Sophos Anti-Virus

User Manual

Windows 95/98

SOPHOS

Sophos Anti-Virus

for Windows 95/98

User Manual
November 1999

YEAR 2000
Y2K
COMPLIANT

This manual documents Sophos Anti-Virus for Windows 95/98, which incorporates SWEEP and InterCheck.

Contents

Installing Sophos Anti-Virus

Using Sophos Anti-Virus

Configuring Sophos Anti-Virus

Updating Sophos Anti-Virus

Dealing with viruses

Other information

Read this first

This manual describes how to install and use Sophos Anti-Virus for on-demand and on-access scanning.

Note that the on-access scanning described in this manual is carried out on the local machine. If you prefer to protect networked Windows 95/98 machines with server based on-access scanning, consult the 'Installing networked InterCheck clients' chapter of the 'InterCheck Advanced User Guide', which is available on the Sophos Anti-Virus CD or website.

About Sophos Anti-Virus

This chapter introduces Sophos Anti-Virus and describes its key features.

What is Sophos Anti-Virus?

Sophos Anti-Virus provides virus checking, automatic reporting and disinfection for individual PCs and entire networks.

How does it work?

Sophos Anti-Virus divides virus checking between two components:

- **SWEEP** provides on-demand scanning of disks, files and documents.
- **InterCheck** checks each item as the user attempts to access it and grants access only if it is virus-free.

About SWEEP

SWEEP is a virus-specific scanner that detects all viruses known to Sophos at the time of release.

It can provide immediate or scheduled scanning of workstations or file servers, and can also be used to deal with requests for on-access virus-checking (see 'About InterCheck' below).

Monthly updates are available by post or from the Sophos website.

About InterCheck

InterCheck ensures that unknown items (e.g. programs, documents, email attachments or Internet downloads) cannot be used until checked for viruses.

How does InterCheck work?

InterCheck splits the task of file authorisation into two processes:

Monitoring all file and disk accesses

Whenever a user attempts to access an item, InterCheck compares it with a list of authorised items. If a match is found, access is permitted; if not, the item is scanned for viruses.

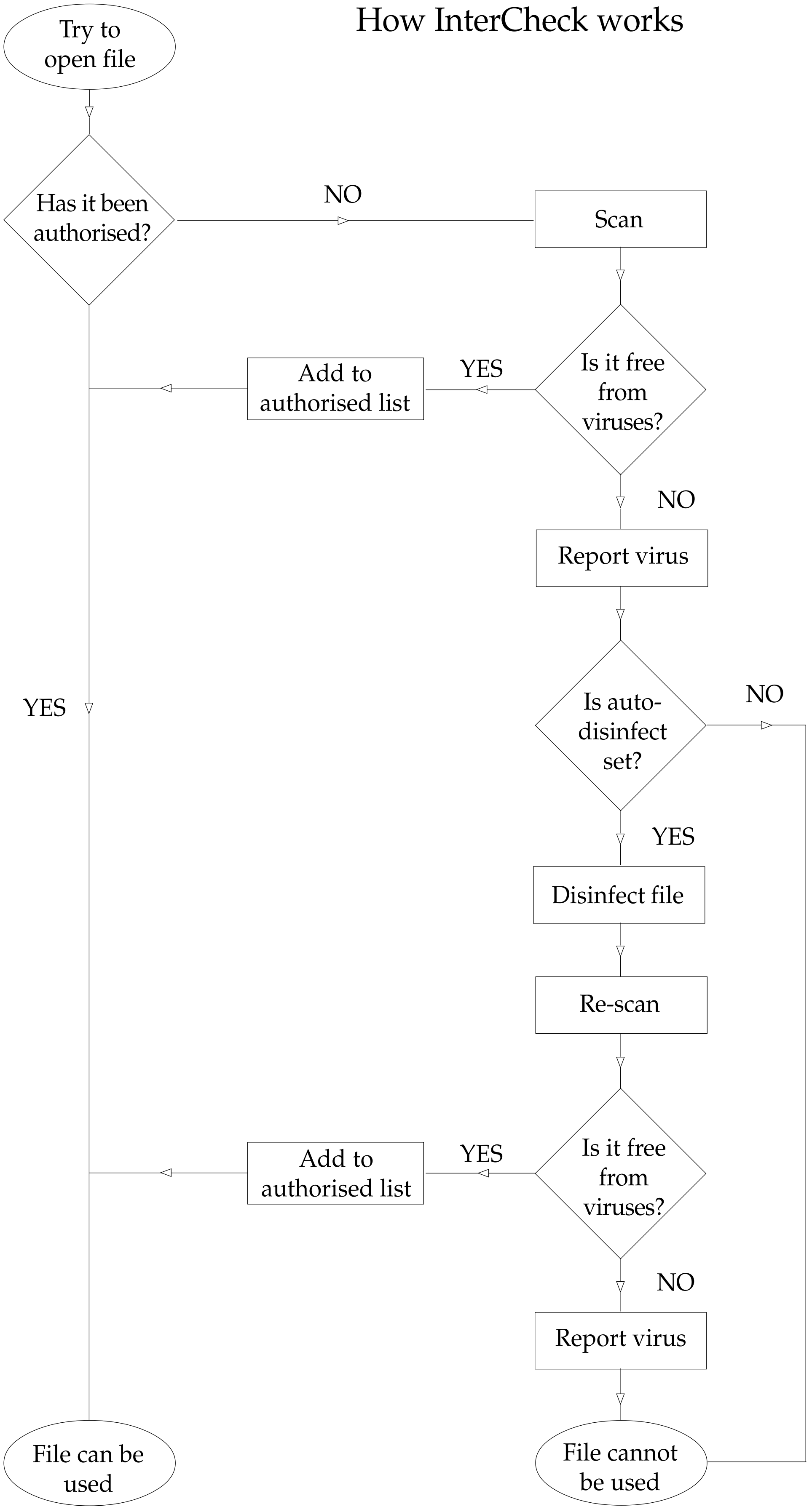
Scanning unknown items

InterCheck sends any unknown item for scanning.

If the item is virus-free, it is added to the list of authorised items (checksum file) and access is granted. Unless the item is modified, users can subsequently access it without further authorisation.

If a virus is found, InterCheck reports the virus and denies access. However, if automatic disinfection has been set up, any item that can be disinfected (documents or floppy disk boot sectors) is cleaned and scanned again. If the item is now virus-free, access can go ahead.

How InterCheck works



About installation

This chapter describes issues to consider before installing Sophos Anti-Virus.

System requirements

- At least 8 Mb of RAM.
- At least 4 Mb hard disk space.

Which kind of installation?

There are two kinds of installation:

On a single or stand-alone workstation

In this case, you install Sophos Anti-Virus directly from the CD (this is known as a local installation). See the 'Installation on a single workstation' chapter.

On networked workstations

In this case, you can install Sophos Anti-Virus on multiple machines across the network. There are two steps:

1. Copy the installation files from CD onto a file server (this is known as a central installation).
2. Make working installations on each workstation from these central installation files.

This approach allows easy distribution and automatic updating. See the 'Installation on a network' chapter.

Installation on a single workstation

This chapter describes how to install Sophos Anti-Virus on a single or stand-alone workstation.

Important! Before you install Sophos Anti-Virus, you should uninstall any other anti-virus program.

Starting the installation program

Start Windows 95/98 and insert the Sophos Anti-Virus CD in the CD drive.

If auto-run is enabled for the CD drive, the CD will auto-start.

If auto-run is not enabled, run

```
D:\Launchcd
```

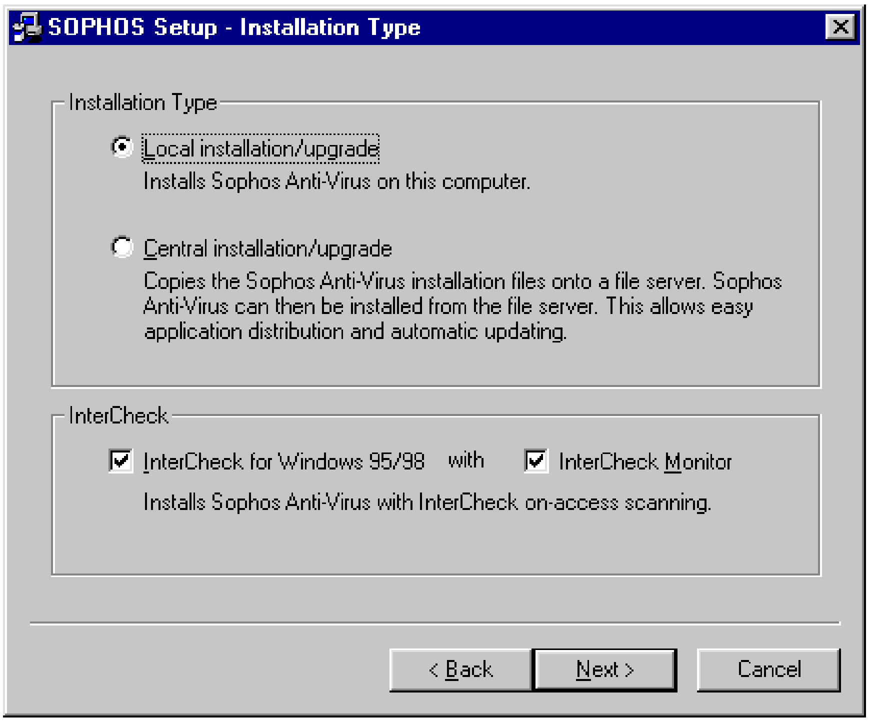
where D: is the CD drive.

To start the installation program, select *Quick installation* at the Sophos Anti-Virus screen.

Installation

The installation program presents the following setup screens.

Installation type



SOPHOS Setup - Installation Type

Installation Type

● Local installation/upgrade
Installs Sophos Anti-Virus on this computer.

○ Central installation/upgrade
Copies the Sophos Anti-Virus installation files onto a file server. Sophos Anti-Virus can then be installed from the file server. This allows easy application distribution and automatic updating.

InterCheck

☑ InterCheck for Windows 95/98 with ☑ InterCheck Monitor
Installs Sophos Anti-Virus with InterCheck on-access scanning.

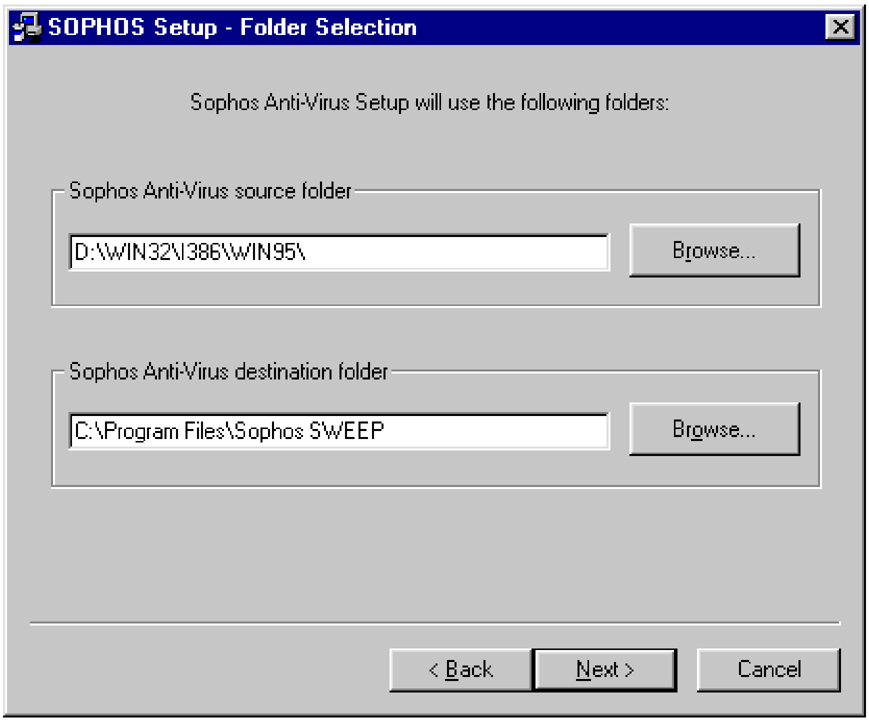
Installation Type

Select ‘Local installation/upgrade’ to install Sophos Anti-Virus on the workstation.

InterCheck

Select ‘InterCheck for Windows 95/98’ to provide local on-access scanning on the workstation. Select ‘InterCheck Monitor’ if you want this monitor to be displayed each time InterCheck is started.

Folder selection



Sophos Anti-Virus Setup will use the following folders:

Sophos Anti-Virus source folder: D:\WIN32\I386\WIN95\

Sophos Anti-Virus destination folder: C:\Program Files\Sophos SWEEP

Sophos Anti-Virus source folder

Confirm the Sophos Anti-Virus source folder. This is the folder on the CD that contains the installation files.

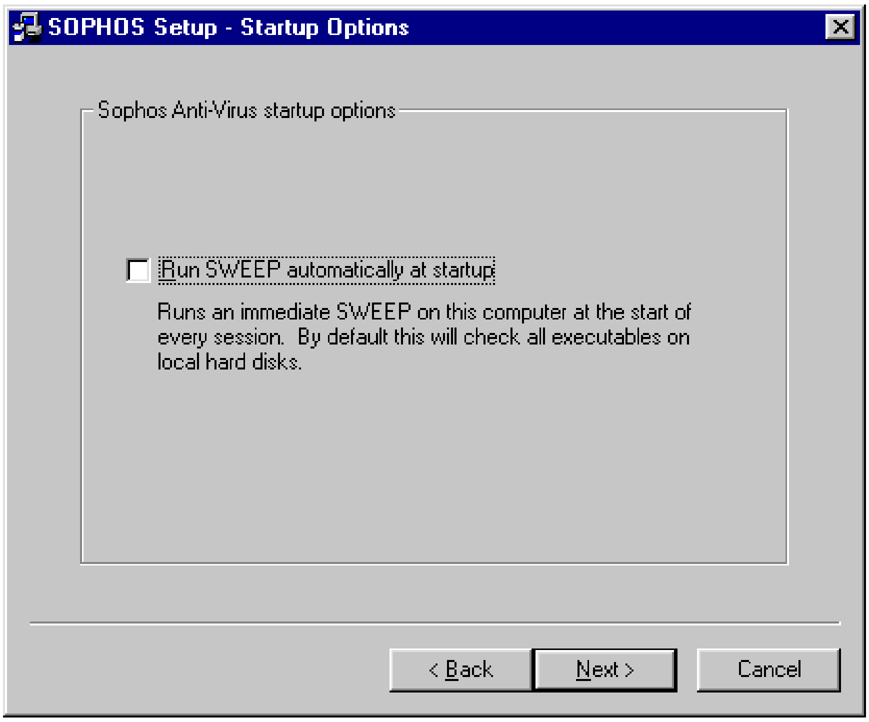
Sophos Anti-Virus destination folder

Confirm or specify the folder on the local hard disk where Sophos Anti-Virus will be installed. The default is C:\Program Files\Sophos SWEEP.

If you selected 'InterCheck for Windows 95/98', you will now see the last setup screen (see 'Completing installation' below).

Startup options

This screen appears only if 'InterCheck for Windows 95/98' was not selected.



SOPHOS Setup - Startup Options

Sophos Anti-Virus startup options

□ Run SWEEP automatically at startup

Runs an immediate SWEEP on this computer at the start of every session. By default this will check all executables on local hard disks.

Sophos Anti-Virus startup options

Select 'Run SWEEP automatically at startup' to perform an immediate scan at the start of every session. By default, this will check all executables on all local hard disks. However, you can later modify what is checked (see the 'Immediate scanning' section of the 'Using Sophos Anti-Virus' chapter.)

Completing installation

You will see a summary of the actions the installation program is going to take. Click *Finish* to complete the installation.

When you restart the workstation, InterCheck on-access scanning will start (if you selected it during installation) and the system will be checked for viruses.

Installation on a network

This chapter describes how to install Sophos Anti-Virus across a network.

Important! Before you install Sophos Anti-Virus, you should uninstall any other anti-virus program.

About network installation

Network installation involves two steps:

1. Central installation.
This places the installation files on a file server.

2. Workstation installation.
This makes working installations of Sophos Anti-Virus on Windows 95/98 workstations.

Step 1: Central installation

The central installation can be made on a Windows 95/98 machine or on a non-Windows 95/98 machine, e.g. a Windows NT file server.

On a Windows 95/98 machine, insert the Sophos Anti-Virus CD.

If auto-run is enabled, the CD will auto-start. If auto-run is not enabled, run

```
D:\Launchcd
```

where D: is the CD drive. Then select *Quick installation* at the Sophos Anti-Virus screen.

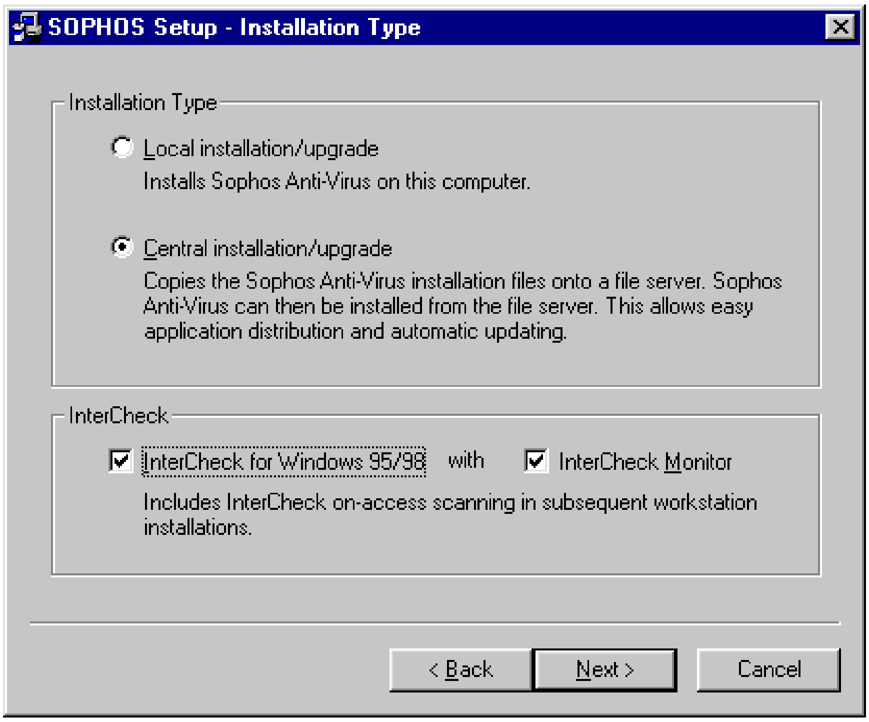
If using another platform, insert the Sophos Anti-Virus CD and run

```
D:\Win32\I386\Win95\Setup.exe
```

where D: is the CD drive.

The installation program will present the following setup screens.

Installation type



SOPHOS Setup - Installation Type

Installation Type

○ Local installation/upgrade

Installs Sophos Anti-Virus on this computer.

● Central installation/upgrade

Copies the Sophos Anti-Virus installation files onto a file server. Sophos Anti-Virus can then be installed from the file server. This allows easy application distribution and automatic updating.

InterCheck

☑ InterCheck for Windows 95/98 with ☑ InterCheck Monitor

Includes InterCheck on-access scanning in subsequent workstation installations.

Installation Type

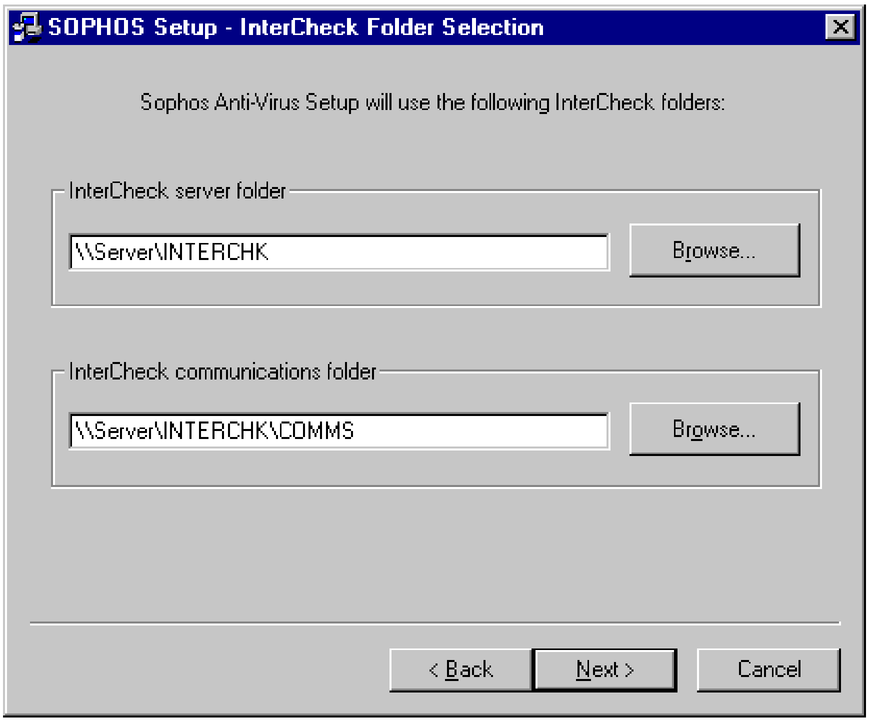
Select 'Central installation/upgrade' to place the installation files on the file server.

InterCheck

Select 'InterCheck for Windows 95/98' to install on-access scanning as part of subsequent local installations. Select 'InterCheck Monitor' if you want this monitor to be displayed on the workstations each time InterCheck is started.

InterCheck folder selection

This screen appears only if ‘InterCheck for Windows 95/98’ was selected.



SOPHOS Setup - InterCheck Folder Selection

Sophos Anti-Virus Setup will use the following InterCheck folders:

InterCheck server folder: \\Server\INTERCHK

InterCheck communications folder: \\Server\INTERCHK\COMMS

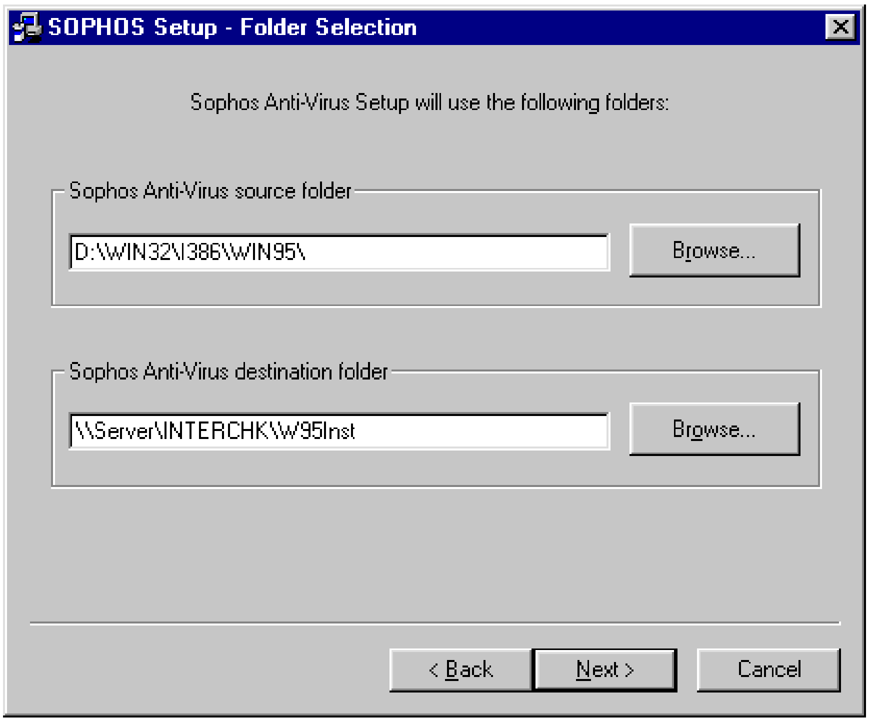
InterCheck Server folder

Specify the folder for the InterCheck configuration file here. If an InterCheck Server is being used on the network for central reporting, the configuration file is normally in the folder from which it is run (e.g. INTERCHK on NT servers, SWEEP on NetWare servers). If you specify a folder that does not include a configuration file, one will be created. For information on the configuration file, see the ‘Configuring InterCheck’ chapter.

InterCheck communications folder

If an InterCheck Server is being used, this folder is used for communicating with it. The communications folder is normally a subfolder of the InterCheck Server folder. If an InterCheck Server is not being used, leave this blank, ignore any warning and click ‘Next’ again.

Folder selection



SOPHOS Setup - Folder Selection

Sophos Anti-Virus Setup will use the following folders:

Sophos Anti-Virus source folder: D:\WIN32\I386\WIN95\

Sophos Anti-Virus destination folder: \\Server\INTERCHK\W95Inst

Sophos Anti-Virus source folder

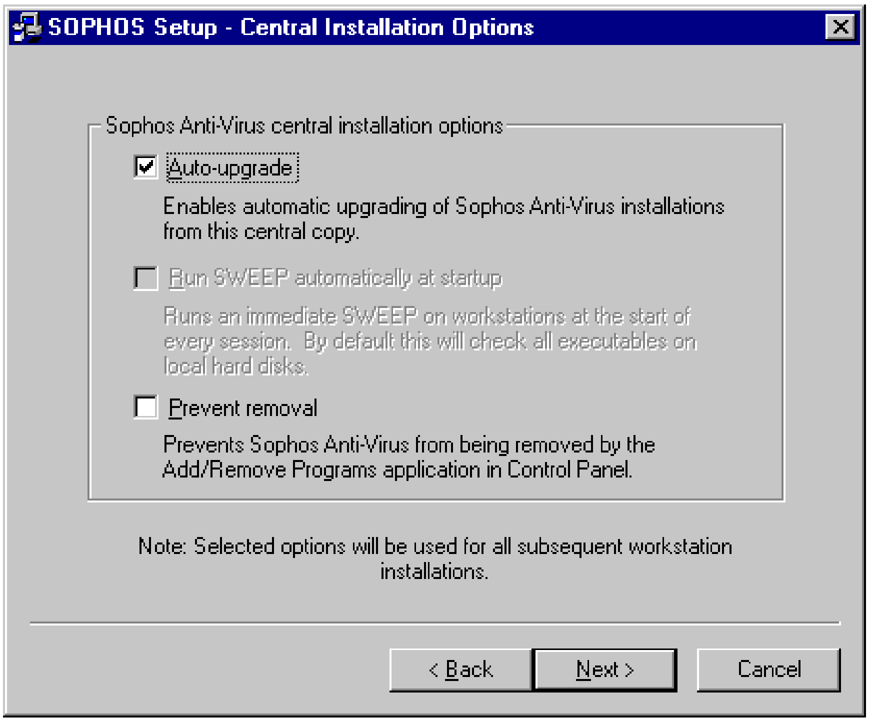
Confirm the source folder. This is the folder on the CD that contains the installation files.

Sophos Anti-Virus destination folder

The destination folder is the folder on the network drive to which the installation files will be copied. This folder must be visible to users.

If you selected ‘InterCheck for Windows 95/98’ earlier, the default folder is W95inst below the InterCheck Server folder (see previous screen).

Central installation options



Sophos Anti-Virus central installation options

☑ Auto-upgrade

Enables automatic upgrading of Sophos Anti-Virus installations from this central copy.

☐ Run SWEEP automatically at startup

Runs an immediate SWEEP on workstations at the start of every session. By default this will check all executables on local hard disks.

☐ Prevent removal

Prevents Sophos Anti-Virus from being removed by the Add/Remove Programs application in Control Panel.

Note: Selected options will be used for all subsequent workstation installations.

Auto-upgrade

Select this if you want subsequent workstation installations to be updated automatically whenever the central installation is updated on the server. See also the 'Updating on a network' chapter.

Run SWEEP automatically at startup

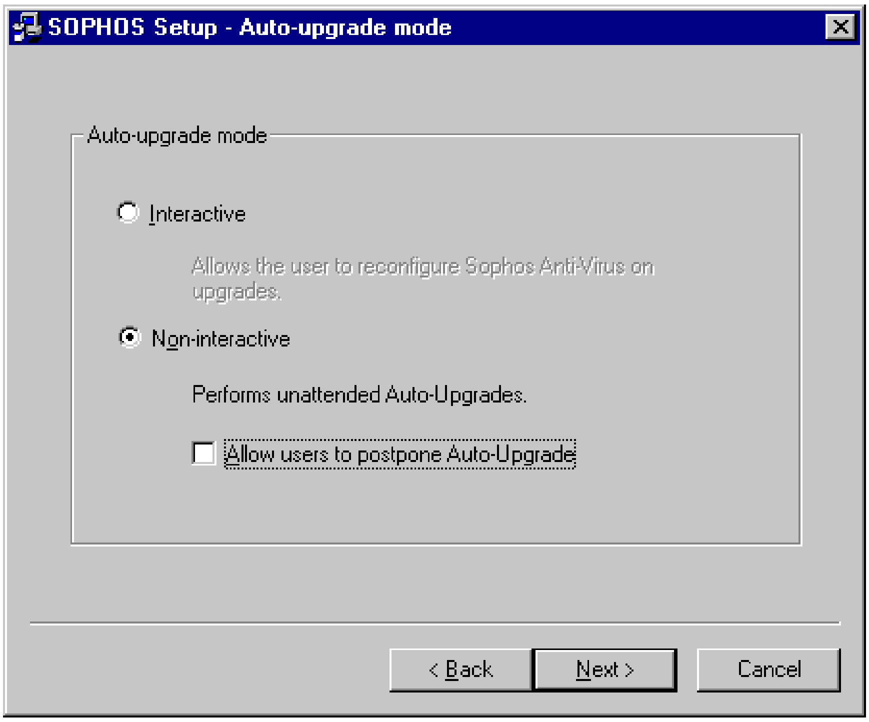
Select this if you want subsequent workstation installations to run SWEEP at the start of each session. This option is available only if 'InterCheck for Windows 95/98' was deselected earlier.

Prevent removal

Select this to ensure that subsequent workstation installations cannot be removed via *Add/Remove Programs* in Control Panel.

Auto-upgrade mode

This screen appears only if ‘Auto-upgrade’ was selected.



○ Interactive

Allows the user to reconfigure Sophos Anti-Virus on upgrades.

● Non-interactive

Performs unattended Auto-Upgrades.

□ Allow users to postpone Auto-Upgrade

Interactive

This will allow the user to reconfigure Sophos Anti-Virus when it is updated.

Non-interactive

Sophos Anti-Virus will be updated from the file server automatically. The user will not be able to reconfigure it. This is the recommended option.

Allow users to postpone Auto-upgrade

If you selected ‘Non-interactive’ updating, you can allow users to postpone the update. Users will be informed when a new version of Sophos Anti-Virus is available and asked if they wish to go ahead. This option is recommended only where users will be connecting over slow links, e.g. via modems.

Completing central installation

You will see a summary of the actions the installation program is going to take. Click *Finish* to complete the installation.

You are now ready to install Sophos Anti-Virus on the workstations.

Step 2: Workstation installation

In step 2, you make workstation installations from the central installation files. This can be done automatically from a login script, or manually at each workstation.

Automatic installation

Workstation installations can be made from the central installation automatically via a login script.

Run Setup.exe from the central installation by entering

```
\\Server\INTERCHK\W95Inst\Setup -INL -A
```

in the workstations' login script, where *Server* is the name of the server and INTERCHK\W95Inst is the path to the directory in which the Sophos Anti-Virus files were placed.

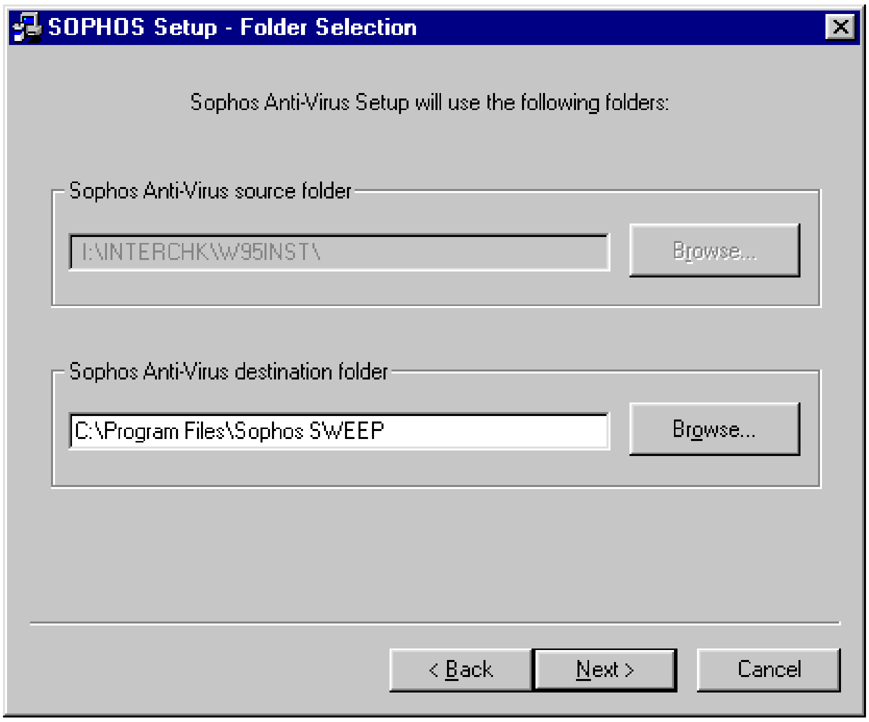
Note: This line should be placed before any call to ICLOGIN in the login script. This is to ensure that local InterCheck on-access scanning is installed, rather than a copy of InterCheck that is run from your file server.

When each workstation logs in, Sophos Anti-Virus will be installed in a folder called Sophos SWEEP within the Windows 95/98 program folder.

InterCheck on-access scanning will start (if selected during installation) and the workstation will be checked for viruses.

Manual installation

On the workstation, run Setup.exe from the folder on the file server where the installation files are held. The 'Folder Selection' screen will appear.



SOPHOS Setup - Folder Selection

Sophos Anti-Virus Setup will use the following folders:

Sophos Anti-Virus source folder: I:\INTERCHK\W95INST\

Sophos Anti-Virus destination folder: C:\Program Files\Sophos SWEEP

Sophos Anti-Virus source folder

This is the location of the central installation directory and cannot be changed.

Sophos Anti-Virus destination folder

This is the folder on the workstation where Sophos Anti-Virus will be installed.

Next you will see a summary of the actions the installation program is going to take. Click *Finish* to complete installation.

When the workstation is restarted, InterCheck on-access scanning will start (if selected during installation) and the workstation will be checked for viruses.

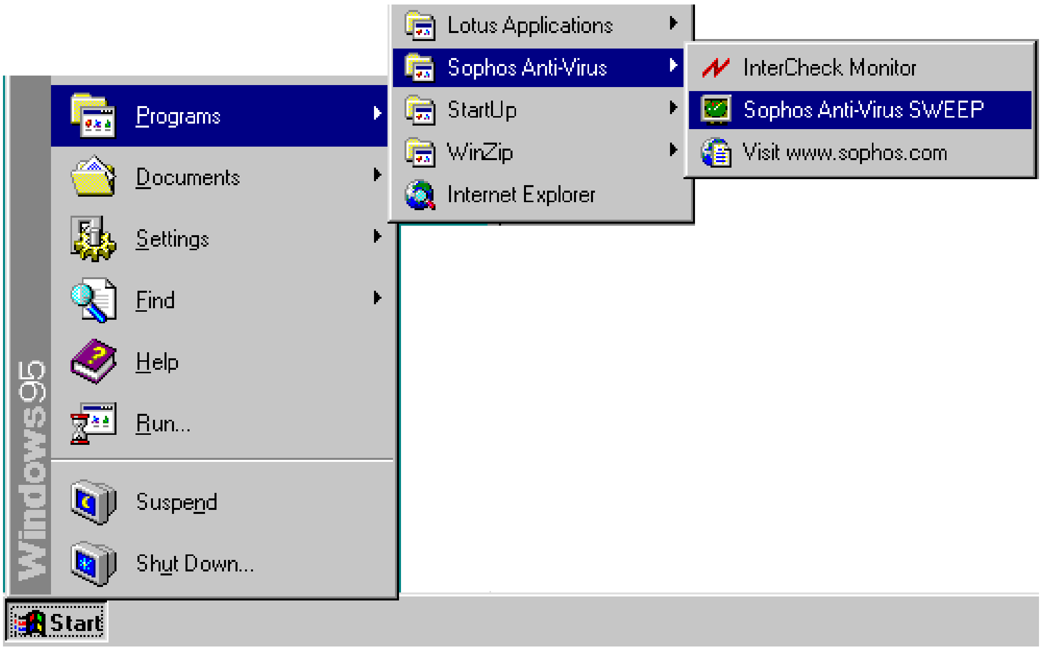
Using Sophos Anti-Virus

This chapter describes how to start the Sophos Anti-Virus GUI, set up immediate or scheduled scanning, and monitor on-access scanning.

It also describes how to test Sophos Anti-Virus and how to close the Sophos Anti-Virus GUI.

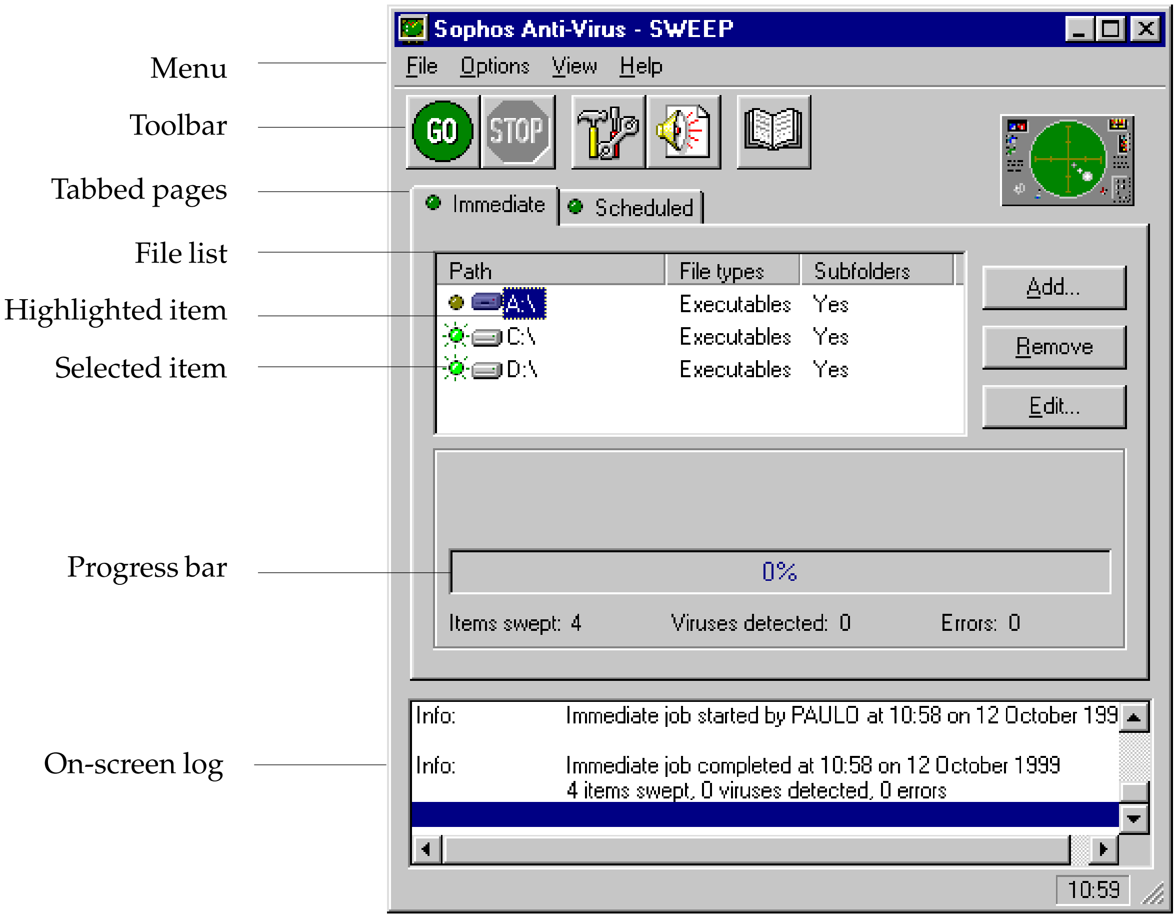
Starting Sophos Anti-Virus

To start Sophos Anti-Virus, click *Start* | *Programs* | *Sophos Anti-Virus* | *Sophos Anti-Virus SWEEP*.



The main Sophos Anti-Virus screen appears.

Overview of the main display



Path	File types	Subfolders
A:\	Executables	Yes
C:\	Executables	Yes
D:\	Executables	Yes

Items swept: 4 Viruses detected: 0 Errors: 0

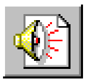
```
Info:    Immediate job started by PAULO at 10:58 on 12 October 199
Info:    Immediate job completed at 10:58 on 12 October 1999
         4 items swept, 0 viruses detected, 0 errors
```

Icon toolbar

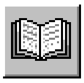
The icons provide short-cuts to commonly used menu options.

Starts scanning. The STOP icon ends scanning.

Lets you configure the immediate or scheduled job.



Lets you set up and configure virus alerts, e.g. notification by email.



Displays the virus library.

Tabbed pages

There is a tabbed page for each scanning mode. A light on the left of each tab is illuminated when that form of scan is being run.

Immediate for scanning on demand.

Scheduled for scanning automatically at set times.

File list

On the **Immediate** page, the file list shows the drives, paths and files that can be scanned on demand.

On the **Scheduled** page, the file list is replaced by the scheduled job list.

An 'active' light indicates currently selected items. Click on the light to select or deselect items.

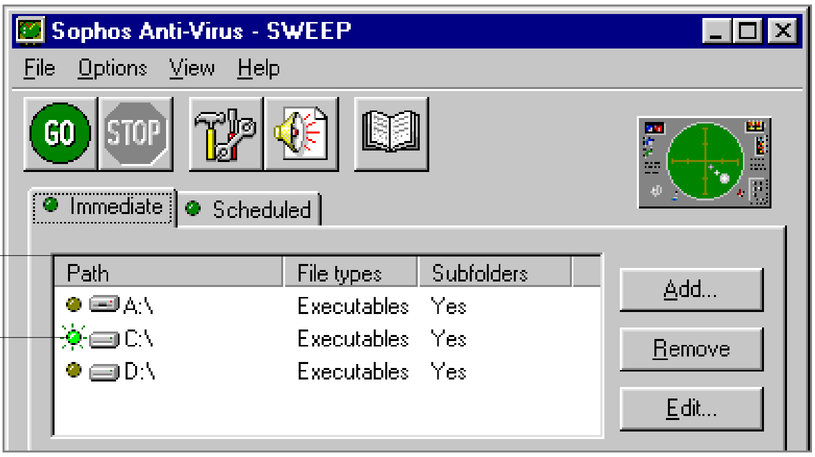
On-screen log

This contains information about the current session, along with all log messages since Sophos Anti-Virus was started.

It appears after a job is started for the first time.

Immediate scanning

To scan files or drives now, ensure that the Immediate tab is selected.



Path	File types	Subfolders
● A:\	Executables	Yes
● C:\	Executables	Yes
● D:\	Executables	Yes

File list

Selected item

The file list shows items that can be included in scans. An 'active' light to the left of an item indicates that it is selected and will be scanned. Click on the light to select or deselect items.

Starting an immediate scan

To scan all the selected drives, paths and files, click the *GO* icon.

Alternatively, select *Sweep* from the *File* menu.

Hint: To scan any individual item in the immediate mode display, double-click on its icon in the file list.

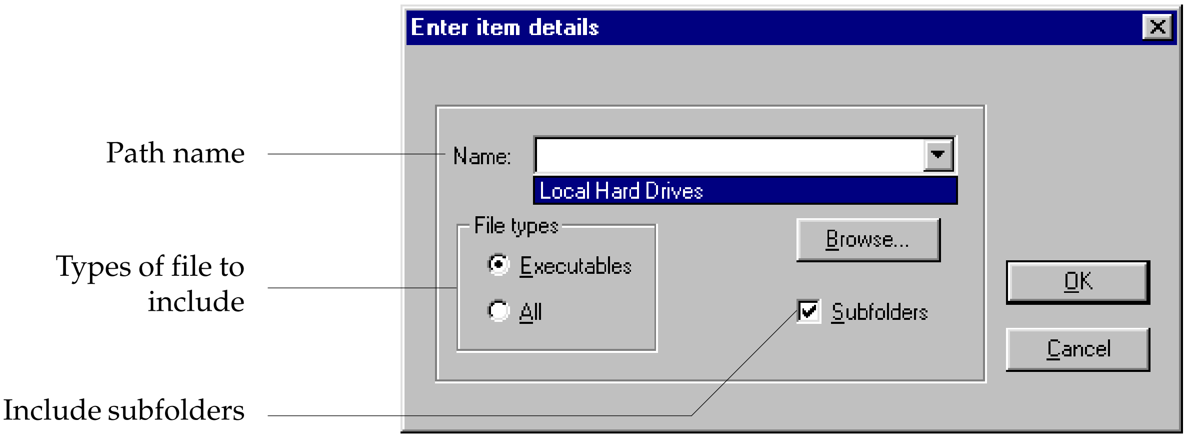
Note: You can test virus detection. See the 'Testing Sophos Anti-Virus' section of this chapter for details.

Default immediate mode file list

By default, all local drives are included in the file list on the Immediate page, and all local hard drives are selected for scanning. You can change the items in the file list as described below.

Adding new items for immediate scanning

To add new items for immediate scanning, click *Add*. This will display the new item details dialog.



Name: Local Hard Drives

File types: ● Executables ○ All

☑ Subfolders

Name

Specify the drive, folder or file to be scanned. Both mapped and UNC path names can be entered and wildcards can be included. Alternatively, use *Browse* to select from available items, or use the drop-down menu to select all 'Local hard drives'.

File types

Only files defined as executables will be scanned, unless 'All' is selected. See 'Executables' in the 'Administration options' chapter for information on changing the files defined as executables.

Subfolders

Subfolders will be scanned if this option is selected.

Removing or editing items for immediate scanning

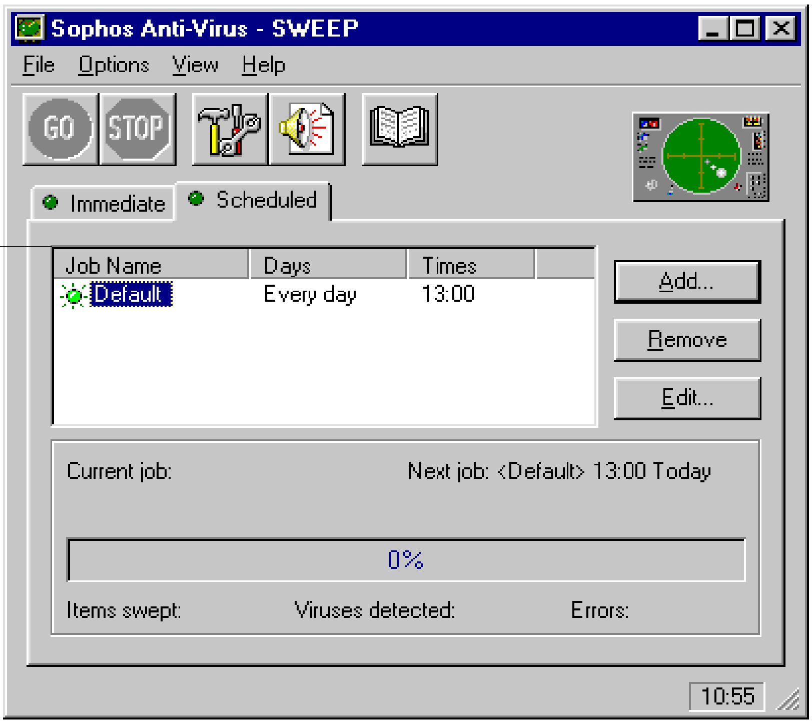
To remove an item, click on its path name to highlight it. Then click *Remove*.

To edit the details of an item in the file list, highlight its path name and click *Edit*. This will display the 'Enter item details' dialog, as described above.

Scheduled scanning

To set up scheduled scans, select the Scheduled tab.

Scheduled jobs are listed on the page. An ‘active’ light to the left of a job indicates that it is selected and will run. Click on this light to select or deselect jobs.



Scheduled job list

Job Name	Days	Times
Default	Every day	13:00

Current job:

Next job: <Default> 13:00 Today

0%

Items swept:

Viruses detected:

Errors:

10:55

Default scheduled mode job list

By default, a job named ‘Default’ is created. This will scan the system at 13:00 every day (12:00 with Japanese regional settings).

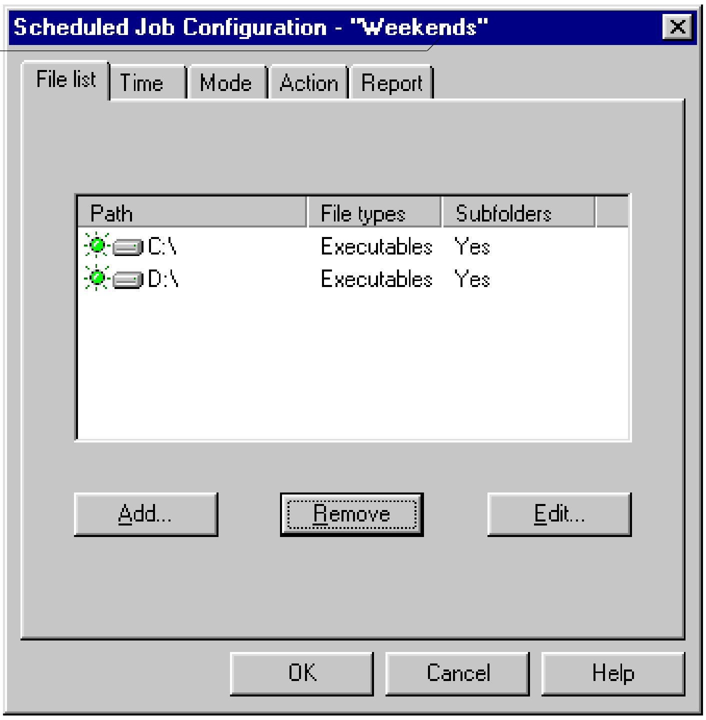
You can set up new scheduled jobs or modify existing jobs as described below.

Adding a new scheduled job

To add a new scheduled job, click *Add* on the scheduled mode page.

You will be prompted for a job name. Enter a name and click *OK*.

The scheduled mode configuration pages will appear.



Path	File types	Subfolders
C:\	Executables	Yes
D:\	Executables	Yes

Scheduled job name

Use the 'File list' and 'Time' tabbed pages to specify what is scanned and when. For full details, see the 'Configuring Sophos Anti-Virus' chapter.

Removing a scheduled job

Highlight the name of the job to be removed on the scheduled mode page and click *Remove*.

Editing a scheduled job

Highlight the name of the job to be edited and click *Edit*. This will display the scheduled mode configuration pages, as described in the 'Configuring Sophos Anti-Virus' chapter.

On-access scanning

InterCheck starts automatically each time Windows 95/98 is started, before any network connections are made. The InterCheck monitor also becomes active, provided that 'InterCheck monitor' was selected during installation.

InterCheck intercepts all access to program files. The renaming of program files is not intercepted, so files can be renamed or moved within a logical drive without being checked.

InterCheck for Windows 95/98 disables access to floppy disks infected with a boot sector virus.

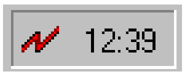
Using the InterCheck monitor

Starting the monitor

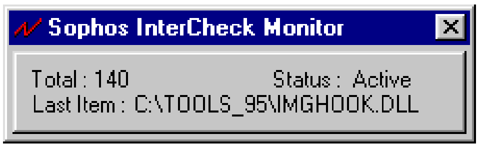
If enabled during installation, the monitor becomes active by default at Windows start-up.

To start the monitor at any other time (i.e. if it has been closed down), click *Start* | *Programs* | *Sophos Anti-Virus* | *InterCheck Monitor.*

While active, the InterCheck monitor can be displayed by double-clicking its icon in the right-hand corner of the Windows taskbar.



The monitor display

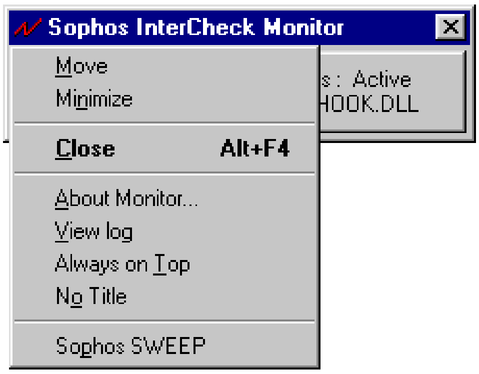


Total : 140 Status : Active
Last Item : C:\TOOLS_95\IMGHOOK.DLL

The monitor displays the total number of items filtered (i.e. checked against the list of authorised items), the status of InterCheck (active or inactive), and the name of the last item filtered.

InterCheck monitor options

Click the upper left hand corner of the InterCheck monitor window title bar to display a list of options.



Minimize

If selected, the monitor window is minimized.

Close

If selected, the monitor window will be closed, but InterCheck will remain active. Note that clicking on ☒ will minimise the window, not close it.

View log

If selected, displays a log of files checked and any viruses found during the initial check at start-up.

Always on top

If selected, the monitor remains visible when other windows are opened.

No Title

If selected, the InterCheck monitor window title bar disappears. To restore the title bar, double-click inside the InterCheck monitor window.

Sophos SWEEP

If selected, this starts the Sophos Anti-Virus GUI.

Testing Sophos Anti-Virus

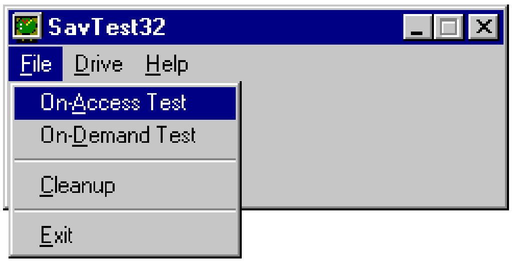
You can test Sophos Anti-Virus with the SavTest32 utility.

Insert the Sophos Anti-Virus CD and locate the Tools\SavTest folder. Open this folder and double-click on SavTest32.exe.

The 'SavTest 32' screen appears.

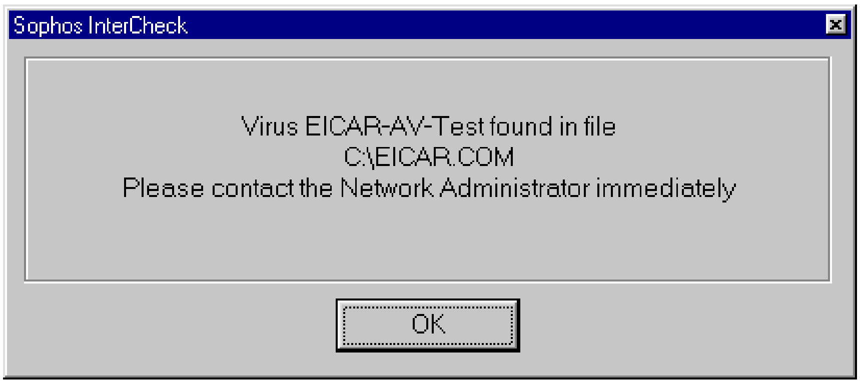
Testing on-access scanning

At the 'SavTest32' screen, select *On-Access test*.



SavTest will create a test file called eicar.com in the root of the C: drive (or in the drive you specify from the 'Drive' menu). This file is a standard test and is **not** infected with a virus.

InterCheck will report a virus find.

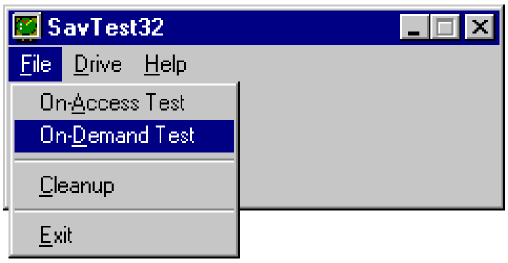


Virus EICAR-AV-Test found in file
C:\EICAR.COM
Please contact the Network Administrator immediately

Click *OK*. You will then see confirmation that on-access scanning is functioning normally.

Testing on-demand scanning

At the 'SavTest32' screen, choose *On-Demand Test*.



SavTest will create a test file called eicar.com in the root of the C: drive (or the drive you specify from the 'Drive' menu). This file is a standard test and is **not** infected with a virus.

Note: If InterCheck on-access scanning is running on your machine, it will issue a virus warning as soon as eicar.com is created. Click *OK* to continue.

SavTest prompts you to run a scan. Click *OK*.

Start the Sophos Anti-Virus GUI. At the Immediate tabbed page, add C:\eicar.com to the file list and ensure that this is the only item selected for scanning.

Click *GO* to run a scan.

Sophos Anti-Virus will report EICAR-AV-TEST in the on-screen log.

Other SavTest32 options

Drive

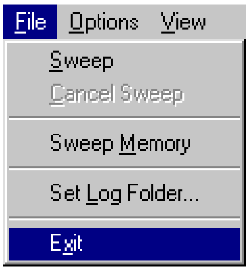
You can specify where the eicar.com test file will be created. Select *Drive* from the menu bar and use the browser to choose a location.

Cleanup

To remove an eicar.com test file, select *Cleanup* from the File menu. Note that the test file is usually deleted automatically after a test.

Closing down the Sophos Anti-Virus GUI

Select *Exit* from the *File* menu to close down the Sophos Anti-Virus GUI.



Sophos Anti-Virus may remind you that scheduled scans will not be run if you close down the GUI. (This warning appears if you have added or changed scheduled jobs at any time).

Configuring Sophos Anti-Virus

This chapter describes how to configure scanning, disinfection and reporting for immediate and scheduled jobs.

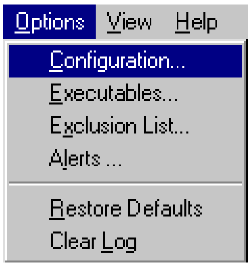
Note: If you want to configure on-access scanning, see the 'Configuring InterCheck' chapter.

About configuration

You configure the immediate mode and the scheduled jobs separately.

Go to the Immediate tabbed page, or highlight a job on the Scheduled tabbed page. Then click the configuration icon.

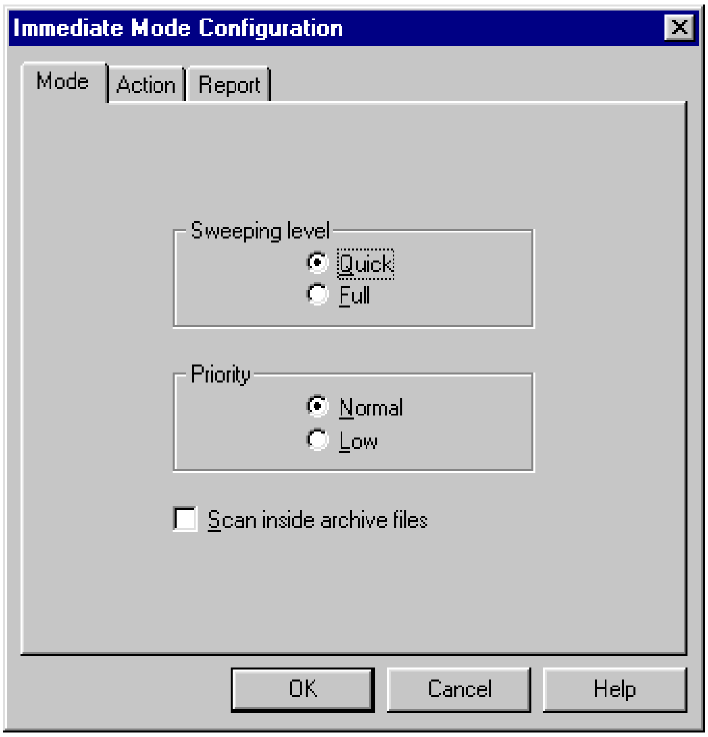
Alternatively, select *Configuration* from the *Options* menu.



The configuration tabbed pages appear.

Mode

This page allows you to configure scanning activity.



Sweeping level
● Quick
○ Full

Priority
● Normal
○ Low

□ Scan inside archive files

Sweeping level

'Quick' scanning checks only those parts of each file that are likely to contain viruses. This level is sufficient for normal operation.

'Full' scanning examines the complete contents of each file. This level is more secure because it can discover viruses buried beneath code attached to a file, minor virus mutations and corruptions.

'Full' scanning is much slower than 'Quick'.

Priority

Set Sophos Anti-Virus to run at 'Low' priority if you want to minimise the impact on system performance. Note that this will increase the time Sophos Anti-Virus takes to scan the system.

Scan inside archive files

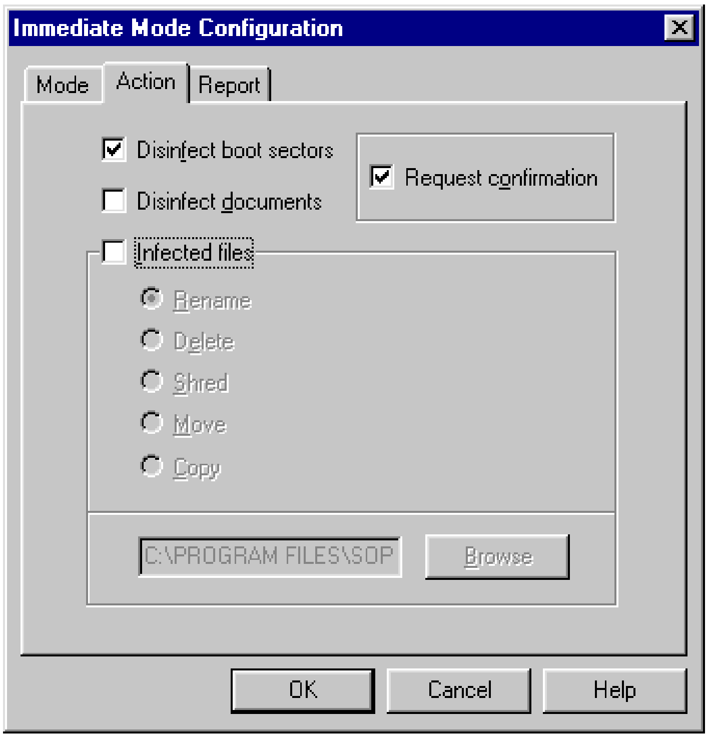
Select this if you want Sophos Anti-Virus to check for viruses inside archive files. Please see the latest readme for the full list of archive types, which includes: ZIP, ARJ, RAR, GZIP, TAR, CMZ.

Note: By default, files compressed with dynamic compression utilities (PKLite, LZEXE and Diet) are also checked.

InterCheck for Windows 95/98 does not scan archive files. However, it does provide automatic protection against viruses. When an archive is decompressed, InterCheck checks any files that the user attemps to access and denies access if they are infected.

Action on virus detection

This page allows you to choose how Sophos Anti-Virus will deal with infected items.



☑ Disinfect boot sectors

□ Disinfect documents

☑ Request confirmation

□ Infected files

● Rename

○ Delete

○ Shred

○ Move

○ Copy

C:\PROGRAM FILES\SOP

Disinfect boot sectors

Sophos Anti-Virus can disinfect most boot sector viruses from floppy disks. It will not automatically disinfect hard disk boot sectors. See the 'Treating viral infection' chapter for information on manual disinfection of boot sectors.

Disinfect documents

Sophos Anti-Virus can disinfect documents infected with certain types of macro viruses. If the document disinfection fails, the infected file will be dealt with in the same way as any other infected file.

Important! Some macro viruses corrupt the infected document. Check any disinfected file carefully before using it.

Infected files

Sophos Anti-Virus can make an infected file safe in several ways other than disinfection.

Renaming or moving an executable file reduces the likelihood of it being run. Deleting or shredding the file disposes of it, so that it cannot be run by accident. Shredding is a more secure type of file deletion that overwrites the contents of the file.

If you choose to move or copy files, you can select a folder for infected files from the browser.

Note: Sophos Anti-Virus will not disinfect infected program files, as it is not possible to ensure that they are restored properly.

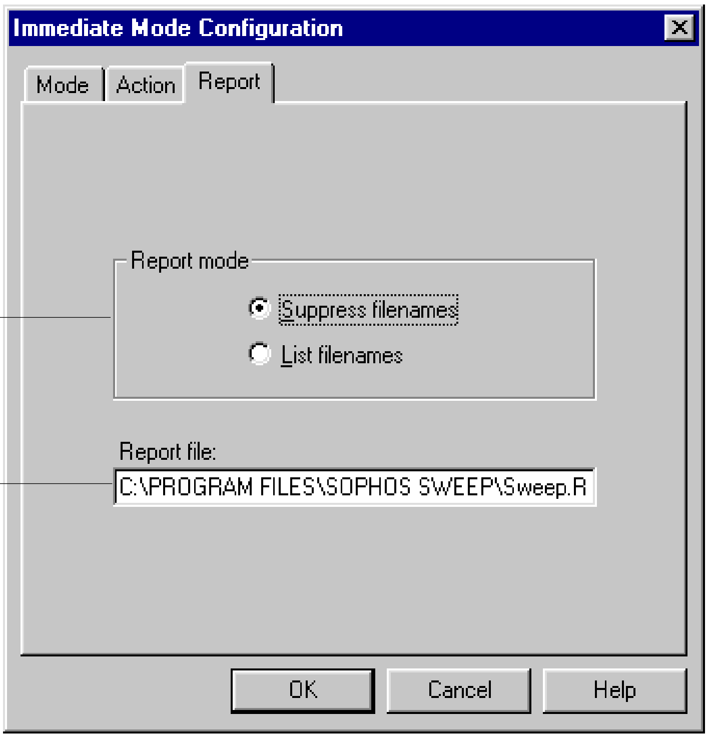
Request confirmation

If you select this option, Sophos Anti-Virus will ask for confirmation before it does anything that involves changing infected items (i.e. disinfection and renaming, deleting, shredding or moving infected files).

Note: This option is available only for immediate mode.

Report

This page allows you to configure the Sophos Anti-Virus report file for each scanning job.



Report mode
● Suppress filenames
○ List filenames

Report file: C:\PROGRAM FILES\SOPHOS SWEEP\Sweep.R

What to include in the report

Where to save the report

Sophos Anti-Virus generates a separate report file for the immediate job and for each scheduled job. This file is generated in addition to the continuous log file.

Report mode

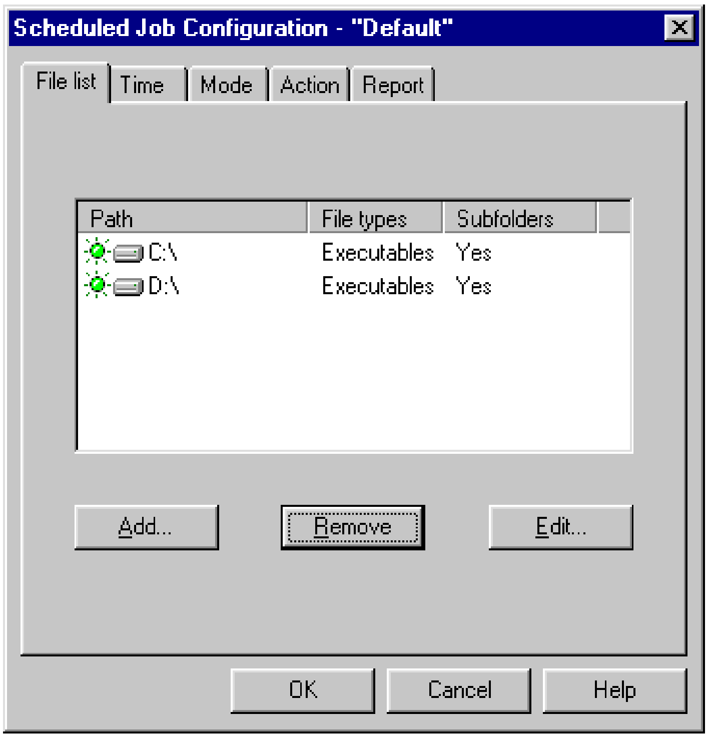
Select 'List filenames' if you want Sophos Anti-Virus to record in the report file the name of every item scanned. Otherwise only infected items are recorded.

Report file

Enter a location for the report file or accept the default. This file is deleted and recreated each time the job is run.

File list (scheduled mode only)

This page allows you to specify the files to be scanned by a scheduled job.



Scheduled Job Configuration - "Default"

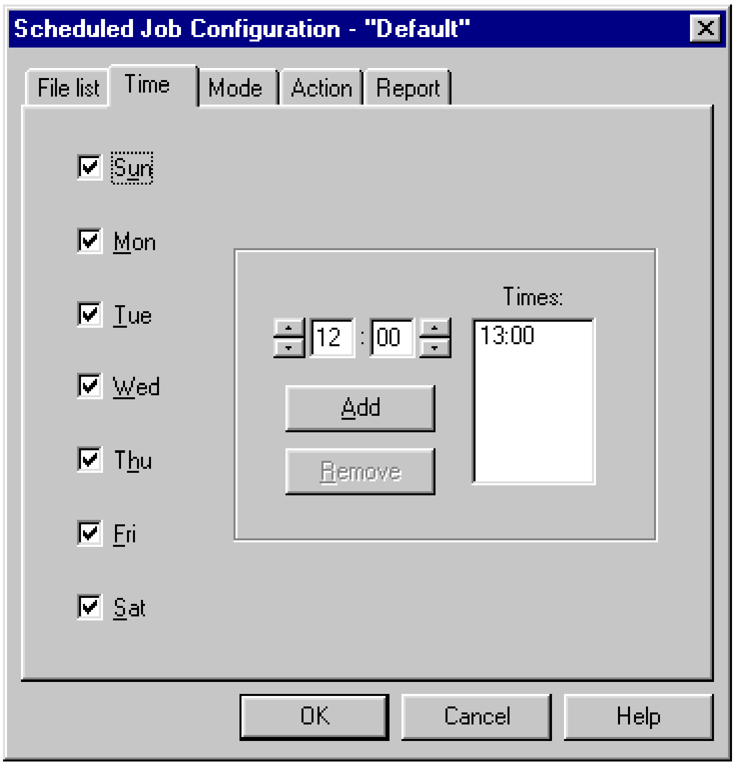
Path	File types	Subfolders
C:\	Executables	Yes
D:\	Executables	Yes

The file list is similar to the file list on the immediate mode page, but shows files to be scanned in a scheduled job. You can modify the list by using the *Add*, *Remove* and *Edit* buttons.

The default file list is the same as that for immediate mode, except that local floppy drives are not listed.

Time (scheduled mode only)

This page allows you to specify the times at which scheduled jobs will run.



Scheduled Job Configuration - "Default"

☑ Sun

☑ Mon

☑ Tue

☑ Wed

☑ Thu

☑ Fri

☑ Sat

12 : 00

Times:
13:00

Sophos Anti-Virus can be configured to run at particular times on specific days of the week. By default, a scheduled job is run at 13:00 each day.

Add

To add a time, set the time, click *Add* and then click *OK*.

Remove

To remove a time, highlight it, click *Remove* and then click *OK*.

Alert message options

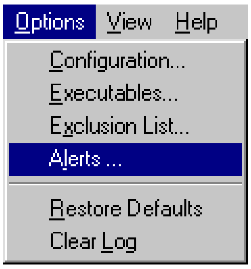
This chapter describes the options available for notifying users of scanning activity, virus finds or errors.

Note: These options apply to immediate and scheduled scanning only.

About alert message options

To display the alerts pages, click the alerts icon.

Alternatively, select *Alerts* from the *Options* menu.



There are three pages for configuring alerts: Desktop Messaging, MAPI email and SMTP email.

Each page shares a number of common features: disable notification, job specification, and notification level.

Disable notification

You can turn off the form of notification whose control page is currently selected.

Job specification

If you select the 'All jobs' option, all configuration options selected for that form of notification will apply to the immediate mode and all scheduled jobs.

The 'Specific jobs' option allows you to choose different notification settings for the immediate mode and for each individual scheduled job. If a specific job is not explicitly configured, it inherits the settings of the <default> job.

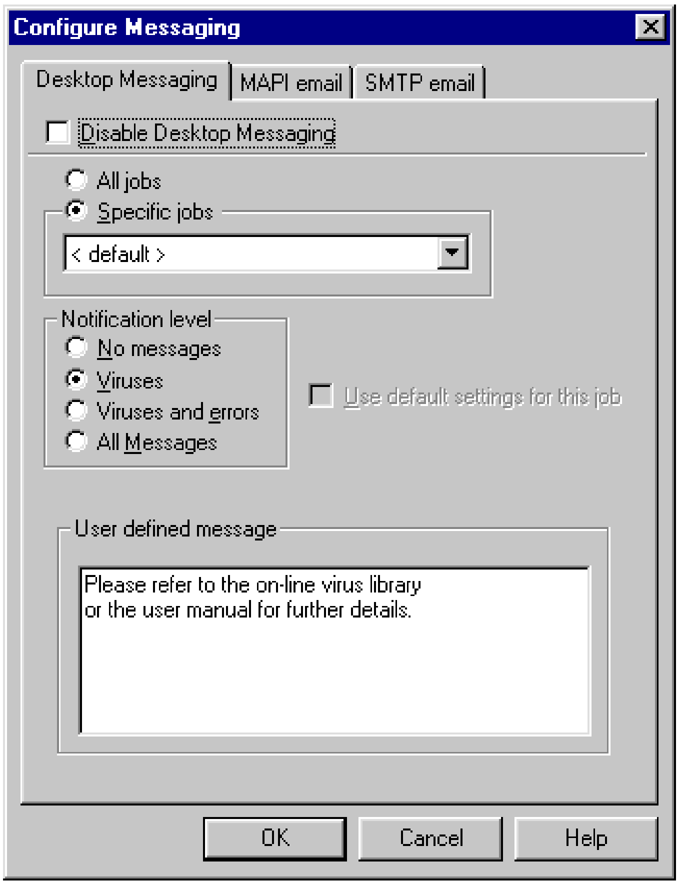
Notification level

There are four levels of notification to choose from:

- No messages.
- Virus detected messages only.
- Virus detected and error messages.
- All messages, including general information, such as the time a job started.

The notification level setting will not affect the level of information placed in the report file, the on-screen log or the log file.

Desktop messaging



Configure Messaging

□ Disable Desktop Messaging

○ All jobs
● Specific jobs

< default >

Notification level
○ No messages
● Viruses
○ Viruses and errors
○ All Messages

□ Use default settings for this job

User defined message

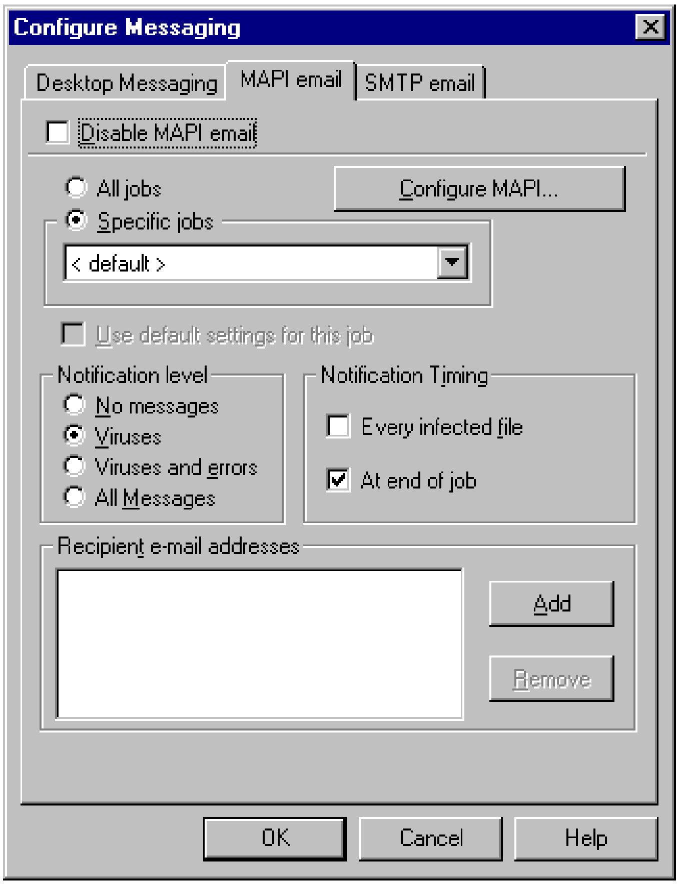
Please refer to the on-line virus library
or the user manual for further details.

Desktop Messaging controls the message displayed when a virus is discovered.

User defined message

The user defined message will be added to the end of the standard virus detected message.

MAPI email



Configure Messaging

Desktop Messaging | MAPI email | SMTP email

□ Disable MAPI email

○ All jobs

● Specific jobs

< default >

□ Use default settings for this job

Notification level

○ No messages

● Viruses

○ Viruses and errors

○ All Messages

Notification Timing

□ Every infected file

☑ At end of job

Recipient e-mail addresses

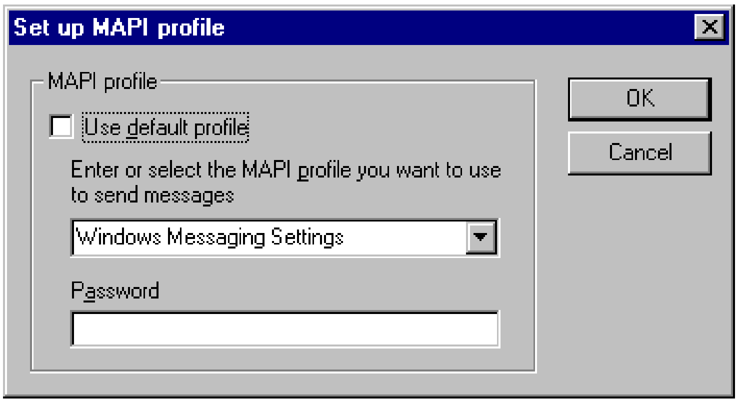
This form of notification is only available if Microsoft Exchange is installed.

You can add and remove email addresses for the recipients of the notification messages.

To send alerts, Sophos Anti-Virus must be able to log on to Exchange without supplying a password. If your default profile requires a password to be entered, do as follows.

Click *Configure MAPI*.

The ‘Set up MAPI profile’ dialog appears.



Set up MAPI profile

MAPI profile

□ Use default profile

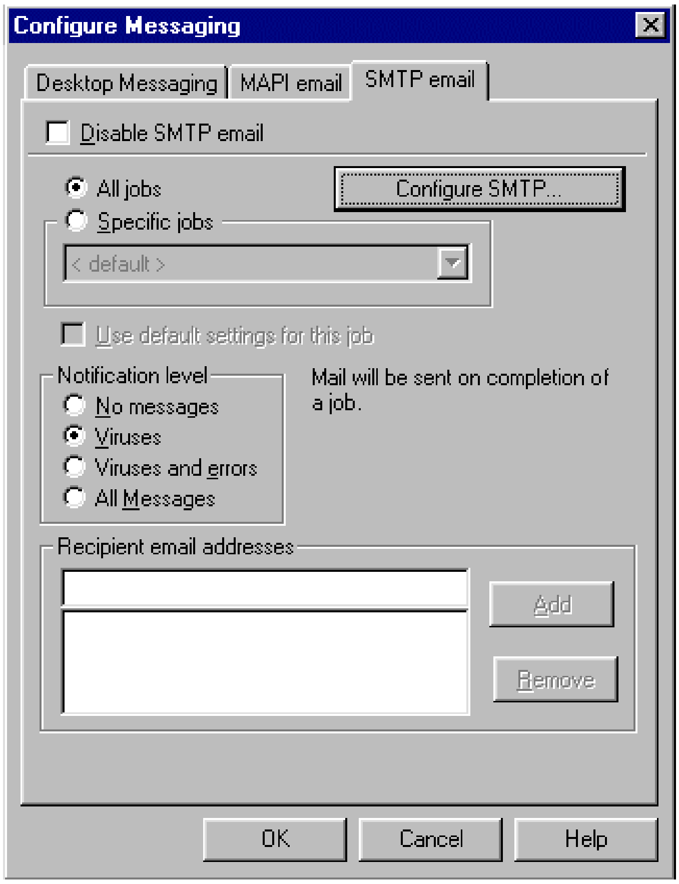
Enter or select the MAPI profile you want to use to send messages

Windows Messaging Settings

Password

Select the MAPI profile you want to use.

SMTP email



□ Disable SMTP email

● All jobs

○ Specific jobs

< default >

□ Use default settings for this job

Notification level

○ No messages

● Viruses

○ Viruses and errors

○ All Messages

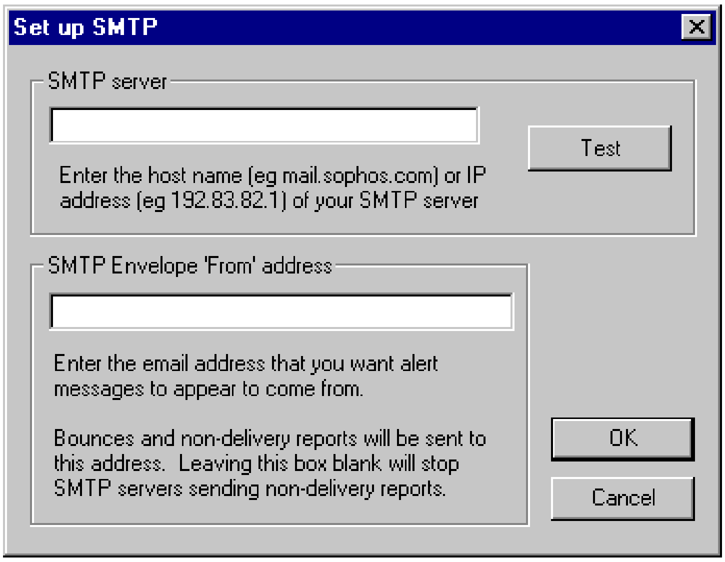
Mail will be sent on completion of a job.

Recipient email addresses

You can configure Sophos Anti-Virus to send email alerts. Mail will be sent when a scanning job has been completed.

You can add and remove email addresses for the recipients of the messages.

It is necessary to enter details of the server. Click *Configure SMTP* to open the ‘Set up SMTP’ screen (see below).



Enter the host name (eg mail.sophos.com) or IP address (eg 192.83.82.1) of your SMTP server

Enter the email address that you want alert messages to appear to come from.

Bounces and non-delivery reports will be sent to this address. Leaving this box blank will stop SMTP servers sending non-delivery reports.

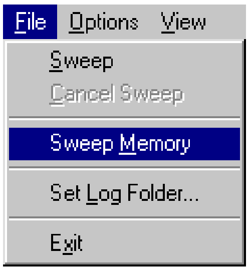
In the ‘SMTP server’ dialog, enter the host name or IP address of the SMTP server.

In ‘SMTP Envelope 'From' address’, enter the email address that alert messages will appear to come from. Bounces and non-delivery reports will be sent to this address. If no address is entered, no non-delivery reports will be sent.

Administration options

This chapter describes further options available through the *File*, *Options* and *View* menus and lists the SWEEP command line qualifiers.

Sweep memory



Sophos Anti-Virus will check memory for memory-resident viruses automatically when it is first started.

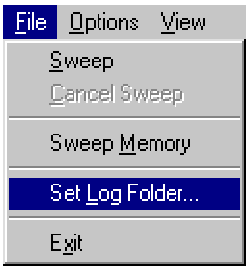
If you want to scan memory at other times, select *Sweep Memory* from the *File* menu.

Set log folder

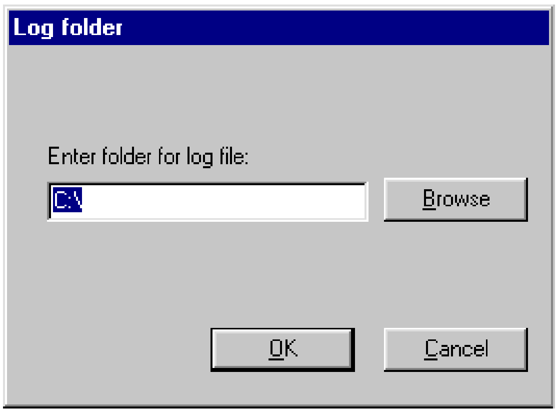
Sophos Anti-Virus maintains a continuous log of all its activity. This log file contains administrative messages along with the messages described in the 'On-screen log messages' chapter.

The log file is generated in addition to the report file (see 'Report' in the 'Configuring Sophos Anti-Virus' chapter).

By default the log file will be saved in the SAV directory, but this can be changed by selecting *Set Log Folder* from the *File* menu.



Specify a folder at the 'Log folder' dialog.


Log folder

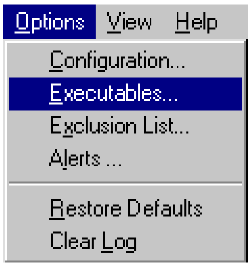
Enter folder for log file:

C:\

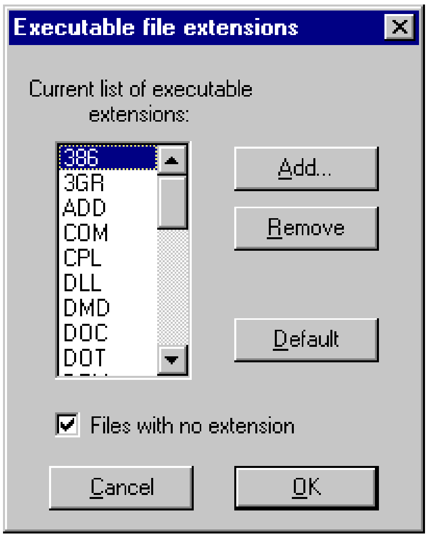
Executables

You can configure the types of files that are scanned if Sophos Anti-Virus is set to scan executables only.

Select *Executables* from the *Options* menu.



Then specify file extensions in the dialog box. Select 'Files with no extension' if you also want to include such files.

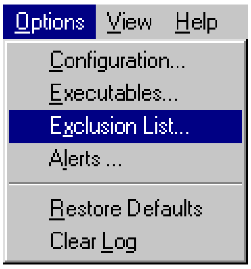

Executable file extensions
Current list of executable extensions:
386
3GR
ADD
COM
CPL
DLL
DMD
DOC
DOT
Add...
Remove
Default
Cancel
OK

☑ Files with no extension

This list is used only if Sophos Anti-Virus is set to check 'executable' rather than 'all' file types. See also 'File types' in the 'Adding new items for immediate scanning' sub-section of the 'Immediate scanning' section of the 'Using Sophos Anti-Virus' chapter.

Exclusion list

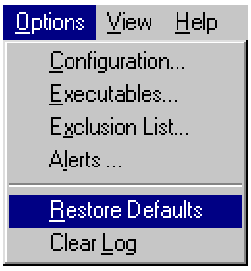
If you want to exclude any files from scanning, enter them in the ‘Exclusion list’. Select *Exclusion list* from the *Options* menu.



Then specify extensions in the dialog box.

Restore defaults

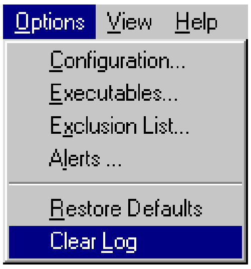
If you want to set all settings back to their defaults, select *Restore Defaults* from the *Options* list.



You will be asked for confirmation.

Important! This option will destroy all scheduled jobs.

Clear log

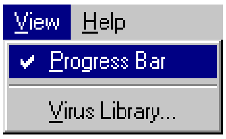


The on-screen log provides a record of activity in the current session, and reflects the information that is appended to the continuous log file.

The *Clear log* option clears the on-screen log, but does not affect the continuous log file on disk.

Progress bar

You can choose whether or not the progress bar is displayed during scans.



Select *Progress Bar* from the *View* menu to enable or disable this option.

Note: In order to display the progress bar, Sophos Anti-Virus has to count the items to be scanned before starting. On large network drives this can take a significant amount of time, which can be saved by disabling this option. This will not affect any jobs that are already running.

The progress bar is set separately for immediate and scheduled modes.

Command line qualifiers

-AUTO Auto start and exit

Starting Sophos Anti-Virus for Windows 95/98 from a command line in the following way

```
SWEEP95 -AUTO
```

will force SWEEP to perform an immediate scan, with all user input, stop and unload options disabled. If no viruses or errors are detected, SWEEP will unload at the end of the job. If viruses or errors are detected, SWEEP will display its normal messages and re-activate all controls.

-I Auto start

If the -I command line qualifier is used, SWEEP will perform an immediate scan as soon as it is loaded. User input is not disabled, and SWEEP will not unload at the end of the immediate job. You can also set SWEEP to start as soon as Windows 95/98 starts by placing a shortcut to it in the Windows 95/98 StartUp folder.

-NI No interrupting

Suppresses all options to stop SWEEP. The STOP button and all internal unload mechanisms are disabled. When combined with the -I option, all these options will be disabled until the end of the immediate job, when they will be re-activated.

-NM No memory check

The -NM qualifier suppresses the scanning of memory during SWEEP startup.

-NW No warning messages

The -NW qualifier suppresses any warning messages during SWEEP startup. This option is used when SWEEP is installed to start automatically.

Configuring InterCheck

This chapter describes the configuration of InterCheck running locally on Windows 95/98 workstations.

Note: This chapter describes commonly used options. For a full list, see the 'InterCheck Advanced User Guide', which is available on the Sophos Anti-Virus CD and website.

Is it necessary to configure InterCheck?

InterCheck can be installed and run without making any changes to the default configuration. However, users may wish to:

- Specify the types of files to be checked.
- Achieve a balance between initial checking of files and subsequent requests for checking.
- Specify disinfection.

How is InterCheck configured?

Configuring InterCheck involves editing the configuration file. This is a text file called INTERCHK.CFG stored in the directory from which InterCheck is started.

By default this is C:\Program Files\Sophos SWEEP.

Using configuration option section headers

Configuration options must be placed under a section header. The default is

[InterCheckGlobal]

Note that it is possible to use other section headers to determine which groups of workstations options will apply to. For details, see the 'InterCheck Advanced User Guide'.

SWEEP VxD section headers

Certain configuration options are used only for the SWEEP VxD, which provides virus checking on the workstation itself. Some of these options must be placed under the following section header:

[SweepVxDGlobal]

Others can be placed under the [InterCheckGlobal] header, if wished. For details, see the 'Configuration options' section.

Configuring what InterCheck checks

InterCheck uses SWEEP to look for viruses:

At start-up, when a check is run on the workstation to ensure it is virus-free.

At run-time, when items that have not previously been authorised are sent for checking before they can be accessed.

The levels of checking at both stages are fully configurable, allowing a trade-off between the initial sweeps and the subsequent authorisation requests. For details, see the sections below.

Virus checking at InterCheck start-up

There are three different times when InterCheck will use SWEEP to check the workstation at start-up:

- When InterCheck is first installed and run.
- Each time the PC is started.
- After a SWEEP update.

The sections below describe each kind of check and the options used to configure it. The 'Checking levels at start-up' section details the different checking levels you can set for each check.

Initial InterCheck start-up

An initial check is run after InterCheck is first installed and activated on a PC. This is to check that the system is initially virus-free and to create the initial authorised items list.

The checking level for this scan can be set with the InstallCheckLevel option. In the default setting (QUICK) this includes all fixed disk boot sectors, memory and files defined as executables.

Normal InterCheck start-up

This normal, day-to-day start-up check is to detect any memory-resident stealth viruses which, if active when InterCheck loads, may be able to subvert the operation of InterCheck.

The LoadCheckLevel option can be used to specify what is scanned. In the default setting (SYSTEM) this includes all fixed disk boot sectors, COMMAND.COM, executables in the root directory, and memory.

InterCheck start-up after a SWEEP update

After a SWEEP update, the checksum file is purged and a check is run to find any new viruses not found by previous versions of SWEEP.

The UpdateCheckLevel option can be used to specify what is scanned. The default setting is QUICK.

Checking levels at start-up

NONE No sweep is performed.

SYSTEM Memory, boot sectors, COMMAND.COM, and hidden system files are swept.

QUICK Memory, boot sectors, and the executables (including COMMAND.COM and hidden system files) on all fixed disks are swept in quick mode.

FULL As QUICK mode, except that the items are swept in full mode.

USER SWEEP is executed with the command line qualifiers specified by InstallSweepOptions, LoadSweepOptions or UpdateSweepOptions. If the relevant SWEEP option is not given, SWEEP will execute without any qualifiers. The command line qualifiers are listed in the Sophos Anti-Virus user manual for DOS.

File types defined as executables

The list of file types that SWEEP will treat as executables at each kind of start-up can be changed if desired. To do this, use the InstallSweepOptions, LoadSweepOptions or UpdateSweepOptions configuration options to run SWEEP with the -EX qualifier and a list of file extensions.

See the ‘InterCheck Advanced User Guide’ for details.

Virus checking at InterCheck run-time

The ProgramExtensions option specifies the list of file extensions to be treated by InterCheck as executable files.

The Exclude option specifies files to be excluded from checking.

Disinfection

Windows and Windows 95/98 InterCheck can be configured to disinfect documents containing macro viruses and disks infected with boot sector viruses. To do this, enter in the configuration file:

```
[InterCheck Global]
SweepVxDLoad=YES

[SweepVxDGlobal]
DisinfectDisks=YES
DisinfectDocuments=YES
```

Configuration options

DisinfectDisks=YES|NO

If this option is enabled, the SWEEP VxD will attempt to disinfect boot sector viruses. By default, it is disabled.

This option is only valid in a SWEEP VxD section of the configuration file.

DisinfectDocuments=YES|NO

If this option is enabled, the SWEEP VxD will attempt to disinfect macro viruses in Office files. By default, it is disabled.

This option is only valid in a SWEEP VxD section of the configuration file.

Exclude=<file>

The Exclude option is used to exempt a file from being checked. The file name must not include a path component. Up to 32 exclusions may be specified and the '?' character can be used as a wildcard. For example

```
Exclude=PROG?.EXE
Exclude=P2.SYS
```

would suppress the checking of PROGA.EXE, PROGB.EXE and P2.SYS.

The Exclude configuration option can also be used to disable all checking of a specified drive. For example

```
Exclude=E:
```

would prevent InterCheck from checking anything on the E: drive, including its boot sector.

Note that directories cannot be excluded.

InstallCheckLevel=NONE | SYSTEM | QUICK | FULL | USER

The InstallCheckLevel option defines which files will be swept for viruses when InterCheck is first executed (i.e. installed and then run) on a workstation. The default is QUICK.

See the 'Configuring what InterCheck checks' section for more information.

InstallSweepOptions=<qualifiers>

The InstallSweepOptions statement defines the command line qualifiers used to run SWEEP when InterCheck is first executed on a workstation. For example, to generate a report as InterCheck is installed, use the option:

```
InstallSweepOptions= -P=C:\INSTALL.REP
```

If the InstallCheckLevel option is set to NONE, InstallSweepOptions will have no effect. If InstallCheckLevel is set to SYSTEM, QUICK or FULL, the checking options specified by InstallSweepOptions will take priority.

LoadCheckLevel=NONE | SYSTEM | QUICK | FULL | USER

The LoadCheckLevel option defines which files will be swept for viruses when InterCheck is run on a workstation. The default is SYSTEM.

See the 'Configuring what InterCheck checks' section for more information.

LoadSweepOptions=<qualifiers>

The LoadSweepOptions statement defines the command line qualifiers used to run SWEEP when InterCheck is loaded on the workstation. For example, to generate a report from each workstation as InterCheck is loaded, use the option:

```
LoadSweepOptions=  -P=C:\ICLOAD.REP
```

If the LoadCheckLevel option is set to NONE, LoadSweepOptions will have no effect. If LoadCheckLevel is set to SYSTEM, QUICK or FULL, the checking options specified by LoadSweepOptions will take priority.

PopUpErrorText=<text>

The PopUpErrorText option defines a text string which is displayed in the virus alert message box. The default is 'Please contact the network Administrator immediately'.

The maximum length of the text is 52 characters. Note that word wrapping may be applied to text in the virus alert message box, which may result in fewer than 52 characters being available for use.

ProgramExtensions=<extensions>

Any file whose extension matches an entry in the list of ProgramExtensions will be considered by InterCheck to be a program and will be checked whenever it is accessed.

If no ProgramExtensions are given, the default extension list will be used, which is equivalent to:

```
ProgramExtensions=COM, CPL, DLL, DOT, DRV, EXE, OV?, SCR, SYS, XL?
```

Note: InterCheck for Windows 95/98 automatically checks Word documents regardless of their extension.

The '?' character can be used as a wild card and '.' can be used to represent no extension. For example

```
ProgramExtensions=COM,CPL,DLL,DOT,DRV,EXE,OV?,SCR, SYS
```

would remove XL? files (normally Microsoft Excel spreadsheet files) from the list of default extensions.

The ProgramExtensions option does not affect checking of files when they are executed, in which case all files are checked irrespective of extension.

See also the 'Configuring what InterCheck checks' section.

SweepVxDLoad=YES | NO

This option controls whether or not to use the SWEEP VxD, which provides virus checking on the local machine. When InterCheck is installed locally on Windows 95/98 workstations, the installation program automatically adds the option SweepVxDLoad=YES . This should not be changed.

SweepVxDMode=FULL | QUICK

The SweepVxDMode option controls the sweeping level used by the VxD to sweep for viruses. The default is QUICK.

This option may be placed under an InterCheck section header or a SweepVxD section header.

SweepVxDLogFile=<filename>

The SweepVxDLogFile option defines the name of the SWEEP VxD log file. Unless a filename has been defined using this option no information is logged.

This option may be placed under an InterCheck section header or a SweepVxD section header.

SweepVxDLogLevel=0..5

The SweepVxDLogLevel controls the amount of information included in the SWEEP VxD log file.

0	No messages
1	Fatal errors
2	Virus alerts
3	Errors
4	Warnings [Default]
5	Information messages

This option may be placed under an InterCheck section header or a SweepVxD section header.

UpdateCheckLevel=NONE|SYSTEM|QUICK|FULL|USER

The UpdateCheckLevel option defines which files will be swept for viruses when InterCheck detects a new version of SWEEP. The default is QUICK.

See the 'Configuring what InterCheck checks' section for more information.

UpdateSweepOptions=<qualifiers>

The UpdateSweepOptions statement defines the command line qualifiers used to run SWEEP when InterCheck detects a new version of SWEEP. For example, to generate a report, use the option:

```
UpdateSweepOptions= -P=C:\ICUPDATE.REP
```

If the UpdateCheckLevel option is set to NONE, UpdateSweepOptions will have no effect. If UpdateCheckLevel is set to SYSTEM, QUICK or FULL, the checking options specified by UpdateSweepOptions will take priority.

About updating

This chapter gives an overview of the updating process.

Overview of updating

Registered users of Sophos Anti-Virus are sent an updated CD at the beginning of every month. Alternatively, a user can download updated versions from the Sophos website.

Updating involves running the installation program, which guides the user through the update.

Users can also add new virus identities, which are used for virus detection, at any time. See the 'Updating with new virus identities' chapter.

Which kind of update?

There are two approaches to updating:

Updating a single workstation

Sophos Anti-Virus can be updated directly from CD on a single or stand-alone workstation.

Updating on a network

On a network, the updated installation files are placed onto a file server, from where workstation installations can be updated automatically or manually.

Updating a single workstation

This chapter describes how to install monthly updates on a single or stand-alone workstation.

Starting the installation program

Start Windows 95/98 and insert the Sophos Anti-Virus CD in the CD drive.

If auto-run is enabled for the CD drive, the CD will auto-start.

If auto-run is not enabled, run

```
D:\Launchcd
```

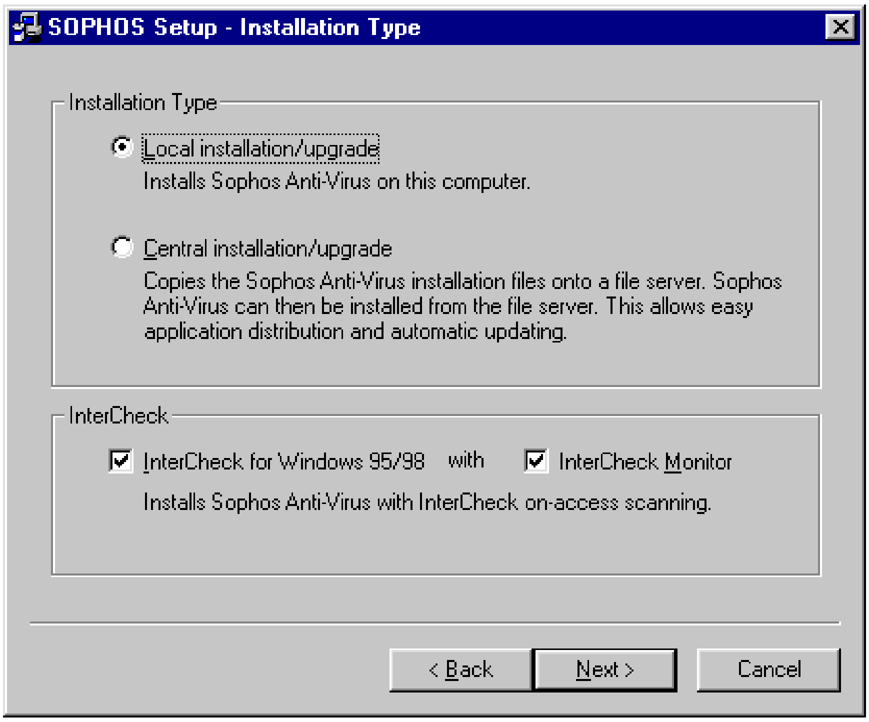
where `D:` is the CD drive.

To start the installation program, select *Quick installation* at the Sophos Anti-Virus screen.

Updating

The installation program presents the following screens.

Installation type



SOPHOS Setup - Installation Type

Installation Type

● Local installation/upgrade
Installs Sophos Anti-Virus on this computer.

○ Central installation/upgrade
Copies the Sophos Anti-Virus installation files onto a file server. Sophos Anti-Virus can then be installed from the file server. This allows easy application distribution and automatic updating.

InterCheck

☑ InterCheck for Windows 95/98 with ☑ InterCheck Monitor
Installs Sophos Anti-Virus with InterCheck on-access scanning.

Installation Type

Select ‘Local installation/upgrade’ to update Sophos Anti-Virus on the workstation.

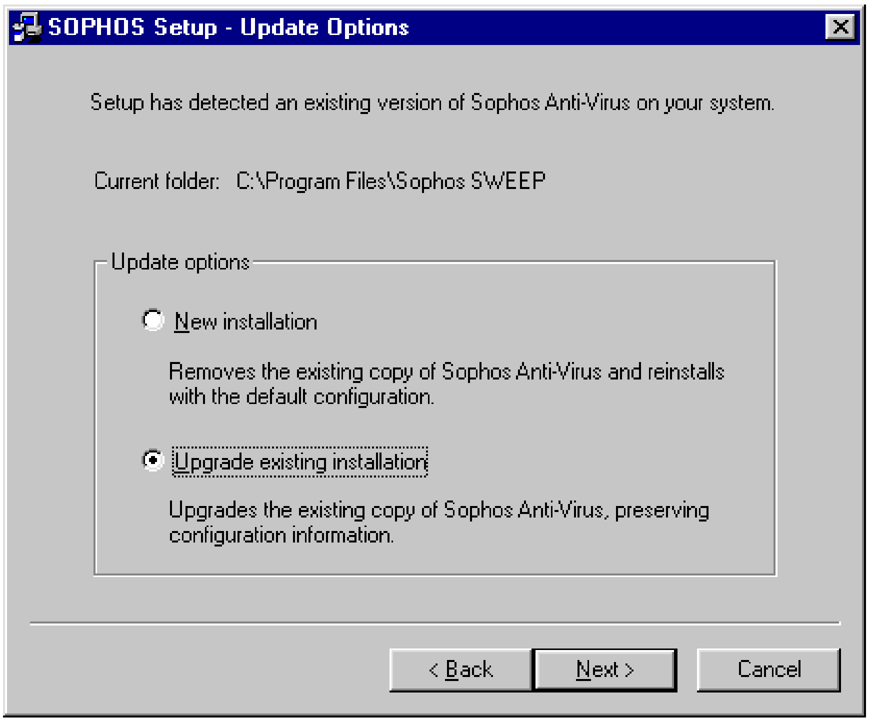
InterCheck

Select ‘InterCheck for Windows 95/98’ to provide on-access scanning on the workstation. Select ‘InterCheck Monitor’ if you want this monitor to be displayed each time the PC is started.

Note: This option can be selected during updating even if InterCheck has not previously been installed.

Now close down the InterCheck monitor and Sophos Anti-Virus GUI if prompted.

Update options



Setup has detected an existing version of Sophos Anti-Virus on your system.

Current folder: C:\Program Files\Sophos SWEEP

Update options

○ New installation

Removes the existing copy of Sophos Anti-Virus and reinstalls with the default configuration.

● Upgrade existing installation

Upgrades the existing copy of Sophos Anti-Virus, preserving configuration information.

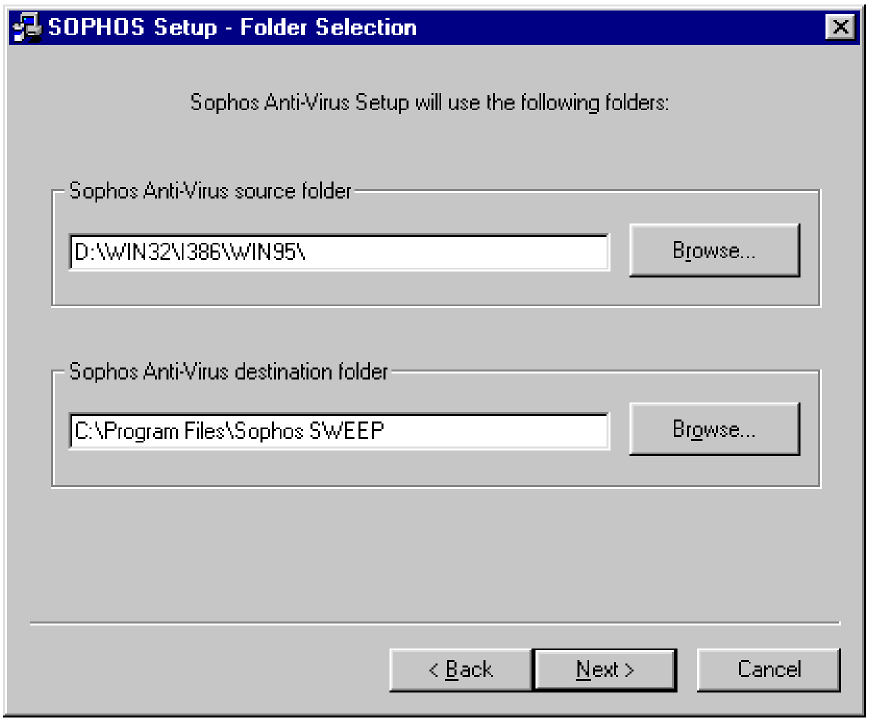
New installation

Installs Sophos Anti-Virus with the default configuration, erasing the previous version and its configuration.

Upgrade existing installation

Retains the existing configuration, updating the software components.

Folder selection



SOPHOS Setup - Folder Selection

Sophos Anti-Virus Setup will use the following folders:

Sophos Anti-Virus source folder: D:\WIN32\I386\WIN95\

Sophos Anti-Virus destination folder: C:\Program Files\Sophos SWEEP

Sophos Anti-Virus source folder

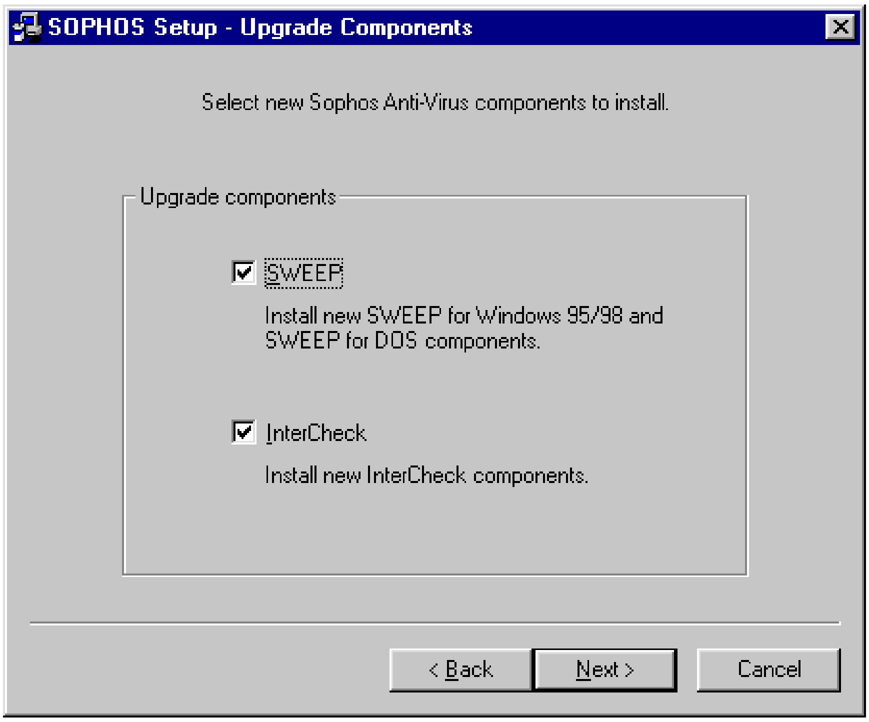
Confirm the Sophos Anti-Virus source folder. This is the folder on the CD that contains the updated installation files.

Sophos Anti-Virus destination folder

Confirm or specify the folder on the local hard disk where the updated software will be installed. If 'Upgrade existing installation' was chosen, this cannot be changed.

Upgrade components

This option is available only if upgrading Sophos Anti-Virus with InterCheck enabled.



SOPHOS Setup - Upgrade Components

Select new Sophos Anti-Virus components to install.

Upgrade components

☑ SWEEP

Install new SWEEP for Windows 95/98 and SWEEP for DOS components.

☑ InterCheck

Install new InterCheck components.

One or both of the following must be selected:

SWEEP

Installs new SWEEP for Windows 95/98 and SWEEP for DOS components.

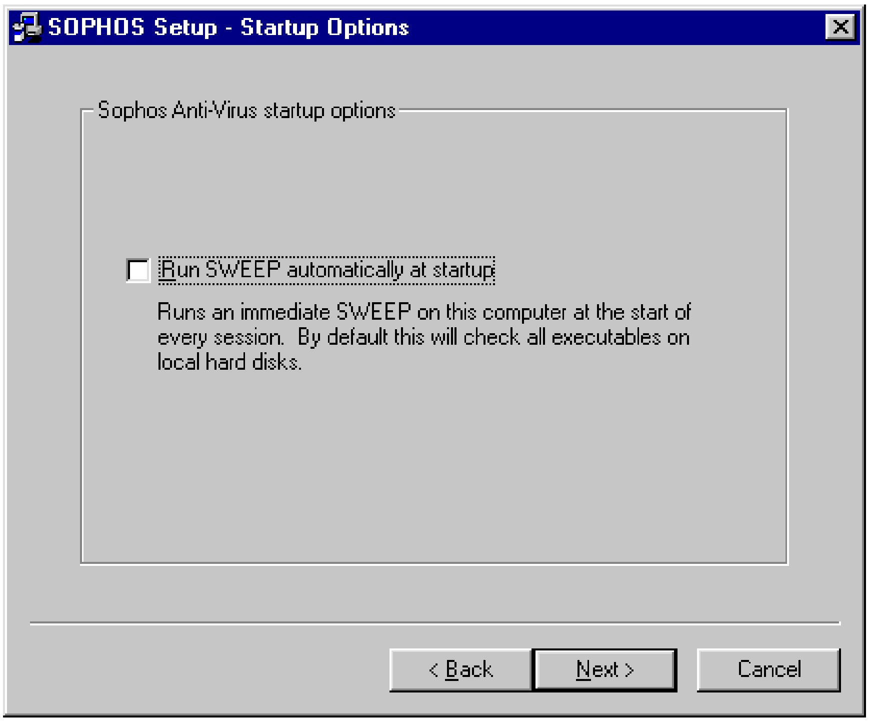
InterCheck

Installs new InterCheck components. This should normally only be selected when a new version of InterCheck is available.

If 'InterCheck for Windows 95/98' was selected at the 'Installation Type' screen, you will now see the final setup screen. See 'Completing installation' below.

Startup options

This screen appears only if ‘InterCheck for Windows 95/98’ was not selected.



SOPHOS Setup - Startup Options

Sophos Anti-Virus startup options

□ Run SWEEP automatically at startup

Runs an immediate SWEEP on this computer at the start of every session. By default this will check all executables on local hard disks.

Sophos Anti-Virus startup options

Select ‘Run SWEEP automatically at startup’ to perform an immediate scan at the start of every session. By default, this will check all executables on all local hard disks.

Completing updating

You will see a summary of the action that the installation program is going to take. Click *Finish* to complete updating.

Updating on a network

This chapter describes how to install monthly updates on a network.

About central updating

Updating Sophos Anti-Virus on a network involves placing the updated installation files on a file server (step 1), from where the workstations can be updated (step 2).

If auto-updating was selected during the original installation, step 2 will be performed automatically.

Step 1: Updating the central installation files

If using a Windows 95/98 machine for the central installation, insert the Sophos Anti-Virus CD. If auto-run is enabled for the CD drive, the CD will auto-start. If auto-run is not enabled, run

```
D:\Launchcd
```

where D: is the CD drive.

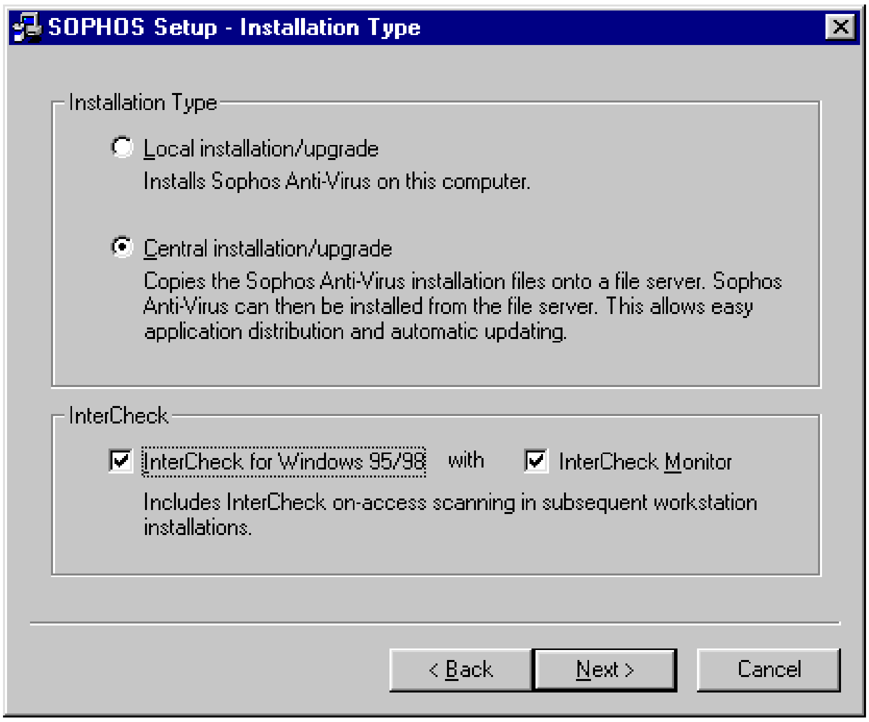
Then select *Quick installation* at the Sophos Anti-Virus screen.

On any other platform, insert the Sophos Anti-Virus CD and run

```
D:\Win32\I386\Win95\Setup.exe
```

where D: is the CD drive.

Installation type



Installation Type

○ Local installation/upgrade

Installs Sophos Anti-Virus on this computer.

● Central installation/upgrade

Copies the Sophos Anti-Virus installation files onto a file server. Sophos Anti-Virus can then be installed from the file server. This allows easy application distribution and automatic updating.

InterCheck

☑ InterCheck for Windows 95/98 with ☑ InterCheck Monitor

Includes InterCheck on-access scanning in subsequent workstation installations.

Installation Type

Select 'Central installation/upgrade' to update the installation files on the file server.

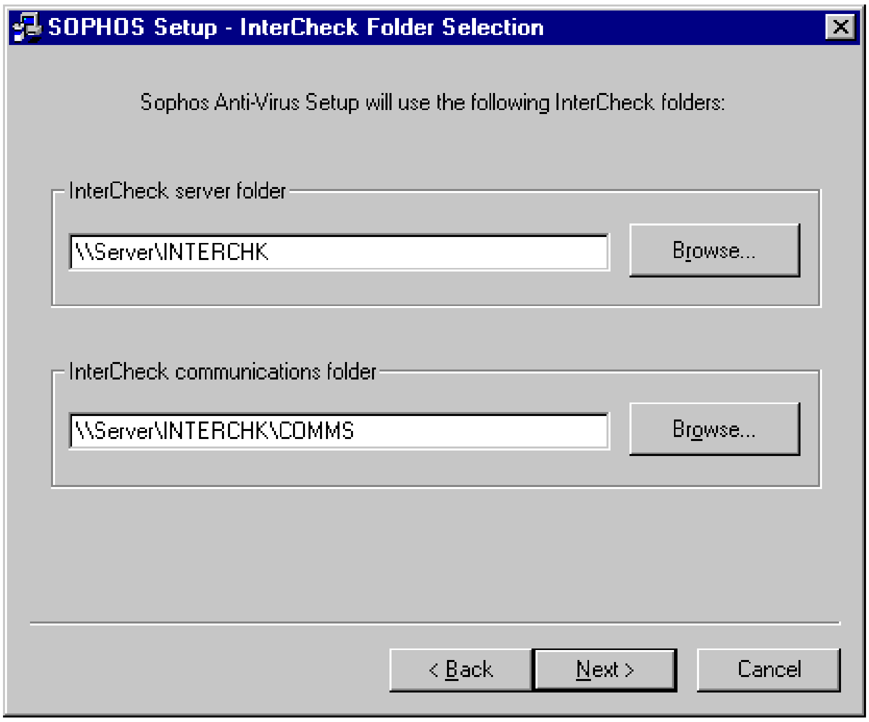
InterCheck

Select 'InterCheck for Windows 95/98' to install on-access scanning as part of subsequent local installations. Select 'InterCheck Monitor' if you want this monitor to be displayed on the workstations each time InterCheck is started.

Note: This option can be selected during updating even if InterCheck has not previously been installed.

InterCheck folder selection

This screen appears only if ‘InterCheck for Windows 95/98’ was selected.



SOPHOS Setup - InterCheck Folder Selection

Sophos Anti-Virus Setup will use the following InterCheck folders:

InterCheck server folder: \\Server\INTERCHK

InterCheck communications folder: \\Server\INTERCHK\COMMS

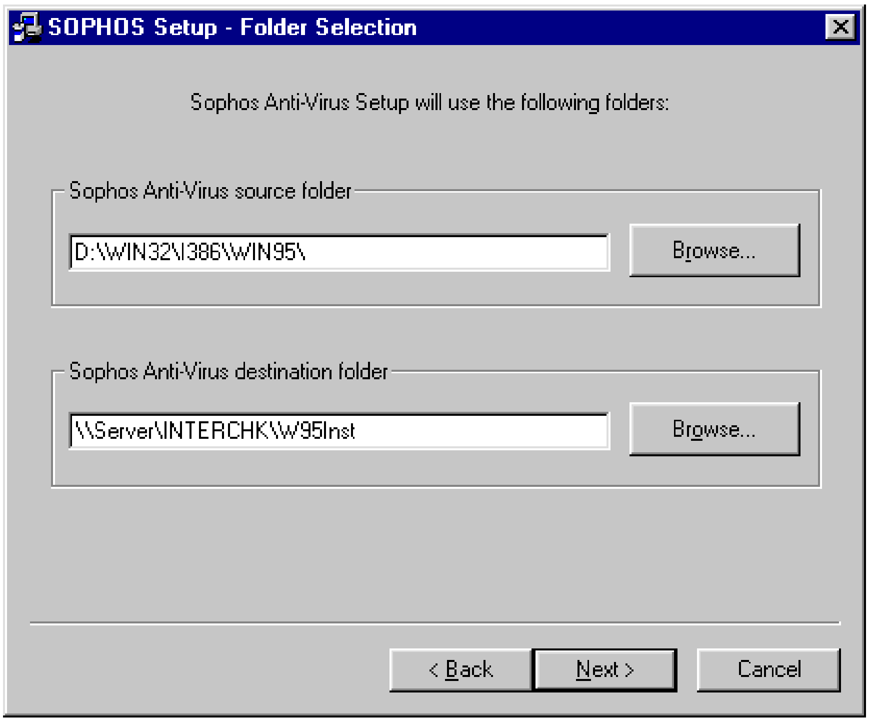
InterCheck Server folder

Specify the folder for the InterCheck configuration file (normally the folder from which the InterCheck Server is run, if one is being used).

InterCheck communications folder

If there is an InterCheck Server on the network, this folder is used for communicating with it. The communications folder is normally a subfolder of the InterCheck Server folder. If an InterCheck Server is not being used, leave this blank, ignore any warning message and click ‘Next’ again.

Folder selection


SOPHOS Setup - Folder Selection

Sophos Anti-Virus Setup will use the following folders:

Sophos Anti-Virus source folder

D:\WIN32\I386\WIN95\

Sophos Anti-Virus destination folder

\\Server\INTERCHK\W95Inst

Sophos Anti-Virus source folder

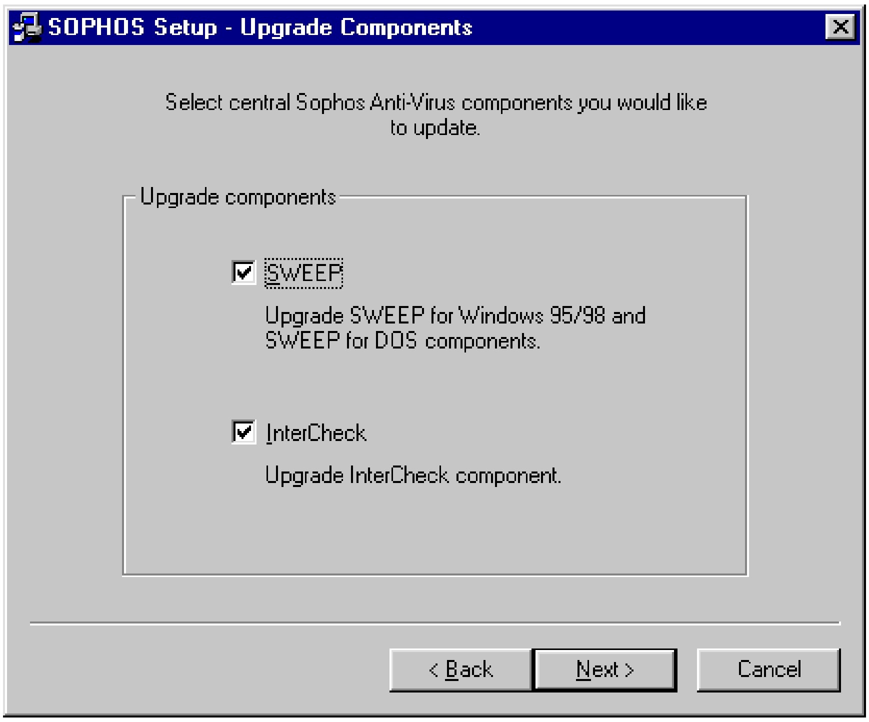
Confirm the source folder. This is the folder that contains the updated installation files.

Sophos Anti-Virus destination folder

The destination folder is the folder on the network drive to which the updated installation files will be copied.

Upgrade components

This screen appears only if updating Sophos Anti-Virus with InterCheck support.



Select central Sophos Anti-Virus components you would like to update.

Upgrade components

☑ SWEEP

Upgrade SWEEP for Windows 95/98 and SWEEP for DOS components.

☑ InterCheck

Upgrade InterCheck component.

Select one or both of the following options:

SWEEP

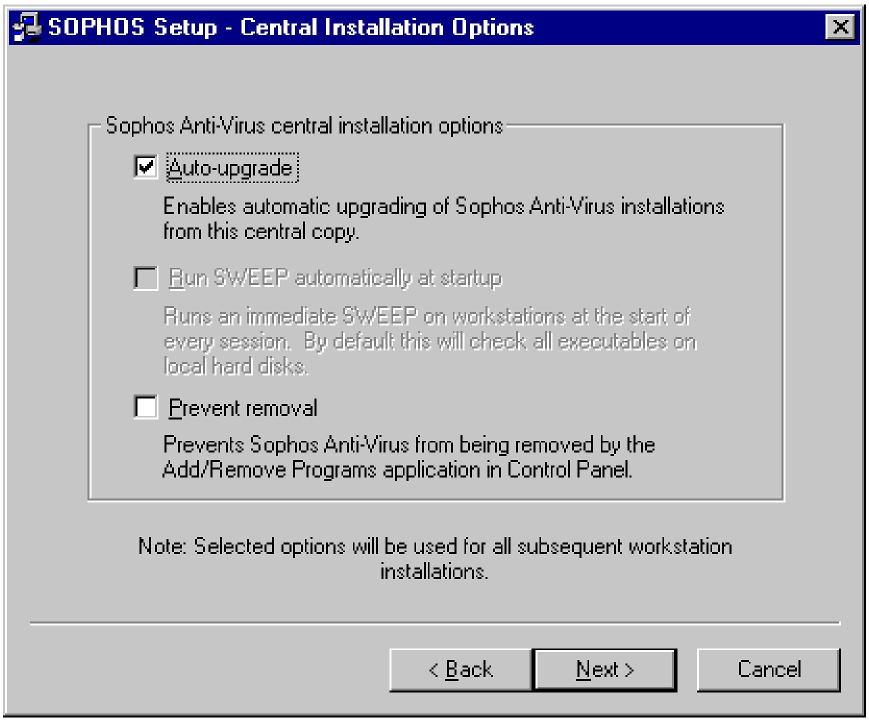
Installs new SWEEP for Windows 95/98 and SWEEP for DOS components.

InterCheck

Installs new InterCheck components. This should normally be selected only when a new version of InterCheck is available.

Central installation options

Important! The options selected here specify the way workstations will update the **next** time the central installation is updated (**not** this time).



SOPHOS Setup - Central Installation Options

Sophos Anti-Virus central installation options

☑ Auto-upgrade

Enables automatic upgrading of Sophos Anti-Virus installations from this central copy.

□ Run SWEEP automatically at startup

Runs an immediate SWEEP on workstations at the start of every session. By default this will check all executables on local hard disks.

□ Prevent removal

Prevents Sophos Anti-Virus from being removed by the Add/Remove Programs application in Control Panel.

Note: Selected options will be used for all subsequent workstation installations.

Auto-upgrade

Select this if you want subsequent workstation installations to be updated automatically whenever the central installation is updated on the server.

Run SWEEP automatically at startup

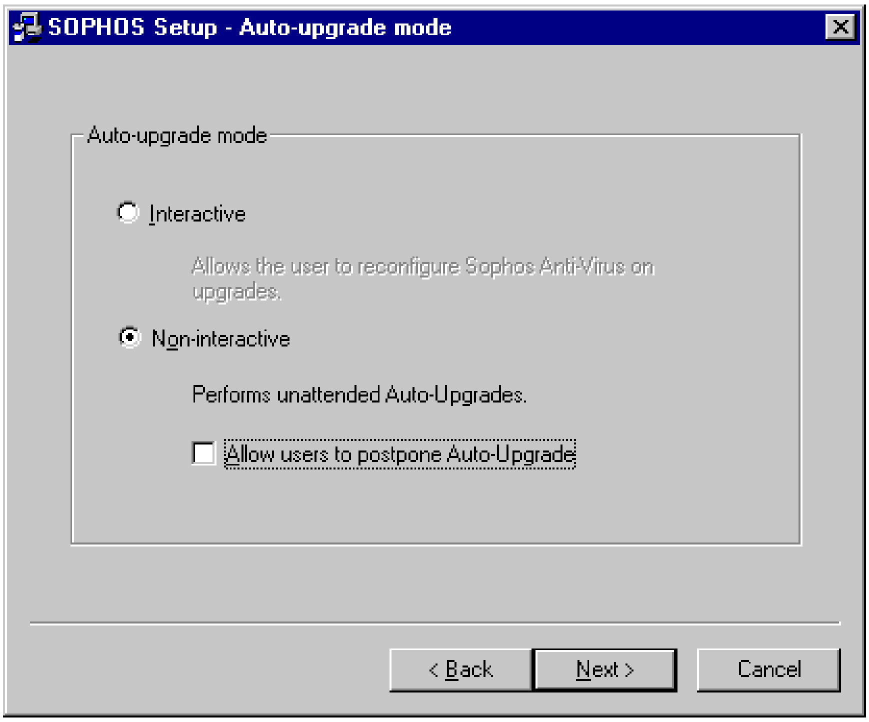
Select this if you want subsequent workstation installations to run SWEEP at the start of each session. This option is available only if 'InterCheck for Windows 95/98' was deselected earlier.

Prevent removal

Select this to ensure that subsequent workstation installations cannot be removed via *Add/Remove Programs* in Control Panel.

Auto-upgrade mode

This screen appears only if you selected ‘Auto-upgrade’.



SOPHOS Setup - Auto-upgrade mode

Auto-upgrade mode

○ Interactive

Allows the user to reconfigure Sophos Anti-Virus on upgrades.

● Non-interactive

Performs unattended Auto-Upgrades.

□ Allow users to postpone Auto-Upgrade

Interactive

This will allow the user to reconfigure Sophos Anti-Virus when it is updated.

Non-interactive

Sophos Anti-Virus will be updated from the file server automatically. This is the recommended option.

Allow users to postpone auto-upgrade

If you selected ‘Non-interactive’ updating, you can allow users to postpone the update.

Completing central updating

You will see a summary of the actions the installation program will take. Click *Finish*. The workstations can now be updated.

Step 2: Updating the workstations

In step 2, the workstation installations are updated from the central installation.

The way that this is done depends on the 'Central installation options' chosen when the previous central installation was made.

If 'Auto-Upgrade' and 'Non-interactive' were selected, updating will proceed automatically. Updating will occur when the workstation installation next checks for a newer version or when the workstation is restarted, unless users have been given the option to postpone updating.

If 'Auto-upgrade' and 'Interactive' mode were selected, users running SWEEP or InterCheck will be informed that the version on the server has been updated and will be offered the option of updating. They will see the setup screens shown below.

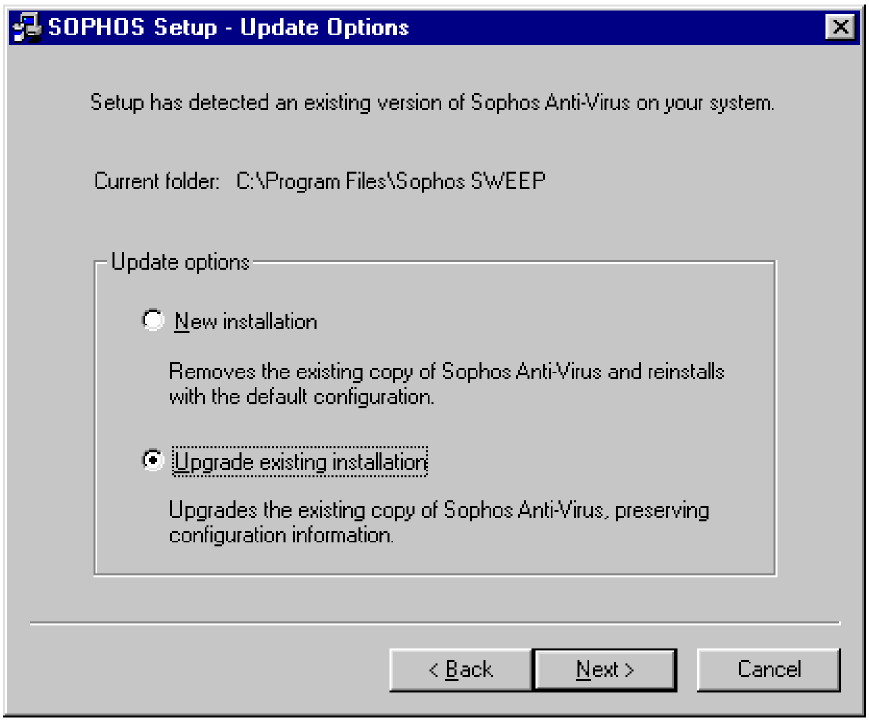
If 'Auto-upgrade' was NOT selected, go to each workstation and run Setup.exe from the central installation directory.

Close down the InterCheck monitor and Sophos Anti-Virus GUI if prompted.

The screens shown below appear.

Note: All setup screens are described, but only those which did not appear in stage 1 are illustrated.

Update options



SOPHOS Setup - Update Options

Setup has detected an existing version of Sophos Anti-Virus on your system.

Current folder: C:\Program Files\Sophos SWEEP

Update options

○ New installation

Removes the existing copy of Sophos Anti-Virus and reinstalls with the default configuration.

● Upgrade existing installation

Upgrades the existing copy of Sophos Anti-Virus, preserving configuration information.

New installation

Installs Sophos Anti-Virus with the default configuration, erasing the previous version and its configuration.

Upgrade existing installation

Retains the existing configuration, updating the software components.

Folder selection

This appears only if 'New installation' was selected.

Sophos Anti-Virus source folder

This is the location of the central installation files and cannot be changed.

Sophos Anti-Virus destination folder

This is the folder on the workstation where the updated software will be placed.

Completing updating

You will see a summary of the actions the installation program is going to take. Click *Finish* to complete the update.

Updating with new virus identities

This chapter describes how to update Sophos Anti-Virus to deal with new virus threats at any time.

Using new virus identities

If a significant new virus threat appears between regular updates, you can still update Sophos Anti-Virus to deal with it.

You do this by adding new virus identities, which Sophos Anti-Virus uses for virus detection.

Sophos can supply virus identities as IDE (identity) files. These consist entirely of printable ASCII characters, and can be faxed, emailed or downloaded from the Sophos website (http://www.sophos.com/).

You can update workstations with IDE files automatically or manually.

Automatic distribution of IDE files

If you have a central installation of Sophos Anti-Virus with ‘Auto-upgrade’ enabled, you can update workstations automatically. Place the IDE file in the central installation folder on the file server. Then open a command prompt, change to the central installation directory and type

```
setup /update
```

This will force the workstations to update when they next check for a central update.

Note: IDE files should be removed from the central installation directory once they are no longer needed.

Manual updating with IDE files

To update an individual workstation, place the IDE files in the Sophos Anti-Virus directory. Sophos Anti-Virus will recognise the new IDEs when the machine is restarted.

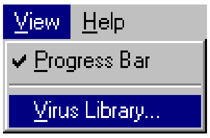
The virus library

This chapter describes the on-line virus library.

Starting the virus library

To start the on-line virus library, click the virus library icon.

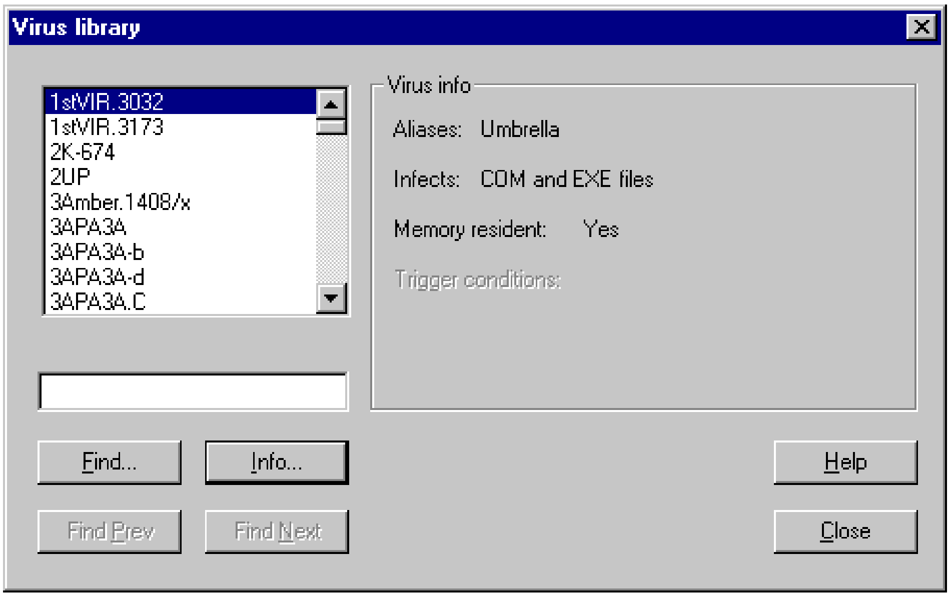
Alternatively, select *Virus Library* from the *View* menu.



The virus library will be initialised and the main window will appear.

Hint: When Sophos Anti-Virus discovers a virus, double-click on the ‘virus detected’ entry in the on-screen log to go straight to the relevant library entry.

Information on a particular virus



Virus library

1stVIR.3032
1stVIR.3173
2K-674
2UP
3Amber.1408/x
3APA3A
3APA3A-b
3APA3A-d
3APA3A.C

Virus info

Aliases: Umbrella

Infects: COM and EXE files

Memory resident: Yes

Trigger conditions:

To find details of a virus, enter the virus name (or part of the name) in the text box. In the list, the first name that matches your entry will be highlighted. If this name is not the one you intended, use the *Find Prev* and *Find Next* buttons to locate the right virus.

Note: Many virus names have prefixes indicating the platform or application they infect, e.g *Melissa* is listed under *WM97/Melissa* as it infects Word 97 documents. Make sure you click *Find Next* until the right name appears.

Basic information about the highlighted virus appears in the 'Virus info' box.

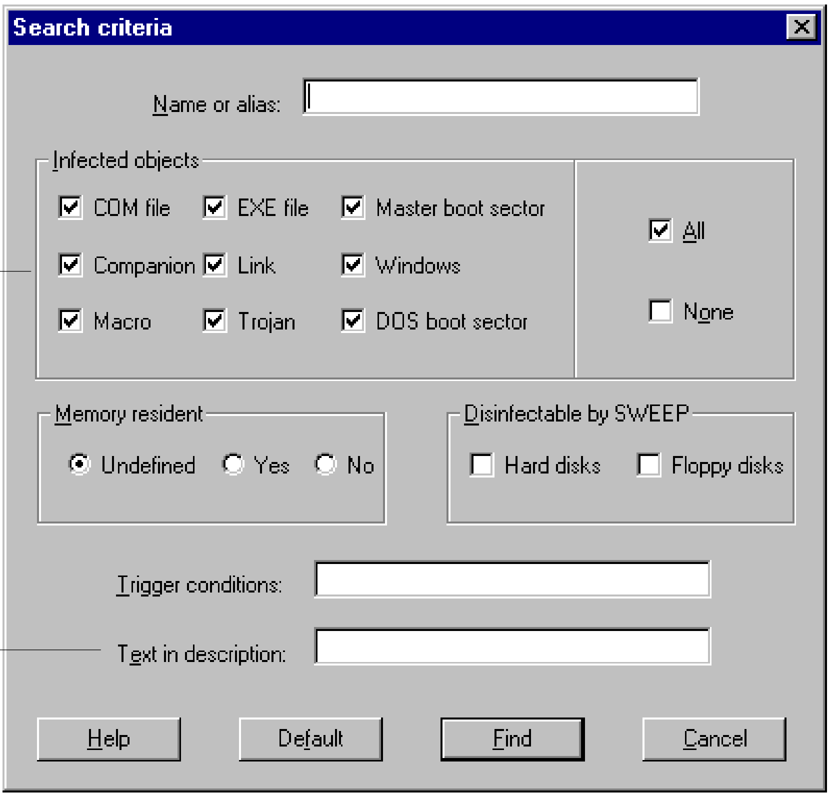
For more information, including advice on disinfection, click *Info ...* or double-click the virus name.

Searching for an unknown virus

You can search for viruses with certain characteristics. In the ‘Virus library’ dialog, click *Find* to open the ‘Search criteria’ screen:

Search according to the kind of objects infected

Search for text in the virus description



Search criteria

Name or alias:

Infected objects

☑ COM file ☑ EXE file ☑ Master boot sector

☑ Companion ☑ Link ☑ Windows

☑ Macro ☑ Trojan ☑ DOS boot sector

☑ All

□ None

Memory resident

● Undefined ○ Yes ○ No

Disinfectable by SWEEP

□ Hard disks □ Floppy disks

Trigger conditions:

Text in description:

Enter criteria in one or more of the sections (described below). Then click the *Find* button. This returns you to the ‘Virus library’ screen and highlights the first entry that matches your criteria. If it is not the one you intended, use the *Find Prev* and *Find Next* buttons to locate other possible matches.

Infected objects

In this section, you can specify which areas or files the virus infects.

Viruses can place themselves in **COM and EXE files**, the **master boot sector** or the **DOS boot sector**.

Companion viruses place the virus code in a COM file with the same name as the EXE file.

Link viruses subvert directory entries to point to the virus code.

Windows viruses affect Windows executables.

Macro viruses place viral macros inside Microsoft Word, Excel, PowerPoint, Access, Office 95 and Office 97 documents.

Trojan horses are not viruses, but programs which provide unanticipated side-effects when run.

You can also use the checkboxes to include 'All' or 'None' of these categories in your search.

Memory-resident

In this section, you can specify whether the virus you are searching for is memory-resident or not. Memory-resident viruses stay in memory after they are executed and infect other objects when certain conditions are fulfilled.

Disinfectable by SWEEP

Check these boxes to include in the search viruses which can be removed from hard and/or floppy disks.

Trigger conditions

In this text box, you can enter conditions (e.g. a certain time or date) that will trigger a virus's side-effects.

Text in description

In this text box, you can enter a text string which appears in the information about the virus you are searching for.

Treating viral infection

This chapter describes automatic disinfection and other mechanisms for dealing with viruses.

Automatic disinfection

In most cases, Sophos Anti-Virus for Windows 95/98 can deal with infected items automatically (see the 'Action on virus detection' section of the 'Configuring Sophos Anti-Virus' chapter). Sophos Anti-Virus can:

- Disinfect documents infected with certain types of macro viruses.
- Disinfect floppy disks infected with boot sector viruses.
- Deal with infected executable files.

Manual disinfection

In some cases, for example when automatic disinfection is deselected, or a hard disk boot sector is infected, manual disinfection may be necessary.

The exact manual disinfection process may also depend upon the specific virus, so consult the virus library before attempting disinfection.

Hint: When a virus is discovered, double-click on the 'virus detected' entry in the on-screen log for advice.

Important! If in doubt, please contact Sophos technical support before performing any of the operations described here.

Creating a clean boot disk

A clean boot disk, i.e. an uninfected write-protected system floppy disk, is normally an essential part of the manual virus recovery procedure. A separate clean boot disk will be required for each different operating system version, and it is vital that these are created on uninfected machines.

Follow the instructions for DOS or Windows 95/98 below. Then make the disk write-protected (to ensure it cannot become infected with a virus), and label it with the operating system for which it was created.

If a computer becomes infected, use the clean boot disk to boot the computer. This will ensure that various items on the computer can be examined through a 'clean' operating system, giving the virus no chance to employ hiding techniques.

Preparing a DOS boot disk

To create a bootable system disk, enter at a DOS prompt **on a DOS machine**:

```
FORMAT A: /S
```

Copy HIMEM.SYS, EMM386.EXE, FDISK.EXE, SYS.COM, DEBUG.EXE, SMARTDRV.EXE, SCANDISK.EXE (or CHKDSK.EXE for MS-DOS 5 and before), and FORMAT.COM onto the disk. HIMEM.SYS is an Extended Memory (XMS) driver which allows SWEEP to use all the PC's memory thereby improving performance. SMARTDRV.EXE is a disk caching program which improves SWEEP's performance by minimising the amount of disk access required when traversing the directory structure of a disk.

Create a CONFIG.SYS file with the following lines:

```
DEVICE=A:\HIMEM.SYS
DEVICE=A:\EMM386.EXE
DOS=HIGH,UMB
FILES=20
BUFFERS=4
```

Create an AUTOEXEC.BAT with the following lines:

```
A:\SMARTDRV.EXE
SET TEMP=C:\
SET TMP=C:\
```

Preparing a Windows 95/98 boot disk

A boot disk for Windows 95 or Windows 98 can be created as follows:

At the taskbar, select *Settings*, *Control Panel*, and then *Add/Remove Programs*. Click on *Properties* and select the *Startup disk* tab. This allows you to create a boot disk.

Alternatively, you can follow the procedure for creating a DOS boot disk (see above) under MS-DOS in Windows 9x. However, as there are some differences between Windows 95, OSR2 and Windows 98, you should create a separate boot disk for each.

Manual disinfection of infected boot sectors

The process for manually disinfecting a boot sector virus depends on whether the virus is on a hard disk or a floppy disk.

Boot sector viruses on the hard disk

If the hard disk is infected with a boot sector virus, Sophos Anti-Virus for Windows 95/98 will not be able to disinfect it automatically. Before manual disinfection, it is advisable to back up important data on the hard disk.

An infected boot sector on the hard disk can either be disinfected with SWEEP or replaced with a clean one:

1. Disinfection

This is the preferred approach.

Boot the PC with a clean boot disk. Use Sophos Anti-Virus for DOS/Windows 3.x to disinfect the virus with the command

```
SWEEP -DI
```

This will also disinfect any infected documents that Sophos Anti-Virus is capable of disinfecting.

2. Replacing the boot sector

Alternatively, the boot sector can in many cases be overwritten with a clean one.

Boot the PC with a clean boot disk, and check that the contents of the infected drive are visible (e.g. with `DIR`).

If the directory listing is okay, the **master boot sector** can be overwritten with the command

```
FDISK /MBR
```

and the **DOS boot sector** can be overwritten with the command

```
SYS C:
```

Boot sector viruses on floppy disks

Reboot the PC with a clean boot disk. Then copy the valuable data from the infected disk to a clean destination (it is safe to copy files if the PC has been booted from a clean boot disk), and reformat the disk.

Manual disinfection of infected executable files

Attempting to disinfect executables is inadvisable because it is impossible to ensure that executables are properly restored after disinfection. Restored files may be unstable, putting valuable data at risk.

Reboot the PC with a clean boot disk. Then locate all the infected executables, delete them, and restore clean versions from the original installation disks, from a clean PC, or from sound backups.

Manual disinfection of infected documents

When dealing with infected documents, it is not necessary to reboot from a clean system disk. However, it is important to ensure that the application that created the document is not open when disinfection is attempted.

In some cases, it is possible to manually edit the macros from the infected document using the relevant application. However, some macro viruses now operate a form of stealth to prevent users from doing this. For example, *WM/ShareFun* prevents the use of the *Tools/Macro* and *File/Templates* menu option. Please consult Sophos technical support before attempting to perform manual disinfection of macro viruses.

Recovering from virus side-effects

Recovery from virus side-effects depends on the virus. In the case of innocuous viruses such as *Cascade*, recovery from side-effects is not necessary, while in the case of a virus such as *Michelangelo*, recovery will usually involve the restoration of a complete hard disk.

Some viruses, such as *WM/Wazzu* gradually make minor changes to users' data. This sort of corruption (e.g. the removal of the word 'not' from a sentence in a Word file) can be very hard to detect and highly undesirable.

The most important thing when recovering from virus side-effects is the existence of **sound backups**. Original executables should be kept on write-protected disks so that any infected programs can easily be replaced by the original clean versions.

Sometimes data can be recovered from disks damaged by a virus. Sophos can also supply utilities for repairing the damage caused by some viruses. Contact Sophos technical support for advice.

After disinfection

After a virus attack, consider the following measures:

- Uncover and close the loopholes which allowed the virus to enter the organisation.
- Inform any possible recipients of infected disks outside the organisation that they may be affected by the virus.

Troubleshooting

This chapter provides answers to some common problems. See also the ‘On-screen log messages’ chapter for details of individual error messages.

Scanning runs slowly

‘Full’ sweeping level

By default, SWEEP will perform a ‘Quick’ scan which checks only the parts of files which are likely to contain a virus. However, if ‘Full’ scanning is set SWEEP will be much slower. The speed difference depends on the configuration of your machine, but typically the ‘Quick’ level is 5 to 10 times faster than the ‘Full’. See also ‘Sweeping level’ in the ‘Mode’ section of the ‘Configuring Sophos Anti-Virus’ chapter.

Checking all files

By default, SWEEP will only check files defined as executables. If SWEEP is configured to check all files, the process will take longer. See ‘Adding new items for immediate scanning’ in the ‘Immediate scanning’ section of the ‘Using Sophos Anti-Virus’ chapter, and the ‘File list’ section of the ‘Configuring Sophos Anti-Virus’ chapter.

Network drives selected

Network drives may be much larger than a local hard disk, and so take significantly longer to check. Most network interfaces provide much slower access than a local hard disk, which can reduce the speed further still.

Progress bar selected

If the progress bar is displayed, SWEEP will have to count all the items that are to be scanned. This can take several minutes on large network drives. You can enable or disable the progress bar by selecting *Progress Bar* from the *View* menu.

Auto-updating fails to happen

Ensure that the central update is made to the central installation directory on the file server where local installations of Sophos Anti-Virus will look for updates.

Virus fragment reported

The report of a virus fragment indicates that part of a file matches part of a virus. There are two possible causes:

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active.

Corrupted virus

Many viruses contain bugs in their replication routines so that they sometimes ‘infect’ target files incorrectly. A portion of the virus body (possibly a substantial part) may appear within the host file, but in such a way that it will never be actuated. In this case, Sophos Anti-Virus will report ‘Virus fragment’ rather than ‘Virus’. A corrupted virus cannot spread.

If a virus fragment is reported, contact Sophos technical support for advice.

False positives

Sophos Anti-Virus may very occasionally report a virus in a file that is not infected. This may happen if a sequence of bytes in a normal program matches part of a known virus (some polymorphic viruses deliberately include code resembling that in normal programs). If you are ever in doubt, contact Sophos’ technical support for advice.

To decrease the chance of false positives:

- Only check executables.
- Perform a ‘Quick’ rather than ‘Full’ scan (see ‘Sweeping level’ in the ‘Mode’ section of the ‘Configuring Sophos Anti-Virus’ chapter).

New viruses

Any virus-specific software will discover only those viruses known to the manufacturer at the time of software release. Sophos Anti-Virus is updated each month, but it may very occasionally encounter a new virus, which it will fail to report.

If a virus unknown to Sophos Anti-Virus is suspected, please send Sophos a sample and a description as soon as possible. If it is a virus, Sophos Anti-Virus must be updated as soon as possible. When the virus has been analysed (which may take from 10 minutes to a few days), we will fax or email the IDE file which can be used for updating. The latest IDE files can also be downloaded from the Sophos website.

See the ‘Updating with new virus identities’ chapter.

Virus not disinfected

Sophos Anti-Virus may report that a virus has not been disinfected. In this case:

- Check that automatic disinfection is selected (see the 'Action on virus detection' section of the 'Configuring Sophos Anti-Virus' chapter).
- If dealing with a disk or removable media, make sure that it is not write-protected.

Note: Sophos Anti-Virus will not attempt to disinfect executable files. This is because it is not possible to guarantee that the disinfected file has been properly restored.

Sophos Anti-Virus will not disinfect a virus fragment because it has not found an exact virus match.

See also the 'On-screen log messages' chapter.

Further help needed

On the website at http://www.sophos.com/

Frequently asked questions (and their answers), virus analyses, the latest IDE files, product downloads and technical reports are available on the Sophos website.

By email to support@sophos.com

Questions can be sent to Sophos by email. Please include as much information as possible, including operating system and patch level, SWEEP and InterCheck version, how Sophos Anti-Virus has been installed and configured, and the exact text of any error messages.

By telephone on +44 1235 559933

Sophos offers 24-hour, 365-day telephone technical support.

On-screen log messages

This chapter describes messages that can appear in the on-screen log.

Message categories

There are three categories of message:

- Administrative messages such as the times that jobs are started and stopped, and information on the number of viruses detected during each job.
- Virus detected messages, which include the virus name, where it was found, and the action taken.
- Error messages, which alert the user to other problems encountered during the job.

This chapter describes only the virus detected messages and the error messages.

Note: The sections in italics in the messages below indicate information that varies.

Virus detected messages

Double-clicking on a line with a virus name will display more information about that virus.

```
Virus:  'virus name' detected in location
        Action
```

SWEEP's 'virus detected' message contains the name and the location of the virus. The `location` will be one of either:

```
filename
Drive drive name: Sector sector number
Disk disk Cylinder cylinder Head head Sector sector
Memory block at address 8 digit hex address
```

The `action` depends on the settings on the Action tab in the Configuration pages (see the 'Action on virus detection' section of the 'Configuring Sophos Anti-Virus' chapter), and will be one of the following:

`No action taken`

No action will be taken if SWEEP has been configured not to disinfect boot sectors or documents and not to rename, delete, shred, move or copy any infected files, or if SWEEP is unable to disinfect a file.

`File deleted`

The file in which the virus was found has been deleted.

`File renamed to filename`

The `filename` will be the old name with the file extension changed to a number. For example, if a virus was named VIRUS.EXE it would be renamed to VIRUS.000, or VIRUS.001 if there was already a file called VIRUS.000.

`File shredded`

The infected file has been deleted and cannot be recovered.

`File moved to` *`new location`*

The *`new location`* is the location specified in the Action tab in the Configuration pages.

`File copied to` *`new location`*

The *`new location`* is the location specified in the Action tab in the Configuration pages.

`Error` *`problem`*

The *`problem`* is one of the following:

```
deleting file
renaming to filename
shredding file
moving to location
copying to location
```

The file could not be deleted/renamed/shredded/moved/copied. If the infected file was found on a floppy disk, check that the disk is not write-protected.

Important! The infected file will remain unchanged and may be able to infect other disks and files.

`Has been disinfected`

SWEEP can automatically disinfect documents infected with certain macro viruses, and can also disinfect or remove certain boot sector viruses on floppy disks. See the 'Action on virus detection' section of the 'Configuring Sophos Anti-Virus' chapter.

`Error:  Disinfection failed`

SWEEP was unable to disinfect the boot sector or document. See the 'Treating viral infection' chapter for advice on disinfection.

Important! An infected disk will remain unchanged and may be able to infect other disks and files.

```
Virus fragment:  'virus name' detected in location
         No action taken
```

The ‘virus fragment detected’ message contains the name and the location of the virus fragment. The `location` will be one of either:

```
filename
Drive drive name: Sector sector number
Disk disk Cylinder cylinder Head head Sector sector
Memory block at address 8 digit hex address
```

SWEEP does not remove virus fragments. See ‘Virus fragment reported’ in the ‘Troubleshooting’ chapter.

Error messages

```
Error:  Could not open filename
```

The file called `filename` was on the list of files to be scanned, but could not be opened for examination. Check that the file is not in use or already open.

```
Error:  Could not read filename
```

The file called `filename` was on the list of files to be scanned, but could not be read. This might indicate that the file or the disk is corrupt.

```
Error:  Sector size of drive drive is too large
```

SWEEP will only currently scan disk sectors of 2 Kb or less. It is highly unlikely that your machine will ever contain sectors larger than this.

```
Error:  Could not open report file filename/folder
```

The filename and folder of the report file are specified on the Report tab of the Configuration pages (see the 'Report' section of the 'Configuring Sophos Anti-Virus' chapter). SWEEP will not be able to open the report file if its filename is not valid, or if it cannot access the file or folder.

```
Error:  Log file filename could not be opened.
        Log data will not be saved.
```

The location of the log file is specified with the *Set Log Folder* option from the *File* menu (see the 'Set log folder' section of the 'Administration options' chapter). SWEEP will not be able to open the log file if it cannot access the file or folder.

```
Error:  Could not notify user
```

The `user` was on the notification list but could not be notified. This could be because the `user` is no longer on the list of recognised Microsoft Exchange users, or because a profile requiring user entry of a password was used.

`Error:   Could not initialize mail system`

SWEEP checks to see if Microsoft Exchange is installed before allowing access to the notification options. However, there might be some situations in which SWEEP allows access even though Microsoft Mail is not setup correctly. For example, the MAPI mail interface might not be installed correctly.

`Error:   Could not login to mail system`

If SWEEP cannot login to the mail system, then the profile name may be invalid.

`Error:   Could not allocate memory for` *`filename/folder`*

SWEEP needs to allocate memory for the report if it is to send it to the users on the notification list. If the report is too big then SWEEP will not be able to load it into memory to send it. The report file can become very large if it is configured to list every file that it examines (see the ‘Report’ section of the ‘Configuring Sophos Anti-Virus’ chapter).

Glossary

Boot Sector: The part of the operating system which is first read into memory when a PC is switched on (booted). The program stored in the boot sector is then executed, which loads the rest of the operating system from the system files on disk.

Boot Sector Virus: A type of computer virus which subverts the initial stages of the boot process. A boot sector virus attacks either the master boot sector or the DOS boot sector.

Checksum: A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered.

DOS Boot Sector: The boot sector which loads the BIOS and DOS into PC RAM and starts their execution.

IDE: The extension given to a file containing a virus identity encoded with Sophos' Virus Description Language (VDL). It will appear as a string of ASCII characters.

InterCheck: Proprietary Sophos technology which ensures that unknown files and disks cannot be accessed until checked for viruses.

InterCheck Server: Component of InterCheck (q.v.) that provides central reporting and, for certain networked workstations, on-access scanning.

IP Address: A numeric Internet address; a 32-bit binary number, normally written in dotted-decimal notation; e.g. '194.82.145.1'.

Macro Virus: A virus which uses macros in a data file to become active in memory and attach itself to other data files. Unlike conventional viruses, macro viruses can be written relatively easily with little specialist knowledge, and can attain a degree of platform independence.

Mapped Directory Path: A network drive known by its locally mapped name, e.g. the UNC directory path \\MAIN\USERS\ might be mapped to F:\ on one particular computer on the network.

Master Boot Sector: The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the PC is booted. It contains the partition table as well as the code to load and execute the boot sector of the 'active' partition.

Memory-resident Virus: A virus which stays in memory after it has been executed and infects other objects when certain conditions are fulfilled. Non-memory-resident viruses are active only while an infected application is running.

Polymorphic Virus: Self-modifying encrypting virus.

Stealth Virus: A virus which hides its presence from the PC user and anti-virus programs, usually by trapping interrupt services.

SWEEP: The component of Sophos Anti-Virus that provides immediate and scheduled virus scanning and disinfection.

Trojan Horse: A computer program whose execution has undesired side-effects, generally unanticipated by the user. The Trojan horse program may otherwise give the appearance of providing normal functionality.

UNC: Universal Naming Convention; a standard system for naming network drives, e.g. the UNC directory \\MAIN\USERS\ would refer to the USERS directory on the server called MAIN.

VDL: Virus Description Language; a proprietary Sophos language used to describe virus characteristics algorithmically. It has extensive facilities to cope with polymorphic viruses.

Virus Identity: An algorithm describing various characteristics of a virus and used for virus recognition.

Index

Sophos Plc • The Pentagon • Abingdon • OX14 3YP • England

Email enquiries@sophos.com • http://www.sophos.com/

Tel +44 1235 559933 • Fax +44 1235 559935

Part # mas9ez0s/991025

This document is also available in electronic form from Sophos.

Technical support hotline:

Email support@sophos.com

England:	**Tel (+44) 1235 559933 (24 hrs)**
Australia:	**Tel (+61) 2 92 12 1600**
USA:	**Tel (+1) 781 213 3456**
Germany:	**Tel (+49) 6136 91193**