VisNetic MailServer

AntiVirus Reference Manual

Version 9.1

Contents

CHAPTER 1

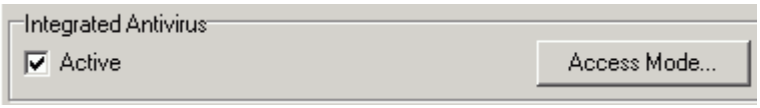
Anti-Virus

The AntiVirus engine can scan incoming and outgoing messages for viruses during SMTP transmission. The award-winning AntiVirus engine from Kaspersky Lab is used.

Various actions can be performed on messages found to contain a virus.

In This Chapter

AntiVirus - General



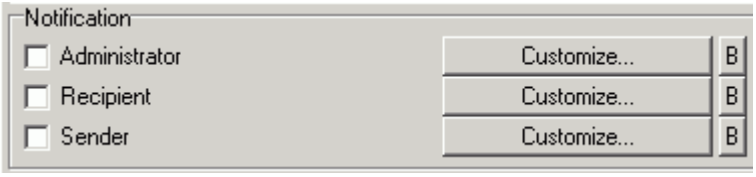
Check the Active box to enable AntiVirus processing.

AntiVirus - Action

In the Action tab you specify the actions to be taken when a message is found to contain a virus.

Field	Description
Choose an Action	**Reject infected messages** Infected messages will be immediately rejected by the server. **Delete infected messages** Infected messages will be accepted and deleted by the server. This option is useful if you want to further process the message even though it contains a virus. For example, you could use Content Filters to forward the message to an AntiVirus team **Remove infected attachments** Any attachments containing a virus will be removed from the message. If an infected attachment cannot be removed then the message is rejected. NOTE that this option will not function properly if the "scan all message parts...." option is checked.
Scan mode	Choose one of the three options: **Attachments** Only message attachments are scanned **All message parts and MIME message** The complete message, including attachments, are scanned **MIME Message** Only the message is scanned (not attachments)

You can further opt to send notification messages to the Domain Administrator, the Recipient and/or the Sender.



Check the recipient(s) you wish to have notified of the virus.

You can customize the message content and use VisNetic MailServer system variables within the message. Press the Customize button next to the recipient to open the message editor dialog. Examples are given within the editor.

You can also define a bypass file for each recipient. Press the B button next to the recipient to define any bypass criteria you wish to impose. Examples are given within the editor.

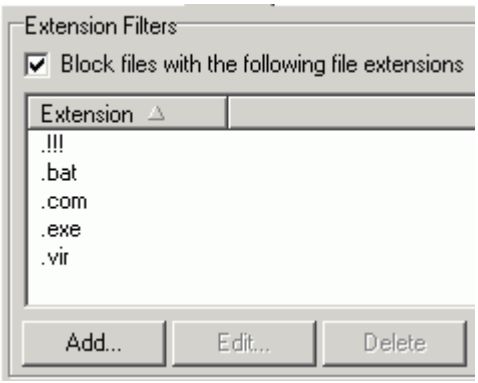
Field	Description
Quarantine infected message to email/directory	Check this option to create an archive of infected messages. Specify a fully qualified directory name where the messages will be stored, or an email address where the messages will be forwarded. Choose one of the following options: **Quarantine infected messages** The whole message will be quarantined. **Quarantine only infected attachments** Only the infected attachments will be quarantined.

NOTE - that this is NOT the same Quarantine function as used by the AntiSpam engine!

AntiVirus - Filters

The Filters tab allows you to define a list of file extensions which will be considered a virus.

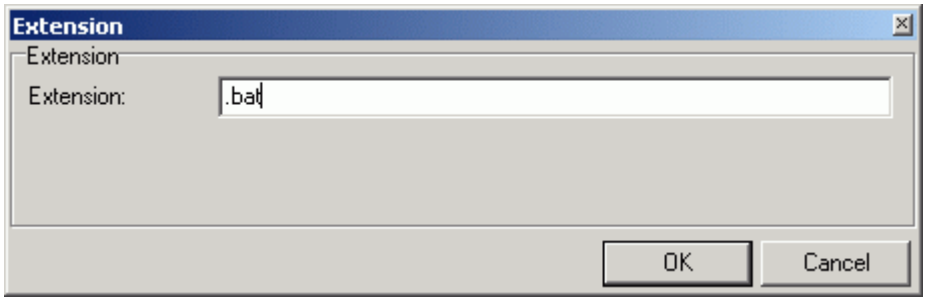
If VisNetic MailServer finds an attached file with a listed extension then the message is processed as if it contained a virus.



Check the **Block files with the following file extensions** box to have VisNetic MailServer process the list of extensions against message attachments.

Use the **Delete** button to delete a selected extensions.

Use the **Add** or **Edit** buttons to add a new extension to the list or edit a selected extension. The **Extensions** dialog is opened:



Enter the extension that you wish to consider a virus and press **OK** to save the extension to the list.

Note that you must specify the dot (.) before the extension.

Also, please be aware that you should not block the .TMP extension as this will cause VisNetic MailServer to categorize all messages as containing a virus.

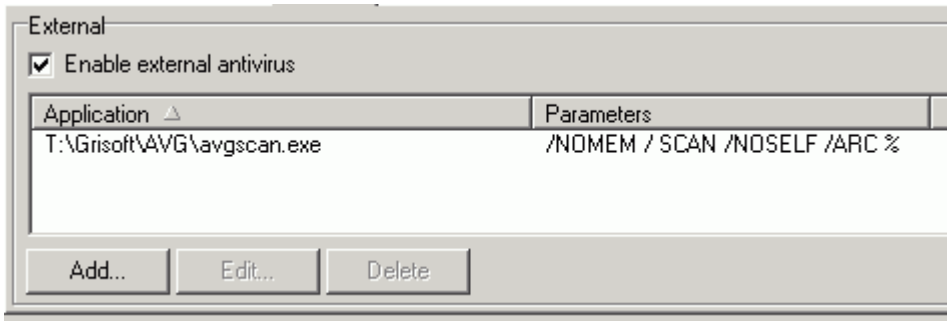
AntiVirus - External

The External Filters tab allows you to configure VisNetic MailServer to use any external filter(s) that support command-line scanning.

VisNetic MailServer Instant AntiSpam allows two typical ways of external AntiVirus usage -

- executable applications
- libraries, for more information about libraries usage please refer to example file `/examples/libraryexternalav.txt.html` that is delivered with standard installation of VisNetic MailServer.

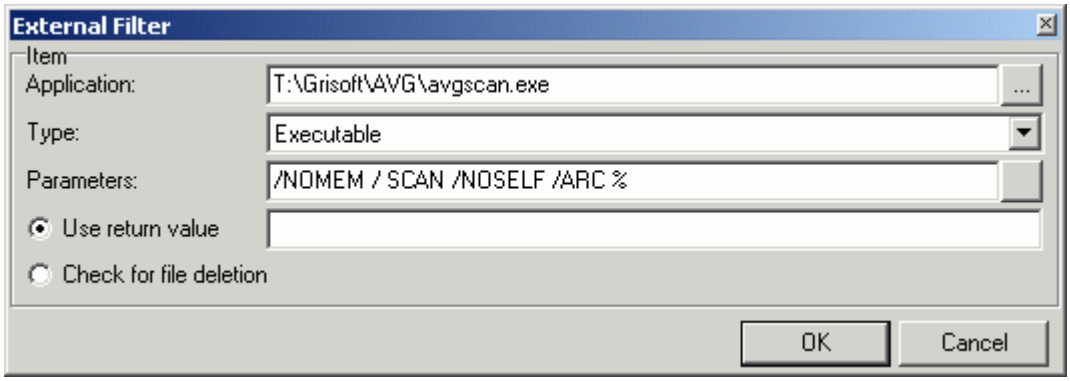
NOTE that if you choose to use any external on-access AntiVirus scanner you should exclude the <InstallDirectory>\Temp folder from the scanning as this could cause severe server slowdown and problems with VisNetic MailServer itself.



Check the Enable external AntiVirus box to enable this feature.

The Delete button will delete any selected filter.

The Add and Edit button allows you to define or modify an external filter. The External Filter dialog is opened:

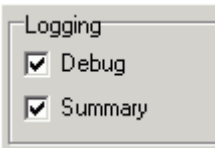


Field	Description
Application	Specify the fully qualified path to the external filter. Use the '...' button to open a standard file browser dialog.
Type	Select the type of module you are calling: **Executable** Choose this for a standard executable module. **StdCall Library, Cdecl Library** Choose this to call the filter from a library. Please refer to example file `/examples/libraryexternalav.txt.html` that is delivered with standard installation of VisNetic MailServer.
Parameters	Here you should specify any parameters required by the external filter.

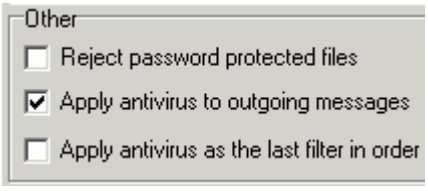
	Refer to your filter's documentation for further information.
Use return value	Enter values here that your external filter returns if a virus is found. Refer to your filters documentation for this information. Multiple values should be separated by commas. For example, if your filter returns a value from 1 to 5 if a virus is found you should specify 1,2,3,4,5 here.
Check for file deletion	Some filters do not return a value, but simply delete the file. If your filter behaves in this manner you should select this option. After the filter is run VisNetic MailServer will check whether the file has been deleted and, if it has, will treat the message as if it contains a virus.

AntiVirus - Other

The Other tab allows you to specify Logging and some other options.

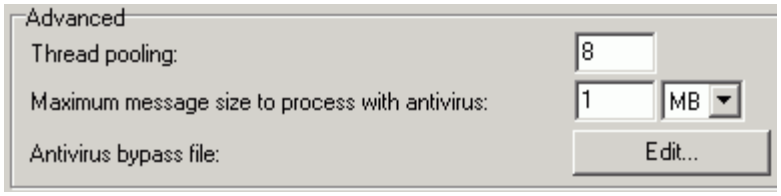


Sets the level(s) of logging for the AntiVirus engine. Debug logging gives detailed entries in the log files and Summary logging gives less detailed informational messages.



Field	Description
Reject password protected files	The AntiVirus engine must unpack attachments to check them for a virus. If an attached file is password protected then VisNetic MailServer cannot check the file contents. By default, the message would be forwarded to the recipient. This scenario could be exploited to get viruses into your system. Check this option to categorize any messages containing password protected

	files as containing a virus.
Apply AntiVirus to outgoing messages	Check this option to have the AntiVirus engine scan outgoing messages as well as incoming messages.
Apply AntiVirus as the last filter in order	The AntiVirus engine is, by default, run before any other major filters. Checking this option instructs VisNetic MailServer to run AntiVirus as the last filter.



Field	Description
Thread pooling	The AntiVirus engine is multi-threading, this can sometimes cause problems on slower servers if the engine takes up too many resources, like 100% CPU. Entering a non-zero value here limits the number of AntiVirus threads that will be run concurrently.
Maximum message size to proceed with antivirus	Select a non-zero vale here to have AntiVirus processing bypassed for messages exceeding the given size.
AntiVirus bypass file	Press the Edit button to edit a bypass file for the AntiVirus engine. This is a standard VisNetic MailServer bypass file. Examples of usage are given within the editor. Messages from Email addresses, Domains, and IP ranges specified within this file will not be processed by the AntiVirus engine.
Integrated AntiVirus setup	Press the Setup button to open the AntiVirus engine settings file. NOTE - We recommend you only modify this file if you know what you are doing or are instructed by Support staff.

Index

A