Version 4.42.9

MailScanner.conf Reference Manual Version 1.1

Table of Content

1. Introduction

Main configuration file for the MailScanner E-Mail Virus Scanner

It's good practice to check through configuration files to make sure they fit with your system and your needs, whatever you expect them to contain.

Note: If your directories are symlinked (soft-linked) in any way, please put their *real* location in here, not a path that includes any links. You may get some very strange error messages from some of the virus scanners if you don't.

Note for Version 4.00 and above: 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.

Note for Version 4.03 and above: As well as rulesets, you can now include your own functions in here. Look at the directory containing Config.pm and you will find CustomConfig.pm. In here, you can add your own "value" function and an Initvalue function to set up any global state you need such as database connections. Then for a setting below, you can put:

```
    Configuration Option = &ValueFunction
```

where "ValueFunction" is the name of the function you have written in CustomConfig.pm.

2. Variables

Definition of variables which are substituted into definitions below. You can add any %variables% that you want to use in addition to the ones provided. You can also use any shell environment variables here such as $HOSTNAME or {HOSTNAME} in configuration settings and rulesets. See the definition of "Hostname" for an example.

%report-dir%

Set the directory containing all the reports in the required language

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

%etc-dir%

Configuration directory containing this file

Default:
%etc-dir% = /etc/MailScanner

%rules-dir%

Rulesets directory containing your ".rules" files

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

%mcp-dir%

Configuration directory containing files related to MCP(Message Content Protection)

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

%org-name%

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. Some other mail servers complain about "_" characters appearing in the names of headers as well. So don't put "." or "_" in this setting.

RULE: It must not contain any spaces!

Default:
%org-name% = yoursite

%org-long-name%

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 "\n" sequences in the text. These will be replaced by line-breaks.

Default:
%org-long-name% = Your Organisation Name Here

%web-site%

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.

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

3. System settings

Max Children

How many MailScanner processes do you want to run at a time? There is no point increasing this figure if your MailScanner server is happily keeping up with your mail traffic. 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. If you are running on a small system with limited RAM, you should note that each child takes just over 20MB. As a rough guide, try 5 children per CPU. But read the notes above.

Default:
Max Children = 5

Run As User

User to run 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 file.
Run As User = mail
Run As User = postfix

Default:
Run As User =

Run As Group

Group to run as (not normally used for sendmail)
Run As Group = mail
Run As Group = postfix

Default:
Run As Group =

Queue Scan Interval

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.

Default:
Queue Scan Interval = 6

Incoming Queue Dir

Set location of incoming mail queue

This can be any one of
1. A directory name
   Default: /var/spool/mqueue.in
2. A wildcard giving directory names
   Default: /var/spool/mqueue.in/*
3. The name of a file containing a list of directory names, which can in turn contain wildcards.
   Default: /etc/MailScanner/mqueue.in.list.conf

If you are using sendmail and have your queues split into qf, df, xf directories, then just specify the main directory, do not give me the directory names of the qf,df,xf directories.
Default: if you have /var/spool/mqueue.in/qf
/var/spool/mqueue.in/df
/var/spool/mqueue.in/xf
then just tell me /var/spool/mqueue.in. I will find the subdirectories automatically.

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

Outgoing Queue Dir

Set location of outgoing mail queue. This can also be the filename of a ruleset.

Default:
Outgoing Queue Dir = /var/spool/mqueue

Incoming Work Dir

Set where to unpack incoming messages before scanning them This can completely safely use tmpfs or a ramdisk, which will give you a significant performance improvement.
NOTE: The path given here must not include any links at all, but must be the absolute path to the directory.

Default:
Incoming Work Dir = /var/spool/MailScanner/incoming

Quarantine Dir

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

Default:
Quarantine Dir = /var/spool/MailScanner/quarantine

PID file

Set where to store the process id number so you can stop MailScanner

Default:
PID file = /var/run/MailScanner.pid

Restart Every

To avoid resource leaks, re-start periodically

Default:
Restart Every = 14400

MTA

Set whether to use postfix, sendmail, exim or zmailer. If you are using postfix, then see the "SpamAssassin User State Dir" setting near the end of this file

Default:
MTA = sendmail

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.

Default:
Sendmail = /usr/sbin/sendmail

Sendmail2

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. This can also be the filename of a ruleset.
For Exim users: Sendmail2 = /usr/sbin/exim -C /etc/exim/exim_send.conf
For sendmail users: Sendmail2 = /usr/sbin/sendmail

Default:
Sendmail2 = /usr/sbin/sendmail

4. Incoming Work Dir Settings

Incoming Work User / Incoming Work Group

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.

If you want to create the temporary working files so they 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 "Incoming Work Group".

Default:
Incoming Work User =
Incoming Work Group =

Incoming Work Permissions

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.

Default:
Incoming Work Permissions = 0600

5. Quarantine and Archive Settings

Quarantine User / Quarantine Group

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!

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".

Default:
Quarantine User =
Quarantine Group =

Quarantine Permissions

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.

Default:
Quarantine Permissions = 0600

6. Processing Incoming Mail

Max Unscanned Bytes Per Scan / Max Unsafe Bytes Per Scan

Max Unscanned Messages Per Scan / Max Unsafe Messages Per Scan

In every batch of virus-scanning, limit the maximum
a) number of unscanned messages to deliver
b) number of potentially infected messages to unpack and scan
c) total size of unscanned messages to deliver
d) total size of potentially infected messages to unpack and scan

Default:
Max Unscanned Bytes Per Scan = 100000000
Max Unsafe Bytes Per Scan = 50000000
Max Unscanned Messages Per Scan = 30
Max Unsafe Messages Per Scan = 30

Max Normal Queue Size

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".

Default:
Max Normal Queue Size = 800

Maximum Attachments Per Message

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.

Default:
Maximum Attachments Per Message = 200

Expand TNEF

Expand TNEF attachments using an external program (or a 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.

Default:
Expand TNEF = yes

Deliver Unparsable TNEF

Some versions of Microsoft Outlook generate unparsable Rich Text format attachments. Do we want to deliver these bad attachments anyway? Setting this to yes introduces the slight risk of a virus getting through, but if you have a lot of troubled Outlook users you might need to do this. We are working on a replacement for the TNEF decoder. This can also be the filename of a ruleset.

Default:
Deliver Unparsable TNEF = no

TNEF Expander

Where the MS-TNEF expander is installed. This is EITHER the full command (including maxsize option) that runs the external TNEF expander binary, OR the keyword "internal" which will make MailScanner use the Perl module that does the same job. They are both provided as I am 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. This can also be the filename of a ruleset. Example:
TNEF Expander = /usr/bin/tnef --maxsize=100000000

Default
TNEF Expander = internal

TNEF Timeout

The maximum length of time the TNEF Expander is allowed to run for 1 message (in seconds)

Default:
TNEF Timeout = 120

File Command

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.

Default:
File Command = #DISABLED /usr/bin/file

File Timeout

The maximum length of time the "file" command is allowed to run for 1 batch of messages (in seconds)

Default:
File Timeout = 20

Unrar Command

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.

Default:
Unrar Command = /usr/bin/unrar

Unrar Timeout

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

Default:
Unrar Timeout = 50

Maximum Message Size

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.

Default:
Maximum Message Size = 0

Maximum Attachment Size

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.

Default:
Maximum Attachment Size = -1

Minimum Attachment Size

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.

Default:
Minimum Attachment Size = -1

Maximum Archive Depth

The maximum depth to which zip archives will be unpacked, to allow for checking filenames and filetypes within zip archives.

Note: This setting does *not* affect virus scanning in archives at all.

To disable this feature set this to 0. A common useful setting is this option = 0, and Allow Password-Protected Archives = no. That block password-protected archives but does not do any filename/filetype checks on the files within the archive. This can also be the filename of a ruleset.

Default:
Maximum Archive Depth = 2

Find Archives By Content

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.

Default:
Find Archives By Content = yes

7. Virus Scanning and Vulnerability Testing

Virus Scanners

Do you want to scan email for viruses? A few people don't have a virus scanner licence and so want to disable all the virus scanning. If you use a ruleset for this setting, then the mail will be scanned if *any* of the rules match (except the default). That way unscanned mail never reaches a user who is having their mail virus-scanned.

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. This can also be the filename of a ruleset.

Default:
Virus Scanning = yes

Which Virus Scanning package to use:

sophos	www.sophos.com
sophossavi	www.sophos.com, using the SAVI perl module
mcafee	www.mcafee.com, or
command	www.command.co.uk, or
bitdefender	www.bitdefender.com, or
drweb	www.dials.ru/english/dsav_toolkit/drwebunix.htm
kaspersky-4.5	www.kaspersky.com (Version 4.5 and newer)
kaspersky	www.kaspersky.com

kavdaemonclient	www.kaspersky.com
etrust	www3.ca.com/Solutions/Product.asp?ID=156
inoculate	www.cai.com/products/inoculateit.htm
inoculan	ftp.ca.com/pub/getbbs/linux.eng/inoctar.LINUX.Z
nod32	www.nod32.com
nod32-1.99	www.nod32.com
f-secure	www.f-secure.com
f-prot	www.f-prot.com
panda	www.pandasoftware.com
rav	www.ravantivirus.com
antivir	www.antivir.de
clamav	www.clamav.net
clamavmodule	www.clamav.net using the ClamAV perl module
trend	www.trendmicro.com
Norman	www.norman.de
Css	www.symantec.com
Avg	www.grisoft.com
Vexira	www.centralcommand.com
Symscanengine	www.symantec.com (Symantec Scan Engine, not CSS)
generic	One you wrote: edit the generic-wrapper and generic-autoupdatexto fit your own needs. The output spec is in generic-wrapper
none	No virus scanning at all.

Note for McAfee users: do not use any symlinks with McAfee at all. It is very strange but 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. For Default: Virus Scanners = sophos f-prot mcafee

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.

This *cannot* be the filename of a ruleset.

Default:
Virus Scanners = none

Virus Scanner Timeout

The maximum length of time the commercial virus scanner is allowed to run for 1 batch of messages (in seconds).

Default:
Virus Scanner Timeout = 300

Deliver Disinfected Files

Should I attempt to disinfect infected attachments and then deliver the clean ones. "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. 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. This can also be the filename of a ruleset.

Default:
Deliver Disinfected Files = no

Silent Viruses

Strings listed here will be searched for in the output of the virus scanners. It is used to list which viruses should be handled differently from other viruses. If a virus name is given here, then
1) The sender will not be warned that he sent it
2) No attempt at true disinfection will take place
   (but it will still be "cleaned" by removing the nasty attachments
    from the message)
3) The recipient will not receive the message,
   unless the "Still Deliver Silent Viruses" option is set

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/Data tags, when they are not allowed.
HTML-Script	: inserting this will stop senders being warned about HTML Script 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 (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. This can also be the filename of a ruleset.

Default:
Silent Viruses = HTML-IFrame All-Viruses

Still Deliver Silent Viruses

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, and 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
Note: this option to "no" so you don't bombard thousands of people with
Note: useless messages they don't want!

This can also be the filename of a ruleset.

Default:
Still Deliver Silent Viruses = no

Non-Forging Viruses

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, when they are not allowed. This will over-ride the All-Viruses setting in the list of "Silent Viruses" above.

Default:
Non-Forging Viruses = Joke/ OF97/ WM97/ W97M/ eicar

Block Encrypted Messages

Should encrypted messages be blocked? This is useful if you are wary about your users sending encrypted messages to your competition. This can be a ruleset so you can block encrypted message to certain domains.

Default:
Block Encrypted Messages = no

Block Unencrypted Messages

Should unencrypted messages be blocked? This could be used to ensure all your users send messages outside your company encrypted to avoid snooping of mail to your business partners. This can be a ruleset so you can just check mail to certain users/domains.

Default:
Block Unencrypted Messages = no

Allow Password-Protected Archives

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.

Default:
Allow Password-Protected Archives = no

Options specific to Sophos Anti-Virus

Allowed Sophos Error Messages

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. If you need to specify more than 1 string to find in the error message, then put each string in quotes and separate them with a comma. Example:
Allowed Sophos Error Messages = "corrupt", "format not supported"

Default:
Allowed Sophos Error Messages =

Sophos IDE Dir

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.

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

Sophos Lib Dir

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.

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

Monitors For Sophos

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.

Default:
Monitors For Sophos Updates = /usr/local/Sophos/ide/*ides.zip

Options specific to ClamAV Anti-Virus

Monitors for ClamAV Updates
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.

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

ClamAVmodule Maximum Recursion Level / ClamAVmodule Maximum Files

ClamAVmodule Maximum File Size / ClamAVmodule Maximum Compression Ratio

ClamAVModule only: set limits when scanning for viruses. The maximum recursion level of archives, The maximum number of files per batch, The maximum file of each file, The maximum compression ratio of archive. These settings *cannot* be the filename of a ruleset, only a simple number.

Default:
ClamAVmodule Maximum Recursion Level = 5
ClamAVmodule Maximum Files = 1000
ClamAVmodule Maximum File Size = 10000000 # (10 Mbytes)
ClamAVmodule Maximum Compression Ratio = 250

8. Removing/Logging dangerous or potentially offensive content

Dangerous Content Scanning

Do you want to scan the messages for potentially dangerous content? Setting this to "no" will disable all the content-based checks except Virus Scanning, Allow Partial Messages and Allow External Message Bodies. This can also be the filename of a ruleset.

Default:
Dangerous Content Scanning = yes

Allow Partial Messages

Do you want to allow partial messages, which only contain a fraction of the attachments, not the whole thing? There is absolutely no way to scan these "partial messages" properly for viruses, as 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.

Default:
Allow Partial Messages = no

Allow External Message

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 dangerous as it can allow viruses to be fetched from other Internet sites by a user's email package. The user would just think it was a normal email attachment and would have been scanned by MailScanner. It is only currently supported by Netscape 6 anyway, and the only people who it are the IETF. So I would strongly advise leaving this switched off. This can also be the filename of a ruleset.

Default:
Allow External Message Bodies = no

Find Phishing Fraud

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 extra load, particularly on systems receiving lots of spam such as secondary MX hosts. This can also be the filename of a ruleset.

Default:
Find Phishing Fraud = yes

Also Find Numeric Phishing

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 can also be the filename of a ruleset.

Default:
Also Find Numeric Phishing = yes

Phishing Safe Sites File

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.

Default:
Phishing Safe Sites File = %etc-dir%/phishing.safe.sites.conf

Allow IFrame Tags

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

Default:
Allow IFrame Tags = disarm

Allow Form Tags

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.
Value: 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
Note: Disarming can be defeated, it is not 100% safe!
This can also be the filename of a ruleset.

Default:
Allow Form Tags = disarm

Allow Script Tags

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.
Value: 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
Note: Disarming can be defeated, **it is not 100% safe!**
This can also be the filename of a **ruleset.**

Default:
Allow Script Tags = disarm

Allow WebBugs

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.
Value: yes => Allow these tags to be in the message
disarm => Allow these tags, but stop these tags from working
Note: Disarming can be defeated, it is not 100% safe!
Note: You cannot block messages containing web bugs as their detection is very vulnerable to false alarms. This can also be the filename of a ruleset.

Default:
Allow WebBugs = disarm

Allow Object Codebase

Do you want to allow <Object Codebase=...> or <Object Data=...> 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.
Value: 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
This can also be the filename of a ruleset, so you can allow them just for specific users or domains.

Default:
Allow Object Codebase Tags = disarm

Convert Dangerous HTML To Text

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

Allow...Tags	Convert Danger...	Action Taken on HTML Message
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

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. This can also be the filename of a ruleset, so you can make this apply only to specific users or domains.

Default:
Convert Dangerous HTML To Text = no

Convert HTML To Text

Do you want to convert all HTML messages into plain text? This is very useful for users who are children or are easily 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.

Default:
Convert HTML To Text = no

9. Attachment Filename Checking

Filename Rules

Set where to find the attachment filename ruleset. The structure of this file is explained elsewhere, but it is used to accept or reject file attachments based on their name, 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 is a ruleset or not!

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

Filetype Rules

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 is a ruleset or not! To disable this feature, set this to just "Filetype Rules =" or set the location of the file command to a blank string.

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

10. Reports and Responses

Quarantine Infections

Do you want to store copies of the infected attachments and messages? This can also be the filename of a ruleset.

Default:
Quarantine Infections = yes

Quarantine Silent Viruses

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

Default:
Quarantine Silent Viruses = no

Quarantine Whole Message

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.

Default:
Quarantine Whole Message = no

Quarantine Whole Messages As Queue Files

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 then body in 1 file)?

Default:
Quarantine Whole Messages As Queue Files = no

Keep Spam And MCP Archive Clean

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.

Default:
Keep Spam And MCP Archive Clean = no

Language Strings

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.

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

Deleted Reports

Set where to find the message text sent to users when one of their attachments has been deleted from a message. These can also be the filenames of rulesets.

Default:
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

Stored Reports

Set where to find 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.

Default:
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

Disinfected Report

Set where to find the message text sent to users explaining about the attached disinfected documents. This can also be the filename of a ruleset.

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

Inline HTML Signature / Inline Text Signature

Set where to find the HTML and text versions that will be added to the end of all clean messages, if "Sign Clean Messages" is set. These can also be the filenames of rulesets.

Default:
Inline HTML Signature = %report-dir%/inline.sig.html
Inline Text Signature = %report-dir%/inline.sig.txt

Inline HTML Warning / Inline Text Warning

Set where to find the HTML and text versions that will be inserted at the top of messages that have had viruses removed from them. These can also be the filenames of rulesets.

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

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

Sender Reports

Set where to find the messages that are delivered to the sender, when they sent an email containing either an error, banned content, a banned filename or a virus infection. These can also be the filenames of rulesets.

Default:
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

Hide Incoming Work Dir

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 just confuse users. This can also be the filename of a ruleset.

Default:
Hide Incoming Work Dir = yes

Include Scanner Name In Reports

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.

Default:
Include Scanner Name In Reports = yes

11. Changes to Message Headers

Mail Header

Add this extra header to all mail as it is processed. This *must* include the colon ":" at the end. This can also be the filename of a ruleset.

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

Spam Header

Add this extra header to all messages found to be spam. This can also be the filename of a ruleset.

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

Spam Score Header

Add this extra header if "Spam Score" = yes. The header will contain 1 character for every point of the SpamAssassin score.

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

Information Header

Add this extra header to all mail as it is processed. The contents is set by "Information Header Value" 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.

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

Add Envelope From Header

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.

Default:
Add Envelope From Header = yes

Add Envelope To Header

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.

Default:
Add Envelope To Header = no

Envelope From Header

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

Default:
Envelope From Header = X-%org-name%-MailScanner-From:

Envelope To Header

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

Default:
Envelope To Header = X-%org-name%-MailScanner-To:

Spam Score Character

The character to use in the "Spam Score Header".
Don't use: x as a score of 3 is "xxx" which the users will think is porn,
as it will cause confusion with comments in procmail as well
as MailScanner itself,

* as it will cause confusion with pattern matches in procmail,
. as it will cause confusion with pattern matches in procmail,
? as it will cause the users to think something went wrong.
"s" is nice and safe and stands for "spam".

Default:
Spam Score Character = s

SpamScore Number Instead Of Stars

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.

Default:
SpamScore Number Instead Of Stars = no

Minimum Stars If On Spam List

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.

Default:
Minimum Stars If On Spam List = 0

Header Value

Set the "Mail Header" to these values for clean/infected/disinfected messages. This can also be the filename of a ruleset.

Default:
Clean Header Value = Found to be clean
Infected Header Value = Found to be infected
Disinfected Header Value = Disinfected

Information Header Value

Set the "Information Header" to this value. This can also be the filename of a ruleset.

Default:
Information Header Value = Please contact the ISP for more information

Detailed Spam Report

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

Default:
Detailed Spam Report = yes

Include Scores In SpamAssassin Report

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

Default:
Include Scores In SpamAssassin Report = yes

Always Include SpamAssassin Report

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.

Default:
Always Include SpamAssassin Report = no

Multiple Headers

What to do when you get several MailScanner headers in one message, from multiple MailScanner servers. Values are
"append" : Append the new data to the existing header
"add" : Add a new header
"replace" : Replace the old data with the new data
Default is "append". This can also be the filename of a ruleset.

Default:
Multiple Headers = append

Hostname

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. Remember you can use $HOSTNAME in here, so you might want to set it to Hostname = the %org-name% ($HOSTNAME) MailScanner. This can also be the filename of a ruleset.

Default:
Hostname = the %org-name% ($HOSTNAME) MailScanner

Sign Messages Already Processed

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.

Default:
Sign Messages Already Processed = no

Sign Clean Messages

Add the "Inline HTML Signature" or "Inline Text Signature" to the end of uninfected messages? This can also be the filename of a ruleset.

Default:
Sign Clean Messages = no

Mark Infected Messages

Add the "Inline HTML Warning" or "Inline Text Warning" to the top of messages that have had attachments removed from them? This can also be the filename of a ruleset.

Default:
Mark Infected Messages = yes

Mark Unscanned Messages

When a message is to not be virus-scanned (which may happen depending upon the setting of "Virus Scanning", especially if it is a ruleset), do you want to add the header advising the users to get their email virus-scanned by you? Very good for advertising your MailScanning service and encouraging users to give you some more money and sign up to virus scanning. This can also be the filename of a ruleset.

Default:
Mark Unscanned Messages = yes

Unscanned Header Value

This is the text used by the "Mark Unscanned Messages" option above. This can also be the filename of a ruleset.

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

Remove These Headers

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. 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.

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

Deliver Cleaned Messages

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.

Default:
Deliver Cleaned Messages = yes

12. Notifications back to the senders of blocked messages

Notify Senders

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.

Default:
Notify Senders = yes

Notify Senders Of Viruses

If "Notify Senders" is set to yes, do you want to notify people who sent you messages containing viruses? 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.

Default:
Notify Senders Of Viruses = no

Notify Senders Of Blocked Filenames Or Filetypes

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.

Default:
Notify Senders Of Blocked Filenames Or Filetypes = yes

Notify Senders Of Other Blocked Content

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.

Default:
Notify Senders Of Other Blocked Content = yes

Never Notify Senders Of Precedence

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.

Default:
Never Notify Senders Of Precedence = list bulk

13. Changes to the Subject: line

Scanned Modify Subject

When the message has been scanned but no other subject line changes have happened, do you want modify the subject line? This can be 1 of 3 values:

```
     no    = Do not modify the subject line, or
     start = Add text to the start of the subject line, or
     end   = Add text to the end of the subject line.
```
This makes very good advertising of your MailScanning service. This can also be the filename of a ruleset.

Default:
Scanned Modify Subject = no # end

Scanned Subject Text

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

Default:
Scanned Subject Text = {Scanned}

Virus Modify Subject

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.

Default:
Virus Modify Subject = yes

Virus Subject Text

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

Default:
Virus Subject Text = {Virus?}

Filename Modify Subject

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.

Default:
Filename Modify Subject = yes

Filename Subject Text

This is the text to add to the start of the subject if the "Filename Modify Subject" option is set. 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.

Default:
Filename Subject Text = {Filename?}

Content Modify Subject

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.

Default:
Content Modify Subject = yes

Content Subject Text

This is the text to add to the start of the subject if the "Content Modify Subject" option is set. 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.

Default:
Content Subject Text = {Dangerous Content?}

Disarmed Modify Subject

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.

Default:
Disarmed Modify Subject = yes

Disarmed Subject Text

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.

Default:
Disarmed Subject Text = {Disarmed}

Spam Modify Subject

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.

Default:
Spam Modify Subject = yes

Spam Subject Text

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.

Default:
Spam Subject Text = {Spam?}

High Scoring Spam Modify Subject

This is just like the "Spam Modify Subject" option above, except that it applies then the score from SpamAssassin is higher than the "High SpamAssassin Score" value. This can also be the filename of a ruleset.

Default:
High Scoring Spam Modify Subject = yes

High Scoring Spam Subject Text

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.

Default:
High Scoring Spam Subject Text = {Spam?}

14. Changes to the Message Body

Warning Is Attachment

Attachment Encoding. 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.

Default:
Warning Is Attachment = yes

Attachment Warning Filename

When a virus or attachment is replaced by a plain-text warning, and that warning is an attachment, this is the filename of the new attachment. This can also be the filename of a ruleset.

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

Attachment Encoding Charset

What character set do you want to use for the attachment that replaces viruses (VirusWarning.txt)? The default is ISO-8859-1 as even Americans have to talk to the rest of the world occasionally :-) This can also be the filename of a ruleset.

Default:
Attachment Encoding Charset = ISO-8859-1

15. Mail Archiving and Monitoring

Archive Mail

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 (they must already exist!) to which mail will be appended in "mbox" format suitable for most Unix mail systems.

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.

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.

Archive Mail = /var/spool/MailScanner/archive

Default:
Archive Mail =

16. Notices to System Administrators

Send Notices

Notify the local system administrators ("Notices To") when any infections are found? This can also be the filename of a ruleset.

Default: Send Notices = yes

Notices Include Full Headers

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.

Default: Notices Include Full Headers = yes

Hide Incoming Work Dir in Notices

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 sys admins. This can also be the filename of a ruleset.

Default: Hide Incoming Work Dir in Notices = no

Notice Signature

What signature to add to the bottom of the notices. To insert a line-break in there, use the sequence "\n".

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

Notices From

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.

Default: Notices From = MailScanner

Notices To

Where to send the notices. This can also be the filename of a ruleset.

Default: Notices To = postmaster

Local Postmaster

Address of the local Postmaster, which is used as the "From" address in virus warnings sent to users. This can also be the filename of a ruleset.

Default:
Local Postmaster = postmaster

17. Spam Detection and Virus Scanner Definitions

Spam List Definitions

This is the name of the file that translates the names of the "Spam List" values to the real DNS names of the spam blacklists.

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

Virus Scanner Definitions

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.

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

18. Spam Detection and Spam Lists (DNS blocklists)

Spam Checks

Do you want to check messages to see if they are spam? Note: If you switch this off then *no* spam checks will be done at all. This includes both MailScanner's own checks and SpamAssassin. If you want to just disable the "Spam List" feature then set "Spam List =" (i.e. an empty list) in the setting below. This can also be the filename of a ruleset.

Default:
Spam Checks = yes

Spam List

This is the list of spam blacklists (RBLs) which you are using. See the "Spam List Definitions" file for more information about what you can put here. This can also be the filename of a ruleset.

Default:
Spam List = # ORDB-RBL SBL+XBL # You can un-comment this to enable them

Spam Domain List

This is the list of spam domain blacklists which you are using (such as the "rfc-ignorant" domains). See the "Spam List Definitions" file for more information about what you can put here. This can also be the filename of a ruleset.

Default:
Spam Domain List =

Spam Lists To Be Spam

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.

Default:
Spam Lists To Be Spam = 1

Spam Lists To Reach High Score

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.

Default:
Spam Lists To Reach High Score = 3

Spam List Timeout

If an individual "Spam List" or "Spam Domain List" check takes longer that this (in seconds), the check is abandoned and the timeout noted.

Default:
Spam List Timeout = 10

Max Spam List Timeouts

The maximum number of timeouts caused by any individual "Spam List" or "Spam Domain List" before it is marked as "unavailable". Once marked, the list will be ignored until the next automatic re-start (see "Restart Every" for the longest time it will wait). This can also be the filename of a ruleset.

Default:
Max Spam List Timeouts = 7

Spam List Timeouts History

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").

Default:
Spam List Timeouts History = 10

Is Definitely Not Spam

Spam Whitelist: Make this point to a ruleset, and anything in that ruleset whose value is "yes" will *never* be marked as spam. The whitelist check is done before the blacklist check. If anyone whitelists a message, then all recipients get the message. If no-one has whitelisted it, then the blacklist is checked. This setting over-rides the "Is Definitely Spam" setting. This can also be the filename of a ruleset. Example:
Is Definitely Not Spam = no

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

Is Definitely Spam

Spam Blacklist: Make this point to a ruleset, and anything in that ruleset whose value is "yes" will *always* be marked as spam. This value can be over-ridden by the "Is Definitely Not Spam" setting. This can also be the filename of a ruleset.

Default:
Is Definitely Spam = no

Definite Spam Is High Scoring

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.

Default:
Definite Spam Is High Scoring = no

Ignore Spam Whitelist If Recipients Exceed

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.

Default:
Ignore Spam Whitelist If Recipients Exceed = 20

19. SpamAssassin

Use SpamAssassin

Do you want to find spam using the "SpamAssassin" package? This can also be the filename of a ruleset.

Default:
Use SpamAssassin = no

Max SpamAssassin Size

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.

Default:
Max SpamAssassin Size = 30000

Required SpamAssassin Score

This replaces the SpamAssassin configuration value 'required_hits'. If a message achieves a SpamAssassin score higher than this value, it is spam. See also the High SpamAssassin Score configuration option. This can also be the filename of a ruleset, so the SpamAssassin required_hits value can be set to different values for different messages.

Default:
Required SpamAssassin Score = 6

High SpamAssassin Score

If a message achieves a SpamAssassin score higher than this value, then the "High Scoring Spam Actions" are used. You may want to use this to deliver moderate scores, while deleting very high scoring messsages. This can also be the filename of a ruleset.

Default:
High SpamAssassin Score = 10

SpamAssassin Auto Whitelist

Set this option to "yes" to enable the automatic whitelisting functions available within SpamAssassin. This will cause addresses from which you get real mail, to be marked so that it will never incorrectly spam-tag messages from those addresses. To disable whitelisting, you must set "use_auto_whitelist 0" in your spam.assassin.prefs.conf file as well as set this to no.

Default:
SpamAssassin Auto Whitelist = no

SpamAssassin Prefs File

Set the location of the SpamAssassin user_prefs file. If you want to stop SpamAssassin doing all the RBL checks again, then you can add "skip_rbl_checks = 1" to this prefs file.

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

SpamAssassin Timeout

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

Default:
SpamAssassin Timeout = 75

Max SpamAssassin Timeouts

If SpamAssassin times out more times in a row than this, then it will be marked as "unavailable" until MailScanner next re-starts itself. This means that remote network failures causing SpamAssassin trouble will not mean your mail stops flowing.

Default:
Max SpamAssassin Timeouts = 10

SpamAssassin Timeouts History

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").

Default:
SpamAssassin Timeouts History = 30

Check SpamAssassin If On Spam List

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 the High Scoring Spam Actions from ever happening. This can also be the filename of a ruleset.

Default:
Check SpamAssassin If On Spam List = yes

Spam Score

Do you want to include the "Spam Score" header. This shows 1 character (Spam Score Character) for every point of the SpamAssassin score. This makes it very easy for users to be able to filter their mail using whatever SpamAssassin

threshold they want. For example, they just look for "sssss" for every message whose score is > 5, for example. This can also be the filename of a ruleset.

Default:
Spam Score = yes

Rebuild Bayes Every

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. 1 day = 86400 seconds. To disable this feature set this to 0.

Default:
Rebuild Bayes Every = 0

Wait During Bayes Rebuild

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.

Default:
Wait During Bayes Rebuild = no

20. What to do with spam

Spam Actions

This is a list of actions to take when a message is spam. It can be 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
   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" as well for the
                             message to reach the original 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.
   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.
   header "name: value"    - Add the header name: value to the message.
                             name must not contain any spaces.
```

This can also be the filename of a ruleset, in which case the filename must end in ".rule" or ".rules". Example:
Spam Actions = store forward anonymous@ecs.soton.ac.uk

Default:
Spam Actions = deliver

High Scoring Spam Actions

```
This is just like the "Spam Actions" option above, except that it applies then
the score from SpamAssassin is higher than the "High SpamAssassin Score" value.
   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" as well for the
                             message to reach the original 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.
   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.
   header "name: value"    - Add the header name: value to the message.
                             name must not contain any spaces.

This can also be the filename of a ruleset, in which case the filename must end
in ".rule" or ".rules".
```

Default:
High Scoring Spam Actions = deliver

Non Spam Actions

```
This is just like the "Spam Actions" option above, except that it applies to
messages that are *NOT* spam.
   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
   header "name: value"    - Add the header name: value to the message.
                             name must not contain any spaces.

This can also be the filename of a ruleset, in which case the filename must end
in ".rule" or ".rules".
```

Default:
Non Spam Actions = deliver

Sender Reports

```
There are 3 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.

These can also be the filenames of rulesets.

Default:
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

Inline Spam Warning

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.

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

Recipient Spam Report

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.

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

Enable Spam Bounce

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. If you enable this, be prepared to handle the irate responses from people to whom you are essentially sending more spam!

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

Bounce Spam As Attachment

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?
NOTE: If you enable this option, be sure to whitelist your local server ie. 127.0.0.1 as otherwise 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.

Default:
Bounce Spam As Attachment = no

21. Logging

Syslog Facility

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 go and 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.

Default:
Syslog Facility = mail

Log Speed

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.

Default:
Log Speed = no

Log Spam

Do you want all spam to be logged? Useful if you want to gather spam statistics from your logs, but can increase the system load quite a bit if you get a lot of spam.

Default:
Log Spam = no

Log Non Spam

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.

Default:
Log Non Spam = no

Log Permitted Filenames

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.

Default:
Log Permitted Filenames = no

Log Permitted Filetypes

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.

Default:
Log Permitted Filetypes = no

Log Silent Viruses

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

Default:
Log Silent Viruses = no

Log Dangerous HTML Tags

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.

Default:
Log Dangerous HTML Tags = no

22. 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

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. If using Postfix, you probably want to set this as shown in the example line at the end of this comment, and do

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

NOTE: SpamAssassin is always called from MailScanner as the same user, and that is the "Run As" user specified above. 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. Example:
SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin

Default:
SpamAssassin User State Dir =

SpamAssassin Install Prefix

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. Example:
SpamAssassin Install Prefix = /opt/MailScanner

Default:
SpamAssassin Install Prefix =

SpamAssassin Site Rules Dir

The site rules are searched for here. Normal location on most systems is /etc/mail/spamassassin.

Default:
SpamAssassin Site Rules Dir = /etc/mail/spamassassin

SpamAssassin Local Rules Dir

The site-local rules are searched for here, and in prefix/etc/spamassassin, prefix/etc/mail/spamassassin, /usr/local/etc/spamassassin, /etc/spamassassin, /etc/mail/spamassassin, and maybe others. If this is set then it adds to the list of places that are searched; otherwise it has no effect. Example:
SpamAssassin Local Rules Dir = /etc/MailScanner/mail/spamassassin

Default:
SpamAssassin Local Rules Dir =

SpamAssassin Default Rules

The default rules are searched for here, and in prefix/share/spamassassin, /usr/local/share/spamassassin, /usr/share/spamassassin, and maybe others. If this is set then it adds to the list of places that are searched; otherwise it has no effect. Example:
SpamAssassin Default Rules Dir = /opt/MailScanner/share/spamassassin

Default:
SpamAssassin Default Rules Dir =

MCP (Message Content Protection)

MCP Checks

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.
See http://www.sng.ecs.soton.ac.uk/mailscanner/install/mcp/ for more info.

Default:
MCP Checks = no

First Check

Do the spam checks first, or the MCP checks first? This cannot be the filename of a ruleset, only a fixed value.

Default:
First Check = mcp

MCP spam options

The rest of these options are clones of the equivalent spam options

Default:
MCP Required SpamAssassin Score = 1
MCP High SpamAssassin Score = 10
MCP Error Score = 1
MCP Header = X-%org-name%-MailScanner-MCPCheck:
Non MCP Actions = deliver
MCP Actions = deliver
High Scoring MCP Actions = deliver
Bounce MCP As Attachment = no
MCP Modify Subject = yes
MCP Subject Text = {MCP?}
High Scoring MCP Modify Subject = yes
High Scoring MCP Subject Text = {MCP?}
Is Definitely MCP = no
Is Definitely Not MCP = no
Definite MCP Is High Scoring = no
Always Include MCP Report = no
Detailed MCP Report = yes
Include Scores In MCP Report = no
Log MCP = no
MCP Max SpamAssassin Timeouts = 20
MCP Max SpamAssassin Size = 100000
MCP SpamAssassin Timeout = 10
MCP SpamAssassin Prefs File = %mcp-dir%/mcp.spam.assassin.prefs.conf
MCP SpamAssassin User State Dir =
MCP SpamAssassin Local Rules Dir = %mcp-dir%
MCP SpamAssassin Default Rules Dir = %mcp-dir%
MCP SpamAssassin Install Prefix = %mcp-dir%
Recipient MCP Report = %report-dir%/recipient.mcp.report.txt
Sender MCP Report = %report-dir%/sender.mcp.report.txt

23. Advanced Settings

Don't bother changing anything below this unless you really know what you are doing, or else if MailScanner has complained about your "Minimum Code Status" setting.

Use Default Rules With Multiple Recipients

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 "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 "*@*".

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.

Default:
Use Default Rules With Multiple Recipients = no

Spam Score Number Format

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.

Default
Spam Score Number Format = %d

MailScanner Version Number

This is the version number of the MailScanner distribution that created this configuration file. Please do not change this value.

Default:
MailScanner Version Number = 4.42.9

Debug

Set Debug to "yes" to stop it running as a daemon and just process one batch of messages and then exit.

Default:
Debug = no

Debug SpamAssassin

Do you want to debug SpamAssassin from within MailScanner?

Default:
Debug SpamAssassin = no

Run In Foreground

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).

Default:
Run In Foreground = no

LDAP Server/LDAP Base/LDAP Site

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

Default:
#LDAP Server = localhost
#LDAP Base   = o=fsl
#LDAP Site   = default

Always Looked Up Last

This option is intended for people who want to log more information about messages than what is put in 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. Its value is completely ignored, it is purely there to have side effects. If you want to use it, read CustomConfig.pm.

Default:
Always Looked Up Last = no

Deliver In Background

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.

Default:
Deliver In Background = yes

Delivery Method

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

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 here so that messages coming to you are immediately delivered, while messages going to any other site are just placed in the queue in case the remote delivery is very slow.

Default:
Delivery Method = batch

Split Exim Spool

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.

Default:
Split Exim Spool = no

Lockfile Dir

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).

Default:
Lockfile Dir = /tmp

Custom Functions Dir

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.

Default:
Custom Functions Dir = /usr/lib/MailScanner/MailScanner/CustomFunctions

Lock Type

How to lock spool files. Don't set this unless you *know* you need to. For sendmail, it defaults to "flock". For sendmail 8.13 onwards, you will probably need to change it to posix. For Exim, it defaults to "posix". No other type is implemented.

Default:
Lock Type =

Minimum Code Status

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. 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.
```

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. READ and UNDERSTAND the above text BEFORE changing this.

Default:
Minimum Code Status = supported

24. File Line Numbers

```
Line  Code
   1  # Main configuration file for the MailScanner E-Mail Virus Scanner
   2  #
   3  # It's good practice to check through configuration files to make sure
   4  # they fit with your system and your needs, whatever you expect them to
   5  # contain.
   6  #
   7  # Note: If your directories are symlinked (soft-linked) in any way,
   8  #       please put their *real* location in here, not a path that
   9  #       includes any links. You may get some very strange error
  10  #       messages from some of the virus scanners if you don't.
  11  #
  12  # Note for Version 4.00 and above:
  13  #       A lot of the settings can take a ruleset as well as just simple
  14  #       values. These rulesets are files containing rules which are applied
  15  #       to the current message to calculate the value of the configuration
  16  #       option. The rules are checked in the order they appear in the ruleset.
  17  #
  18  # Note for Version 4.03 and above:
  19  #       As well as rulesets, you can now include your own functions in
  20  #       here. Look at the directory containing Config.pm and you will find
  21  #       CustomConfig.pm. In here, you can add your own "value" function and
  22  #       an Initvalue function to set up any global state you need such as
  23  #       database connections. Then for a setting below, you can put:
  24  #               Configuration Option = &ValueFunction
  25  #       where "ValueFunction" is the name of the function you have
  26  #       written in CustomConfig.pm.
  27  #
  28
  29  #
  30  # Definition of variables which are substituted into definitions below.
  31  #
  32  # You can add any %variables% that you want to use in addition to the
  33  # ones provided.
  34  #
  35  # You can also use any shell environment variables here such as $HOSTNAME
  36  # or ${HOSTNAME} in configuration settings and rulesets. See the
  37  # definition of "Hostname" for an example.
  38  #
  39
  40  # Set the directory containing all the reports in the required language
  41  %report-dir% = /etc/MailScanner/reports/en
  42
  43  # Configuration directory containing this file
  44  %etc-dir% = /etc/MailScanner
  45
  46  # Rulesets directory containing your ".rules" files
```

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

# Configuration directory containing files related to MCP
# (Message Content Protection)
%mcp-dir% = /etc/MailScanner/mcp

# 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.
#       Some other mail servers complain about "_" characters
#       appearing in the names of headers as well.
#       So don't put "." or "_" in this setting.
#
# **** RULE: It must not contain any spaces! ****
%org-name% = yoursite

# 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 "\n" sequences in the text. These will
# be replaced by line-breaks.
%org-long-name% = Your Organisation Name Here

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

#
# System settings
# ---------------
#

# How many MailScanner processes do you want to run at a time?
# There is no point increasing this figure if your MailScanner server
# is happily keeping up with your mail traffic.
# 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.
# If you are running on a small system with limited RAM, you should
# note that each child takes just over 20MB.
#
# As a rough guide, try 5 children per CPU. But read the notes above.
```

```
Max Children = 5

# User to run 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 file.
#Run As User = mail
#Run As User = postfix
Run As User =

# Group to run as (not normally used for sendmail)
#Run As Group = mail
#Run As Group = postfix
Run As Group =

# 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.
Queue Scan Interval = 6

# Set location of incoming mail queue
#
# This can be any one of
# 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: /etc/MailScanner/mqueue.in.list.conf
#
# If you are using sendmail and have your queues split into qf, df, xf
# directories, then just specify the main directory, do not give me the
# directory names of the qf,df,xf directories.
# Example: if you have /var/spool/mqueue.in/qf
#                      /var/spool/mqueue.in/df
#                      /var/spool/mqueue.in/xf
# then just tell me /var/spool/mqueue.in. I will find the subdirectories
# automatically.
#
Incoming Queue Dir = /var/spool/mqueue.in

# Set location of outgoing mail queue.
# This can also be the filename of a ruleset.
Outgoing Queue Dir = /var/spool/mqueue

# Set where to unpack incoming messages before scanning them
# This can completely safely use tmpfs or a ramdisk, which will
```

```
147  # give you a significant performance improvement.
148  # NOTE: The path given here must not include any links at all,
149  # NOTE: but must be the absolute path to the directory.
150  Incoming Work Dir = /var/spool/MailScanner/incoming
151
152  # Set where to store infected and message attachments (if they are kept)
153  # This can also be the filename of a ruleset.
154  Quarantine Dir = /var/spool/MailScanner/quarantine
155
156  # Set where to store the process id number so you can stop MailScanner
157  PID file = /var/run/MailScanner.pid
158
159  # To avoid resource leaks, re-start periodically
160  Restart Every = 14400
161
162  # Set whether to use postfix, sendmail, exim or zmailer.
163  # If you are using postfix, then see the "SpamAssassin User State Dir"
164  # setting near the end of this file
165  MTA = sendmail
166
167  # Set how to invoke MTA when sending messages MailScanner has created
168  # (e.g. to sender/recipient saying "found a virus in your message")
169  # This can also be the filename of a ruleset.
170  Sendmail = /usr/sbin/sendmail
171
172  # Sendmail2 is provided for Exim users.
173  # It is the command used to attempt delivery of outgoing cleaned/disinfected
174  # messages.
175  # This is not usually required for sendmail.
176  # This can also be the filename of a ruleset.
177  #For Exim users: Sendmail2 = /usr/sbin/exim -C /etc/exim/exim_send.conf
178  #For sendmail users: Sendmail2 = /usr/sbin/sendmail
179  #Sendmail2 = /usr/sbin/sendmail -C /etc/exim/exim_send.conf
180  Sendmail2 = /usr/sbin/sendmail
181
182  #
183  # Incoming Work Dir Settings
184  # -------------------------
185  #
186  # You should not normally need to touch these settings at all,
187  # unless you are using ClamAV and need to be able to use the
188  # external archive unpackers instead of ClamAV's built-in ones.
189
190  # If you want to create the temporary working files so they are owned
191  # by a user other than the "Run As User" setting at the top of this file,
192  # you can change that here.
193  # Note: If the "Run As User" is not "root" then you cannot change the
194  #       user but may still be able to change the group, if the
195  #       "Run As User" is a member of both of the groups "Run As Group"
196  #       and "Incoming Work Group".
```

```
197  Incoming Work User =
198  Incoming Work Group =
199
200  # If you want processes running under the same *group* as MailScanner to
201  # be able to read the working files (and list what is in the
202  # directories, of course), set to 0640. If you want *all* other users to
203  # be able to read them, set to 0644. For a detailed description, if
204  # you're not already familiar with it, refer to `man 2 chmod`.
205  # Typical use: external helper programs of virus scanners (notably ClamAV),
206  # like unpackers.
207  # Use with care, you may well open security holes.
208  Incoming Work Permissions = 0600
209
210  #
211  # Quarantine and Archive Settings
212  # ------------------------------
213  #
214  # If, for example, you are using a web interface so that users can manage
215  # their quarantined files, you might want to change the ownership and
216  # permissions of the quarantined so that they can be read and/or deleted
217  # by the web server.
218  # Don't touch this unless you know what you are doing!
219
220  # If you want to create the quarantine/archive so the files are owned
221  # by a user other than the "Run As User" setting at the top of this file,
222  # you can change that here.
223  # Note: If the "Run As User" is not "root" then you cannot change the
224  #       user but may still be able to change the group, if the
225  #       "Run As User" is a member of both of the groups "Run As Group"
226  #       and "Quarantine Group".
227  Quarantine User =
228  Quarantine Group =
229
230  # If you want processes running under the same *group* as MailScanner to
231  # be able to read the quarantined files (and list what is in the
232  # directories, of course), set to 0640. If you want *all* other users to
233  # be able to read them, set to 0644. For a detailed description, if
234  # you're not already familiar with it, refer to `man 2 chmod`.
235  # Typical use: let the webserver have access to the files so users can
236  # download them if they really want to.
237  # Use with care, you may well open security holes.
238  Quarantine Permissions = 0600
239
240  #
241  # Processing Incoming Mail
242  # ------------------------
243  #
244
245  # In every batch of virus-scanning, limit the maximum
246  # a) number of unscanned messages to deliver
```

```
# b) number of potentially infected messages to unpack and scan
# c) total size of unscanned messages to deliver
# d) total size of potentially infected messages to unpack and scan

Max Unscanned Bytes Per Scan = 100000000
Max Unsafe Bytes Per Scan = 50000000
Max Unscanned Messages Per Scan = 30
Max Unsafe Messages Per Scan = 30

# 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".
Max Normal Queue Size = 800

# 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.
Maximum Attachments Per Message = 200

# Expand TNEF attachments using an external program (or a 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.
Expand TNEF = yes

# Some versions of Microsoft Outlook generate unparsable Rich Text
# format attachments. Do we want to deliver these bad attachments anyway?
# Setting this to yes introduces the slight risk of a virus getting through,
# but if you have a lot of troubled Outlook users you might need to do this.
# We are working on a replacement for the TNEF decoder.
# This can also be the filename of a ruleset.
Deliver Unparsable TNEF = no

# Where the MS-TNEF expander is installed.
# This is EITHER the full command (including maxsize option) that runs
# the external TNEF expander binary,
# OR the keyword "internal" which will make MailScanner use the Perl
# module that does the same job.
# They are both provided as I am 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.
```

```
297  # This can also be the filename of a ruleset.
298  #TNEF Expander = /usr/bin/tnef --maxsize=100000000
299  TNEF Expander  = internal
300
301  # The maximum length of time the TNEF Expander is allowed to run for 1 message.
302  # (in seconds)
303  TNEF Timeout = 120
304
305  # Where the "file" command is installed.
306  # This is used for checking the content type of files, regardless of their
307  # filename.
308  # To disable Filetype checking, set this value to blank.
309  File Command = #DISABLED /usr/bin/file
310
311  # The maximum length of time the "file" command is allowed to run for 1
312  # batch of messages (in seconds)
313  File Timeout = 20
314
315  # Where the "unrar" command is installed.
316  # If you haven't got this command, look at www.rarlab.com.
317  #
318  # This is used for unpacking rar archives so that the contents can be
319  # checked for banned filenames and filetypes, and also that the
320  # archive can be tested to see if it is password-protected.
321  # Virus scanning the contents of rar archives is still left to the virus
322  # scanner, with one exception:
323  # If using the clavavmodule virus scanner, this adds external RAR checking
324  # to that scanner which is needed for archives which are RAR version 3.
325  Unrar Command = /usr/bin/unrar
326
327  # The maximum length of time the "unrar" command is allowed to run for 1
328  # RAR archive (in seconds)
329  Unrar Timeout = 50
330
331  # The maximum size, in bytes, of any message including the headers.
332  # If this is set to zero, then no size checking is done.
333  # This can also be the filename of a ruleset, so you can have different
334  # settings for different users. You might want to set this quite small for
335  # dialup users so their email applications don't time out downloading huge
336  # messages.
337  Maximum Message Size = 0
338
339  # The maximum size, in bytes, of any attachment in a message.
340  # If this is set to zero, effectively no attachments are allowed.
341  # If this is set less than zero, then no size checking is done.
342  # This can also be the filename of a ruleset, so you can have different
343  # settings for different users. You might want to set this quite small for
344  # large mailing lists so they don't get deluged by large attachments.
345  Maximum Attachment Size = -1
346
```

```
# 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.
Minimum Attachment Size = -1

# The maximum depth to which zip archives will be unpacked, to allow for
# checking filenames and filetypes within zip archives.
#
# Note: This setting does *not* affect virus scanning in archives at all.
#
# To disable this feature set this to 0.
# A common useful setting is this option = 0, and Allow Password-Protected
# Archives = no. That block password-protected archives but does not do
# any filename/filetype checks on the files within the archive.
# This can also be the filename of a ruleset.
Maximum Archive Depth = 2

# 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.
Find Archives By Content = yes

#
# Virus Scanning and Vulnerability Testing
# ----------------------------------------
#

# Do you want to scan email for viruses?
# A few people don't have a virus scanner licence and so want to disable
# all the virus scanning.
# If you use a ruleset for this setting, then the mail will be scanned if
# *any* of the rules match (except the default). That way unscanned mail
# never reaches a user who is having their mail virus-scanned.
#
# 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.
# This can also be the filename of a ruleset.
Virus Scanning = yes

# Which Virus Scanning package to use:
# sophos    from www.sophos.com, or
# sophossavi (also from www.sophos.com, using the SAVI perl module), or
```

```
397  # mcafee    from www.mcafee.com, or
398  # command   from www.command.co.uk, or
399  # bitdefender from www.bitdefender.com, or
400  # drweb     from www.dials.ru/english/dsav_toolkit/drwebunix.htm, or
401  # kaspersky-4.5 from www.kaspersky.com (Version 4.5 and newer), or
402  # kaspersky from www.kaspersky.com, or
403  # kavdaemonclient from www.kaspersky.com, or
404  # etrust    from http://www3.ca.com/Solutions/Product.asp?ID=156, or
405  # inoculate from www.cai.com/products/inoculateit.htm, or
406  # inoculan  from ftp.ca.com/pub/getbbs/linux.eng/inoctar.LINUX.Z, or
407  # nod32     for No32 before version 1.99 from www.nod32.com, or
408  # nod32-1.99 for Nod32 1.99 and later, from www.nod32.com, or
409  # f-secure  from www.f-secure.com, or
410  # f-prot    from www.f-prot.com, or
411  # panda     from www.pandasoftware.com, or
412  # rav       from www.ravantivirus.com, or
413  # antivir   from www.antivir.de, or
414  # clamav    from www.clamav.net, or
415  # clamavmodule (also from www.clamav.net using the ClamAV perl module), or
416  # trend     from www.trendmicro.com, or
417  # norman    from www.norman.de, or
418  # css       from www.symantec.com, or
419  # avg       from www.grisoft.com, or
420  # vexira    from www.centralcommand.com, or
421  # symscanengine from www.symantec.com (Symantec Scan Engine, not CSS), or
422  # generic   One you wrote: edit the generic-wrapper and generic-autoupdate
423  #           to fit your own needs. The output spec is in generic-wrapper, or
424  # none      No virus scanning at all.
425  #
426  # Note for McAfee users: do not use any symlinks with McAfee at all. It is
427  #                        very strange but may not detect all viruses when
428  #                        started from a symlink or scanning a directory path
429  #                        including symlinks.
430  #
431  # Note: If you want to use multiple virus scanners, then this should be a
432  # space-separated list of virus scanners. For example:
433  # Virus Scanners = sophos f-prot mcafee
434  #
435  # Note: Make sure that you check that the base installation directory in the
436  #       3rd column of virus.scanners.conf matches the location you have
437  #       installed each of your virus scanners. The supplied
438  #       virus.scanners.conf file assumes the default installation locations
439  #       recommended by each of the virus scanner installation guides.
440  #
441  # This *cannot* be the filename of a ruleset.
442  Virus Scanners = none
443
444  # The maximum length of time the commercial virus scanner is allowed to run
445  # for 1 batch of messages (in seconds).
446  Virus Scanner Timeout = 300
```

```
447
448  # Should I attempt to disinfect infected attachments and then deliver
449  # the clean ones. "Disinfection" involves removing viruses from files
450  # (such as removing macro viruses from documents). "Cleaning" is the
451  # replacement of infected attachments with "VirusWarning.txt" text
452  # attachments.
453  # Less than 1% of viruses in the wild can be successfully disinfected,
454  # as macro viruses are now a rare occurrence. So the default has been
455  # changed to "no" as it gives a significant performance improvement.
456  #
457  # This can also be the filename of a ruleset.
458  Deliver Disinfected Files = no
459
460  # Strings listed here will be searched for in the output of the virus scanners.
461  # It is used to list which viruses should be handled differently from other
462  # viruses. If a virus name is given here, then
463  # 1) The sender will not be warned that he sent it
464  # 2) No attempt at true disinfection will take place
465  #    (but it will still be "cleaned" by removing the nasty attachments
466  #     from the message)
467  # 3) The recipient will not receive the message,
468  #    unless the "Still Deliver Silent Viruses" option is set
469  # Other words that can be put in this list are the 5 special keywords
470  #    HTML-IFrame   : inserting this will stop senders being warned about
471  #                    HTML Iframe tags, when they are not allowed.
472  #    HTML-Codebase : inserting this will stop senders being warned about
473  #                    HTML Object Codebase/Data tags, when they are not allowed.
474  #    HTML-Script   : inserting this will stop senders being warned about
475  #                    HTML Script tags, when they are not allowed.
476  #    HTML-Form     : inserting this will stop senders being warned about
477  #                    HTML Form tags, when they are not allowed.
478  #    Zip-Password  : inserting this will stop senders being warned about
479  #                    password-protected zip files, when they are not allowed.
480  #                    This keyword is not needed if you include All-Viruses.
481  #    All-Viruses   : inserting this will stop senders being warned about
482  #                    any virus, while still allowing you to warn senders
483  #                    about HTML-based attacks. This includes Zip-Password
484  #                    so you don't need to include both.
485  #
486  # The default of "All-Viruses" means that no senders of viruses will be
487  # notified (as the sender address is always forged these days anyway),
488  # but anyone who sends a message that is blocked for other reasons will
489  # still be notified.
490  #
491  # This can also be the filename of a ruleset.
492  Silent Viruses = HTML-IFrame All-Viruses
493
494  # Still deliver (after cleaning) messages that contained viruses listed
495  # in the above option ("Silent Viruses") to the recipient?
496  # Setting this to "yes" is good when you are testing everything, and
```

```
497  # because it shows management that MailScanner is protecting them,
498  # but it is bad because they have to filter/delete all the incoming virus
499  # warnings.
500  #
501  # Note: Once you have deployed this into "production" use, you should set
502  # Note: this option to "no" so you don't bombard thousands of people with
503  # Note: useless messages they don't want!
504  #
505  # This can also be the filename of a ruleset.
506  Still Deliver Silent Viruses = no
507
508  # Strings listed here will be searched for in the output of the virus scanners.
509  # It works to achieve the opposite effect of the "Silent Viruses" listed above.
510  # If a string here is found in the output of the virus scanners, then the
511  # message will be treated as if it were not infected with a "Silent Virus".
512  # If a message is detected as both a silent virus and a non-forging virus,
513  # then the ___non-forging status will override the silent status.___
514  # In simple terms, you should list virus names (or parts of them) that you
515  # know do *not* forge the From address.
516  # A good example of this is a document macro virus or a Joke program.
517  # Another word that can be put in this list is the special keyword
518  #    Zip-Password  : inserting this will cause senders to be warned about
519  #                    password-protected zip files, when they are not allowed.
520  #                    This will over-ride the All-Viruses setting in the list
521  #                    of "Silent Viruses" above.
522  #
523  Non-Forging Viruses = Joke/ OF97/ WM97/ W97M/ eicar
524
525  # Should encrypted messages be blocked?
526  # This is useful if you are wary about your users sending encrypted
527  # messages to your competition.
528  # This can be a ruleset so you can block encrypted message to certain domains.
529  Block Encrypted Messages = no
530
531  # Should unencrypted messages be blocked?
532  # This could be used to ensure all your users send messages outside your
533  # company encrypted to avoid snooping of mail to your business partners.
534  # This can be a ruleset so you can just check mail to certain users/domains.
535  Block Unencrypted Messages = no
536
537  # Should archives which contain any password-protected files be allowed?
538  # Leaving this set to "no" is a good way of protecting against all the
539  # protected zip files used by viruses at the moment.
540  # This can also be the filename of a ruleset.
541  Allow Password-Protected Archives = no
542
543  #
544  # Options specific to Sophos Anti-Virus
545  # ------------------------------------
546  #
```

```
547
548  # Anything on the next line that appears in brackets at the end of a line
549  # of output from Sophos will cause the error/infection to be ignored.
550  # Use of this option is dangerous, and should only be used if you are having
551  # trouble with lots of corrupt PDF files, for example.
552  # If you need to specify more than 1 string to find in the error message,
553  # then put each string in quotes and separate them with a comma.
554  # For example:
555  #Allowed Sophos Error Messages = "corrupt", "format not supported"
556  Allowed Sophos Error Messages =
557
558  # The directory (or a link to it) containing all the Sophos *.ide files.
559  # This is only used by the "sophossavi" virus scanner, and is irrelevant
560  # for all other scanners.
561  Sophos IDE Dir = /usr/local/Sophos/ide
562
563  # The directory (or a link to it) containing all the Sophos *.so libraries.
564  # This is only used by the "sophossavi" virus scanner, and is irrelevant
565  # for all other scanners.
566  Sophos Lib Dir = /usr/local/Sophos/lib
567
568  # SophosSAVI only: monitor each of these files for changes in size to
569  # detect when a Sophos update has happened. The date of the Sophos Lib Dir
570  # is also monitored.
571  # This is only used by the "sophossavi" virus scanner, not the "sophos"
572  # scanner setting.
573  Monitors For Sophos Updates = /usr/local/Sophos/ide/*ides.zip
574
575  #
576  # Options specific to ClamAV Anti-Virus
577  # -------------------------------------
578  #
579
580  # ClamAVModule only: monitor each of these files for changes in size to
581  # detect when a ClamAV update has happened.
582  # This is only used by the "clamavmodule" virus scanner, not the "clamav"
583  # scanner setting.
584  Monitors for ClamAV Updates = /usr/local/share/clamav/*.cvd
585
586  # ClamAVModule only: set limits when scanning for viruses.
587  #
588  # The maximum recursion level of archives,
589  # The maximum number of files per batch,
590  # The maximum file of each file,
591  # The maximum compression ratio of archive.
592  # These settings *cannot* be the filename of a ruleset, only a simple number.
593  ClamAVmodule Maximum Recursion Level = 5
594  ClamAVmodule Maximum Files = 1000
595  ClamAVmodule Maximum File Size = 10000000 # (10 Mbytes)
596  ClamAVmodule Maximum Compression Ratio = 250
```

```
597
598  #
599  # Removing/Logging dangerous or potentially offensive content
600  # ------------------------------------------------------------
601  #
602
603  # Do you want to scan the messages for potentially dangerous content?
604  # Setting this to "no" will disable all the content-based checks except
605  # Virus Scanning, Allow Partial Messages and Allow External Message Bodies.
606  # This can also be the filename of a ruleset.
607  Dangerous Content Scanning = yes
608
609  # Do you want to allow partial messages, which only contain a fraction of
610  # the attachments, not the whole thing? There is absolutely no way to
611  # scan these "partial messages" properly for viruses, as MailScanner never
612  # sees all of the attachment at the same time. Enabling this option can
613  # allow viruses through. You have been warned.
614  # This can also be the filename of a ruleset so you can, for example, allow
615  # them in outgoing mail but not in incoming mail.
616  Allow Partial Messages = no
617
618  # Do you want to allow messages whose body is stored somewhere else on the
619  # internet, which is downloaded separately by the user's email package?
620  # There is no way to guarantee that the file fetched by the user's email
621  # package is free from viruses, as MailScanner never sees it.
622  # This feature is dangerous as it can allow viruses to be fetched from
623  # other Internet sites by a user's email package. The user would just
624  # think it was a normal email attachment and would have been scanned by
625  # MailScanner.
626  # It is only currently supported by Netscape 6 anyway, and the only people
627  # who it are the IETF. So I would strongly advise leaving this switched off.
628  # This can also be the filename of a ruleset.
629  Allow External Message Bodies = no
630
631  # Do you want to check for "Phishing" attacks?
632  # These are attacks that look like a genuine email message from your bank,
633  # which contain a link to click on to take you to the web site where you
634  # will be asked to type in personal information such as your account number
635  # or credit card details.
636  # Except it is not the real bank's web site at all, it is a very good copy
637  # of it run by thieves who want to steal your personal information or
638  # credit card details.
639  # These can be spotted because the real address of the link in the message
640  # is not the same as the text that appears to be the link.
641  # Note: This does cause extra load, particularly on systems receiving lots
642  #       of spam such as secondary MX hosts.
643  # This can also be the filename of a ruleset.
644  Find Phishing Fraud = yes
645
646  # While detecting "Phishing" attacks, do you also want to point out links
```

```
647  # to numeric IP addresses. Genuine links to totally numeric IP addresses
648  # are very rare, so this option is set to "yes" by default. If a numeric
649  # IP address is found in a link, the same phishing warning message is used
650  # as in the Find Phishing Fraud option above.
651  # This can also be the filename of a ruleset.
652  Also Find Numeric Phishing = yes
653
654  # There are some companies, such as banks, that insist on sending out
655  # email messages with links in them that are caught by the "Find Phishing
656  # Fraud" test described above.
657  # This is the name of a file which contains a list of link destinations
658  # which should be ignored in the test. This may, for example, contain
659  # the known websites of some banks.
660  # See the file itself for more information.
661  # This can only be the name of the file containing the list, it *cannot*
662  # be the filename of a ruleset.
663  Phishing Safe Sites File = %etc-dir%/phishing.safe.sites.conf
664
665  # Do you want to allow <IFrame> tags in email messages? This is not a good
666  # idea as it allows various Microsoft Outlook security vulnerabilities to
667  # remain unprotected, but if you have a load of mailing lists sending them,
668  # then you will want to allow them to keep your users happy.
669  # Value: yes     => Allow these tags to be in the message
670  #        no      => Ban messages containing these tags
671  #        disarm  => Allow these tags, but stop these tags from working
672  # This can also be the filename of a ruleset, so you can allow them from
673  # known mailing lists but ban them from everywhere else.
674  Allow IFrame Tags = disarm
675
676  # Do you want to allow <Form> tags in email messages? This is a bad idea
677  # as these are used as scams to pursuade people to part with credit card
678  # information and other personal data.
679  # Value: yes     => Allow these tags to be in the message
680  #        no      => Ban messages containing these tags
681  #        disarm  => Allow these tags, but stop these tags from working
682  #                   Note: Disarming can be defeated, it is not 100% safe!
683  # This can also be the filename of a ruleset.
684  Allow Form Tags = disarm
685
686  # Do you want to allow <Script> tags in email messages? This is a bad idea
687  # as these are used to exploit vulnerabilities in email applications and
688  # web browsers.
689  # Value: yes     => Allow these tags to be in the message
690  #        no      => Ban messages containing these tags
691  #        disarm  => Allow these tags, but stop these tags from working
692  #                   Note: Disarming can be defeated, it is not 100% safe!
693  # This can also be the filename of a ruleset.
694  Allow Script Tags = disarm
695
696  # 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.
# Value: yes     => Allow these tags to be in the message
#        disarm  => Allow these tags, but stop these tags from working
#                   Note: Disarming can be defeated, it is not 100% safe!
# Note: You cannot block messages containing web bugs as their detection
#       is very vulnerable to false alarms.
# This can also be the filename of a ruleset.
Allow WebBugs = disarm

# Do you want to allow <Object Codebase=...> or <Object Data=...> 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.
# Value: 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
# This can also be the filename of a ruleset, so you can allow them just
# for specific users or domains.
Allow Object Codebase Tags = disarm

# This option interacts with the "Allow ... Tags" options above like this:
#
# Allow...Tags    Convert Danger...    Action Taken on HTML Message
# ============    ================    ===========================
#   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
#
# 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.
#
# This can also be the filename of a ruleset, so you can make this apply
# only to specific users or domains.
Convert Dangerous HTML To Text = no

# Do you want to convert all HTML messages into plain text?
# This is very useful for users who are children or are easily 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.
Convert HTML To Text = no
```

```
747
748  #
749  # Attachment Filename Checking
750  # ----------------------------
751  #
752
753  # Set where to find the attachment filename ruleset.
754  # The structure of this file is explained elsewhere, but it is used to
755  # accept or reject file attachments based on their name, regardless of
756  # whether they are infected or not.
757  #
758  # This can also point to a ruleset, but the ruleset filename must end in
759  # ".rules" so that MailScanner can determine if the filename given is
760  # a ruleset or not!
761  Filename Rules = %etc-dir%/filename.rules.conf
762
763  # Set where to find the attachment filetype ruleset.
764  # The structure of this file is explained elsewhere, but it is used to
765  # accept or reject file attachments based on their content as determined
766  # by the "file" command, regardless of whether they are infected or not.
767  #
768  # This can also point to a ruleset, but the ruleset filename must end in
769  # ".rules" so that MailScanner can determine if the filename given is
770  # a ruleset or not!
771  #
772  # To disable this feature, set this to just "Filetype Rules =" or set
773  # the location of the file command to a blank string.
774  Filetype Rules = %etc-dir%/filetype.rules.conf
775
776  #
777  # Reports and Responses
778  # ---------------------
779  #
780
781  # Do you want to store copies of the infected attachments and messages?
782  # This can also be the filename of a ruleset.
783  Quarantine Infections = yes
784
785  # There is no point quarantining most viruses these days as the infected
786  # messages contain no useful content, so if you set this to "no" then no
787  # infections listed in your "Silent Viruses" setting will be quarantined,
788  # even if you have chosen to quarantine infections in general. This is
789  # currently set to "yes" so the behaviour is the same as it was in
790  # previous versions.
791  # This can also be the filename of a ruleset.
792  Quarantine Silent Viruses = no
793
794  # Do you want to quarantine the original *entire* message as well as
795  # just the infected attachments?
796  # This can also be the filename of a ruleset.
```

```
797  Quarantine Whole Message = no
798
799  # When you quarantine an entire message, do you want to store it as
800  # raw mail queue files (so you can easily send them onto users) or
801  # as human-readable files (header then body in 1 file)?
802  Quarantine Whole Messages As Queue Files = no
803
804  # Do you want to stop any virus-infected spam getting into the spam or MCP
805  # archives? If you have a system where users can release messages from the
806  # spam or MCP archives, then you probably want to stop them being able to
807  # release any infected messages, so set this to yes.
808  # It is set to no by default as it causes a small hit in performance, and
809  # many people don't allow users to access the spam quarantine, so don't
810  # need it.
811  # This can also be the filename of a ruleset.
812  Keep Spam And MCP Archive Clean = no
813
814  # Set where to find all the strings used so they can be translated into
815  # your local language.
816  # This can also be the filename of a ruleset so you can produce different
817  # languages for different messages.
818  Language Strings = %report-dir%/languages.conf
819
820  # Set where to find the message text sent to users when one of their
821  # attachments has been deleted from a message.
822  # These can also be the filenames of rulesets.
823  Deleted Bad Content Message Report  = %report-dir%/deleted.content.message.txt
824  Deleted Bad Filename Message Report = %report-dir%/deleted.filename.message.txt
825  Deleted Virus Message Report        = %report-dir%/deleted.virus.message.txt
826
827  # Set where to find the message text sent to users when one of their
828  # attachments has been deleted from a message and stored in the quarantine.
829  # These can also be the filenames of rulesets.
830  Stored Bad Content Message Report  = %report-dir%/stored.content.message.txt
831  Stored Bad Filename Message Report = %report-dir%/stored.filename.message.txt
832  Stored Virus Message Report        = %report-dir%/stored.virus.message.txt
833
834  # Set where to find the message text sent to users explaining about the
835  # attached disinfected documents.
836  # This can also be the filename of a ruleset.
837  Disinfected Report = %report-dir%/disinfected.report.txt
838
839  # Set where to find the HTML and text versions that will be added to the
840  # end of all clean messages, if "Sign Clean Messages" is set.
841  # These can also be the filenames of rulesets.
842  Inline HTML Signature = %report-dir%/inline.sig.html
843  Inline Text Signature = %report-dir%/inline.sig.txt
844
845  # Set where to find the HTML and text versions that will be inserted at
846  # the top of messages that have had viruses removed from them.
```

```
847  # These can also be the filenames of rulesets.
848  Inline HTML Warning = %report-dir%/inline.warning.html
849  Inline Text Warning = %report-dir%/inline.warning.txt
850
851  # Set where to find the messages that are delivered to the sender, when they
852  # sent an email containing either an error, banned content, a banned filename
853  # or a virus infection.
854  # These can also be the filenames of rulesets.
855  Sender Content Report        = %report-dir%/sender.content.report.txt
856  Sender Error Report        = %report-dir%/sender.error.report.txt
857  Sender Bad Filename Report = %report-dir%/sender.filename.report.txt
858  Sender Virus Report        = %report-dir%/sender.virus.report.txt
859
860  # Hide the directory path from all virus scanner reports sent to users.
861  # The extra directory paths give away information about your setup, and
862  # tend to just confuse users.
863  # This can also be the filename of a ruleset.
864  Hide Incoming Work Dir = yes
865
866  # Include the name of the virus scanner in each of the scanner reports.
867  # This also includes the translation of "MailScanner" in each of the report
868  # lines resulting from one of MailScanner's own checks such as filename,
869  # filetype or dangerous HTML content. To change the name "MailScanner", look
870  # in reports/...../languages.conf.
871  #
872  # Very useful if you use several virus scanners, but a bad idea if you
873  # don't want to let your customers know which scanners you use.
874  Include Scanner Name In Reports = yes
875
876  #
877  # Changes to Message Headers
878  # -------------------------
879  #
880
881  # Add this extra header to all mail as it is processed.
882  # This *must* include the colon ":" at the end.
883  # This can also be the filename of a ruleset.
884  Mail Header = X-%org-name%-MailScanner:
885
886  # Add this extra header to all messages found to be spam.
887  # This can also be the filename of a ruleset.
888  Spam Header = X-%org-name%-MailScanner-SpamCheck:
889
890  # Add this extra header if "Spam Score" = yes. The header will
891  # contain 1 character for every point of the SpamAssassin score.
892  Spam Score Header = X-%org-name%-MailScanner-SpamScore:
893
894  # Add this extra header to all mail as it is processed.
895  # The contents is set by "Information Header Value" and is intended for
896  # 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.
Information Header = X-%org-name%-MailScanner-Information:

# 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 From Header = yes

# 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.
Add Envelope To Header = no

# This is the name of the Envelope From header
# controlled by the option above.
# This can also be the filename of a ruleset.
Envelope From Header = X-%org-name%-MailScanner-From:

# This is the name of the Envelope To header
# controlled by the option above.
# This can also be the filename of a ruleset.
Envelope To Header = X-%org-name%-MailScanner-To:

# The character to use in the "Spam Score Header".
# Don't use: x as a score of 3 is "xxx" which the users will think is porn,
#            # as it will cause confusion with comments in procmail as well
#              as MailScanner itself,
#            * as it will cause confusion with pattern matches in procmail,
#            . as it will cause confusion with pattern matches in procmail,
#            ? as it will cause the users to think something went wrong.
# "s" is nice and safe and stands for "spam".
Spam Score Character = s

# 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.
SpamScore Number Instead Of Stars = no

# 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.
```

```
947  Minimum Stars If On Spam List = 0
948
949  # Set the "Mail Header" to these values for clean/infected/disinfected messages.
950  # This can also be the filename of a ruleset.
951  Clean Header Value       = Found to be clean
952  Infected Header Value    = Found to be infected
953  Disinfected Header Value = Disinfected
954
955  # Set the "Information Header" to this value.
956  # This can also be the filename of a ruleset.
957  Information Header Value = Please contact the ISP for more information
958
959  # Do you want the full spam report, or just a simple "spam / not spam" report?
960  Detailed Spam Report = yes
961
962  # Do you want to include the numerical scores in the detailed SpamAssassin
963  # report, or just list the names of the scores
964  Include Scores In SpamAssassin Report = yes
965
966  # Do you want to always include the Spam Report in the SpamCheck
967  # header, even if the message wasn't spam?
968  # This can also be the filename of a ruleset.
969  Always Include SpamAssassin Report = no
970
971  # What to do when you get several MailScanner headers in one message,
972  # from multiple MailScanner servers. Values are
973  #      "append"  : Append the new data to the existing header
974  #      "add"     : Add a new header
975  #      "replace" : Replace the old data with the new data
976  # Default is "append"
977  # This can also be the filename of a ruleset.
978  Multiple Headers = append
979
980  # Name of this host, or a name like "the MailScanner" if you want to hide
981  # the real hostname. It is used in the Help Desk note contained in the
982  # virus warnings sent to users.
983  # Remember you can use $HOSTNAME in here, so you might want to set it to
984  # Hostname = the %org-name% ($HOSTNAME) MailScanner
985  # This can also be the filename of a ruleset.
986  Hostname = the %org-name% ($HOSTNAME) MailScanner
987
988  # If this is "no", then (as far as possible) messages which have already
989  # been processed by another MailScanner server will not have the clean
990  # signature added to the message. This prevents messages getting many
991  # copies of the signature as they flow through your site.
992  # This can also be the filename of a ruleset.
993  Sign Messages Already Processed = no
994
995  # Add the "Inline HTML Signature" or "Inline Text Signature" to the end
996  # of uninfected messages?
```

```
# This can also be the filename of a ruleset.
Sign Clean Messages = no

# Add the "Inline HTML Warning" or "Inline Text Warning" to the top of
# messages that have had attachments removed from them?
# This can also be the filename of a ruleset.
Mark Infected Messages = yes

# When a message is to not be virus-scanned (which may happen depending
# upon the setting of "Virus Scanning", especially if it is a ruleset),
# do you want to add the header advising the users to get their email
# virus-scanned by you?
# Very good for advertising your MailScanning service and encouraging
# users to give you some more money and sign up to virus scanning.
# This can also be the filename of a ruleset.
Mark Unscanned Messages = yes

# This is the text used by the "Mark Unscanned Messages" option above.
# This can also be the filename of a ruleset.
Unscanned Header Value = Not scanned: please contact your Internet E-Mail Service Provider for details

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

# 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.
Deliver Cleaned Messages = yes

#
# Notifications back to the senders of blocked messages
# ----------------------------------------------------
#

```

```
1047  # Do you want to notify the people who sent you messages containing
1048  # viruses or badly-named filenames?
1049  # This can also be the filename of a ruleset.
1050  Notify Senders = yes
1051
1052  # *If* "Notify Senders" is set to yes, do you want to notify people
1053  # who sent you messages containing viruses?
1054  # The default value has been changed to "no" as most viruses now fake
1055  # sender addresses and therefore should be on the "Silent Viruses" list.
1056  # This can also be the filename of a ruleset.
1057  Notify Senders Of Viruses = no
1058
1059  # *If* "Notify Senders" is set to yes, do you want to notify people
1060  # who sent you messages containing attachments that are blocked due to
1061  # their filename or file contents?
1062  # This can also be the filename of a ruleset.
1063  Notify Senders Of Blocked Filenames Or Filetypes = yes
1064
1065  # *If* "Notify Senders" is set to yes, do you want to notify people
1066  # who sent you messages containing other blocked content, such as
1067  # partial messages or messages with external bodies?
1068  # This can also be the filename of a ruleset.
1069  Notify Senders Of Other Blocked Content = yes
1070
1071  # If you supply a space-separated list of message "precedence" settings,
1072  # then senders of those messages will not be warned about anything you
1073  # rejected. This is particularly suitable for mailing lists, so that any
1074  # MailScanner responses do not get sent to the entire list.
1075  Never Notify Senders Of Precedence = list bulk
1076
1077  #
1078  # Changes to the Subject: line
1079  # ----------------------------
1080  #
1081
1082  # When the message has been scanned but no other subject line changes
1083  # have happened, do you want modify the subject line?
1084  # This can be 1 of 3 values:
1085  #      no    = Do not modify the subject line, or
1086  #      start = Add text to the start of the subject line, or
1087  #      end   = Add text to the end of the subject line.
1088  # This makes very good advertising of your MailScanning service.
1089  # This can also be the filename of a ruleset.
1090  Scanned Modify Subject = no # end
1091
1092  # This is the text to add to the start/end of the subject line if the
1093  # "Scanned Modify Subject" option is set.
1094  # This can also be the filename of a ruleset.
1095  Scanned Subject Text = {Scanned}
1096
```

```
# 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.
Virus Modify Subject = yes

# This is the text to add to the start of the subject if the
# "Virus Modify Subject" option is set.
# This can also be the filename of a ruleset.
Virus Subject Text = {Virus?}

# 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.
Filename Modify Subject = yes

# This is the text to add to the start of the subject if the
# "Filename Modify Subject" option is set.
# 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.
Filename Subject Text = {Filename?}

# 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.
Content Modify Subject = yes

# This is the text to add to the start of the subject if the
# "Content Modify Subject" option is set.
# 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.
Content Subject Text = {Dangerous Content?}

# 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 Modify Subject = yes

# 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.
Disarmed Subject Text = {Disarmed}

# 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.
```

```
1147  Spam Modify Subject = yes
1148
1149  # This is the text to add to the start of the subject if the
1150  # "Spam Modify Subject" option is set.
1151  # The exact string "_SCORE_" will be replaced by the numeric
1152  # SpamAssassin score.
1153  # This can also be the filename of a ruleset.
1154  Spam Subject Text = {Spam?}
1155
1156  # This is just like the "Spam Modify Subject" option above, except that
1157  # it applies then the score from SpamAssassin is higher than the
1158  # "High SpamAssassin Score" value.
1159  # This can also be the filename of a ruleset.
1160  High Scoring Spam Modify Subject = yes
1161
1162  # This is just like the "Spam Subject Text" option above, except that
1163  # it applies then the score from SpamAssassin is higher than the
1164  # "High SpamAssassin Score" value.
1165  # The exact string "_SCORE_" will be replaced by the numeric
1166  # SpamAssassin score.
1167  # This can also be the filename of a ruleset.
1168  High Scoring Spam Subject Text = {Spam?}
1169
1170  #
1171  # Changes to the Message Body
1172  # --------------------------
1173  #
1174
1175  # When a virus or attachment is replaced by a plain-text warning,
1176  # should the warning be in an attachment? If "no" then it will be
1177  # placed in-line. This can also be the filename of a ruleset.
1178  Warning Is Attachment = yes
1179
1180  # When a virus or attachment is replaced by a plain-text warning,
1181  # and that warning is an attachment, this is the filename of the
1182  # new attachment.
1183  # This can also be the filename of a ruleset.
1184  Attachment Warning Filename = %org-name%-Attachment-Warning.txt
1185
1186  # What character set do you want to use for the attachment that
1187  # replaces viruses (VirusWarning.txt)?
1188  # The default is ISO-8859-1 as even Americans have to talk to the
1189  # rest of the world occasionally :-)
1190  # This can also be the filename of a ruleset.
1191  Attachment Encoding Charset = ISO-8859-1
1192
1193  #
1194  # Mail Archiving and Monitoring
1195  # -----------------------------
1196  #
```

```
1197
1198  # Space-separated list of any combination of
1199  # 1. email addresses to which mail should be forwarded,
1200  # 2. directory names where you want mail to be stored,
1201  # 3. file names (they must already exist!) to which mail will be appended
1202  #    in "mbox" format suitable for most Unix mail systems.
1203  #
1204  # Any of the items above can contain the magic string _DATE_ in them
1205  # which will be replaced with the current date in yyyymmdd format.
1206  # This will make archive-rolling and maintenance much easier, as you can
1207  # guarantee that yesterday's mail archive will not be in active use today.
1208  #
1209  # If you give this option a ruleset, you can control exactly whose mail
1210  # is archived or forwarded. If you do this, beware of the legal implications
1211  # as this could be deemed to be illegal interception unless the police have
1212  # asked you to do this.
1213  #Archive Mail = /var/spool/MailScanner/archive
1214  Archive Mail =
1215
1216  #
1217  # Notices to System Administrators
1218  # --------------------------------
1219  #
1220
1221  # Notify the local system administrators ("Notices To") when any infections
1222  # are found?
1223  # This can also be the filename of a ruleset.
1224  Send Notices = yes
1225
1226  # Include the full headers of each message in the notices sent to the local
1227  # system administrators?
1228  # This can also be the filename of a ruleset.
1229  Notices Include Full Headers = yes
1230
1231  # Hide the directory path from all the system administrator notices.
1232  # The extra directory paths give away information about your setup, and
1233  # tend to just confuse users but are still useful for local sys admins.
1234  # This can also be the filename of a ruleset.
1235  Hide Incoming Work Dir in Notices = no
1236
1237  # What signature to add to the bottom of the notices.
1238  # To insert a line-break in there, use the sequence "\n".
1239  Notice Signature = -- \nMailScanner\nEmail Virus Scanner\nwww.mailscanner.info
1240
1241  # The visible part of the email address used in the "From:" line of the
1242  # notices. The <user@domain> part of the email address is set to the
1243  # "Local Postmaster" setting.
1244  Notices From = MailScanner
1245
1246  # Where to send the notices.
```

```
# This can also be the filename of a ruleset.
Notices To = postmaster

# Address of the local Postmaster, which is used as the "From" address in
# virus warnings sent to users.
# This can also be the filename of a ruleset.
Local Postmaster = postmaster

#
# Spam Detection and Virus Scanner Definitions
# ---------------------------------------------
#

# This is the name of the file that translates the names of the "Spam List"
# values to the real DNS names of the spam blacklists.
Spam List Definitions = %etc-dir%/spam.lists.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.
Virus Scanner Definitions = %etc-dir%/virus.scanners.conf

#
# Spam Detection and Spam Lists (DNS blocklists)
# ----------------------------------------------
#

# Do you want to check messages to see if they are spam?
# Note: If you switch this off then *no* spam checks will be done at all.
#       This includes both MailScanner's own checks and SpamAssassin.
#       If you want to just disable the "Spam List" feature then set
#       "Spam List =" (i.e. an empty list) in the setting below.
# This can also be the filename of a ruleset.
Spam Checks = yes

# This is the list of spam blacklists (RBLs) which you are using.
# See the "Spam List Definitions" file for more information about what
# you can put here.
# This can also be the filename of a ruleset.
Spam List = # ORDB-RBL SBL+XBL # You can un-comment this to enable them

# This is the list of spam domain blacklists which you are using
# (such as the "rfc-ignorant" domains). See the "Spam List Definitions"
# file for more information about what you can put here.
# This can also be the filename of a ruleset.
Spam Domain List =

# 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 Be Spam = 1

# 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 Lists To Reach High Score = 3

# If an individual "Spam List" or "Spam Domain List" check takes longer
# that this (in seconds), the check is abandoned and the timeout noted.
Spam List Timeout = 10

# The maximum number of timeouts caused by any individual "Spam List" or
# "Spam Domain List" before it is marked as "unavailable". Once marked,
# the list will be ignored until the next automatic re-start (see
# "Restart Every" for the longest time it will wait).
# This can also be the filename of a ruleset.
Max Spam List Timeouts = 7

# 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").
Spam List Timeouts History = 10

# Spam Whitelist:
# Make this point to a ruleset, and anything in that ruleset whose value
# is "yes" will *never* be marked as spam.
# The whitelist check is done before the blacklist check. If anyone whitelists
# a message, then all recipients get the message. If no-one has whitelisted it,
# then the blacklist is checked.
# This setting over-rides the "Is Definitely Spam" setting.
# This can also be the filename of a ruleset.
#Is Definitely Not Spam = no
Is Definitely Not Spam = %rules-dir%/spam.whitelist.rules

# Spam Blacklist:
# Make this point to a ruleset, and anything in that ruleset whose value
# is "yes" will *always* be marked as spam.
# This value can be over-ridden by the "Is Definitely Not Spam" setting.
# This can also be the filename of a ruleset.
Is Definitely Spam = 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.
Definite Spam Is High Scoring = no

# 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.
Ignore Spam Whitelist If Recipients Exceed = 20

#
# SpamAssassin
# ------------
#

# Do you want to find spam using the "SpamAssassin" package?
# This can also be the filename of a ruleset.
Use SpamAssassin = no

# 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.
Max SpamAssassin Size = 30000

# This replaces the SpamAssassin configuration value 'required_hits'.
# If a message achieves a SpamAssassin score higher than this value,
# it is spam. See also the High SpamAssassin Score configuration option.
# This can also be the filename of a ruleset, so the SpamAssassin
# required_hits value can be set to different values for different messages.
Required SpamAssassin Score = 6

# If a message achieves a SpamAssassin score higher than this value,
# then the "High Scoring Spam Actions" are used. You may want to use
# this to deliver moderate scores, while deleting very high scoring messsages.
# This can also be the filename of a ruleset.
High SpamAssassin Score = 10

# Set this option to "yes" to enable the automatic whitelisting functions
# available within SpamAssassin. This will cause addresses from which you
# get real mail, to be marked so that it will never incorrectly spam-tag
# messages from those addresses.
# To disable whitelisting, you must set "use_auto_whitelist 0" in your
# spam.assassin.prefs.conf file as well as set this to no.
SpamAssassin Auto Whitelist = no

# Set the location of the SpamAssassin user_prefs file. If you want to
```

```
1397  # stop SpamAssassin doing all the RBL checks again, then you can add
1398  # "skip_rbl_checks = 1" to this prefs file.
1399  SpamAssassin Prefs File = %etc-dir%/spam.assassin.prefs.conf
1400
1401  # If SpamAssassin takes longer than this (in seconds), the check is
1402  # abandoned and the timeout noted.
1403  SpamAssassin Timeout = 75
1404
1405  # If SpamAssassin times out more times in a row than this, then it will be
1406  # marked as "unavailable" until MailScanner next re-starts itself.
1407  # This means that remote network failures causing SpamAssassin trouble will
1408  # not mean your mail stops flowing.
1409  Max SpamAssassin Timeouts = 10
1410
1411  # The total number of SpamAssassin attempts during which "Max SpamAssassin
1412  # Timeouts" will cause SpamAssassin to be marked as "unavailable".
1413  # See the previous comment for more information.
1414  # The default values of 10 and 20 mean that 10 timeouts in any sequence of
1415  # 20 attempts will trigger the behaviour described above, until the next
1416  # periodic restart (see "Restart Every").
1417  SpamAssassin Timeouts History = 30
1418
1419  # If the message sender is on any of the Spam Lists, do you still want
1420  # to do the SpamAssassin checks? Setting this to "no" will reduce the load
1421  # on your server, but will stop the High Scoring Spam Actions from ever
1422  # happening.
1423  # This can also be the filename of a ruleset.
1424  Check SpamAssassin If On Spam List = yes
1425
1426  # Do you want to include the "Spam Score" header. This shows 1 character
1427  # (Spam Score Character) for every point of the SpamAssassin score. This
1428  # makes it very easy for users to be able to filter their mail using
1429  # whatever SpamAssassin threshold they want. For example, they just look
1430  # for "sssss" for every message whose score is > 5, for example.
1431  # This can also be the filename of a ruleset.
1432  Spam Score = yes
1433
1434  # If you are using the Bayesian statistics engine on a busy server,
1435  # you may well need to force a Bayesian database rebuild and expiry
1436  # at regular intervals. This is measures in seconds.
1437  # 1 day = 86400 seconds.
1438  # To disable this feature set this to 0.
1439  Rebuild Bayes Every = 0
1440
1441  # The Bayesian database rebuild and expiry may take a 2 or 3 minutes
1442  # to complete. During this time you can either wait, or simply
1443  # disable SpamAssassin checks until it has completed.
1444  Wait During Bayes Rebuild = no
1445
1446  #
```

```
1447  # What to do with spam
1448  # --------------------
1449  #
1450
1451  # This is a list of actions to take when a message is spam.
1452  # It can be any combination of the following:
1453  #   deliver              - deliver the message as normal
1454  #   delete               - delete the message
1455  #   store                - store the message in the quarantine
1456  #   bounce                 - send a rejection message back to the sender
1457  #   forward user@domain.com - forward a copy of the message to user@domain.com
1458  #   striphtml             - convert all in-line HTML content to plain text.
1459  #                         You need to specify "deliver" as well for the
1460  #                         message to reach the original recipient.
1461  #   attachment              - Convert the original message into an attachment
1462  #                         of the message. This means the user has to take
1463  #                         an extra step to open the spam, and stops "web
1464  #                         bugs" very effectively.
1465  #   notify               - Send the recipients a short notification that
1466  #                         spam addressed to them was not delivered. They
1467  #                         can then take action to request retrieval of
1468  #                         the original message if they think it was not
1469  #                         spam.
1470  #   header "name: value"    - Add the header
1471  #                           name: value
1472  #                         to the message. name must not contain any spaces.
1473  #
1474  # This can also be the filename of a ruleset, in which case the filename
1475  # must end in ".rule" or ".rules".
1476  #Spam Actions = store forward anonymous@ecs.soton.ac.uk
1477  Spam Actions = deliver
1478
1479  # This is just like the "Spam Actions" option above, except that it applies
1480  # then the score from SpamAssassin is higher than the "High SpamAssassin Score"
1481  # value.
1482  #   deliver              - deliver the message as normal
1483  #   delete               - delete the message
1484  #   store                - store the message in the quarantine
1485  #   forward user@domain.com - forward a copy of the message to user@domain.com
1486  #   striphtml             - convert all in-line HTML content to plain text.
1487  #                         You need to specify "deliver" as well for the
1488  #                         message to reach the original recipient.
1489  #   attachment              - Convert the original message into an attachment
1490  #                         of the message. This means the user has to take
1491  #                         an extra step to open the spam, and stops "web
1492  #                         bugs" very effectively.
1493  #   notify               - Send the recipients a short notification that
1494  #                         spam addressed to them was not delivered. They
1495  #                         can then take action to request retrieval of
1496  #                         the original message if they think it was not
```

```
#                       spam.
#   header "name: value"    - Add the header
#                         name: value
#                       to the message. name must not contain any spaces.
#
# This can also be the filename of a ruleset, in which case the filename
# must end in ".rule" or ".rules".
High Scoring Spam Actions = deliver

# This is just like the "Spam Actions" option above, except that it applies
# to messages that are *NOT* spam.
#   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
#   header "name: value"    - Add the header
#                         name: value
#                       to the message. name must not contain any spaces.
#
# This can also be the filename of a ruleset, in which case the filename
# must end in ".rule" or ".rules".
Non Spam Actions = deliver

# There are 3 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.
#
# These can also be the filenames of rulesets.
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

# 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.
Inline Spam Warning = %report-dir%/inline.spam.warning.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.
Recipient Spam Report = %report-dir%/recipient.spam.report.txt

# 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.
```

```
1547  # Beware that many sites will automatically delete the bounce messages
1548  # created by using this option unless you have agreed this with them in
1549  # advance.
1550  # If you enable this, be prepared to handle the irate responses from
1551  # people to whom you are essentially sending more spam!
1552  Enable Spam Bounce = %rules-dir%/bounce.rules
1553
1554  # When you bounce a spam message back to the sender, do you want to
1555  # encapsulate it in another message, rather like the "attachment" option
1556  # when delivering spam to the original recipient?
1557  # NOTE: If you enable this option, be sure to whitelist your local server
1558  #       ie. 127.0.0.1 as otherwise the spam bounce message will be detected
1559  #       as spam again, which will cause another spam bounce and so on
1560  #       until your mail queues fill up and your server crashes!
1561  # This can also be the filename of a ruleset.
1562  Bounce Spam As Attachment = no
1563
1564  #
1565  # Logging
1566  # -------
1567  #
1568
1569  # This is the syslog "facility" name that MailScanner uses. If you don't
1570  # know what a syslog facility name is, then either don't change this value
1571  # or else go and read "man syslog.conf". The default value of "mail" will
1572  # cause the MailScanner logs to go into the same place as all your other
1573  # mail logs.
1574  Syslog Facility = mail
1575
1576  # Do you want to log the processing speed for each section of the code
1577  # for a batch? This can be very useful for diagnosing speed problems,
1578  # particularly in spam checking.
1579  Log Speed = no
1580
1581  # Do you want all spam to be logged? Useful if you want to gather
1582  # spam statistics from your logs, but can increase the system load quite
1583  # a bit if you get a lot of spam.
1584  Log Spam = no
1585
1586  # Do you want all non-spam to be logged? Useful if you want to see
1587  # all the SpamAssassin reports of mail that was marked as non-spam.
1588  # Note: It will generate a lot of log traffic.
1589  Log Non Spam = no
1590
1591  # Log all the filenames that are allowed by the Filename Rules, or just
1592  # the filenames that are denied?
1593  # This can also be the filename of a ruleset.
1594  Log Permitted Filenames = no
1595
1596  # Log all the filenames that are allowed by the Filetype Rules, or just
```

```
1597  # the filetypes that are denied?
1598  # This can also be the filename of a ruleset.
1599  Log Permitted Filetypes = no
1600
1601  # Log all occurrences of "Silent Viruses" as defined above?
1602  # This can only be a simple yes/no value, not a ruleset.
1603  Log Silent Viruses = no
1604
1605  # Log all occurrences of HTML tags found in messages, that can be blocked.
1606  # This will help you build up your whitelist of message sources for which
1607  # particular HTML tags should be allowed, such as mail from newsletters
1608  # and daily cartoon strips.
1609  # This can also be the filename of a ruleset.
1610  Log Dangerous HTML Tags = no
1611
1612  #
1613  # Advanced SpamAssassin Settings
1614  # ------------------------------
1615  #
1616  # If you are using Postfix you may well need to use some of the settings
1617  # below, as the home directory for the "postfix" user cannot be written
1618  # to by the "postfix" user.
1619  # You may also need to use these if you have installed SpamAssassin
1620  # somewhere other than the default location.
1621  #
1622
1623  # The per-user files (bayes, auto-whitelist, user_prefs) are looked
1624  # for here and in ~/.spamassassin/. Note the files are mutable.
1625  # If this is unset then no extra places are searched for.
1626  # If using Postfix, you probably want to set this as shown in the example
1627  # line at the end of this comment, and do
1628  #      mkdir /var/spool/MailScanner/spamassassin
1629  #      chown postfix.postfix /var/spool/MailScanner/spamassassin
1630  # NOTE: SpamAssassin is always called from MailScanner as the same user,
1631  #       and that is the "Run As" user specified above. So you can only
1632  #       have 1 set of "per-user" files, it's just that you might possibly
1633  #       need to modify this location.
1634  #       You should not normally need to set this at all.
1635  #SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin
1636  SpamAssassin User State Dir =
1637
1638  # This setting is useful if SpamAssassin is installed in an unusual place,
1639  # e.g. /opt/MailScanner. The install prefix is used to find some fallback
1640  # directories if neither of the following two settings work.
1641  # If this is set then it adds to the list of places that are searched;
1642  # otherwise it has no effect.
1643  #SpamAssassin Install Prefix = /opt/MailScanner
1644  SpamAssassin Install Prefix =
1645
1646  # The site rules are searched for here.
```

```
# Normal location on most systems is /etc/mail/spamassassin.
SpamAssassin Site Rules Dir = /etc/mail/spamassassin

# The site-local rules are searched for here, and in prefix/etc/spamassassin,
# prefix/etc/mail/spamassassin, /usr/local/etc/spamassassin, /etc/spamassassin,
# /etc/mail/spamassassin, and maybe others.
# If this is set then it adds to the list of places that are searched;
# otherwise it has no effect.
#SpamAssassin Local Rules Dir = /etc/MailScanner/mail/spamassassin
SpamAssassin Local Rules Dir =

# The default rules are searched for here, and in prefix/share/spamassassin,
# /usr/local/share/spamassassin, /usr/share/spamassassin, and maybe others.
# If this is set then it adds to the list of places that are searched;
# otherwise it has no effect.
#SpamAssassin Default Rules Dir = /opt/MailScanner/share/spamassassin
SpamAssassin Default Rules Dir =

#
# 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.
#
# See http://www.sng.ecs.soton.ac.uk/mailscanner/install/mcp/ for more info.
#

MCP Checks = no

# Do the spam checks first, or the MCP checks first?
# This cannot be the filename of a ruleset, only a fixed value.
First Check = mcp

# The rest of these options are clones of the equivalent spam options
MCP Required SpamAssassin Score = 1
MCP High SpamAssassin Score = 10
MCP Error Score = 1

MCP Header = X-%org-name%-MailScanner-MCPCheck:
Non MCP Actions = deliver
MCP Actions = deliver
High Scoring MCP Actions = deliver
Bounce MCP As Attachment = no

MCP Modify Subject = yes
MCP Subject Text = {MCP?}
```

```
High Scoring MCP Modify Subject = yes
High Scoring MCP Subject Text = {MCP?}

Is Definitely MCP = no
Is Definitely Not MCP = no
Definite MCP Is High Scoring = no
Always Include MCP Report = no
Detailed MCP Report = yes
Include Scores In MCP Report = no
Log MCP = no

MCP Max SpamAssassin Timeouts = 20
MCP Max SpamAssassin Size = 100000
MCP SpamAssassin Timeout = 10

MCP SpamAssassin Prefs File = %mcp-dir%/mcp.spam.assassin.prefs.conf
MCP SpamAssassin User State Dir =
MCP SpamAssassin Local Rules Dir = %mcp-dir%
MCP SpamAssassin Default Rules Dir = %mcp-dir%
MCP SpamAssassin Install Prefix = %mcp-dir%
Recipient MCP Report = %report-dir%/recipient.mcp.report.txt
Sender MCP Report = %report-dir%/sender.mcp.report.txt

#
# Advanced Settings
# -----------------
#
# Don't bother changing anything below this unless you really know
# what you are doing, or else if MailScanner has complained about
# your "Minimum Code Status" setting.
#

# 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 "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 "*@*".
#
# 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.
Use Default Rules With Multiple Recipients = no
```

```
1747
1748  # When putting the value of the spam score of a message into the headers,
1749  # how do you want to format it. If you don't know how to use sprintf() or
1750  # printf() in C, please *do not modify* this value. A few examples for you:
1751  # %d     ==> 12
1752  # %5.2f  ==> 12.34
1753  # %05.1f ==> 012.3
1754  # This can also be the filename of a ruleset.
1755  Spam Score Number Format = %d
1756
1757  # This is the version number of the MailScanner distribution that created
1758  # this configuration file. Please do not change this value.
1759  MailScanner Version Number = 4.42.9
1760
1761  # Set Debug to "yes" to stop it running as a daemon and just process
1762  # one batch of messages and then exit.
1763  Debug = no
1764
1765  # Do you want to debug SpamAssassin from within MailScanner?
1766  Debug SpamAssassin = no
1767
1768  # Set Run In Foreground to "yes" if you want MailScanner to operate
1769  # normally in foreground (and not as a background daemon).
1770  # Use this if you are controlling the execution of MailScanner
1771  # with a tool like DJB's 'supervise' (see http://cr.yp.to/daemontools.html).
1772  Run In Foreground = no
1773
1774  # If you are using an LDAP server to read the configuration, these
1775  # are the details required for the LDAP connection. The connection
1776  # is anonymous.
1777  #LDAP Server = localhost
1778  #LDAP Base   = o=fsl
1779  #LDAP Site   = default
1780
1781  # This option is intended for people who want to log more information
1782  # about messages than what is put in syslog. It is intended to be used
1783  # with a Custom Function which has the side-effect of logging information,
1784  # perhaps to an SQL database, or any other processing you want to do
1785  # after each message is processed.
1786  # Its value is completely ignored, it is purely there to have side
1787  # effects.
1788  # If you want to use it, read CustomConfig.pm.
1789  Always Looked Up Last = no
1790
1791  # When attempting delivery of outgoing messages, should we do it in the
1792  # background or wait for it to complete? The danger of doing it in the
1793  # background is that the machine load goes ever upwards while all the
1794  # slow sendmail processes run to completion. However, running it in the
1795  # foreground may cause the mail server to run too slowly.
1796  Deliver In Background = yes
```

```
1797
1798  # Attempt immediate delivery of messages, or just place them in the outgoing
1799  # queue for the MTA to deliver when it wants to?
1800  #      batch -- attempt delivery of messages, in batches of up to 20 at once.
1801  #      queue -- just place them in the queue and let the MTA find them.
1802  # This can also be the filename of a ruleset. For example, you could use a
1803  # ruleset here so that messages coming to you are immediately delivered,
1804  # while messages going to any other site are just placed in the queue in
1805  # case the remote delivery is very slow.
1806  Delivery Method = batch
1807
1808  # Are you using Exim with split spool directories? If you don't understand
1809  # this, the answer is probably "no". Refer to the Exim documentation for
1810  # more information about split spool directories.
1811  Split Exim Spool = no
1812
1813  # Where to put the virus scanning engine lock files.
1814  # These lock files are used between MailScanner and the virus signature
1815  # "autoupdate" scripts, to ensure that they aren't both working at the
1816  # same time (which could cause MailScanner to let a virus through).
1817  Lockfile Dir = /tmp
1818
1819  # Where to put the code for your "Custom Functions". No code in this
1820  # directory should be over-written by the installation or upgrade process.
1821  # All files starting with "." or ending with ".rpmnew" will be ignored,
1822  # all other files will be compiled and may be used with Custom Functions.
1823  Custom Functions Dir = /usr/lib/MailScanner/MailScanner/CustomFunctions
1824
1825  # How to lock spool files.
1826  # Don't set this unless you *know* you need to.
1827  # For sendmail, it defaults to "flock".
1828  # For sendmail 8.13 onwards, you will probably need to change it to posix.
1829  # For Exim, it defaults to "posix".
1830  # No other type is implemented.
1831  Lock Type =
1832
1833  # Minimum acceptable code stability status -- if we come across code
1834  # that's not at least as stable as this, we barf.
1835  # This is currently only used to check that you don't end up using untested
1836  # virus scanner support code without realising it.
1837  # Levels used are:
1838  # none          - there may not even be any code.
1839  # unsupported   - code may be completely untested, a contributed dirty hack,
1840  #                 anything, really.
1841  # alpha         - code is pretty well untested. Don't assume it will work.
1842  # beta          - code is tested a bit. It should work.
1843  # supported     - code *should* be reliable.
1844  #
1845  # Don't even *think* about setting this to anything other than "beta" or
1846  # "supported" on a system that receives real mail until you have tested it
```

```
1847  # yourself and are happy that it is all working as you expect it to.
1848  # Don't set it to anything other than "supported" on a system that could
1849  # ever receive important mail.
1850  #
1851  # READ and UNDERSTAND the above text BEFORE changing this.
1852  #
1853  Minimum Code Status = supported
```