

# SOPHOS



**Windows 95/98/Me**

User manual

For network and single users

## About this manual

This user manual explains how to use Sophos Anti-Virus for Windows 95/98/Me and how to configure

- virus scanning
- virus alerts
- disinfection
- logging.

The manual also provides help in resolving common problems.

## Where to find installation and update instructions

For installation instructions, find your network type in the list below and use the installation guide indicated.

- **Windows 95/98/Me workstations connected to a Windows NT or 2000 server**

If you want automatic updates via the internet, see the *Enterprise Manager installation guide*.

Otherwise, see the *Sophos Anti-Virus Windows NT server installation guide* or the *Sophos Anti-Virus Windows 2000 server installation guide*.

- **Windows 95/98/Me peer-to-peer network**

See the *Sophos Anti-Virus Windows 95/98/Me peer-to-peer network installation guide*.

- **Windows 95/98/Me workstations connected to a NetWare server**

See the *Sophos Anti-Virus NetWare server installation guide*.

- **Windows 95/98/Me workstations connected to a Unix server**

See the *Sophos Anti-Virus Unix server installation guide*.

- **Single Windows 95/98/Me computer**

See the *Sophos Anti-Virus Windows 95/98/Me single user installation guide*.

For update instructions, see the Sophos Anti-Virus update guide for your network type (or the Sophos Anti-Virus installation guide in the case of a single user or peer-to-peer network).

## Technical support

UK (24 hours):	(+44) 1235 559933	<a href="mailto:support@sophos.com">support@sophos.com</a>
USA (24 hours):	(+1) 888 767 4679	<a href="mailto:supportus@sophos.com">supportus@sophos.com</a>
Australia (24 hours):	(+61) 2 9409 9111	<a href="mailto:support@sophos.com.au">support@sophos.com.au</a>
France:	(+33) 1 40 90 20 90	<a href="mailto:support@sophos.fr">support@sophos.fr</a>
Germany (24 hours):	(+49) 6136 91193	<a href="mailto:support@sophos.de">support@sophos.de</a>
Italy:	(+39) 02 662810 0	<a href="mailto:support@sophos.it">support@sophos.it</a>
Japan (24 hours):	(+81) 45 227 1800	<a href="mailto:support@sophos.co.jp">support@sophos.co.jp</a>
Singapore (24 hours):	(+65) 6776 7467	<a href="mailto:supportasia@sophos.com">supportasia@sophos.com</a>

A support knowledgebase and virus information are available on the Sophos website [www.sophos.com](http://www.sophos.com)

If you contact technical support, provide as much information as possible, including Sophos software version number(s), operating system(s) and patch level(s), and the exact text of any error messages.

Copyright © 2002–2006 by Sophos Plc

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Any name should be assumed to be a trademark unless stated otherwise. *InterCheck* and *Sophos* are registered trademarks of Sophos Plc.

## Contents

### **Using Sophos Anti-Virus**

1 Using the Sophos Anti-Virus window	6
2 Using InterCheck Monitor	14
3 Disinfection	15
4 On-screen log messages	21

### **Configuration**

5 Configuring immediate and scheduled scanning	28
6 Configuring InterCheck	36
7 Alerts configuration options	44
8 Global configuration options	49
9 Sophos Anti-Virus command line qualifiers	54

### **Troubleshooting**

10 Troubleshooting	56
--------------------	----

### **Glossary and index**

Glossary	60
Index	63

# ***Using Sophos Anti-Virus***

**Using the Sophos Anti-Virus window**

**Using InterCheck Monitor**

**Disinfection**

**On-screen log messages**

# 1 Using the Sophos Anti-Virus window

This section contains the following information about using Sophos Anti-Virus on both standalone and networked workstations.

- Overview of the Sophos Anti-Virus window ([section 1.1](#)).
- How to run immediate scans ([section 1.2](#)).
- How to schedule scans ([section 1.3](#)).
- Information about InterCheck ([section 1.4](#)).

## 1.1 Overview of the Sophos Anti-Virus window

### 1.1.1 Features of the Sophos Anti-Virus window

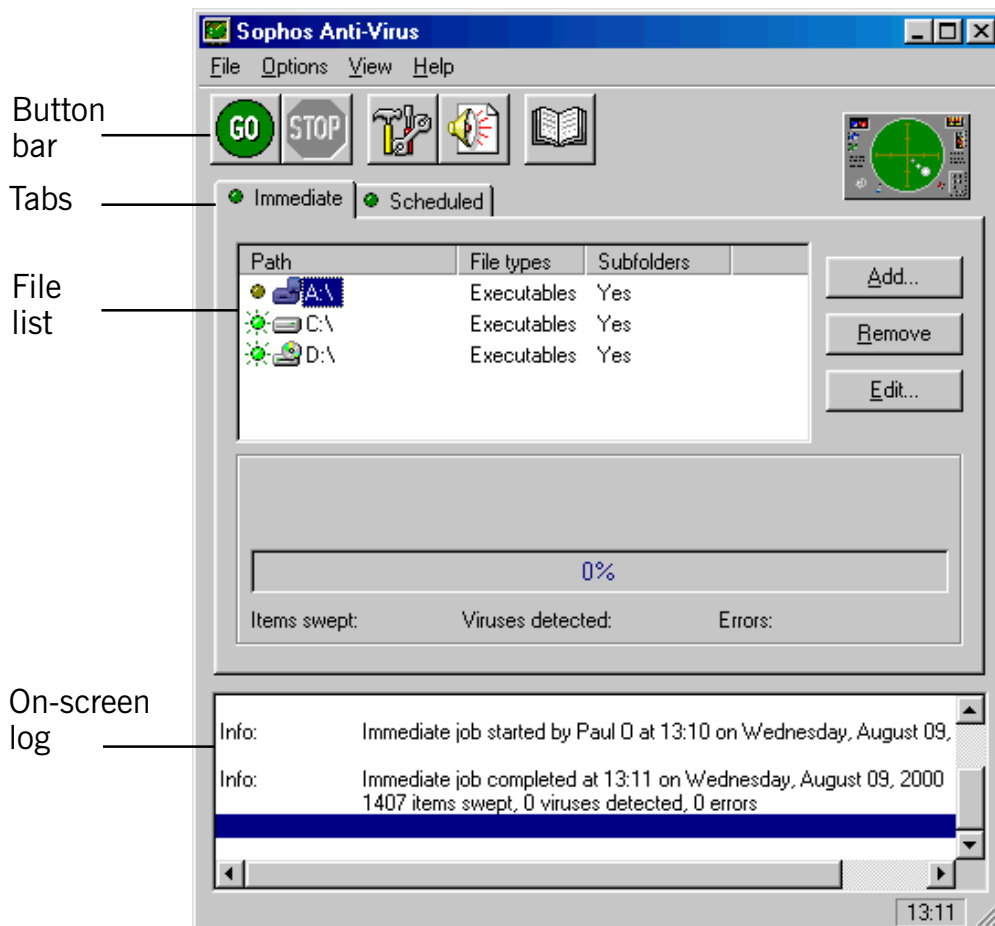
This section describes the main features of the **Sophos Anti-Virus** window.

- ❗ Closing the **Sophos Anti-Virus** window does not stop InterCheck from functioning, although any immediate scans in progress will be terminated.

To start Sophos Anti-Virus, at the taskbar, click

**Start | Programs | Sophos Anti-Virus | Sophos Anti-Virus SWEEP.**

The **Sophos Anti-Virus** window is displayed.



#### Tabs

There is a tabbed page for each type of scan.

Which tabs are available depends on your user status and on whether you view the **Sophos Anti-Virus** window from the server or from a client.

A light on the left of each tab is illuminated when that mode is active or scanning. The tabs are as follows:

- **Immediate** to trigger a scan at any time.
- **Scheduled** for scanning automatically at set times, as long as the computer is switched on.

### The button bar

The buttons are shortcuts to commonly-used menu options.



Starts scanning.



Ends scanning.



Opens a dialog box in which you can configure scanning.



Opens a dialog box in which you can configure virus alerts.



Connects you to Virus Info on the Sophos website.

### File list

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

On the **Scheduled** tabbed page, the file list is replaced with the scheduled job list. This is a list of the currently active or inactive jobs.

An active light indicates currently selected items. Click the light to include or exclude items in a scan.

### The on-screen log

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

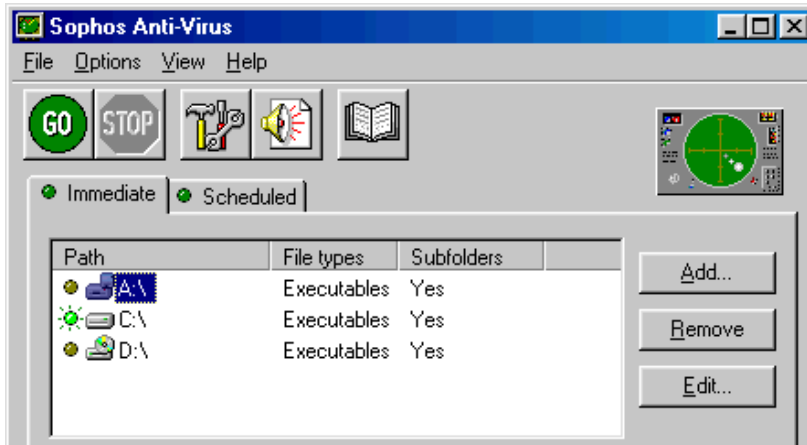
## 1.1.2 Closing the Sophos Anti-Virus window

To close the **Sophos Anti-Virus** window, on the **File** menu, click **Exit**.

Sophos Anti-Virus may warn you that scheduled scans will not be run if you close down the window. This means that if you want scheduled scans to execute, the **Sophos Anti-Virus** window *must be open*.

## 1.2 How to run immediate scans

- ❓ An **immediate scan** is a virus scan of the computer, or parts of the computer that you can carry out at any time.



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

### 1.2.1 Starting an immediate scan

Ensure the **Immediate** tab is selected.

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



Alternatively, on the **File** menu, click **Go**.

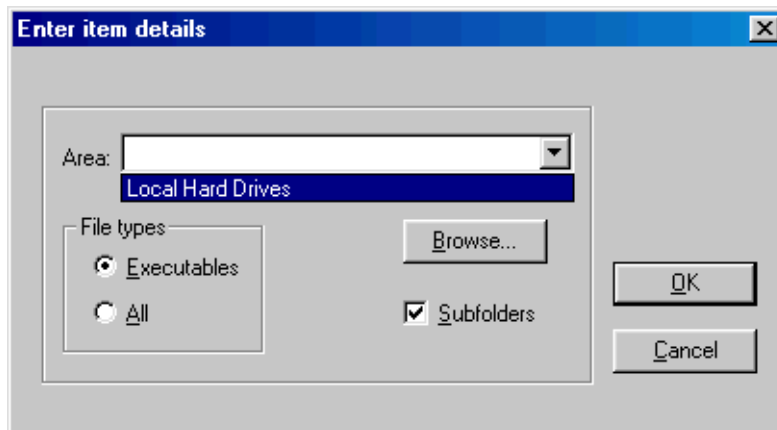
To scan any individual item in the immediate mode display, double-click its icon in the file list.

### 1.2.2 Default immediate mode file list

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

### 1.2.3 Adding new items for immediate scanning

To add new items for immediate scanning, click **Add**. The **Enter item details** dialog box is displayed.



#### Area

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 [section 8.3](#) to find out how to change the files defined as executables.

#### Subfolders

Subfolders are scanned if this option is selected.

### 1.2.4 Removing or editing items for immediate scanning

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

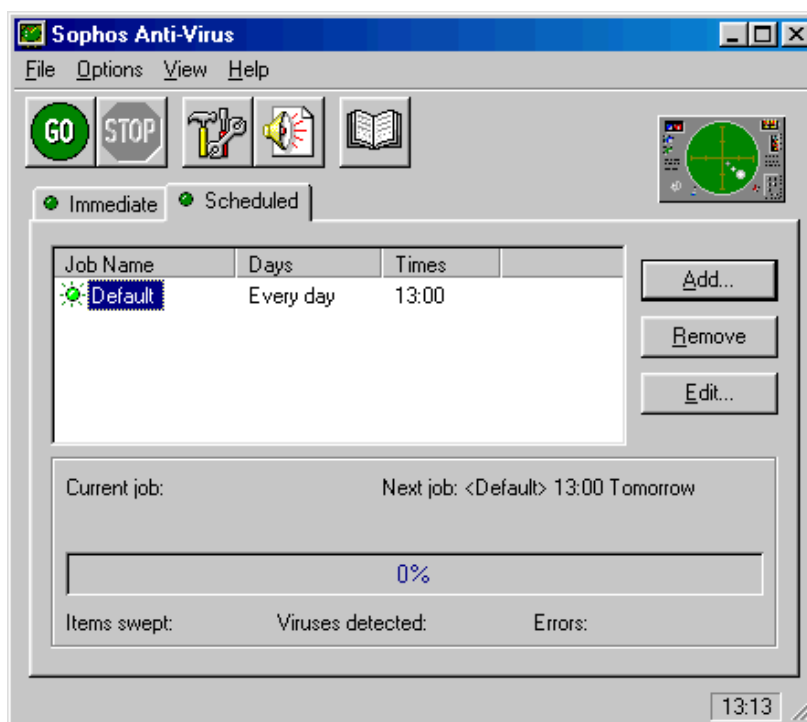
To edit the details of an item in the file list, highlight its path name and click **Edit**. The **Enter item details** dialog box (described above) is displayed.

## 1.3 How to schedule scans

- ❓ A **scheduled scan** is a scan of the computer or parts of the computer that takes place at a pre-specified time.
- ❗ A **scheduled scan will only execute if the Sophos Anti-Virus window is open at the time the scan is due and throughout the duration of the scan.**

To set up a scheduled scan, click the **Scheduled** tab.

The tabbed page lists the available scheduled jobs. An illuminated light to the left of a job indicates that it is selected and will run. Click this light to activate or deactivate jobs.



### 1.3.1 Default scheduled mode job list

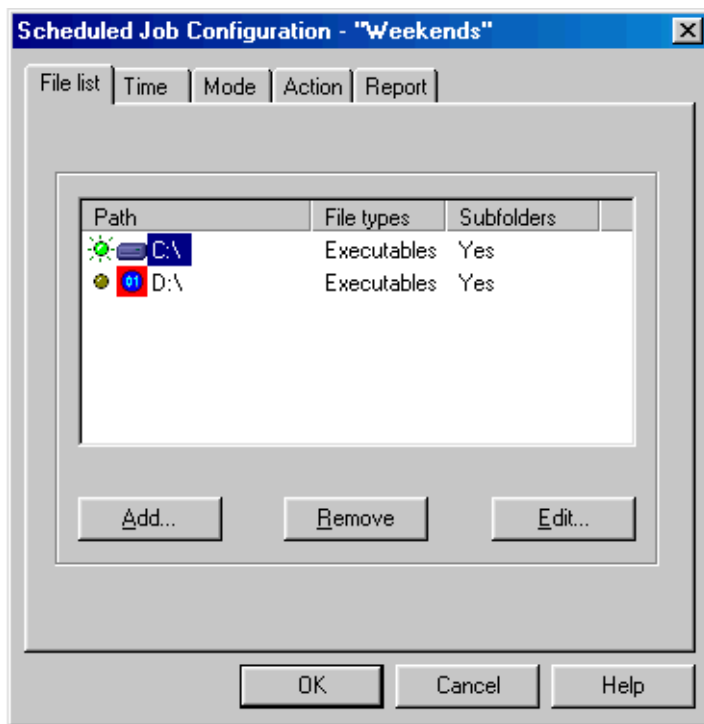
A default job called **Daily** scans the computer at 21.00 every day, as long as it is switched on **and the Sophos Anti-Virus window is open**.

### 1.3.2 Adding a new scheduled job

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

You are prompted to add a job name. Type a name then click **OK**.

The **Scheduled Job Configuration** dialog box is displayed.



Use the **File list** and **Time** tabbed pages to specify what is scanned and when. For more information about using this dialog box, see [section 5.4](#).

### 1.3.3 Removing a scheduled job

Highlight the name of the job to be removed and click **Remove**.

### 1.3.4 Editing a scheduled job

Highlight the name of the job you want to edit and click **Edit**. The **Scheduled Job Configuration** dialog box is displayed. For more information about using this dialog box, see [section 5.4](#).

## 1.4 About InterCheck

- ❓ **InterCheck** is the on-access scanning component of Sophos Anti-Virus that intercepts files as they are accessed, and grants access only to those that are virus free.

InterCheck starts automatically each time Windows 95/98/Me is started, before any network connections are made. InterCheck Monitor also becomes active, provided that **InterCheck Monitor** was selected during installation (this is a default setting). See [section 2](#) for information about InterCheck Monitor.

InterCheck for Windows 95/98/Me 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 attempts to access and denies access if they are infected.

By default, InterCheck for Windows 95/98/Me disables access to floppy disks infected with boot sector viruses.

See [section 6](#) for information about configuring InterCheck.

## 2 Using InterCheck Monitor

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

Its function is to confirm that InterCheck Client is active. When it is active, a red lightning flash is displayed in the system tray.

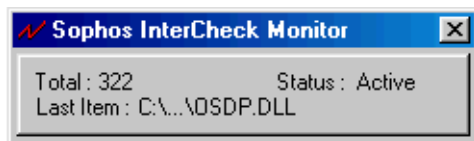


When InterCheck is inactive, the lightning flash is grey.

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

To display InterCheck Monitor, double-click the lightning flash in the system tray.

### InterCheck Monitor display



The monitor displays

- the total number of items filtered (i.e. checked against the list of items authorised by InterCheck Client)
- the status of InterCheck Client (active or inactive)
- the name of the last item filtered.

To display the InterCheck Monitor menu, click the left-hand side of its title bar. You can open the **Sophos Anti-Virus** window from this menu.

- 💡 Closing InterCheck Monitor does not stop InterCheck. As long as the red lightning flash is present in the system tray, InterCheck is active.

## 3 Disinfection

This section provides some general information about disinfection. ***It does not explain how to disinfect a computer of specific viruses***, as disinfection methods are varied and can be virus-specific.

- ❗ **It is recommended that you get information about the virus (see below), then either use the Sophos website for help with disinfection or contact Sophos [technical support](#).**

### 3.1 Getting information about the virus

If Sophos Anti-Virus reports a virus, first isolate the infected computers from the network and internet.

Write down the name of the virus, then, from an uninfected computer, look up its virus analysis on the Sophos website. The virus analysis search page is located at

[www.sophos.com/virusinfo/analyses](http://www.sophos.com/virusinfo/analyses)

The analysis tells you what types of files the virus infects, and provides information about disinfection. It may also include a link to detailed disinfection instructions.

If there are no instructions, or if the virus analysis tells you to seek advice, contact Sophos [technical support](#).

## **3.2 Disinfection**

Sophos Anti-Virus can disinfect many viruses automatically. This includes

- almost all macro viruses
- most boot sector viruses
- some executable file viruses.

To attempt automatic disinfection, enable automatic disinfection for immediate scanning (see [section 5.2](#)) then click the **GO** button to run a full scan of the computer.

If the number of viruses reported in the on-screen log decreases, continue running scans until no viruses are found.

If disinfection fails, you should carry out a manual disinfection, specific to that virus and Windows 95/98/Me. This is described on the Sophos website, either in its virus analysis, or on the web page that describes how to disinfect that *type* of virus.

### **3.2.1 If the virus has infected a document**

Sometimes you can manually edit the macros from infected documents.

However, contact Sophos technical support before attempting manual disinfection of a macro virus.

### **3.2.2 If the virus has infected a program**

It is impossible to guarantee executable files will be fully restored after disinfection. Restored files may be unstable and put valuable data at risk. You should therefore delete then replace infected programs.

Make a note of the name of the infected executable file/s. Reboot the computer with a clean startup disk (see [section 3.3](#)). Locate all the infected executables, delete them, then restore clean versions from the original installation disks, from a clean computer, or from sound backups.

### **3.2.3 If the virus has infected a boot sector on a floppy disk**

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

### 3.2.4 If the virus has infected a boot sector on the hard disk

Before carrying out this procedure, it is advisable to back up important data on the hard disk.

An infected boot sector on the hard disk should be disinfected. If this is not possible, the boot sector should be replaced with a clean one.

You will need a clean boot disk for the infected computer's operating system (or a startup disk for Windows Me) and a set of Sophos Anti-Virus emergency floppy disks.

See [section 3.3](#) to find out how to create a startup or clean boot disk, and [section 3.4](#) to find out about making Sophos Anti-Virus floppy disk sets.

#### To disinfect a boot sector

1. Insert the startup disk in the disk drive and restart the computer.
2. If using Windows Me, press 'Ctrl' + 'F5' when the computer restarts.
3. Insert the first emergency disk. Change to the A: drive and run Sophos Anti-Virus for DOS/Windows 3.1x by entering

```
A:
SWEEP *:-DIB
```

#### To replace a boot sector

If you cannot disinfect the boot sector, overwrite it as follows.

1. Insert the startup disk in the disk drive and reboot the computer.
2. If using Windows Me, press 'Ctrl' + 'F5' when the computer restarts.
3. Check that the contents of the infected drive are visible (e.g. by using DIR C:).
- ❗ If the contents of the infected drive are not visible, contact Sophos technical support.
4. If the contents of the infected drive are visible, overwrite the master boot sector with the command

```
FDISK /MBR
```

or overwrite the DOS boot sector with the command

```
SYS C:
```

### 3.3 How to create a startup disk

Booting your computer with a startup disk enables you to examine it through a 'clean' operating system, which can be essential to the disinfection process.

#### 3.3.1 To create a startup disk for Windows 95/98/Me

The startup disk must be created on a computer with the same operating system and from the same manufacturer as the infected computer.

- ❗ Some early versions of Windows 95 do not offer the facility to create a startup disk. If this is the case, or if the disk-creation process does not work, go to section 3.3.2 and create a clean boot disk.

You need one clean floppy disk.

1. On a virus-free Windows 95/98/Me computer, at the taskbar, click **Start | Settings | Control Panel**.
2. In **Control Panel**, click **Add/Remove Programs**.
3. Click the **Startup Disk** tab, then click **Create Disk**. Follow the on-screen instructions, inserting the disk in the floppy disk drive when prompted.
4. Label the disk clearly, write-protect and store it carefully.

#### 3.3.2 To create a clean boot disk (Windows 95/98 only)

If it is necessary for you to create a clean boot disk, use it in place of the startup disk.

A separate disk is required for Windows 95 (and for different versions of Windows 95) and Windows 98. It is vital that the clean boot disk is created on an uninfected machine.

1. Restart the computer in MS-DOS mode, then insert a disk in the disk drive.
2. At the MS-DOS prompt enter

```
FORMAT A: /S
```

3. Copy the following files onto the disk:

HIMEM.SYS, FDISK.EXE, SYS.COM, DEBUG.EXE, SCANDISK.EXE (or CHKDSK.EXE for MS-DOS 5 and earlier), FORMAT.COM and EDIT.COM.

HIMEM.SYS is an Extended Memory (XMS) driver which enables Sophos Anti-Virus to use all the computer's memory thereby improving performance.

- ❗ These files can be found in C:\Windows and C:\Windows\Command.

4. Create a CONFIG.SYS file that contains the following lines:

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

5. Create an AUTOEXEC.BAT that contains the following lines:

```
SET TEMP=C:\
SET TMP=C:\
```

6. Now write-protect the disk (to ensure it cannot become infected with a virus), and label it with the operating system for which it was created.

### 3.4 How to create Sophos Anti-Virus floppy disk sets

To create a Sophos Anti-Virus floppy disk set do the following.

1. Insert the Sophos CD at any Windows computer.
2. Using Windows Explorer, browse to the CD and open

```
Diskimg\Diskmake.exe
```

This opens the Sophos disk set creation program.

3. From the drop-down menu, select the type of disk set you would like to make (e.g. **Emergency SAV distribution**). On the screens that follow, accept the defaults by clicking **Next**, until you click **Finish**. Label your disks as instructed.
4. Follow the on-screen instructions to create the disks.

When the process is complete, write-protect the disks and store them carefully.

### **3.5 Recovering from virus side-effects**

Recovery from virus infection depends on how the virus infected the computer. Some viruses leave you with no side-effects to deal with, others may have such extreme side-effects that you have to restore a hard disk or replace the BIOS in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect. It is therefore very important that you read the virus analysis on the Sophos website, and check documents carefully after disinfection.

Sound backups are crucial. You should keep original executables on write-protected disks so that infected programs can easily be replaced. If you did not have them before you were infected, create or obtain them in case of future infections.

Sometimes you can recover data from disks damaged by a virus. Sophos can supply utilities for repairing the damage caused by some viruses. Contact Sophos [technical support](#) for advice.

## 4 On-screen log messages

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

### 4.1 Message categories

There are three kinds of log message:

- Administrative messages, such as the times that jobs are started and stopped, and information on the number of viruses detected during a 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 the virus-detected messages and the error messages. Administrative messages are self explanatory.

- ❗ The sections in square brackets in the messages below indicate information that varies.

## 4.2 Virus detected messages

Double-clicking a virus name connects you to that virus's analysis on the Sophos website.

### **Virus: [virus name] detected in [location] [Action]**

This message is displayed if a virus is found during an immediate or scheduled scan. The [location] is one of:

[filename]

Drive [drive name]:

Sector [sector number]

Disk [...]

Cylinder [...]

Head [...]

Sector [...]

Memory block at address [8 digit hex address]

The [action] taken depends on the settings on the **Action** tabbed page of the **Immediate Mode** or **Scheduled Job Configuration** dialog box (see [section 5.2](#)), and is one of the following:

#### **No action taken**

No action is taken if you have configured Sophos Anti-Virus not to disinfect boot sectors or documents, and not to rename, delete, shred, move or copy any infected files.

#### **File deleted**

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

#### **File renamed to [filename]**

The [filename] is 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 on the **Action** tabbed page of the **Immediate Mode** or **Scheduled Job Configuration** dialog box (see [section 5.2](#)).

### **File copied to [new location]**

The [new location] is the location specified in the **Action** tabbed page of the **Immediate Mode** or **Scheduled Job Configuration** dialog box (see [section 5.2](#)).

### **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 or copied. If the infected file was found on a floppy disk, check that the disk is not write-protected.

#### **❗ The infected file remains unchanged and may be able to infect other disks and files.**

Sophos Anti-Virus has automatically disinfected an item. Run an immediate scan to ensure the computer is now virus free (see [section 1.2](#)).

### **Error: Disinfection failed**

Sophos Anti-Virus was unable to disinfect a document or boot sector. See the Sophos website for information about disinfecting specific viruses.

#### **❗ The infected item remains unchanged and may be able to infect other disks and files.**

### **Virus fragment: [virus name] detected in [location]**

#### **No action taken**

The [location] is one of:

[filename]  
Drive [drive name]:  
Sector [sector number]  
Disk [...]  
Cylinder [...]  
Head [...]  
Sector [...]  
Memory block at address [8 digit hex address]

Sophos Anti-Virus does not remove virus fragments. See [section 10.4](#).

## 4.3 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**

Sophos Anti-Virus will only currently scan disk sectors of 2KB 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** tabbed page of the **Immediate Mode** or **Scheduled Job Configuration** dialog box (see [section 5.3](#)). Sophos Anti-Virus cannot open the report file if its filename is not valid, or if it does not have sufficient access rights to the folder.

### **Error: Log file [filename] could not be opened. Log data will not be saved.**

You can specify the location of the log file by using the **Set Log Folder** option on the **File** menu in the **Sophos Anti-Virus** window (see [section 8.2](#)). Sophos Anti-Virus cannot open the log file if it does not have sufficient access rights to the file or folder.

### **Error: Could not notify [user]**

The [user] is on the notification list but cannot be notified. This may be because the [user] is no longer on the list of recognised Microsoft Exchange users, or because a profile that requires the user to enter a password was used.

**Error: Could not initialize mail system**

Sophos Anti-Virus checks to see if Microsoft Exchange is installed before allowing access to the notification options. However, there might be some situations in which Sophos Anti-Virus allows access even though Microsoft Mail is not set up correctly (e.g. if the MAPI mail interface is not installed correctly).

**Error: Could not login to mail system**

If Sophos Anti-Virus cannot log in to the mail system, the profile name may be invalid.

**Error: Could not allocate memory for [filename/folder]**

Sophos Anti-Virus 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 Sophos Anti-Virus 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 it examines (see [section 5.3](#)).



# ***Configuration***

**Configuring immediate and scheduled scanning**

**Configuring InterCheck**

**Alerts configuration options**

**Global configuration options**

**Sophos Anti-Virus command line qualifiers**

## 5 Configuring immediate and scheduled scanning

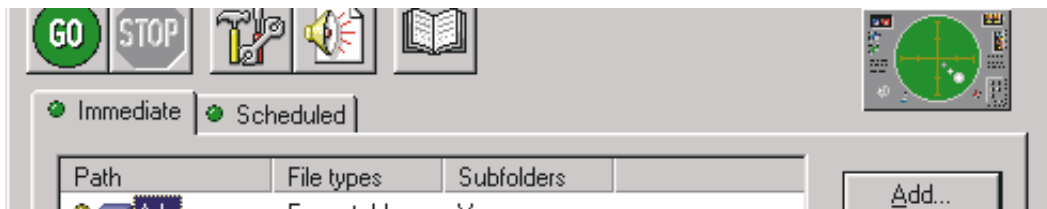
This section describes how to configure immediate and scheduled scanning.

- ❗ If you want to configure InterCheck (on-access scanning), see [section 6](#).

The different scanning modes are explained in [section 1](#).

Immediate and scheduled scanning each has a configuration dialog box which contains tabbed pages in which you specify which items each mode scans and what action it takes on finding a virus.

To open the required configuration dialog box, in the **Sophos Anti-Virus** window, click the tab for the scanning mode you would like to configure.



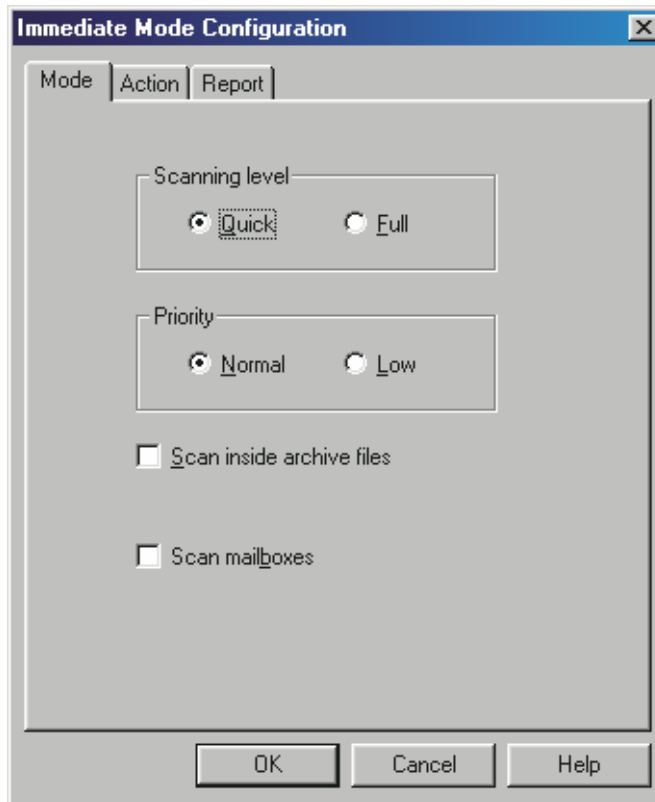
Then click the **Configuration** button.



The sub-sections in this section describe each tabbed page you will find in the configuration dialog boxes. Some tabbed pages are only available for one type of scan.

## 5.1 Mode

The **Mode** tabbed page enables you to configure scanning activity for both immediate and scheduled scanning.



### Scanning 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 but is much slower than **Quick**.

- ❗ **Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).**

### Priority

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

### **Scan inside archive files**

Select this if you want Sophos Anti-Virus to scan for viruses inside archive files. You can find a full list of archive types scanned in the Sophos Anti-Virus Windows 95/98/Me ReadMe.

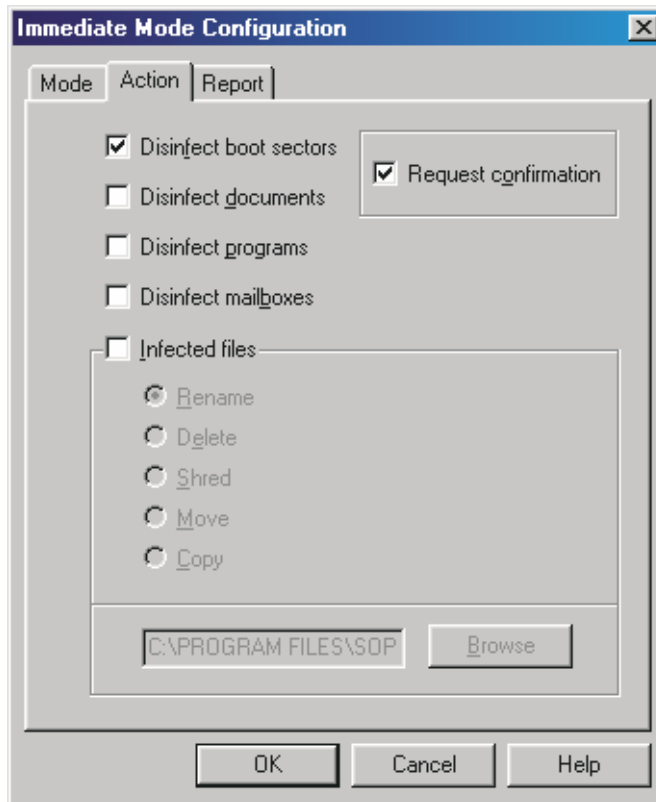
- By default, files compressed with dynamic compression utilities (PKLite, LZEXE and Diet) are also checked.

### **Scan mailboxes**

Select this option if you want Sophos Anti-Virus to scan emails and attachments in Outlook Express mailboxes.

## 5.2 Action

The **Action** tabbed page enables you to choose how scheduled and immediate scanning deal with infected items.



### 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 [section 3](#) or the Sophos website for information about disinfecting hard disk boot sectors.

### Disinfect documents

Sophos Anti-Virus can disinfect documents infected with most types of macro virus. If disinfection fails, the infected file is dealt with in the same way as any other infected file (see **Infected files**, below).

- ❗ Some macro viruses corrupt the infected document. Check disinfected files carefully before using them. Check the virus analysis on the Sophos website to find out how the virus affects documents it infects.

### **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. 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.

The **Infected files** option does not apply to infected mailboxes.

### **Disinfect programs**

Sophos Anti-Virus can disinfect programs. However, it is not recommended that you check this option by default. If Sophos Anti-Virus locates a virus in a program, return to this dialog box and check the **Disinfect programs** option, then run an immediate scan. After disinfection, uncheck this option.

You should subsequently replace the program from a clean backup.

### **Disinfect mailboxes**

Sophos Anti-Virus can disinfect emails and attachments in Outlook Express mailboxes. All infected emails and attachments that can be disinfecting, including those that are multiply-infected, are disinfecting in one scan. At the end of the scan, Sophos Anti-Virus reports any emails or attachments that it could not disinfect.

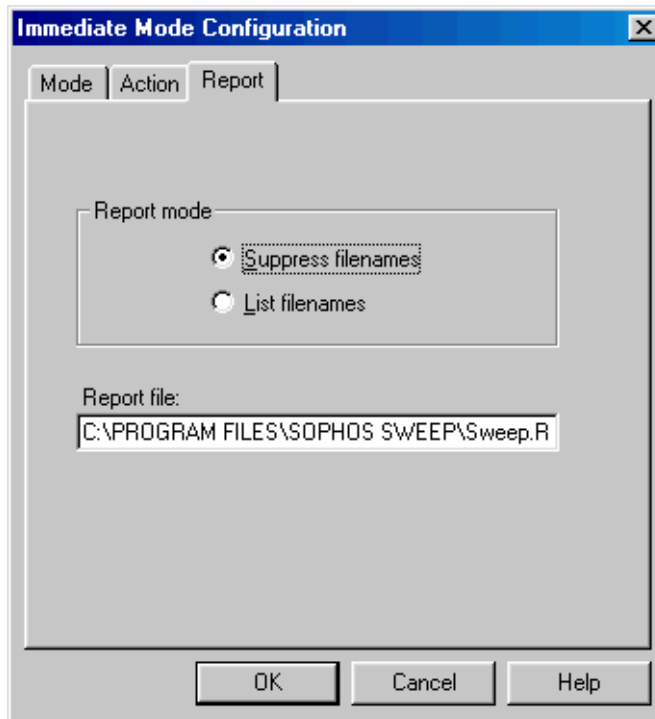
### **Request confirmation**

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). If you also select **Disinfect mailboxes**, Sophos Anti-Virus will ask for confirmation only before disinfecting the *first* email or attachment that it finds to be infected; it does *not* ask for confirmation before performing subsequent disinfections of the same mailbox in the same scan.

This option is available only for immediate scanning.

## 5.3 Report

The **Report** tabbed page enables you to configure the report file for each immediate or scheduled scan.



Sophos Anti-Virus generates a separate report file for the immediate job and for each scheduled job. This file is provided for the user. It is not the same as the continuous log file.

### Report mode

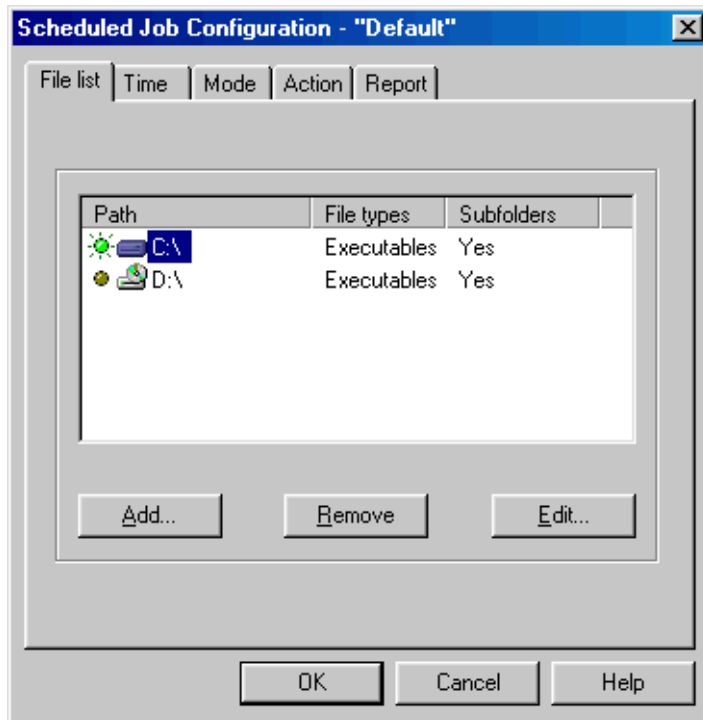
Select **List filenames** if you want Sophos Anti-Virus to record in the report file the name of every item scanned. Otherwise only infected items are recorded.

### 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.

## 5.4 File list (scheduled mode only)

This page enables you to specify what files should be scanned by the scheduled job currently selected in the job list in the **Sophos Anti-Virus** window.

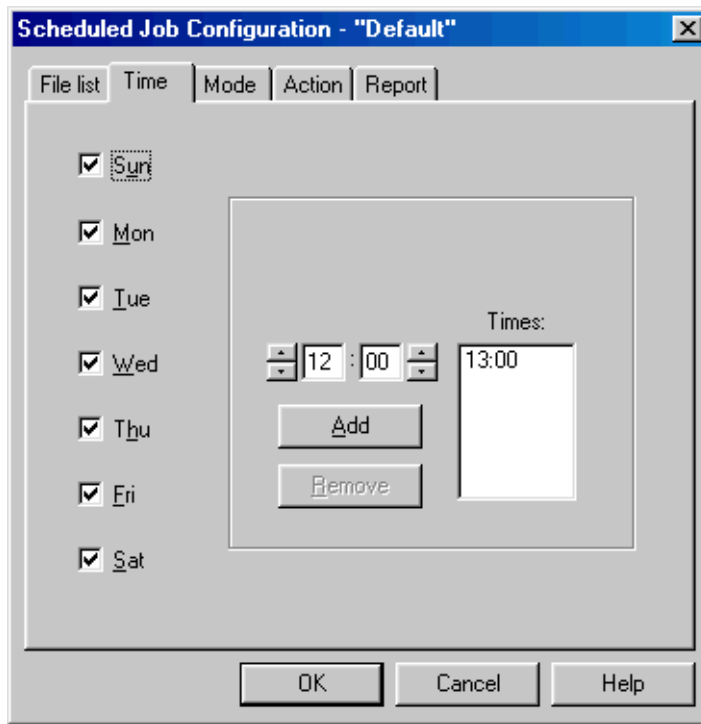


The file list shows drives and files to be scanned by a scheduled job. You can modify the list by using the **Add**, **Remove** and **Edit** buttons.

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

## 5.5 Time (scheduled mode only)

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



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** then click **OK**.

### Remove

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

## 6 Configuring InterCheck

This chapter describes how to configure InterCheck (on-access scanning) running on Windows 95/98/Me workstations.

- ❓ **InterCheck** (also called InterCheck Client) intercepts files as they are accessed by the user. It uses checksumming to determine whether files have changed since the last time they were last scanned. If they have changed, InterCheck sends them for scanning. If not, InterCheck grants the user access.
- 💡 This section only describes commonly-used options. For the full list, see the *InterCheck advanced user guide*, available from the Sophos website.

This section contains the following information:

- Is it necessary to configure InterCheck (section 6.1)?
- How is InterCheck configured (section 6.2)?
- Configuring what InterCheck checks (section 6.3).
- Configuring disinfection (section 6.4).
- A list of commonly-used configuration options (section 6.5).

### 6.1 Is it necessary to configure InterCheck?

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

- specify the types of file to be checked
- achieve a balance between initial checking of files and subsequent requests for checking
- configure InterCheck to specify that a file sent for scanning should be disinfected if found to contain a virus.

## 6.2 How is InterCheck configured?

To configure InterCheck, edit the configuration file Interchk.cfg.

**If you installed Sophos Anti-Virus on a standalone computer**, edit the Interchk.cfg file in the Sophos SWEEP folder. By default, this folder is located at

C:\Program Files\Sophos SWEEP

**If you installed Sophos Anti-Virus on networked computers from a central installation directory (CID)**, edit the central Interchk.cfg file by default located in

- the Interchk share on a Windows NT/2000 server
- the SWEEP folder in the SYS volume on a NetWare server
- the InterChk or Sophos directory on a Unix server.

When you edit InterChk.cfg in a CID, the changes will take effect on all Windows 95/98/Me workstations the next time they log in.

### 6.2.1 Editing the configuration file

InterChk.cfg consists of one or more section headers under which you enter configuration options (listed in [section 6.4](#)). Here is an example:

```
[InterCheckGlobal]
Exclude=Config.sys
[SweepVxDGlobal]
DisinfectDisks=YES
DisinfectDocuments=YES
```

The section headers indicate different kinds of options, and differentiate options that apply to all workstations from those that apply to specific workstations.

**[InterCheckGlobal]** applies to all workstations.

**[InterCheckWorkStation]** applies to specified workstations.

**[SweepVxDGlobal]** applies to all workstations.

**[SweepVxDWorkStation]** applies to specified workstations.

Certain options can be used only under the **[SweepVxDGlobal]** or the **[SweepVxDWorkStation]** header. They are indicated in [section 6.5](#).

## 6.3 Configuring what InterCheck checks

InterCheck sends files for scanning at the following times:

- **At start up**, when a scan is run on the workstation to ensure it is virus-free (see section 6.3.1).
- **During run-time**, when modified items and items that have not previously been checksummed are sent for scanning before they can be accessed (see [section 6.3.2](#)).

The levels of checking and scanning at both stages are fully configurable.

### 6.3.1 Virus scanning at InterCheck start up

InterCheck sends files for scanning

- when InterCheck is first installed and run
- each time the computer is started
- after a Sophos Anti-Virus or IDE update.

The sections below describe each kind of scan and the options used to configure it.

#### 1. Initial InterCheck start up

An initial scan is run after InterCheck is first installed and activated on the computer. This is to check that the system is initially virus-free and to create the initial authorised list of checksums.

The level of scanning at this stage can be set using `InstallCheckLevel`. The default setting (QUICK) includes all fixed disk boot sectors, memory and files defined as executables.

#### 2. Normal InterCheck start up

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

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

### 3. InterCheck start up after a Sophos Anti-Virus or IDE update

After an update the default level of scanning is the same as that at normal InterCheck startup.

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

#### Scanning levels at start up

NONE	No scan is performed.
SYSTEM	Memory, boot sectors, COMMAND.COM and hidden system files are scanned.
QUICK	A quick scan of all memory, boot sectors and executables (including COMMAND.COM and hidden system files) on all fixed disks.
FULL	A full scan of memory, boot sectors and executables (including COMMAND.COM and hidden system files) on all fixed disks.
USER	The scan is executed with the command line qualifiers specified by InstallSweepOptions, LoadSweepOptions or UpdateSweepOptions. If the relevant option is not given, the scan executes without any qualifiers.

#### File types defined as executables

You can change the list of file types treated as executables at each kind of start up. To do this, use InstallSweepOptions, LoadSweepOptions or UpdateSweepOptions to run W95SWEEP with the -EX qualifier and a list of file extensions.

See the *InterCheck advanced user guide* for details.

### 6.3.2 Virus checking at InterCheck run-time

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

The Exclude option specifies files to be excluded from scanning.

## 6.4 Configuring disinfection

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

```
[InterCheck Global]
SweepVxDLoad=YES

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

## 6.5 Configuration options

### **DisinfectDisks=YES|NO**

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

This option is valid only under a SweepVxD header.

### **DisinfectDocuments=YES|NO**

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

This option is valid only under a SweepVxD header.

### **Exclude= <file>**

This option is used to exempt a file from checking. The filename 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 scanning 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**

This option defines which files are scanned for viruses when InterCheck is first executed (i.e. installed and then run) on a workstation. The default is QUICK.

See [section 6.3.1](#) for more information.

**InstallSweepOptions= <qualifiers>**

This option defines the command line qualifiers used when InterCheck is first executed on a workstation. For example, to generate a report as InterCheck is installed, use

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

If InstallCheckLevel is set to NONE, InstallSweepOptions has no effect. If InstallCheckLevel is set to SYSTEM, QUICK or FULL, the scanning options specified by InstallSweepOptions take priority.

**LoadCheckLevel=NONE|SYSTEM|QUICK|FULL|USER**

This option defines which files are scanned for viruses at normal InterCheck startup. The default is SYSTEM.

See [section 6.3.1](#) for more information.

**LoadSweepOptions= <qualifiers>**

This option defines the command line qualifiers used at normal InterCheck start up. For example, to generate a report from each workstation as InterCheck is loaded, use

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

If LoadCheckLevel is set to NONE, LoadSweepOptions has no effect. If LoadCheckLevel is set to SYSTEM, QUICK or FULL, the scanning options specified by LoadSweepOptions take priority.

**PopUpErrorText= <text>**

This option defines a text string 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. This can result in fewer than 52 characters being available for use.

### **ProgramExtensions= <extensions>**

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

If no extensions are given, the default extension list will be used. To see the default list of extensions, open the **Sophos Anti-Virus** window and on the **Options** menu click **Executables**.

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

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

See also [section 6.3.2](#).

### **SweepVxDLoad=YES|NO**

This option controls whether or not to use any options defined under a SweepVxD header. When InterCheck is installed locally on Windows 95/98/Me workstations, the installation program automatically adds the option SweepVxDLoad=YES. This should not be changed.

### **SweepVxDMode=FULL|QUICK**

This option controls the level used by InterCheck to scan 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 SWEEPVxD 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**

This option controls the amount of information included in the SweepVxD 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 scanned for viruses when InterCheck detects a new version of Sophos Anti-Virus. The default is SYSTEM.

See [section 6.3.1](#) for more information.

**UpdateSweepOptions= <qualifiers>**

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

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

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

## 7 Alerts configuration options

This section describes how to configure the alert options available for notifying users about

- scanning activity
- virus finds
- errors.

💡 These options apply to immediate and scheduled scanning only.

These options are configured in the **Notification configuration** dialog box. To open the dialog box, open the **Sophos Anti-Virus** window and click **Alerts**.



The sub-sections in this section describe the tabbed pages in the **Notification configuration** dialog box.

## 7.1 Common options

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

### Disable notification

You can turn off the form of notification in the currently-selected tabbed page.

### Job specification

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

**Specific jobs** enables 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

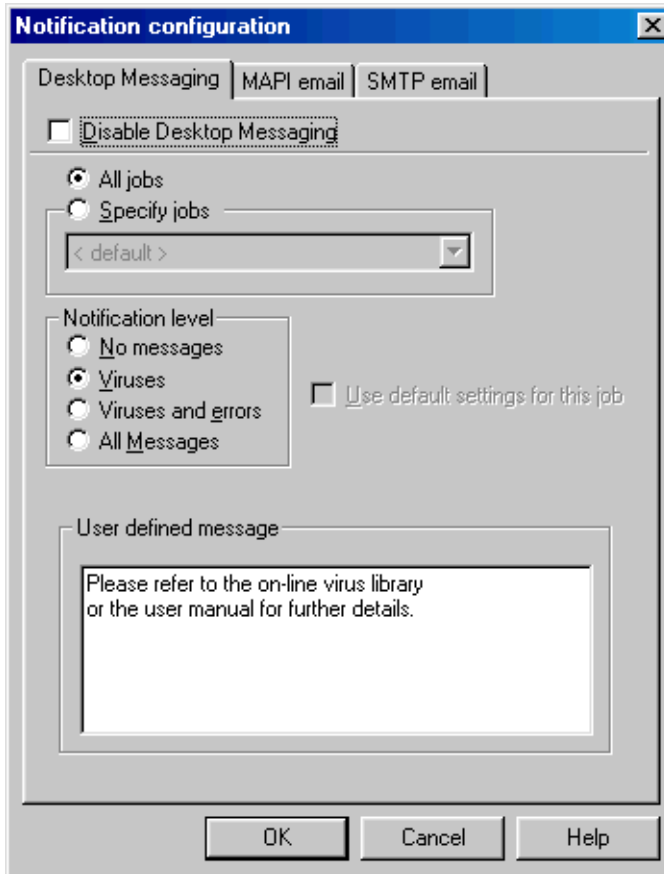
There are four levels of notification to choose from:

- 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.

## 7.2 Desktop messaging

The **Desktop Messaging** tabbed page controls the message displayed when a virus is discovered.



### User defined message

The message in this text box is added to the end of the standard virus-detected message.

## 7.3 MAPI email

The **MAPI email** tabbed page enables you to configure immediate and scheduled scanning to send email notifications on discovery of a virus. This form of notification is only available if Microsoft Exchange is installed.



### Recipient e-mail addresses

Add and remove email addresses for the recipients of the notification emails.

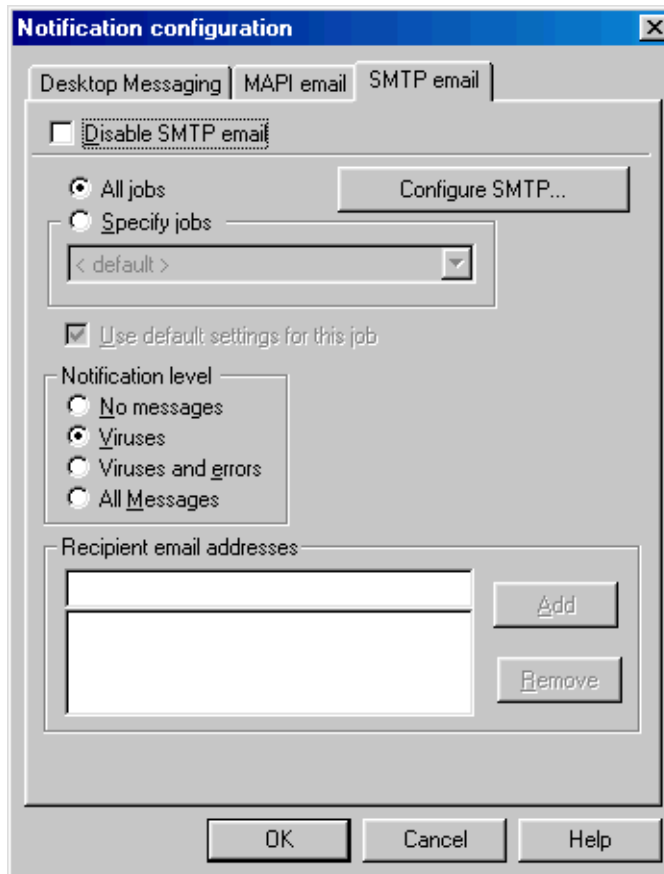
### Configure MAPI

To send emails, 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.

1. Click **Configure MAPI**.
2. In the **Set up MAPI profile** dialog box, choose the MAPI profile you want to use.

## 7.4 SMTP email

The **SMTP email** tabbed page enables you to configure Sophos Anti-Virus to send SMTP email alerts. Mail is sent when a scanning job is completed.



### Recipient email addresses

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

### Configure SMTP

It is necessary to enter details of the SMTP server as follows.

1. Click **Configure SMTP**.
2. In the **Set up SMTP** dialog box, under **SMTP server** enter the host name or IP address of the SMTP server.
3. Under **SMTP sender address**, type the email address from which alert emails should appear to originate. Bounces and non-delivery reports will be sent to this address. If no address is entered, no bounces or non-delivery reports will be sent.

## 8 Global configuration options

This section describes the global configuration options accessible from the menu bar in the **Sophos Anti-Virus** window. It contains the following information:

- How to trigger an immediate scan of memory (section 8.1).
- How to change the location of the Sophos Anti-Virus log folder (section 8.2).
- How to change the files defined as executables for all scanning modes (section 8.3).
- How to exclude files or file types from scanning by all scanning modes (section 8.4).
- How to restore the default configuration (section 8.5).
- How to clear the Sophos Anti-Virus log (section 8.6).
- How to disable the progress bar displayed during a scan (section 8.7).

These options are independent of the scanning mode tabbed pages.

### 8.1 Sweep memory

Prompts Sophos Anti-Virus to carry out an immediate scan of memory to locate memory-resident viruses.

On the **File** menu, click **Sweep memory**.

- 💡 Sophos Anti-Virus scans memory for memory-resident viruses automatically when it is first started.

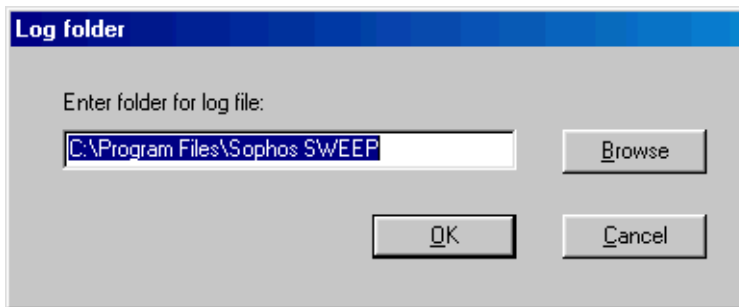
## 8.2 Set log folder

Enables you to change the location of the log file.

Sophos Anti-Virus maintains a continuous log of all its activity. This log file contains administrative messages along with the on-screen log messages (see [section 4](#)). It is generated in addition to the report file, which is aimed at the user (see [section 5.3](#)).

By default the log file is saved in the Sophos SWEEP folder, but you can change it as follows.

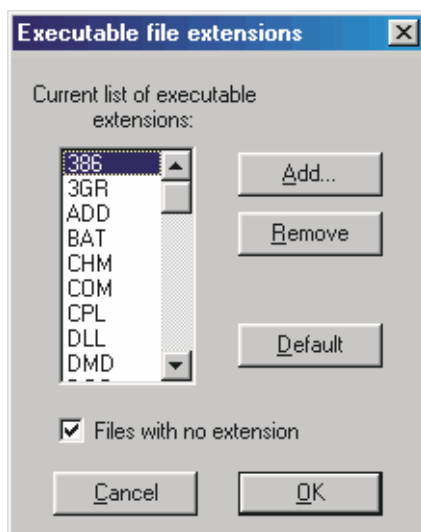
1. In the **Sophos Anti-Virus** window, on the **File** menu, click **Set log folder**.
2. In the **Log folder** dialog box, specify a folder either by typing the path or by using the **Browse** button, and click **OK**.



## 8.3 Executables

Enables you to configure the types of files scanned when Sophos Anti-Virus is configured to scan executables only.

1. On the **Options** menu, click **Executables**.
2. In the **Executable file extensions** dialog box, specify the file extensions you want to define as executables. Select **Files with no extension** if you also want to include such files.

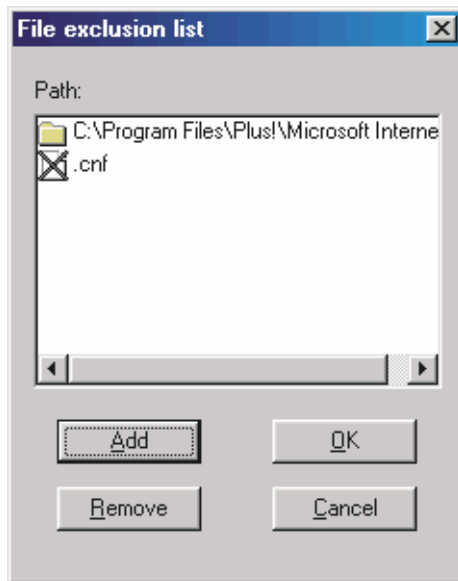


This list is used by Sophos Anti-Virus only if it is set to check **Executables** rather than **All** file types. See [section 1.2.3](#) for more information.

## 8.4 Exclusion List

Enables you to exclude files from scanning as follows.

1. On the **Options** menu, click **Exclusion List**.
2. To add or remove files from the list, click **Add** or **Remove**. You can also specify file extensions to be excluded from scans.



## 8.5 Restore defaults

Restores the default settings.

On the **Options** menu, click **Restore Defaults**.

**!** This option destroys all scheduled jobs.

## 8.6 Clear log

Clears the on-screen log. The on-screen log records information from the current session only. Selecting this option does not clear the continuous log.

On the **Options** menu, click **Clear Log**.

For information about the on-screen log, see [section 4](#).

## 8.7 Progress bar

Determines whether or not the progress bar is displayed during the type of scanning whose tabbed page is currently selected.

On the **View** menu, click **Progress Bar**.

- 🔦 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 is saved by disabling this option. It will not affect any jobs that are already running.

## 9 Sophos Anti-Virus command line qualifiers

### **-AUTO Auto start and exit**

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

```
SWEEP95 -AUTO
```

forces it to perform an immediate scan, with all user-input, stop and unload options disabled.

If no viruses or errors are detected, Sophos Anti-Virus unloads at the end of the job. If viruses or errors are detected, Sophos Anti-Virus displays its normal messages and re-activates all controls.

### **-I Auto start**

Forces Sophos Anti-Virus to perform an immediate scan as soon as it is loaded. User input is not disabled, and Sophos Anti-Virus will not unload at the end of the immediate job.

You can also set Sophos Anti-Virus to start as soon as Windows 95/98/Me starts by placing a shortcut to it in the Windows 95/98/Me StartUp folder.

### **-NI No interrupting**

Suppresses all options to stop Sophos Anti-Virus. The **STOP** button and all internal unload mechanisms are disabled.

When combined with the -I option, all these options are disabled until the end of the immediate job, when they will be re-activated.

### **-NM No memory check**

Suppresses the scanning of memory during Sophos Anti-Virus startup.

### **-NW No warning messages**

Suppresses any warning messages during Sophos Anti-Virus startup. This option is used when Sophos Anti-Virus is installed to start automatically.

## ***Troubleshooting***

## 10 Troubleshooting

This section provides answers to some common problems that you may encounter when using Sophos Anti-Virus for Windows 95/98/Me. [Section 4](#) describes error messages in the on-screen log.

If your problem is not described in either of these sections, refer to the Sophos website [www.sophos.com](http://www.sophos.com) which includes a support knowledgebase, virus analyses, the latest IDEs, product downloads and technical articles.

If your problem is not described on the website, contact Sophos [technical support](#).

### 10.1 Scanning runs slowly

#### Full scan

By default, Sophos Anti-Virus performs a quick scan, which scans only the parts of files likely to contain viruses. However, if scanning is set to full, it scans everything, and takes significantly longer to carry out a scan. See [section 5.1](#).

- ❗ **Full scanning is needed in order to detect some viruses, but should only be enabled on a case-by-case basis (e.g. on advice from Sophos technical support).**

#### Checking all files

By default, Sophos Anti-Virus checks only files defined as executables. If it is configured to check all files the process takes longer (see [section 1.2.3](#)). If you would like to scan other specific extensions, as well as executable files, add those extensions to the list of extensions Sophos Anti-Virus defines as executables (see [section 8.3](#)).

#### Network drives selected

Network drives may be much larger than a local hard disk, so take significantly longer to scan. Most network interfaces provide much slower access than a local hard disk, which can further slow down the scan.

#### Progress bar selected

If the progress bar is displayed, Sophos Anti-Virus must count all the items it will scan. This can take several minutes on large network drives. Enable or disable the progress bar by opening the **Sophos Anti-Virus** window and clicking **Progress Bar** on the **View** menu.

## 10.2 Auto-updating fails to happen

### **The central installation directory (CID) has not been updated**

Ensure you have updated the CID that workstations poll for updates. You can use SAVAdmin to check which CID a computer is polling, as long as Sophos Anti-Virus was installed in such a way as to enable SAVAdmin to access Windows 95/98/Me workstations (see the installation guide that you used to install Sophos Anti-Virus).

In SAVAdmin, locate a workstation that has not auto-updated. Scroll right to the **Central Installation Directory** column. The CID that the computer polls for updates is displayed in the column.

If this CID is not the one you updated, update it now.

### **Workstations do not update until they are restarted**

A Windows 95/98/Me workstation will normally only update from an updated CID the next time it is restarted.

You can configure the workstation to poll the CID for updates during a session by adding the qualifier `-poll=x` (where `x` is the polling frequency in seconds) to the login script. See the installation guide that you used to install Sophos Anti-Virus.

## 10.3 Scheduled scans do not run

In Sophos Anti-Virus for Windows 95/98/Me scheduled scans only run if the computer is switched on and the **Sophos Anti-Virus** window is open.

You can configure Sophos Anti-Virus to run scheduled scans when the **Sophos Anti-Virus** window is not open using AT.INI. This is described in the appendix of the *Sophos Anti-Virus DOS/Windows 3.1x user manual*.

## 10.4 Virus fragment reported

The report of a virus fragment indicates that part of a file matches part of a virus. There are three 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. If you suspect that this is the case, please send Sophos a sample and a description.

### **Corrupted virus**

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by Sophos Anti-Virus. A corrupted virus cannot spread. If a virus fragment is reported, contact Sophos [technical support](#) for advice.

### **Database containing a virus**

When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file. Contact Sophos [technical support](#) for advice.

## **10.5 Virus not disinfected**

If Sophos Anti-Virus has not attempted to disinfect a virus ('No action taken'), check that automatic disinfection is selected (see [section 5.2](#)).

If Sophos Anti-Virus could not disinfect the virus, ('Disinfection failed'), it may be that it cannot disinfect that type of virus (see [section 3](#) or contact Sophos [technical support](#)).

If dealing with a disk or removable media, make sure that it is not write-protected.

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

See also [section 3](#).

## **10.6 Sophos Anti-Virus reports errors**

After a scan, Sophos Anti-Virus may report that some errors were found. There are two main reasons for errors:

### **File is corrupt**

It can therefore not be scanned by Sophos Anti-Virus.

### **File is encrypted**

If the file contains macros (for example it is a .doc or .xls file), only the main body of the file will have been encrypted (not the macros). You may be warned that the file is encrypted, but the parts of the file that can contain macro viruses will still be scanned.

## ***Glossary and index***

## Glossary

<b>Boot sector</b>	The first part of the operating system to be read into memory when a computer 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.
<b>Boot sector virus</b>	A type of virus that subverts the initial stages of the booting process. A boot sector virus attacks either the master boot sector or the DOS boot sector.
<b>Checksum</b>	A value calculated from item(s) of data. InterCheck creates a list of checksums of the files on the computer. If the checksum of a file is found to have changed, it is sent for scanning because it may have become infected with a virus.
<b>CID</b>	Central installation directory; a central copy of Sophos Anti-Virus files from which Sophos Anti-Virus is installed and updated automatically on the server and workstations. You must create a different CID for each platform on the network, and remember to keep every CID up to date.
<b>DOS boot sector</b>	The boot sector which loads the BIOS and DOS into RAM and starts their execution. A common point of attack by boot sector viruses.
<b>Executables</b>	By default Sophos Anti-Virus will check only files it defines as executables (even when full scanning is enabled). It is possible to configure Sophos Anti-Virus to check all files ( <a href="#">section 1.2.3</a> ), or to change the list of files defined as executables ( <a href="#">section 8.3</a> ).
<b>Full scan</b>	If configured to full scanning, Sophos Anti-Virus scans all files and all parts of files in the area it has been configured to scan. A full scan takes significantly longer than a quick scan. It is occasionally necessary in order to locate certain viruses. See <a href="#">section 5.1</a> .

<b>IDE</b>	Virus identity file; enables Sophos Anti-Virus to detect a specific virus. You need IDEs to protect your network against viruses discovered since your version of Sophos Anti-Virus was compiled.
<b>Immediate scan</b>	A virus scan that is triggered by the user from the Sophos Anti-Virus window. It is possible to configure what is scanned, how it is scanned and what action should be taken if a virus is found.
<b>InterCheck/InterCheck Client</b>	A component of Sophos Anti-Virus that intercepts files as they are accessed, and uses checksumming to determine whether or not they should be sent for virus scanning. It can be installed on servers, then switched off if found to affect performance.
<b>InterCheck Server</b>	A component of Sophos Anti-Virus that enables workstations to send virus alerts to a central location.
<b>Macro virus</b>	A type of virus that uses macros in a data file to become active in memory and attach itself to other data files. Unlike other types of virus, macro viruses can attain a degree of platform independence.
<b>Mapped directory</b>	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.
<b>Master boot sector</b>	The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the computer is switched on (booted). It contains the partition table as well as the code to load and execute the boot sector of the 'active' partition.
<b>Memory-resident virus</b>	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.

<b>Quick scan</b>	The default scan type. Sophos Anti-Virus scans only the parts of files that can potentially contain executable code.
<b>SAVAdmin</b>	A Sophos administration tool that enables you to copy and paste installations of Sophos Anti-Virus between Windows NT/2000/XP computers on a network, and check they are up to date. See also the <i>SAVAdmin user manual</i> .
<b>Scheduled scan</b>	A virus scan that is scheduled by the user to take place at a particular time. As with immediate scanning, it is possible to configure what is scanned, how it is scanned and what action should be taken if a virus is found. Sophos Anti-Virus for Windows 95/98/Me by default carries out a scheduled scan at 9pm every day, as long as the computer is switched on and the Sophos Anti-Virus window is open.
<b>SMTP</b>	Simple Mail Transport Protocol; the delivery system for Internet email.
<b>SWEEP</b>	A less common term used to describe the component of Sophos Anti-Virus that carries out immediate and scheduled scanning.
<b>SweepVxD</b>	An InterCheck driver file.
<b>UNC</b>	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.
<b>Virus</b>	A computer program that can spread across computers and networks by attaching itself to a program (such as a macro or boot sector) and making copies of itself.

# Index

## A

alert messages  
 desktop messaging 46  
 disabling 45  
 job specification 45  
 MAPI email 47  
 notification level 45  
 SMTP email 48  
 archive files  
 scanning 30  
 automatic disinfection 16

## B

boot sector  
 DOS, replacing 17  
 master, replacing 17  
 boot sector virus  
 disinfection 31

## C

compressed files  
 scanning 30

## D

default settings  
 restoring 52  
 desktop messaging 46  
 disinfection 15–20, 31  
 automatic 16  
 boot sector 31  
 documents 31  
 mailboxes 32  
 removing infected files 32  
 unsuccessful 58  
 documents  
 disinfection 31

## E

excluding files from scanning 52  
 executables  
 defining 51  
 limiting scanning to 10

## F

floppy disk  
 disinfecting boot sector 16, 31  
 full scan 29

## H

hard disk  
 disinfecting boot sectors 17, 31

## I

immediate scanning 9–25  
 adding items for scanning 10  
 level 29  
 priority 29  
 removing items from scanning 10  
 starting 9  
 infected executables  
 dealing with 32  
 infected files  
 removal 32  
 shredding 32  
 InterCheck 13–25  
 disinfection 40  
 virus alert message 41  
 what is checked 38–54  
 InterCheckGlobal section header 37  
 InterCheckWorkStation section header 37  
 INTERCHK.CFG 37  
 IP address 48

## L

log file 33, 45, 50

## M

mailboxes  
 disinfection 32  
 scanning 30  
 MAPI email 47  
 master boot sector  
 disinfection 17  
 memory  
 scanning 49

## N

notification level 45

## O

on-demand scanning 9–25  
 removing items from scanning 10  
 starting a scan 9  
 on-screen log 45  
 clearing 52

## P

progress bar 53

## **Q**

quick scan 29

## **R**

report file 45

## **S**

scanning mailboxes 30

scheduled scanning

  changing a job 12

  default job 11

  file list 34

  level 29

  priority 29

  setting times 35

SMTP email 48

Sophos Anti-Virus

  configuring 28–54

  disinfection 31

  excluding files to be checked 52

  log file 50

  log folder 50

  on-access scanning 13–25

  priority 29

  reporting 33–54

  restoring default settings 52

  scanning archive files 30

  scanning level 29

subfolders

  scanning 10

SWEEP VxD

  log file 42–43

SweepVxDGlobal section header 37

SweepVxDWorkStation section header 37

## **V**

virus

  disinfection 15–20, 31

  recovery from 20

  side-effects 20–25

virus fragment 57