VisNetic MailServer

AntiSpam Reference Manual V9.0

Version 9.1

Contents

CHAPTER 1

Anti-Spam

VisNetic MailServer integrates many AntiSpam technologies to protect your Users from Spam.

VisNetic MailServer uses SpamAssassin, Bayesian Filters, Greylisting, Razor and Content Filters, giving you one of the most comprehensive AntiSpam toolsets on the market today.

Whether a message is marked as spam or not is based on a score, out of 10. All of the AntiSpam technologies modify this score according to their findings. At the end of the whole process VisNetic MailServer checks the spam score and acts accordingly. You have control over what spam score causes a message be classified as Spam, Quarantined, or Deleted.

In This Chapter

AntiSpam - Spam Scores

One of the first things you need to understand is the concept of a Spam Score.

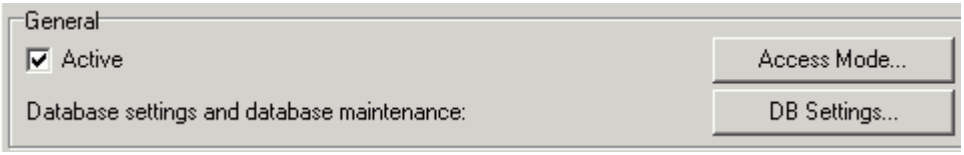
As VisNetic MailServer processes messages with its many AntiSpam technologies and checks, it modifies a Spam Score value dependent on the results of each test.

The Spam score is a value from 0.00 to 10.00 and indicates the probability that the message is Spam, with 10.00 being an indication that the message is very likely to be Spam.

Some of the settings within VisNetic MailServer allow you to set a value to modify the Spam Score (for example - the ***Content checks*** (see "Miscellaneous - Content" on page 38)). The Value you enter in this section is the amount that VisNetic MailServer will modify the Spam Score by. So if you enter 1.5 for "Score message containing blank subject and blank body" then the Spam score will be increased by 1.5 if that test evaluates as true.

AntiSpam - General

AS General - General



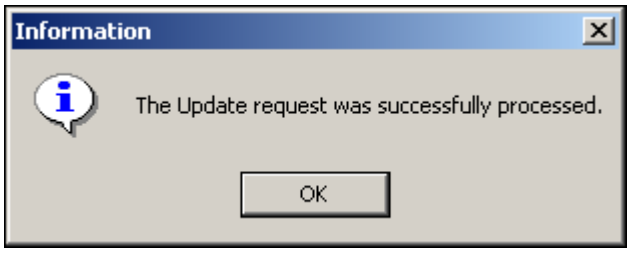
Field	Description
Active	Check this option to activate AntiSpam processing (Highly recommended).
Access Mode	Press this button to specify which accounts and/or domains should use the AntiSpam service.
ODBC settings and database maintenance	Press this button to modify ODBC settings. By default, VisNetic MailServer installs with an MS Access database to store data. You should be aware that Access can become severely slow when the database contains more than 10K records and at this point you should consider moving to an industrial-strength database.

The "Updates Schedule" section allows you to schedule hands-free updates to the AntiSpam Reference Base, which is used by the Bayesian filters for accurate Spam recognition.

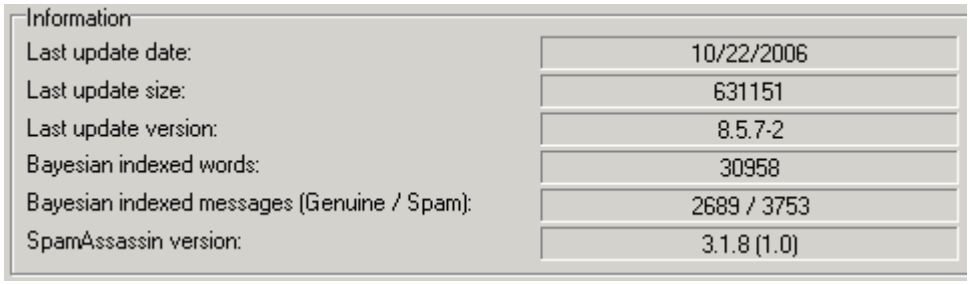
This Reference Base is maintained by our staff and ensures optimum Bayesian Filter performance for most users. Millions of spam and genuine emails have been processed to give you near 100% accuracy.

Note that server-based indexing (see ***AS Bayesian*** (on page 27)) creates a separate User Reference Base.

Field	Description
Enable	Check this box to enable automatic updates of the Reference Base.

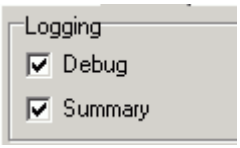
At:	Specify a time that the update should take place.
Su - Sa	Check the days on which the update should take place.
Update Now	Press this button to immediately update the Reference base, if required. If all is well you will get a message box similar to the following. 

The Reference Base is around 800Kb in size and the download time will depend on your connection speed.



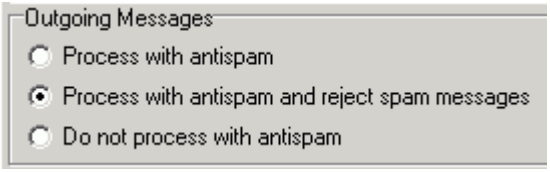
Field	Description
Last update date	The date that the reference Base was last updated.
Last update size	Shows the size of the last update file. Can be useful for troubleshooting
Last update version	Which version of the Reference Base is in use.
Bayesian indexed words	Shows the number of words in the Bayesian database
Bayesian indexed messages (Genuine/Spam)	Shows the number of Genuine and Spam messages that have been analyzed to produce the Bayesian database.
SpamAssassin version.	Which version of the SpamAssassin engine is running.

AS General - Other



Field	Description
Debug	Check this option to include detailed records in the AntiSpam log.
Summary	Check this option to include Summary records in the AntiSpam log.

The log files are located in standard location '<InstallDirectory>\log\antispam\'

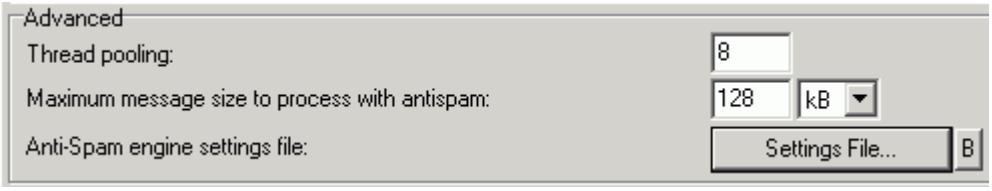


These options allow you to define what AntiSpam processing will be performed on outgoing messages.

Choose from the options listed:

Field	Description
Process with AntiSpam	Use this option to have all messages processed but then forwarded no matter what the result. Messages identified as Spam will be marked according to your settings and sent.
Process with AntiSpam and reject Spam messages	Use this option to have all messages processed and any that are identified as Spam will be rejected.
Do not process with AntiSpam	Use this option to bypass AntiSpam processing. You should only use this if you trust all Users on your system.

Field	Description
Process unknown accounts	This option is to tell VisNetic MailServer what to do when a message comes in for an undefined Account (for example an account that is going to be forwarded to a defined Account via Rules). Check the box to have these messages processed by the AntiSpam engine.



Field	Description
Thread pooling	Specify here the maximum number of threads to use when processing messages with the AntiSpam engine. This can be useful for reducing (or increasing) server load
Maximum message size to process with AntiSpam	Specify a maximum size of message to be processed with the AntiSpam engine.
AntiSpam engine settings file	Press the Settings File button to open up the AntiSpam settings file in a simple text editor. Comments are included in the file. You can change the settings here but you should be sure you know what you are doing.
The 'B' button	Press this button to open up the AntiSpam Bypass file, listing any users, accounts or domains from which messages will not undergo AntiSpam processing.

Note - that you can get comprehensive spamassassin rule statistics by specifying a file name in the settings file. Do this under the spamassassinrulestats entry in the format:

spamassassinrulestats="<filename>"

You can use Time/date variables here if you want to create daily/hourly files etc.

spamassassinrulestats="yyyymmddhhmmss.txt"

The contents of the files will allow you to see which rules have been used and how many times and also you can analyse which rules have ***not*** been hit, allowing you to delete them to speed up processing and save processing power on your server. A simple example from a statistics file is shown below

```
SpamAssassin statistics 2007-08-15 00:00


Genuine: 649
SpamQuarantine: 0
SpamMarked: 416
SpamRefused: 205
SpamAssassin: 481
Rules: 1293
Hits: 254
TotalHits: 13588
NoHits: 1039


Rules with hits:
__FRAUD_DBI (1.00) 29
.... list of rules
Total: 254, Hits: 13588


Rules with no hits:
DRUGS_DEPR_EREC (1.00) # Refers to both an erectile and an antidepressant ... list
   of rules
Total: 1039
```

AS - Action

AS Action - General

The Action tab allows you to define what actions should be taken according to the Spam score.

You should be aware that the spam score is always a value from 0 to 10, with 10 signifying the highest probability that the message is Spam.

A score of 0 is assigned to a message if it bypasses Spam processing.

Field	Description
Score required to quarantine message	Check this option to have a message quarantined if it's spam score is equal to or higher than the value selected. Move the slider to change the value. NOTE - that the ***Quarantine*** (see "AS Quarantine" on page 12) function must be enabled for this control to work.
Score required to classify message as spam	Check this option to have a message classified as spam if it's spam score is equal to or higher than the value selected. Move the slider to change the value.
Score required to refuse message	Check this option to have a message deleted if it's spam score is equal to or higher than the value selected. Move the slider to change the value.

NOTE - that Quarantined messages are held in a pending queue until they are authorized, manually delivered, or deleted.

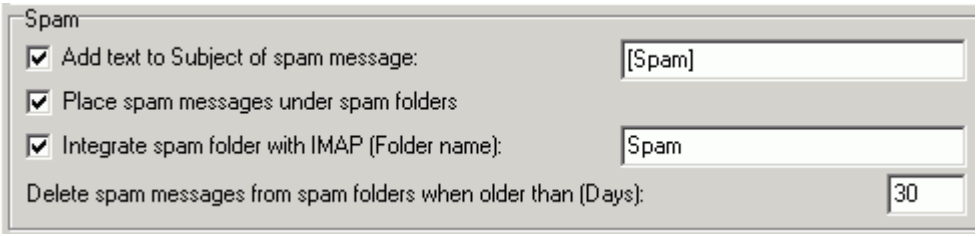
Authorization is either manual, by a User or Domain Administrator using WebAdmin or WebMail, or automatic if the sender responds to a Challenge Response email (see ***Trust - Quarantine*** (see "AS Quarantine" on page 12)).

Deletion is either manual, by a User or Domain Administrator using WebAdmin or WebMail, or automatic if set within VisNetic MailServer (see ***Trust - Quarantine*** (see "AS Quarantine" on page 12)).

Manual delivery can only be done by a User or Domain Administrator using WebMail or WebAdmin.

Field	Description
Refuse message	Select an action for messages that are refused.

action	**Delete** Choosing this option causes VisNetic MailServer to "delete" the message without informing the sending server, so the Sender does not get to know about it. **Reject** Choosing this option causes VisNetic MailServer to reject the message and issue an informational message to the sending server to that effect.
Archive refused messages to account	Select an account to have refused messages archived to. Use the '...' button to open the Account Selection Dialog. This option works whether the Delete or Reject option is chosen above.



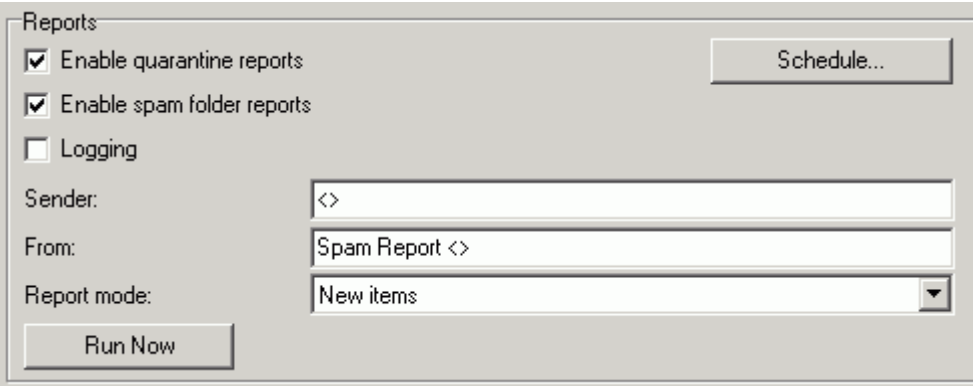
Field	Description

Add text to Subject of spam message	Check this option to have text added to the subject of messages classified as spam.
	Specify the required text in the text box.
	Note that system variables can be used in this field, as shown in the previous screenshot.
	Example:
	With the setting as shown in the previous screenshot, a message with the subject
	`Cheap Meds Here`
	will have it's subject modified to something like
	`[Spam 5.97] Cheap Meds Here`
	if it is identified as spam.
	This enables your Users to define rules in their email clients to deal with suspected spam messages.

Place spam messages under spam folders	Check this option to enable the use of Spam Folders for Users. Messages marked as spam will not be saved to the User's Inbox, but will be saved to a separate Spam Folder. You can further define Spam Administrator(s) who can maintain one or more Spam Folders.

	This can be a great time saver for busy executives, allowing an assistant to check the Spam Folder for any "real" messages and moving them accordingly.
Integrate spam folder with IMAP (Folder name)	Check this option to have the Spam folder integrated with your IMAP accounts. Enter the name of the IMAP folder to be used for Spam.
Delete spam messages from spam folders when older than (Days)	Specify a number of days after which messages are automatically deleted from the Spam Folder.

AS Action - Reports



Field	**Description**
Enable quarantine reports	Check this box to have quarantine report emails sent to your users.
Enable spam folder reports	Check this box to have spam folder reports sent to your users.
Logging	Check this option to have detailed report logging enabled.
Schedule	Press this button to define a schedule for sending Quarantine reports. A simple dialog is opened allowing you to pick a schedule.
Sender	Enter the sender you wish the reports to be sent from. This should be something meaningful.
From	Enter the From header information you wish to appear in the reports.
Report Mode	Choose one of the following: **New items** - and the reports will only contain items that have been added

	since the last report. **All items** - and the reports will always contain all items.

AS Quarantine

The Quarantine function of VisNetic MailServer allows you to place incoming messages in a pending queue awaiting authorization.

Users can manage their own pending queue via WebMail.

Domain Administrators can manage all pending messages in their Domain via WebMail or WebAdmin.

Valid options for a pending messages are:

Authorize - delivers the message and adds the sender to the Quarantine Whitelist and no further messages from him will be quarantined.

Deliver - delivers the message to the recipient without adding the sender to the whitelist.

Blacklist - simply deletes the message from the pending queue.

You can specify that external recipients of messages sent by your Users are automatically added to the WhiteList (see ***Action*** (see "AS Action - General" on page 8)).

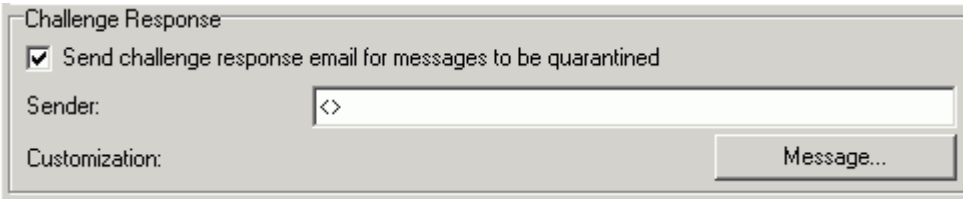
You can specify a period of time after which pending messages are deleted from the queue (see later in this section).

You can also Activate a Challenge Response system, whereby an un-authorized sender can prove he is a real person by visiting a website (see later in this section).

You can see the status of the pending queue and the Quarantine Whitelist in the Spam Queues node of the Administration Console or WebAdmin.

Field	Description
Active	Check this option to enable Greylist processing.
Access Mode	Press this button to specify which Accounts and Domains will have access to Greylisting.
Quarantine	Press this button to jump to the Quarantine queue in Spam Queues

Field	Description
Remove Pending messages after Days	Specify the number of days a message is held awaiting action.
Deliver expired messages to mailbox as Spam	Check this box to have messages delivered to your Users, marked as Spam, when the Quarantine period is up.
Local Users Mode	Select one of the three options defining how you wish to process messages from other Users on the same server (but maybe in different Domains). **Do not Quarantine local Users** Users from Domains on this server will not be challenged. Use this if you trust all users in all Domains. **Quarantine all local Users** All users will be Challenged. Use this if you host any Domain(s) of un-trusted, unrelated Users. **Quarantine local users from other domains** Local Users will be challenged if they are from a different Domain on the Server. Use this if you host domains of trusted and un-trusted Users (e.g. corporate domains).
Engine URL	Enter the URL of the confirmation page on the VisNetic MailServer. You should specify the port that VisNetic MailServer is using if it not the standard (port 80). If you have a multi-Domain server then you should use the system variable %%Recipient_Domain%% like so **http://%%Recipient_Domain%%:32000/challenge/** The above setting says to use the Domain of the email Recipient, on port 32000, so for an email to john@vmsdemo.com it will read **http://vmsdemo.com:32000/challenge** NOTE that the VisNetic MailServer webserver must be running for this function to work.



The Challenge Response that is delivered to the sender by VisNetic MailServer contains a URL that must be accessed in order to process the sender's confirmation (see the ***How it works section*** (see "Challenge Response - How It Works" on page 20)).

This URL points to a page that is served by VisNetic MailServer's Integrated Webserver that is installed by default with VisNetic MailServer.

This same engine is used by the Web-based Administration and by Web Mail.

Field	**Description**
Send Challenge response email for messages to be quarantined	Check this option to have a Challenge Response email sent to senders of quarantined messages
Sender	Specify here the sender that will be used in the SMTP protocol. We do not recommend changing this from the default (empty) option, as this will cut down on unwanted auto-responses etc.
Customization.	Press the Message button to customize the Challenge Response message content. The Message dialog will open allowing you to specify the From: and Subject: headers, and the message body content. You can use system variables within the message body. Note that the special variable %s ***must*** be included within the message body as this contains the URL to be visited.

Example:

The following confirmation request message has been generated by the mail server in response to the sender user@vmsdemo.com who sent a message to the user xxx@webmail.domaina.com.

The Challenge Response URL was defined as: **http://%%Recipient_Domain%%:32000/challenge/**

From:

To: <user@vmsdemo.com>

Received: from webmail.domaina.com

by mail.vmsdemo.com (VisNetic MailServer 7.2.3) with SMTP id DEMO

for <user@vmsdemo.com>; Sun, 07 Mar 2004 01:48:16 +0100

Date: Sun, 07 Mar 2004 01:48:16 +0100

From: Challenge Response <info@vmsdemo.com>

To: xxx@webmail.domaina.com

Message-Id: <812060168@mail.vmsdemo.com>

Subject: [Challenge Response] Confirm your email by visiting this URL

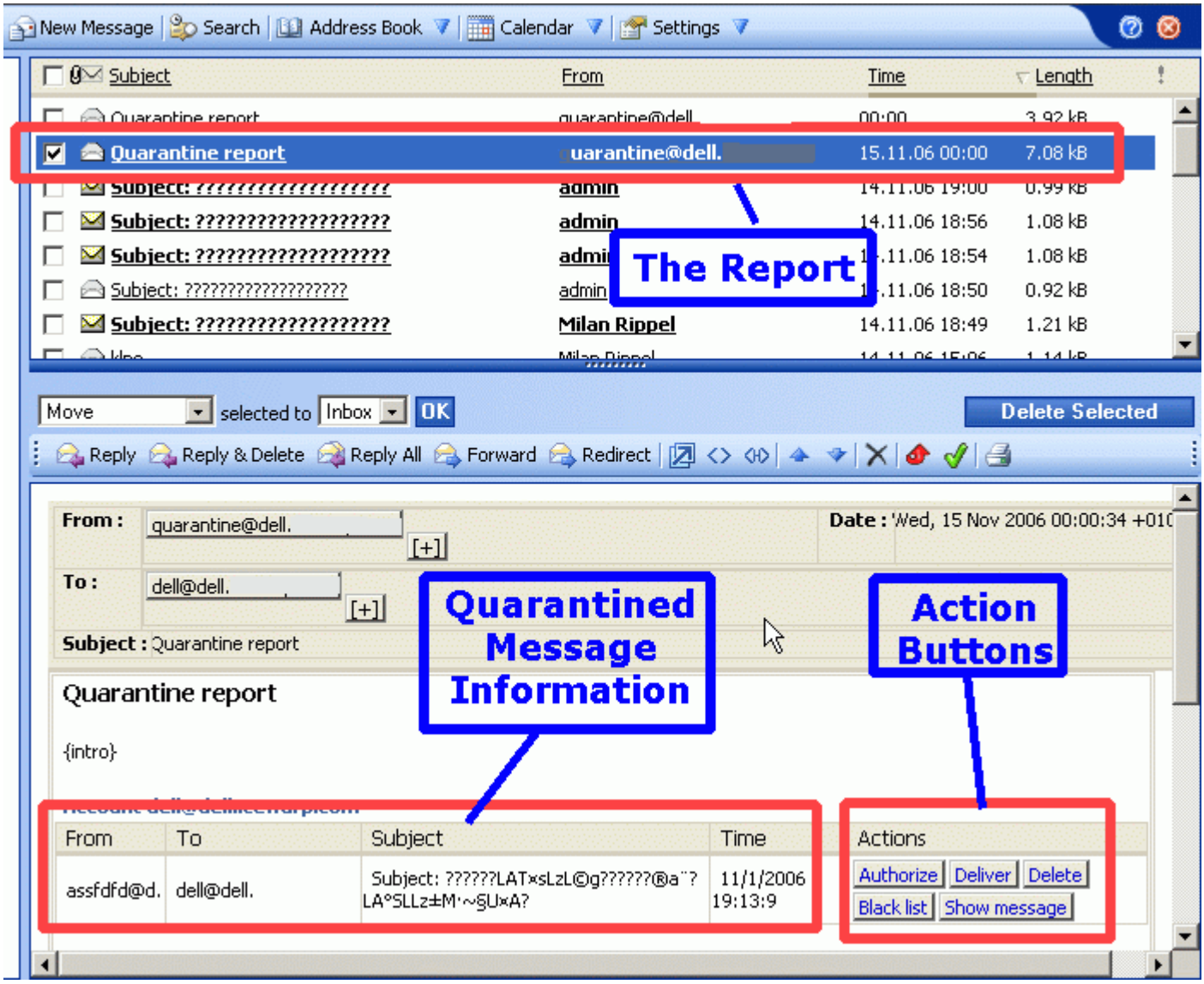
http://mail.vmsdemo.com:32000/challenge/?folder=c42c1a770e2d6d07ff358b2c22d7cf71

To prove your message was sent by a human and not a computer, visit the URL below and type in the alphanumeric text you will see in the image. You will only be asked to do this once for this email address.

http://webmail.domaina.com:32000/challenge/?folder=c42c1a770e2d6d07ff358b2c22d7cf71

Quarantine - The Quarantine Report

If enabled, as described above, each quarantine user will receive an email report listing quarantined messages with clickable links to action the message:



Details of the message are shown as in the screenshot above and a set of Action Buttons are available to process the message:

Authorize - What?

Deliver - Deliver the message to the recipient.

Delete - Delete the message.

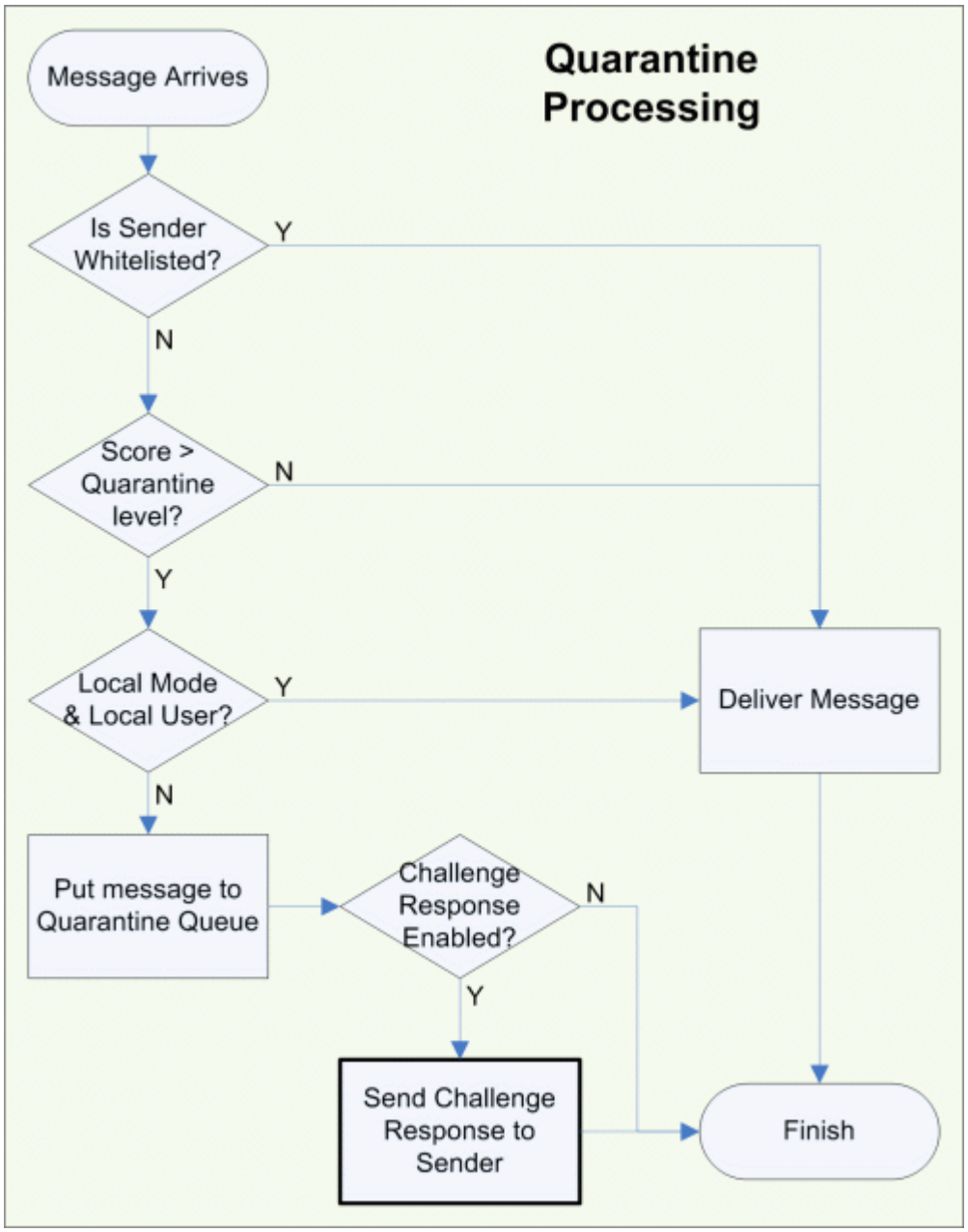
Black list - Add the sender to the blacklist.

Show message - Opens a new browser window showing the message, including headers, in text format

Quarantine - Processing for Incoming Messages

If the Quarantine function is enabled, all inbound message senders are checked against the Quarantine Whitelist. If the sender is Whitelisted the message is processed as normal. If the sender is not on the Whitelist, the message is held in the Quarantine pending queue.

In addition, if the Challenge Response system is enabled, a Challenge Response email is sent to the Sender, which allows him to authorize himself by visiting a web-page and effectively confirming he is a real person.

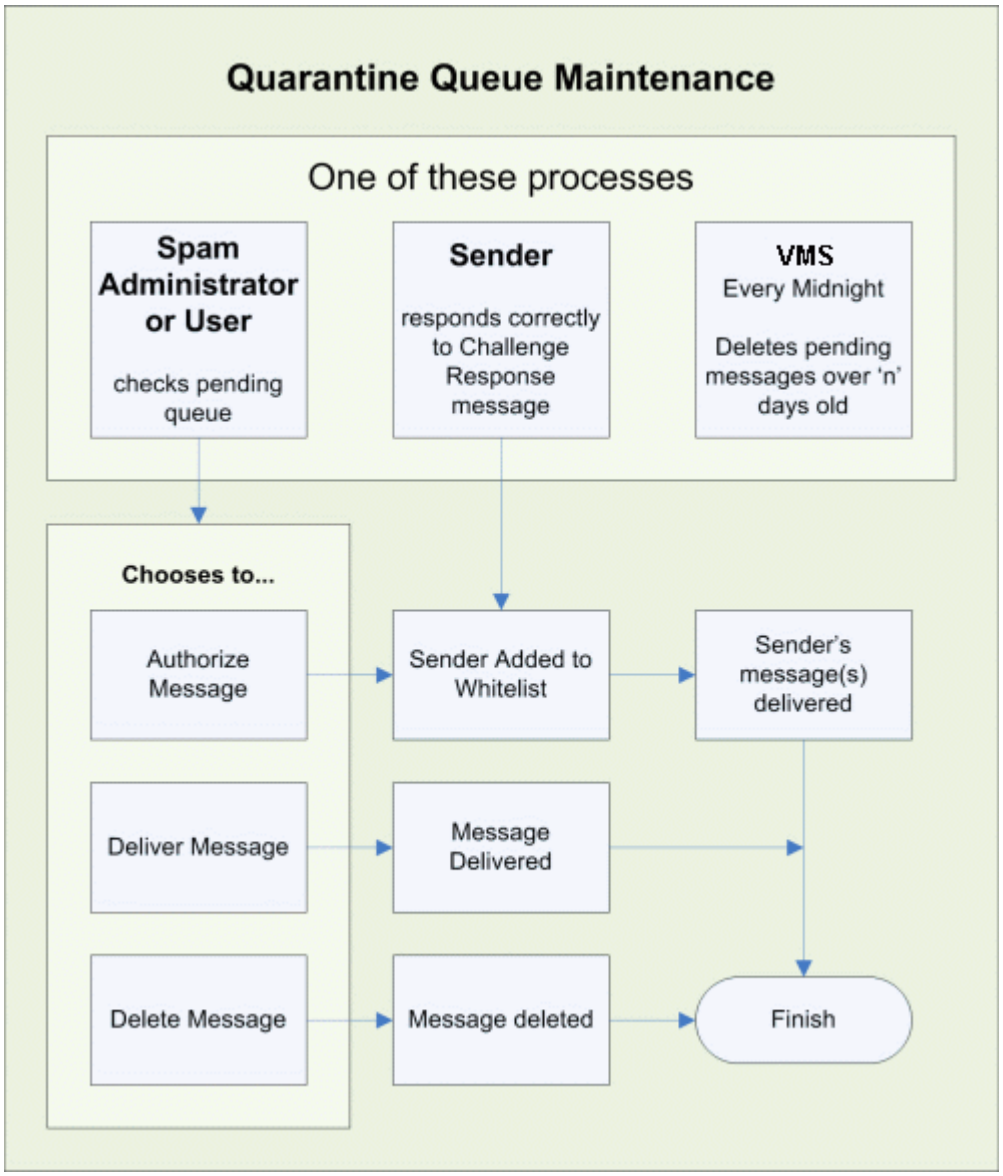


Quarantine - Processing for the Pending Queue

Messages held in the pending queue are dealt with in multiple ways:

- A Sender correctly responds to a Challenge Response email, and authorizes himself.
- A User checks his Quarantine Queue via WebMail and chooses to Authorize, Deliver or Delete message(s).
- A Spam Administrator checks any Quarantine Queues he is responsible for via WebMail or the Administration Console and chooses to Authorize, Deliver or Delete message(s).
- VisNetic MailServer automatically deletes a message after a selected number of days.

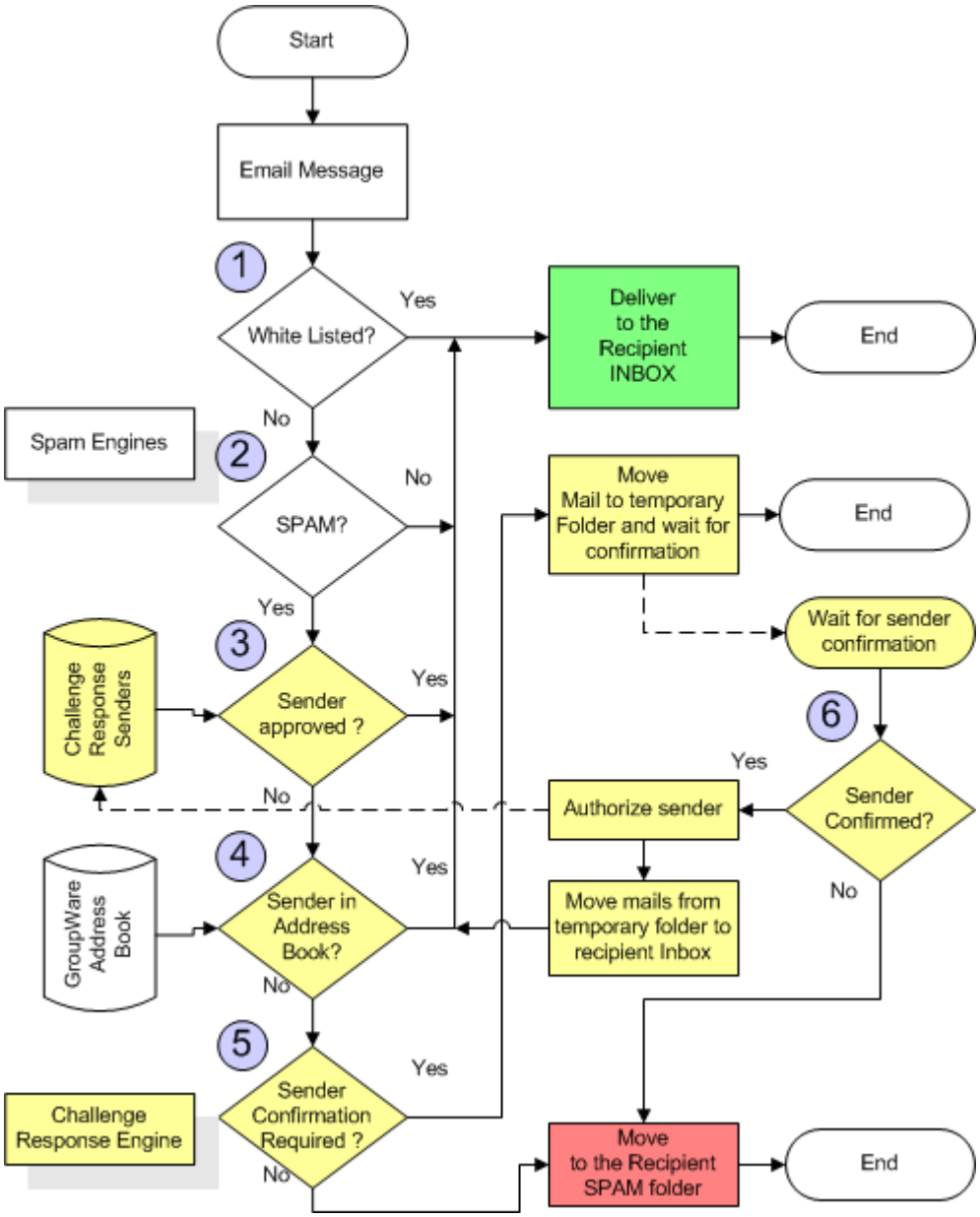
The following flowchart outlines the processing:



Challenge Response - How It Works

Challenge/Response is a system that requires the sender of an email to verify that he/she actually sent the email. This confirmation must be provided manually by visiting a web page and entering a code.

The Challenge/Response system is a critical component of the full Anti-Spam solution. The **yellow components** below are the full Instant Anti-Spam data diagram.



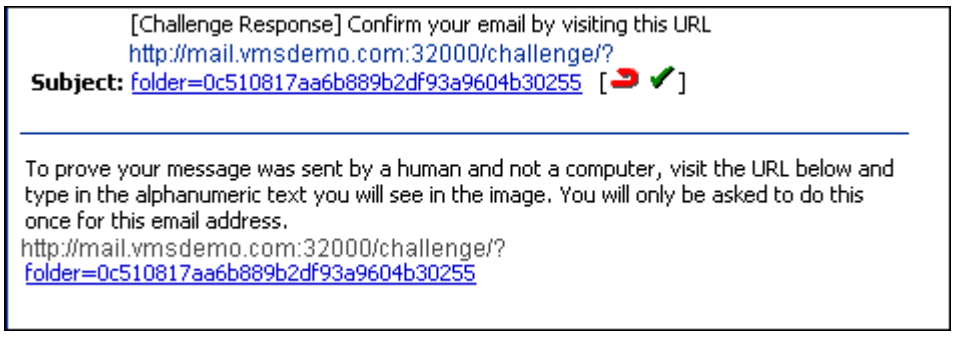
In the most typical situations, messages arrive at the Challenge/Response system after they have already passed all "white listing" possibilities as described in the Black & White Listing Techniques and are already marked as Spam.

- When the email is received by the server, it is not delivered to the recipient, but stored in a temporary folder. If more messages are sent from the same sender then all messages are stored in the same folder. Such messages are marked as "pending message(s)". If the pending message is not authorized within the specified number of days - it is automatically deleted.
- The Server will generate the request for confirmation, which will be delivered to the sender of the e-mail. It uses the sender from the SMTP protocol, which can be different from the "Mail From:" displayed in the message.
- The Sender (if they exist) will receive the request for confirmation and must confirm it. The confirmation requires visiting a special web site and entering some characters in a text field. It prevents usage of automated confirmation systems.
- The Server will receive the confirmation from the sender and will deliver the e-mail(s) to the recipient. The sender is also entered to the "approved senders list" so confirmation will not be requested the next time.

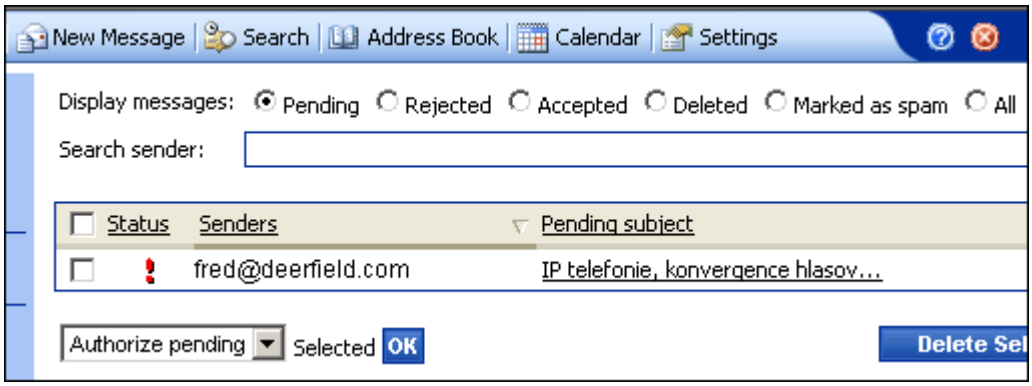
Emails with blank Mail From (it looks like MAIL FROM: <> in SMTP session) are bypassed by the Challenge Response engine. To handle such messages you should use Content Filters or Black & White Lists.

Screenshot Examples:

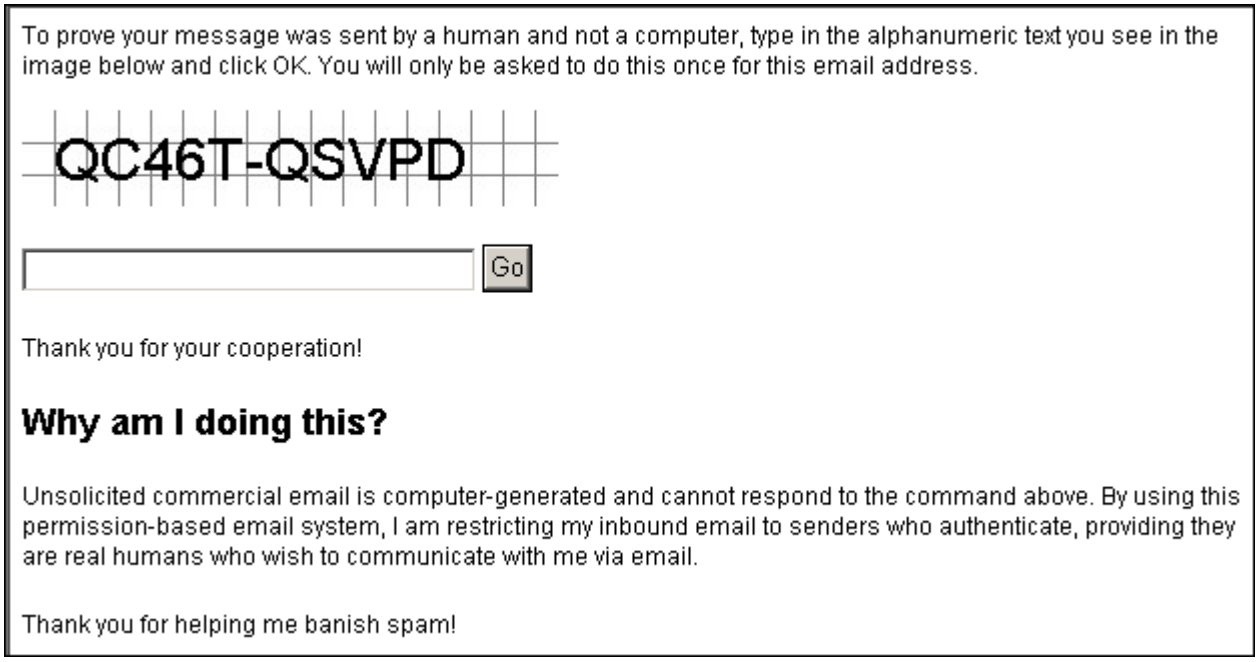
Request for confirmation sent by the mail server to the sender



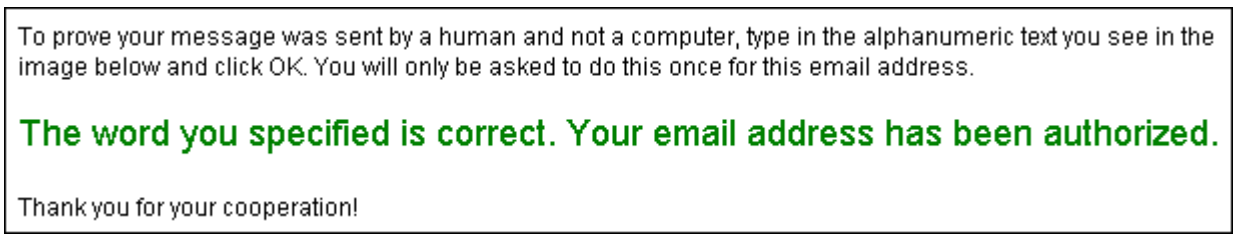
Sender waiting for authorization - pending in the database



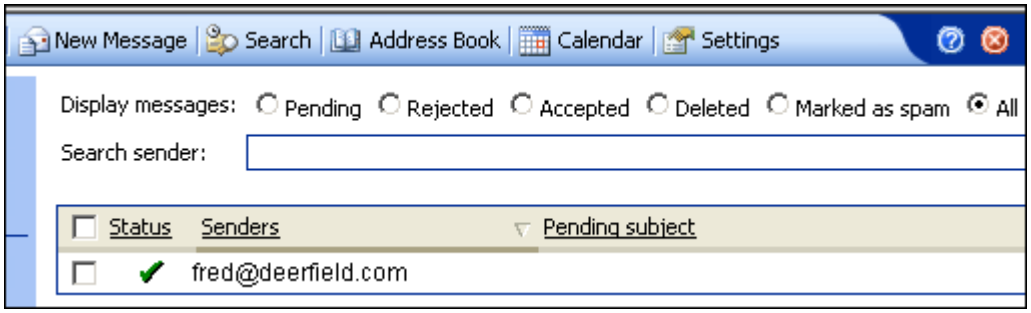
The URL of the page with sender confirmation request



If the sender enters the code properly they are automatically authorized



Sender is added to the Challenge Response as authorized.



Depending on the setup of the Challenge response system, the sender can be authorized for just one recipient, or for all recipients on the server.

AS - SpamAssassin

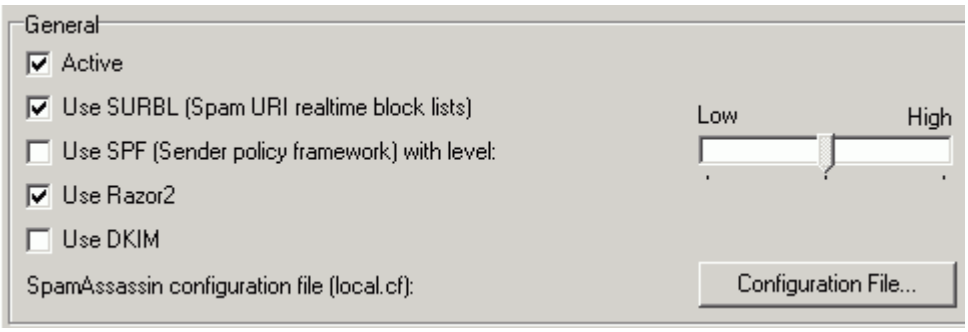
SpamAssassin is an open source project dedicated to fighting spam. Software is provided that uses a set of complex rules to ascertain whether a message is spam or genuine. The rules basically check against typical Spam templates.

These rules are constantly being updated as new spamming techniques are introduced.

Spamassassin is very good at identifying "phishing" messages that are trying to fool a User into giving out financial information.

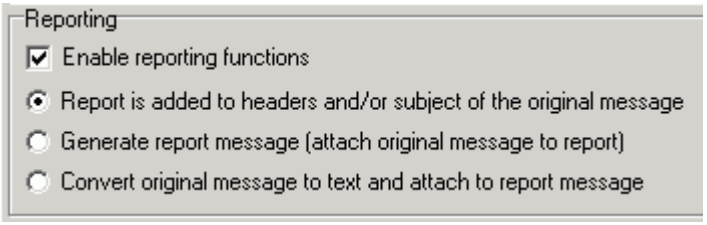
SpamAssassin uses a wide variety of local and network tests to identify spam signatures. This makes it harder for spammers to identify one aspect which they can craft their messages to work around.

VisNetic MailServer uses the SpamAssassin rules but has its own in-house written engine to process them.



Field	Description
Active	Enables the SpamAssassin filters. This is the recommended option.
Use SURBL	Check this option to enable Spam URI Realtime Blocklist technology. Rather than trying to identify Spam senders, SURBL works by identifying the presence of the URI's of Spam hosters in the message body. It is much more difficult for a spammer to change his host URI than anything else so this is a very reliable way of identifying them. SURBL is an excellent way of identifying "Phishing" sources, i.e. sources that are well known for sending out messages intended to defraud people by the capture of bank login or credit card details. You can find more information at ***http://www.surbl.org.***
Use SPF	Check this option to enable SPF (Sender Policy Framework) technology. SPF Technology uses DNS to determine whether a message reported as coming from one domain and originating from another is valid. This relies on the DNS records being published, which is not always the case, and a "soft fail" can occur, whereby the technology believes the sending host is not valid but cannot be sure. Use the slider to tell VisNetic MailServer what to do when the SPF check returns a "soft fail". Low - Adds 0.1 to the spam score Medium - Adds 0.5 to the spam score High - Adds 5.0 to the spam score - very strict! For an introduction to SPF please visit ***www.openspf.org*** http://www.openspf.org/.
Use Razor2	Check this option to have VisNetic MailServer use the Razor2 AntiSpam Technology. Razor2 is a distributed, collaborative, spam detection and filtering network. Through user contribution, Razor2 establishes a distributed and constantly updating catalogue of spam in propagation that is consulted by email clients to filter out known spam. Emails are identified by a hashed random portion of the email itself. Because the portion is random, and the position of the portion is constantly changing, it is very difficult for Spammers to create a message that will bypass Razor2. You can find out more about Razor2 at ***http://razor.sourceforge.net/*** http://razor.sourceforge.net NOTE - for Razor2 to function correctly you will need to open port 2703 on your firewall and/or router.
Use DKIM	Check this option to enable DKIM technology. See ***antispam.yahoo.com/domainkeys***

	http://antispam.yahoo.com/domainkeys for a full introduction. If an incoming email from a domain which has a DNS DomainKey record is not signed, the total "spam" score is increased. If an incoming email is not signed at all, the score is also increased (but less than in the first case).
Configuration file	Press this button to open the SpamAssassin configuration file. Please do not change any option within this file unless you are sure you know what you are doing.



Field	Description
Enable reporting functions	Check this option if you wish to enable SpamAssassin Reporting. Choose one of the three options for how you want reporting to function.
Report is added to headers and/or subject of the original message	The message will be received with modified headers. NOTE - this is the recommended option
Generate report message (attach original message to report)	A SpamAssassin report message will be received, with the original message attached.
Convert original message to text and attach to report message	A SpamAssassin report message will be received, with the original message attached as a text file.

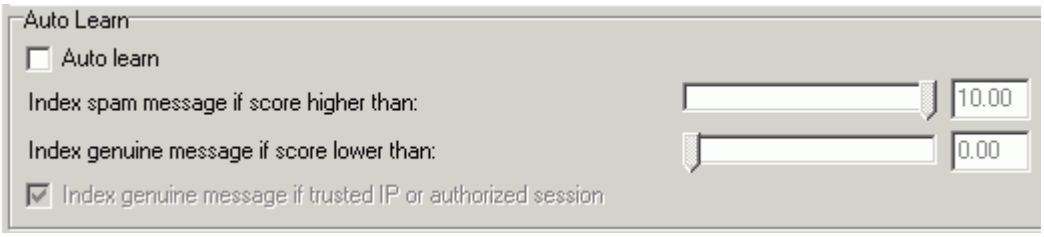
AS SpamAssassin - RBL

Field	Description
Active	Enables the use of RBL servers.
RBL Server list	Check the box against each RBL server you want to use. An RBL contains a list of IP addresses whose owners refuse to stop the proliferation of Spam from their servers. The RBL usually lists ISPs whose customers are responsible for Spam or email servers that are hijacked by spammers to send Spam. NOTE - extended RBL codes are supported, see ***www.us.sorbs.net/using.shtml*** http://www.us.sorbs.net/using.shtml for further information. If you use dnsbl.sorbs.net as your RBL it will return a code that signifies which blacklist(s) contained an entry. For example 127.0.0.3 is returned for an open SOCKS Server 127.0.0.5 is returned for an Open SMTP Relay Server

AS Bayesian

Bayesian Filters are a statistical approach to identifying spam. A database of words, and their frequency of occurrence in both spam and ham messages, is built up and used to give a probability that a word contained in a message identifies it as spam.

Field	Description
Active	Enables the Bayesian filters. It is recommended that this option is enabled.
Compact the Bayesian Database	By pressing this button, you will remove words that occur at a low frequency. These words are mostly random words that you usually see included in Spam e-mail. By compacting your database, the accuracy of the Bayesian filter will increase because these low frequency words have been removed. Only the "User Reference Base" is compacted by this button.



Field	Description
Auto learn	Check this option to enables VisNetic MailServer's Bayesian Auto Learn function. Messages with spam scores in the range you specify will automatically be indexed to the User Reference Base.
Index spam message if score higher than	Specify a value here by moving the slider Any messages assigned a score equal to or higher than this value will be indexed as a spam message.
Index genuine message if score lower than	Specify a value here by moving the slider. Any messages assigned a spam score equal to or lower than this value will be indexed as a genuine message.

Index genuine message if trusted IP or authorized session	Check this option to have messages indexed as genuine if it comes from a trusted IP address or from an authorized session (i.e. outgoing sessions that are SMTP authorized, POP before SMTP authorized, or from a trusted IP)

Field	Description
Stop words	Contains the words that will be ignored during the Spam Reference Base update (indexing process). We highly recommend that you propagate this with words that are often used in your own internal communications, such as company name, products, services etc.

Bayesian Filters - A basic explanation

Bayesian Filters, as implemented within VisNetic MailServer, use two reference databases to decide the probability that a message is spam:

The Reference Base, which is built and supplied by us using real-world messages in a real-world mail server. Updates are supplied through the AntiSpam update function.

The User Reference Base, which is built by VisNetic MailServer using the Auto Learn and/or Learn Rules functions, and uses actual messages passing through the Server, and consequently becomes much more specific to the individual installation.

User Reference Base information overrides Reference Base information.

Bayesian filters are based on the Bayesian probability theory,

The basic Bayesian theory says that the probability something will happen is the same as the probability that it has happened in the past. For them to work correctly a good selection of both spam and real (ham) messages should be analyzed.

Its implementation within VisNetic MailServer is as follows:

Take the Probability that a spam message contains a certain word

Multiply by the probability that any email is spam

Divide by the probability that a ham message contains the certain word

Gives you the probability that this message is spam.

Example

Assume:

We have received and analyzed 100,000 messages in total.

80,000 messages are spam.

48,000 spam messages contain the word viagra.

400 ham messages contain the word viagra.

Then:

The probability that spam contains viagra = 48,000 / 80,000 = 0.6

The probability that a message is spam = 80,000 / 100,000 = 0.8

The probability that any message contains viagra is (48,000 + 400) / 100,000 = 0.484

So Bayesian theory says the probability that a message containing viagra is spam = 0.6 * 0.8 / 0.484 = 0.991

Meaning a message containing viagra has a 99.1% chance of being Spam

We recommend an initial Auto Learn period of about two weeks, and a Compact and re-learn every 3-4 months at least. This will allow the User Reference Base to follow any changes in company message content (for example, the company start selling mortgages)

The User Reference Base can hold a maximum of 100,000 words. You can see how many words are actually stored in the ***General*** (see "AS General - General" on page 4) tab.

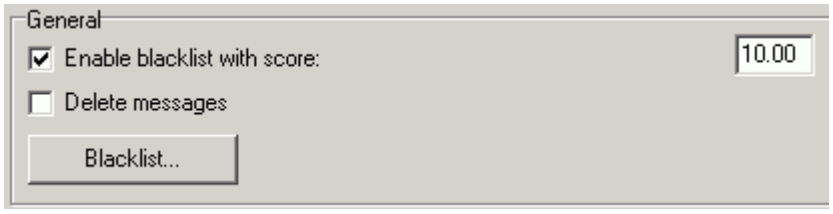
Once the limit is reached you should Compact the database (which removes lower frequency, less important, words) and enable the Auto Learn feature again for a time.

The Reference Base is contained within file <InstallDirectory>/spam/spam.db

The User Reference Base is contained within file <InstallDirectory>/spam/spam.usr

AS - Black & White Lists

AS - Blacklist



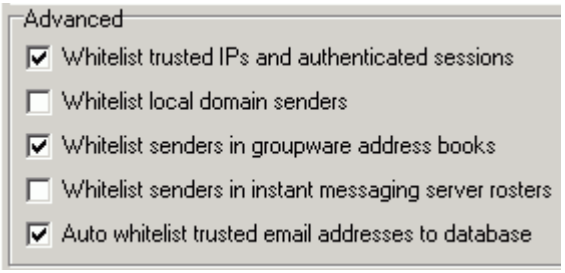
Field	Description
Enable blacklist with score	Check this option to enable Blacklist processing to modify the spam score of a message. Enter a value to modify the score by.
Delete messages	Check this box to have messages that achieve the spam score given deleted immediately.
Blacklist	Press this button to jump to the Spam Blacklist Queue.

The Blacklist Keywords section allows you to define a list of words that, if found within a message, will cause the message to have it's spam score increased.

Field	Description
Add	Press this button to add a word to the list.
Edit	Press this button to modify the selected word.
Delete	Press this button to remove a word from the list

AS - WhiteList

Field	Description
Enable Whitelist	Check this button to Enable AntiSpam Whitelist processing.
Whitelist mode	Choose from one of the following: **User** The email address is added to the whitelist of the recipient. This mode is best for ISP's whose customer base within a domain are unrelated. **Domain** The email address is added to the whitelist of the Recipient's Domain. This mode is best for ISP's who host multiple "company" domains, where all domain Users are related somehow. **System** The email address is added to the whitelist for the whole VisNetic MailServer installation. This mode is best for a Company installation of VisNetic MailServer.
Whitelist	Press this button to switch to the Spam Queues Node, with the Whitelist selected.



Field	Description
Whitelist trusted	Check this option to automatically add IP addresses in "trusted"

IPs and authenticated sessions	lists to the whitelist. Also adds authenticated session items to the whitelist.
Whitelist Local domain senders	Check this option to have senders from local domains added to the whitelist.
Whitelist senders in Groupware address books	Check this option and VisNetic MailServer will automatically add addresses within Groupware Address Books to the Whitelist
Whitelist senders in instant messaging server rosters	Check this option and VisNetic MailServer will automatically add addresses from any IM rosters to the Whitelist
Auto Whitelist	Check this option to have trusted email addresses added to the whitelist database.
Auto whitelist trusted email addresses to database	Check this option to have all trusted addresses added to the Whitelist Database.

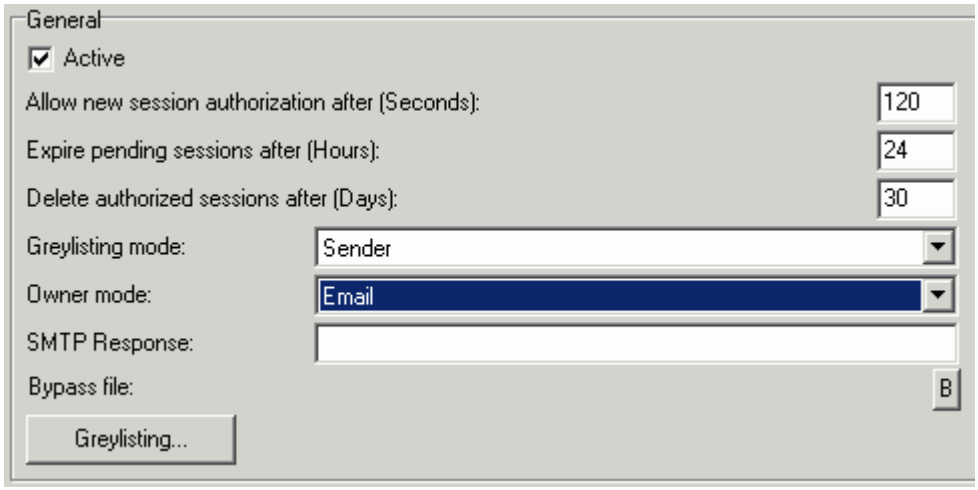
The Whitelist Keywords section allows you to define a list of words/phrases that, if found within a message, will cause the message to be bypassed by AntiSpam processing.

Field	**Description**
Add	Press this button to add a word/phrase to the list.
Edit	Press this button to modify the selected word.
Delete	Press this button to remove a word from the list

AS - Greylisting

Most Spammer's servers will try to deliver a message to the receiving server and give up if they don't get a quick response. A "real" server will retry the session after a period of time.

Greylisting allows you to reject an incoming session for a specified period of time. This will deter many spam servers from sending their messages.



NOTE - that for Greylisting these local bypasses are important:

Bypass trusted IPs,

Exclude outgoing messages from spam scanning,

Local-Local bypass filter.

The Greylisting bypass file (greylist.dat)

If these are not applied, the users will get a temporary error 4.5.1 in their mail clients and will be allowed to send the message after x seconds.

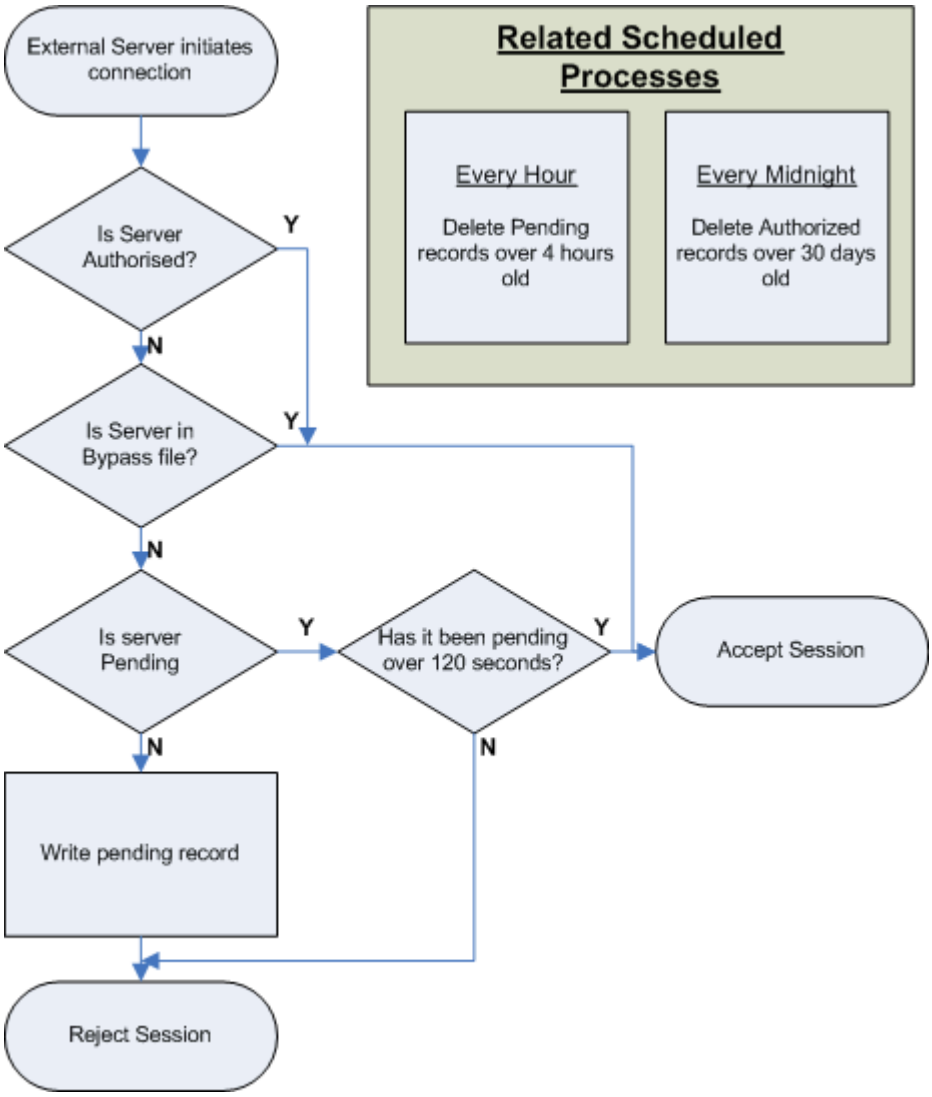
Field	Description
Active	Check this option to enable Greylisting.
Allow new authorization after (Seconds)	Specify the amount of time that incoming connections should be rejected. Any retries within this time period will be rejected.
Expire pending sessions after (Hours)	Specify the amount of time after which any "pending" IP addresses are expired within the database. "Pending" addresses are addresses which have tried to connect and been rejected by Greylisting.
Delete authorized sessions after (Days)	Specify the number of days that an authorized IP address is held in the database. A value of 0 means authorized IP addresses will never be deleted. "Authorized" addresses are addresses that were rejected by

	Greylisting, but then accepted at a later retry from the address.
Greylisting mode	Select the data that should be stored in the Greylisting database. There are four possible modes: ▪ **Sender** - The e-mail address of the person sending the e-mail. ▪ **IP** - The IP address of the machine sending the e-mail. ▪ **Sender&IP** - Both of the above. ▪ **IP+HELO/EHLO -** IP address of the machine sending the e-mail and hostname sent in the HELO/EHLO command at the beginning of the SMTP session. NOTE - that the recommended mode is **Sender**. Multi-IP systems, such as gmail, may retry the connection from a different IP address, and this would in turn be greylisted.
Owner mode	Choose from two options: **Email** Select this option to have a greylist associated to individual email accounts. Once a message comes out of greylisting it is only accepted for that specific account. **Domain** Select this option to have the greylist entry associated to the domain. So once a message passes greylisting it is accepted for the whole domain.
SMTP Response	If you wish, you can specify a custom SMTP response to be used when a connection is rejected by Greylisting. If left blank, the default SMTP response message is returned.
Bypass file (greylist.dat)	Press the B button to edit a Greylisting Bypass file, where you can specify Users, domains and IP address ranges that will not be Greylisted. Examples are given within the file.
Greylisting	Press this button to jump to the Spam Greylist Queue

Greylisting Flowchart

The Following Flowchart is designed to give you an idea of how Greylisting works.

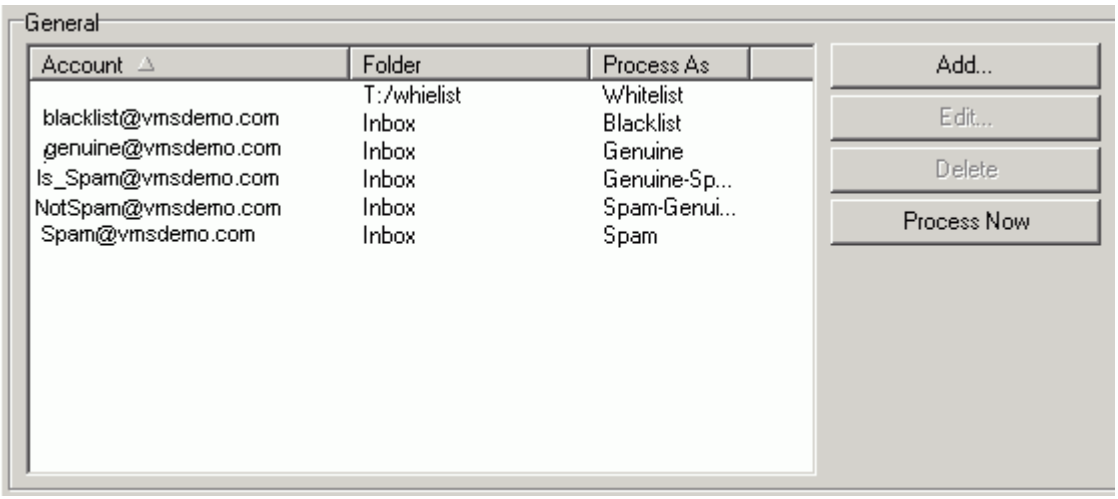
It is not an accurate representation of the code, just a visual guide to the philosophy.



AS - Learning Rules

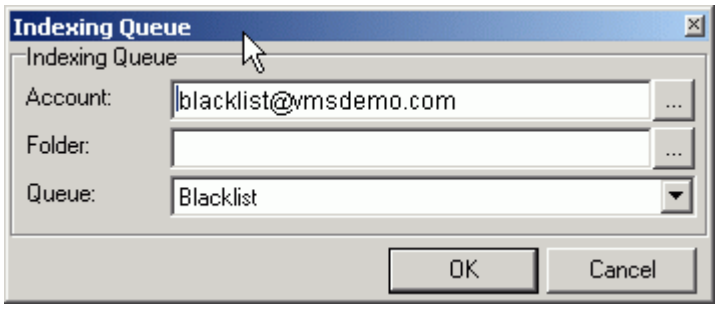
With Spammer's techniques evolving all the time there are occasions when a message will be incorrectly identified as genuine and, more rarely, incorrectly identified as spam.

The Learn Rules section allow you to let your users address these situations automatically, either by have an incorrectly identified message indexed, or by adding the sender of the message to the Blacklist or Whitelist.



Queues can be either a mailbox folder identified by it's account name, or any IMAP folder that copies of messages are copied to.

The **Add** and **Edit** Buttons are used to create or modify queue definitions, the Learn Rule dialog is opened:



Field	Description
Account	If this queue is to based on a mailbox folder enter the account here. The '...' button will open the standard Select Item dialog.
Folder	If this queue is to be based on an IMAP folder enter the folder name here. The '...' button will open a standard dialog allowing you to navigate to the folder required.
Queue	Select the type of Queue this is from the dropdown box. The following queue types are supported.

	Spam - This queue contains messages to index as Spam. **Genuine** - This queue contains messages to index as genuine. **Blacklist** - This queue contains messages whose Senders should be Blacklisted. **Whitelist** - This queue contains messages whose senders should be Whitelisted. **Spam -> Genuine** - This queue contains genuine messages that were incorrectly identified as Spam. **Genuine -> Spam** - This queue contains spam messages that were incorrectly identified as Genuine. NOTE - For Blacklisting to work correctly it must be enabled (See ***Trust - Black & White*** (see "AS - WhiteList" on page 31)). It is also valid to have multiple queues for each type.

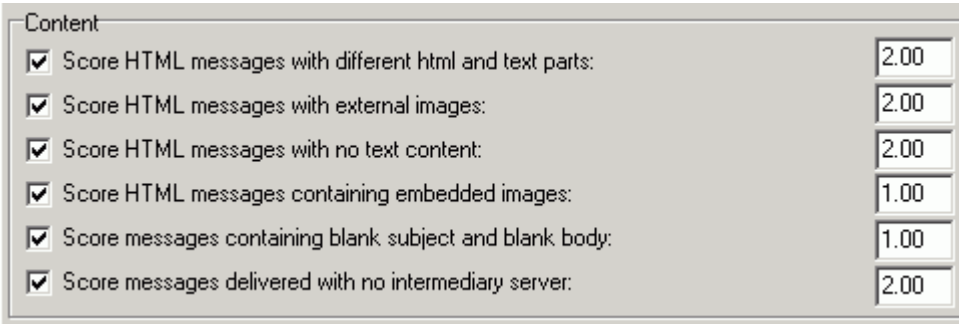
It is recommended that you use shared IMAP folders for these queues. This will allow your users to make them visible in Outlook and then they can copy any messages that need to indexed directly into them from their client.

AS - Miscellaneous

The AntiSpam Technologies node allows you to choose which AntiSpam technologies to use, such as RBL, Razor2, Reporting, Bayesian Fiters, Message Content checks, etc.

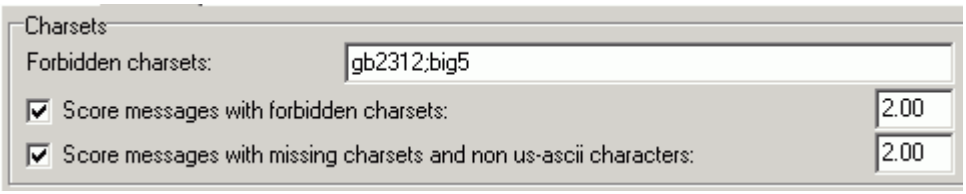
Miscellaneous - Content

The Content Filter selection has been developed to catch the most common spam messages, which are usually incorrectly formatted, or "blasted" at your server to multiple recipients, or the content structure is simply not typical of a regular messages created by regular email clients.



Fields	Description
NOTE	Check an option and enter a value. The value will be added to the spam score if the test evaluates as true.
Score HTML messages with different html and text parts	If a message contains HTML and plain-text parts then they should match exactly. Many spam emails have both parts, but they do not match. Check this option to have VisNetic MailServer increase the spam score of such messages. NOTE - some email clients do not generate the plain-text part correctly, so this option should be used with care, especially if you are checking outgoing messages.
Score HTML messages with external images	It is unusual for a normal message to contain a link to an external image.
Score HTML messages with no text content	HTML messages should have a text part.
Score HTML messages containing embedded images	Embedded images are not common in normal messages.
Score messages containing blank subject and blank body	Messages should have at least a subject or some content.
Score messages delivered with no intermediary server	Regular messages tend to be delivered via an intermediary server (e.g. their ISP's server or a corporate server)

Miscellaneous - Charsets

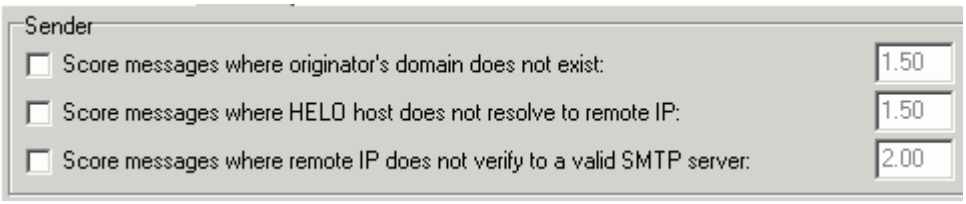


Field	Description
Forbidden charsets	Specify a list of charsets that you consider likely to be spam.
Score messages with forbidden charsets	Check this option to have VisNetic MailServer increase the spam score of messages containing any charsets listed. The spam score is increased by the value you specify. A table of the more common charsets is given below.
Score messages with missing charsets and non us-ascii characters.	Check this option to have VisNetic MailServer increase the spam score of messages with missing charsets or containing non us-ascii characters.

Important Note

If you send messages through VisNetic MailServer from a website HTML form you should be aware that these messages will often contain high-value characters (for example, in some foreign names). Always try to construct the message with a correctly defined charset and consider whitelisting the IP address of the website.

Miscellaneous - Senders



Field	Description
Score messages where sender's domain does not exist	Check this option to have VisNetic MailServer check if the sender's domain exists. If it does not then VisNetic MailServer will increase the spam score by the value specified.
Score messages where HELO host does not resolve to remote IP	Check this option and VisNetic MailServer will check that the Hostname given in the HELO command resolves to the same IP address that the message is being delivered from. If it does not then VisNetic MailServer will increase the spam score by the value specified.
Score message where remote IP does not verify to a valid SMTP server	Check this option to have VisNetic MailServer verify that the IP address that is delivering the message is a valid SMTP server. If it does not then VisNetic MailServer will increase the spam score by the value specified. WARNING - This is achieved by attempting to connect to port 25 (the standard SMTP port) of the domain this message is coming from. A response to this could take up to 5 seconds and could therefore seriously slow down your server.

AntiSpam Templates

At the bottom of the all AntiSpam screens you will find the Reset button.

This allows you to select an AntiSpam Template of either High, Medium or Low settings from the drop-down box and press the Reset to apply that level.

AntiSpam Level	Description
Low	Very lax level of AntiSpam. Greylisting not used. Quarantine not used. High Spam classification scores. Sender technology not used. SpamAssassin SPF, Razor2 and DomainKeys not used. This is the least resource-hungry template but will not catch as much Spam as

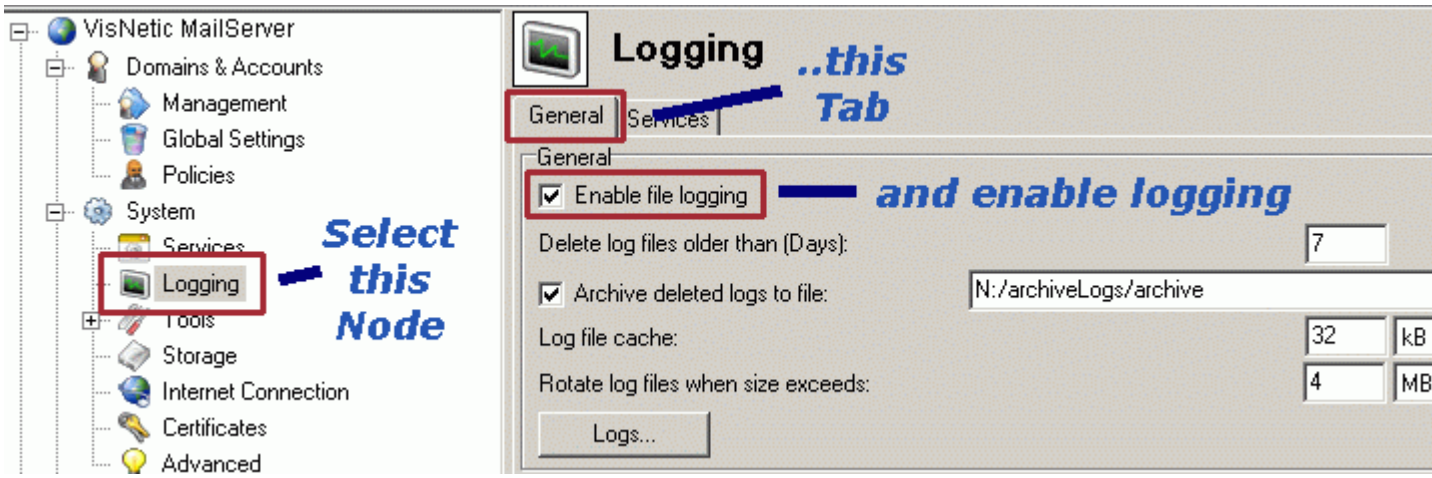
	the other settings
Medium	Greylisting enabled. Quarantine enabled. Spam Classification scores lowered. Sender Technology used. SPF technology enabled. The recommended option. Uses more Server resources for the extra processing but with a much better chance of correctly identifying Spam.
High	Very strict AntiSpam settings. All available technologies are used. Spam classification scores lowered. Spam score adjustment values are set higher than in other templates. The most resource-hungry template, with the best chance of correctly identifying Spam but with an increased chance of false positives.

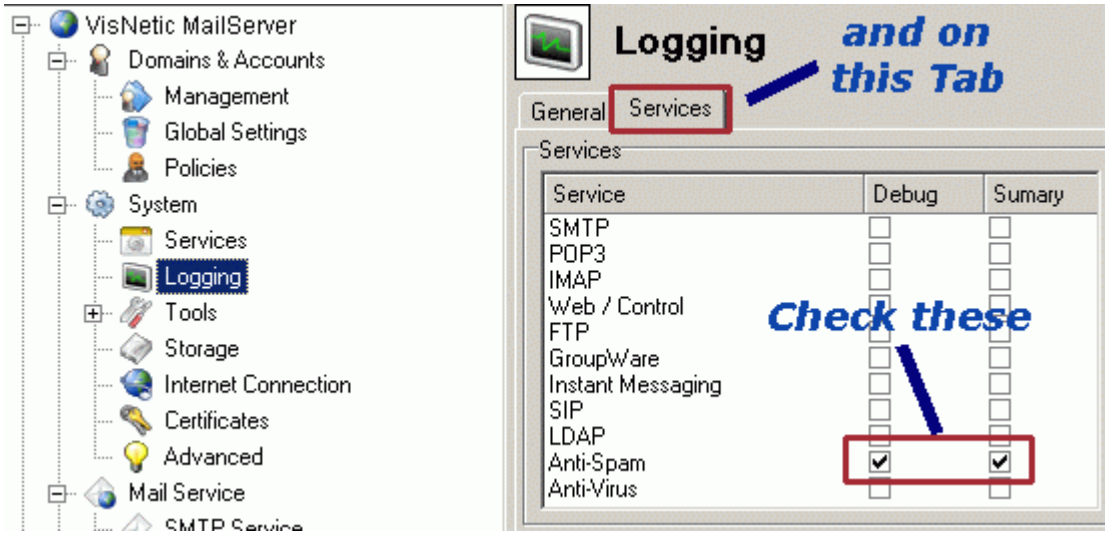
CHAPTER 2

AntiSpam - Logging

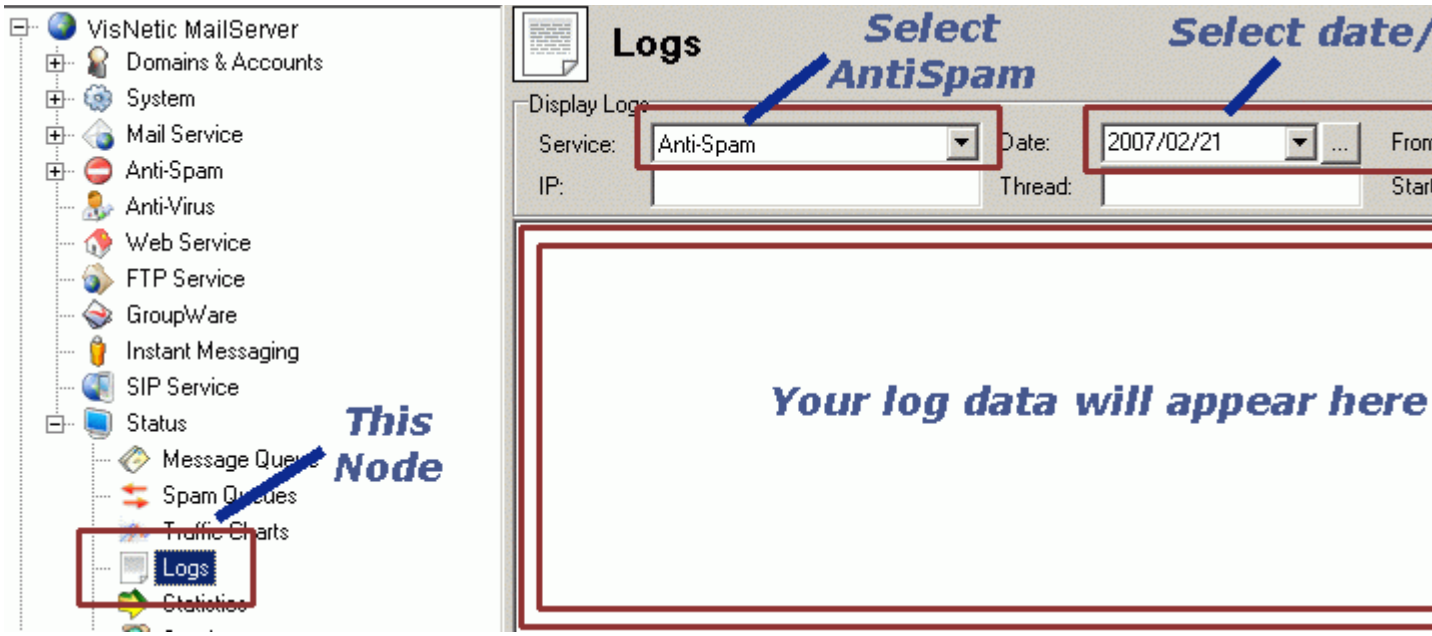
If you have set the AntiSpam logging options then you can browse the AntiSpam logs to see what happened to a message, why it was marked as Spam, or wasn't marked as Spam.

Logging is enabled in the System->Logging Node of the main Console. You should enable logging itself and enable Summary and Debug logging for AntiSpam.





Now you have logging enabled and you can view your AntiSpam logs in the Status->Logs Node.



In the screenshot above there is no actual log information included but we will now look at a few example lines of a log and discuss what they mean.

Example 1

```
127.0.0.1  [0BD4] 21:04:22 ZWY87507 '<tech@at.domain.com>'
'<ErikViking@hotmail.com>' score 4,39 reason [SpamAssassin=4,39,Body=R,Sender]
action NONE
```

In this manual the line is split but within the log screen it would be continuous on on line. The separate fields are described in the table below:

Field	Description
127.0.0.1	This is the IP address that VisNetic MailServer is connected to to send/receive this message.
[0BD4]	
21:04:22	The timestamp for this log entry.
ZWY87507	
'<tech@at.domain.com>'	The User this message is intended for.
'<ErikViking@hotmail.com>'	The User who reportedly sent this message.
Score 4,39	The Spam Score this message achieved.

reason [SpamAssassin=4,39, Body=R,Sender]	SpamAssassin=4,39 - A score from Spamassassin of 4.39. Body=R - message had no subject and no body content (see ***Reason Codes*** (see "AntiSpam - Reason Codes" on page 46)). Sender
action NONE	This is the action taken based on the spam score - in this case NONE, meaning the message was delivered as intended.

Example 2

127.0.0.1 [0BD4] 21:05:47 ZWZ96937 '<John@demoaccount.freeserve.co.uk>' '<tech@vmsdemo.com>' score 10,00 reason [SpamAssassin=10,00,Body=NI,Sender] action QUARANTINE

Field	Description
127.0.0.1	This is the IP address that VisNetic MailServer is connected to to send/receive this message.
[0BD4]	
21:05:47	The timestamp for this log entry.
ZWZ96937	
'<John@demoaccount.freeserve.co.uk>'	The User this message is intended for.
'<tech@vmsdemo.com>'	The User who reportedly sent this message.
score 10,00	The Spam Score this message achieved.
reason [SpamAssassin=10,00,Body=NI,Sender]	SpamAssassin=10.00 - The Score from SpamAssassin. Body=NI - message had no text part and an embedded image (see ***Reason Codes*** (see "AntiSpam - Reason Codes" on page 46)).
action QUARANTINE	This message has been put to the Quarantine queue for manual intervention.

Example 3

127.0.0.1 [0BD4] 21:18:55 ZWM21954 '<Brian@Mylifedemo.com>' '<support@vmsdemo.com>' score 2,09 reason [SpamAssassin=2,09,Bypass=W] action NONE

Field	Description
127.0.0.1	This is the IP address that VisNetic MailServer is connected to to send/receive this message.
[0BD4]	
21:18:55	The timestamp for this log entry.

ZWM21954	
'<Brian@Mylifedemo.com>'	The User this message is intended for.
'<support@vmsdemo.com>'	The User who reportedly sent this message.
Score 2,09	The Spam Score this message achieved.
reason [SpamAssassin=2,09,Bypass=W]	SpamAssassin=2,09 - The Score from SpamAssassin. Bypass=W - this sender is on a WhiteList and the message has been passed on.
action NONE	This message has been delivered to the recipient's mailbox.

CHAPTER 3

AntiSpam - Reason Codes

The AntiSpam engine issues reason codes when it scores a message as spam, and when it bypasses AntiSpam processing for a message.

There are three logical sets of codes - Spam Reasons, Charset Reasons and Bypass Reasons, which are described in the tables below:

Spam Reasons

Code Issued	Reason
P	HTML and Text parts don't match
E	External images in content
N	No Text part
I	Embedded image in content
B	No Body and No Subject
R	No intermediary Server
S	Message contains a script
F	Spam scored via a Filter
K	Spam scored via Blacklist Keyword

Charset Reasons

Code Issued	Reason
F	Charset not allowed
M	Missing Charset information

Bypass Reasons

Code Issued	Reason
L	License is invalid
W	Sender is on Whitelist
T	Sender is Trusted
O	Message is Outgoing
S	Message exceeds size threshold for checking
B	Sender information is in Bypass file

A	Message is from a Non-User account (e.g. mailing list)
M	Spam processing was bypassed because the Access Mode was set for specific accounts, and this account is not one of them.
G	Sender exists in GroupWare address books.
K	Words found in Whitelist keywords
Q	Quarantine bypass for local domains/users

Intrusion Prevention Reasons

Reason Code	Explanation
C	Tarpitting invoked via Content Filters
I	IP blocked for exceeding connections in one minute
M	IP blocked for delivering oversized message
R	IP blocked for exceeding RSET command count
D	IP blocked for being listed on DNSBL
A	The account that this message was sent to was a "tarpit" account so the sending IP is tarpitted
P	IP block for exceeding unknown User delivery count
Y	IP blocked for Relaying
S	IP blocked for exceeding Spam score in a message
U	IP blocked Manually via Console

Index