MailScanner.conf

DOCUMENTATION

NAME

MailScanner.conf − Main configuration for MailScanner

SYNOPSIS

none

DESCRIPTION

MailScanner is configured using the file MailScanner.conf. The location of this file varies from operating system to operating system:

Linux: /etc/MailScanner

FreeBSD: /usr/local/etc/MailScanner
Other: /opt/MailScanner/etc

Blank lines are ignored, as are leading and trailing spaces. Comments start at a '#' character and extend to the end of the line. All options are expressed in the form

option = value

Many of the options can also be the filename of a ruleset, which can be used to control features depending on the addresses of the message, and/or the IP address where the message came from. You will find some examples of rulesets and an explanation of them in the "rules" directories within the MailScanner installation and in the section "RULESETS" later in this manpage.

The options are best listed in a few categories. If this list looks very large then don't worry, the supplied MailScanner.conf file (or MailScanner.conf.sample) contains sensible defaults for all the values. You will probably only need to change a very few of them to start with.

Starting with version 4.40.10 of MailScanner you can use shell

environment variables such as $HOSTNAME or ${HOSTNAME} in MailScanner.conf and its relatives.

You should define the following variables:

%report-dir%

Default: /opt/MailScanner/etc/reports/en
Default FreeBSD: /usr/local/share/MailScanner/reports/en

Set the directory containing all the reports in the required language.

%etc-dir%

Default: /opt/MailScanner/etc
Default FreeBSD: /usr/local/etc/MailScanner

Configuration directory containing this file

%rules-dir%

Default: /opt/MailScanner/etc/rules
Default FreeBSD: /usr/local/etc/MailScanner/rules

Rulesets directory containing your ".rules" files

%org-name%

Default: yoursite

Enter a short identifying name for your organisation below, this is used to make the X-MailScanner headers unique for your organisation. Multiple servers within one site should use an identical value here to avoid adding multiple redundant headers where mail has passed through several servers within your organisation.
Note: Some Symantec scanners complain (incorrectly) about "." characters appearing in the names of headers.

%org-long-name%

Default: Your Organisation Name Here

Enter the full name of your organisation below, this 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 "0 sequences in the text. These will be replaced by line-breaks.

%web-site%

Default: www.your-organisation.com

Enter the location of your organisation's web site below. This is used in 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.

System Settings

Max Children

Default: 5

MailScanner uses your server efficiently by running several identical processes at the same time, all processing mail. This is the number of these processes to run at once. Turning this figure will optimise the performance of your system if you process a lot of mail. A good figure to start with is 5 children per CPU. So if you have 4 CPUs in your server, start by setting this to 20.

Run as User

Default: not to change user

Provided for Exim users (and anyone not running sendmail as root), this changes the user under which MailScanner runs.

Run as Group

Default: not to change group

Provided for Exim users (and anyone not running sendmail as root), this changes the group under which MailScanner runs.

Queue Scan Interval

Default: 5

How often (in seconds) should each process check the incoming mail queue for new messages? 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 to be processed.

Incoming Queue Dir

Default: /var/spool/mqueue.in

Directory in which MailScanner should find e−mail messages for scanning. This can be any of the following:

1. a directory name.

   Example: /var/spool/mqueue.in

2. a wildcard giving directory names.

   Example: /var/spool/mqueue.in/*

3. the name of a file containing a list of directory names, which can in turn contain wildcards.

Example: /usr/local/etc/MailScanner/mqueue.in.list.conf

Outgoing Queue Dir

Default: /var/spool/mqueue

Directory in which MailScanner should place scanned e−mail messages. This can also be the filename of a ruleset.

Incoming work dir

Default: /opt/MailScanner/var/incoming
Default FreeBSD: /var/spool/MailScanner/incoming

Directory in which to temporarily store unpacked MIME messages during scanning process.

Quarantine Dir

Default: /opt/MailScanner/var/quarantine
Default FreeBSD: /var/spool/MailScanner/quarantine

Set where to store infected messages and attachments (if they are kept). This can also be the filename of a ruleset.

PID file

Default: /opt/MailScanner/var/MailScanner.pid
Default FreeBSD: /var/run/MailScanner.pid

Set where to store the process id number so you can stop MailScanner. In the FreeBSD port this should remain /var/run/MailScanner.pid in order for the start/stop script to work.

Restart Every

Default: 14400

To avoid resource leaks the MailScanner parent process stops and restarts its child processes from time to time. Set the amount of seconds each child process is supposed to live here.

MTA

Default:
sendmail

MailScanner works with sendmail and exim. Since the queue handling differs a bit, you have to tell MailScanner which MTA you are using. Valid options are sendmail and exim.

Sendmail

Default: /usr/lib/sendmail
Default FreeBSD: /usr/sbin/sendmail

Set how to invoke MTA when sending messages MailScanner has created (e.g. to sender/recipient saying "found a virus in your message"). This can also be the filename of a ruleset.

Sendmail2

Default: same value as the Sendmail setting

Sendmail2 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.
For Exim users this could be: Sendmail2 = /usr/sbin/exim −C /usr/local/etc/exim/configure.out

Incoming Work Dir Settings

You should not normally need to touch these settings at all, unless you are

using ClamAV and need to be able to use the external archive unpackers instead of ClamAV's built−in ones.

Incoming Work User

Default:

If you want to create the temporary working files so they are owned by a user other than the "Run As User" setting, you can change that here. Note: If the "Run As User" 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".

Incoming Work Group

Default:

If you want to create the temporary working files so they are owned by a group other than the "Run As User" setting, you can change that here. Note: If the "Run As User" 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".

Incoming Work Permissions

Default: 0600

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* other users to be able to read them, set to 0644. For a detailed description, if you're not already familiar with it, refer to 'man 2 chmod'. Typical use: external helper programs of virus scanners (notably ClamAV), like unpackers. Use with care, you may well open security holes.

Quarantine and Archive Settings

If, for example, you are using a web interface so that users can manage their quarantined files, you might want to change the ownership and permissions of the quarantined 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

Default:

If you want to create the quarantine/archive so the files are owned by a user other than the "Run As User" setting at the top of this file, you can change that here. Note: If the "Run As User" 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 "Quarantine Group".

Quarantine Group

Default:

If you want to create the quarantine/archive so the files are owned by a user other than the "Run As User" setting at the top of this file, you can change that here. Note: If the "Run As User" 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 "Quarantine Group".

Quarantine Permissions

Default: 0600

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, of course), set to 0640. If you want *all* other users to be able to read them, set to 0644. For a detailed description, if you’re not already familiar with it, refer to ‘man 2 chmod‘. Typical use: let the webserver have access to the files so users can download them if they really want to. Use with care, you may well open security holes.

Process Incoming Mail

Max Unscanned Bytes Per Scan

Default: 100000000

MailScanner handles messages in batches for efficiency. Messages are gathered (in strict date order) from the incoming queue directory, one at a time, until this or one of the following three limits is reached or the queue is empty.

This setting limits the total size of messages per batch for which no scanning is done (i.e. Virus Scanning = no).

Max Unsafe Bytes per Scan

Default: 50000000

This setting limits the total size of messages per batch for which scanning is done (i.e. Virus Scanning = yes).

Max Unscanned Messages Per Scan

Default: 100

This setting limits the total number of messages per batch for which no scanning is done (i.e. Virus Scanning = no).

Max Unsafe Messages per Scan

Default: 100

This setting limits the total number of messages per batch for which scanning is done (i.e. Virus Scanning = yes).

Max Normal Queue Size

Default: 1000

If more messages are found in the queue than this, then switch to an "accelerated" mode of processing messages. This will cause it to stop scanning messages in strict date order, but 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 "in emergency only".

Maximum Attachments Per Message

Default: 200

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. This can also be the filename of a ruleset.

Expand TNEF

Default: yes

TNEF is primarily used by Microsoft programs such as Outlook and Outlook Express when mails are formatted/sent in Rich−Text−Format. Attachments are all put together in one WINMAIL.DAT file.

Should we use a TNEF decoder (external or Perl module)? This should be "yes" unless the scanner you are using (Sophos, McAfee) has the facility built−in. However, if you set it to "no", then the filenames within the TNEF attachment will not be checked against the filename rules.

Deliver Unparsable TNEF

Default: no

Rich Text format attachments produced by some versions of Microsoft Outlook cannot be completely decoded at present. Setting this option to yes allows compatibility with the behaviour of earlier versions where these attachments were still delivered.

This would introduce the slight chance of a virus getting through in the segment of the attachment that could not be decoded, but the setting may be necessary if you have a large number of Microsoft Outlook users who are troubled by the new behaviour.

TNEF Expander

Default: /opt/MailScanner/bin/tnef
Default FreeBSD: /usr/local/bin/tnef

Full pathname giving location of the MS−TNEF expander/decoder program, or the keyword internal which will force use of the optional Perl Convert::TNEF module instead of the external program.

TNEF Timeout

Default: 120

The maximum length of time (in seconds) the TNEF Expander is allowed to run for diassembling one attachment.

File Command

Default: /usr/bin/file

Where the "file" command is installed. This is used for checking the content type of files, regardless of their filename. To disable Filetype checking, set this value to blank.

File Timeout

Default: 20

The maximum length of time the "file" command is allowed to run for one batch of messages (in seconds).

Unrar Command

Default: /usr/bin/unrar

Where the "unrar" command is installed. If you haven't got this command, look at www.rarlab.com. This is used for unpacking rar archives so that the contents can be checked for banned filenames and filetypes, and also 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.

Unrar Timeout

Default: 50

The maximum length of time the "unrar" command is allowed to run for 1 RAR archive (in seconds)

Block Encrypted Messages

Default: no

This is inteded for use with a ruleset to ensure that none of your users is covertly mailing sites with which you would not normally communicate (e.g. your competitors). If this is set to yes (or the ruleset evaluates to yes) encrypted messages are blocked.

Block Unencrypted Messages

Default: no

This is intended for use with a ruleset to ensure that mail is always encrypted before being sent. This could be used to ensure that mail to your business partners is sent securely.

Allow Password−Protected Archives

Default: no

Should archives which contain any password−protected files be allowed? Leaving this set to "no" is a good way of protecting against all the protected zip files used by viruses at the moment. This can also be the filename of a ruleset.

Maximum Message Size

Default: 0

The maximum size, in bytes, of any message including the headers. If this is set to zero, then no size checking is done. 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 dialup users so their email applications don’t time out downloading huge messages.

Maximum Attachment Size

Default: −1

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. 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.

Maximum Archive Depth

Default: 3

The maximum depth to which zip archives will be unpacked to allow for checking filenames and filetypes within zip archives. Setting this to 0 will disable filename/−type checks within zip files while still allowing to block password protected zip files.

Find Archives By Content

Default: yes

Find zip archives by filename or by file contents? Finding them by content is a far more reliable way of finding them, but it does mean that you cannot tell your users to avoid zip file checking by renaming the file from ".zip" to "_zip" and tricks like that. 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.

Options specific to Sophos Anti-Virus

Allowed Sophos Error Messages

Default:

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 lots of corrupt PDF files, for example. This option allows for multiple strings as well. In this case, the strings should be put in double quotes (") and each string separated with commas. Examples:
Allowed Sophos Error Messages = corrupt format not supported
Allowed Sophos Error Messages = "corrupt", "format not supported"

The first version will match "corrupt format not supported" only. The second version will match "corrupt" and "format not supported".

Sophos IDE Dir

Default: /usr/local/Sophos/ide

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.

Sophos Lib Dir

Default: /usr/local/Sophos/lib

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.

Monitors For Sophos Updates

Default: /usr/local/Sophos/ide/*ides.zip

SophosSAVI only: monitor each of these files for changes in size to detect when a Sophos update has happened. The date of the Sophos Lib Dir is also monitored. This is only used by the "sophossavi" virus scanner, not the "sophos" scanner setting.

Virus scanning and vulnerability testing

Virus Scanning

Default: yes

Do you want to scan email for viruses? A few people don't have virus scanner licence and so want to disable all the virus scanning.
NOTE: Switching this to no completely disables all virus−scanning functionality. If you just want to switch of actual virus scanning, then set "Virus Scanners = none" instead.
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.

Virus Scanners

Default: none

Which Virus Scanning package to use. Possible choices are sophos, sophossavi, mcafee, command, bitdefender, kaspersky, kaspersky−4.5, kavdaemonclient, inoculate, inoculan, nod32, nod32−1.99, f−secure, f−prot, panda, rav,

antivir, clamav, clamavmodule, css, trend, norman, avg, vexira, symscanengine, generic, none (no virus scanning at all). This *cannot* be the filename of a ruleset.

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 scanning a directory path including symlinks.

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

Note: Make sure that you check that the base installation directory in the 3rd column of virus.scanners.conf matches the location you have installed each of your virus scanners. The supplied virus.scanners.conf file assumes the default installation locations recommended by each of the virus scanner installation guides.

Virus Scanner Timeout

Default: 300

The maximum time (in seconds) that the cirus scanner is allowed to take to scan one batch of messages.

Deliver Disinfected Files

Default: yes

Should infected attached documents be automatically disinfected and sent on to the original recipients? Less than 1% of viruses in the wild can be successfully disinfected,as macro viruses are now a rare occurrence. So the default has been changed to "no" as it gives a significant performance improvement.

Silent Viruses

Default: HTML−IFrame All−Viruses

Messages whose virus reports contain any of the words listed here will be treated as "silent" viruses. No messages will be

sent back to the senders of these viruses, and the delivery to the recipient of the message can be controlled by the next option "Still Deliver Silent Viruses". This is primarily designed for viruses such as "Klez" and "Bugbear" which put fake addresses on messages they send, so there is no point informing the sender of the message, as it won't actually be them who sent it anyway. Other words that can be put in this list are the 5 special keywords

- 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.
- Zip−Password: inserting this will stop senders being warned about password−protected zip files when they are not allowd. 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 (as the sender address is always forged these days anyway), but anyone who sends a message that is blocked for other reasons will still be notified.

Still Deliver Silent Viruses

Default: no

If this is set to yes then disinfected messsages that originally contained one of the "silent" viruses will still be delivered to the original recipients, even those addresses were chosen at random by the infected PC and do not correspond to anything a user intended to send. Set this to yes so that your users (and your management) appreciate how much MailScanner is doing to protect them, but set it to no if they complain a lot about

receiving lots of virus warnings.

Non−Forging Viruses

Default: Joke/ OF97/ WM97/ W97M/

Strings listed here will be searched for in the output of the virus scanners. It works to achieve the opposite effect of the "Silent Viruses" listed 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, whey they are not allowed.

Options specific to ClamAV Anti-Virus

Monitors for ClamAV Updates

Default: /usr/local/share/clamav/*.cvd

ClamAVModule only: monitor each of these files for changes in size to detect when a ClamAV update has happened. This is only used by the "clamavmodule" virus scanner, not the "clamav" scanner setting.

ClamAVmodule Maximum Recursion Level

Default: 5

ClamAVModule only: The maximum recursion level of archives. This setting *cannot* be the filename of a ruleset, only a simple number.

ClamAVmodule Maximum Files

Default: 100

ClamAVModule only: The maximum number of files per batch. This setting *cannot* be the filename of a ruleset, only a simple number.

ClamAVmodule Maximum File Size

Default: 10000000

ClamAVModule only: The maximum file of each file (Default = 10MB). This setting *cannot* be the filename of a ruleset, only a simple number.

ClamAVmodule Maximum Compression Ratio

Default: 250

ClamAVModule only: The maximum compression ration of archives. This setting *cannot* be the filename of a ruleset, only a simple number.

Removing/Logging dangerous or potentially offensive content

Allow Partial Messages

Default: no

Do you want to allow partial messages, which only contain a fraction of the attachments, not the whole thing? There is no way that "partial messages" can be scanned for viruses properly, as only a fragment of the message is ever processed, never the whole message at once.
Setting this option to yes is **very dangerous** as it can let viruses in. But you might want to use a ruleset to set it for some customers' outgoing mail, for example.

Allow External Message Bodies

Default: no

There is a mechanism, very rarely used, in which the body of a message is contained on a remote server, which the user's email application should download when it displays the message. Currently, I am only aware of this feature being supported by a few versions of Netscape, and the only people who use it are the IETF. There is no way to guarantee that the fetched file has no viruses in it, as MailScanner never sees it. Setting this option to yes is **very dangerous** as it can let viruses in from remote "message body servers".

Find Phishing Fraud

Default: yes

Do you want to check for "Phishing" attacks? These are attacks that look like a genuine email message from your bank, 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. Except it is not the real bank's web site at all, 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. Note: This does cause significant extra load, particularly on systems receiving lots of spam such as secondary MX hosts. This *cannot* be the filename of a ruleset, it must be 'yes' or 'no'.

Also Find Numeric Phishing

Default: 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 value cannot be the name of a ruleset, only a simple yes or no.

Phishing Safe Sites File

Default: %etc−dir%/phishing.safe.sites.conf

There are some companies, such as banks, that insist on sending out email messages with links in them that are caught by the "Find Phishing Fraud" test described above. This is the name of a file which contains a list of link destinations which should be ignored in the test. This may, for example, contain the known websites of some banks. See the file itself for more information. This can only be the name of the file containing the list, it *cannot* be the filename of a ruleset.

Allow IFrame Tags

Default: no

Do you want to allow HTML <IFrame> tags in email messages? This is not a good idea as it allows various Microsoft Outlook security vulnerabilities to go unprotected, but if you have a load of mailing lists sending them, then you will want to allow them to keep your users happy. This can also be the filename of a ruleset, so you can allow them from known mailing lists but ban them from everywhere else. Possible Values:

- yes => Allow these tags to be in the message
- no => Ban messages containing these tags
- disarm => Allow these tags, but stop these tags from working

Log IFrame Tags

Default: no

You may receive complaints from your users that HTML mailing lists they subscribe to have been stopped by the "Allow IFrame Tags" option above. So before you use the

option above, set this option to "yes" and MailScanner will log the senders all messages which contain IFrame tags. You can then setup a ruleset for the option above which will allow IFrame tags in messages sent by well known (and trusted) mailing lists, while banning them from everywhere else.

Allow Form Tags

Default: disarm

Do you want to allow <Form> tags in email messages? This is a bad idea as these are used as scams to persuade people to part with credit card information and other personal data. This can also be the filename of a ruleset. Possible values:

- yes => Allow these tags to be in the message
- no => Ban messages containing these tags
- disarm => Allow these tags, but stop these tags from working

Allow Script Tags

Default: no

Do you want to allow <Script> tags in email messages? This is a bad idea as these are used to exploit vulnerabilities in email applications and web browsers. This can also be the filename of a ruleset. Possible values:

- yes => Allow these tags to be in the message
- no => Ban messages containing these tags
- disarm => Allow these tags, but stop these tags from

working

Allow WebBugs

Default: 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. It is not dangerous, it is just used to make you give away information. This can also be the filename of a ruleset. Possible values:

- yes => Allow these tags to be in the message
- no => Ban messages containing these tags
- disarm => Allow these tags, but stop these tags from working

Allow Object Codebase Tags

Default: no

Do you want to allow <Object Codebase=...> tags in email messages? This is a bad idea as it leaves you unprotected against various Microsoft−specific security vulnerabilities. But if your users demand it, you can do it. This can also be the filename of a ruleset. Possible values:

- yes => Allow these tags to be in the message
- no => Ban messages containing these tags
- disarm => Allow these tags, but stop these tags from working

Convert Dangerous HTML To Text

Default: no

This option interacts with the "Allow ... Tags" options above like this:

Allow...Tags Convert Danger... Action
========== ==========
==========
no no Blocked
no yes Blocked
disarm no Specified HTML tags disarmed
disarm yes Specified HTML tags disarmed
yes no Nothing
yes yes All HTML tags stripped

If an "Allow ... Tags = yes" is triggered by a message, and this "Convert Dangerous HTML To Text" is set to "yes", then the HTML message will be converted to plain text. This makes the HTML harmless, while still allowing your users to see the text content of the messages. Note that all graphical content will be removed.

Convert HTML To Text

Default: no

If you have users who are children, or who are offended by things like pornographic spam email, you can protect them by converting incoming HTML email messages into plain text. HTML attachments will not be affected. You could set this to be a ruleset so you only convert messages addressed to some of your users, or not convert messages from some known trusted sources. This can be essential if you have a "duty of care" for some of your users.

Allow Form Tags

Default: no

Do you want to allow <Form> tags in email messages? This is a bad idea as these are used as scams to pursuade people to part with credit card information and other personal data. This can also be the filename of a ruleset.

Attachment filename checking

Filename Rules

Default: %etc−dir%/filename.rules.conf

File in which to store the attachment filename ruleset. This can be a ruleset allowing different filename rules to apply to different users or domains. The syntax of this file is described in section "Attachment Filename Ruleset".

Filetype Rules

Default: %etc−dir%/filetype.rules.conf

Set where to find the attachment filetype ruleset. The structure of this file is explained elsewhere, but it is used to accept or reject file attachments based on their content as determined by the "file" command, regardless of whether they are infected or not. This can also point to a ruleset, but the ruleset filename must end in ".rules" so that MailScanner can determine if the filename given a ruleset or not!

Reports and responses

Quarantine Infections

Default: yes

Set this to store infected / dangerous attachments in directories created under the quarantine directory. Without this, they will be deleted. Due to laws on privacy and data protection in your country, you may be forced to set this to "no".

Quarantine Silent Viruses

Default: yes

There is no point quarantining most viruses these days, 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. This is currently set to "yes" so the behaviour is the same as it was in in previous versions. This can also be the filename of a ruleset.

Quarantine Whole Message

Default: no

When an infected message is stored in the quarantine, a copy of the entire message will be saved, in addition to copies of the infected attachments.

Quarantine Whole Messages As Queue Files

Default: no

When an entire message is saved in the quarantine for any reason, do you want to save it as the raw data files out of the mail queue (which can be processed with the df2mbox script, and which is easier to send to its original recipients), or do you want a conventional message file consisting of the header followed by the body of the message. If the previous option is switched off, then this will only affect archived mail and quarantined spam. If the previous option is on, then this also affects quarantined infections.

Keep Spam And MCP Archive Clean

Default: 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, so don't need it. This can also be the filename of a ruleset.

Language Strings

Default: %reports−dir%/languages.conf

Set where to find all the strings used so they can be translated into your local language. This can also be the filename of a ruleset so you can produce different languages for different messages.

Deleted Bad Filename Message Report

Default: %reports−dir%/deleted.filename.message.txt

When an attachment is deleted from a message because the filename failed the filename rules in force for the message, it is replaced by the contents of this file. A few variable substitutions can be made in this file, an example of each of which is contained in the supplied sample file.

Deleted Virus Message Report

Default: %reports−dir%/deleted.virus.message.txt

When an attachment is deleted from a message because the attachment contained a virus or other dangerous content, it is replaced by the contents of this file. A few variable substitutions can be made in this file, an example of each of which is contained in the supplied sample file.

Stored Bad Filename Message Report

Default: %reports−dir%/stored.filename.message.txt

When an attachment is deleted and stored from a message

(and the attachment has been stored in the quarantine) because the filename failed the filename rules in force for the message, it is replaced by the contents of this file. A few variable substitutions can be made in this file, an example of each of which is contained in the supplied sample file.

Deleted Bad Content Message Report

Default: /%reports−dir%/deleted.content.message.txt

This report is sent when a message is deleted because it contained bad or dangerous content. A few variable substitutions can be made in this file, an example of each of which is contained in the supplied sample file.

Stored Bad Content Message Report

Default: %reports−dir%/stored.content.message.txt

This report is sent when a message is stored because it contained bad or dangerous content. A few variable substitutions can be made in this file, an example of each of which is contained in the supplied sample file.

Disinfected Report

Default: %reports−dir%/disinfected.report.txt

When, for example, a Microsoft Word macro virus has been safely removed from a document, leaving the original document intact, it is delivered on to the original recipient. The contents of this text file will be put in the body of the new message, explaining to the user what has happened.

Inline HTML Signature

Default: %reports−dir%/inline.sig.html

If the "Sign Clean Messages" option is set, then the contents of

this file will be appended to the end of the body of every message that is scanned by MailScanner. You can use this to inform your users that MailScanner has scanned it, and you can also add any disclaimers you feel should be on mail travelling through your servers. This option corresponds to the contents that is appended to HTML messages.

Inline Text Signature

Default: %reports-dir%/inline.sig.txt

If the "Sign Clean Messages" option is set, then the contents of this file will be appended to the end of the body of every message that is scanned by MailScanner. You can use this to inform your users that MailScanner has scanned it, and you can also add any disclaimers you feel should be on mail travelling through your servers. This option corresponds to the contents that is appended to text messages.

Sender Error Report

Default: %reports-dir%/sender.error.report.txt

When a message could not be processed completely for some reason, such as bad message structure or unreadable winmail.dat TNEF attachments, this message is sent back to the sender. Read the example file supplied for a demonstration of what variables can be used inside the file.

Sender Bad Filename Report

Default: %reports-dir%/sender.filename.report.txt

When an attachment is trapped by the filename rules, this message is sent back to the sender.

Sender Virus Report

Default: %reports-dir%/sender.virus.report.txt

When an attachment is removed because of a virus, this message is sent back to the sender.

Hide Incoming Work Dir

Default: yes

When this option is set, the full directory in which the virus was found will be removed from report messages sent to users. This makes the infection reports a lot easier to understand.

Include Scanner Name in Reports

Default: 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/...../languages.conf.
Very useful if you use several virus scanners, but a bad idea if you don't want to let your customers know which scanners you use.

Changes to message headers

Mail Header

Default: X−MailScanner:

Extra header that should be added to all scanned messages to show they have been scanned. You might want to add an abbreviation of your site name to this, so that you can find headers that are added by your MailScanner server.

Spam Header

Default: X−MailScanner−SpamCheck:

Name of the header to add to mail detected as spam. The text of the header is a list of the causes that think the message is spam.

Spam Score Header

Default: X−MailScanner−SpamScore:

If the option "Spam Score" is set, this is the name of the header that is used to contain the list of characters.

Information Header

Default: X−MailScanner−Information:

Name of the header to add to all messages, to be used for simply providing a URL or contact information for anyone receiving mail that has gone through MailScanner. If you do not want this header, simply set it blank.

Add Envelope From Header

Default: 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.

Add Envelope To Header

Default: no

Do you want to add the Envelope−To: header? This can be useful for tracking span 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.

Evelope From Header

Default: X−%org−name%−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.

Evelope To Header

Default: X−%org−name%−MailScanner−To:

This is the name of the Envelope To header controlled by the option above. This can also be the filename of a ruleset.

Detailed Spam Report

Default: yes

If this is set to yes then you get the normal fully detailed spam report in spam messages. If this is set to no then you simply get a "spam" or "not spam" report. The exact text inserted can be configured in the languages.conf file for your language.

Include Scores In SpamAssassin Report

Default: yes

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

Spam Score Character

Default: s

If the option "Spam Score" is set, this is the character that will be repeated in the "Spam Score Header", one letter for each

point in the SpamAssassin score.

SpamScore Number Instead Of Stars

Default: no

If this option is set to yes, you will get a spam−score header saying just the value of the spam score, instead of the row of characters representing the score. This can also be the filename of a ruleset.

Minimum Stars If on Spam List

Default: 0

This sets the minimum number of "Spam Score Characters" which will appear if a message triggered the "Spam List" setting 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.

Clean header Value

Default: Found to be clean

This is the text that is added to the "Mail Header" when a message is found to be clean and free of viruses and other dangerous content.

Infected Header Value

Default: Found to be infected

This is the text that is added to the "Mail Header" when a message is found to be infected with a virus or other dangerous content.

Disinfected Header Value

Default: Disinfected

This is the text that is added to the "Mail Header" of a message that is created by MailScanner to contain disinfected documents containing macro viruses that could be completely removed, leaving the original document intact.

Information Header Value

Default: Please contact the ISP for more information

This is the text that is added to the "Information Header" of a message that has passed through MailScanner at all. It could be used to provide a URL or contact address for recipients if they have any queries about the messages they have received. If the setting "Information Header" is blank, this message will not be added to the Mail Header.

Multiple Headers

Default: append

When a message passes through more than one MailScanner server on your site, they will each try to add their own headers. This option controls what should happen when trying to add a MailScanner header that already exists in the message. Valid options are append (append the new data to the existing header), add (add a new header) and replace (replace the old data with the new data).

Hostname

Default: the MailScanner

This is the name of the MailScanner server that is put in messages to users. If you have more than one MailScanner server on your site, you will want to change this on each server so that you can tell them apart.

Sign Messages Already Processed

Default: no

If a message has already been processed by another MailScanner server on your site, then the "Inline HTML/Text Signature" is not added to the message again if this option is set. Without it, you will get one signature added for every MailScanner server that processes the message.

Sign Clean Messages

Default: no

If this option is set, then the "Inline HTML/Text Signature" will be added to the end of every clean message processed by MailScanner. You can use this to inform the recipient that the message has been checked, and also to add any legal disclaimer or copyright statement you want to add to every message. Using a ruleset for this option, you could very simply set it so that only messages leaving your site are signed, for example.

Mark Infected Messages

Default: yes

If this option is set, then the "Inline HTML/Text Warning" is added to the start of every message that is found to be infected or has had attachments removed for any reason. This can be used to guide the recipients to read the infection reports contained in the replacement attachments.

Mark Unscanned Messages

Default: yes

If this option is set, then any message which is not scanned by MailScanner gets the "Mail Header" added to it with the string

contained in the "Unscanned Header Value" option. This can be used to advertise your MailScanner service to customers/clients who are currently not using it.

Unscanned Header Value

Default: Not scanned: please contact your Internet E−Mail Service Provider for details

This supplies the text that is placed in the "Mail Header" of messages that have not been scanned, if the option "Mark Unscanned Messages" is set. It is a useful place to advertise your MailScanner service to new customers/clients.

Remove These Headers

Default:

If any of these headers are included in a 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, such as # X−Mozilla−Status. 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.

Deliver Cleaned Messages

Default: yes

Once a message has had all viruses and dangerous content removed from it, it will then be delivered to the original recipients if this option is set. If you want the behaviour from previous versions of MailScanner that had the "Deliver From Local Domains" keyword, then you should set this to be a ruleset that only returns "yes" for messages destined for inside your site, and "no" for messages going out of your site.

Notifications back to the senders of blocked messages

Notifiy Senders

Default: yes

Do you want to notify the people who sent you messages containing viruses or badly−named filenames? The default value has been changed to "no" as most viruses now fake sender addresses and therefore should be on the "Silent Viruses" list. This can also be the filename of a ruleset.

Notify Senders Of Blocked Filenames Or Filetypes

Default: yes

If "Notify Senders" 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.

Notify Senders Of Other Blocked Content

Default: yes

If "Notify Senders" 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.

Notify Senders Of Viruses

Default: no

If "Notify Senders" is set to yes, do you want to notify people who sent you messages containing viruses? This can also be the filename of a ruleset.

Never Notify Senders Of Precedence

Default: 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.

Changes to subject line

Scanned Modify Subject

Default: no # end

If this is set to "start" or "end" then the "Scanned Subject Text" is inserted at the start or the end of the Subject: line. This only happens if the Subject: line has not already been modified for any other reason.

Scanned Subject Text

Default: {Scanned}

This is the text inserted at the start or the end of the Subject: line if the "Scanned Modify Subject" option above is in effect.

Virus Modify Subject

Default: yes

If this is set, then the "Subject:" line of a message that was infected with a virus will have the "Virus Subject Text" text inserted at the start.

Virus Subject Text

Default: {Virus?}

This is the text inserted at the start of the "Subject:" line if the

"Virus Modify Subject" option is set.

Filename Modify Subject

Default: yes

If this is set, then the "Subject:" line of a message that had an attachment with a dangerous filename will have the "Filename Subject Text" text inserted at the start.

Filename Subject Text

Default: {Virus?}

This is the text inserted at the start of the "Subject:" line if the "Filename Modify Subject" option is set.

Content Modify Subject

Default: yes

If this is set, then the "Subject:" line of a message that triggered a content check without anything else wrong in the message will have the "Content Subject Text" text inserted at the start.

Content Subject Text

Default: {Filename?}

This is the text inserted at the start of the "Subject:" line if the "Content Modify Subject" option is set.

Disarmed Modify Subject

Default: 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.

Disarmed Subject Text

Default: {Disarmed}

This is the text to add to the start of the subject if the "Disarmed Modify Subject" option is set. This can also be the filename of a ruleset.

Spam Modify Subject

Default: yes

If this is set, then the "Subject:" line of a message that was determined to be spam will have the "Spam Subject Text" text inserted at the start.

Spam Subject Text

Default: {Spam?}

This is the text to add to the start of the subject if the "Spam Modify Subject" option is set. The exact string "_SCORE_" will be replaced by the numeric SpamAssassin score. This can also be the filename of a ruleset.

High Scroing Spam Modify Subject

Default: yes

If this is set, then the "Subject:" line of a message that was determined to be spam, and had a SpamAssassin score greater than the "High SpamAssassin Score" will have the "High Scoring Spam Subject Text" text inserted at the start.

High Scoring Spam Subject Text

Default: {Spam?}

This is just like the "Spam Subject Text" option above, except that it applies then the score from SpamAssassin is higher than the "High SpamAssassin Score" value. The exact string "_SCORE_" will be replaced by the numeric SpamAssassin score. This can also be the filename of a ruleset.

Changes to the message body

Warning Is Attachment

Default: yes

When an infected or dangerous attachment is replaced with a text message containing the infection report, should the replacement be an attachment (yes) or should it be included inline in the main text of the message (no).

Attachment Warning Filename

Default: %org−name%−Attachment−Warning.txt

What an infected or dangerous attachment is replaced with a text message containing the infection report, this is the filename of the attachment that appears in the message.

Attachment Encoding Charset

Default: ISO−8859−1

This is the name of the encoding character set used for the contents of "VirusWarning.txt" attachments.

Mail archiving and monitoring

Archive Mail

Default:

Space−separated list of any combination of

1. email addresses to which mail should be forwarded,
2. directory names where you want mail to be stored,
3. file names to which mail will be appended.

The files (option 3) are using the "mbox" format suitable for most Unix mail systems. These files must already exist since MailScanner will not create them!

If you give this option a ruleset, you can control exactly whose mail is archived or forwarded. If you do this, beware of the legal implications as this could be deemed to be illegal interception unless the police have asked you to do this.

Any of the items above can contain the magic string _DATE_ in them which will be replaced with the current date in yyyymmdd format. This will make archive−rolling and maintenance much easier, as you can guarantee that yesterday's mail archive will not be in active use today.

Notices to system administrators

Send Notices

Default: yes

Should system administrators listed in the "Notices To" option be notified of every infection found?

Notices Include Full Headers

Default: no

If this option is set, then the system administrator notices will include the full headers of every infected message. If this option is set to "no" then only a restricted set of headers is included in the notices.

Hide Incoming Work Dir in Notices

Default: no

When this option is set, the full directory in which the virus was found will be removed from report messages sent to administrators. This makes the infection reports a lot easier to understand. It is also very useful if your notices go to your customer sites.

Notice Signature

Default: −− \nMailScanner\nEmail Virus Scanner\nwww.mailscanner.info

This string is added to the bottom of all system administrator notices, and is intended to be the signature of your MailScanner system. To insert "line−breaks" or "newline" characters, use the sequence 0

Notices From

Default: 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.

Notices To

Default: postmaster

This option provides a list of the addresses to which virus

notices should be sent. You may want to set this to be a ruleset, providing different notification addresses for different domains that you administer.

Local Postmaster

Default: postmaster

When virus warnings are sent to any users, this is the email address used as the "From:" header in the messages.

Definitions of virus scanners and spam detectors

Spam List Definitions

Default: %etc−dir%/spam.lists.conf

This file contains all the definitions of the "Spam Lists" (also known as RBL's or DNSBL's) which can be used to try to detect spam based on where each message came from. Many more spam lists can be added to this file, but it contains the most popular ones to get you started.

Virus Scanner Definitions

Default: %etc−dir%/virus.scanners.conf

This file contains the locations of all the commands that are run for each virus scanner. Check this file before starting MailScanner to make sure it will run the correct command or wrapper script.

Spam detection and spam lists (DNS blocklists)

Spam Checks

Default: yes

If this option is set, messages will be checked to see if they are spam.

Spam List

Default: ORDB−RBL Infinite−Monkeys

This provides a space−separated list of "Spam Lists" (or RBL's or DNSBL's) which are checked for each message. These lists are based on the numeric IP address of the server that sent the message to your MailScanner server. Every list used here must be defined in the "Spam List Definitions" file mentioned above.

Spam Domain List

Default:

This provides a space−separated list of "Spam Lists" (or RBL's or DNSBL's) which are checked for each message. These lists are based on the domain name of the sender address of each message. Every list used here must be defined in the "Spam List Definitions" file mentioned above.

Spam Lists To Be Spam

Default: 1

If a message appears in at least this number of "Spam 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 behaviour, 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.

Spam Lists To Reach High Score

Default: 5

If a message appears in at least this number of "Spam Lists" (as defined above), then the message will be treated as "High Scoring Spam" and so the "High Scoring Spam Actions" will happen. You probably want to set this to 2 if you are actually using this feature. 5 is high enough that it will never happen unless you use lots of "Spam Lists". This can also be the filename of a ruleset.

Spam List Timeout

Default: 10

This is the number of seconds to wait for each "Spam List" lookup to complete. If the lookup takes longer than this, it is killed and ignored.

Max Spam List Timeouts

Default: 7

If a "Spam List" lookup times out for this many consecutive checks without ever succeeding, then the particular "Spam List" entry will not be used any more, as it appears to be unreachable. When MailScanner restarts itself after a few hours, MailScanner will try to use the entry again, in case service has resumed properly.

Spam List Timeouts History

Default: 10

The total number of Spam List attempts during which "Max Spam List Timeouts" will cause the spam list fo be marked as "unavailable". See the previous comment for more information. The default values of 5 and 10 mean that 5 timeouts in any sequence of 10 attempts will cause the list to be marked as "unavailable" until the next periodic restart (see "Restart Every").

Is Definitely Not Spam

Default: %rules-dir%/spam.whitelist.rules

This option would normally be a ruleset. Any messages for which the ruleset result is "yes" will never be marked as spam. This is used to create a spam "whitelist" of addresses which are never spam. You will probably want to include your own site (or your own site's IP addresses) in this ruleset.

Is Definitely Spam

Default: no

This option would normally be a ruleset. Any messages for which the ruleset result is "yes" will always be marked as spam. This is used to create a spam "blacklist" of addresses of known spammers.

Definite Spam Is High Scoring

Default: no

Setting this to yes means that spam found in the blacklist is treated as "High Scoring Spam" in the "Spam Actions" section below. Setting it to no means that it will be treated as "normal" spam. This can also be the filename of a ruleset.

Ignore Spam Whitelist If Recipients Exceed

Default: 20

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

SpamAssassin

Use SpamAssassin

Default: no

Do you want to detect spam using the very good SpamAssassin package? You must have installed SpamAssassin before using this option, otherwise MailScanner will not start properly.
NOTE for FreeBSD port user: The SpamAssassin port is not automatically installed with the MailScanner port. You can find it at /usr/ports/mail/p5−Mail−SpamAssassin.

Max SpamAssassin Size

Default: 90000

SpamAssassin is quite slow when processing very large messages. To work round this problem, this option provides a maximum size for messages that are processed with SpamAssassin. Most real spam is usually less than about 50,000 bytes per message.

Required Spam Assassin Score

Default: 6

This gives the minimum SpamAssassin score value above which messages are spam. This replaces SpamAssassin's own "required_hits" value, so that it can be a ruleset and set to different values for different users/domains.

High SpamAssassin Score

Default: 20

Messages with a SpamAssassin score greater than this value are labelled as being "High Scoring Spam", and a different set of "Spam Actions" are applied to messages scoring at least this value.

SpamAssassin Auto Whitelist

Default: no

SpamAssassin has a feature which measures the ratio of spam to non−spam originating from different addresses, and will automatically add addresses to its own internal "whitelist" if most of the messages from an address is not spam. This option enables this feature of SpamAssassin. Please read their documentation for more information.

SpamAssassin Prefs File

Default: %etc−dir%/spam.assassin.prefs.conf

SpamAssassin uses a "user preferences" file which can be used to set the values of various SpamAssassin options. This is the name of that file. Its most useful feature is that the RBL/DNSBL/"Spam List" checks done by SpamAssassin can be disabled as MailScanner already does them and there is little to be gained by doing these checks twice for every message.

SpamAssassin Timeout

Default: 30

This option sets the maximum number of seconds to wait for SpamAssassin to process a message. This is a useful protection against occasional bugs in SpamAssassin that can cause it to take hours to process a single message.

Max SpamAssasin Timeouts

Default: 20

If several consecutive calls to SpamAssassin time out, then MailScanner decides that there is something stopping SpamAssassin from working properly. It will therefore be disabled for the next few hours until MailScanner restarts itself, at which point it will be tried again.

SpamAssassin Timeouts History

Default: 30

The total number of SpamAssassin attempts during which "Max SpamAssassin Timeouts" will cause SpamAssassin to be marked as "unavailable". See the previous comment for more information. The default values of 10 and 20 mean that 10 timeouts in any sequence of 20 attempts will trigger the behaviour described above, until the next periodic restart (see "Restart Every").

Check SpamAssassin If On Spam List

Default: yes

If a message has already triggered any of the "Spam List" checks, the SpamAssassin check will be skipped if this option is set to "no". This can help reduce the load on your server if SpamAssassin checks take a long time for some reason.

Always Include SpamAssasin Report

Default: no

If this option is set, then the "Spam Header" will be included in the header of every message, so its presence cannot be used to filter out spam by your users' e−mail applications.

Spam Score

Default: yes

If a message is spam, and this option is set, then a header will be added to the message containing 1 character for each point in the SpamAssassin score. This allows users to choose for themselves the SpamAssassin scores at which they want to do different things with the message, such as file it or delete it.

Rebuild Bayes Every

Default: 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. This is measures in seconds. 24 hours = 86400 seconds. To disable this feature set this to 0.

Wait During Bayes Rebuild

Default: no

The Bayesian database rebuild 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. WaitDuringBayesRebuild = no

What to do with spam

Spam Actions

Default: deliver

This can be any combination of 1 or more of the following keywords, and these actions are applied to any message which is spam.

- deliver − the message is delivered to the recipient as normal
- delete − the message is deleted
- store − the message is stored in the quarantine
- forward − an email address is supplied, to which the message is forwarded
- 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 orginal message if they think it was not spam.

- striphtml − convert all in−line HTML content in the message to be stripped to plain text, which removes all images and scripts and so can be used to protect your users from offensive spam. Note that using this action on its own does not imply that the message will be delivered, you will need to specify "deliver" or "forward" to actually deliver the message.

- 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.

- bounce − bounce the spam message. This option should not be used and must be enabled with the "Enable Spam Bounce" option first.

- header "name: value" − Add the header "name: value" to the message. name must not contain any spaces.

High Scoring Spam Actions

Default: deliver

This is the same as the "Spam Actions" option above, but it gives the actions to apply to any message whose SpamAssassin score is above the "High Scoring" threshold described above.

Non Spam Actions

Default: deliver

This is the same as the "Spam Actions" option above, except that it applies to messages that are NOT spam. The bounce option does not make much sense here so do not use it.

Sender Spam Report

Default: %reports−dir%/sender.spam.report.txt

When the "bounce" spam action is applied to a message that triggered both a "Spam List" check and SpamAssassin, this file gives the text to put in that message.

Sender Spam List Report

Default: %reports−dir%/sender.spam.rbl.report.txt

When the "bounce" spam action is applied to a message that triggered a "Spam List" check, this file gives the text to put in that message.

Sender SpamAssassin Report

Default: %reports−dir%/sender.spam.sa.report.txt

When the "bounce" spam action is applied to a message that triggered SpamAssassin, this file gives the text to put in that message.

Inline Spam Warning

Default: %reports−dir%/inline.spam.warning.txt

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

Recipient Spam Report

Default: %reports−dir%/recipient.spam.report.txt

If you use the ’notify’ Spam Action or High Scoring Spam Action

then this is the location of the notification message that is sent to the original recipients of the message.

Enable Spam Bounce

Default: %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 mis−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.

System logging

Syslog Facility

Default: mail

This is the name of the "facility" used by syslogd to log MailScanner’s messages. If this doesn’t mean anything to you, then either leave it alone or else read the "syslogd" man page.

Log Speed

Default: 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.

Log Spam

Default: no

If this option is set, then every spam message will be logged to

syslog. If you get a lot of spam, or your server load is high, you will want to leave this option switched off. But if you are having trouble with spam detection, setting this to "yes" temporarily can provide useful debugging output.

Log Non Spam

Default: no

Do you want all non−spam to be logged? Useful if you want to see all the SpamAssassin reports of mail that was marked as non−spam. Note: It will generate a lot of log traffic.

Log Permitted Filenames

Default: no

If this option is set, then every attachment filename that passes the "filename rules" checks will be logged to syslog. Normally this is of no interest. But if you are having trouble getting your filename rules correct, setting, this can provide useful debugging output.

Log Permitted Filetypes

Default: 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.

Log Silent Viruses

Default: no

Log all occurrences of "Silent Viruses" as defined above? This can only be a simple yes/no value, not a ruleset.

Log Dangerous HTML Tags

Default: no
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.

Advanced SpamAssassin Settings

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

SpamAssassin User State Dir

Default:

The per−user files (bayes, auto−whitelist, user_prefs) are looked for here and in ~/.spamassassin/. Note the files are mutable. If this is unset then no extra places are searched for. NOTE: SpamAssassin is always called from MailScanner as the same user, and that is the "Run As" user specified in MailScanner.conf. So you can only have 1 set of "per−user" files, it's just that you might possibly need to modify this location. You should not normally need to set this at all. If using Postfix, you probably want to set this to /var/spool/MailScanner/spamassassin and do

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

SpamAssassin Install Prefix

Default:

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.

SpamAssassin Local Rules Dir

Default:

This tells MailScanner where to look for the site−local rules. If this is set it adds to the list of places that are searched. MailScanner will always look at the following places (even if this option is not set):

- prefix/etc/spamassassin
- prefix/etc/mail/spamassassin
- /usr/local/etc/spamassassin
- /etc/spamassassin
- /etc/mail/spamassassin
- maybe others as well

SpamAssassin Default Rules Dir

Default:

This tells MailScanner where to look for the default rules. If this is set it adds to the list of places that are searched. MailScanner will always look at the following places (even if this option is not set):

- prefix/share/spamassassin

- /usr/local/share/spamassassin
- /usr/share/spamassassin
- maybe others as well

Advanced Settings

Spam Score Number Format

Default: %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. This can also be the filename of a ruleset. A few examples for you:

%d	==> 12
%5.2f	==> 12.34
%05.1f	==> 012.3

Debug

Default: no

Not for use by normal users. Setting this option to "yes" will put MailScanner into debugging mode, in which it creates slightly more output and will not become a daemon.

Debug SpamAssassin

Default: no

Do you want to debug SpamAssassin from within MailScanner?

Run In Foreground

Default: 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).

LDAP Server

Default:

If you are using an LDAP server to read the configuration, these are the details required for the LDAP connection. The connection is anonymous. Example: localhost

LDAP Base

Default:

If you are using an LDAP server to read the configuration, these are the details required for the LDAP connection. The connection is anonymous. Example: o=fsl

LDAP Site

Default:

If you are using an LDAP server to read the configuration, these are the details required for the LDAP connection. The connection is anonymous. Example: default

Always Looked Up Last

Default: no

The value of the option is actually never used, but it is evaluated at the end of processing a batch of messages. It is designed to be used in conjunction with a Custom Function. The Custom Function should then be written to have a "side effect" of doing something useful such as logging lots of information about the batch of messages to a file or an SQL database.

Deliver in Background

Default: yes

When attempting delivery of any messages (when the "Delivery Method = batch") the sendmail/Exim command will be run in the background so that MailScanner does not have to wait for the delivery attempt to complete. There are very few good reasons for setting this to "no".

Lockfile Dir

Default: /tmp

This is the directory in which lock files are placed to stop the virus scanners used while they are in the middle of updating themselves with new virus definitions. If you change this at all, you will need to edit the "autoupdate" scripts for all your virus scanners.

Custom Functions Dir

Default: /opt/MailScanner/lib/MailScanner/CustomFunctions
Default FreeBSD:
/usr/local/lib/MailScanner/MailScanner/CustomFunctions

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.

Lock Type

Do not set this option to anything unless you know exactly what you are doing. For sendmail and Exim, MailScanner will choose the correct value by default. This affects how mail queue files are locked, and your mail will be totally screwed up if you set this option to anything other than the correct value for your MTA. So leave it alone and let MailScanner choose the correct value for you.

Minimum Code Status

Default: supported

Minimum acceptable code stability status −− if we come across code that's not at least as stable as this, we barf. This is currently only used to check that you don't end up using untested virus scanner support code without realising it. 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. Levels used 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.

Split Exim Spool

Default: yes

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

Use Default Rules With Multiple Recipients

Default: no

When trying to work out the value of configuration parameters which are using a ruleset, this controls the behaviour when a rule is checking the "To:" addresses. 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.
If this option is set to "yes", then the following happens when checking the ruleset:

a) 1 recipient. Same behaviour as normal.

b) Several recipients, but all in the same domain (domain.com for example). The rules are checked for one that matches the string "*@domain.com".

c) Several recipients, not all in the same domain. The rules are checked for one that matches the string "*@*".

RULESETS

Ruleset files should all be put in /opt/MailScanner/etc/rules (FreeBSD: /usr/local/etc/MailScanner/rules) and their filename should end in ".rules" wherever possible.

All blank lines are ignored, and comments start with "#" and continue to the end of the line, like this: # This line is just a comment

Other than that, every line is a rule and looks like this example: From: john.doe@domain.com yes

As you can see, each rule has 3 fields:
1. Direction
2. Pattern to match
3. Result value (or values)

1. Direction should be one of the following:

From:	Matches when the message is from a matching address
To:	Matches when the message is to a matching address
FromOrTo:	Matches when the message is from or to a matching address
FromAndTo:	Matches when the message is from and to a matching address

The syntax of these is very loosely defined. Any word containing "from", any word containing "to", any word containing "from" and "to" (in either order), and any word containing "and" will work just fine. You can put them in upper or lower case, it doesn't matter. And any additional punctuation will be ignored.

This specifies the whether the rule should be matched against the sender's address (or IP address), or the recipient's address.

2. The pattern describes what messages should match this rule. Some examples are:

user@sub.domain.com # Individual address
user@* # 1 user at any domain
*@sub.domain.com # Any user at 1 domain

@.domain.com # Any user at any sub−domain of "domain.com"
*@domain.com # Any user at 1 specific domain
/pattern/ # Any address matching this Perl regular
expression
192.168. # Any SMTP client IP address in this network
/pattern−with−no−letters/ # Any SMTP client IP address matching this
Perl regular expression
/^192.168.1[4567]./ # Any SMTP client IP address in the networks
192.168.14 − 192.168.17
@ # Default value
default # Default value

You should be able to do just about anything with that.

3. The result value is what you could have put in the entry in the main mailscanner.conf file had you not given the filename of a ruleset instead.

See the file EXAMPLES for a few ideas on how to do things with this system.

ATTACHMENT FILENAME RULESET

This is held in the filename pointed to by the configuration option Filename rules. It contains a set of rules that are used to judge whether any given file attachment should be accepted or rejected on the basis of its filename, regardless of whether it is found to be virus−infected or not. This can not only be used for draconian measures such as banning all .exe attachments, but it can be used with any Perl regular expression to provide facilities such as detection of attempts at hiding filenames.

Many Windows e−mail programs (eg. Microsoft Outlook) hide common file extensions in an attempt to not baffle the user. The result is that while an attachment called "Your Document.doc" is helpfully displayed as "Your Document", a more sinister attachment just as "Looks Safe.txt.pif" will appear simply as "Looks Safe.txt". Many users recognise the .txt filename extension as applying to plain text files, which they know are safe. So even an experienced user may well double−click on this attachment thinking it is just going to start Notepad and display the text file. However, the file is really an MS−Dos shortcut (.pif file) and can execute any arbitrary commands the author wanted: all without any indication to the unwitting user.

The rules are matched in order from the top to the bottom of the file, and the first rule containing a matching regular expression is used. Each line of the file is either blank, a comment (in which case it starts with a '#' character) or is a rule made up of 4 fields separated by one or more TAB characters:

allow / deny

Accept or reject the attachment if its filename matches the regular expression

regular expression

The rule is executed if the attachment matches this expression. It may optionally be surrounded in '/' characters.

log text

If the rule matches, this text is placed in the syslog. If the text is "−", no string is logged.

user text

If the rule matches, this text is placed in the text message sent to the user. If the text is "−", no text is used.

Please have a look at the filename.rules.conf or filename.rules.conf.sample file provided with this distribution/package/port.

SEE ALSO

MailScanner(8)

> *MailScanner would like to thank the following for their support:*