = no

If this value points to a ruleset, that ruleset will be used to determine which sites or senders are always marked as MCP. See Appendix C, Practical Ruleset Examples for instructions on changing the value to a ruleset.

This can also be the filename of a ruleset.

This value is typically customized for each site only if MCP is enabled. A ruleset similar to `spam.blacklist.rules` is created in %rules-dir%. Sites listed in this file will be treated as defined by the Definite MCP Is High Scoring setting (see below).

`Is Definitely Not MCP = no`

If this value points to a ruleset, that ruleset will be used to determine which sites or senders are never marked as MCP. See Appendix C, Practical Ruleset Examples for instructions on changing the value to a ruleset.

This can also be the filename of a ruleset.

This value is typically customized for each site only if MCP is enabled. A ruleset similar to `spam.blacklist.rules` is created in %rules-dir%. Sites listed in this file will be treated as defined by the Definite MCP Is High Scoring setting (see below).

`Definite MCP Is High Scoring = no`

Setting this to **`yes`** results in MCP found in the blacklist being treated as High Scoring MCP in the **`High Scoring MCP Actions`** (see Above). Setting the value to **`no`** means that it will be treated as "normal" MCP.

This can also be the filename of a ruleset.

Many Sites typically set this value to yes.

`Always Include MCP Report = no`

Do you want to always include the MCP Report in the MCPCheck header, even if the message wasn't MCP?

This can also be the filename of a ruleset.

If MCP is enabled, some sites change this setting is changed to **`yes`** to allow MCP score checking of messages that should have been marked as MCP.

`Detailed MCP Report = yes`

Do you want the full MCP report, or just a simple "MCP / not MCP" report?

If MCP is enabled, this setting should be changed to reflect your site’s preferences.

`Always Include Scores In MCP Report = yes`

Do you want to include the numerical scores in the detailed MCP report, or just list the names of the scores?

Typically this setting does not need to be changed.

`MCP Max SpamAssassin Timeouts = 20`

If consecutive MCP SpamAssassin time outs exceed this value, then MCP SpamAssassin will be marked as "unavailable" (MCP SpamAssassin spam detection will stop, but mail will flow) until the next MailScanner re-start.

Permissible values = integer

Typically this setting does not need to be changed.

MCP Max SpamAssassin Size = 100000

SpamAssassin is not very fast when scanning huge messages, so messages bigger than this value will be truncated to this length for MCP SpamAssassin testing. The original message will not be affected by this. This value is a good compromise and its value needs to be carefully considered if MCP is enabled.

Permissible values = integers

This can also be the filename of a ruleset.

Typically this setting does need to be changed if MCP is enabled.

MCP SpamAssassin Timeout = 10

If MCP SpamAssassin takes longer than this value, in seconds, the MCP SpamAssassin check is abandoned and the timeout is noted in the logs.

Permissible values = integer

Typically this setting does need to be changed if MCP Is enabled.

MCP SpamAssassin Prefs File =
%etc-dir%/mcp.spam.assassin.prefs.conf

This value sets the location of the MCP SpamAssassin user_prefs file. See Chapter 6 for configuring SpamAssassin preferences.

Typically this setting does not need to be changed.

MCP SpamAssassin User State Dir = <blank>

The per-user files for MCP checking (bayes, auto-whitelist, user_prefs) are looked for in this directory and in `~/.spamassassin/` (where ~ is the home directory of the user running the MailScanner processes). If this is unset (left blank) then no additional directories other than `~/.spamassassin` are searched. If you are using Postfix, you probably want to set this value to:

```
MCP SpamAssassin User State Dir = /var/spool/MailScanner/mcp
```

and then run the following commands:

```
mkdir /var/spool/MailScanner/mcp
chown postfix.postfix /var/spool/MailScanner/mcp
```

Typically this setting does not need to be changed unless you are using Postfix.

MCP SpamAssassin Local Rules Dir = %mcp-dir%

The local MCP SpamAssassin rules are searched for in this directory. If this is set it adds to the locations that will be searched for MCP SpamAssassin.

Typically this setting does not need to be changed.

MCP SpamAssassin Default Rules Dir = %mcp-dir%

The default MCP SpamAssassin rules are searched for in this directory. If this is set it changes the location where the default MCP SpamAssassin rules are located.

Typically this setting does not need to be changed.

MCP SpamAssassin Install Prefix = %mcp-dir%

This option specifies the location of the MCP SpamAssassin installation directory.

Typically this setting does not need to be changed.

Recipient MCP Report =

%report-dir%/recipient.mcp.report.txt

This option specifies the location of the MCP SpamAssassin report that is sent to the Recipient of a message that is determined to be MCP.

Typically this setting does not need to be changed.

Sender MCP Report = %report-dir%/sender.mcp.report.txt

This option specifies the location of the MCP SpamAssassin report that is sent to the Recipient of a message that is determined to be MCP.

Typically this setting does not need to be changed.

Advanced Settings

Please don't change anything below this unless you really know what you are doing, or unless MailScanner has complained about your "Minimum Code Status" setting (very unusual).

Use Default Rules With Multiple Recipients = no

When trying to work out the value of configuration parameters which are using a ruleset, this controls the behavior when a rule is checking the "To:" addresses.

If this option is set to yes, then the following happens when checking the ruleset:

- 1 recipient. Same behavior as normal.
- Several recipients, but all in the same domain (domain.com for example). The rules are checked for one that matches the string "*@domain.com".
- Several recipients, not all in the same domain. The rules are checked for one that matches the string "*@*".

If this option is set to **no**, then some rules will use the result they get from the first matching rule for any of the recipients of a message, so the exact value cannot be predicted for messages with more than 1 recipient.

This value cannot be the filename of a ruleset.

Typically this setting does not need to be changed.

Spam Score Number Format = %d

When putting the value of the spam score of a message into the headers,how do you want to format it? If you don't know how to use sprintf() or printf() in C, please *do not modify* this value. A few examples for you:

%d ==> 12

%5.2f ==> 12.34

%05.1f ==> 012.3

This can also be the filename of a ruleset.

Typically this setting does not need to be changed.

MailScanner Version Number = 4.43.8

This is the version number of the MailScanner distribution that created this configuration file.

Please do not change this value. It will automatically be changed by the upgrade script.

Debug = no

Set Debug to **yes** to stop MailScanner from running as a daemon and just process one batch of messages and then exit. See http://wiki.mailscanner.info/doku.php?id=documentation:test_troubleshoot:spamassassin:timeouts. Don't forget to set it back to yes after troubleshooting!

Typically this setting does not need to be changed. It is used only for troubleshooting.

Debug SpamAssassin = no

Do you want to debug SpamAssassin from within MailScanner?

Typically this setting does not need to be changed. It is used only for troubleshooting.

Run In Foreground = no

Set Run In Foreground to **yes** if you want MailScanner to operate normally in foreground (and not as a background daemon). Use this if you are controlling the execution of MailScanner with a tool like DJB's 'supervise' (see http://cr.yp.to/daemontools.html).

Typically this setting does not need to be changed.

#LDAP Server = localhost

#LDAP Base = o=fsl

#LDAP Site = default

If you are using an LDAP server to read the configuration, these Configuration settings should be uncommented and the values changed to those appropriate for your site. The values provide the details required for the LDAP connection. The connection is anonymous.

Typically this setting does not need to be changed.

Always Looked Up Last = no

This option is intended for people who want to log more information about messages than what is written to syslog. It is intended to be used with a Custom Function which has the side-effect of logging information, perhaps to

an SQL database, or any other processing you want to do after each message is processed. The default value of **no** disables this function. If you want to use Custom Functions, please read `MyExample.pm` file typically located in `/usr/lib/MailScanner/Mailscanner/CustomFunctions`.

If MailWatch is installed this is typically changed to:

`Always Looked Up Last = &MailWatchLogging`

This setting does not need to be changed unless MailWatch or other Custom Functions are installed.

`Deliver In Background = yes`

When attempting delivery of outgoing messages, should we do it in the background or wait for it to complete? The danger of doing it in the background is that the machine load goes ever upwards while all the slow sendmail processes run to completion. However, running it in the foreground may cause the mail server to run too slowly.

Typically this setting does not need to be changed.

`Delivery Method = batch`

Attempt immediate delivery of messages, or just place them in the outgoing queue for the MTA to deliver when it wants to?

Permissible settings for this value are:

- batch attempt delivery of messages, in batches of up to 20 at once
- queue just place them in the queue and let the MTA find them

This can also be the filename of a ruleset. For example, you could use a ruleset to insure that messages coming to you are immediately delivered, while messages going to any other site are just placed in the queue to handle the case the remote delivery is very slow.

Typically this setting should not be changed.

`Split Exim Spool = no`

Are you using Exim with split spool directories? If you don't understand this question, the answer is probably "no". Refer to the Exim documentation for more information about split spool directories.

Typically this setting does not need to be changed.

`Lockfile Dir = /tmp`

This describes where to put the virus scanning engine lock files. These lock files are used between MailScanner and the virus signature "autoupdate" scripts, to ensure that they aren't both working at the same time (which could cause MailScanner to let a virus through).

Typically this setting should not be changed.

`Custom Functions Dir =`
`/usr/lib/MailScanner/MailScanner/CustomFunctions`

This describes where to put the code for your "Custom Functions". No code in this directory should be over-written by the installation or upgrade process. All files starting with "." or ending with ".rpmnew" will be ignored, all other files will be compiled and may be used with Custom Functions.

Typically this setting should not be changed.

Lock Type = flock

How to lock spool files. Don't set (uncomment) this value unless you *know* you need to. For sendmail (8.12.x or older), it defaults to "flock". For Exim, it defaults to "posix". No other type is implemented.

Typically this setting should be changed to "posix" for Sendmail version 8.13.X.

Minimum Code Status = supported

The value sets minimum acceptable code stability status. If we come across code that's not at least as stable as this, MailScanner complains and may become unstable. This is currently only used to check that you don't end up using untested virus scanner support code without realizing it.

Permissible settings for this value are:

- none — There may not even be any code.
- unsupported — Code may be completely untested, a contributed dirty hack, anything, really.
- alpha — Code is pretty well untested. Don't assume it will work.
- beta — Code is tested a bit. It should work.
- supported — Code should be reliable.

Don't even *think* about setting this to anything other than "beta" or "supported" on a system that receives real mail until you have tested it yourself and are happy that it is all working as you expect it to. Don't set it to anything other than "supported" on a system that could ever receive important mail.

Please READ and UNDERSTAND the above text BEFORE changing this value.

Typically this setting should never be changed.

Chapter 4

SpamAssassin Configuration

This chapter will explain how to configure SpamAssassin from within MailScanner. When MailScanner calls SpamAssassin, messages scanning and how rules are applied is a bit different than running SpamAssassin from procmail or Milter.

While MailScanner will support older versions of SpamAssassin, it is strongly recommend that you install or upgrade to the latest version of MailScanner to obtain the best anti-spam results.

If configured to use SpamAssassin, MailScanner calls SpamAssassin once for each batch of messages not once for each message. A quick look at the MailScanner Process Flow diagram in Chapter 1 shows that a MailScanner child process picks up a batch of messages from the incoming mail queue and first runs its own RBL checks on the messages in the batch. If MailScanner is configured to use SpamAssassin, it then calls SpamAssassin, by directly calling the SpamAssassin Perl modules, not the executable spamassassin or spamd, and runs the SpamAssassin rules against this batch of messages.

> Do not call the SpamAssassin modules using procmail and spamd. It is not necessary and will simply pass the messages thru SpamAssassin twice!

Each time MailScanner starts or reloads, it reads its configuration files and SpamAssassin's configuration files. These setting are retained and used to process messages until the next time MailScanner reload or restarts.

SpamAssassin configuration settings may be located in several places (See SpamAssassin Settings, Chapter 3) but the default and most common files used are:

- `/etc/MailScanner/spam.assassin.prefs.conf`
- `/etc/mail/spamassassin/*`
- `/root/.spamassassin/*`

SpamAssassin's own standard rules are typically located in /usr/share/spamassassin.

> Modify files in /usr/share/spamassassin at your own risk. They will be overwritten when you upgrade SpamAssassin.

All of your custom SpamAssassin configuration settings should be stored in the spam.assassin.prefs.conf file. All of your custom rulesets should be stored in files which end in .cf in the `/etc/mail/spamassassin` directory

Following these simple rules for locating and storing your custom SpamAssassin configurations and rules will preserve them when SpamAssassin is upgraded

spam.assassin.prefs.conf

This file may contain SpamAssassin configuration setting and custom rulesets. For a full description of all the possible SpamAssassin configuration setting please see:

http://spamassassin.apache.org/doc.html

Here we will explain only a most commonly used subset of all the possible configuration settings.

SpamAssassin uses UNIX style configuration files:

```
# this character starts a comment, which continues until
# end of line.
# blank lines are allowed
```

The most configuration settings are described by

<Configutation_setting_string> <value>

The left hand side must be separated from the right hand side by any “white space” character.

The format for SpamAssassin scoring rulesets is discussed below.

SpamAssassin settings are most easily configured by adding configuration settings to your `spam.assassin.prefs.conf` file. All of the configuration settings described in this Section should be added to or changed in your spam.assassin.prefs.conf file.

SpamAssassin and DNS

SpamAssassin uses DNS lookups extensively. If you are on a slow network or DNS lookups are failing, you can expect to have problems. Typically these problems manifest themselves as “spamassassin timeouts” in your log files.

You can speed up SpamAssassin’s DNS lookup by simply over-riding its default behavior by adding a line to the `spam.assassin.prefs.conf` file. Each time MailScanner calls the SpamAssassin modules, SpamAssassin check to see if DNS services are available. It randomly checks one of 13 MX records. This is unnecessary (If DNS is not working on a mail gateway you have bigger problems than SpamAssassin failing) and can be turned off by adding:

dns_available yes

For additional tips on speeding up DNS please see chapter 7, Tuning and Performance.

White and Black Listing

While white and black listing of users and domains can be accomplished by adding entries in the spam.assassin.prefs.conf file, this is better done by adding these entries in your spam.whitelist.rules and spam.blacklist.rules in the MailScanner/rules directory.

Bayesian Filtering

By default, SpamAssassin uses the Bayesian engine to help identify spam. This is very CPU intensive and on a small overloaded system, you might need to disable it. The settings to use are:

use_bayes (0|1)

This convention of using (0|1) to display the possible values for the configuration setting will be used throughout this Chapter. The values shown mean:

use_bayes 0 (turns Bayesian Filtering off)

use_bayes 1 (turns Bayesian Filtering on - default)

By default the Bayes database is created in the home directory of the user running SpamAssassin. When SpamAssassin is called from MailScanner, the user ID used by SpamAssassin is the user ID of the MailScanner process, most typically root or postfix. This can create problems. If the MailScanner user is root, the Bayes tokens are stored in /root/.spamassassin. If /root is located on a small partition, the Bayes database will quickly fill up the partition. The location of the Bayes is easily changed. To move the Bayes Database:

Create a new directory to store the Bayes database tokens. A typical location is `/etc/MailScanner/bayes` (assuming you have adequate space in `/etc`).

1. Stop MailScanner
2. Move all of the Bayes files to the new directory. These will be the files starting with "`bayes_`".
3. Change the ownership and read-write permissions of the new directory and moved files to match the user of the MailScanner processes.
4. Add the following lines to your spam.assassin.prefs.conf file:

   bayes_path /etc/MailScanner/bayes/bayes

   bayes_file_mode 0660 (**0660** if using MailWatch)

This example assumes you have created the directory `/etc/MailScanner/bayes` to store your database. Note that the configuration value must end with "`/bayes`" appended to the actual directory name. This allows SpamAssassin to identify the actual Bayes files (they all start with "bayes") in the directory.

If you have a new installation of SpamAssassin, bayes filtering will not be used until the Bayesian database accumulates at least 200 spam and 200 ham (ham is the opposite of spam) messages.

> Starter Bayes databases for several Operating systems may be found at: http://www.fsl.com/support

The Bayesian database, by default is set to "auto learn" from messages that pass through SpamAssassin. The SpamAssassin configuration settings that control this behavior are:

bayes_auto_learn (0 | 1) (default: 1)

The score threshold below which a mail has to score, to be fed into SpamAssassin's learning systems automatically as a non-spam message is set by:

bayes_auto_learn_threshold_nonspam n.nn (default: 0.1)

Where n = an integer

The score threshold below which a mail has to score, to be fed into SpamAssassin's learning systems automatically as a spam message.

bayes_auto_learn_threshold_spam n.nn (default: 12.0.)

SpamAssassin requires at least 3 points from the header, and 3 points from the body to auto-learn as spam. Therefore, the minimum working value for this option is 6.

One additional setting which is needed for SpamAssassin to interpret the information in the header of the message is to set the **bayes_ignore_header** to match the value you supplied in `MailScanner.conf`. For example, if you set:

%org-name% = example-com

in your `MailScanner.conf` file, you should add the following lines to your SpamAssassin configuration file:

```
bayes_ignore_header   X-example.com-MailScanner
bayes_ignore_header   X-example.com-MailScanner-SpamCheck
bayes_ignore_header   X-example.com-MailScanner-SpamScore
bayes_ignore_header   X-example.com-MailScanner-Information
```

Another Bayes setting controls how the Bayes database expires old tokens from the database. By default the Bayes system will try to automatically expire old tokens from the database. This auto-expiry occurs when the number of tokens in the database surpasses the **`bayes_expiry_max_db_size`** value (default 150,000). This occurs randomly and will cause Bayes locking problems if not controlled. While the MailScanner.conf setting:

```
Rebuild Bayes Every = <value>
```

Will control this behavior. A safer way to accomplish the auto expiry is in `MailScanner.conf` set:

```
Rebuild Bayes Every = 0
```

and then run a daily cron job at a quiet time on you system. The cron job to run is:

For SpamAssassin 2.xx: (file must be executable)

```
#! /bin/bash
# re-build the Bayes database daily
sa-learn -p /etc/MailScanner/spam.assassin.prefs.conf \
   --rebuild --force-expire
```

For SpamAssassin 3.xx: (file must be executable)

```
#! /bin/bash
# re-build the Bayes database daily
/usr/bin/sa-learn --sync --force-expire \
   -p /etc/MailScanner/spam.assassin.prefs.conf
```

While auto learning spam and ham will usually produce reasonable spam detection results, manually feeding missed spam and ham to the database will result in better Bayesian filtering.

> Starting with SpamAssassin 3.0x, the bayes database may be stored in PostgreSQL or MySQL database. Please see: http://wiki.mailscanner.info/doku.php?id=documentation:anti_spam:spamassassin:bayes:sql

Network Checks

By default, SpamAssassin will run network (Real-time Black Hole - RBL) checks. If you have a slow or unreliable Internet connection, you may need to turn off this feature. Network checks are enabled or disable in SpamAssassin:

```
skip_rbl_checks      (0|1) ( 1 disables the RBL checking)
```

Using additional applications such as DCC, Pyzor and Razor (see Chapter 6, Related Applications) can substantially enhance accurate spam detection. In most cases

SpamAssassin will automatically find Pyzor and DCC if they are installed in the default locations or are in the directories included in the PATH variable of the effective UID of the process running MailScanner. If this fails, the following settings will enable SpamAssassin to find the applications:

pyzor_path /usr/bin/Pyzor (or the actual full path to the Pyzor executable)

dcc_path /usr/local/bin/dccproc (or the actual full path to the dccproc executable)

> Due to licensing concerns, the automatic detection of DCC and possible other applications will change in the 3.1 release of SpamAssassin. You will need to enable these applications by editing `/etc/mail/spamassassin/init.pre` to enable these applications.

There is no corresponding SpamAssassin setting for Razor so the razor executable must be located in PATH variable of the user that runs MailScanner.

While the correct DCC servers automatically selected by the application, the list of Pyzor and Razor servers periodically changes and should be updated daily. The following daily cron jobs will update these server lists:

`/etc/cron.daily/pyzor-discover`: (file must be executable)

```
#! /bin/bash
# get a list of the Pyzor servers
SLEEP=`echo $RANDOM | cut -b1-3`
sleep $SLEEP

/usr/bin/pyzor discover
```

/etc/cron.daily/razor-discover: (file must be executable)

```
#! /bin/bash
# refresh /root/.razor/
SLEEP=`echo $RANDOM | cut -b1-3`

sleep $SLEEP

/usr/bin/razor-admin -discover
```

While these services are usually reliable, there have been service interruptions. If you experience such an interruption, these services may be disabled with SpamAssassin by using the following settings:

```
use_razor2      (0|1) ( 0 disables the service )
use_pyzor       (0|1) ( 0 disables the service )
use_dcc         (0|1) ( 0 disables the service )
```

The default SpamAssassin timeouts for blacklists and Razor are rather generous. Reducing these defaults on busy or heavily loaded systems will stops timeouts from removing SpamAssassin scores.

```
rbl_timeout 20
razor_timeout 10
```

```
pyzor_timeout 10
```

Adding SpamAssassin Rules

The default location for SpamAssassin's basic rulesets is `/usr/share/spamassassin`. If you want to augment these rules by writing you own or downloading contributed extra rulesets you should start with the excellent instructions which can be found at the SpamAssassin Rules Emporium:

http://www.rulesemporium.com/

Another excellent source for obtaining and automatically updating several of the most popular rulesets is the `rules_du_jour` script written by Chris Thielen. The current version of this script supports many (very popular) rulesets.

To obtain and install an easy to install version of `rules_du_jour`:

```
wget http://www.fsl.com/support/Rules_Du_Jour.tar.gz
```

Please read and follow the instructions in the INSTALL. The rules_du_jour and RulesDuJour files may be edited to suit your site's configuration

The script `rules_du_jour_wrapper` is run as a daily cron job and will automatically update the SARE rules and the `rules_du_jour` script itself.

Changing SpamAssassin Rule Scores

SpamAssassin ruleset scores go through extensive testing before release and you should seldom need to modify the basic ruleset scores and you should have a very good understanding of how SpamAssassin scores are used before implementing any such changes. If you do need to change a ruleset score you should add a line to the spam.assassin.prefs.conf similar to:

```
<Name_of_SA_Rule>      nn.nn
```

Where n = integer, for example, to change the score of the HABEAS_SWE rule from the default of -8 to -2 set add:

```
score HABEAS_SWE       -2.0
```

To disable a ruleset, set the score of the rule to 0.0

For a complete listing of standard SpamAssassin tests and scores, please visit

http://www.spamassassin.org/tests.html

SpamAssassin SURBL rules

SURBLs differ from most other RBLs in that they're used to block messages based on the domain names in message body URIs (usually web sites), for example those which have been previously reported to SpamCop as "Spamvertised sites". So SURBLs are not used to block spam senders like most other RBLs; instead they allow you to block messages based on spam domains that occur in their message bodies. Please visit:

www.surbl.org

SURBL checks are an integral feature in SpamAssassin 3.0x. A Kit for implementing SURBL checks in SpamAssassin 2.64 may be downloaded using:

```
wget http://www.fsl.com/support/SURBL.tar.gz
```

Chapter 5

Advanced Configuration via Rulesets

Rulesets provide a very powerful way to configure many options that usually are set to “yes” or “no”. Through the use of rulesets, many configuration options may be selectively applied, based on matching criteria. For example, if there is one email address or domain name for which different options need to be applied, a ruleset can easily be created to allow this, by using the email address or domain name as the matching criteria. Matching criteria is extremely flexible and may be applied in a variety of ways. Below is a description of the format of a rule, as well as several examples.

Rulesets should be placed in the directory set by the MailScanner configuration setting:

`%rule-dir% =`

Typically this is `/etc/MailScanner/rules.`
MailScanner rulesets must end with the extension “.rules”, for example:

`use.spamassassin.rules`

Ruleset Formats

Rulesets are made up of individual rule lines, and each rule line of the ruleset has three parts.

- The **LEFT** side of the rule describes the direction the message is moving
- The **MIDDLE** section describes the pattern to match
- The **RIGHT** side describes the result of matching the pattern

The following is an example of a typical line in a ruleset:

Direction	**pattern** (regular expression)	**result**
`From:`	`john.doe@domain.com`	`yes`

The **LEFT, MIDDLE** and **RIGHT** parts may be separated by spaces or tabs.

Direction

The **direction** (left side) may be any one of the following:

- From: Applies the matching criteria to the email address From field.
- To: Applies the matching criteria to the email address To field.
- FromOrTo: Applies the matching criteria to both email address To and From fields, causing the rule to be applied when either field matches.
- FromAndTo: Applies the matching criteria to both email address To and From fields, causing the rule to be applied when both field match.

- Virus: Applies the matching criteria to any message that contains a virus, and matches when the virus report contains the matching criteria.

While using the case sensitive FromOrTo makes the rule more readable, MailScanner actually ignores case and order; toorfrom will be treated exactly the same as FromOrTo

Pattern

The pattern (middle field) contains criteria to match in the form of a regular expression. A regular expression is a string of characters that defines a set of one or more other strings.

Any string that is defined by a regular expression is said to match that expression. To get a regular expression to match more than one string you use special characters (such as * or ?) that have special meaning. A complete explanation of regular expressions is beyond the scope of this Manual, however some examples are provided below. There are many fine books and websites available on the subject of regular expressions. The Perl site is a good place to start.

http://www.perldoc.com/perl5.6/pod/perlre.html

In the simplest form, a regular expression will be exactly what should be matched, such as an email address. In addition, regular expressions allow more broad matches that offer great flexibility, such as the following examples:

`user@domain.com`

Matches exactly the listed user at the list domain. If the entry is joshua@email.com then the rule will match `joshua@email.com`.

`user@*`

Matches this user at any domain. If the entry is "`joshua@*`" then the rule will match `joshua@email.com, joshua@fsl.com, joshua@example.com`, and `joshua@` any domain.

`*@domain.com`

Matches any user at the listed domain. If the entry is *@example.com then the rule will match tom@example.com, dick@example.com, harry@example.com, and any other user at example.com

`*@*.domain.com`

Matches any user at any sub-domain of domain.com. If the entry is `*@*.example.com` then the rule will match `joshua@hr.example.com, ivan@hr.example.com, steve@it.example.com`, and any user at any sub domain of `example.com`.

`192.168.`

Matches any SMTP client IP address that starts with 192.168.

`default`

This is the default matching rule when no other rule matches.

All rulesets must end with a default ruleset! Typically this is:

```
FromOrTo default             yes (or no)
```

Regular expressions can also be fairly complex, for example;

```
/^192\.168\.1[4567]\./
```

Matches any SMTP client IP address in the networks 192.168.14.0 to 192.168.17.0.

If the Perl module Net::CIDR is installed, the matching criteria may also be a network address in CIDR address notion, such as:

```
10.1.1.0/24
```

This matches any SMTP client IP address in the class c network 10.1.1.0.

Result

The result (third field contains) the value for the configuration option that is using this ruleset. Typically this is yes or no, but it may also be a filename. Please see Appendix C, Practical Ruleset Examples.

This Page is intentionally blank

Chapter 6

Related Applications

Other applications may be installed with MailScanner to simplify administration and provide additional functionality. These applications include:

- MailWatch for MailScanner
- MailScanner Webmin Module
- Vispan
- MailScanner-mrtg
- phplistadmin

MailWatch for MailScanner

MailWatch for MailScanner is a web-based front-end to MailScanner written in PHP, MySQL and JpGraph and is available for free under the terms of the GNU Public License.

It comes with CustomConfig modules for MailScanner which allow MailScanner to log all message data (excluding body text) to a MySQL database which is then queried by MailWatch for reporting and statistics. Features include:

- Displays the inbound/outbound mail queue size (currently for Sendmail users only), load average and today's totals for Messages, Spam, Viruses and blocked content on each page header.
- Color-coded display of recently processed mail.
- Drill-down onto each message to see detailed information.
- Quarantine management allows users and administrators to release, delete or run sa-learn across any quarantined messages.
- Reports with customizable filters and graphs by JpGraph
- Tools to view Virus Scanner status (currently Sophos only), MySQL database status and to view the MailScanner configuration files.
- Tools to create user logins to allow users to view and release messages using the MailWatch interface
- Tools to create administrator logins to allow administrators to view and release all email for a domain using the MailWatch interface
- Management of Quarantines files from within MailWatch
- Utilities for Sendmail to monitor and display the mail queue sizes and to record and display message relay information.

MailWatch for MailScanner and instructions for installing are available from:

http://mailwatch.sourceforge.net/

To install MailWatch you must have a working MailScanner set-up and have running copies of MySQL, Apache, and PHP (with MySQL and GD support). For MailScanner to log to MySQL you need Perl-DBI and Perl-DBD-MySQL installed.

MailScanner Webmin Module

The MailScanner Webmin module was created to provide a simple front-end for administering MailScanner. Before installing the MailScanner Webmin Module, you must install Webmin. Webmin and instructions for installing are available from:

http://www.webmin.com/

Webmin and instructions for installing are available from:

http://sourceforge.net/projects/msfrontend/

Vispan

Vispan is a PERL script which analyses the mail log file to produce useful statistics. It requires MailScanner to provide the necessary log file entries. At the moment the virus list is dependent on the virus scanner you have installed.

Vispan can also use heuristics in the senders of the spam emails and can then automatically add them to the sendmail access file which will cause further mails to be rejected. After a definable period of time they will be removed from the access file and once again allowed to send mail to you.

Vispan and instructions for installing are available from:

http://www.while.homeunix.net/mailstats/

mailscanner-mrtg

mailscanner-mrtg provides configuration files, web pages, and related perl scripts for mrtg to monitor many aspects of your MailScanner machine. With it you will be able to monitor:

- Mail Relayed
- Files in incoming queue
- Spam Identified
- Files in outgoing queue
- Viruses Caught
- Memory (Ram) Used
- Copies of MTA Running Load Average
- Copies of MailScanner Running
- CPU Utilization
- Disk Space Used in /var/spool
- Disk Space Used in /
- IP Traffic
- Files in quarantine
- Space used in ramdisk
- Spam and virus ratios

MailScanner-mrtg for MailScanner and instructions for installing are available from:

http://mailscannermrtg.sourceforge.net/

phplistadmin

phplistadmin is a php web GUI used to edit/create SQL and bydomain/byemail white and blacklists for MailScanner. For SQL black/whitelists you must use the CustomConfig functions available from:

http://filelister.linuxkernel.at/?current=/tarballs/Mailscanner

phplistadmin for MailScanner and instructions for installing are available from:

http://sourceforge.net/projects/phplistadmin/

MSRE

MailScanner Ruleset Editor (msre) provides a web interface for administrators to view and modify their MailScanner rulesets. MSRE is available from:

http://msre.sourceforge.net/

Network Spam Checks

Other applications may be installed with SpamAssassin to improve spam detection accuracy. These applications include:

- DCC
- Pyzor
- Razor

DCC

SpamAssassin uses DCC to add to the total SpamAssassin score. The use of DCC alone will not identify a spam message. DCC or Distributed Checksum Clearinghouse is a system of thousands of clients and about 200 servers collecting and counting checksums related to more than 100 million mail messages per day. The counts can be used by SMTP servers and mail user agents to detect and reject or filter spam or unsolicited bulk mail. DCC servers exchange or "flood" common checksums. The checksums include values that are constant across common variations in bulk messages, including "personalizations".

DCC is based on the concept that if mail recipients could compare the mail they receive, they could recognize unsolicited bulk mail. A DCC server totals reports of checksums of messages from clients and answers queries about the total counts for checksums of mail messages. A DCC client reports the checksums for a mail message to a server and is told the total number of recipients of mail with each checksum. If one of the totals is higher than a threshold set by the client and according to local whitelists the message is unsolicited, the DCC client can log, discard, or reject the message.

Because simplistic checksums of spam would not be effective, the main DCC checksums are fuzzy and ignore aspects of messages. The fuzzy checksums are changed as spam evolves. Since the DCC started being used in late 2000, the fuzzy checksums have been modified several times.

If you email volume is high (+100,000 message per day) you should consider running your own DCC server.

DCC and instructions for installing are available from:

http://www.rhyolite.com/anti-spam/dcc/

Razor

SpamAssassin uses Razor to add to the total SpamAssassin score. The use of Razor alone will not identify a spam message. Vipul's Razor is a distributed, collaborative, spam detection and filtering network. Through user contribution, Razor establishes a distributed and constantly updating catalogue of spam in propagation that is consulted by email clients to filter out known spam. Detection is done with statistical and randomized signatures that efficiently spot mutating spam content. User input is validated through reputation assignments based on consensus on report and revoke assertions which in turn is used for computing confidence values associated with individual signatures.

Razor and instructions for installing are available from: http://razor.sourceforge.net/

Pyzor

SpamAssassin uses Pyzor to add to the total SpamAssassin score. The use of Pyzor alone will not identify a spam message. Pyzor is a methodology for detecting spam similar to that used by razor but Pyzor has been completely rewritten in Python. It is extremely easy and quick to install. An excellent overview of how Pyzor works and download of the application may be found at:

http://pyzor.sourceforge.net/

This Page is intentionally blank

Chapter 7

Tuning and Troubleshooting

We've attempted to list a few commonly used tuning tips and very basic trouble shooting information in this manual. For a more complete and up-to-date information, please visit the MailScanner Wiki documentation section:

http://wiki.mailscanner.info/doku.php?idx=documentation:test_troubleshoot

While many of the techniques covered below are Linux specific, the principals may be applied to all operating systems. The commands and file locations used in the examples below are Linux specific and the actual command you may need to run may be different.

Tuning

There are a few quick steps that may be taken to improve performance. These specific instructions are for Linux distributions only, but similar techniques may be used on other operations systems.

Using a tmpfs files system: MailScanner "unpacks" messages for scanning on `/var/spool/MailScanner/incoming.` If your system has sufficient memory, mounting this directory on a tmpfs (in memory) file system will improve performance. To setup this tmpfs, modify `/etc/fstab` to add the line:

```
none  /var/spool/MailScanner/incoming   tmpfs   defaults      0 0
```

> Be sure to add this line in the `/etc/fstab` below the point at which all of the other disk partitions are mounted and available.

Then as root, issue the command:

```
mount -a
```

Issuing the command:

```
mount
```

Should show that `/var/spool/MailScanner/incoming` is now mounted on the tmpfs.

No email will be lost if the system crashes. MailScanner never removes a message from the incoming mail queue until it is fully written to the outgoing mail queue. If the system crashes, when MailScanner restarts, it will find the "lost" messages in the incoming mail queue and process these messages normally.

Speed Logging: `/etc/syslog.conf` may be modified to omit file syncing the log file after each log event is written. Note that you might lose information if the system crashes right behind a write attempt, but this will give better performance since email gateways log extensively in a very verbose manner.

Trouble shooting

Reading logs: The most effective method of locating a MailScanner problem is **reading the logs**! This should always be your starting point for identifying a problem. The exact location of the relevant logs is operating system and MTA dependent. On Linux MailScanner systems using sendmail as the MTA, all MailScanner and sendmail log information is typically written to `/var/log/maillog`. Errors or anomalies in this file will give you an indication of what is causing the problem.

Debugging MailScanner: Temporarily modify your `MailScanner.conf` file to set:

```
Debug = yes
Debug SpamAssassin = yes
```

Then restart MailScanner. This will cause one MailScanner process to scan one batch of messages from the incoming mail queue and print verbose output to the terminal. Carefully check this output for error messages.

> Be sure to also check:http://wiki.mailscanner.info/doku.php?id=documentation:test_troubleshoot:spamassassin:timeouts

Don't forget to modify the MailScanner.conf file to turn off debugging and restart MailScanner after these modifications have been made

Debugging SpamAssassin: An excellent method to find out if Bayesian filtering, Pyzor, Razor and DCC are being used by SpamAssassin is to run the command:

```
spamassassin -D - p /etc/Mailscanner/spam.assassin.prefs.conf \
      --lint
```

Or

```
spamassassin -D - p /etc/Mailscanner/spam.assassin.prefs.conf \
     < <path_to_message_to_test>
```

This will run a test message through SpamAssassin and print verbose output to the terminal.

Getting Help

Useful detailed installation instructions for different operating systems, MTAs and specific virus scanners may be found at:

> http://wiki.mailscanner.info/doku.php?id=&idx=documentation:install_upgrade

Search the MailScanner FAQs. This is especially useful for help with installations and configuration problems. The FAQs are located at:

> http://wiki.mailscanner.info/doku.php?id=maq:index

If the information above fails to solve your problem, first search the MailScanner List Archives located at:

> http://www.jiscmail.ac.uk/cgi-bin/wa.exe?S1=mailscanner

Search the archive using short identifying terms from the error messages you found while reading the logs and using debug as described above.

If these methods fail (and they seldom do), join the MailScanner List and post your problem. This is an excellent support list and questions are almost always answered very quickly. Be prepared for a mild rebuke:

- If you failed to follow the steps listed above first.
- If you post in HTML format (please use “plain text” format)
- If you top post
- If you hijack threads
- If you send “out of office” replies to the list
- If you fail to include the following information in you request for help:
  - Your Operating System including version
  - The version of MailScanner you are using
  - A complete description of your problem
  - Relevant “snippets” for your logs or debug output. (Not the whole log please.)

If you don’t understand “top post” or “hijack threads”, please visit:

http://www.chiark.greenend.org.uk/~sgtatham/bugs.html

or

http://www.chiark.greenend.org.uk/~sgtatham/bugs.html

There are 2 mailing lists for MailScanner users.

- The "announcements only" list is where all announcements will be made of new versions of MailScanner and associated software such as MailWatch and MailScanner-MRTG. You can subscribe to this list by sending an email to:

  `jiscmail@jiscmail.ac.uk`

  Containing:

  ```
  join mailscanner-announce your-first-name your-last-name
  ```

- The general discussion list is where all new features, configuration issues and Mailscanner problems are discussed. This is where to go if you need troubleshooting help. You can subscribe to this list by sending an email to;

  `jiscmail@jiscmail.ac.uk`

  Containing, in the Subject or Body:

  ```
  join mailscanner your-first-name your-last-name
  ```

This Page is intentionally blank

Appendix A

Installing Red Hat Enterprise Linux

This appendix currently only contains instructions for installing Red Hat ES and As version 3.0, It is hoped that contributions for other operating system installations will soon follow.

This section provides step by step instructions for installing Red Hat Enterprise Linux, ES and AS version 3.0 for use with MailScanner and Related applications. For information regarding any problems encountered while installing RHEL, please contact Red Hat support.

> These instructions do NOT install a graphical user interface.

Installation of Red Hat Enterprise Linux 3 (ES or AS)

1. Boot the machine to be installed with the first Red Hat CD.
2. Press Enter at the first text prompt
3. If the CDs were downloaded and burned, the installer will prompt to perform a Media Check. Perform this check.
4. Welcome: click next.
5. Language Selection: Accept the default of English and click next.
6. Keyboard: Accept the default of U. S. English and click next.
7. Mouse Configuration: Choose your mouse, and click next.
8. Disk Partitioning Setup: Accept the default of Automatically Partition and click next.
9. Automatic Partitioning: Accept the default of Remove All Partitions and click next.
10. Click Yes at the Warning confirmation.
11. Partitioning: Accept the default partition scheme and click next.
12. Boot Loader Configuration: Accept the default and click next.
13. Network Configuration: Make the following changes
    a. Click the “Edit” button under Network Devices
    b. Unselect “Configure using DHCP”
    c. Fill in the IP address and Netmask for your network
    d. Click OK
    e. Under Hostname, fill in the hostname that resolves to the IP entered for this machine.
    f. Fill in the information under Miscellaneous Settings. If you are unsure as to this information, see your Network Administrator. Note: Tertiary DNS may be left blank.
    g. Click next.
14. Firewall: Select “No Firewall” and click next.

15. Time Zone Selection: Choose your time zone, and click next.
16. Set Root Password: Enter a password for the system's root account. This password is used for system administration. It is important to keep this password in a safe place. Once the password is entered, click next.
17. Package Defaults: Select “Customize the set of packages to be installed” and click next.
18. Package Group Selection: Accept the defaults that are checked and add the following:
    a. Scroll down and select “Mail Server”
    b. Scroll down and select “MySQL Database”
    c. Click “Details” for MySQL Database
    d. Select “php-mysql” in the Details popup window
    e. Click OK
    f. Scroll down and select “Network Servers”
    g. Unselect all optional packages
    h. Select only “openldap-servers”
    i. Click OK
    j. Select “System Tools”
    k. Scroll down and select “Development”
19. Click next.
20. About to Install: Click next.
21. Insert the RHEL CDs as they are requested.
22. Graphical Interface (X) Configuration: Select your video card, or accept the default and click next.
23. Monitor Configuration: Select your monitor, or accept the default and click next.
24. Customize Graphical Configuration: Select “Text” as the login type and click next.

Click Exit and the installation is complete!

The mysql-server rpm is no longer shipped with Red Hat ES or AS. You will need this package if you plan to run MailWatch. It may be obtained from:

http://www.mysql.com/downloads/mysql-4.0.html

Appendix B

Installing Third Party Virus Scanners

MailScanner can be configured to use one or more virus scanner to scan incoming email for viruses, however installing multiple virus scanning engines will have an impact on performance.

Installing most virus scanners to work with MailScanner is as simple as

1. Install the virus scanning engine according to the products installation instructions
2. Configure MailScanner to use the installed Virus Scanner (Chapter 3 Configuring MailScanner)

Please review the table below for any additional instructions which may be required to install your specific Virus Scanner or Scanners.

MailScanner configuration name	Installation note	Product Name	Manufacturers Web Site
sophos	note 2 & 5	Linux on Intel	www.sophos.com
sophossavi (SAVI perl module)	note 3 & 5	Linux on Intel	http://www.sng.ecs.soton.ac.uk/mailscanner/install/SAVI.shtml
mcafee		McAfee VirusScan Unix	www.mcafee.com
command	note 1	Command AntiVirus for Linux	www.command.co.uk
kaspersky-4.5		discontinued	www.kaspersky.com
kaspersky (older versions)	note 1	Kaspersky® Anti-Virus for Linux File Server	www.kaspersky.com
kavdaemonclient	note 1	Kaspersky® Anti-Virus for Linux File Server	www.kaspersky.com
etrust	note 1		http://www3.ca.com/Solutions/Product.asp?ID=156
inoculate (CAI)		discontinued	www.cai.com

inoculan (CAI)		discontinued	www.cai.com
nod32-1.99	note 1	for No32 before version 1.99	www.nod32.com
nod32	note 1	NOD32 for Linux Mail Server	www.nod32.com
f-secure	note 1	F-Secure Anti-Virus for Servers for Linux	www.f-secure.com
f-prot	note 1	F-Prot Antivirus for Linux Mail Servers	www.f-prot.com
panda	note 1	Panda Antivirus for Linux	www.pandasoftware.com
rav		discontinued	linux support discontinued
antivir	note 1	AntiVir for Linux	http://www.hbedv.com
clamav	note 1	ClamAV	www.clamav.net
clamavmodule (ClamAV perl module)	note 4	ClamAV	http://www.sng.ecs.soton.ac.uk/mailscanner/install/ClamAVModule.shtml
trend (a.k.a.TrendMicro)	note 1	InterScan VirusWall for Linux	www.trendmicro.com
norman	note 1	Norman Virus Control for Linux	www.norman.de
css	note 1	CSS anti-virus Software	www.symantec.com
avg	note 1	File Server Edition	grisoft.com
vexira	note 1	Vexira Antivirus for Linux Server	www.centralcommand.com
symscanengine	note 1	Symantec Scan Engine, not CSS	www.symantec.com

Note 1: Install According to Manufacturer's directions

Note 2: Use the following steps.

1. Obtain the file `linux.intel.libc6.tar.Z` by:
Copy from the Sophos CDROM to /tmp/Sophos
Or
Get the file MajorSophos.sh from:

http://www.tippingmar.com/majorsophos/

and place in

Edit the file `/usr/sbin/MajorSophos.sh` to add your Sophos username and password, i.e.:

```
WEBUSER="<your_username>"
WEBPASS="<your_password>"
```

2. Then run: `/usr/sbin/MajorSophos.sh -download`

This command will download linux.intel.libc6.tar.Z to `/tmp/MajorSophos.sh.xxxx` where `xxxxx` is a string dependent on the version downloaded.

3. After copying or downloading `linux.intel.libc6.tar.Z`, cd to the directory where the file was copied or downloaded

`cd /tmp/MajorSophos.sh.xxxx` (downloaded)
or
`cd /tmp/Sophos` (copied)

Uncompress and un-tar the file linux.intel.libc6.tar.Z

```
uncompress linux.intel.libc6.tar.Z
```

This will create a directory `sav-install` in the current directory

```
cd sav-install
```

Then run the command

```
/usr/sbin/Sophos.install
```

This installs Sophos in /usr/local/Sophos

Note 3: First install Sophos according to the directions in Note 2 above. Then download and install the SAVI perl module according to the instructions at:
http://www.sng.ecs.soton.ac.uk/mailscanner/install/SAVI.shtml

EXCEPT you will NOT need to change the MailScanner.conf variable:
Minimum Code Status = beta

Note 4: Install ClamAV first and the install the SAVI perl module according to the instructions at:

http://www.sng.ecs.soton.ac.uk/mailscanner/install/ClamAVModule.shtml

Note 5: While IDE files for new viruses will be updated hourly by default. You must manually update the Major Sophos virus definition file monthly using the CD supplied by Sophos or by running the following command (see instructions above).

```
/usr/sbin/MajorSophos.sh
```

Virus scanner product and pricing comparisons from the MailScanner list archives: http://www.jiscmail.ac.uk/cgi-bin/wa.exe?A2=ind0309&L=mailscanner&P=R145271&I=-1

Appendix C

Practical Ruleset Examples

The use of rulesets gives you great power and flexibility in configuring MailScanner. Almost any MailScanner configuration value that can be set to yes or no can also be pointed at a ruleset.

MailScanner provide a ruleset as the value for whitelisted addresses:

`Is Definitely Not Spam = %rules-dir%/spam.whitelist.rules`

You can add the same function for black listing addresses or domains

Spam Black List

In MailScanner.conf set:

`Is Definitely Spam = %rules-dir%/spam.blacklist.rules`

In the new `spam.blacklist.rules` file, set addresses to be blacklisted using rules such as

```
# Addresses to be blacklisted.
# Rules which match below will always be marked as spam
From:           user@nasty.domain.com   yes
From:           *@spammers.com          yes
# Mark an entire network used by spammers
From:           123.231.3.              yes
ToOrFrom:       default                  no
```

Always end every ruleset with a default value. This should be the default value for anything that does not match a regular expression listed in the ruleset.

Only Sign Outgoing Messages

In MailScanner.conf set:

`Sign Clean Messages = %rules-dir%/signing.rules`

If your messages come from "yourdomain.com" and yourdomain.com can be identified by IP addresses that all start with 192.168., your `signing.rules` file would look like this:

```
# Addresses which should not be signed by MailScanner.
From:        192.168.               yes
FromOrTo:    default                no
```

Whenever possible, use IP addresses not domain names to identify systems or network blocks.

Use Different Signatures for Different Domains

In MailScanner.conf set:

`Inline Text Signature = %rules-dir%/sig.text.rules`

And

`Inline HTML Signature = %rules-dir%/sig.html.rules`

In the new `sig.text.rules` file, set addresses to receive different signatures similar to the example below:

```
# Addresses which should signed differently by MailScanner.
From:         *@domain1.com
/opt/MailScanner/etc/reports/domain1.sig.txt
From:         *@domain2.com
/opt/MailScanner/etc/reports/domain2.sig.txt
```

And add equivalent rules in the `sig.html.rules` file.

Only Virus Scan Some Domains

In MailScanner.conf set:

`Virus Scanning = %rules-dir%/virus.scanning.rules`

In the new `virus.scanning.rules` file, set addresses which should not be virus scanned similar to the example below:

```
# Addresses which should not be virus scanned by MailScanner.
FromOrTo:    user@morespam.com       yes
FromOrTo:    *@scanme.com            yes
FromOrTo:    *@scanme-too.com        yes
FromOrTo:    default                 no
```

Send System Administrator Notices to Several People

Note: Rulesets may be “Nested”; that means a ruleset may call another ruleset. The following rules set is an example of a “Nested Ruleset”

In MailScanner.conf set:

`Notices To = %rules-dir%/notices.to.rules`

Create the new `notices.to.rules` file, following the example below:

```
# Send notices to administrators to different lists
To:          @abc.com     postmaster@me.com george@abc.com
To:          @def.com     /etc/MailScanner/rules/techies.txt
FromOrTo:    default      postmaster@me.com
```

Note a reference to a file must include the full path and filename. It must start with a "/" and end in something other than "/". The rule will be replicated for all the entries in the file. Note that a reference to a file can contain another (nested) reference to a file. Beware of too many levels of indirection.

For the @def.com notices, create the file `/etc/MailScanner/rules/techies.txt` which should contain entries similar to:

```
# comment - MailScanner notices for def.com will be sent to
jim@def.com
frank@def.com
*@techies.def.com
hank@somewhereelse.com
/etc/MailScanner/rules/nested-filename.txt
```

Nested file format rules:

1. One pattern or address per line. The allowable patterns are the same as the normal patterns in any normal ruleset file.
2. Comments start with # and continue until the end of the line.
3. Blank lines are ignored.
4. Leading and trailing white space is ignored.
5. Further filenames can be included, allowing you to nest these files if you really need to.

Scan for spam only from certain domains

In MailScanner.conf set:

`Use SpamAssassin = %rules-dir%/use.sa.rules`

Create the new `use.sa.rules` file, following the example below:

```
# Don't use SpamAssassin for entries on this list
To:         *@checkme.com           yes
To:         *@dontcheck.com         no
FromOrTo:   default                 no
```

Filename and Filetype Checking for Specified Domains

Create the files:

`%etc-dir%/filetype.rules.allowall.conf`
`%etc-dir%/filename.rules.allowall.conf`

Where the contents of both files is:

```
# This Ruleset will allow all attached files to pass
allow   .*      -       -
```

The four fields in these files MUST be separated by tabs

Then create the file:

%rules-dir%/filename.rules

Where the contents of this file are:

```
# File to control which domains get filename checking
# mail from or to noscan.com will not have filenames checked
FromOrTo: noscan.com /etc/MailScanner/filename.rules.allowall.conf

# Allow local to let MailWatch release quarantined files
From:   127.0.0.1 /etc/MailScanner/filename.rules.allowall.conf
FromOrTo: default /etc/MailScanner/filename.rules.conf
```

Then create the file:

%rules-dir%/filetype.rules

Where the contents of this file are:

```
# File to control which domains get filetype rule checking
# mail from or to noscan.com will not have filetypes checked
FromOrTo: noscan.com /etc/MailScanner/filetype.rules.allowall.conf

# Allow local to let MailWatch release quarantined files
From:   127.0.0.1   /etc/MailScanner/rules/filetype.rules.allowall.conf
FromOrTo: default   /etc/MailScanner/filetype.rules.conf
```

> Each rule should be typed on one line in these files

In MailScanner.conf set:

```
Filename Rules = %rules-dir%/filename.rules
Filetype Rules = %rules-dir%/filetype.rules
```

Then reload MailScanner

Chaining filename.rules.conf files

In the filename.rules file example above, you can supply a single filename or a space-separated list of filename.rules.conf files for the filename to be used when the expression to be matched is met.

When multiple filenames are used, the filename allow/deny rules that are applied are simply the concatenation of all the filename.rules.conf files that you have used, in the order they are listed.

The allow/deny rule that is used for a particular attachment is the first one that matches. It stops processing there and performs allow or deny (or deny+delete) action that is matched.

So you DON'T need to have a filename.rules.conf file that is a copy of the supplied one with an extra rule at the top (deny \.zip$ - -). If you have a lot of these files this can be very difficult to maintain and administer. All you actually need is one copy of the supplied filename.rules.conf file, and one file for each modification. In the example below we will to block IP files for mail to/from 'domain1.com'.

In MailScanner.conf set:

```
Filename Rules = %rules-dir%/filename.rules
```

Where the contents of this file are:

```
# the rule below is entered on a single line
FromOrTo: *@domain1.ie /etc/MailScanner/filename.domain1.com.conf
 /etc/MailScanner/filename.rules.conf
# The default rule
FromOrTo: default /etc/MailScanner/filename.rules.conf
```

And the `/etc/MailScanner/filename.rules.conf` file is exactly as originally distributed

And the contents of `/etc/MailScanner/filename.domain1.com.conf` are:

```
Deny  \.zip$      -     -
```

The four fields in this file MUST be separated by tabs

This page is left intentionally blank

Appendix D

Upgrading MailScanner (rpm Version)

Upgrading the rpm vision of MailScanner is typically relatively quick and painless. First make sure that you have a system backup.

The second step is to download the latest version of MailScanner from:

http://www.sng.ecs.soton.ac.uk/mailscanner/downloads.shtml

The Upgrade

After downloading simply unpack the upgrade and, as the root user, cd into the newly created directory, i.e.:

```
cd MailScanner-4.43.8-1
```

And then simply run the install script:

```
./install.sh
```

This will update all MailScanner files.

After the script successfully completes, you will need to:

- Update MailScanner.conf
- Check for any .rpmnew files

Upgrading Mailscanner.conf

Most often the newer version of MailScanner will include new Configuration Variables. The script `/usr/sbin/upgrade_MailScanner_conf` will automatically create a new `MailScanner.conf` file which preserves all of your current MailScanner configurations values. To use this utility:

```
cd /etc/MailScanner
```

Backup a copy of your current `MailScanner.conf` file:

```
cp MailScanner.conf MailScanner.conf.<old-version-id>
```

Then stop MailScanner and update `Mailscanner.conf`:

```
/usr/sbin/upgrade_MailScanner_conf \
MailScanner.conf MailScanner.conf.rpmnew > \
MailScanner.new

mv MailScanner.conf MailScanner.old
mv MailScanner.new  MailScanner.conf
```

Next check to see if `languages.conf` needs to be updated. If the file `/etc/MailScanner /reports/en/languages.conf.rpmnew` exists. You will need to run `/usr/sbin/upgrade_languages_conf`

```
cd /etc/MailScanner/reports/en
upgrade_languages_conf languages.conf \
     languages.conf.rpmnew > languages.new
mv -f languages.conf languages.old
mv -f languages.new  languages.conf
```

Installing .rpmnew files

If you have changed any of MailScanner's standard files, your changes will not be overwritten. Instead the MailScanner upgrade will leave your changed files in place and install the new version of the file with an `.rpmnew` added to the filename.

If you watch the output of the `upgrade_MailScanner_conf` script, it will tell you which `.rpmnew` files were installed.

For the rpm MailScanner distribution, these files will typically be in or under the `/etc/MailScanner` and `/usr/lib/MailScanner directories.` Another way to quickly identify these files:

```
find /etc/MailScanner "*.rpmnew"
find /usr/lib/MailScanner "*.rpmnew"
```

Once you have located the new .rpmnew files you will need to **`diff`** the existing file and the `.rpmnew` file to determine if you need to edit your existing file.

Once all of the `.rpmnew` new files have been incorporated, restart MailScanner. Your upgrade is complete.

Be sure to tail the log files to be certain that MailScanner has restarted correctly and is processing mail normally.

Keeping Comments

While you may add comments to the `MailScanner.conf` file you should note that they may be lost if you automatically upgrade MailScanner using the `upgrade_MailScanner_conf` script. To keep your old comments in your original file, add "`--keep-comments`" to the command line. Note that this will mean you don't get to see out any extra new values you might be able to use in existing "improved" configuration options.