VisNetic MailServer

Mail Service Reference

Version 9.1

Printed on 7 November, 2007

Contents

CHAPTER 1

Mail Service

The **Mail Service** Node contains four subnodes:

SMTP Service - various settings for the SMTP service

Security - comprehensive set of options for stopping unwanted use of your server.

Filters - allows you to define Content Filters, Rules Filters (Black & White lists) and External filters.

ETRN Download - allows you to define ETRN (or ATRN) collection options.

In This Chapter

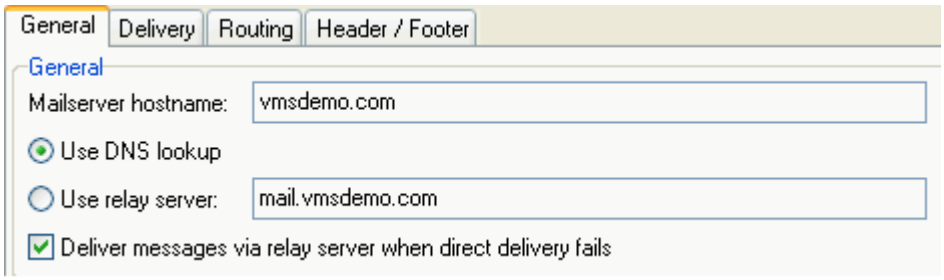
CHAPTER 2

SMTP Service

The SMTP (Simple Mail Transfer Protocol) Service is the core of VisNetic MailServer's functionality, as it is the protocol used for sending messages from one server to another.

In This Chapter

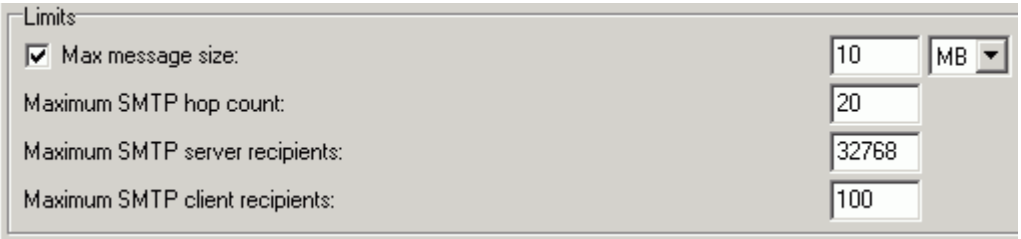
General



Field	Description
Mailserver hostname	This specifies the name of the mail server computer. This field must not be left blank as it is used when the mail server authenticates or introduces itself to another mail server. This should be the hostname of your mail server which is registered on DNS. You may also want to ensure your mail server's IP address has a PTR record registered as this is a spam-fighting requirement that some receiving mail servers require.
Use DNS lookup	Select this option if your server is going to send messages directly. When sending a message, VisNetic MailServer will query DNS servers to locate the receiving server's IP address. DNS servers can be specified in the Internet Connection node.
Use relay server	Select this option if you wish VisNetic MailServer to use a relay server to send messages.

	This is useful when your domain has no public IP address or you are on a slow dial-up connection via an ISP that allows you to use their email server to send messages.
	Connections to your ISP's mail server tend to be faster than other servers on the internet so your messages may be delivered more quickly, keeping your connection costs down.
	You should enter the hostname or IP address of the relay server.
	If your relay server requires authentication this can be achieved by using one of the following 'full URL' forms of the hostname:
	`<username>:<password>@<MyISPhostname>`
	or
	`<username%domain.com>:<password>@ <MyISPhostname>`
	The second option should be used if your username is a full email address.
	Example:
	john%doe.com:johnspassword@mail.MyISP.com
	You can specify multiple relay servers here, separated by semicolons. If VisNetic MailServer cannot connect to the first relay server, it will try to the second etc..

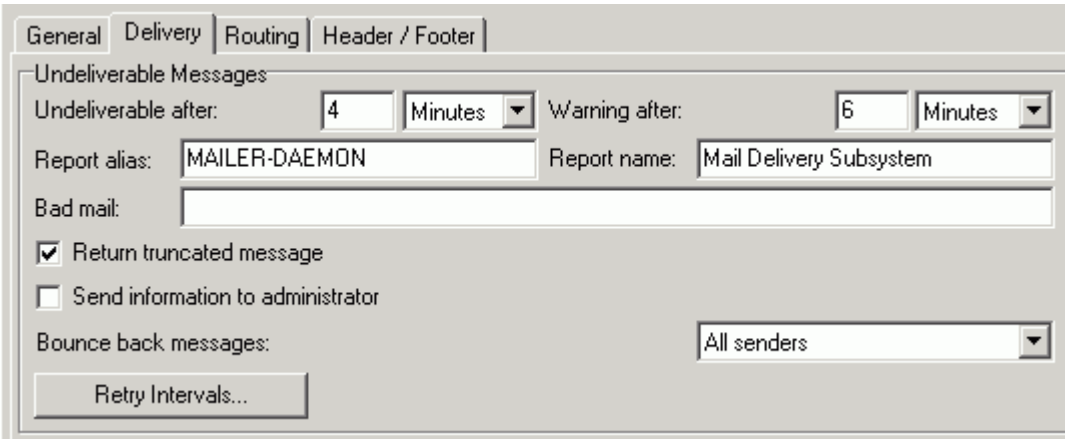
Deliver messages via relay server when direct delivery fail	Checking this option only has an effect if you have selected Use DNS lookup and you have defined a relay server (or servers) in the **Use relay server text** box, VisNetic MailServer will attempt delivery to via these server(s) if all direct delivery attempts fail. NOTE This option overrides the SMTP retry interval settings.



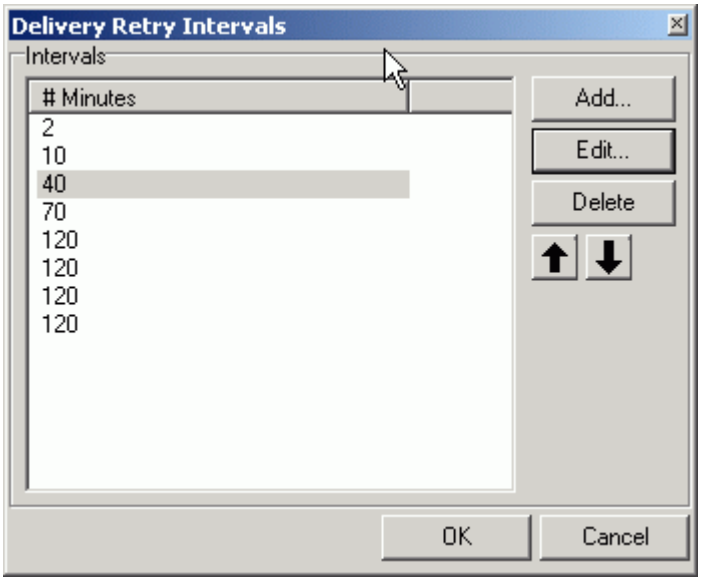
Field	Description
Max message size	Check this box and enter a value to limit the size of messages that can be sent via the mail server (in the above screenshot 10MB). If a user tries to send a message larger than the specified size it will be rejected. NOTE that this limit will be overridden by any Domain-specific limits if

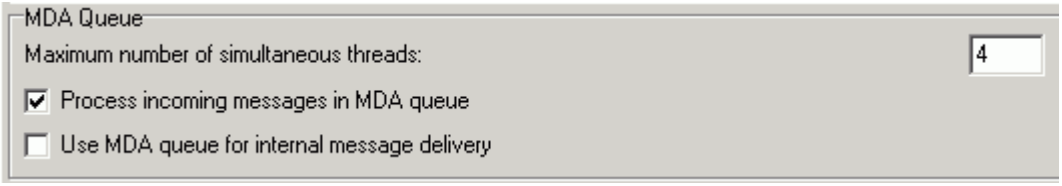
	Override global limits is checked within Global Settings - Domains.
Maximum SMTP hop count	Sometime a message can get into a 'relay loop', where it is being passed between servers trying to find a delivery point. A hop is defined as one pass of the message to a server. Specifying a value here instructs VisNetic MailServer to count the number of servers the message has been through, compare it with this value, and reject the message if the number of hops exceeds the specified value.
Maximum SMTP server recipients	Specify the maximum number of Server session recipients allowed in an outgoing message. This can be used to protect your server from overload.
Maximum SMTP client recipients	Specify the maximum number of Client session recipients allowed in an outgoing message. If the number is exceeded the message will be split into multiple sessions.

Delivery

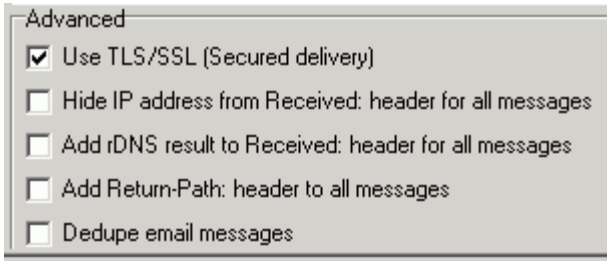


Field	Description
Undeliverable after	If VisNetic MailServer cannot contact a server to deliver a message it will queue the message and retry delivery at regular intervals. Specify a value and time unit..
Undeliverable warning after	If VisNetic MailServer cannot contact a server for the specified number of hours the sender is informed. This message is only a warning, VisNetic MailServer will continue trying to deliver the message. Specify a Value and time unit.
Report alias /	The report alias and name are used to generate the From: header in any system generated report messages (for example the undeliverable report, disk space

Report name	monitor report etc.).
Bad mail	If the sender of a message cannot be ascertained (e.g. there is no From: header) and an undeliverable message report is generated it will be sent to the recipient(s) listed here. Multiple addresses can be specified, separated by semicolons.
Return truncated message	Check this option and only message headers are returned if the message cannot be delivered.
Send information to administrator	Check this option and all undeliverable messages will be copied to the administrator.
Bounce back messages	Choose a process option for bounce back messages. **All senders** - Process bounce back messages for all senders. **Local senders only** - Process only for Local Senders. **Disabled** - do not process bounce back messages. NOTE - In MDA mode a message is accepted and then processed by other filters at a later time. If a message is then refused a bounce back is sent to the sender. If the sender's address is spoofed than an innocent recipient could get the bounce back which would be considered as spamming - because of this the recommended bounce back level in MDA mode is "local senders"
Retry Intervals	Press this button to open a dialog allowing you to specify retry intervals for failed deliveries:  Use the **Add** button to add a new retry time. Use the **Edit** and Delete buttons to modify or remove a retry time. Use the **Up** and **Down** arrows to move a retry time in the list.



Field	Description
Maximum number of simultaneous threads	Specify the maximum number of threads to use for processing incoming messages. This can help alleviate problems on high-load servers where the sending server times out, but VisNetic MailServer still processes and delivers the message. The Sending Server then tries again, and a duplicate message is received. If you enter a non-zero value here then any incoming messages are stored immediately to an incoming folder, for later processing, and the session is closed so there are no timeouts. You should only consider using this option on high-traffic servers or servers that have major AntiSpam and/or AntiVirus processing. NOTE - In MDA mode a message is accepted and then processed by other filters at a later time. If a message is then refused a bounce back is sent to the sender. If the sender's address is spoofed than an innocent recipient could get the bounce back which would be considered as spamming - because of this the recommended bounce back level in MDA mode is "local senders"
Processing incoming messages in MDA queue	Check this option to have the MDA queue used.
Use MDA queue for internal message delivery	Check this option to have all internal messages processed via the MDA queues. This means that any internal message (bounce back, server generated message, Account Forwarder message etc.) will be processed via an MDA queue and all filter, rule, AntiSpam, AntiVirus etc. processing will be performed on the message.



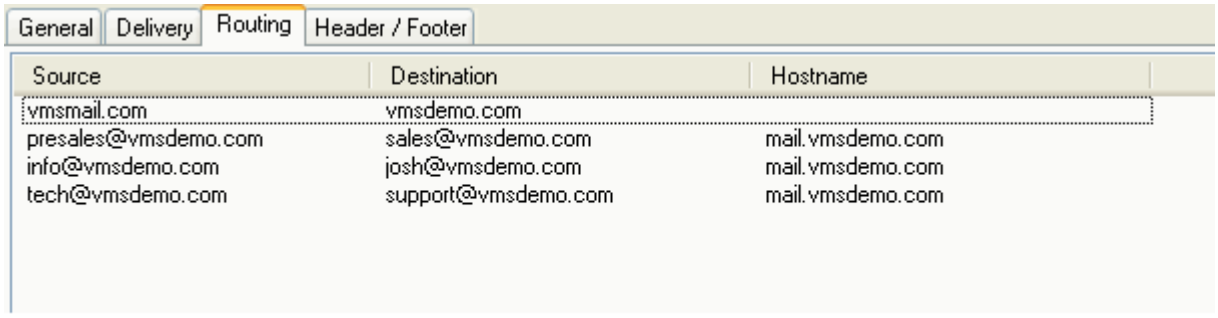
Field	Description
Use TLS/SSL	Check this box and VisNetic MailServer will connect to remote servers using TLS/SSL, if the remote server is capable of this.

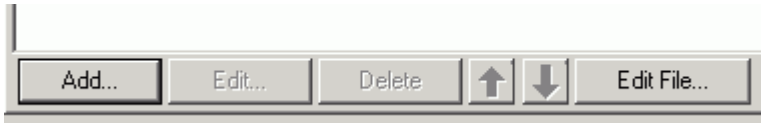
Hide IP address from Received: header for all messages	Checking this option tells VisNetic MailServer not to put the IP address in a messages Received: header. This effectively stops people from being able to work out your local network configuration.
Add rDNS result to Received: header for all messages	Check this option and a reverse DNS lookup will be performed for each incoming message and the result added to the message headers. NOTE - Using this option improves security but can severely impact performance on high-load Servers.
Dedupe email messages	If a User has multiple aliases and a message is sent to more than one of the aliases the end User will receive multiple copies. Check this option and VisNetic MailServer will check for duplicate message to the same end user and only deliver one of them.

Routing

The SMTP Routing feature allows you to redirect messages based on the recipient address.

A list of routing rules is displayed:





The **Source** column shows the original recipient.

The **Destination** column shows where the message will be redirected.

The **Hostname** column shows the hostname that messages will be forwarded through.

Press the **Delete** button to delete a selected routing rule.

Pressing the **Add** or **Edit** button will open the **Route** dialog, where you can add or modify a routing rule.

Field	Description
Source	The email address or domain which should be replaced and redirected. You can use the '...' button to select accounts, domains or groups through Select Account Dialog.
Destination	The email address or domain by which the source one is replaced and redirected. You can use the '...' button to select accounts, domains or groups through Select Account Dialog. **Syntax:** emailaddress | domain [;parameter] The parameter is 0, 1,2 or 3, with the following functions: 0 - all recipients - other filters will be processed (e.g. reject message in Content Filters) 1 - local recipients only - other filters will be processed (e.g. reject / delete message) 2 - all recipients - ignore other filters 3 - local recipients only - ignore other filters You can use VisNetic MailServer Variables in this field e.g. %%var_name%% If the destination needs authentication with a full email address you must use % instead of @ in the address: Example - username%domain:password@host
Hostname	A hostname, with an optional port, that will be used for extended routing, using the following syntax: @hostname#port:alias@domain Example: aol.com=@relay.isp.com#2525:%%Recipient_Alias%%@vmsdemo.com

	This says that all messages for ***anyone***@aol.com will be routed to relay.isp.com.

Pressing the **Edit** button will open the simple text file containing the rules. You can edit this file directly, examples are given in the editor

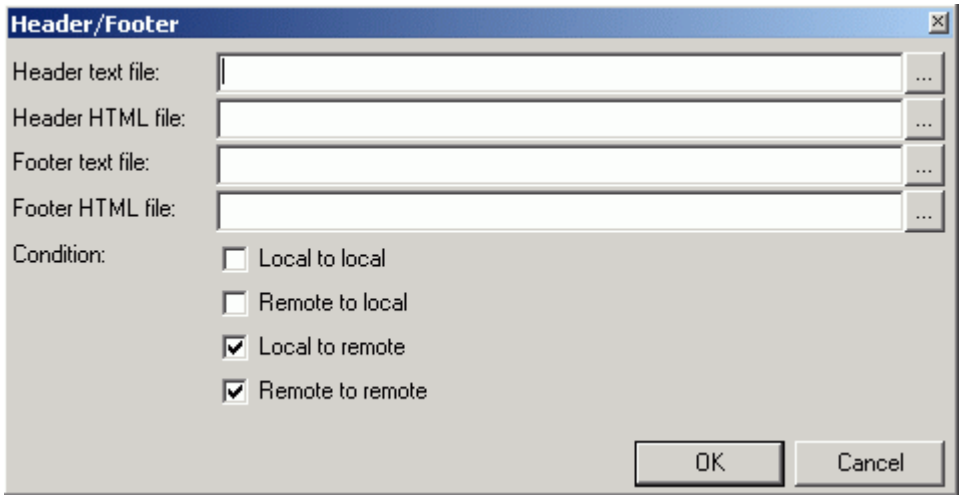
Header / Footer

VisNetic MailServer can automatically insert a header and/or footer to messages using this option.

This will affect all domains within your server. If you want to specify different headers and footers for different domains you should use the domain-based **Header/Footer** button in Domain - Options - but you must enable the facility in this panel.

Check the **Active** option to enable Header/Footer processing

Pressing the **Header / Footer** button opens the **Header/Footer** dialog:



Field	Description
Header text file	A fully qualified path to a text file which will be inserted as a header to text format

	messages.
Header HTML file	A fully qualified path to an HTML file which will be inserted as a header to HTML format messages. NOTE - that the extension of this file must be htm or html for this function to work correctly.
Footer text file	A fully qualified path to a text file which will be inserted as a footer to text format messages.
Footer HTML file	A fully qualified path to an HTML file which will be inserted as a footer to HTML format messages. NOTE - that the extension of this file must be htm or html for this function to work correctly.
Local to local	Header and Footer will be inserted in a message if the sender and recipient are local.
Remote to local	Header and Footer will be inserted in a message if the sender is remote and recipient is local.
Local to remote	Header and Footer will be inserted in a message if the sender is local and recipient is remote.
Remote to remote	Header and Footer will be inserted in a message if the sender is remote and recipient is remote.

NOTE - If you are using HTML headers or footers you should **only** use HTML found within the <BODY> tag.

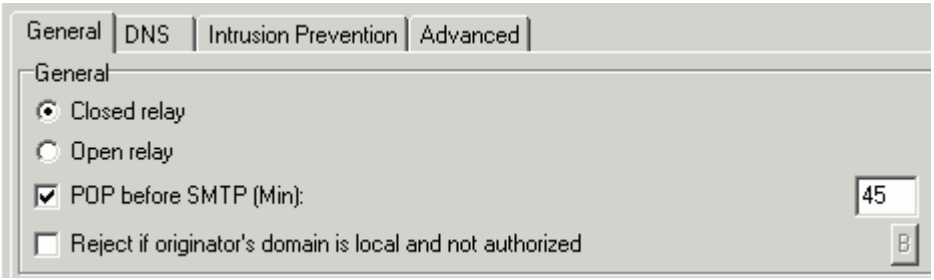
CHAPTER 3

Security

One of the more important areas of VisNetic MailServer, the SMTP Security options are designed to protect your server from unwanted access and use.

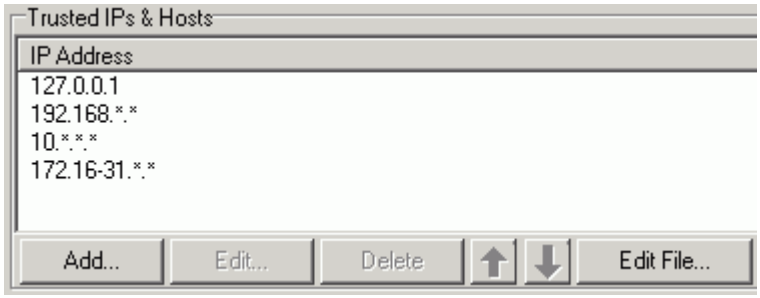
In This Chapter

General



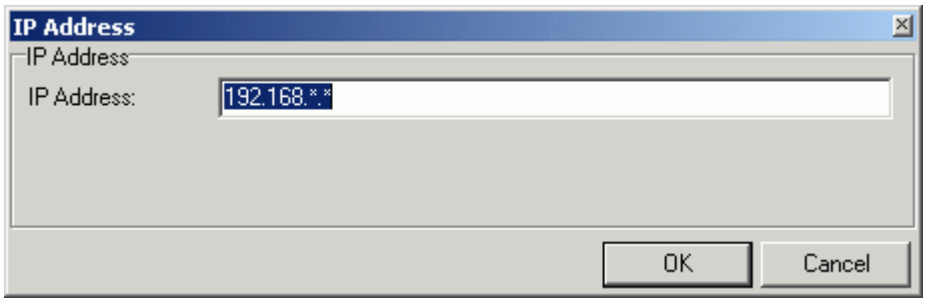
Field	Description
Relay	**Close relay** - The recommended option. Choosing this option will require users to be authenticated on your server, unless they are from a trusted Relay IP (see below). Authentication can be done via a user/password combination or by selecting POP before SMTP (see below). **Open relay** Choose Open relay if you want to allow ***anyone*** to use your SMTP server to send messages. This is not a recommended option as it leaves your server open to abuse by spammers and hackers.
POP before SMTP	Check this option and VisNetic MailServer will remember the IP address of any POP or IMAP connections (which are always authenticated) for the number of minutes specified. If an SMTP session is initiated from one of the cached IP addresses it will be allowed.
Reject if	If the sender of the message is a local user (claims to be from your local

originator's domain is local and not authorized	domain) they have to authorize themselves. Authorization can be done using the SMTP authentication, relaying from IP address or the POP before SMTP feature. This option can reject also local users if they authenticate against different SMTP server, e.g. their ISP SMTP server.



The **Trusted IPs** list show the IP address ranges you consider trustworthy. SMTP connections from these IP addresses will be allowed without authentication.

Using the **Add** or **Edit** buttons opens the **IP Address** dialog:



You can use masks, as shown above, and ranges, for example 192.168.0.1-50

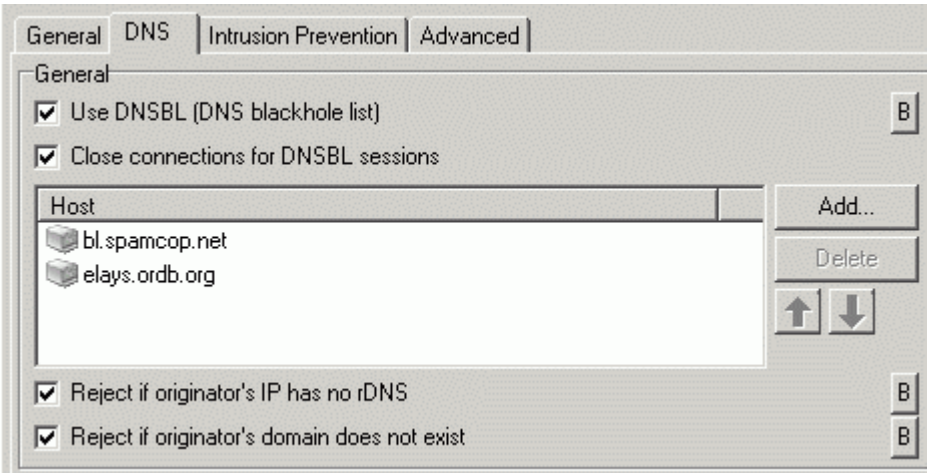
Use the **Delete** button to delete a selected IP range

Use the **arrow** buttons to move ranges up and down the list

Use the **Edit File** button to open the simple text file containing the IP ranges. Examples are given.

NOTE - that you can use Host names as well as IP addresses

DNS

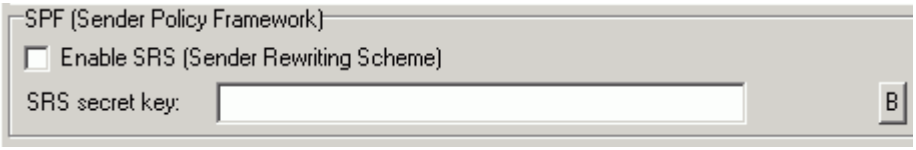


A DNSBL is basically a DNS server which only lists IP addresses of known spammers.

If you query an address against a DSNBL server and get a positive result then the address is most likely that of a known spammer.

This can be used as an AntiSpam technique.

Field	Description
Use DNSBL	Check this option to use DSNBL checking. Use the B button to specify a list of Ip addresses, Domains and email address that you will not perform the DSNBL check for (effectively a list of trusted addresses).
Close connections for DNSBL sessions	Check this option and any connections from IP addresses which are listed on the blacklist will be closed immediately.
Host List	Here you must define a list of DSNBL server(s) you wish to query. Use the Add and Delete buttons to populate and de-populate the list. You can use as many DSNBLs as you wish but you should be aware that each query will add some processing time.
Reject if sender's IP has no rDNS	Check this option to enable rDNS (reverse DNS) checking. Any connection from a server that does not have an rDNS record (PTR record) will be rejected.
Reject if originator's domain does not exist	Check this option to check for the existence of a DNS A record for an incoming message senders domain. If the senders domain has no A record the message is rejected.



Field	Description
Enable SRS (Sender Rewriting Scheme)	Activates the SRS technology fixing the SPF forwarding mail issue, by forcing the agent to change the "mail from" address
SRS secret key	The secret key is any arbitrary string you can make up - it is your own passphrase. The secret key will be used for ciphering the data (for hash creation). This field must not be left blank.
The 'B' button	Use this button to open and edit the SRS bypass file srsbypass.dat. See the example in the bypass file for the correct syntax.

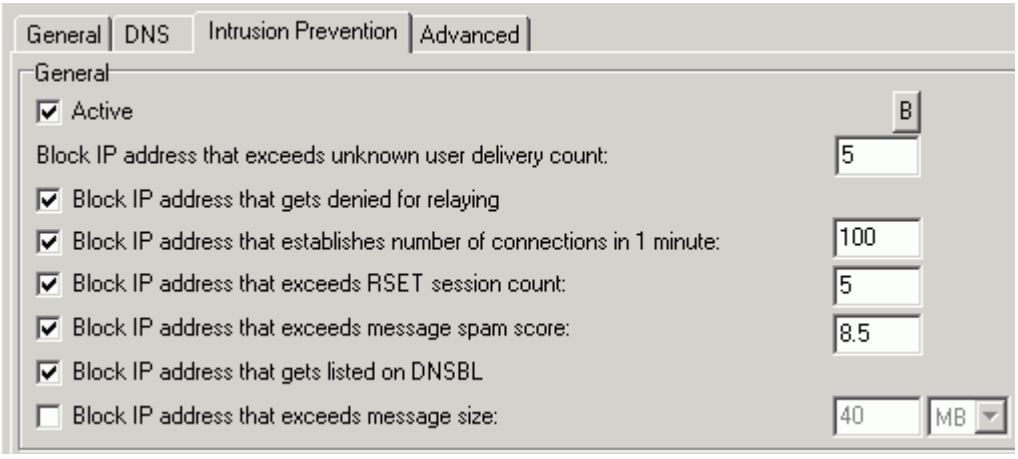
Intrusion Prevention

Intrusion Prevention enables you to block any IP addresses performing suspicious activities.

When activated the Server will monitor all unsuccessful remote server attempts to deliver email to unknown recipients. If the number of attempts from one server exceeds the threshold setting then that IP address will be blocked (denied access) for a specified amount of time.

This option serves as protection against spammers who are trying to spam your mail server accounts based on email address dictionary attacks.

There is an option to create a "bypass list" of IP addresses which will never be blocked.



Field	Description
Active	Enables the feature.
The "B' for Bypass button	Click here to edit a bypass list of IP addresses. These addresses will never be blocked.
Block IP address that exceeds unknown user delivery count	Check this option and specify a value. In the above screenshot an address will be blocked after it attempts to deliver 5 messages to unknown users.
Block IP address that gets denied for relaying	Check this option to automatically block addresses that attempt to relay through VisNetic MailServer.
Block IP address that establishes number of connections in one minute	Check this option and specify a value. In the above example an IP address that establishes 100 connections in one minute will be automatically blocked.
Block IP address that exceeds RSET session count	Check this option and specify a value. In the above example any connection that issues 5 RSET commands in one session will be blocked.
Block IP address that exceeds message spam score	Check this option and specify a value. In the above example any IP address that delivers a message with a spam score higher than 8.5 will be automatically blocked
Block IP address that gets listed on DNSBL	Check this option and any connection that is refused because it is on a DNSBL will also be blocked.
Block IP address that exceeds message size	Check this option to have the IP address blocked for any connection that attempts to deliver a message greater than the specified size. Specify a value and choose Kilobytes, Megabytes or Gigabytes from the drop-down box.

NOTE - this check differs from the standard SMTP "maximum message size" check in that the connection is closed ***as soon as the size threshold is reached*** and the IP address blocked. This is useful for stopping potential bandwidth abusers who send large messages.

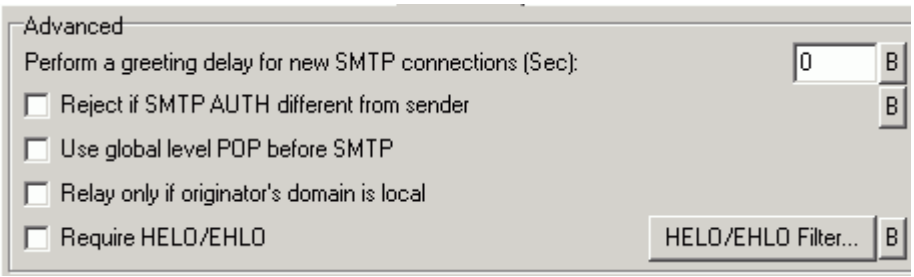
For example:

With the settings shown above, someone sends a 1GB message to one of your users. As soon as the system has received the first 100MB it will close the connection and block the IP address for 4 hours. The sending SMTP server may try to re-send the message but it will be denied access until the 4 hours is up, at which point the first 100MB will be accepted then the block happens again. Eventually the sending SMTP server will give up trying to send the message.

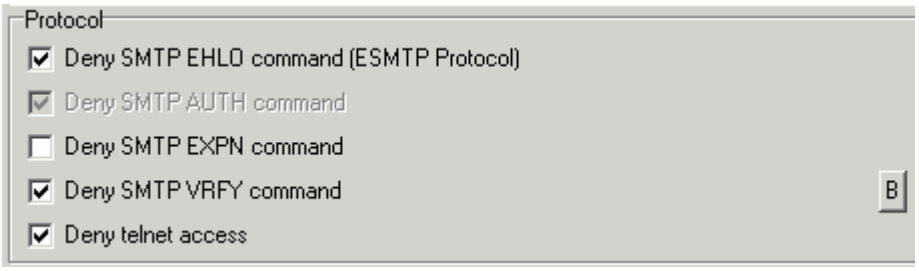
The effect on your server is that instead of having a high bandwidth usage for a 1GB duration it will have high bandwidth usage every 4 hours for a 100MB duration until the sending server gives up, freeing your bandwidth for other send/receive operations in the meantime.

Field	Description
Amount of time for IP address to be blocked	Specify here how many minutes an IP address should be blocked for
Refuse blocked IP address	Checking this option will store the blocked IP in a database and refuse any further connection attempts. Be aware that this could cause large growth of the database with performance degradation. The unchecked state lets you use the blocking feature and the IP DB is not used.
Close blocked connection	If checked then any IP address that is blocked will also have any open connection(s) closed immediately.
Cross session processing	Check this option to have VisNetic MailServer collect Intrusion Prevention stats across multiple sessions (connections) from the same server. Stats are accumulated over the time selected in "Amount of time for IP address to be blocked". In the above example connections from HostA would be collected and acted upon for 30 minutes.
Blocked IPs	Press this button to jump to the Intrusion Prevention queue, where you can manage your Blocked IP addresses.

Advanced

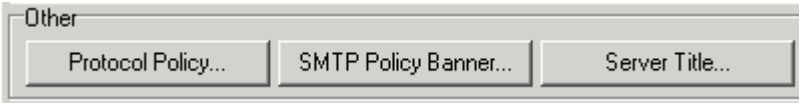


Field	Description
Perform a greeting delay for new SMTP connection	Specify a non-zero value here and VisNetic MailServer will wait that many seconds before responding to an incoming SMTP session. Most spammers systems will time out very quickly as they want to get as much mail delivered as possible within a short time. Genuine connections will wait.
Reject if SMTP AUTH is different from sender	Check this option to reject any connections where the Sender information differs from the information used in the SMTP AUTH command.
Use global level POP before SMTP	Check this option to allow POP accesses to authorize SMTP accesses from the same IP address
Relay only if originator's domain is local	Check this option to only allow relaying from local domains.
Require HELO/EHLO	Check this option to deny any connections that do not use the HELO or EHLO commands when they connect.



Field	Description
Deny SMTP EHLO command (ESMTP Protocol)	This option prevents servers from connecting with the ESMTP service. If a remote server issues the EHLO command VisNetic MailServer will reply with an error code. Outgoing SMTP connections will use the standard SMTP commands. This can be useful where remote servers and routers/proxies have implementation bugs. This is not a recommended option.
Deny SMTP AUTH command	If checked, VisNetic MailServer will not accept the SMTP AUTH command.
Deny SMTP EXPN command	The EXPN command is used to display the contents (addresses) within a mailing list.

	Check this option to instruct VisNetic MailServer not to accept the request.
Deny SMTP VRFY command	The VRFY command is used to verify the existence of an email address on a server. This can be used by spammers to send spam to real addresses. Check this option and VisNetic MailServer will not respond to the command. NOTE that you should not check this option if you are using a **Distributed Domain** with VRFY querying.
Deny telnet access	This prevents anyone from using telnet to access the ports used by VisNetic MailServer.



Field	Description
Protocol Policy	Press this button to specify Protocol Policy settings. Examples are given within the file.
SMTP Policy Banner	Press this button to specify banner text that will be presented to any client connect to the server to send messages. Examples are given within the file.
Server Title	By default, VisNetic MailServer will identify itself to a connecting server. Some hackers can use this information to exploit your server. Press this button to change the identification text so no-one can identify the server software you are running. An example is given within the file.

CHAPTER 4

Filters

These filters can help you catch spam and viruses.

If you want to filter messages using advanced rules and make adjustments to messages we recommend using ***Content Filters*** (on page 19).

If you just want to restrict message acceptance using keywords it is better to use Black & White Lists.

Additionally, you can design your own filters and create your own filters in any programming language and then call such filters in ***External Filters*** (on page 38) dialog.

In This Chapter

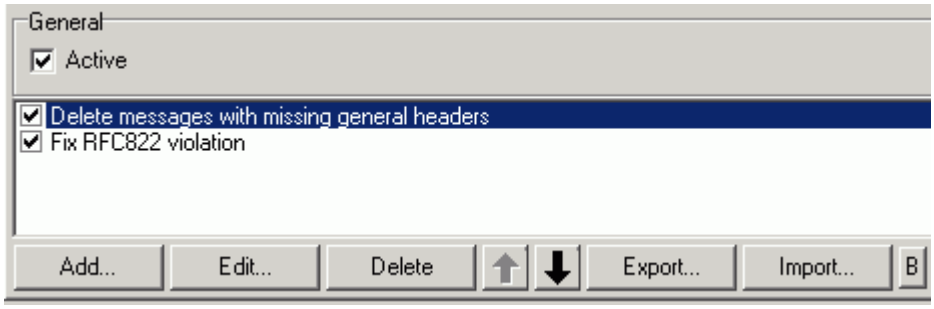
Content Filters

Content Filters (CF) are able to parse message content (headers and body) and perform various actions based on the results.

CFs basically work at the server level, however you can set the CF to only act on messages from selected users, domains etc..

You can define an unlimited number of filters within VisNetic MailServer but you should be aware that too many filters can seriously affect the performance of your server, causing a slowdown of message processing and high CPU usage.

Selecting the **Mail Service - Filters - Content Filters** presents a list of defined filters:



The two filters shown in the above screenshot are pre-defined within VisNetic MailServer and are discussed later in this section.

The **Active** checkbox should be checked if you wish VisNetic MailServer to process Content Filters.

Check the box next to a filter to enable that filter. In the above screenshot Content Filters are enabled and the two filters are being applied to messages.

The buttons at the bottom of the screen are briefly described here and in detail later in this chapter.

The **Add** button opens the Filter dialog to add a new filter.

The **Edit** button opens the Filter dialog to edit the selected filter.

The **Delete** button is used to delete the selected filter.

The **Up** and **Down** buttons are used to change the order in which the filters are applied to messages (top first).

TIP - if you select a rule in the list and hold CTRL while you press the **Add** button, the new rule is positioned above the selected rule

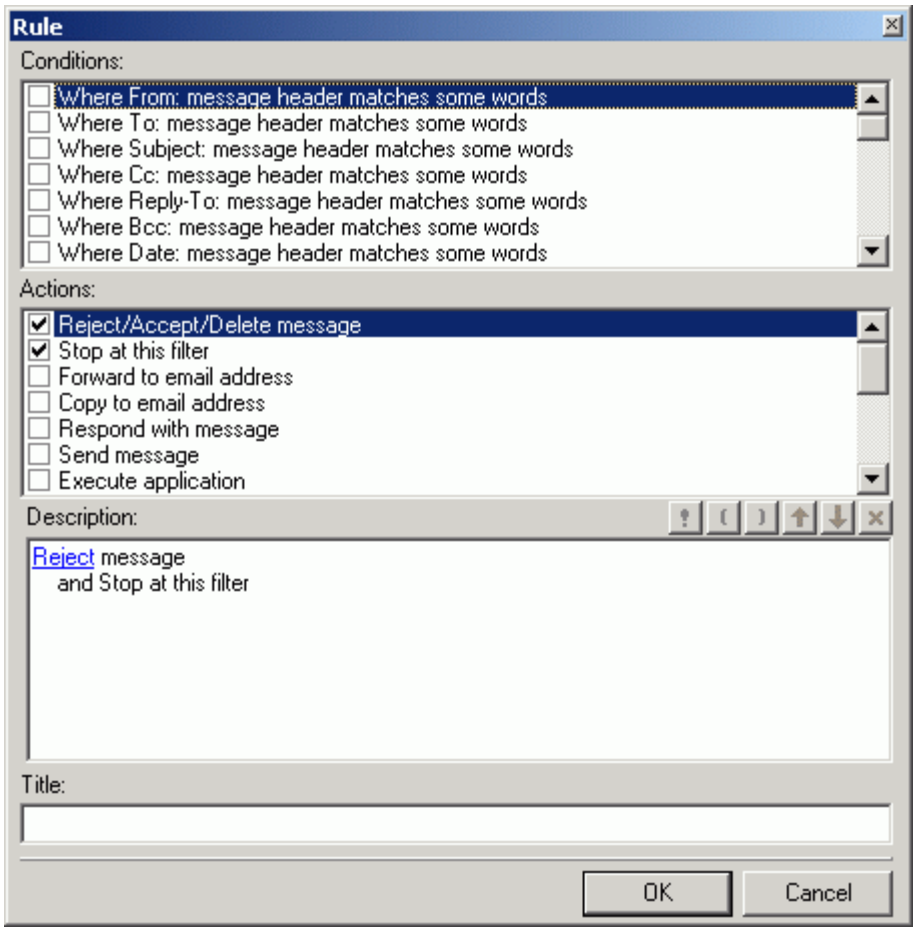
The **Export** button allows you to export filters to an XML file.

The **Import** button allows you to import filters from an XML file.

The **B** button allows you to define a list of items that filters are not applied to.

Adding a new Filter

Pressing the **Add** button opens the Rule dialog which allows you to define a new filter:



All rules consist of one or more **Conditions** to be evaluated and one or more **Actions** to be performed on the message if the evaluation is TRUE.

The top pane of the dialog allows you to add **Conditions** to your rule.

The middle pane allows you to add **Actions** to your rule.

The bottom pane shows the structure of your rule and allows you to add values to the **Conditions** and **Actions**, where necessary.

The **Title** text box allows you to name your filter. We recommend using meaningful descriptive names so you can identify rules easily.

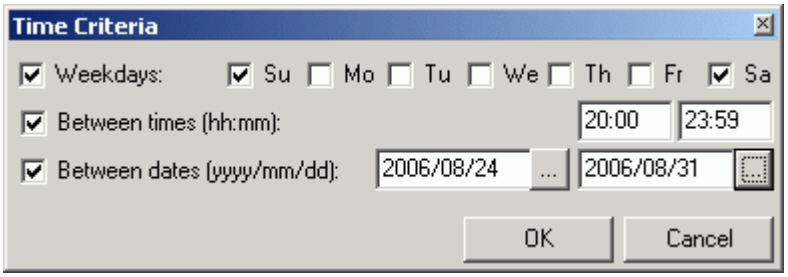
The next sections describe all the conditions and actions you can choose.

Filter Conditions

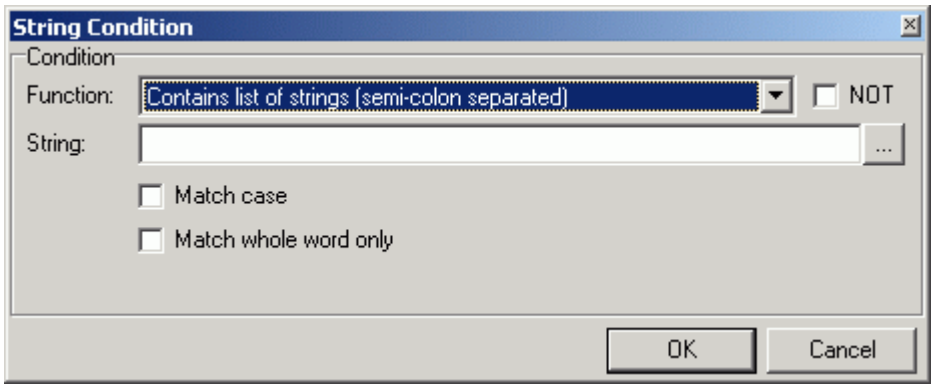
Condition	Use this condition to..
Where From: message header matches some words	check the From: header for text. Adds a **some words** option to the rule description (explained below).
Where To: message header matches some words	check the To: header for text. Adds a **some words** option to the rule description (explained below).
Where Subject: message header matches some words	check the Subject: header for text. Adds a **some words** option to the rule description (explained below).
Where Cc: message header matches some words	check the Cc: header for text. Adds a **some words** option to the rule description (explained below).
Where Reply-To: message header matches some words	check the Reply-To: header for text. Adds a **some words** option to the rule description (explained below).
Where Bcc: message header matches some words	check the Bcc: header for text. Adds a **some words** option to the rule description (explained below).
Where Date: message header matches some words	check the date: header for text. Adds a **some words** option to the rule description (explained below).
Where Message priority is value	check the priority of the message. Adds **Where message priority is Normal** to the rule description. Click on **Normal** to select a priority.
Where Message is Spam	check if the message is marked as spam
Where message is size	check the size of the message. Adds a **0 kB** option to the rule Description. Click on this to chose whether to check the message for a size Greater than or Less than and a size in kilobytes. 
Where Message body matches	check the whole message body for some text.

some words	**Parse XML** function removes all HTML tags from an HTML email body and allows you to search for the text in an HTML part of a message Adds a **some words** option to the rule description (explained below).
Where Custom message header matches some words	check any custom headers for some text. Adds a **some words** option to the rule description (explained below).
Where Any message header matches some words	check all message headers for some text. Adds a **some words** option to the rule description (explained below).
Where Attachment name matched some words	check attachment names for some text. Adds a **some words** option to the rule description (explained below).
Strip Attachment where name matches some words	Strip any attachment(s) whose name contains some text. Adds a **some words** option to the rule description (explained below).
Rename Attachment where name matches some words	Rename any attachment(s) whose name contains some text. This adds **some words** to the rule Description. This is a special case and usage examples follow: Syntax 1 - newstr;oldstr Syntax 2 - *.new;old Syntax once is a simple string replacement, any occurrence of "oldstr" in an attachment name will be replaced by "newstr" Syntax 2 adds ".new" as an extension to the name of any attachment whose name contains "old" Examples: the rule `dog;cat` would rename attachment `mycat.jpg` to `mydog.jpg` the rule ***.ex_;.exe*** would rename attachment ***Myprogram.exe*** to ***Myprogram.exe.ex_*** it would also rename ***not.an.exe.file.jpg*** to ***not.an.exe.file.jpg.ex_***
Where Message contains attachment	evaluates TRUE if the message contains an attachment.
Where Message charset matches some words	check the messages character set name for some text. Adds a **some words** option to the rule description (explained below).
Where Sender matches some	check the sender's address for some text. Adds a **some words** option to the rule description (explained below).

words	
Where Recipient matches some words	check the recipient's address for some text. Adds a **some words** option to the rule description (explained below).
Where Sender/Recipient is local/remote	
Where Sender's hostname matches some words	check the sender and the recipient for some text. Adds a **some words** option to the rule description (explained below).
Where message violates RFC822	check the message for any RFC822 violations. Adds **RFC822** to the rule Description. Click on this to open a dialog that allows you to choose the 4 most common RFC822 violations that can cause email clients to hang when trying to receive a message. 
Where Condition is execution of application	
Where Sender's IP address matches some words	check the Sender's IP address for some text. Adds a **some words** option to the rule description (explained below).
Where rDNS (PTR) matches some words	check the rDNS record for some text. Adds a **some words** option to the rule description (explained below).
Where Sender's IP address is listed on DNSBL server	check a DSNBL server for the Sender's IP address of this message. Adds **server** to the rule description. Click this to enter the name of the DNSBL server you wish to interrogate.
Where Sender's IP address is trusted	Check the Sender's IP address against the Trusted IP's list.
Where Spam score is Value	check the spam score assigned by the AntiSpam engine. Adds **0.00** to the rule Description. Click on this to choose Greater or Lower than and a value. Note that the maximum value that the AntiSpam engine will assign is 10, so specifying a rule that says greater than 10 will never evaluate TRUE, similarly less than 10 will always evaluate FALSE unless the score is exactly 10.

Where Bayes score is percentage	check the score (%) assigned by the Bayesian filter processing. Adds **0%** to the rule Description. Click on this to select Greater or Lower and a percentage value.
Where SMTP AUTH	check whether this message was delivered using the SMTP AUTH command (authenticated login).
Where Scanned by Antivirus	check messages that were scanned by the antivirus engine. Adds **antivirus** to the rule Description. Click on this to open a dialog where you can choose any of the three antivirus engine results.  Note that you should not choose both Message contains a virus AND Message does not contain a virus as this would always evaluate TRUE, as one of those two messages will be within the message.
Where Local time meets criteria	check the local time (of the VisNetic MailServer). Adds **criteria** to the rule Description. Click on this to open a dialog where you can specify local time checking criteria:  The above example will evaluate TRUE only if: The date is between 24th August 2006 and 31st August 2006 AND it is a Saturday or Sunday AND the time is between 20:00 and 23:59. This condition is supplied so that you could create a rule that only runs at weekends, or overnight etc..
Where DB query returns records value	Runs a query against a database and checks for a returned value. Click on Value in the rule description to specify the Database connection to use and the query to run.
All messages	Evaluates TRUE for all messages. This is useful if you want to apply an action to every incoming message.

When **some words** is added to a rule **Description** you should click it to define the text you wish to check for. The **String Condition** dialog is presented:

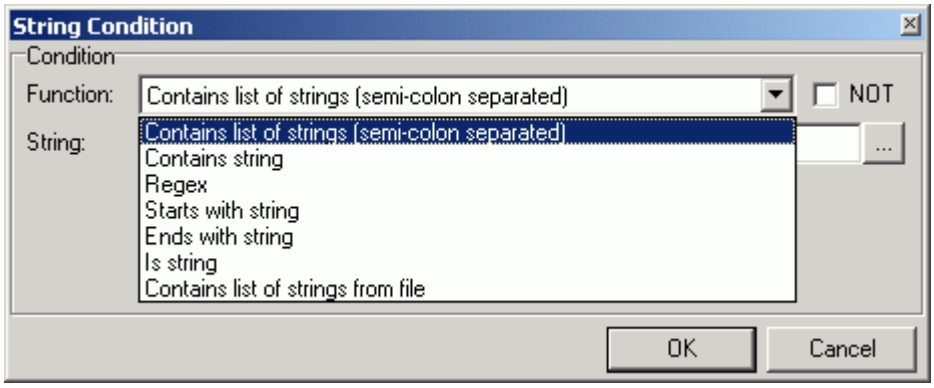


The **Function** drop-down shows the various string selection options available (see below).

The **String** text box contains the string you are evaluating against the **Condition**.

Check **Match Case** if you want the comparison to be case sensitive, i.e. "Viagra" will match "Viagra" but not "viagra".

Check **Match whole word only** and the comparison will only be true if the string is not part of another word, i.e. "Viagra" will match "Viagra works" but will not match "Viagraworks".



The **Function** box describes the type of test you are doing against the value specified in the **String** text box:

Function	**Use this condition to..**
Contains list of strings (semi-colon separated)	Specify a list of semicolon separated strings. Each string will be checked against the Condition and TRUE will be returned if any string matches. Example:

	Viagra;Cialis;spam
Contains string	Specify a single string. If the specified string exists in the Condition, TRUE will be returned
Regex	Specify a Regex (Regular Expression). See the next section for a simple Regex Tutorial. For comprehensive Regex information see ***www.regular-expressions.info*** (http://www.regular-expressions.info).
Starts with string	Specify a string that Condition must start with.
Ends with string	Specify a string that Condition must end with.
Is string	Specify a string that must be an exact match with the Condition
Contains list of strings from file	Specify a filename containing a list of strings n the **String** text box. This must be a fully qualified path to the file. The file must contain one string per line. This Function works like "Contains list of strings" but reads the strings from the file.

Filter Actions

When a Rule is evaluated as true you have the following **actions** which you can apply to the message.

Multiple actions can be applied.

Checking an action will modify the **Rule Description** and may inset a clickable option to refine the action.

Action	**Description**
Reject/Accept/Delete/Spam message	Check this option to mark the message for Rejection, Acceptance or Deletion. The text **Reject** is added to the rule description. Click on Reject to open the **Message Action** dialog, where you can choose to Reject, Accept or Delete the message, or mark it as spam.
Stop processing more rules	Check this option to stop processing this message against further rules. This is useful once you have reached a decision on what to do with this message and saves any further processing power. For example - if you set up a rule to delete all messages from the domain spamcity.com you can set the action to Delete the message and Stop at this

	rule. The rules processing is completed and the message deleted.
Forward to email address	Check this option to Forward a copy of the message to another email address. The text **email address** is added to the rule description. Click on this to open the Email address dialog, allowing you to specify the address(es) to forward the message to. Multiple accounts can be specified, separated by semicolons. You can use the '...' button to select accounts.
Move to folder	Check this option to move the message to a folder. Click on folder in the rule description to open a folder-tree view dialog where you can select the folder to use
Copy to folder	Check this option to copy the message to a folder. Click on folder in the rule description to open a folder-tree view dialog where you can select the folder to use
Encrypt message	Check this option to have VisNetic MailServer encrypt the message.
Respond with message	Check this option to send a message back to the sender of this message. The text **message** is added to the rule description. Click on this to open the Message dialog, where you can specify the From address, the Subject, the message Text (or a file containing the message text) and whether the message Type (Email, Instant message, or both).
Send message	Check this option to send a message to any user. The text **message** is added to the rule description. Click on this to open the Message dialog, where you can specify the From address, the To address, the Subject, the message Text (or a file containing the message text) and whether the message Type (Email, Instant message, or both).
Edit message header	Check this option to edit the message headers. You can add, remove or change headers. The text **header** is added to the rule description. Click this to open the Headers dialog, where you can specify the action to take, and which header to take it on. System variables are allowed here, so for example you could modify the Subject: header to add some text: Subject: [MyNewText] %%Subject%%
Set message priority to value	Check this to change the message priority. Click on Normal in the rule description to select the priority.
Set message flags	Check this option to set message flags. Click on flags in the rule description to select which flags to set
Add score	Check this option to add a value to the spam score of the message. Click on 1.00 in the rule description to set the value to be added. NOTE - that you can specify a negative value to have the spam score decreased.

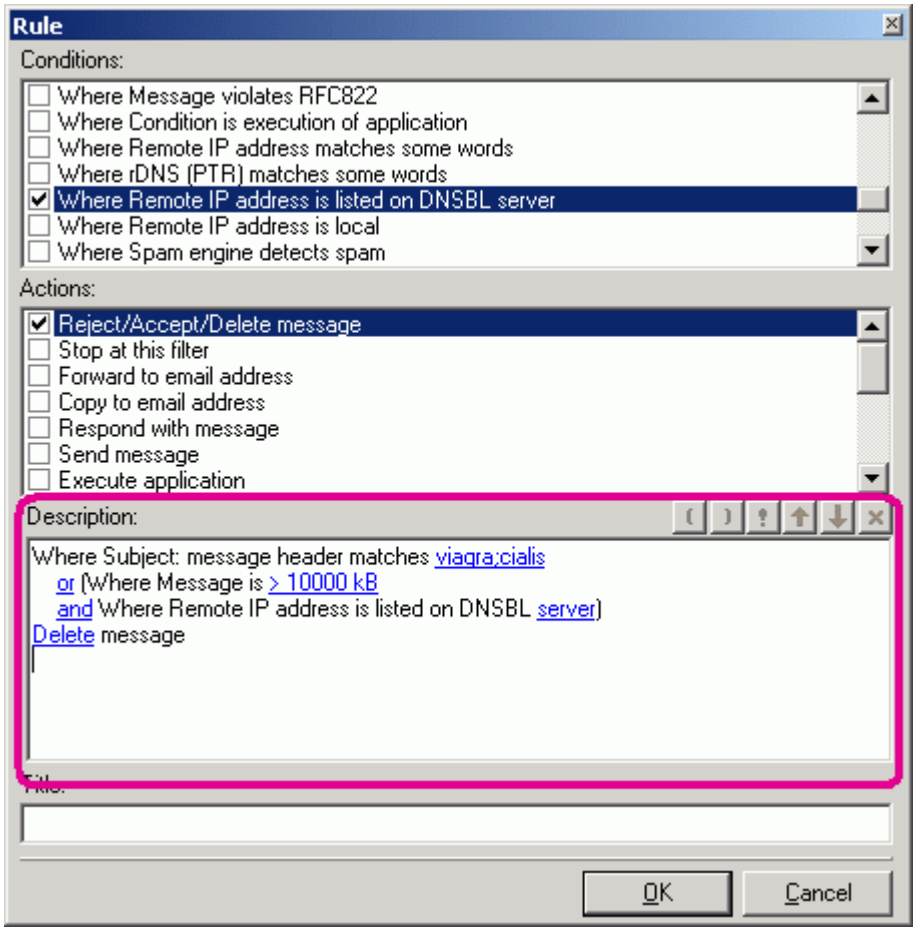
Execute application	Check this option to run an executable. The text **executable** will be added to the rule description. Click this to open the Executable dialog where you can specify the fully qualified path to the executable and it's type (Executable, StdCall, Cdecl or URL)
Add header/footer	Check this option to add a header and/or footer to the email. Headers and Footers are stored in files and can be plain text or HTML. The text **header/footer** is added to the rule description. Click this to open the Header/Footer dialog, which allows you to specify the fully qualified paths to the header and or footer files you want to add to the message.
Strip all attachments	Check this option to strip any attachments from the message.
Extract all attachments to directory	Check this option to store all attachments to a folder. The text **directory** is added to the rule description. Click this to open the extract attachments dialog, where you can specify the directory in which attachments should be stored. If the attachments is an IDP (IW Data Packager) file you can optionally choose to have the files extracted from the package. You can also optionally choose to overwrite existing files.
Add text to a file	Check this option to add a line of text to a file. The text **text** is added to the rule description. Click this to open the Add Text dialog, where you can specify the fully qualified filename to write to and the text to be written. You can optionally choose to create a new file each time. System variables can be used within the text. This option can be useful to create your own format logs containing any information you wish to record
Respond with SMTP message text	Check this option to specify the SMTP servers response to the incoming message. The text **text** is added to the rule description. Click on this to open the SMTP Response dialog, which allows you to specify the text to send back to the originating server. The format of the text should be a numeric response code followed by your freeform text.
Fix RFC822 message	Check this option to fix messages that are not RFC822 compliant. These messages can cause problems with your server and with your user's email clients. Non-compliant messages are usually spam or hacker attacks and we recommend that you delete them with the condition "Where message violates RFC822" combined with Action "Delete" and "Stop at this filter" rather than allowing them through.
Block sender's IP	Check this option to invoke Intrusion Prevention blocking rules to block this

address	senders IP address for an amount of time.
Execute DB SQL statement value	Check this box to execute an SQL query against a database. Click value in the rule description to define the database connection parameters and the query to be run.

Filter Description

Once you have built your rule there is a description of the rule in the lower pane of the Rule.

This section discusses the description and the ways you can manipulate it.



All conditions are initially linked with or conditions, these can be changed to and conditions by clicking on them.

Brackets can be inserted in your rule by placing your cursor where you want the bracket and pressing the appropriate button. "**(**" or "**)**".

A condition can be negated by placing your cursor before the condition and pressing the exclamation mark "**!**" button.

Conditions can be moved up and down the list by placing your cursor within the condition and using the up and down buttons.

A condition can be deleted from the rule by placing the cursor within the condition and pressing the delete button "**X**"

Editing a filter

Pressing the **Edit** button opens the currently selected rule for editing.

The same **Rule** dialog is opened as for adding a rule. The difference is that all conditions and actions will be selected as appropriate and the rule description will be populated.

Please refer to ***Adding a new Rule*** (see "Adding a new Filter" on page 20) for full information.

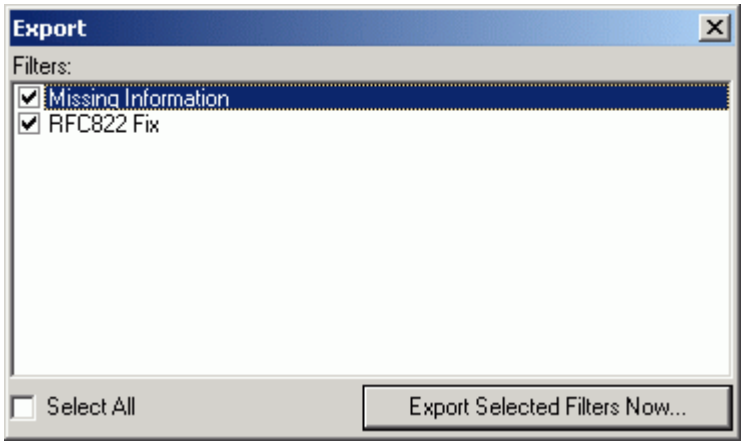
Deleting a filter

Pressing the Delete button will delete the currently selected rule.

A confirmation dialog will be presented.

Exporting filters

The **Export** button will open the **Export** dialog where you can select rules to be exported to an XML file.



Check all the rules that you want to export and press the **Export Selected Filters Now** button.

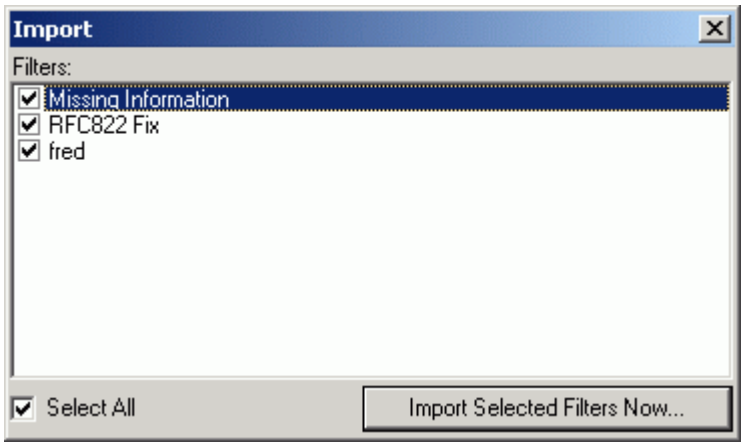
A standard file dialog will open allowing you to name and place your XML file.

This can be useful as a backup copy of your filters or if you want to copy your filters from one VisNetic MailServer to another.

Importing filters

The **Import** button opens a standard file browser dialog to locate and open your XML file of exported filters.

Once the XML file is opened you will be presented with the **Import** dialog



You should check the filters you wish to import and press the **Import Selected Filters Now** button

Bypassing filters

You may wish to bypass Rules processing for certain senders, recipients, domains or email addresses.

The "**B**" button allows you to specify a bypass list. Press the button to open the edit dialog where you specify the bypass items.

Examples and rules are given within the file.

Understanding the SMTP protocol and message headers

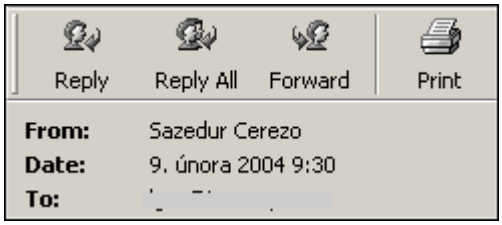
To implement Rules properly, you should understand the structure of an emails and how they are transferred via the SMTP protocol.

An email is transferred over the network using the SMTP protocol as a plain text file with a header and body part.

Instead of the term email, we will use the term "**message**". A "message" is a plain text file which contains an e-mail and all of its attachments and other parts.

Confusion is often caused by the fact that the SMTP sender and recipient can be completely different to the From and To information displayed in an email client.

To understand the difference, look at the VisNetic MailServer system variables, which are related to messages.

%%From%% %%From_Email%% %%From_Alias%% %%From_Domain%% %%From_Name%%	"From:" is taken from the message header, displayed in the recipient client. 
%%To%% %%To_Email%% %%To_Alias%% %%To_Domain%% %%To_Name%%	"To:" is also taken from the message header. Both - From and To are taken from the message header and they NEED NOT be the same as the one used in the SMTP protocol during message transmission.
%%Sender%% %%Sender_Email%% %%Sender_Alias%% %%Sender_Domain%%	The Sender is the real sender in the SMTP protocol. The "From:" in the message header can be different.
%%Recipient%% %%Recipient_Email%% %%Recipient_Alias%% %%Recipient_Domain%%	This is the real recipient in the SMTP protocol. The message will be delivered to this recipient regardless of the message's To: header.

An Email client displays the information from the message header, while the delivery of the message is given by the information in the SMTP protocol.

Example:

The following is an extract from the SMTP log:

The message delivered from xxx@vmsdemo.com to the admin@vmsdemo.com - SMTP protocol:

```
127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 Connected

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 220 mail.vmsdemo.com
ESMTP VMS 7.2.4; Wed, 10 Mar 2004 21:41:16 +0100

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 <<< MAIL
From:xxx@vmsdemo.com

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 250 2.1.0
<xxx@vmsdemo.com>... Sender ok

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 <<< RCPT
To:admin@vmsdemo.com

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 250 2.1.5
<admin@vmsdemo.com>... Recipient ok

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 <<< DATA

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 354 Enter mail, end with "."
on a line by itself

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 *** <xxx@vmsdemo.com>
<admin@vmsdemo.com> 1 1605 00:00:00 OK

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 250 2.6.0 1605 bytes
received in 00:00:00; Message accepted for delivery

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 <<< QUIT

127.0.0.1 [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 >>> 221 2.0.0 mail.vmsdemo.com
closing connection

SYSTEM [000009F8] Wed, 10 Mar 2004 21:41:16 +0100 Disconnected
```

It shows that the message is from xxx@vmsdemo.com and should be delivered to admin@vmsdemo.com.

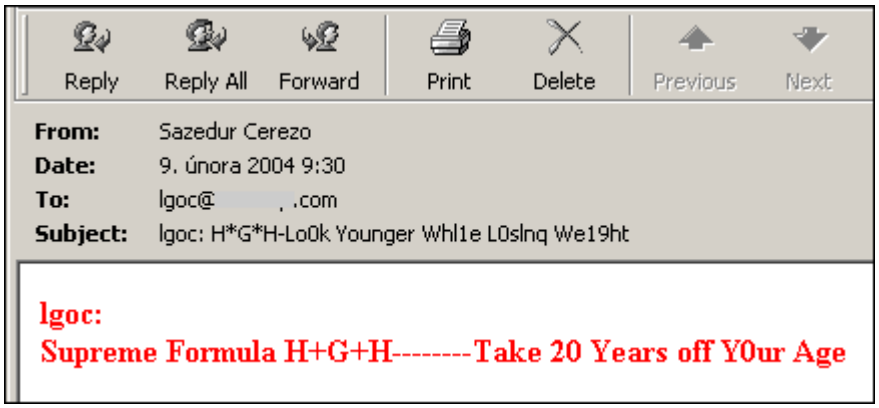
The following shows the actual headers of the message

```
Received: from servcom2.DOMAINE.local ([213.223.244.1])

by mail.vmsdemo.com (VMS 7.2.1) with ESMTP id CRA73883

for <lgoc@vmsdemo.com>; Mon, 09 Feb 2004 09:28:40 +0100

Received: from metallography ([219.95.18.216]) by servcom2.DOMAINE.local with Microsoft
SMTPSVC(5.0.2195.5329);

Mon, 9 Feb 2004 09:30:12 +0100

From: "Sazedur Cerezo"<lgoclgoc@YAHOO.COM>

To: lgoc@vmsdemo.com

Subject: lgoc: H*G*H-Lo0k Younger Whl1e L0slnq We19ht

Mime-Version: 1.0

Content-Type: text/html; charset=us-ascii

Content-Transfer-Encoding: 7bit
```

```
Return-Path: lgoclgoc@YAHOO.COM
Message-ID: <SERVCOM2QFgkASNplKc000165d3@servcom2.DOMAINE.local>
X-OriginalArrivalTime: 09 Feb 2004 08:30:15.0039 (UTC) FILETIME=[F10A78F0:01C3EEE6]
Date: 9 Feb 2004 09:30:15 +0100
```

This shows that the headers say that the message is from "Sazedur Cerezo" and is sent to lgoc@vmsdemo.com.

This is the information that is displayed in the email client:

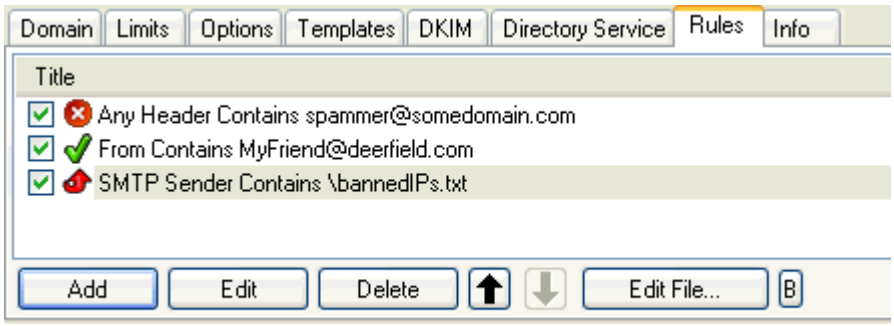


From & To used in the Content Filter Condition correspond to the From: and To: of the HEADER of the message, while the **Sender & Recipient** are taken from SMTP protocol.

CHAPTER 5

Rules

This dialog is the same for all accounts and domains.



Selecting **Mail Service -> Rules** or the **Rules** tab with a Domain or User selected will give you access to the Rules list, allowing you to perform maintenance on the rules.

NOTE - that the above graphics may be incorrect depending upon where you are accessing a Rules tab.

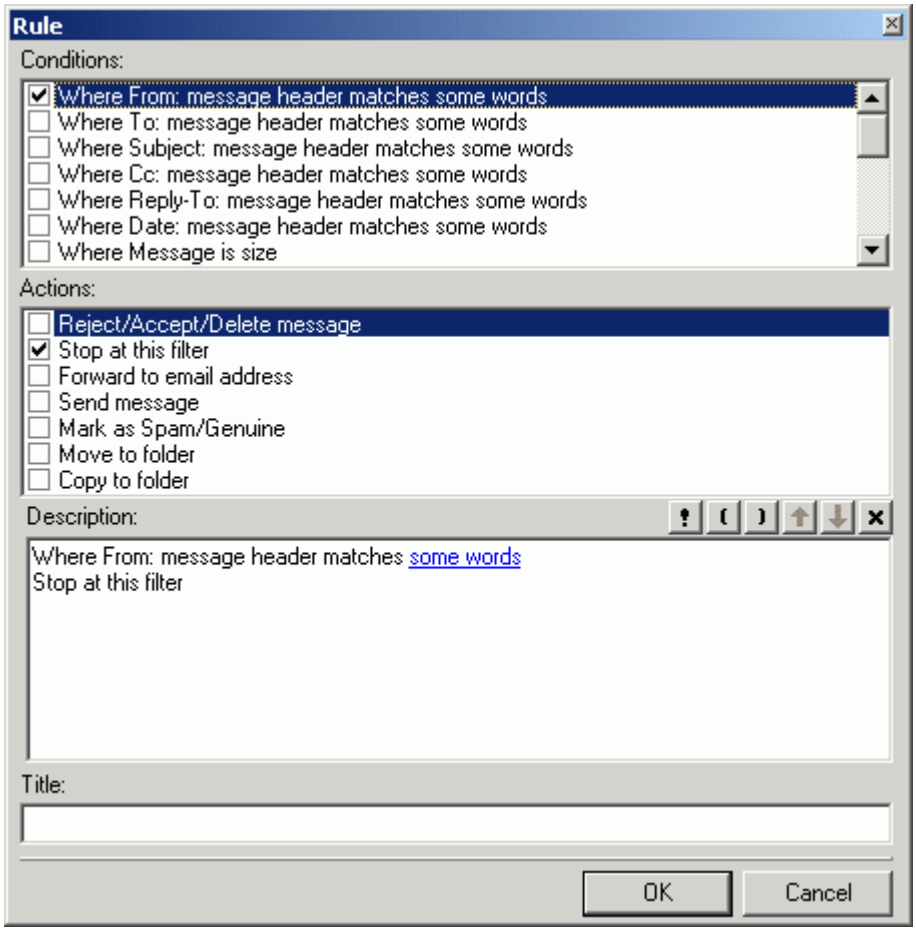
The filter is a text file with a strictly defined format. The file can be edited directly using a standard text file editor but we ***highly*** recommend that you use the **Add**, **Edit** and **Delete** buttons as even the simplest mistake can cause valid emails to be rejected.

Multiple rules can be selected for deletion by holding the Ctrl key and clicking multiple rules.

A range of rules can be selected by clicking the first rule and then clicking the second rule while holding down the Shift key.

Rules can be activated and de-activated by checking/un-checking the box to the left of the rule. This is useful for testing purposes or to disable a rule for a time without deleting it.

Clicking on the **Add** or **Edit** button will open a dialog like this, which allows you to define or modify your rule:



The various options, and the **String conditions** dialog, are discussed in detail in the following table but first we will explain basic use of the three sections of the dialog:

The Conditions block

In this area you can select the properties of the message that you wish to perform some test on.

- Multiple conditions can be tested by checking multiple boxes.
- The same condition can be added multiple times by double clicking the Condition when it is checked.

The Actions block

In this area you select the Action(s) that you want to perform on the message if the Rule evaluates as True

- Multiple actions can be selected by checking multiple boxes.

The Logic Buttons

The buttons below the Actions block are used to add logic to the rule

- The Exclamation mark will negate (NOT) the Condition you are currently modifying.
- The open and close brackets buttons will place the corresponding bracket within the rule that you are building.
- The up and down arrows will move the conditions up and down within the rule.
- The X button will delete the current Condition.

We recommend experimentation with these buttons to familiarize yourself with their function

The Description block

This will show the rule you are building or modifying and will change dynamically as you select or de-select Conditions and Actions.

Areas of the rules that can be modified are highlighted in this block and clicking on them will open a further dialog box to allow you to define your test.

Title

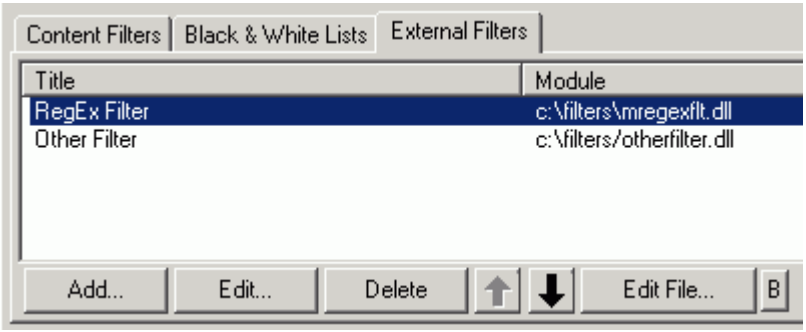
The name of the rule, for identification purposes.

External Filters

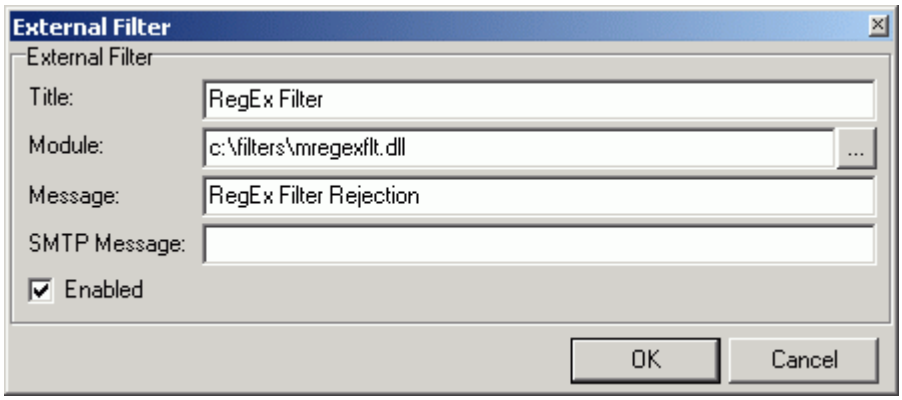
External filters are DLL modules that are loaded in memory and invoked each time a message is received.

Multiple external filters can be defined but you should be aware that too many Filters, or even a few badly coded Filters, can have a detrimental effect on your server.

The filter should return a result if it wants VisNetic MailServer to mark the message in some way.



The Add button opens the External Filter dialog, which allows you to define an external filter:



Field	Description
Title	Just a descriptive text.
Module	The DLL library which is called to evaluate messages.
Message	If no SMTP message is defined, this one is used plus it has pre-defined prefix.
SMTP Message	This message is used in SMTP connections as a response when the message was caught by this filter.
Enabled	Activates/deactivates the filter.

The **Edit** and **Delete** buttons are used to Edit or Delete Filter definitions, respectively..

The **up** and **down** arrow buttons are used to change the order that filters are applied (top first).

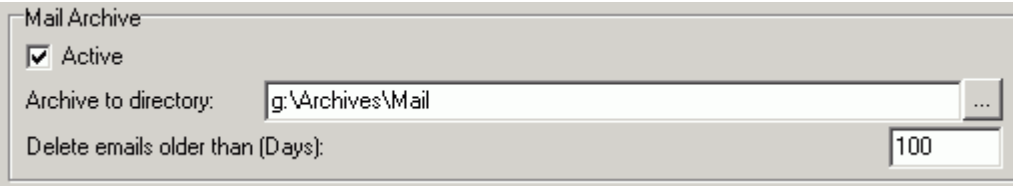
The **Edit File** button opens up the text file of filter definitions. Examples are included.

The **B** button opens up a bypass file where you can specify senders, recipients, domains and IP address ranges that will not have these filters applied.

Archive

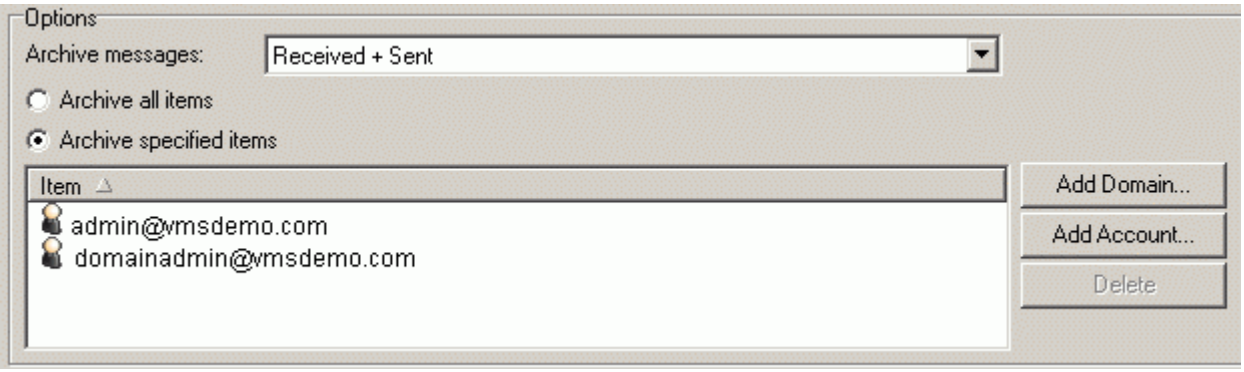
The Archive Sub-node allows you to specify mail Archive and Backup options:

Mail Archive



Field	Description
Active	Check this option to activate Mail Archiving
Archive to Directory	Select the diraectory where mail should be archived
Delete emails older than (Days)	Enter a number here and emails older than that many days will be deleted.

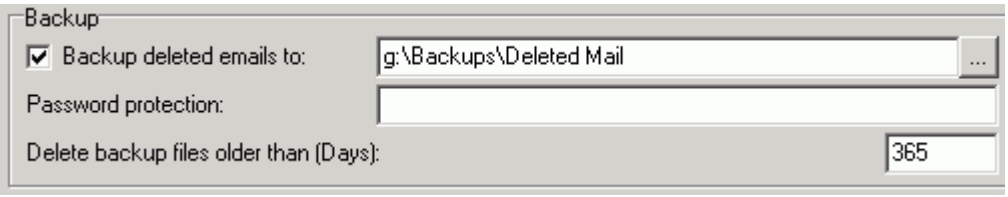
Options



Field	Description
Archive messages	Select from three options: **Received** Archive only Received mail. **Sent** Archive only Sent mail. **Received + Sent** Archive all mail items.
Archive all items	Choose this option to archive mail for all users in all domains

or Archive specified items	Choose this option to select specific domains and/or users to archive mail for. Use the **Add Domain** and/or **Add Account** buttons to choose domains and/or users.

Backup



Field	Description
Backup deleted emails to	Check this option and enter a directory name to have deleted emails backed up to the specified directory
Password protection	Optionally specify a password here to have the backup file password protected.
Delete Backup files older than (Days)	Enter a number here and backups older than that many days will be deleted.

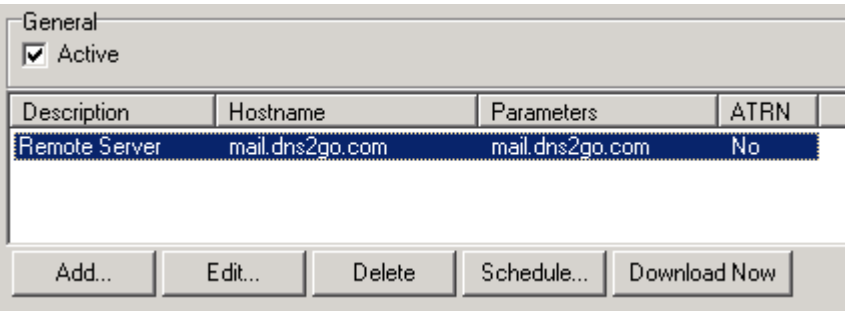
CHAPTER 6

ETRN Download

Short for Extended Turn, ETRN is an extension to the SMTP mail delivery protocol that allows an SMTP server to request from another SMTP server any e-mail messages it has for a specific domain. ETRN is typically used by a mail server that does not have a dedicated connection to the Internet.

The ETRN download node lets you to define ETRN or ATRN client requests to remote mail servers, allowing you to have VisNetic MailServer pick up messages held on other servers.

Multiple downloads can be defined and message collection(s) can be scheduled.

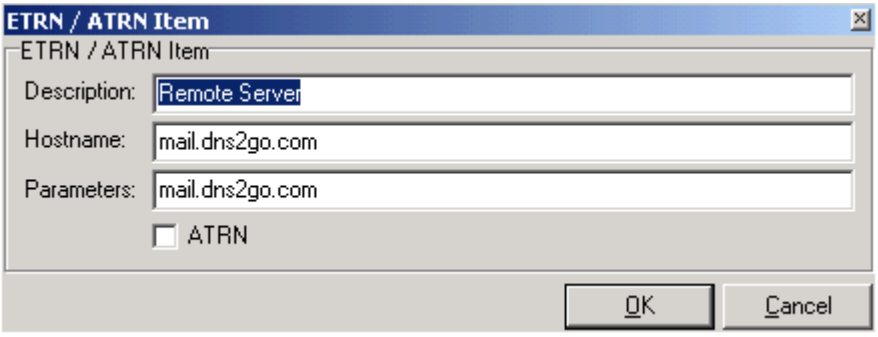


The **Delete** button is used to delete a selected download definition.

The **Schedule** button allows you to define a schedule for downloads.

The **Download Now** button allows to start a manual connection and collection of mail.

The **Add** and **Edit** buttons open the ETRN / ATRN Item dialog, allowing you to add or modify a downloads definition.



Field	Description
Description	A description of this download so you can identify it.
Hostname	Specifies the full hostname or IP address of the remote mail server

	including the port if required.
Parameters	Specifies the parameters to be sent in the ETRN or ATRN command. This is usually the domain name, and possibly a password for password protected ETRN domains. You should consult the documentation for the server you are collecting from for the complete parameter requirements.
ATRN	The default mode for collecting messages is ETRN. If the server you are collecting from requires ATRN (Authenticated Turn) then you should check this box and specify the parameters accordingly. The usual parameter requirement for ATRN is domain.com;userid:password

Index