Mailgate Ltd.

MailGate Virus Scanner Extension User Manual

Mailgate

Mail Server & Proxy Gateway

Microsoft is a registered trademark and Windows 95, Windows 98 and Windows NT are trademarks of Microsoft Corporation.

Edited by Lani K. and David D. Thompson.

Contents

Figures

Virus Scanner Extension Introduction

The MailGate Virus Scanner Extension is an optional module that provides a link between MailGate and your anti-virus software.

Currently full support is provided for the Sophos range of Anti-Virus software and limited support for any Anti-Virus product which supports 'On Access' scanning.

The extension allows all mail attachments passed through MailGate to be scanned for viruses. If a virus is found the mail will be stopped and various actions taken according to the settings found on the **Settings Tab** (see page 3). This can include removing the attachment, quarantining a copy and notifying the system administrator of the virus.

Virus Scanner Extension Configuration

Virus Scanner Extension Installation

To install the MailGate Virus Scanner Extension, run the self-extracting executable set-up program. This program, after you have read and confirmed your acceptance of the software licence, will install all the necessary components into your MailGate system folder.

Once the install process has completed you must access the extension and configure it to your requirements. Use the Extensions option to configure the module. When you have completed and saved your settings, stop and restart the MailGate service to initialise the extension.

Anti-Virus Software Installation Information

You should complete the installation of your AV software and select the correct scanning mode on the About Tab before the MailGate module is activated.

Using Sophos AV Products

- On NT/2000 Systems: install the current Sophos NT product. This includes the required SAVI software. Select Sophos SAVI for the scanning mode. See **Using with Sophos SAVI** on page 9 for more information.
- On Win 95/98/ME Systems: install the 95 product for normal machine protection and then also install the DOS Sweep product for MailGate to use. Select Sophos sweep.exe for the scanning mode. See **Using with Sophos Sweep.exe** on page 10 for more information.

If you have the Sophos Intercheck product installed, this program must be disabled.

Using other AV Products

Ensure your product has an 'On Access' scanner (it checks files as they are opened) and that this is correctly installed. Select Generic Compatibility for the scanning mode. See **Using in Generic Mode** on page 10 for more information.

Note

On Win 95/98/ME platforms and when using 'On Access' scanners, because of the technology used, the anti-virus checking process can have a significant impact on the system performance.

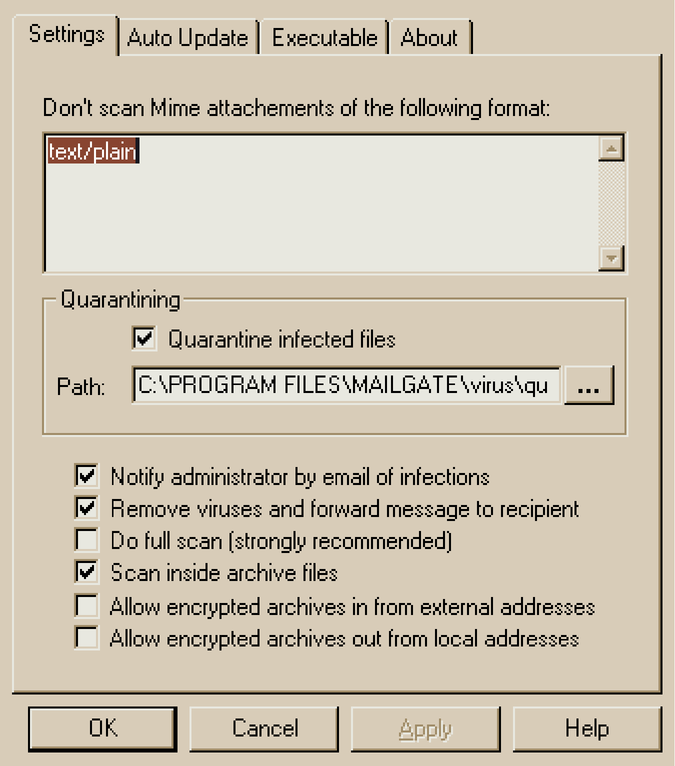
Module Configuration

There are a number of tabs for the module configuration which should be reviewed:

1. **Settings Tab** (page 3) - this sets the options for the virus check interface, including which files to exclude from scanning, whether to quarantine infected files and what actions to take when a virus is found.

2. **Auto Update Tab** (page 5) - use this to configure the settings for the auto-update option.
3. **Executable Tab** (page 6) - only used on a Sophos Win 95/98/ME installation to specify the location of the Sophos sweep program.
4. **About Tab** (page 6) - Select the Scanning Mode and apply the registration key

Settings Tab



Don't scan Mime attachements of the following format:

text/plain

Quarantining

☑ Quarantine infected files

Path: C:\PROGRAM FILES\MAILGATE\virus\qu

☑ Notify administrator by email of infections
☑ Remove viruses and forward message to recipient
□ Do full scan (strongly recommended)
☑ Scan inside archive files
□ Allow encrypted archives in from external addresses
□ Allow encrypted archives out from local addresses

Figure 1 - Settings Tab

The Settings Tab specifies how MailGate should interface with the Anti-Virus software and what actions should be taken if a virus is found.

▸ MIME Types

The MIME type section specifies which MIME types are **excluded** from scanning. Any MIME type not listed will be scanned. In general only plain text or image attachments are excluded.

Some common MIME types are:

- text/plain
- text/html
- text/MIME
- image/image-type (jpeg, bmp, gif)
- application/application-name
- audio/audio-type

Quarantining

Quarantine places a file infected by a virus in a separate folder.

Check "Quarantine infected files" to enable and specify where to place the files in the Path field. You can use the Browse (...) button to find the quarantine folder.

If you do not quarantine infected files, they are deleted from the system.

Options

The following options control give more control between MailGate and the Anti-Virus software.

Notify administrator by email of infections - check to send an email to the administrator when an infected file is found. The administrator mail address is defined in the main MailGate Gateway Setup dialog on the Email tab with the "System reports to" field.

Remove viruses and forward message to recipient - if checked, the infected file is removed and the mail message is forwarded to the recipient.

If not checked no message is forwarded to the recipient.

Do full scan - if checked (strongly recommended), Sophos AV will perform a full scan on the file. This type of scan requires a little more system resources but is required to identify all virus types.

Scan inside archive files - if checked, check archive files such as zip format for viruses.

If not checked, archive files will not be scanned for viruses.

Allow encrypted archives from external addresses

If checked, passes through encrypted archive files from outside addresses. Encrypted formats can not be checked for viruses.

If not checked, MailGate will not pass encrypted archive files from external addresses and will treat them as infected files.

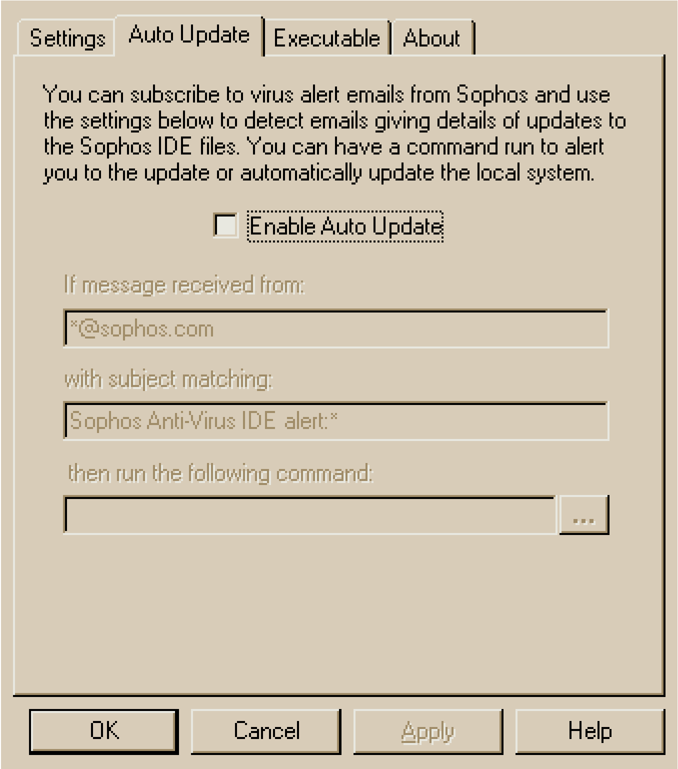
Allow encrypted archives from local addresses

If checked, MailGate passes through encrypted archive files from inside addresses. Encrypted formats can not be checked for viruses.

If not checked, MailGate does allow encrypted archive files to be sent out. Any encrypted files are archived and a message sent to the sender with the information that it can't be sent and the name of the archive file.

Scan for Macintosh viruses too - check to scan for Macintosh as well as PC viruses. This is available only on Sophos NT systems.

Auto Update Tab



You can subscribe to virus alert emails from Sophos and use the settings below to detect emails giving details of updates to the Sophos IDE files. You can have a command run to alert you to the update or automatically update the local system.

□ Enable Auto Update

If message received from: *@sophos.com

with subject matching: Sophos Anti-Virus IDE alert:*

then run the following command:

Figure 2 - Auto Updated Tab

Use this tab if you want to subscribe to an Email based Virus Alert service and have MailGate automatically run a command when an Alert mail is received. The Virus Scanner extension will run your command when a mail message matching the defined conditions is received by the system.

Sophos provide this service to all users and you can subscribe by visiting their website.

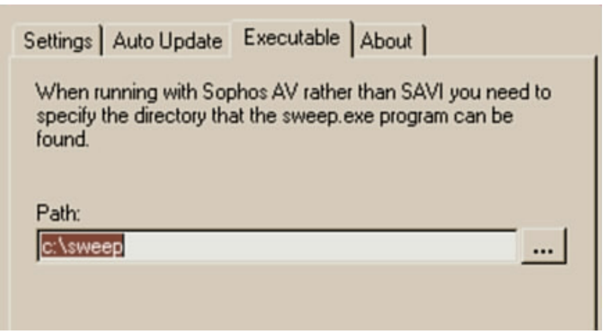
There is a sample command batch file called sav_up.bat installed into your MailGate system folder that can be used to set-up an automatic update process. You should enable auto update on this tab and set the patterns for the From address and Subject to identify your alert mails.

For the Sophos service the defaults are:-

From:	*@Sophos.com
Subject	Sophos Anti-Virus IDE alert*

For more details see **Using Auto Update** on page 12.

Executable Tab



When running with Sophos AV rather than SAVI you need to specify the directory that the sweep.exe program can be found.

Path: c:\sweep

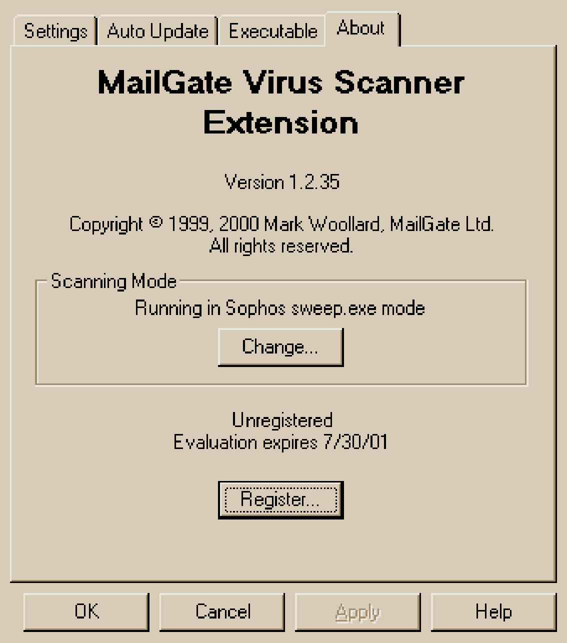
Figure 3 - Executable Tab

This tab is only available on Sophos Win 95/98/ME systems.

Use this tab to specify the location of the DOS Sweep.exe program. By default this will be c:\sweep.

See **Using with Sophos Sweep.exe** on page 10 for more details.

About Tab



MailGate Virus Scanner Extension

Version 1.2.35

Copyright © 1999, 2000 Mark Woollard, MailGate Ltd.
All rights reserved.

Scanning Mode
Running in Sophos sweep.exe mode

Unregistered
Evaluation expires 7/30/01

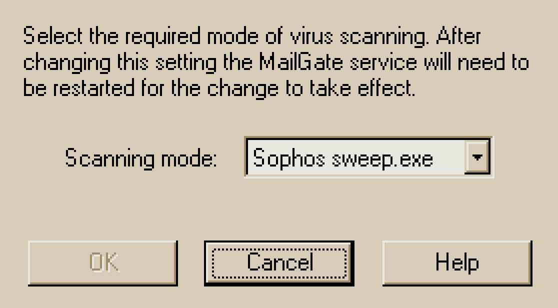
Figure 4 - About Tab

The About tab shows the version of the MailGate Virus Scanner Extension and the current scanning mode.

Use the Change button to select the required scanning mode (see **Scanning Mode Dialog** below). If you make a change you must close and re-open the configuration screen before the change can take effect.

The Registration (see page 8) button is used to enter the activation code for the extension.

Scanning Mode Dialog



Select the required mode of virus scanning. After changing this setting the MailGate service will need to be restarted for the change to take effect.

Scanning mode: Sophos sweep.exe

Figure 5 - Scanning Mode Dialog

In the Scanning Mode dialog you can select how the extension reacts with your AV Software. There are currently three modes available.

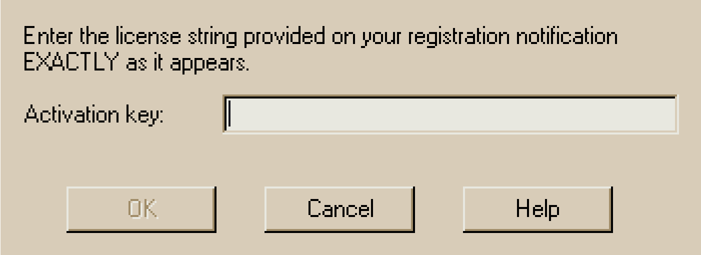
Using Sophos AV Products

- On NT/2000 Systems: Select Sophos SAVI for the scanning mode. See **Using with Sophos SAVI** on page 9 for more information.
- On Win 95/98/ME Systems: Select Sophos sweep.exe for the scanning mode. See **Using with Sophos Sweep.exe** on page 10 for more information.

Using other AV Products with On Access scanning

Select Generic Computability for the scanning mode. See **Using in Generic Mode** on page 10 for more information.

Register Dialog



Enter the license string provided on your registration notification EXACTLY as it appears.

Activation key:

Figure 6 - Register Dialog

The Virus Scanner Extension requires a separate registration activation key from the main MailGate program. Contact your reseller to purchase a licence.

To register the virus scanner extension, click on the Register button on the About tab to display this dialog. Enter your activation code exactly as provided by your reseller.

Note: all letters are entered in capitals.

Using the Virus Scanner Extension

How Mail is Scanned

The MailGate Virus Scanner Extension checks every mail message that passes through the system for viruses.

Mail borne viruses are contained in mail attachments. When attached to a mail these attachments are encoded and are not generally visible to anti-virus software. To allow an attachment to be scanned it must first be decoded and made available to the AV software.

When a mail with an attachment is processed by the extension, MailGate decodes the attachment and saves it to a temporary file on the disk. It then requests scanning of the saved file and checks the results. If the file is identified as containing a virus, the extension will perform the actions defined on the **Settings Tab** {see page 3). These can include:-

i. Move the infected file to the quarantine folder.
ii. Create a notification email to send to the administrator advising of the virus.
iii. Replace the attachment with a text file advising of the virus and release the message to the intended recipient.

If the file is found to be clean then the message is simply released for normal delivery.

Using with Sophos SAVI

If your MailGate system is installed on Windows NT/2000 and you wish to use Sophos for scanning your Emails, then you should select the scanning mode Sophos SAVI (see **About Tab** on page 6).

SAVI is an API level interface between the MailGate extension and the Sophos AV engine. It installs automatically as part of the Sophos for NT product.

When you install Sophos you should note the following:-

i. Do not install or enable the Intercheck Client.
ii. If you want to use the auto update facility, you must install to a central installation then install the working (local) copy from this central copy. For full details refer to the Sophos manual.

Once your Sophos installation is complete, stop and restart the MailGate service and send through a test mail with a file attachment. Open the Sophos Sweep application and click on the SAVI tab. You should now see MailGate registered in SAVI and a report near the bottom of the tab showing the scanning of the attachment.

Using with Sophos Sweep.exe

If your MailGate system is installed on Windows 95/98/ME and you wish to use Sophos for scanning your Emails, then you should select the scanning mode Sophos Sweep.exe (see **About Tab** on page 6).

Sweep is an executable program interface between the MailGate extension and the Sophos AV engine. To install it you must install the Sophos DOS product which can be found on your Sophos CD. You may also like to install Sweep for windows to provide normal AV facilities on the MailGate PC.

When you install Sophos you should note the following:-

i. Do not install or enable the Intercheck Client.

ii. Note the location used to install DOS Sweep and ensure you set your MailGate executable path to suit. (See the **Executable Tab** on page 6)

iii. If you want to use the auto update facility, you must install to a central installation then install the working (local) copy from this central copy. For full details refer to the Sophos manual.

Once your Sophos installation is complete, stop and restart the MailGate service and check the log file. You should see a line which reports *Loaded extension Virus.dll*. This indicates the extension has found Sweep.exe and loaded correctly.

Using in Generic Mode

If you wish to use an anti-virus product other than Sophos for scanning your Emails, then you should select the scanning mode Generic Mode (see **About Tab** on page 6).

Generic Mode scanning relies on the 'On Access' scanning facility available with most Anti-Virus products. With this the AV software will prevent either the writing or reading of an infected file. The MailGate extension will identify this and treat the attachment file as containing a virus, performing the actions set on the **Settings Tab** (page 3).

Limitations of Generic Mode

There are some limitations to using this method of scanning that should be noted:

i. The extension is not able to report the type of virus found. All viruses are reported as 'Generic'
ii. System problems can be reported as virus events if the extension can not write or read the attachment file for some reason other than a virus.
iii. Some AV 'On Access' scanners may not detect all mail related viruses. In particular HTML script viruses can be missed. It is your responsibility to ensure your AV software is suitable.
iv. Some AV scanners will display a warning screen when a virus is found and may stop other processing until the warning is acknowledged. This could stop your mail system.
v. The quarantine option may not work if the AV scanner prevents writing of an infected file.

Technical Reference

Using Auto Update

The Virus Scanner extension provides an facility to trigger an automatic AV software update process when a recognised mail message is received by the system.

Sophos provides such a service to all users and you can subscribe by visiting their website.

There is a sample batch file called sav_up.bat installed into your MailGate system folder that can be used to set-up an automatic update process. First you should enable auto update on the **Auto Update Tab** (page 5) and set the patterns for the From address and Subject to identify your alert mails.

For the Sophos service the defaults are:-

From:	*@Sophos.com
Subject	Sophos Anti-Virus IDE alert*

Next you set-up a folder to run your update from. Into this place a copy of sav_up.bat and any other utilities you require. For a Sophos system you will need a copy of sget.exe from the CD and an command line unzip utility. Enter the location and name for your command in the *then run the following command* entry on this tab.

Now edit sav_up.bat to suit your installation drives, folders and software. For Sophos you will be required to install the software into a central folder and install the working (local) copy from this. Refer to the Sophos manuals for more detail on how to do this.

You can test your configuration by manually running your command file.

With other AV products you should create your own command file to perform the tasks required. If your software vendor does not provide a notification service, you could define matching criteria for any available service or even send trigger messages from your own Email client.

Note - When MailGate runs your command it will use the same account as the MailGate service. Generally this is the system account on NT. You will need to ensure that your access rights are correctly set for the tasks in your process.

Troubleshooting

Testing your installation

You can test your Anti Virus installation by using the EICAR test string. Follow the steps below:-

1. Create a new text document on your system.
2. Edit this document with Notepad, copy the EICAR test virus lines (below) and paste then into it.
3. Save the document and then rename the file to test.com.
4. In your Email client, create a test mail message and attach the file test.com to it.
5. Send the mail. You should get a reply returned by MailGate informing you of the virus.

Note - If you have anti-virus software installed on your PC you may need to disable this first.

Copy the following two lines to create an EICAR test virus file. Note ensure there are no blank lines in the file.

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

End of test virus file
```

Checking the MailGate log file

You can confirm the correct loading and initialisation of the Virus Scanner extension by referring to the MailGate log file.

To do this, first stop and start the MailGate service.

Open the current log file and go to the end of the log.

Starting from the bottom of the log file, scroll up until you find a line similar to the line containing "MailGate 3.4.163 service starting". An extract from a 'healthy' log file is shown below, if your log file is similar to this then the Virus Scanner extension has started correctly:

```
MGATESVC I 15:50:29 0xfff073e7 MailGate 3.4.163 service starting

MGATESVC I 15:50:29 0xfff073e7 Operating system is Windows 95 4.0 build 1111 B

MGATESVC I 15:50:29 0xfff073e7 virus: Extension version 1.1.32 starting

MGATESVC I 15:50:29 0xfff073e7 virus: Licenced serial number 006666

MGATESVC I 15:50:29 0xfff073e7 Loaded extension Virus.dll
```

If there is a problem with your installation then you will see an error reported in place of the last line. Review your installation to resolve the error.

Using Sophos SAVI on NT/2000

If you have MailGate installed with Sophos SAVI, open the Sophos Sweep user interface. If the Virus Scanner extension has correctly loaded and connected to SAVI you will see a SAVI tab with MailGate registered as a connection on it. Near the bottom of the tab there are counters giving information on the files that have been checked. You should see these counters change as mails with attachments are passed through MailGate.

Virus Scanner Windows Registry

Windows Registry

The Virus Scanner extension stores its configuration in the Windows Registry. All settings are stored under the section:-

```
HKEY_LOCAL_MACHINE
        Software
                IDSL
                        MailGate
                                Virus
```

Within the Virus key are found the main configuration settings. See the following pages for details.

Registry - Virus

The Virus Scanner Extension configuration settings are stored in this Registry key.

Value Name (Data Type)	Description
FeatureNotification (DWORD)	Set this to non-zero if you don't want the warning about limitations of generic compatibility mode when opening the configuration screen.
ForwardToUser (DWORD)	Controls whether infected messages are allowed through to the recipient with the virus removed. 1 = allow through, 0 = don't allow through.
FullScan (DWORD)	Controls whether Sophos full scanning of suspect attachments is undertaken. See Sophos documentation for full details. 1 = full scan, 0 = basic scanning. This setting does not apply in generic mode.
LicenceString (String)	When the extension is registered contains the registration key.
MacVirusCheck (DWORD)	Controls whether Sophos scans for Macintosh virii. See Sophos documentation for full details. 1 = full scan, 0 = basic scanning. This setting does not apply in generic mode.
MimeTypes (Multi-String)	List of wildcard patterns to match against mime types of message segments. If matched scanning is skipped for that section. Default array is single entry 'text/plain'.
NotifyAdmin (DWORD)	Indicates whether an email is sent to the system administrator when a virus is detected. 1 = send email, 0 = don't.
PassLocalLocked Archives (DWORD)	Controls whether password protected archives attached to messages being sent from a local user are allowed through. 1 = allow through, 0 = remove.
PassLockedArchives (DWORD)	Controls whether password protected archives attached to messages collected from external servers are allowed through to local mailboxes. 1 = allow through, 0 = remove.
Quarantine (DWORD)	Controls whether infected files are quarantined or deleted. 1 = quarantine, 0 = delete.
QuarantinePath (String)	Path to quarantine area.
ScanArchives (DWORD)	Controls whether archive file contents are scanned by Sophos. See Sophos documentation for full details. 1 = scan archive, 0 = skip scanning. This setting does not apply in generic mode.
UpdateCommand (String)	Command to execute when auto-update conditions are met.
UpdateEnabled (DWORD)	Controls whether auto-update is enabled. 1 = enabled, 0 = disabled.
UpdateFrom (String)	Wildcard pattern to be matched against email from addresses to detect auto-update email.
UpdateSubject (String)	Wildcard pattern to be matched against email subject to detect auto-update email.
Version (String)	Version of currently installed Virus Scanner Extension.
VirusEngine (DWORD)	Mode that Virus Scanner is running in. 0 = Sophos SAVI 1 = Sophos sweep.exe 2 = Generic compatibility