Sophos Anti-Virus

User Manual

Windows 95

SOPHOS

Sophos Anti-Virus

for Windows 95

User Manual
May 1998

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

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

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

Tel +44 1235 559933 • Fax +44 1235 559935

9 8 7 6 5 4 3 2 1

Part # mas9ez0s/980420

This document is also available in electronic form from Sophos.

Technical support hotline:
Email support@sophos.com, Tel +44 1235 559933

Contents

About Sophos Anti-Virus 9

What is Sophos Anti-Virus? 9
How does it work? 9
Features of Sophos Anti-Virus for Windows 95 10
How to use this manual 11
Summary of each chapter 11

About InterCheck 13

What is InterCheck? 13
How does InterCheck work? 14
What types of InterCheck installation are there? 14
Local and central checksum files 16
Features of InterCheck 16
Overview of InterCheck installation and configuration 17
Networked InterCheck clients 17
Stand-alone InterCheck clients 17
Cross-platform support 18
InterCheck server 18
Networked InterCheck clients 18
Stand-alone InterCheck clients 18

Installing SWEEP 19

System requirements 19
Preparing for installation 19
Local or central installation? 19
Which features should be installed? 20
Starting the SWEEP installation program 21

Local installation of SWEEP 22
Installation type 22
Folder selection 23
Startup options 24
Updating a local installation of SWEEP 25
Installation type 25
Update options 26
Folder selection 26
Upgrade components 27
Startup options 28
Central installation of SWEEP (stage 1) 29
Installation type 29
InterCheck folder selection 30
Folder selection 31
Central installation options 32
Auto-upgrade mode 33
Central installation of SWEEP (stage 2) 34
Manual installation 34
Automatic installation 35
Updating a central installation of SWEEP (stage 1) 35
Installation type 36
InterCheck folder selection 36
Folder selection 36
Upgrade components 37
Central installation options 38
Auto-upgrade mode 38
Updating a central installation of SWEEP (stage 2) 39
Update options 40
Folder selection 40
Updating SWEEP with new virus identities 41

Using SWEEP 43

Starting SWEEP 43
Overview of the SWEEP display 44
Immediate mode 45
Starting an immediate sweep 45
Default immediate mode file list 45
Adding new items for immediate sweep 46
Removing items from immediate sweep 47
Editing an item for immediate sweep 47

Scheduled mode ... 47
Default scheduled mode job list ... 47
Adding a new scheduled job ... 48
Removing a scheduled job ... 49
Editing a scheduled job ... 49

Configuring SWEEP ... 51

About configuring SWEEP ... 51
Sweeping mode ... 52
Sweeping level ... 52
Priority ... 52
Compressed files ... 53
Action on virus detection ... 53
Disinfect boot sectors ... 53
Disinfect documents ... 54
Infected files ... 54
Request confirmation ... 54
Notification on virus detection ... 55
Notify timing ... 55
Notification list ... 56
Reporting results ... 56
Report mode ... 56
Report file ... 57
File list (scheduled mode only) ... 57
Time (scheduled mode only) ... 58

SWEEP options ... 59

Sweep memory ... 59
Set log folder ... 59
Executables ... 60
Exclusion list ... 61
Mail profile ... 62
Restore defaults ... 62
Clear log ... 63
Progress bar ... 63
SWEEP command line qualifiers ... 63
-AUTO Auto start and exit ... 63
-I Auto start ... 64
-NI No interrupting ... 64
-NM No memory check ... 64
-NW No warning messages ... 64

The virus library **65**

Starting the virus library 65
Information on a particular virus 66
Searching for a particular virus 67
Infected objects 67
Memory-resident 68
Disinfectable by SWEEP 68
Trigger conditions 68
Text in description 68

Using Windows 95 InterCheck clients **69**

Stand-alone and networked clients 69
Installing InterCheck clients 69
Starting InterCheck clients 70
InterCheck clients in operation 70
Configuring InterCheck clients 71

Configuring InterCheck clients **73**

Is it necessary to configure the InterCheck client? 73
How is the InterCheck client configured? 73
Configuration option section headers 74
Workstation and global options 74
Configuring individual InterCheck workstations 75
Using network addresses 76
What InterCheck checks 77
Virus checking at InterCheck start-up 77
Virus checking at InterCheck run-time 80
Checksumming options 81
Critical program support 81
Configuring stand-alone InterCheck clients 82
Updating local InterCheck configuration files 82
Configuring the WFWG InterCheck client installation program 83
Configuration options 83
Address=<text> 83
AllowDisable=YES|NO 83
AllowUnload=YES|NO 83
AltCommsDir=<directory> 84
AutoInstallExclude[1...n]=<computer1>,<computer2>... 84
AutoUpdate=ON|OFF 84
CheckFile=<filename> 85
CheckNetwork=YES|NO 85

CheckOn=[EXEC],[ACCESS],[FLOPPY] 85
CommsDirectory=<path> 85
CriticalProgram=<files> 86
DisableTSR=YES | NO 86
Exclude=<file> 86
FileTypeDetection=OFF | WINDOWS_EXE | WORD_MACRO | ALL 87
HaltOnError=YES | NO 88
HaltOnVirus=YES | NO 88
InstallCheckLevel=NONE | SYSTEM | QUICK | FULL | USER 88
InstallDirectory=<path> 88
InstallSweepOptions=<qualifiers> 89
InteractiveInstall=1 | 0 89
LoadCheckLevel=NONE | SYSTEM | QUICK | FULL | USER 89
LoadLow=YES | NO 89
LoadSweepOptions=<qualifiers> 90
MaxAddressLength=<length> 90
MaxPathLength=<length> 90
MemoryCheck=YES | NO 91
MonoMonitor=YES | NO 91
NoDefaultExcludes=YES | NO 91
NoStandardCriticalPrograms 91
PopUpDisplay=OFF | ERROR | ALL 91
PopUpErrorText=<text> 92
ProgramExtensions=<extensions> 92
PurgeChecksumsOnUpdate=YES | NO | DEFAULT 93
ReportEvents=[LOAD],[UPDATE],[INSTALL],[ALL],[NONE] 93
ScanNetPath=YES | NO 94
ServerTimeout=<time> 94
SourceDirectory=<path> 94
StartUpDisplay=NONE | NORMAL | VERBOSE 95
Swap=YES | NO 95
SwapFlags=ANY,EMS,XMS,EXT,DISK 95
SweepVxDLoad=YES | NO 95
SweepVxDMode=FULL | QUICK 96
SweepVxDScanCompressed=YES | NO 96
SweepVxDLogFile=<filename> 96
SweepVxDLogLevel=0..5 96
SystemDirectory=<directory> 96
UpdateCheckLevel=NONE | SYSTEM | QUICK | FULL | USER 97
UpdateLocalCFG=YES | NO 97
UpdateSweepOptions=<qualifiers> 97
UseNetList=YES | NO 98

UseNetSyntax=YES | NO 98
WarnCriticalProgramMissing 98
INTERCHK and ICWIN95 command line qualifiers 99
-ADDRESS=<address> 99
-DISABLE 99
-ENABLE 100
-HELP or -? 100
-NETWORK=NETBIOS | NETWARE 100
-SILENT 100
-STATUS 100
-UNLOAD 101
-VERBOSE 101

Treating viral infection 103

Automatic disinfection 103
Manual disinfection 103
Creating a clean DOS boot disk 104
Manual disinfection of infected boot sectors 105
Manual disinfection of infected executable files 106
Manual disinfection of infected documents 106
Recovering from virus side-effects 107
After disinfection 107

Troubleshooting 109

SWEEP runs slowly 109
Virus fragments 110
False positives 111
Virus not disinfected 111
New viruses 112

On-screen log messages 113

Message categories 113
Virus detected messages 113
Error messages 116

Glossary 119

Index 123

About Sophos Anti-Virus

This chapter introduces Sophos Anti-Virus, describes its key features, and helps users identify the most relevant chapters for their needs.

What is Sophos Anti-Virus?

Sophos Anti-Virus offers on-demand, scheduled and on-access 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 immediate and scheduled scanning of all disks, files and documents, and
- **InterCheck** checks each item as you try to access it, and grants access only if it is virus-free.

SWEEP can be used on its own; the use of InterCheck is optional.

For an introduction to InterCheck, see the 'About InterCheck' chapter.

Features of Sophos Anti-Virus for Windows 95

- Checks local hard disks, floppy disks and networks for the presence of all viruses known to Sophos at the time of release.
- Features an ‘immediate mode’ which allows checking on demand, along with a ‘scheduled mode’ which allows multiple scheduled jobs to be configured for automatic operation.
- Incorporates a stand-alone InterCheck client for on-access scanning.
- Offers two levels of security, allowing a ‘quick sweep’ which looks for virus identities in the parts of a file that are likely to contain a virus, and a ‘full sweep’ which looks for virus fragments in every part of a file.
- Easily detects polymorphic viruses using Sophos’ advanced Virus Description Language (VDL) and a built-in code emulator.
- Detects and disinfects Microsoft Word, Excel and Office 97 macro viruses.
- Can be installed automatically on multiple workstations from a login script.
- Is updated twelve times a year, and urgent updates can be distributed by fax or email or downloaded from the Sophos Web site.
- Provides automatic updating for networked PCs.
- Can notify network managers automatically, via Microsoft Exchange, if a virus is found.
- Includes an extensive on-line virus information database.

Sophos Anti-Virus is also available for Windows NT (Intel & Alpha AXP), Novell NetWare, DOS/Windows 3.x, OpenVMS (VAX & Alpha AXP), OS/2 and Banyan VINES.

How to use this manual

The chapters that will be most helpful depend on the use(s) to which Sophos Anti-Virus will be put.

On-demand scanning

If using SWEEP only for on-demand scanning of a workstation or a network drive, read the 'Installing SWEEP' and 'Using SWEEP' chapters.

More advanced features

If performing a central installation to help distribute SWEEP across a network, and using SWEEP's more advanced features such as scheduling, read the 'Installing SWEEP', 'Using SWEEP', 'Configuring SWEEP' and 'SWEEP options' chapters.

On-demand and on-access scanning

If using SWEEP and InterCheck for on-demand and on-access scanning on a workstation, read the 'Installing SWEEP', 'About InterCheck', 'Using Windows 95 InterCheck clients' and 'Configuring InterCheck clients' chapters.

Summary of each chapter

This manual contains the following chapters:

- **'About Sophos Anti-Virus'**, this chapter.
- **'About InterCheck'** presents an overview of Sophos' InterCheck technology.
- **'Installing SWEEP'** describes how to install and upgrade SWEEP, with or without stand-alone InterCheck support.
- **'Using SWEEP'** describes how to start SWEEP, start an immediate sweep, change the items to be included in immediate jobs, and set up scheduled jobs.

- **‘Configuring SWEEP’** describes the options for configuring the immediate and scheduled modes.
- **‘SWEEP options’** describes the other options available to SWEEP users and lists the SWEEP command line qualifiers.
- **‘The virus library’** describes the virus library.
- **‘Using Windows 95 InterCheck clients’** gives information on the installation and running of InterCheck clients for Windows 95.
- **‘Configuring InterCheck clients’** describes the configuration of InterCheck clients running under Windows 95, Windows for Workgroups, Windows 3.x, and DOS.
- **‘Treating viral infection’** describes how to deal with a virus once it has been discovered.
- **‘Troubleshooting’** provides help with possible problems.
- **‘On-screen log messages’** contains information about the on-screen log messages.

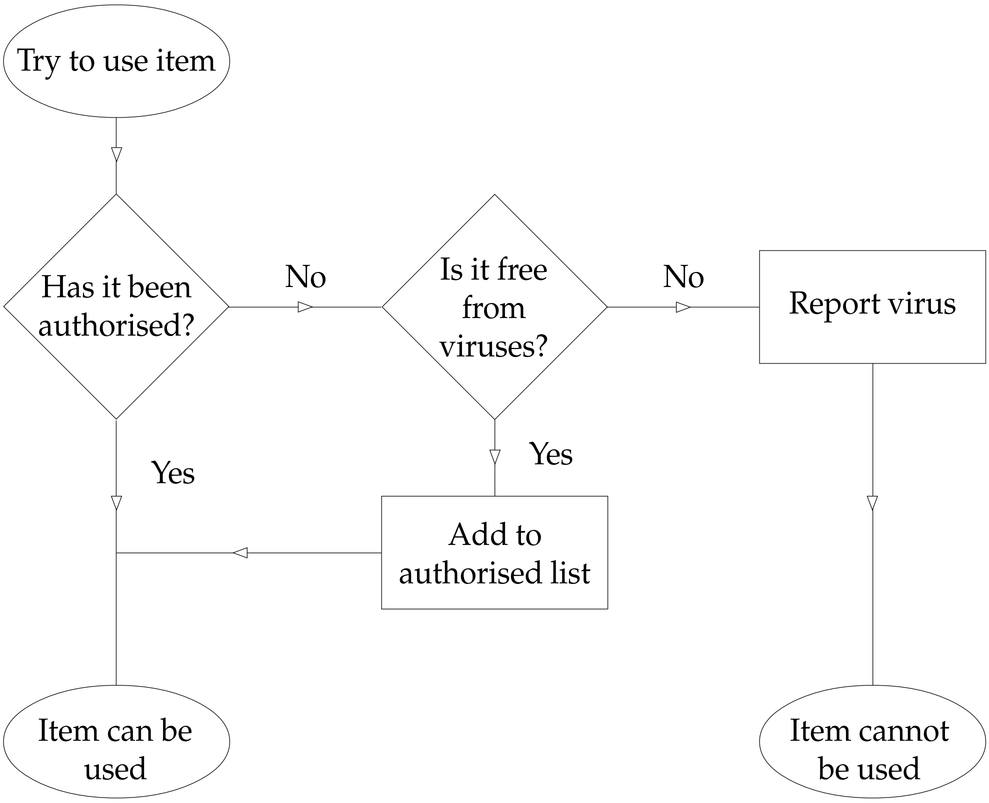
In addition, the ‘Glossary’ contains explanations of some technical terms used in this guide.

About InterCheck

This chapter presents an overview of Sophos' InterCheck technology.

What is InterCheck?

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



The InterCheck principle

How does InterCheck work?

InterCheck splits the task of virus detection between a client and a server.

- The **InterCheck client** identifies items that have not been virus checked.
- The **InterCheck server**, using an installation of SWEEP, performs the actual virus checks.

Whenever an item is accessed, the **client** compares it with a list of authorised items. If a match is found, the access is granted. If a match is not found, the file is sent to the **server** for virus checking.

If the item is found to be clean, it is added to the list of authorised items (a **checksum file**) and access is granted. From then on, access to this item is granted immediately, unless it is modified, in which case authorisation is again automatically requested.

However, if a virus is found, InterCheck denies access, so the workstation cannot be infected.

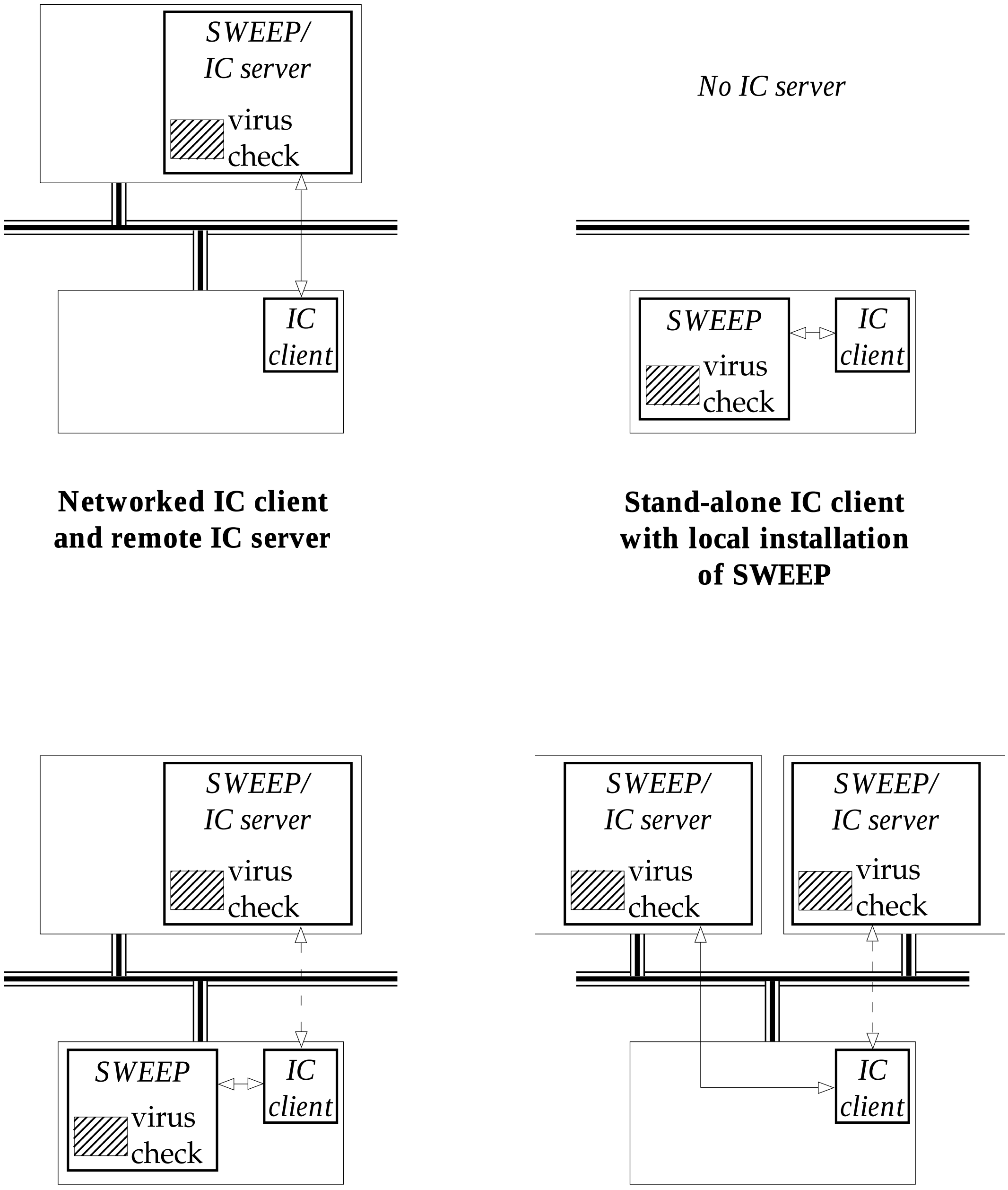
What types of InterCheck installation are there?

There are two main types of InterCheck installation:

- **With networked InterCheck clients.**
  The clients are placed on the workstations to be protected, while the InterCheck server is on a remote machine. The client sends files over the network to the server for virus checking.
- **With stand-alone InterCheck clients.**
  The clients do not have to communicate with a remote InterCheck server, and use a local installation of SWEEP for virus checking.

Networked clients are easier to administer and use fewer system resources on the client workstations.

Stand-alone clients generally offer faster initial authorisation of files, and can also be used on machines not always connected to the network.



Networked IC client and remote IC server

Stand-alone IC client with local installation of SWEEP

Stand-alone IC client with local SWEEP and optional IC server

Networked IC client with remote IC server and backup IC server

Different InterCheck client and server configurations

Local and central checksum files

InterCheck’s list of authorised items can be held locally or centrally.

A **local checksum file** is stored on every workstation, whether it is a stand-alone or networked InterCheck client.

A **central checksum file**, where supported, is stored by the InterCheck server.

A networked InterCheck client, when configured to use the central checksum file, will check it for items that are not in its local checksum file. This means that when one InterCheck client has had an item checked, all other InterCheck clients can access that item without further checking.

Features of InterCheck

Complete cover Of the network: InterCheck provides complete virus-protection for the entire network with minimal performance and memory overheads, and supports the widest range of client and server platforms.

Of the workstation: InterCheck monitors access to all programs, boot sectors, documents, email attachments, Internet downloads, CD-ROMs etc.

Performance Once an item has been authorised, further virus checking is not needed unless it changes or SWEEP is updated. Checking that an item has been authorised is much faster than performing a full virus check.

Automatic reporting Many virus incidents are more serious than they need to be because users fail to report viruses to their managers. If an InterCheck client is connected to the network and a virus is found, a report can be sent to the network supervisor automatically.

Easy administration InterCheck clients can be centrally controlled, configured and updated. Networked InterCheck clients can in many cases be installed automatically over the network.

Portable PCs Stand-alone InterCheck clients can provide the same protection even when a PC is not connected to the network, and can be automatically upgraded when the PC is reconnected to the network.

Overview of InterCheck installation and configuration

Networked InterCheck clients

Networked InterCheck clients are installed by:

1. Installing SWEEP and InterCheck on a file server, and running SWEEP as an InterCheck server.
2. Installing networked InterCheck clients on connected workstations.

For details of installation and configuration, see the Sophos Anti-Virus user manual for the server platform.

Stand-alone InterCheck clients

Stand-alone InterCheck clients are installed on workstations, either from a file server or from CD.

For details of installation, see the ‘Installing SWEEP’ chapter of the Sophos Anti-Virus user manual for the client platform (but in the case of the Windows for Workgroups client, see the ‘Installing InterCheck clients’ chapter of the Sophos Anti-Virus user manual for the server platform).

For details of configuration, see the ‘Configuring InterCheck clients’ chapter of the Sophos Anti-Virus user manual for the client platform (but in the case of the Windows NT client, see the ‘Configuring SWEEP’ chapter of the Sophos Anti-Virus user manual for Windows NT).

Cross-platform support

InterCheck server

‘Native’ versions of SWEEP can provide an InterCheck server on these server platforms:

- Windows NT (Intel & Alpha AXP).
- Novell NetWare & IntranetWare.
- DOS/Windows 3.x.
- OpenVMS (VAX & Alpha AXP).
- OS/2.
- Banyan VINES.

SWEEP for DOS/Windows 3.x can provide an InterCheck server on other operating systems.

Networked InterCheck clients

Networked InterCheck clients are available for the following workstation platforms:

- DOS.
- Windows.
- Windows 95.
- Macintosh (currently with Windows NT and NetWare file servers only).

Stand-alone InterCheck clients

Stand-alone InterCheck clients are available for the following workstation platforms:

- DOS/Windows 3.x.
- Windows for Workgroups.
- Windows 95.
- Windows NT.

Installing SWEEP

This chapter describes how to install and upgrade SWEEP, with or without stand-alone InterCheck support.

Note: If **on-access scanning only** is required, SWEEP does not have to be installed on Windows 95 workstations. Instead, a networked InterCheck client can be used. See ‘Which features should be installed?’ below.

System requirements

- A Windows 95 PC.
- At least 8 Mb of RAM.
- At least 4 Mb hard disk space.

Preparing for installation

This section introduces important points to be considered before installing SWEEP.

Local or central installation?

There are two kinds of installation:

Local installation is used to install SWEEP on a stand-alone PC or single workstation.

Central installation is used to install SWEEP on networked PCs. There are two stages:

1. The installation files are placed on the file server.

2. Installations are made on each workstation from the server to provide a functioning installation.

Central installations allow easy distribution to multiple workstations and automatic upgrading.

Which features should be installed?

SWEEP can be installed with either, or both, of the following optional features:

InterCheck on-access scanning

InterCheck allows on-access checking of all files. There are two ways to install it on Windows 95 workstations.

A stand-alone InterCheck client

This performs virus checking locally, so it is ideal for workstations with no network access.

It can also be used in a networked environment, where it can be installed and updated from a central installation of InterCheck, and can report to a central directory. It provides faster virus scanning than a networked client, but has a higher memory overhead.

The Windows 95 stand-alone client is installed as part of the SWEEP installation process.

A networked InterCheck client

This sends files to an InterCheck server on a remote machine for virus checking. It can be installed and run from the workstation's login script, and is easy to install and administer on large networks.

For instructions on installing the Windows 95 networked client, see the 'Installing InterCheck clients' chapter of the Sophos Anti-Virus user manual for the InterCheck server platform.

Automatic upgrading

A central installation of SWEEP allows subsequent workstation installations to be upgraded automatically whenever the version on the file server is upgraded.

Starting the SWEEP installation program

Start Windows 95 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.bat
```

where `D:` is the CD drive.

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

The installation can also be started by running

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

where `D:` is the CD drive.

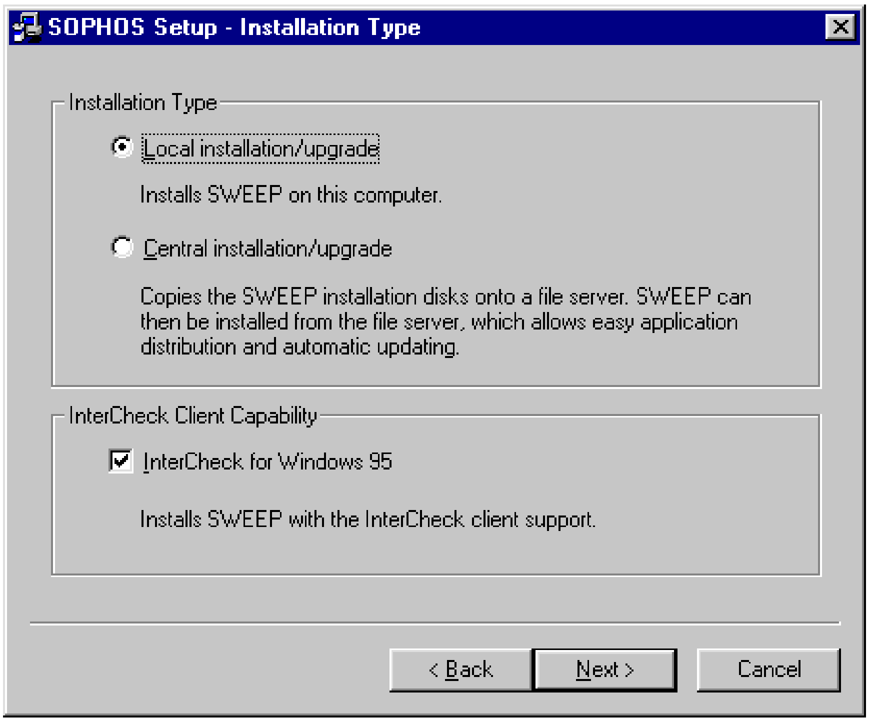
Local installation of SWEEP

This section describes installation of SWEEP on a single workstation.

Start the installation program from the Sophos Anti-Virus CD, as described in the 'Starting the SWEEP installation program' section above.

The installation program presents a series of screens.

Installation type



SOPHOS Setup - Installation Type

Installation Type

● Local installation/upgrade

Installs SWEEP on this computer.

○ Central installation/upgrade

Copies the SWEEP installation disks onto a file server. SWEEP can then be installed from the file server, which allows easy application distribution and automatic updating.

InterCheck Client Capability

☑ InterCheck for Windows 95

Installs SWEEP with the InterCheck client support.

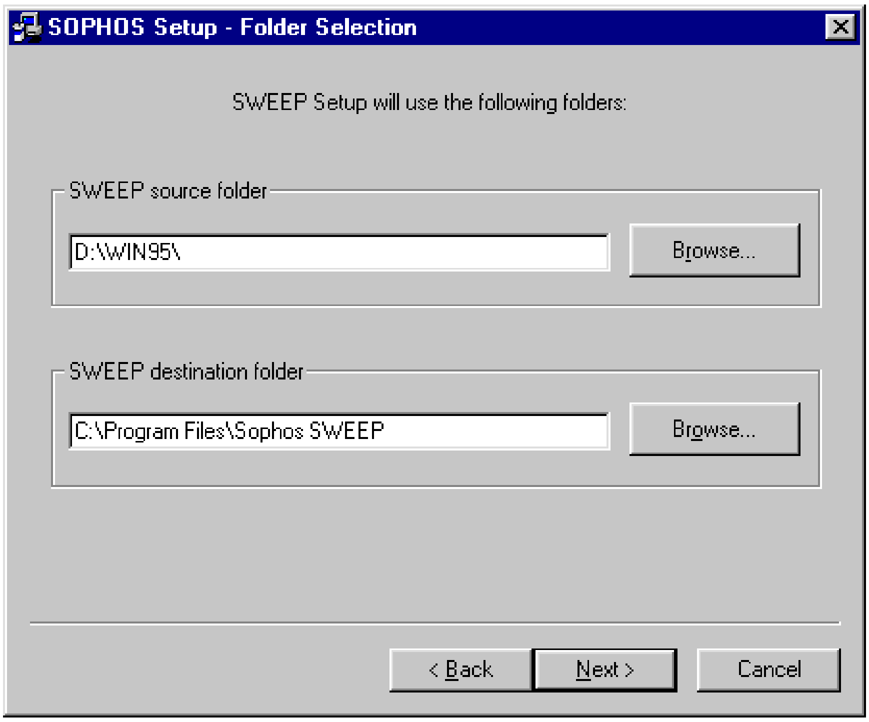
Installation Type

Select 'Local installation/upgrade' to install SWEEP on the workstation.

InterCheck Client Capability

If selected, 'InterCheck for Windows 95' will install SWEEP with the stand-alone InterCheck client. This provides local on-access scanning on the workstation.

Folder selection



SOPHOS Setup - Folder Selection

SWEEP Setup will use the following folders:

SWEEP source folder

D:\WIN95\

SWEEP destination folder

C:\Program Files\Sophos SWEEP

SWEEP source folder

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

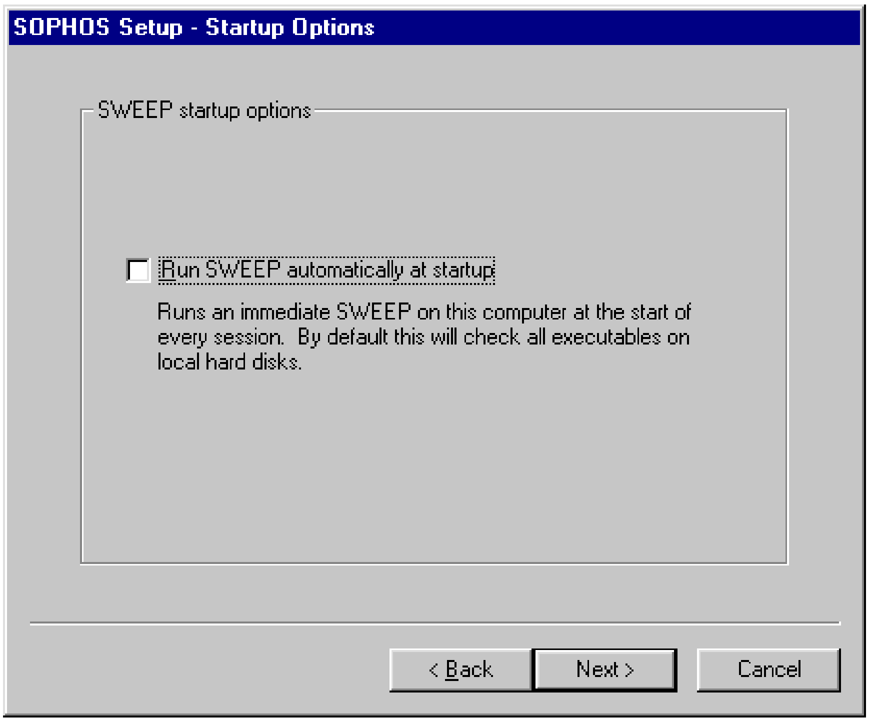
SWEEP destination folder

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

If 'InterCheck for Windows 95' was selected, this is the final installation screen and installation will now be completed.

Startup options

This screen appears only if 'InterCheck for Windows 95' was deselected.



SOPHOS Setup - Startup Options

SWEEP 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.

SWEEP startup options

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

Installation will now be completed.

Updating a local installation of SWEEP

Start the installation program from the Sophos Anti-Virus CD, as described in the 'Starting the SWEEP installation program' section above.

The installation program will run.

When it detects a previous installation, it presents specific update options, in addition to the options usually presented during installation.

In these step-by-step instructions, all screens are described although only those specific to updating are illustrated.

Installation type

Installation Type

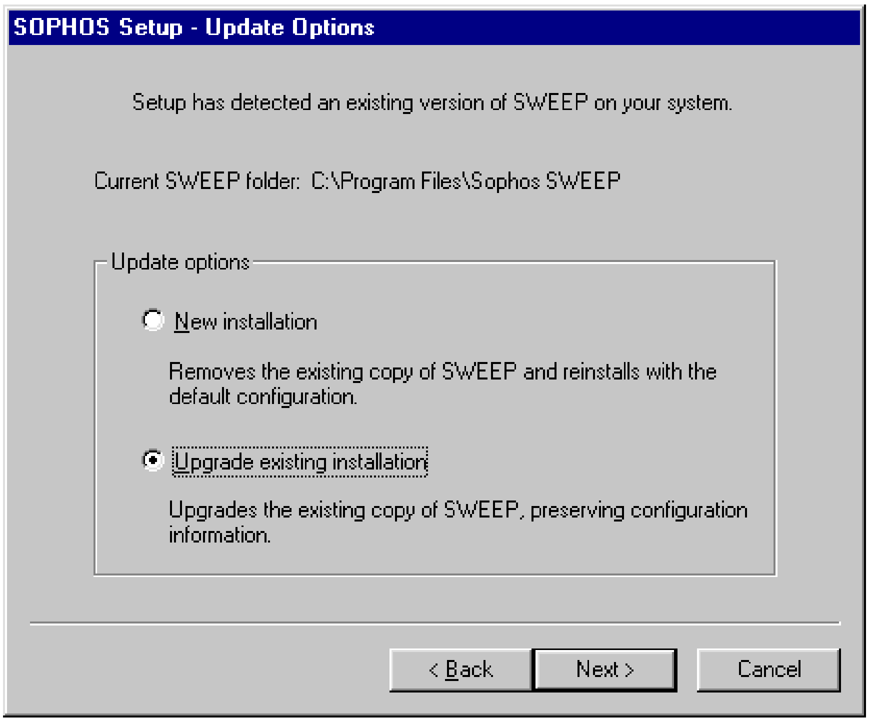
Select 'Local installation/upgrade' to upgrade SWEEP on the workstation.

InterCheck Client Capability

If selected, 'InterCheck for Windows 95' will provide stand-alone on-access scanning on the workstation.

Note: This option can be selected during upgrading even if InterCheck for Windows 95 has not previously been installed.

Update options



SOPHOS Setup - Update Options

Setup has detected an existing version of SWEEP on your system.

Current SWEEP folder: C:\Program Files\Sophos SWEEP

Update options

○ New installation

Removes the existing copy of SWEEP and reinstalls with the default configuration.

● Upgrade existing installation

Upgrades the existing copy of SWEEP, preserving configuration information.

New installation

Installs SWEEP with the default configuration, erasing the previous version and its configuration. Offers the option to change the destination folder.

Upgrade existing installation

Retains the existing configuration, updating the software components.

Folder selection

SWEEP source folder

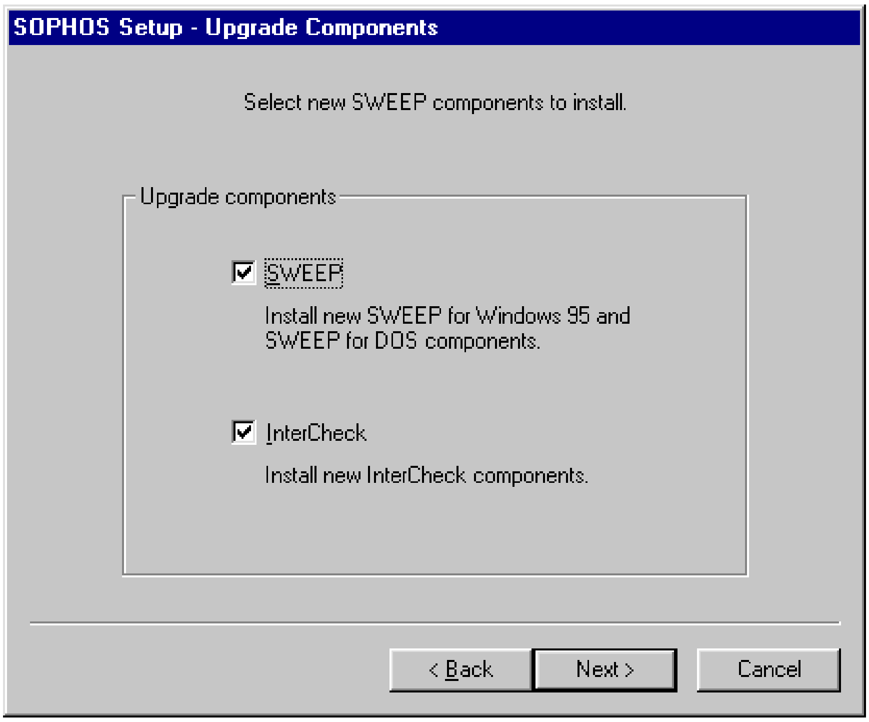
Confirm the SWEEP source folder. This is the folder that contains the SWEEP installation files.

SWEEP destination folder

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

Upgrade components

This option is available only if upgrading SWEEP with InterCheck support.



SOPHOS Setup - Upgrade Components

Select new SWEEP components to install.

Upgrade components

☑ SWEEP

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

☑ InterCheck

Install new InterCheck components.

Either or both of the following must be selected:

SWEEP

Installs new SWEEP for Windows 95 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’ was selected at the ‘Installation Type’ screen, this is the final screen. The upgrade will now be completed.

Startup options

This screen appears only if ‘InterCheck for Windows 95’ was deselected.

SWEEP startup options

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

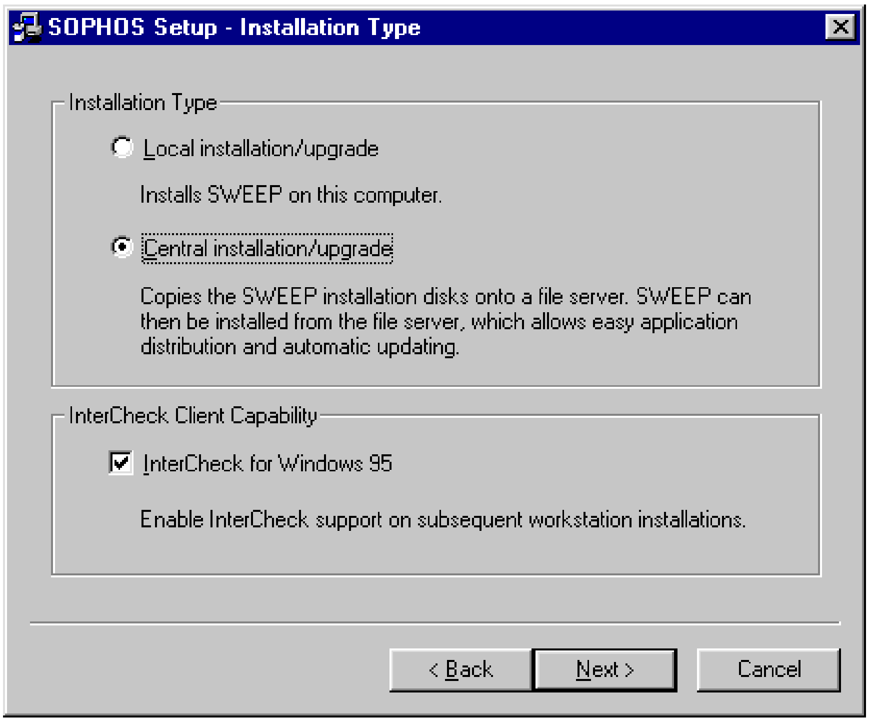
The upgrade will now be completed.

Central installation of SWEEP (stage 1)

In stage 1 of central installation, the SWEEP installation files are placed on a file server.

Start the installation program from the Sophos Anti-Virus CD, as described in the 'Starting the SWEEP installation program' section above.

Installation type



SOPHOS Setup - Installation Type

Installation Type

○ Local installation/upgrade

Installs SWEEP on this computer.

● Central installation/upgrade

Copies the SWEEP installation disks onto a file server. SWEEP can then be installed from the file server, which allows easy application distribution and automatic updating.

InterCheck Client Capability

☑ InterCheck for Windows 95

Enable InterCheck support on subsequent workstation installations.

Installation Type

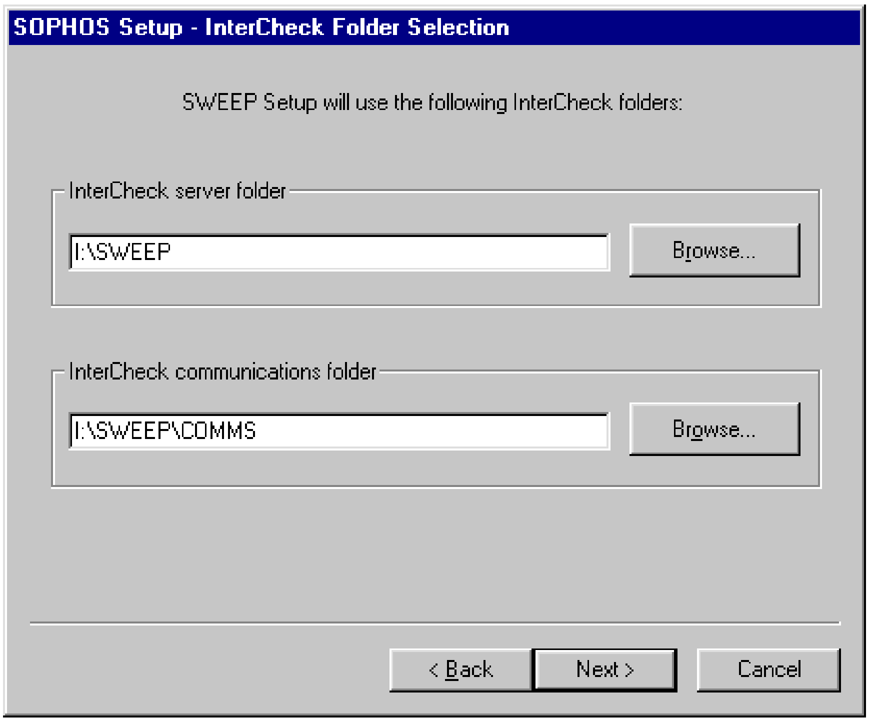
Select 'Central installation/upgrade' to place the SWEEP installation files on the file server.

InterCheck Client Capability

If selected, 'InterCheck for Windows 95' will enable the stand-alone InterCheck client to be installed on subsequent local installations. This will provide local on-access scanning.

InterCheck folder selection

This screen appears only if 'InterCheck for Windows 95' was selected.



SOPHOS Setup - InterCheck Folder Selection

SWEEP Setup will use the following InterCheck folders:

InterCheck server folder: I:\SWEEP

InterCheck communications folder: I:\SWEEP\COMMS

InterCheck server folder

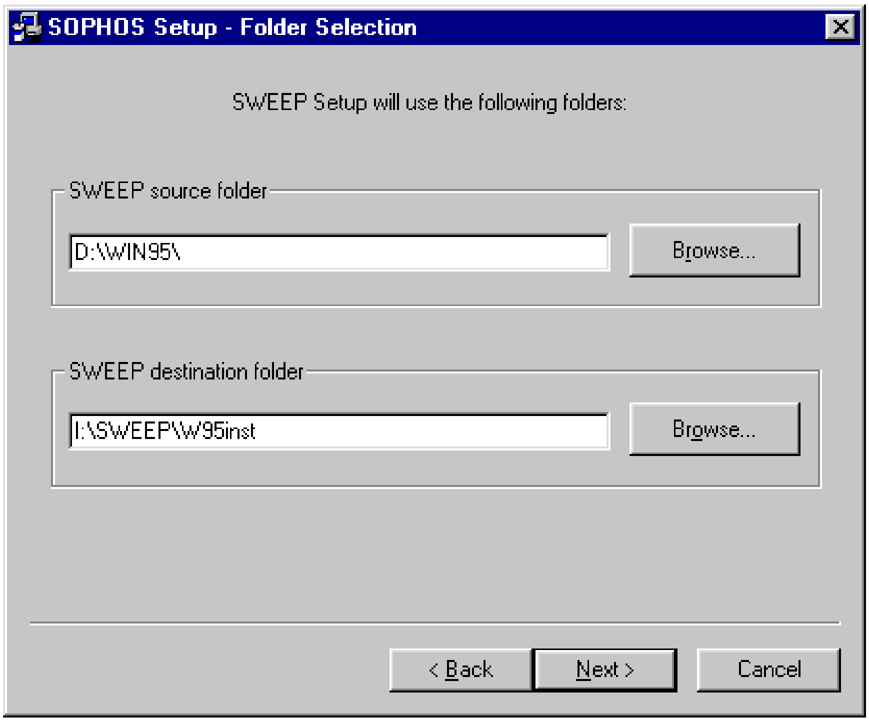
Specify the folder for the InterCheck configuration file here. If an InterCheck server is being used, the configuration file is normally in the folder from which the InterCheck server is run. If a folder is specified that does not include a configuration file, one will be created.

See the 'Configuring InterCheck clients' chapter for information on the InterCheck configuration file.

InterCheck communications folder

If an InterCheck server is being used, it will use this folder for communicating with InterCheck clients. The communications folder is normally a subfolder of the InterCheck server folder. If an InterCheck server is not being used, leave this blank.

Folder selection



SWEEP Setup will use the following folders:

SWEEP source folder: D:\WIN95\

SWEEP destination folder: I:\SWEEP\W95inst

SWEEP source folder

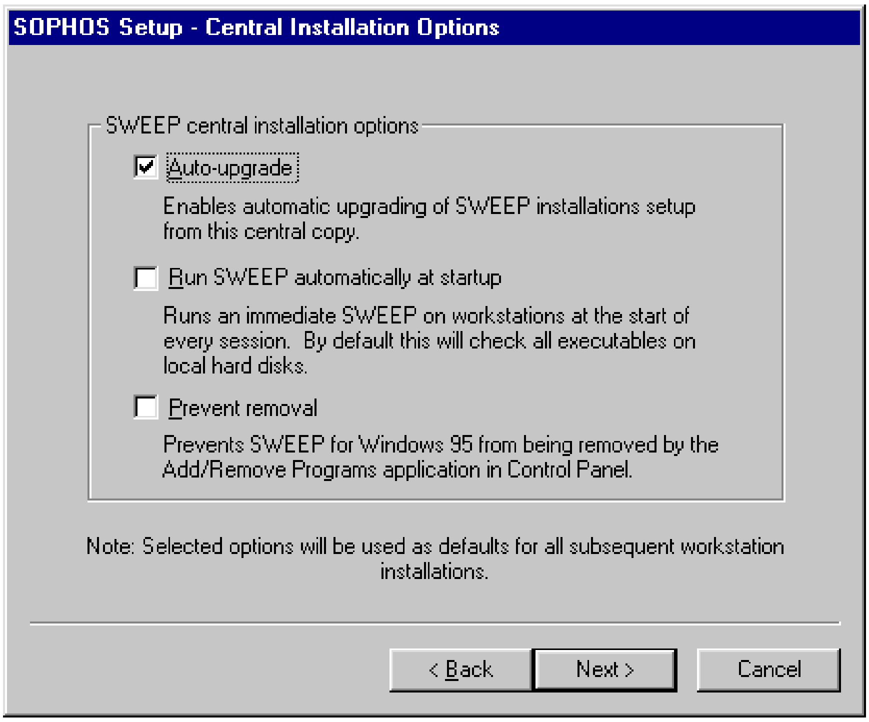
Confirm the source folder. This is the folder that contains the SWEEP installation files.

SWEEP destination folder

The destination folder, e.g. `I:\SWEEP\W95inst`, is the folder on the network drive to which the central SWEEP installation files will be copied.

Both drive-mapped and UNC paths are valid.

Central installation options



SOPHOS Setup - Central Installation Options

SWEEP central installation options

☑ Auto-upgrade

Enables automatic upgrading of SWEEP installations setup 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 SWEEP for Windows 95 from being removed by the Add/Remove Programs application in Control Panel.

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

SWEEP central installation options

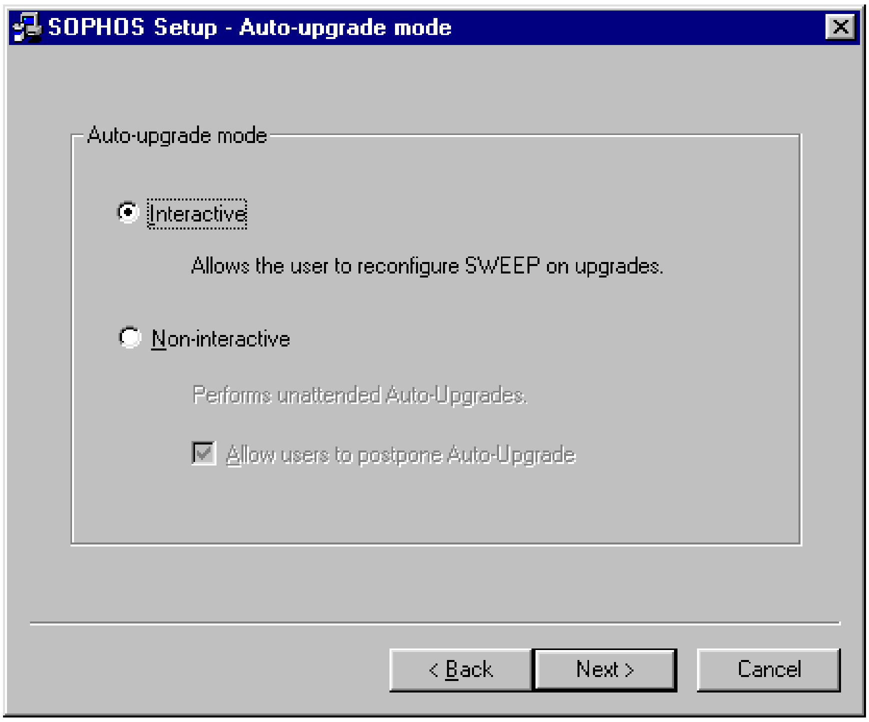
Select 'Auto-upgrade' for subsequent workstation installations to be updated automatically whenever the central installation is updated on the server. See the 'Updating a central installation of SWEEP' sections for more information.

Select 'Run SWEEP automatically at startup' for subsequent workstation installations to run SWEEP at the start of each session.

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

Auto-upgrade mode

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


SOPHOS Setup - Auto-upgrade mode

Auto-upgrade mode

● Interactive

Allows the user to reconfigure SWEEP on upgrades.

○ Non-interactive

Performs unattended Auto-Upgrades.

☑ Allow users to postpone Auto-Upgrade

Interactive

If selected, this allows the user to reconfigure SWEEP when it is upgraded.

Non-interactive

If this is selected, SWEEP will be upgraded from the file server automatically, so the user cannot reconfigure it.

Allow users to postpone upgrade

If ‘Non-interactive’ upgrading was selected, users may be allowed to postpone the upgrade. Users will be informed when a new version of SWEEP is available and asked if they wish to proceed.

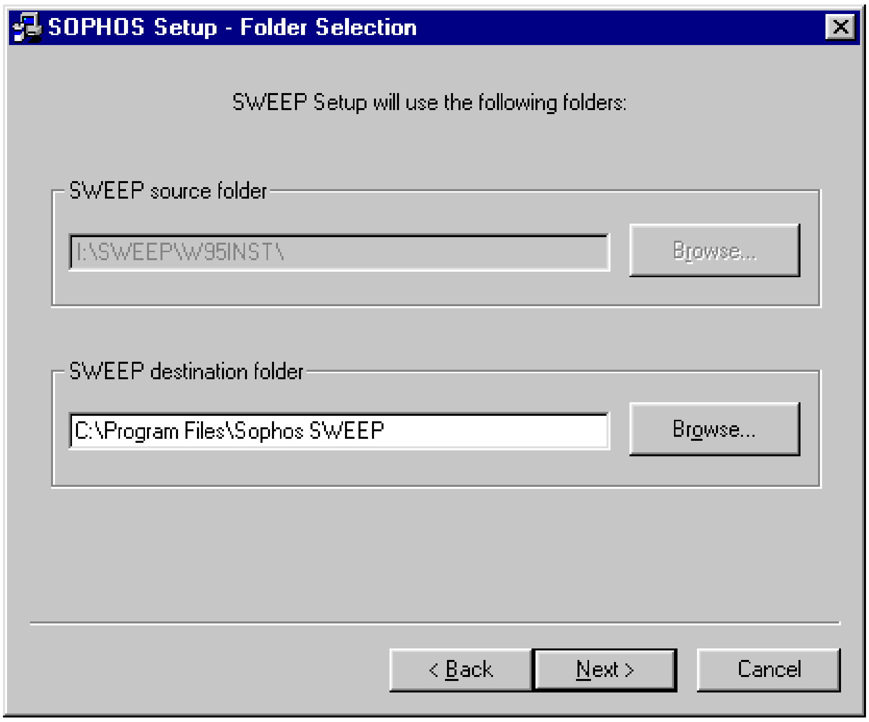
Central installation of SWEEP (stage 2)

In stage 2 of central installation, workstation installations are made from the central installation files. This can be done manually at each workstation, or automatically from a login script.

Manual installation

On the workstation, run `Setup.exe` from the folder on the file server where the SWEEP installation files are held (the 'SWEEP destination folder' specified in stage 1 of central installation).

The 'Folder Selection' screen will be presented.



SOPHOS Setup - Folder Selection

SWEEP Setup will use the following folders:

SWEEP source folder: I:\SWEEP\W95INST\

SWEEP destination folder: C:\Program Files\Sophos SWEEP

SWEEP source folder

This cannot be changed.

SWEEP destination folder

This is the folder on the workstation where SWEEP will be installed.

Automatic installation

Run `Setup.exe` from the central installation by entering

```
\\Server\SWEEP\W95inst\Setup -INL -A
```

in the workstations' login script, where *`Server`* is the name of the file server and `SWEEP` the name of the directory in which the SWEEP files were placed.

Note: This line should be placed before any call to ICLOGIN in the login script. This is to ensure that stand-alone InterCheck clients take precedence over networked InterCheck clients.

SWEEP will be installed in a folder called `Sophos SWEEP` within the `Windows 95` program folder.

Updating a central installation of SWEEP (stage 1)

Upgrading SWEEP on a network involves placing the upgraded SWEEP installation files on a file server (stage 1), from where workstation upgrades can be made (stage 2).

If auto-upgrading was selected during the original installation, the workstations will be upgraded automatically.

At the file server, start the installation program from the Sophos Anti-Virus CD, as described in the 'Starting the SWEEP installation program' section above.

The installation program will present the screens usually seen during SWEEP installation. If it detects an earlier version of SWEEP on the server, it will also present a specific update screen.

In these step-by-step instructions, all screens are described although only those specific to updating are illustrated.

Installation type

Installation Type

Select ‘Central installation/upgrade’ to place the SWEEP installation files on the file server.

InterCheck Client Capability

If selected, ‘InterCheck for Windows 95’ will enable the stand-alone InterCheck client to be installed on subsequent local installations. This will provide local on-access scanning.

Note: This option can be selected during upgrading even if InterCheck for Windows 95 has not previously been installed.

InterCheck folder selection

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

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

This is used by the InterCheck server (if one is being used) for communicating with InterCheck clients. It is normally a subfolder of the InterCheck server folder. If an InterCheck server is not being used, leave this blank.

Folder selection

SWEEP source folder

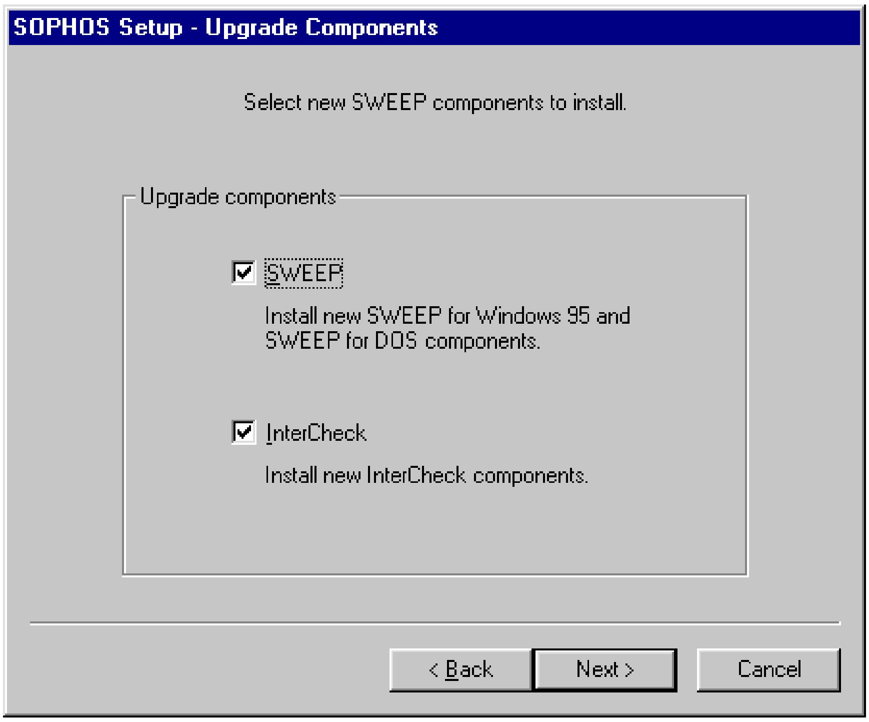
Confirm the source folder. This is the folder that contains the SWEEP installation files.

SWEEP destination folder

The destination folder, e.g. `I:\SWEEP\W95inst`, is the folder on the network drive to which the central SWEEP installation files will be copied.

Upgrade components

This screen appears only if upgrading SWEEP with InterCheck support.



SOPHOS Setup - Upgrade Components

Select new SWEEP components to install.

Upgrade components

☑ SWEEP

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

☑ InterCheck

Install new InterCheck components.

Select either or both of the following options:

SWEEP

Installs new SWEEP for Windows 95 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 for auto-upgrading selected here will **not** affect the way workstations upgrade this time. They will determine the way that workstation installations are upgraded when the **next** update from the central installation occurs.

SWEEP central installation options

Select 'Auto-upgrade' for subsequent workstation installations to be updated automatically whenever the central installation is updated on the server.

Select 'Run SWEEP automatically at startup' for subsequent workstation installations to run SWEEP at the start of each session.

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

Auto-upgrade mode

This screen is presented only if 'Auto-upgrade' was selected.

Interactive

If selected, this allows the user to reconfigure SWEEP when it is upgraded.

Non-interactive

If this is selected, SWEEP will be upgraded from the file server automatically, so the user cannot reconfigure it.

Allow users to postpone upgrade

If 'Non-interactive' upgrading was selected, users may be allowed to postpone the upgrade. Users will be informed when a new version of SWEEP is available and asked if they wish to proceed.

Updating a central installation of SWEEP (stage 2)

In stage 2 of central updating, the workstation installations are updated from the central installation.

The way that workstations are upgraded depends on the 'Central installation options' chosen when the central installation was made.

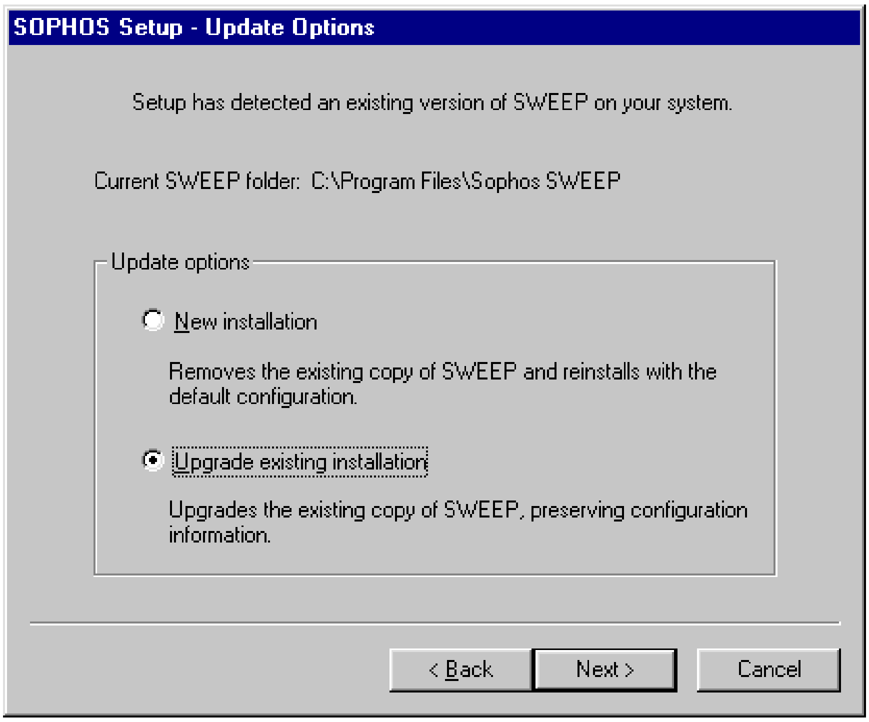
If 'Auto-upgrade' was selected in 'Central installation options', with 'Interactive' mode specified, users running SWEEP or InterCheck will be informed that the version on the server has been updated and will be offered the option of upgrading.

If 'Auto-Upgrade' was selected, with 'Non-interactive' mode selected, upgrading will proceed automatically, unless users have been given the option to postpone upgrading.

If 'Auto-upgrade' was not selected, start `Setup.exe` from the local hard disk at each workstation to be upgraded.

The following screen(s) are presented:

Update options



SOPHOS Setup - Update Options

Setup has detected an existing version of SWEEP on your system.

Current SWEEP folder: C:\Program Files\Sophos SWEEP

Update options

○ New installation

Removes the existing copy of SWEEP and reinstalls with the default configuration.

● Upgrade existing installation

Upgrades the existing copy of SWEEP, preserving configuration information.

New installation

Installs SWEEP with the default configuration, erasing the previous version and its configuration. Offers the option to change the destination folder.

Upgrade existing installation

Retains the existing configuration, updating the software components.

Folder selection

This screen is presented only if ‘New installation’ was selected.

SWEEP source folder

This cannot be changed.

SWEEP destination folder

This is the folder on the network drive to which the central SWEEP installation files will be copied.

Updating SWEEP with new virus identities

SWEEP is updated each month. However, users can add new ‘virus identities’, which SWEEP uses for virus detection, at any time.

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

The IDE files should be placed in files with an IDE extension in the current default directory. SWEEP must be stopped and restarted for any changes to take effect.

SWEEP IDE files should be removed once they are no longer needed.

Centralised distribution of IDE files

With a central installation of SWEEP with ‘Auto-upgrade’ enabled, the IDE file can be placed in the SWEEP destination folder on the file server. The local installations will receive the new IDE file the next time they are automatically upgraded.

IDE files and the InterCheck client

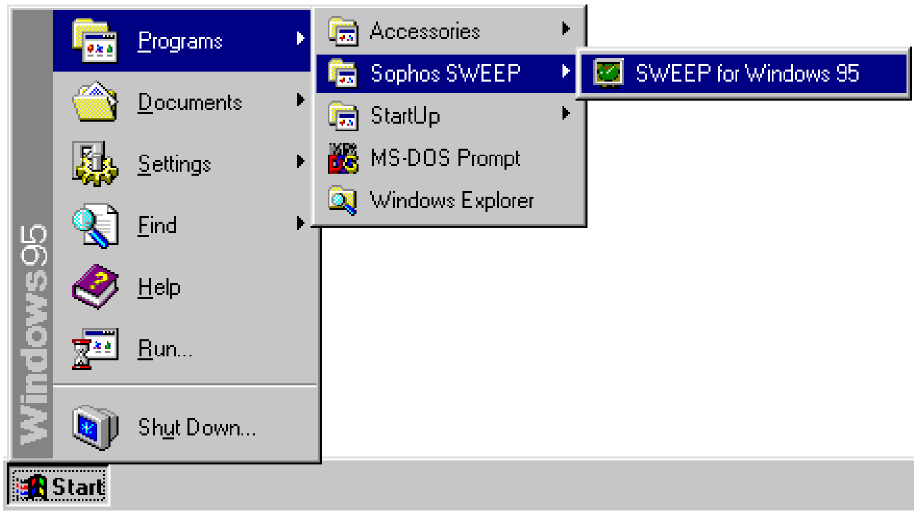
A new IDE file introduced to a local installation of the SWEEP for Windows 95 InterCheck client will not be recognised until InterCheck is restarted. When InterCheck is restarted, the virus check on start-up will behave as if SWEEP has been updated. The local checksum file will therefore normally be purged. See the ‘What InterCheck checks’ section of the ‘Configuring InterCheck clients’ chapter.

Using SWEEP

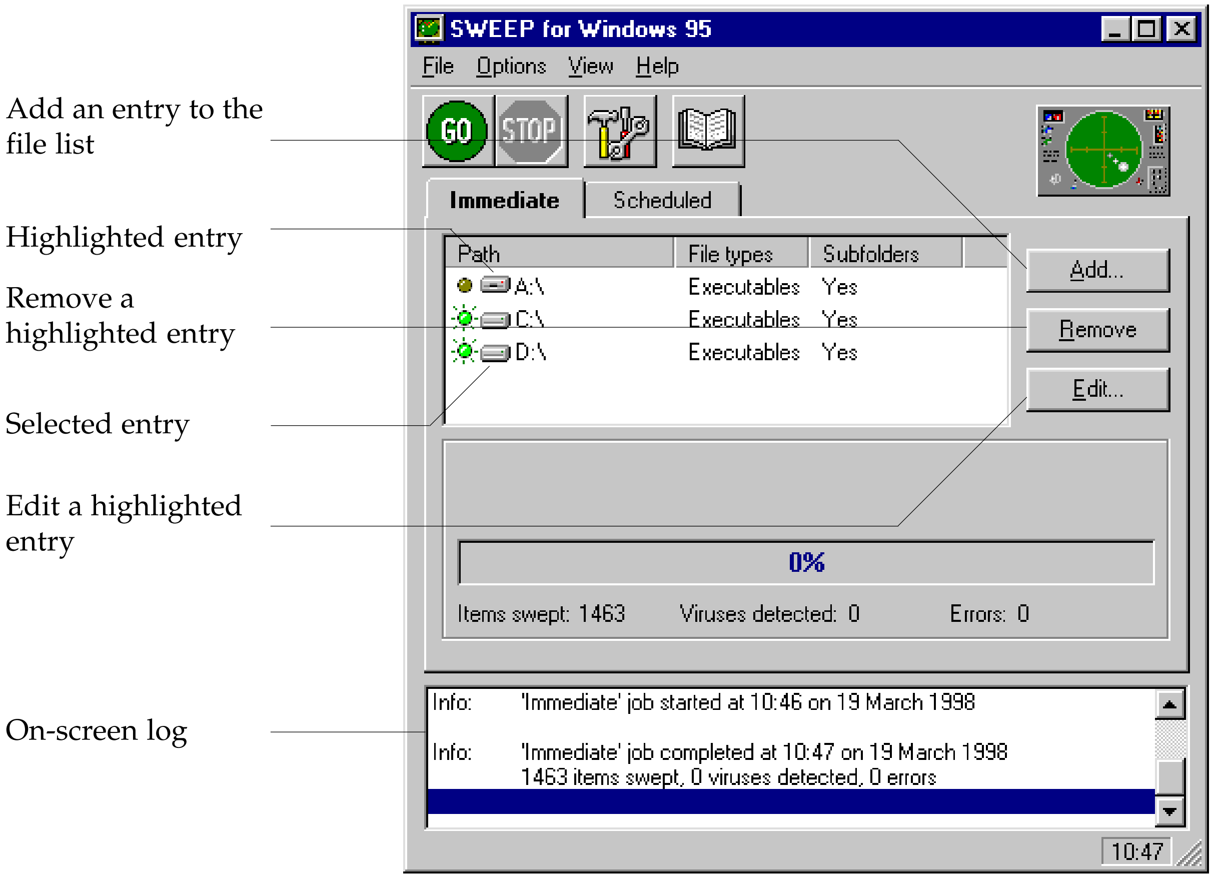
This chapter describes how to start SWEEP, start an immediate sweep, change the items to be included in immediate jobs and set up scheduled jobs.

Starting SWEEP

To start SWEEP, click *Start*, click *Programs*, click the *Sophos SWEEP* folder, and then click the *SWEEP for Windows 95* icon.



Overview of the SWEEP display



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

Items swept: 1463 Viruses detected: 0 Errors: 0

```
Info:     'Immediate' job started at 10:46 on 19 March 1998

Info:     'Immediate' job completed at 10:47 on 19 March 1998
          1463 items swept, 0 viruses detected, 0 errors
```

The main SWEEP display contains:

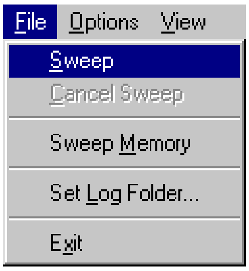
- The menu and toolbar. The icons in the toolbar provide short-cuts to commonly used menu options.
- The immediate and scheduled mode tabbed pages. The immediate mode page is displayed on start-up, and contains the file list along with the progress indicator for immediate operation.
- The on-screen log. After a job is started for the first time, the SWEEP display expands to incorporate the on-screen log. This contains information about the current session including all log messages since SWEEP was started.

The immediate mode file list shows the drives, paths and files that can be swept on demand. An ‘active’ light indicates currently selected entries. The selection status of an entry can be toggled by clicking the selection indicator to the left of its icon.

Immediate mode

Starting an immediate sweep

To sweep all the selected drives, paths and files, select *Sweep* from the *File* menu



or click the associated *GO* icon:

Hint: Any individual item in the immediate mode display can be swept by double-clicking on its icon in the file list.

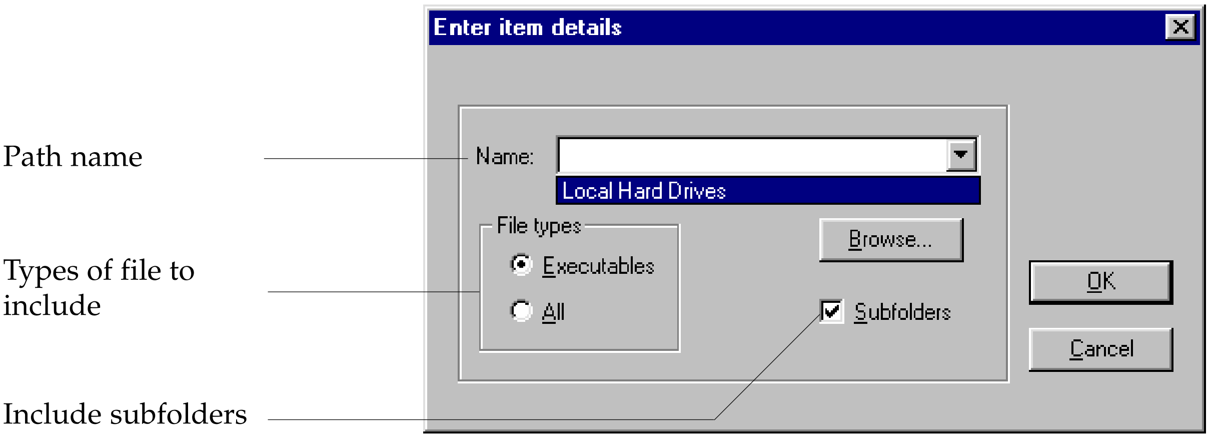
Default immediate mode file list

All local drives are displayed on the immediate mode page and all local hard drives are marked as selected.

See the ‘Configuring SWEEP’ chapter for information on immediate mode configuration settings.

Adding new items for immediate sweep

To add new items for immediate sweep, press *Add* on the immediate mode page. This will display the new item details dialog:



Name: Local Hard Drives

File types
● Executables
○ All

☑ Subfolders

Path name

Specifies the drive, folder or filename to be swept. Both mapped and UNC path names can be entered. Wildcards can also be included. *Browse* can be used to select from a list of available items. Alternatively, the drop-down menu can be used to select ‘Local hard drives’, rather than specific paths.

File types

Only those files defined as executables will be swept, unless the all file types option is selected. See the ‘Executables’ section of the ‘SWEEP options’ chapter for information on changing the files defined as executables.

Subfolders

Subfolders will be swept if this option is selected.

Removing items from immediate sweep

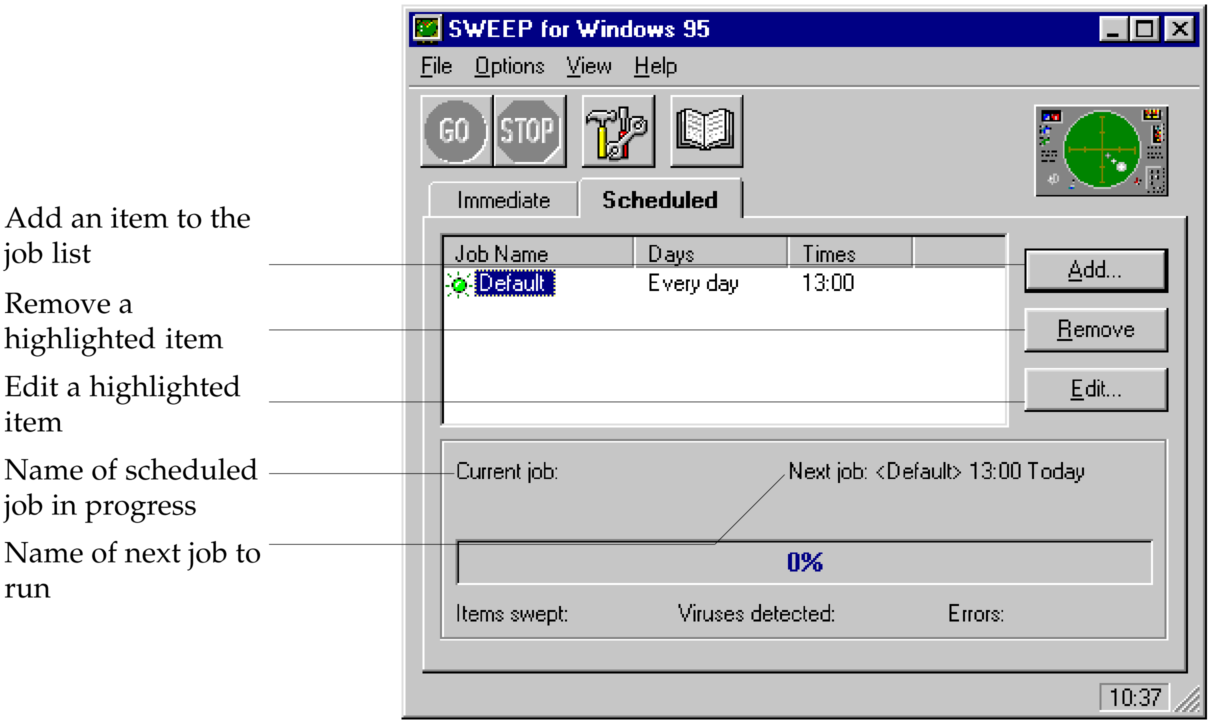
Highlight the name of the path to be removed and click *Remove*. An entry in the file list is highlighted by clicking on the path name.

Editing an item for immediate sweep

To edit an entry in the file list, highlight the name of the path to be edited and click *Edit*. This will display the item selection dialog, as described in the 'Adding new items for immediate sweep' section above.

Scheduled mode

To view or edit scheduled options, click the *Scheduled* tab.



Job Name	Days	Times
Default	Every day	13:00

Current job:

Next job: <Default> 13:00 Today

Items swept:

Viruses detected:

Errors:

Default scheduled mode job list

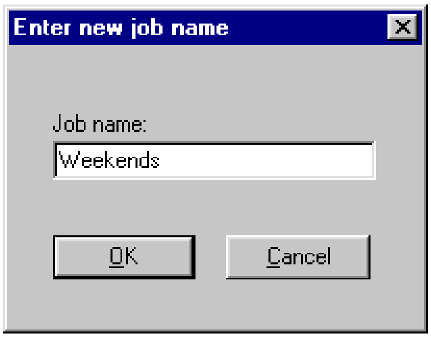
By default, a job named 'Default' is created. This will sweep the system at 13:00 every day (12:00 with

Japanese regional settings), unless it is deselected or removed from the job list.

See the ‘Configuring SWEEP’ chapter for information on scheduled mode configuration settings.

Adding a new scheduled job

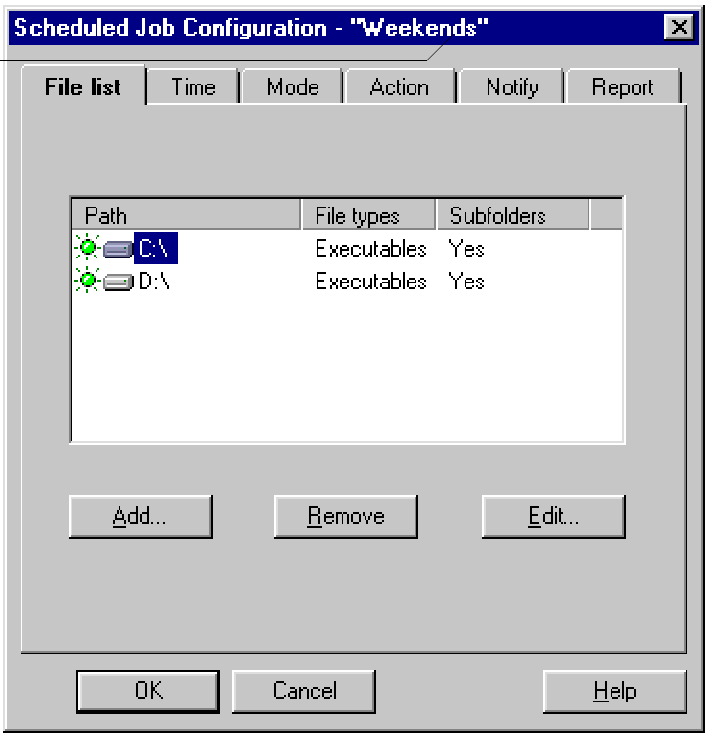
To add a new scheduled job, press *Add* on the scheduled mode page. SWEEP will prompt for a job name:



Enter new job name

Job name: Weekends

The scheduled mode configuration page will then appear.



Scheduled job name

Scheduled Job Configuration - "Weekends"

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

Click *OK* to accept the settings for the new job. See the 'Configuring SWEEP' chapter for information on these scheduled mode configuration settings.

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

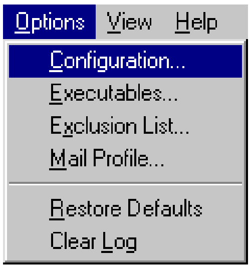
Highlight the name of the job to be edited and click *Edit*. This will display the scheduled mode configuration page as described in the 'Configuring SWEEP' chapter.

Configuring SWEEP

This chapter describes the options for configuring the immediate and scheduled modes.

About configuring SWEEP

Select *Configuration* from the *Options* menu

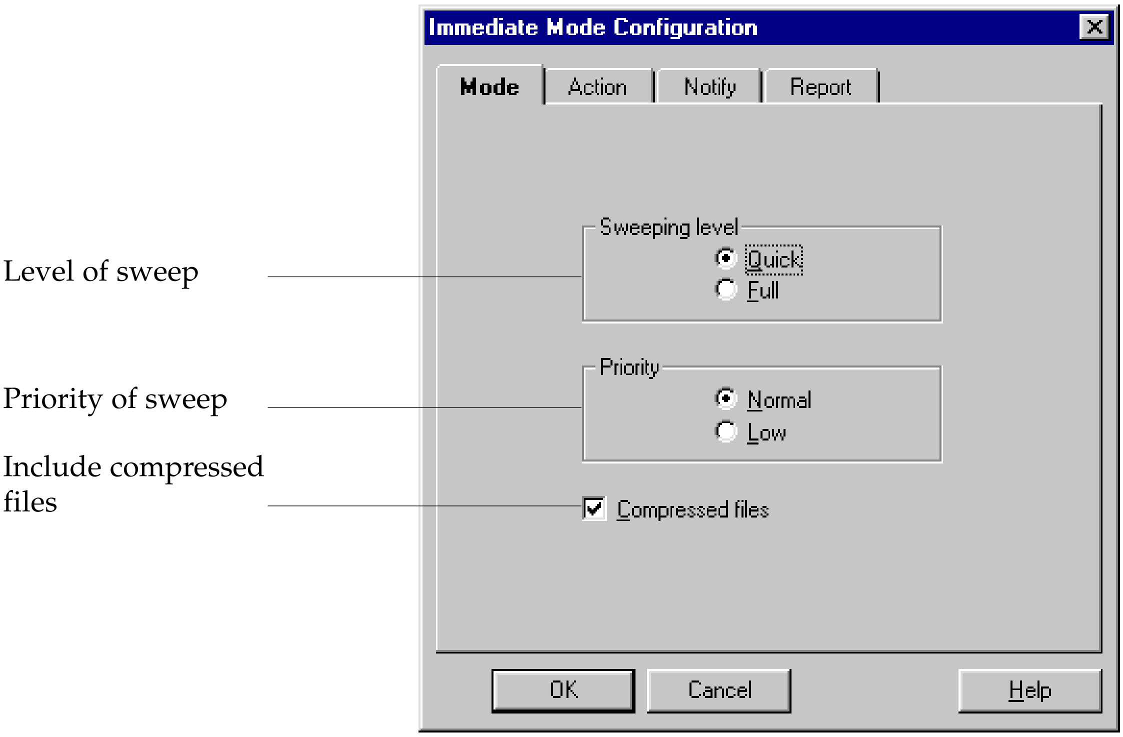


or click the associated icon

to display the configuration page for the mode whose tabbed page is currently selected.

Note: Immediate and scheduled modes are configured independently.

Sweeping mode



Immediate Mode Configuration

Sweeping level
● Quick
○ Full

Priority
● Normal
○ Low

☑ Compressed files

Level of sweep

Priority of sweep

Include compressed files

Sweeping level

The 'quick' sweeping level checks only the parts of a file likely to contain viruses, while the 'full' level examines the complete contents of each file. The 'full' level is more secure because it can discover viruses 'buried' underneath other code appended to a file, as well as minor virus mutations and corruptions. However, 'full' sweeping level is much slower, and for normal operation 'quick' sweeping is sufficient.

Priority

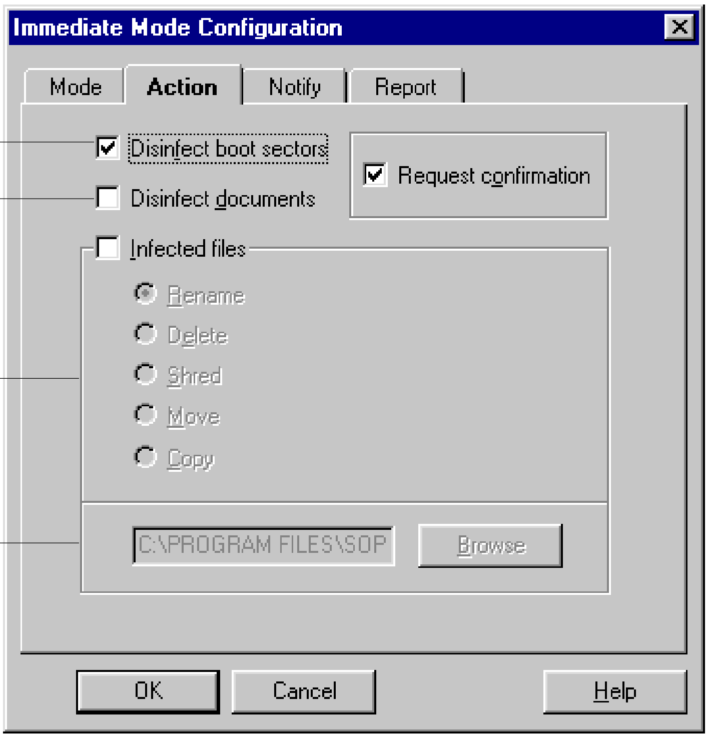
To minimise SWEEP's impact on system performance it can be set to run at 'low' priority. This will increase the time taken to sweep the system.

Compressed files

SWEEP is capable of looking for viruses inside files compressed with PKLite, LZEXE and Diet.

SWEEP does not currently look inside files which have been compressed using static compression utilities such as ARC, ZIP and ZOO. These files will need to be decompressed before sweeping. InterCheck provides automatic protection from viruses in files which have been compressed, because access to every unrecognised item (e.g. a newly decompressed file) is only granted after that item has been checked for viruses.

Action on virus detection



☑ Disinfect boot sectors

□ Disinfect documents

☑ Request confirmation

□ Infected files

● Rename
○ Delete
○ Shred
○ Move
○ Copy

C:\PROGRAM FILES\SOP

Automatically deal with infected boot sectors

Automatically deal with infected documents

Automatically deal with infected files

Folder for infected files

Disinfect boot sectors

SWEEP can disinfect most boot sector viruses from floppy disks. Confirmation will be requested before a floppy disk is disinfected. Normally this option should only be used in immediate mode, because scheduled jobs will be suspended until confirmation is granted or refused by the user.

SWEEP will not disinfect a hard disk's boot sector because some boot sector viruses are capable of performing stealth functions under Windows 95. To disinfect a hard disk boot sector, boot from a clean floppy disk and use the DOS version of SWEEP. See the 'Treating viral infection' chapter.

See the on-line virus library for specific details on individual viruses.

Disinfect documents

SWEEP can remove the viral macros from 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 (see 'Infected files' below).

Important! Some macro viruses corrupt the infected document, e.g. by switching words at random. SWEEP cannot reverse this corruption. It is therefore essential to check any disinfected file carefully before using it.

Infected files

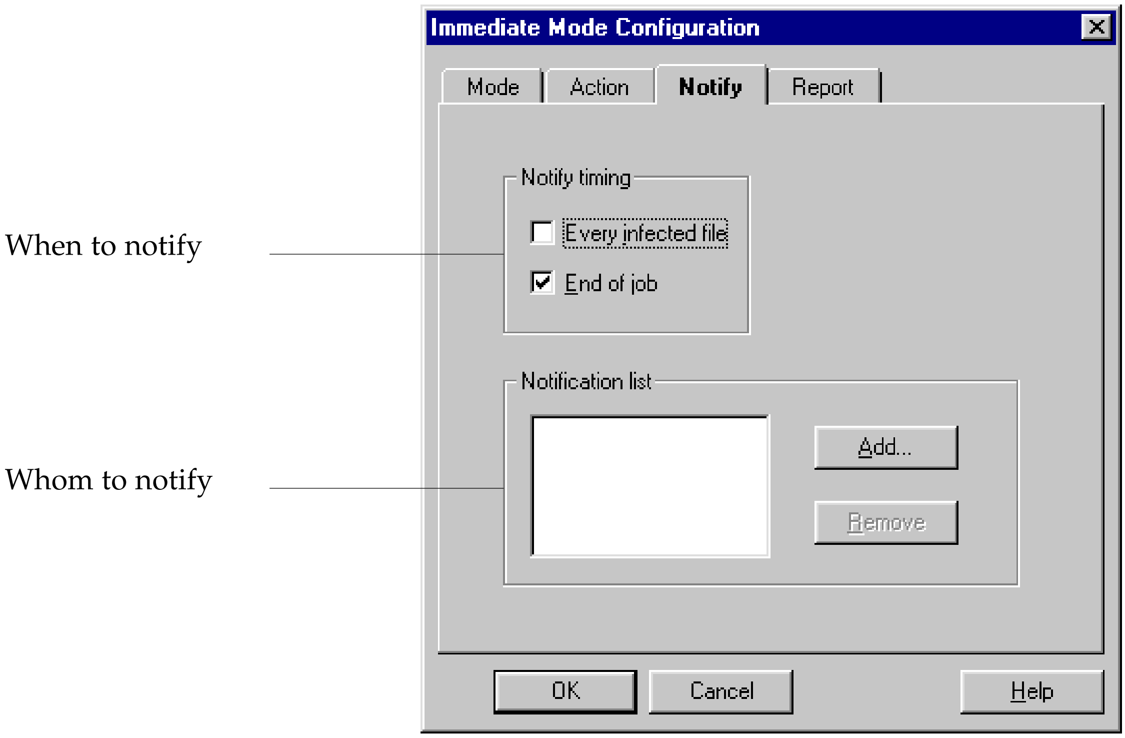
If an infected file is found, there are several actions that can be taken to make that file safe. Renaming or moving an executable file should prevent it from being run, but deleting or shredding the file will ensure that it cannot be run accidentally. Shredding is a more secure type of file deletion that overwrites the contents of the file.

Note: SWEEP does not disinfect infected program files, since disinfection cannot guarantee their integrity.

Request confirmation

If this option is selected, any action that involves changing infected items (i.e. disinfecting boot sectors, disinfecting documents, and renaming, deleting, shredding and moving infected files) will ask for confirmation before proceeding.

Notification on virus detection



Notify timing

☐ Every infected file

☑ End of job

Notification list

When SWEEP detects one or more viruses, it can send a notification message through Microsoft Exchange. If Microsoft Exchange is not installed, this option will not be available.

Note: For SWEEP to send notification messages it must log on to Microsoft Exchange using a profile with either no password or a preset password. See the ‘Mail profile’ section of the ‘SWEEP options’ chapter for further details.

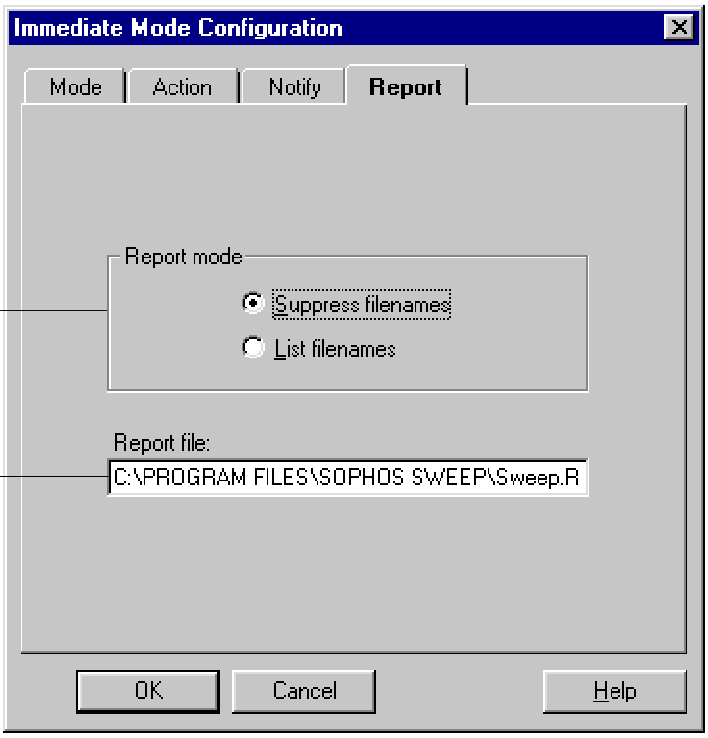
Notify timing

The notification message can be the full report file sent at the end of each job, and/or a brief message for every infected file found.

Notification list

The notification list defines the users who will be notified. Clicking *Add* will connect to Microsoft Exchange, and the list of possible users will be displayed.

Reporting results



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

The report file contains information about individual immediate or scheduled jobs. It is generated in addition to the continuous log file.

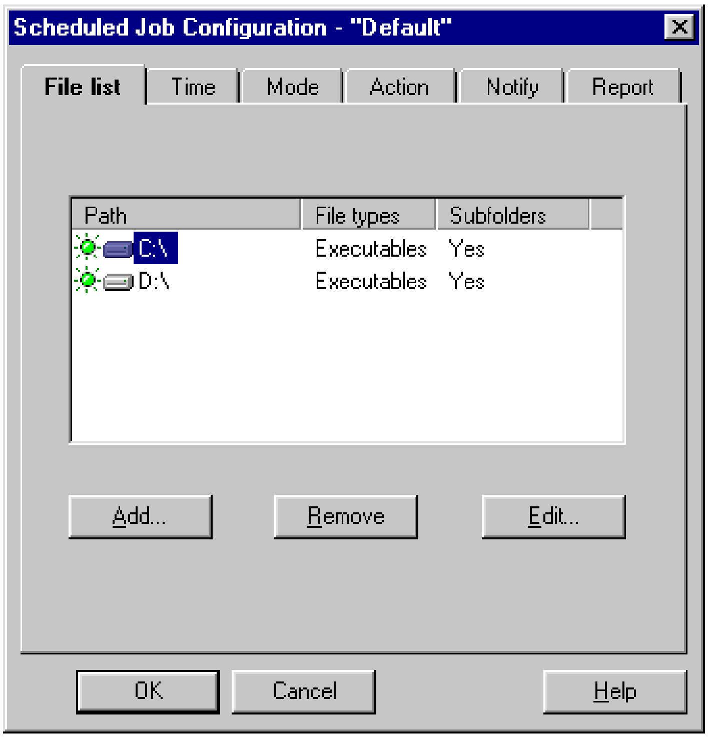
Report mode

Setting ‘List filenames’ will cause SWEEP to record in the report file the names of every item examined. Otherwise only infected items will be recorded.

Report file

The report file generated for this job will be saved in the location specified here. This file is deleted and recreated each time the job is run.

File list (scheduled mode only)



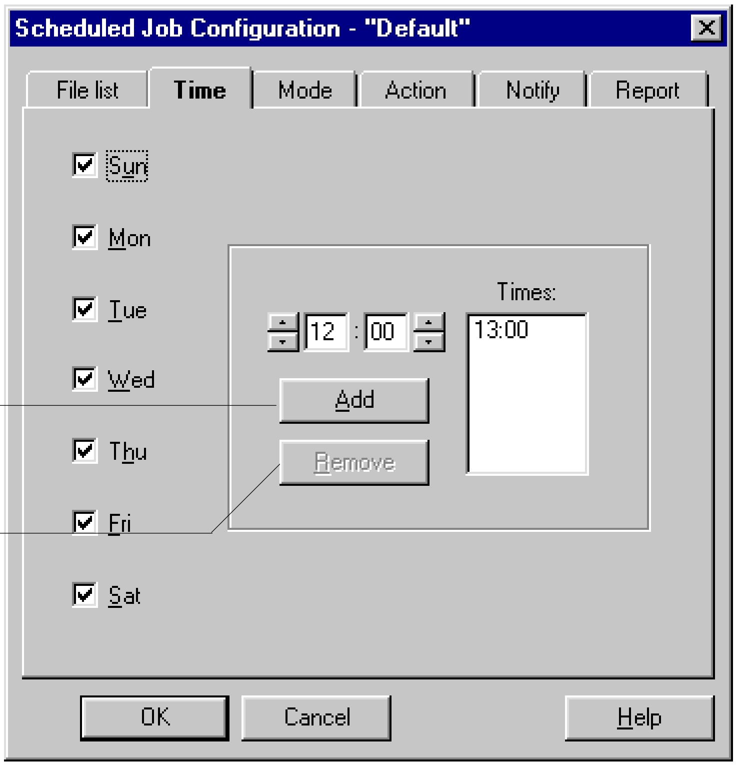
Path	File types	Subfolders
C:\	Executables	Yes
D:\	Executables	Yes

File list, functionally equivalent to the immediate mode file list

Add, *Remove* and *Edit* equivalent to those on the immediate mode page

The scheduled mode file list is similar to the immediate mode file list, but specifies the files to be swept in a scheduled job. The default scheduled mode file list is the same as that for immediate mode, except that local floppy drives are not listed.

Time (scheduled mode only)



☑ Sun
☑ Mon
☑ Tue
☑ Wed
☑ Thu
☑ Fri
☑ Sat

12 : 00

Times:
13:00

Add a new time

Remove the highlighted time

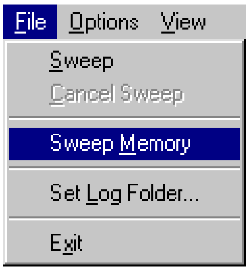
SWEEP can be configured to run at particular times on specific days of the week. For example, by specifying two separate jobs, SWEEP could be run once a day on weekdays and twice a day at weekends.

By default, a scheduled job is run at 13:00 each day (12:00 with Japanese regional settings).

SWEEP options

This chapter describes the other options available to SWEEP users and lists the SWEEP command line qualifiers.

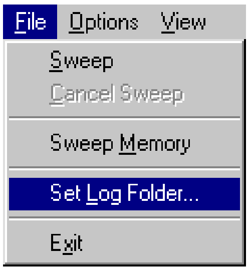
Sweep memory



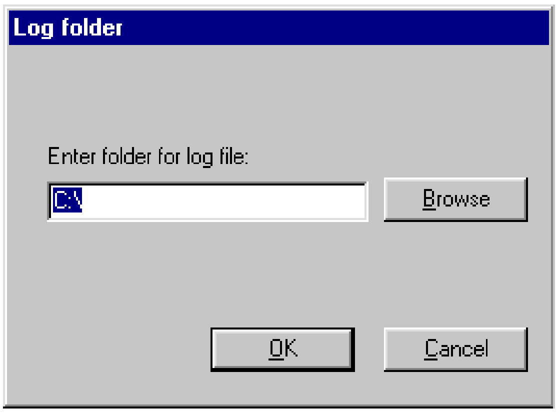
SWEEP will check memory automatically for memory-resident viruses when it is first started. Memory can also be swept at other times by clicking *Sweep Memory* from the *File* menu.

Set log folder

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

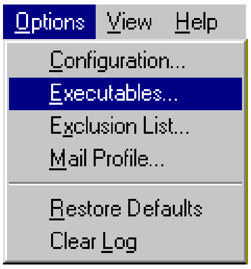


By default the log file will be saved in the root folder of the first local hard drive, but this can be changed by clicking *Set Log Folder* from the *File* menu.

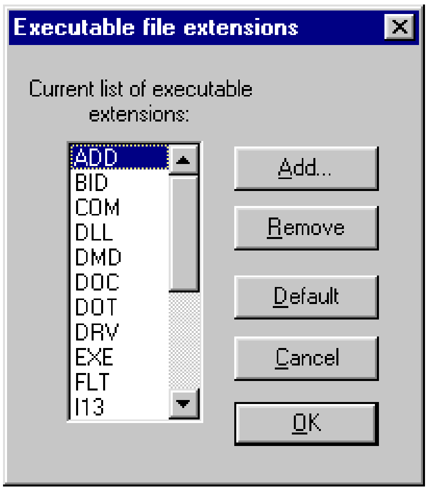


Enter folder for log file: C:\

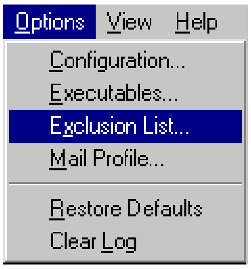
Executables



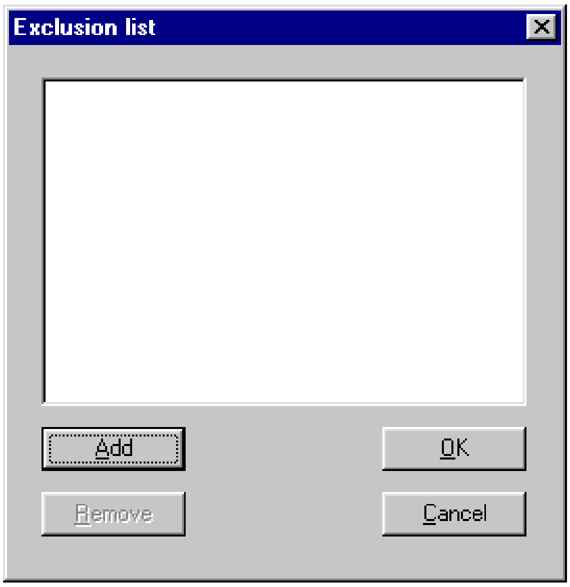
The list of file extensions to be treated as executables by SWEEP can be edited with this option. This list is only used if SWEEP is set to check 'executable' rather than 'all' file types. See also 'File types' in the 'Adding new items for immediate sweep' sub-section of the 'Immediate mode' section of the 'Using SWEEP' chapter.


Executable file extensions
Current list of executable extensions:
ADD
BID
COM
DLL
DMD
DOC
DOT
DRV
EXE
FLT
I13
Add...
Remove
Default
Cancel
OK

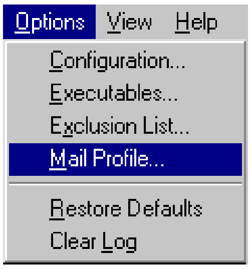
Exclusion list



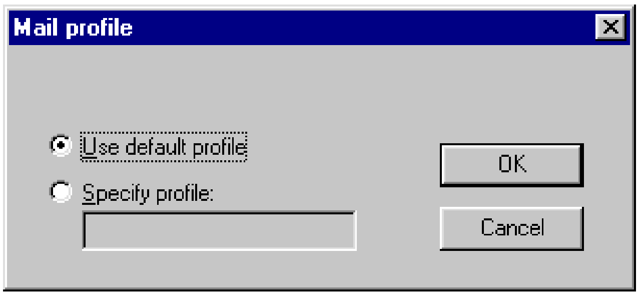
The exclusion list contains the specific files to be excluded from all SWEEP operations.



Mail profile

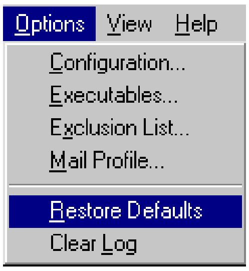


This option is only available if Microsoft Exchange is installed.



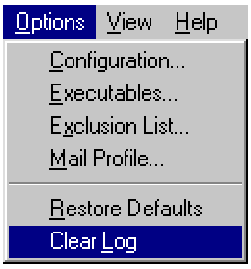
To send notification messages, SWEEP must be able to log on to Microsoft Exchange without supplying a password. If your default profile requires a password to be entered, create a new profile with a preset password and use this option to select it.

Restore defaults



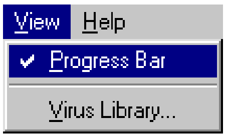
This option will set all SWEEP settings back to their defaults, after requesting confirmation. This will remove all scheduled jobs as well as resetting other options.

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

Progress bar



In order to display the progress bar, SWEEP has to count all the items to be swept before starting the virus check. On large network drives this can take a significant length of time, which can be saved by disabling this option. This option will not affect any SWEEP jobs that are already running at the time the option is selected.

SWEEP command line qualifiers

-AUTO Auto start and exit

Starting SWEEP for Windows 95 from a command line in the following way

```
SWEEP95 -AUTO
```

will force SWEEP to perform an immediate sweep, 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

The -I command line qualifier causes SWEEP to perform an immediate sweep as soon as it is loaded. User input is not disabled, and SWEEP will not unload at the end of the immediate job.

SWEEP can also be set to start as soon as Windows 95 starts, by placing a shortcut to it in the Windows 95 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 sweeping of memory during SWEEP startup.

-NW No warning messages

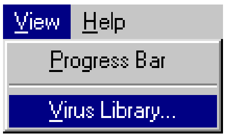
The -NW qualifier suppresses any warning messages during SWEEP startup. This option is used when SWEEP is installed to start automatically.

The virus library

This chapter describes the on-line virus library, which provides information on the viruses that SWEEP can detect.

Starting the virus library

Select *Virus Library* from the *View* menu

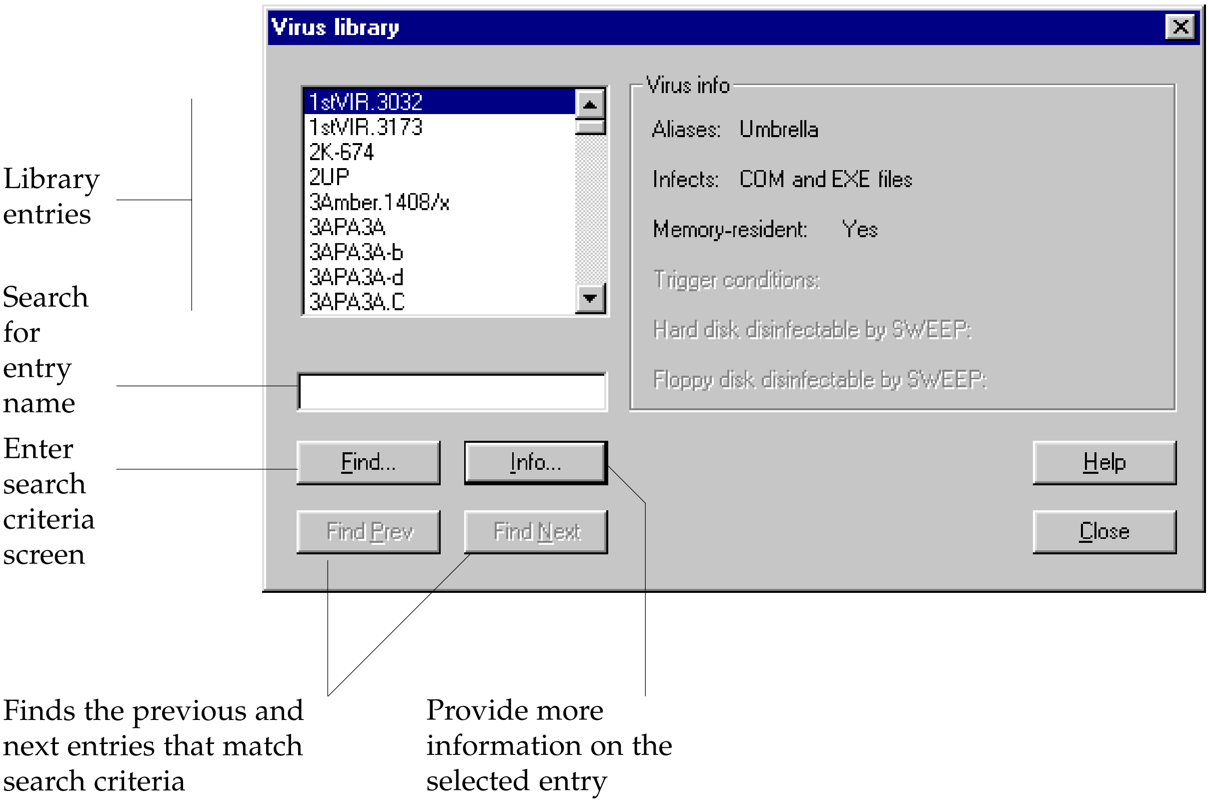


or click the associated icon

📖

to start the on-line virus library.

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:

Hard disk disinfectable by SWEEP:

Floppy disk disinfectable by SWEEP:

Find...
Info...
Help
Find Prev
Find Next
Close
Library entries
Search for entry name
Enter search criteria screen
Finds the previous and next entries that match search criteria
Provide more information on the selected entry

Information about the highlighted virus can be displayed by clicking *Info* or by double-clicking its name. This information includes advice on disinfection.

Searching for a particular virus

Include infected objects in search

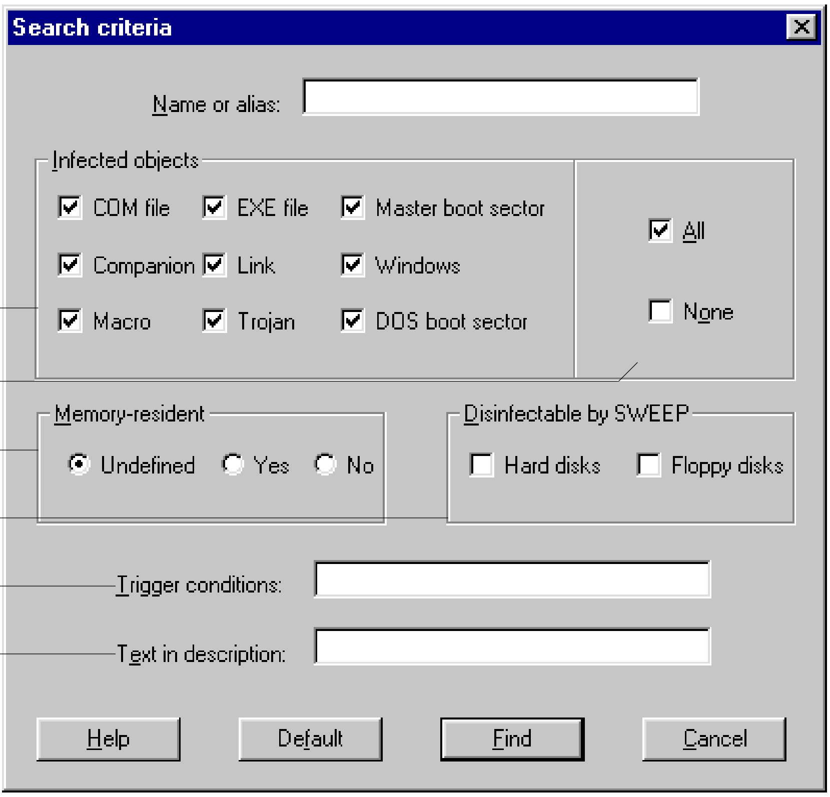
All infected objects, or none

Memory-resident

Can be disinfected by SWEEP

Trigger conditions

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:

The virus library can be searched for viruses with certain characteristics. Click the *Find* button to enter search criteria.

After a search, *Find Prev* and *Find Next* will find the previous (or the next) entry in the database which matches the search criteria.

Infected objects

Some viruses infect **COM** or **EXE** files. Others infect 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 and **macro viruses** place viral macros inside documents capable of containing macro sequences. **Trojan horses** are not viruses, but programs which provide unanticipated and undesired side-effects when executed.

Memory-resident

Memory-resident viruses stay in memory after they are executed and infect other objects when certain conditions are fulfilled.

Disinfectable by SWEEP

A tick in these boxes will include in the search viruses which can be removed from floppy and hard disks.

Trigger conditions

Many viruses require specific conditions, such as a certain time or date, in order to exhibit side-effects.

Text in description

The ‘text description’ option will search for a string which appears in the information about that virus.

Using Windows 95 InterCheck clients

This chapter gives information on the installation and operation of InterCheck clients for Windows 95.

Stand-alone and networked clients

There are two types of InterCheck client for Windows 95:

Stand-alone InterCheck clients

The Windows 95 stand-alone InterCheck client is incorporated in the SWEEP software, and performs all on-access scanning locally.

Networked InterCheck clients

Networked InterCheck clients for Windows 95 workstations require a remote InterCheck server to provide the virus checking features.

See the ‘About InterCheck’ chapter for an overview of InterCheck and the types of InterCheck client.

Installing InterCheck clients

Stand-alone InterCheck clients

The stand-alone client is installed by the SWEEP installation program (see the ‘Installing SWEEP’ chapter).

Networked InterCheck clients

Networked clients are installed from the server (see the ‘Installing InterCheck clients’ chapter of the Sophos Anti-Virus manual for the InterCheck server platform).

Starting InterCheck clients

Stand-alone InterCheck clients

The stand-alone Windows 95 InterCheck client starts automatically each time Windows 95 is started, before any network connections are made.

Networked InterCheck clients

Networked Windows 95 InterCheck clients are started from the user’s login script. For details, see the ‘Installing InterCheck clients’ chapter of the Sophos Anti-Virus user manual for the InterCheck server platform.

InterCheck clients in operation

Neither the stand-alone nor networked InterCheck clients require user input during normal operation.

InterCheck intercepts all access to program files. This includes accessing a program to extract its icon, as Explorer does the first time a program’s icon is displayed. Thus, there may be a small delay browsing the network using Explorer while InterCheck is active.

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

The Windows 95 InterCheck clients disable access to floppy disks infected with a boot sector virus.

Stand-alone InterCheck clients

The stand-alone Windows 95 InterCheck client does not display ‘requesting authorisation’ messages, thus speeding up the checking process.

Networked InterCheck clients

Networked Windows 95 InterCheck clients display a ‘requesting authorisation’ message when communicating with an InterCheck server. There may sometimes be a delay before the InterCheck client can display this message because Windows 95 does not allow the display to be updated while certain system functions are being performed.

Configuring InterCheck clients

Both types of client are configured with the InterCheck configuration file, as described in the ‘Configuring InterCheck clients’ chapter.

Configuring InterCheck clients

This chapter describes the configuration of InterCheck clients running under Windows 95, Windows for Workgroups, Windows 3.x, and DOS.

Note: For information on configuring the Windows NT InterCheck client, see the ‘Configuring SWEEP’ chapter of the Sophos Anti-Virus user manual for Windows NT.

Is it necessary to configure the InterCheck client?

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

- Specify the types of files to be checked.
- Achieve a balance between initial checking of files and subsequent requests for checking.
- Configure InterCheck differently for a specific workstation or workstations on the network.

How is the InterCheck client configured?

Configuring the InterCheck client involves editing the configuration file. This is a text file called INTERCHK.CFG stored in the directory from which InterCheck is started. The directory can either be on the server for networked InterCheck clients (central configuration file), or on the workstation for stand-alone InterCheck clients (local configuration file).

Important! If the central configuration file is modified, InterCheck clients may be updated. This may mean that local configuration files are over-written by the central configuration file (see the 'Updating local InterCheck configuration files' section below).

Configuration option section headers

The configuration options can be placed under the following 'global' or 'workstation' section headers, depending on which group of workstations or individual workstation(s) these options will apply to.

[InterCheckGlobal]
All workstations.

[InterCheckW95Global]
All Windows 95 workstations.

[InterCheckDOSGlobal]
All DOS/Windows workstations.

[InterCheckWorkStation]
All specified workstations.

[InterCheckW95WorkStation]
Specified Windows 95 workstations.

[InterCheckDOSWorkStation]
Specified DOS/Windows workstations.

[InstallOptions]
Options for the Windows for Workgroups stand-alone InterCheck client installation program. See the 'Configuring the WFWG InterCheck client installation program' section below.

Workstation and global options

The options in the workstation sections override the global options. This means that individual InterCheck workstations can be configured as required (see the

‘Configuring individual InterCheck workstations’ section below).

Where conflicting options are encountered, the sections are assigned the following order of precedence (with the highest priority listed first):

1. [InterCheckW95WorkStation] or [InterCheckDOSWorkStation].
2. [InterCheckWorkStation].
3. [InterCheckW95Global] or [InterCheckDOSGlobal].
4. [InterCheckGlobal].

Configuring individual InterCheck workstations

If different settings are made for individual workstations, these must be specified by including one or more address options in the [InterCheckWorkStation], [InterCheck95WorkStation], or [InterCheckDOSWorkStation] section.

For example, the following file defines a new virus alert message for all PCs and disables InterCheck on the PC at network address Oldfield.

```
[InterCheckGlobal]
PopUpErrorText=Ring Tim on Ext 2534

[InterCheckWorkStation]
Address=Oldfield
DisableTSR=YES
```

For details of network addresses, see the ‘Using network addresses’ section below.

Note: Comments can be added to the configuration file after a semi-colon.

Using network addresses

Each client workstation should have a unique network address, which InterCheck uses to:

- Identify the target of any workstation specific configuration options in INTERCHK.CFG.
- Identify the workstation in reports such as virus alerts.
- Construct a unique name for the checksum file on diskless workstations.

On NetBIOS compatible networks, such as Microsoft networks, Digital's Pathworks, and Novell NetWare networks, InterCheck is usually able to determine the workstation address automatically.

On a NetBIOS network, the machine name is used to represent the workstation address. This can be determined in a number of ways. For example, to find the computer name on a Windows 95 machine, double-click on the *Networks* icon on the Control Panel and click the Identification tab.

On a NetWare network, the address is automatically set to the physical address of the workstation (i.e. the Ethernet address). This can be determined by using the NETADR program supplied with InterCheck, which will display the network address for the workstation.

Where a NetBIOS and a NetWare type network are both active, InterCheck will use the NetBIOS machine name as the workstation address by default because it is generally more meaningful to the user than a NetWare address. The -NETWORK command line qualifier can be used to override this.

On other networks, the user must specify the address manually, using the -ADDRESS command line qualifier.

For further information, see the Address configuration option, along with the -ADDRESS and -NETWORK command line qualifiers.

What InterCheck checks

There are two main ways in which InterCheck uses SWEEP to look for viruses.

- **At start-up**, InterCheck passes control to SWEEP and the check is performed on the workstation. See the 'Virus checking at InterCheck start-up' section below.
- **At run-time**, items that have to be checked are passed to the server for networked InterCheck clients, and are checked locally for stand-alone InterCheck clients. See the 'Virus checking at InterCheck run-time' section below.

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

Virus checking at InterCheck start-up

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

- **Initial InterCheck start-up**
  (i.e. after InterCheck is first installed). This is to check the system is initially virus-free and to create the initial authorised items list. The checking level can be set with the InstallCheckLevel option (see the 'Initial InterCheck start-up' subsection below).
- **Normal InterCheck start-up**
  This is to detect any memory-resident stealth viruses which, if active when InterCheck loads, may be able to subvert the operation of InterCheck. The checking level can be set with the LoadCheckLevel option (see the 'Normal InterCheck start-up' subsection below).

- **InterCheck start-up after a SWEEP update**
  This is to find any new viruses not found by previous versions of SWEEP. The checking level can be set with the UpdateCheckLevel and/or PurgeChecksumsOnUpdate options (see the 'InterCheck start-up after a SWEEP update' subsection below).

Checking levels

The checking level can be set to NONE, SYSTEM, QUICK, FULL or USER:

NONE No sweep is performed.

SYSTEM Memory, boot sectors, COMMAND.COM, and hidden system files are swept. If a SystemDirectory option has been defined, SWEEP will also check all programs in the specified directory. If the MemoryCheck option has been set to NO then the memory will not be checked.

QUICK Memory, boot sectors, and the executables (including COMMAND.COM and hidden system files) on all fixed disks are swept in quick mode. If the MemoryCheck option has been set to NO then the memory will not be checked.

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 'Configuring SWEEP' chapter of the Sophos Anti-Virus user manual for DOS.

Initial InterCheck start-up

The InstallCheckLevel option defines what is swept and authorised the first time InterCheck is activated on a PC. In the default setting (QUICK) this includes all fixed disk boot sectors and memory. However, the files which are checked depend on whether the PC is stand-alone or networked.

On a **stand-alone PC** when InterCheck cannot detect a network, all files on all fixed disks are swept.

On a **networked PC** only executables are swept, but the scan is extended to include all the executables in the directories defined by the Path environment variable if the ScanNetPath option is set to YES.

The default executables are files with extensions COM, DLL, DOT, DRV, EXE, OV?, SYS and XL?. This can be changed with the ProgramExtensions option.

The number of files scanned can be modified to increase security or reduce the time taken for the initial installation. Sweeping fewer files reduces installation time, but increases the number of subsequent requests for authorisation.

Normal InterCheck start-up

The LoadCheckLevel option defines what is checked on a normal day-to-day start-up. 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

The PurgeChecksumsOnUpdate and/or UpdateCheckLevel options determine what will be swept after an update.

The PurgeChecksumsOnUpdate option can be used to ensure that the checksum file is completely rebuilt each time SWEEP and/or InterCheck are updated.

The default setting is ON if central checksumming is enabled, but OFF if it is not, in order to reduce start-up time for users. For details of checksumming see the 'Checksumming options' section below.

If **PurgeChecksumsOnUpdate is ON**, the items defined by the InstallCheckLevel option will be swept. In other words, InterCheck will carry out the same checks, at start-up and run-time, as it did at initial start-up (see the 'Initial InterCheck start-up' section).

If **PurgeChecksumsOnUpdate is OFF**, the UpdateCheckLevel option will define what is swept when SWEEP is updated. By default, all executables on all fixed disks are scanned as well as memory and the boot sectors.

Virus checking at InterCheck run-time

The CheckOn option can be set to any combination of EXEC (check all programs executed irrespective of their extension), ACCESS (check the files defined as executables if they are accessed), and FLOPPY (check all floppy disk boot sectors). The default setting includes all three areas.

The ProgramExtensions option specifies the list of file extensions to be treated by InterCheck as executable files. If the CheckOn configuration option has been set to ACCESS, any file whose extension matches an entry in the list will be considered by InterCheck to be a program and will be checked whenever it is opened, closed (if changes have been made) or renamed.

The Exclude, NoDefaultExcludes, FileTypeDetection, CheckNetwork and UseNetList configuration options can also have a bearing on the normal operation of InterCheck.

Checksumming options

When SWEEP is used to check an item, and access to that item is granted, that item does not need to be checked again unless it is changed. InterCheck notes which items have been verified in its checksum file. This is normally stored in the root directory of the client workstation, although the CheckFile configuration option can be used to change its location.

Centralised checksumming

SWEEP for NetWare, SWEEP for Windows NT and VSWEEP for OpenVMS also support centralised checksumming. This means that a checksum file is stored on the server in addition to the checksum file on each client. The central checksum file can be accessed by all networked InterCheck clients, and is checked if an unverified item is not listed in the local checksum file. Therefore, when one client accesses an item, and access to that item is granted, any other client that tries accessing that item will not need to send it to the server for checking.

By default, centralised checksumming is enabled for InterCheck clients if has been enabled on the InterCheck server. The UseNetList option can be used to disable this feature.

Critical program support

InterCheck holds the checksums for a number of ‘critical programs’ in memory, so that they can always be accessed. This is especially important on diskless workstations where the LOGIN program must be executable after one user has logged out and the next user wishes to log in. This removes the need to exclude such files from checking. By default, the following programs are considered critical:

- COMMAND.COM.
- LOGIN.EXE (if the workstation is networked).
- The boot sector of the disk in drive A: (if the workstation has been booted from the floppy disk).

The CriticalProgram and NoStandardCriticalPrograms configuration options allow the use of the critical program checksums to be customised.

Configuring stand-alone InterCheck clients

If a stand-alone InterCheck client has been installed, then InterCheck will continue to protect the workstation from viruses even when it is not connected to the network. In the Windows and Windows 95 environments, a Windows Virtual Device Driver (VxD) is used to authorise files.

The SWEEP VxD shares many of the configuration options used by networked InterCheck clients, and also uses the following options: SweepVxDLoad, SweepVxDMode, SweepVxDScanCompressed, SweepVxDLogFile, SweepVxDLogLevel. See the 'Configuration options' section below for more information.

Updating local InterCheck configuration files

If the InterCheck client has been installed locally on a client workstation, the local configuration file can be updated automatically when the workstation logs in to the server. The UpdateLocalCFG option, which allows this, is set to NO by default.

Important! The stand-alone Windows 95 InterCheck client, and the Windows for Workgroups client installed with the automatic installation program, always update local configuration files.

Configuring the WFWG InterCheck client installation program

The Windows for Workgroups stand-alone InterCheck client installation program can be configured by placing the following options under the [InstallOptions] header in the configuration file: AutoInstallExclude[1...n], CommsDirectory, DestinationDirectory, InteractiveInstall, and SourceDirectory. See the 'Configuration options' section below for more information.

Configuration options

Address=<text>

The address option must be included at some point in an [InterCheckWorkStation], [InterCheckW95WorkStation] or [InterCheckDOSWorkStation] section. Multiple address options can be included in one section. The address option defines the workstation(s) to which the options in the section will be applied.

See also the 'Using network addresses' section and the -ADDRESS command line qualifier.

AllowDisable=YES|NO

InterCheck can be disabled if this is set to YES. For security reasons, disabling is not allowed by default.

See also the -DISABLE command line qualifier.

This option is not currently supported by the Windows 95 client.

AllowUnload=YES|NO

InterCheck can be unloaded from memory if this option is set to YES. For security reasons, unloading is not allowed by default.

See also the -UNLOAD command line qualifier.

AltCommsDir=<directory>

This option can be used to define up to 4 alternative COMMS directories. For example:

```
AltCommsDir=\\BackupServer1\INTERCHK\COMMS
AltCommsDir=\\BackupServer2\INTERCHK\COMMS
```

This will be used if the primary server is unavailable. When using multiple alternative directories, the order in which they are defined in the configuration file determines the search order when attempting to detect an active server.

This option is not currently supported by the Windows 95 client.

AutoInstallExclude[1...n]=<computer1>,<computer2>...

This option excludes named computers from ICSETUPW installations started by ICLOGIN. For example

```
  AutoInstallExclude=Onion, Cheese, Marco
  AutoInstallExclude1=Mini Marco, Derek
```

will exclude the computers with network names Onion, Cheese, Marco, Mini Marco and Derek. Computer names are not case sensitive.

This option is only relevant to the automatic InterCheck client installation program.

AutoUpdate=ON | OFF

This option can be used to disable the automatic updating of local copies of InterCheck from the network. It is ON by default.

This option is not relevant to the Windows 95 client.

CheckFile=<filename>

Checksums are stored in the file C:\INTERCHK.CHK on the client workstation by default. A different filename can be specified by using this option, e.g.

```
CheckFile=D:\MYCHECKS.CHK
```

CheckNetwork=YES|NO

The CheckNetwork configuration option provides the ability to disable the checking of any program files on networked drives. This reduces file validation delay if the file is on the network and can be assumed to be clean. In order to disable checking of files on networked drives use

```
CheckNetwork=NO
```

CheckOn=[EXEC],[ACCESS],[FLOPPY]

The CheckOn option defines which functions InterCheck will intercept. The following options are available:

EXEC	Check all programs executed.
ACCESS	Check all program files accessed, i.e. opened, closed (if changes have been made), or renamed.
FLOPPY	Check all floppy disk boot sectors.

Any combination may be specified, separated by commas. The default is equivalent to:

```
CheckOn=EXEC,ACCESS,FLOPPY
```

See also the ‘What InterCheck checks’ section.

CommsDirectory=<path>

The default location for the InterCheck communications directory is COMMS in the InterCheck server directory. Use the CommsDirectory option to specify a different InterCheck communications directory. For example

```
CommsDirectory=I:\SWEEP\COMMS
```

CriticalProgram=<files>

Defines the critical program(s) whose checksum will be held in memory. Up to 16 critical programs can be defined. See the 'Critical program support' section.

To include a boot sector, specify the drive letter, e.g. 'D:'.

All critical programs are displayed when InterCheck loads if the StartUpDisplay=VERBOSE configuration option is selected.

This option is not relevant to the Windows 95 client.

DisableTSR=YES | NO

The DisableTSR option can be used to prevent InterCheck loading. Once the option has been set to YES, any attempt to run InterCheck results in the message "InterCheck has been disabled".

The DisableTSR option can also disable the Windows 95 SWEEP VxD.

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.

There are a number of default excludes: 386SPART.PAR, CONFIG.SYS, WIN386.SWP and ~$??????.DOT. The latter is included to suppress the checking of temporary template files used by Microsoft Word for Windows. The inclusion of the default exclusions can be disabled using the configuration option NoDefaultExcludes=YES.

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.

FileTypeDetection=OFF | WINDOWS_EXE | WORD_MACRO | ALL

InterCheck can examine the contents and structure of a file to determine its type and therefore whether it has to be checked for viruses. InterCheck is currently able to determine if a file is either a Windows Program or a Microsoft Word template containing macros. This option is useful for ensuring that all Word documents are checked for viruses, even if they do not have the extension DOT.

OFF	Disables this feature.
WINDOWS_EXE	Detects Windows programs only.
WORD_MACRO	Detects Word macros only.
ALL	Enables all detection methods.

By default, ALL FileTypeDetection options are enabled.

This feature is only available with Windows and Windows 95 InterCheck clients, and is not supported in a DOS environment.

HaltOnError=YES | NO
HaltOnVirus=YES | NO

These two configuration options provide the system Administrator with the ability to halt a PC if InterCheck detects a virus or encounters an error while loading. For example:

```
HaltOnVirus=YES
HaltOnError=NO
```

Both options are disabled by default.

Neither option is currently supported by the Windows 95 client.

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.

This option also defines what is swept when InterCheck is run for the first time after a SWEEP update and purge of checksum file.

See the 'What InterCheck checks' section for more information.

InstallDirectory=<path>

The default destination for the local Windows for Workgroups InterCheck installation is C:\INTERCHK. Use the InstallDirectory option to specify a different location. For example

```
InstallDirectory=C:\INTERCHK\COMMS
```

This option is only relevant to the automatic InterCheck client installation program.

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 from each workstation 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.

InteractiveInstall=1|0

If InteractiveInstall is set to 1, ICSETUPW will always run in interactive mode. If set to 0, ICSETUPW will not run in interactive mode, even if it started with the -I command line qualifier.

This option is only relevant to the automatic InterCheck client installation program.

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 ‘What InterCheck checks’ section for more information.

LoadLow=YES|NO

The LoadLow option is used to force InterCheck to load into low memory. By default InterCheck will be loaded into the upper memory area.

This is not relevant to the Windows 95 client.

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.

MaxAddressLength=<length>
MaxPathLength=<length>

These configuration options can be used to instruct InterCheck to reserve additional memory ready for subsequent configuration changes. Under normal circumstances these options are not required. However, if InterCheck reports any of the following error messages

```
WARNING: Could not update the program directory.
WARNING: Could not update the communication directory.
WARNING: Could not update the workstation address.
```

you may need to use one or both of these options. For example:

```
MaxPathLength=255
MaxAddressLength=64
```

The MaxPathLength option defines the maximum length of the program and communication directory names that will be supported by InterCheck. The MaxAddressLength parameter defines the maximum length of the workstation address. The defaults are defined by the directories and address in use when InterCheck is first loaded. The maximum values for the MaxPathLength and MaxAddressLength parameters are 255 and 64 bytes respectively.

Neither option is relevant to the Windows 95 client.

MemoryCheck=YES|NO

The MemoryCheck option enables and disables checking for viruses in memory when InterCheck loads. Memory checking is enabled by default. The memory check is an integral part of the protection provided by InterCheck and should not normally be disabled.

MonoMonitor=YES|NO

This option overrides the automatic detection of a mono monitor.

This is not relevant to the Windows 95 client.

NoDefaultExcludes=YES|NO

If this option is set to YES, the default file exclusions will be disabled. See also the Exclude configuration option.

NoStandardCriticalPrograms

InterCheck will normally adopt the default critical programs list (see the ‘Critical programs support’ section). If this parameter is used, the default programs are not used.

This is not relevant to the Windows 95 client.

PopUpDisplay=OFF|ERROR|ALL

The PopUpDisplay option determines how much information is presented to the user in the pop-up message boxes:

OFF	No messages are displayed.
ERROR	Only alert messages are displayed (e.g. detecting a virus).
ALL	Status messages are displayed while InterCheck is working.

The default is ALL.

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,DLL,DOT,DRV,EXE,OV?,SYS,XL?
```

Note: Windows and Windows 95 clients automatically check files with a DOC extension. See the ‘FileTypeDetection’ option.

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

For example

```
ProgramExtensions=COM,DLL,DOT,DRV,EXE,OV?,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 their extension.

See also the 'What InterCheck checks' section.

PurgeChecksumsOnUpdate=YES | NO | DEFAULT

If this option is set to YES, the checksum file will be deleted whenever InterCheck and/or SWEEP are updated. InterCheck will then run SWEEP in the level defined for use during installation. This can be used to increase security, but is not enabled by default. The DEFAULT option purges checksums on a SWEEP/InterCheck update only if the InterCheck client is using the SWEEP VxD and/or a central checksum list.

Note: Enabling this option will introduce an overhead on the server whenever InterCheck and/or SWEEP are updated.

ReportEvents=[LOAD],[UPDATE],[INSTALL],[ALL],[NONE]

InterCheck can record usage information in the server's SWEEP log file. The type of information that is recorded is determined with the ReportEvents configuration option.

LOAD	Records an entry every time InterCheck loads.
UPDATE	Records an entry every time InterCheck or SWEEP is updated.
INSTALL	Records an entry when InterCheck is first installed on a workstation.
ALL	Records all of the above.
NONE	Records nothing.

If InterCheck reports an event it will also record the current user, the network address of the workstation, and the time and date the event occurs.

Any combination of events can be specified, separated by commas. For example

```
ReportEvents=LOAD,UPDATE
```

will record an entry every time InterCheck loads and every time InterCheck or SWEEP is updated.

By default no events are reported to the server.

ScanNetPath=YES | NO

This option controls the scanning of program files when InterCheck is first installed and run on a client workstation.

If set to YES, InterCheck will search any remote directories specified in the PATH environment variable, and any program files it discovers will be swept for viruses.

The default setting for ScanNetPath depends on whether InterCheck can detect a central checksum file on the server. The ScanNetPath option is disabled when centralised checksumming is active.

ServerTimeout=<time>

The ServerTimeout option defines the time, in seconds, which InterCheck will wait for a reply from the server before reporting that the server is unavailable. The default is 60 seconds.

SourceDirectory=<path>

The default location of Windows for Workgroups InterCheck source files is the directory from which ICSETUPW is run. If for some reason the source files are stored elsewhere, use the SourceDirectory option. For example

```
SourceDirectory=I:\INTERCHK\WFWG
```

This option is only relevant to the automatic InterCheck client installation program.

StartUpDisplay=NONE|NORMAL|VERBOSE

The StartUpDisplay option determines how much information is displayed as InterCheck loads. The default is NORMAL which only displays the program name and version information. Selecting NONE suppresses all output unless an error is detected, whereas the VERBOSE option displays additional information about which InterCheck options have been selected.

Swap=YES|NO

When the InterCheck loader program runs SWEEP, it is swapped out of memory by default in order to minimise the memory requirement. If this causes problems, the swapping can be disabled:

```
Swap=NO
```

This is not relevant to the Windows 95 client.

SwapFlags=ANY,EMS,XMS,EXT,DISK

When the InterCheck loader program runs SWEEP, it is swapped out. By using this option you can specify where the swapping should take place. EMS means EMS memory, XMS means XMS memory, EXT means extended memory, DISK means disk and ANY means any of these. Swapping to disk is always used as the last option. ANY is used by default. For example:

```
SwapFlags=EXT,DISK
```

This is not relevant to the Windows 95 client.

SweepVxDLoad=YES|NO

The SweepVxDLoad option controls whether or not to use the SWEEP VxD. The default is NO. However, the VxD is required for stand-alone InterCheck clients, so the installation program automatically adds the option SweepVxDLoad=YES when installing locally.

SweepVxDMode=FULL|QUICK

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

SweepVxDScanCompressed=YES|NO

The SweepVxDScanCompressed option can be used to suppress sweeping inside compressed files.

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 will be logged.

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

SystemDirectory=<directory>

The SystemDirectory option specifies which directory contains the system files. InterCheck will sweep any programs in this directory when any of the three check levels (InstallCheckLevel, LoadCheckLevel or UpdateCheckLevel) have been set to SYSTEM. By default no directory is specified.

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 ‘What InterCheck checks’ section for more information.

Note: If PurgeChecksumsOnUpdate is set to YES, or if the default is to purge checksums, the InstallCheckLevel will be used instead of the UpdateCheckLevel option.

UpdateLocalCFG=YES | NO

If the InterCheck client has been installed locally on the client workstation, the local InterCheck configuration file can be updated automatically whenever the workstation logs into the server and runs InterCheck from there. If the configuration option

```
UpdateLocalCFG=YES
```

is present in the server based configuration file, the local configuration file will be replaced by the one held on the server as part of InterCheck’s auto-update procedure. By default, the UpdateLocalCFG option is NO.

Windows 95 InterCheck clients and clients installed with the automated installation program always update local configuration files.

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.

UseNetList=YES | NO

The InterCheck client utilises checksum lists generated by the InterCheck server (if supported by the server). Any program that has been swept by the server can be automatically authorised for use on all clients. To disable the use of this feature use

```
UseNetList=NO
```

UseNetSyntax=YES | NO

The UseNetSyntax option removes from InterCheck any dependence on the currently selected DOS drive mappings. The initial drive mapping, from which InterCheck was started, is no longer required to maintain communication with the server. The workstation must, however, remained logged in or attached to the server providing the InterCheck service. To enable support for this feature, use

```
UseNetSyntax=YES
```

The option should not be used with Windows 3.1 if the name of the server running the InterCheck service is longer than 11 characters. When a long server name is encountered, Windows is unable to load the support programs required by InterCheck. This problem does not occur with Windows for Workgroups.

WarnCriticalProgramMissing

If InterCheck cannot find a critical program (as defined with the CriticalProgram option), it will not display any error messages. If this parameter is used, an error message will be displayed.

This is not relevant to the Windows 95 client.

INTERCHK and ICWIN95 command line qualifiers

This section describes the command line qualifiers that can be used with INTERCHK.EXE to start the DOS/Windows 3.x InterCheck client, and with ICWIN95.EXE to start the networked Windows 95 InterCheck client.

-ADDRESS=<address>

The command line qualifier

```
-ADDRESS=<address>
```

allows the workstation address to be specified on networks where InterCheck cannot determine the workstation address automatically.

Note: If the network address contains a space, the -ADDRESS command line qualifier should be enclosed in double quotation marks, for example:

```
ICWIN95 "-ADDRESS=PC 10"
```

See also the ‘Using network addresses’ section and the -NETWORK command line qualifier.

-DISABLE

This command line qualifier stops all the checking performed by InterCheck, although the TSR remains loaded in memory. Checking can be restarted using the -ENABLE command line qualifier. For security reasons, this is not available by default. In order to use it, the line ‘AllowDisable=YES’ must be included in the InterCheck configuration file.

For example:

```
INTERCHK -DISABLE
```

This is not currently supported by the Windows 95 client.

-ENABLE

This command line qualifier restarts InterCheck after it has been disabled. For example:

```
INTERCHK -ENABLE
```

This is not currently supported by the Windows 95 client.

-HELP or -?

Displays a list of available command line qualifiers.

-NETWORK=NETBIOS | NETWARE

This command line qualifier is only required when multiple network types are in use. It selects the preferred network type for InterCheck, and only affects how InterCheck obtains the workstation address. If NetWare and NetBIOS type networks are both active, InterCheck will use the NetBIOS machine name by default.

See also the ‘Using network addresses’ section and the -ADDRESS command line qualifier.

This is not currently supported by the Windows 95 client.

-SILENT

If this command line qualifier is used, screen output will be suppressed. For example:

```
INTERCHK -SILENT
```

-STATUS

This command line qualifier displays information about the status of the InterCheck TSR. It can be used to determine if InterCheck is currently active by examining the returned DOS errorlevel:

0 Success (InterCheck active)
1 Parameter error
2 Other error (InterCheck not loaded)

For example, if TEST.BAT contains:

```
INTERCHK -STATUS -SILENT
IF ERRORLEVEL 1 GOTO NOTACTIVE
ECHO InterCheck active
GOTO END
:NOTACTIVE
ECHO InterCheck not active
:END
```

running it will display 'InterCheck active' if InterCheck is loaded and active.

The normal report only indicates whether or not InterCheck is active. If combined with the -VERBOSE command line qualifier, additional information concerning the configuration of the memory-resident part of InterCheck can be obtained.

-UNLOAD

This command line qualifier removes InterCheck from memory. For security reasons, the unload option is not available by default. In order to use the unload option the line 'AllowUnload=YES' must be included in the InterCheck configuration file.

For example:

```
INTERCHK -UNLOAD
```

Note that it may not be possible to unload InterCheck if other TSR programs have been loaded since InterCheck was first started.

-VERBOSE

This command line qualifier causes additional information to be displayed when InterCheck is run.

Treating viral infection

This chapter describes SWEEP for Windows 95's automatic disinfection facility and other mechanisms for dealing with viruses.

Automatic disinfection

In most cases, SWEEP for Windows 95 can deal with infected items automatically (see the 'Action on virus detection' section of the 'Configuring SWEEP' chapter).

SWEEP for Windows 95 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 SWEEP's virus library before attempting disinfection.

Hint: When SWEEP discovers a virus, 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 DOS 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.

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=15
BUFFERS=40
```

Create an AUTOEXEC.BAT with the following line:

```
A:\SMARTDRV.EXE
```

Make the disk write-protected (to ensure that 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.

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, SWEEP for Windows 95 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 SWEEP for DOS to disinfect the virus with the command

```
SWEEP -DI
```

This will also disinfect any infected documents that SWEEP 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

It is generally inadvisable to attempt to disinfect infected executables. This is because it is not possible to ensure that the executable has been properly restored after disinfection; it may be unstable which may put 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, *Winword/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 *Winword/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 it is possible to recover data 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

There are a few other things worth bearing in mind after a virus attack:

- 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 which can be encountered when using SWEEP. See also the ‘On-screen log messages’ chapter for details of individual error messages.

SWEEP runs slowly

Full sweep

By default, SWEEP will perform a ‘quick sweep’ which checks only the parts of files which are likely to contain a virus. However, if ‘full sweep’ is set SWEEP will be much slower. The speed difference between ‘full sweep’ and ‘quick sweep’ depends on the configuration of the computer, but typically the ‘quick’ level is 5 to 10 times faster than the ‘full’. See also ‘Sweeping level’ in the ‘Sweeping mode’ section of the ‘Configuring SWEEP’ chapter.

Checking all files

By default, SWEEP will only check files defined as executables. If SWEEP is checking all files, it will take longer than if only executable files are being checked. See the ‘Adding new items for immediate sweep’ sub-section of the ‘Immediate mode’ section of the ‘Using SWEEP’ chapter, and the ‘File list’ section of the ‘Configuring SWEEP’ chapter.

Network drives selected

Some network drives will be much larger than a local hard disk, and so will 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 selected then SWEEP will have to count all the items that are to be swept. This can take several minutes on large network drives.

Virus fragments

The report of a virus fragment indicates that a part of a file matches a 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 SWEEP has detected a new virus, which could become active. The file affected should be replaced with a clean copy.

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 SWEEP will report ‘Virus fragment’ rather than ‘Virus’. A corrupted virus cannot spread.

If a file contains a corrupted virus, remove the infected file and replace it with a clean copy.

False positive

This may happen for various reasons. Swap files, for example, may contain fragments of real viral code on a computer on which infected files were recently used. See ‘False positives’ below.

False positives

SWEEP may very occasionally report a virus in a file that is not infected. This may be because polymorphic viruses (which change their appearance on every infection) are deliberately written to look like normal programs.

If in doubt, contact Sophos’ technical support for advice.

To decrease the chance of false positives:

- Only sweep executables.
- Perform a ‘quick sweep’ rather than a ‘full sweep’ (see ‘Sweeping level’ in the ‘Sweeping mode’ section of the ‘Configuring SWEEP’ chapter).

Virus not disinfected

SWEEP may report that a virus has not been disinfected. In this case:

- Check that ‘disinfect documents’ is selected (see the ‘Action on virus detection’ section of the ‘Configuring SWEEP’ chapter).
- If dealing with a disk or removable media, make sure that it is not write-protected.

Note: SWEEP will not disinfect a virus fragment, as it has not found an exact virus match.

New viruses

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

If a virus unknown to SWEEP is suspected, please send Sophos a sample and a description as soon as possible. If it is a virus, SWEEP 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 to update SWEEP. The latest IDE files can also be downloaded from the Sophos Web site.

See the ‘Updating SWEEP with new virus identities’ section in the ‘Installing SWEEP’ chapter.

On-screen log messages

This chapter describes messages that can appear in SWEEP's 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` will depend on the settings on the Action tabbed page of the Configuration option (see the 'Action on virus detection' section of the 'Configuring SWEEP' 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 tabbed page of the Configuration option.

`File copied to` *`new location`*

The *`new location`* is the location specified in the Action tabbed page of the Configuration option.

```
Error problem
```

The *problem* will be one of either:

```
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! If there has been an error, the infected file will remain unchanged and may be able to infect other disks and files.

```
Has been disinfected
```

SWEEP for Windows 95 can automatically disinfect, or remove, certain boot sector viruses on floppy disks. SWEEP can also automatically remove the viral macros from documents infected with certain types of macro viruses.

Note: SWEEP for DOS will be required to disinfect a hard disk boot sector.

```
Error:  Disinfection failed
```

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

Important! If disinfection has failed, the infected item 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 fragments' in the 'Troubleshooting' chapter.

Error messages

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

The file called `filename` was on the list of files to be swept, 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 swept, 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 sweep 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 tabbed page of the Configuration option (see the 'Reporting results' section of the 'Configuring SWEEP' 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 'SWEEP 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 ‘Reporting results’ section of the ‘Configuring SWEEP’ chapter).

Glossary

ASCII: American Standard Code for Information Interchange; the standard system for representing letters and symbols. Each letter or symbol is assigned a unique number between 0 and 127.

BIOS: The Basic Input/Output System of MS-DOS which constitutes the lowest level of software which interfaces directly with the hardware of the computer.

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

Booting-up: A process carried out when a computer is first switched on or reset, where the operating system software is loaded from disk.

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. Usually 32 or 64 bits long.

COM: The extension given to a type of executable file in MS-DOS. A COM file is similar to an EXE file, but can only contain up to 64K of code and data. In operating systems other than DOS, the extension COM can have a different significance.

Companion Virus: A virus which ‘infects’ EXE files by creating a COM file with the same name which contains the virus code. It exploits the DOS property that if two programs with the same name exist, the operating system will execute a COM file in preference to an EXE file.

Compressed File: See File Compression.

DOS: Disk Operating System. See MS-DOS.

DOS Boot Sector: The boot sector which loads the BIOS and DOS into PC RAM and starts their execution. Common point of attack by boot sector viruses.

False Negative: An existent event reported as non-existent, e.g. the absence of a virus when the virus is present.

False Positive: A non-existent event reported as existent, e.g. the presence of a virus when no virus is present.

File Compression: The compacting of a file through the process of recoding its bit structure into a shorter form. File compression must be reversible.

Hexadecimal: A system of counting using number base 16. The numbers 10 to 15 are represented by the characters 'A' through 'F' respectively. Hexadecimal is often abbreviated to Hex. Each Hex digit is equivalent to four bits (half a byte) of information.

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.

IP: Internet Protocol; the base level of the TCP/IP system. It is a connectionless, unreliable datagram service. 'Datagram' means that all communications are made up of packets; 'connectionless', that each network packet is separate and individually routed; and 'unreliable' means that packets are not guaranteed to get through. An IP packet contains two IP addresses for its source and destination.

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

LAN: Local Area Network; a data communications network covering a limited area (up to several kilometres in radius) with moderate to high data transmission speeds.

Link Virus: A virus which subverts directory entries to point to the virus code.

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 also attain a degree of platform independence.

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 bootstrapped. It contains the partition table as well as the code to load and execute the boot sector of the 'active' partition. Common point of attack by boot sector viruses.

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.

MS-DOS: The Disk Operating System sold by Microsoft. It is the most common microcomputer operating system in the world, and operates on the IBM PC.

Multipartite Virus: A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector viruses and parasitic viruses.

OVL: The extension commonly given to overlay files in MS-DOS. Overlay files are used with large programs which cannot fit into RAM: parts of the program are loaded as and when needed. Overlay files can have any extension, not just OVL.

Parasitic Virus: A computer virus which attaches itself to another computer program, and is activated when that program is executed. A parasitic virus can attach itself to either the beginning or the end of a program, or it can overwrite part of the program.

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.

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

TSR: Terminate and Stay Resident; a term used to describe an MS-DOS program which remains in memory after being executed. A TSR can be re-activated either by a specific sequence of keystrokes, or at some specific time, or by some specific signal from an I/O port.

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. Sophos describe viruses using the proprietary Virus Description Language (VDL).

Virus Pattern: A sequence of bytes extracted from a virus and used for virus recognition.

WAN: Wide Area Network; a set of computers that communicate with each other over long distances.

Index

A

ARC 53
ASCII 119

B

BIOS 119
boot sector 119
  disinfecting 53, 105
  DOS 120
    replacing 106
  master 121
    replacing 106
  virus 119
booting-up 119

C

checksum files 14
  central 16, 81, 94, 98
  deletion 79, 93
  local 16
checksums 119
COM files 67, 79, 119
command line qualifiers
  ICWIN95 99
  INTERCHK 99
  SWEEP95 63–64
COMMAND.COM 82
communications directory 30, 36, 84, 85
companion virus 67, 119
compressed files 120
  sweeping 96
continuous log 59, 63
critical program 81, 86, 91

D

Diet 53
disinfection 103–107
disk
  operating system, see DOS
documents
  disinfection 54, 106
DOS 120
  boot sector 67, 120
DOT files 79, 87

E

email attachments 13
Ethernet
  address 76
excluding files from checking by InterCheck 81, 86, 91
excluding files from sweeping 61
EXE files 67, 79
executables 109
  dealing with infected 54, 106
  defining 60
  limiting sweep to 46

F

false negative 120
false positive 111, 120
FAT 120
file
  COM 119
  compression 120
  IDE 120
  OVL 121
floppy disk
  disinfecting boot sector 53, 106
full sweep 10, 52, 109

H

hard disk
  disinfecting boot sectors 105
hexadecimal 120

I

ICWIN95 99
  command line qualifiers 99

IDE file, 120
  centralised distribution 41
  for new virus 41, 112
identity
  of a virus 122
immediate mode
  configuration 51
  file list
    adding an entry 46
    default 45
    file types 46
    path name 46
    removing an entry 47
    subdirectories 46
  starting a sweep 45
infected boot sectors
  dealing with 53, 105
infected documents
  dealing with 54, 106
infected executables
  dealing with 54, 106
InstallOptions
  section in INTERCHK.CFG 74
InterCheck 9, 13–18, 120
  automatic updating 84
  checking networked drives 85
  command line qualifiers 100
  communications directory 30, 36, 84, 85
  configuration file, see INTERCHK.CFG
  critical program support 81, 86, 91
  disabling 83, 99
  DOS drive mappings 98
  enable 100
  excluding files from checking 81, 86
  excluding programs from checking 91
  halt on virus detection 88
  installation overview 17
  interception 85
  loading in low memory 89
  loading prevention 86
  memory checking 91
  messages on loading 95
  NetBIOS 76
  NetWare 76
  network address specification 99
  output suppression 100
  pop up message 91
  running SWEEP on initial start-up 79
  running SWEEP on installing 89
  running SWEEP on loading 79, 89
  running SWEEP on updating 79, 97
  server is unavailable message 94
  status testing 100
  swapping 95
  timeout 94
  unloading from memory 83, 101
  virus alert message 92
  virus checking at run-time 80
  virus checking at start-up 77
  what is checked 85, 88, 89, 93, 97
InterCheck client 14
  address 83, 99
  configuration 73–101
  configuring individual workstations 75
  in operation 70
  installing 69
  networked 14, 20
  stand-alone 14, 20
  starting 70
  using 69–71
InterCheck server 14
InterCheckDOSGlobal
  section in INTERCHK.CFG 74
InterCheckDOSWorkStation
  section in INTERCHK.CFG 74
InterCheckGlobal
  section in INTERCHK.CFG 74
InterCheckW95Global
  section in INTERCHK.CFG 74
InterCheckW95WorkStation
  section in INTERCHK.CFG 74
InterCheckWorkStation
  section in INTERCHK.CFG 74
INTERCHK 99
  command line qualifiers 99
INTERCHK.CFG 73
  automatic updating 82, 97
INTERCHK.CHK 85
  deletion 93
Internet downloads 13
Internet Protocol, see IP
IP 120
  address 120

L

LAN 120
link virus 67, 121
Local Area Network, see LAN
log file 93, 116
LOGIN.EXE 82
low memory
  InterCheck 89
LZEXE 53

M

macro virus 54, 67, 87, 121
  removal 106
master boot sector 67, 121
  disinfection 106

memory-resident virus 68, 121
Microsoft Exchange 55, 62, 117
monochrome monitor 91
MS-DOS 121
multipartite virus 121

N

NETADR 76
NetBIOS 76, 100
NetWare 76, 100
network
  address specification by InterCheck 99
  drive checking by InterCheck 85
  local area 120
  wide area, see WAN

O

on-screen log 63
  clearing 63
OV? files 79
OVL files 121

P

parasitic virus 121
PKLite 53
polymorphic virus 111, 121, 122
portable PCs 17
progress bar 63

Q

quick sweep 10, 52, 109

R

report file 56, 116
reporting
  automatic 16

S

scheduled mode
  configuration 48, 51
  job list
    adding an entry 48
    default 47
    editing an entry 49
    removing an entry 49
shredding
  of infected files 54
Sophos Anti-Virus
  about 9–12
stealth virus 54, 121
SWEEP 9
  auto start 64
  auto start and exit 63
  checking system areas under InterCheck 96
  command line qualifiers 63–64
  excluding files to be checked 61
  immediate mode 10
  restoring default settings 62
  scheduled mode 10
  started by InterCheck 77
  starting 43
  troubleshooting 109–112
SWEEP configuration
  action 53
    disinfect boot sectors 53
    disinfect documents 54
    infected files 54
    request confirmation 54
  file list 57
  mode 52
    compressed files 53
    priority 52
    sweeping level 52
  notify 55
    notification list 56
    notify timing 55
  report 56
    report file 57
    report mode 56
  time 58
SWEEP installation 19–42
  central 19, 29–33, 34–35
    auto-upgrade mode 33
    central installation options 32
    folder selection 31
    installation type 29
    InterCheck folder selection 30
    SWEEP destination folder 31
    SWEEP source folder 31
  local 19, 22–24
    folder selection 23
    installation type 22
    startup options 24
    SWEEP destination folder 23
    SWEEP source folder 23
  starting the installation program 21
  system requirements 19
SWEEP updating
  central 35–38, 39–41
    update options 40
    upgrade components 37
  local 25–28
    update options 26
    upgrade components 26
  with new virus identities 41
SWEEP VxD 82, 95
  disabling 86
  load option 95
  log file 96

level 82, 96
name 96
scanning compressed files 96
sweeping mode 96
SYS files 79

T

technical support
Sophos 2
Terminate and Stay Resident, see TSR
Trojan horse 67, 121
troubleshooting
SWEEP 109–112
TSR 122

U

UNC 122
Universal Naming Convention, see UNC
upper memory
InterCheck 89

V

VDL 122
virus
boot sector 119
Cascade 107
companion 67, 119
disinfection 53–55, 103–107
fragment 110
identity 122
link 67, 121
macro 54, 67, 87, 121
memory-resident 68, 121
Michelangelo 107
multipartite 121
new 112
parasitic 121
pattern 122
polymorphic 121, 122
recovery from 105, 107
stealth 121
Windows 67
Winword/Wazzu 107
Winword/ShareFun 106
Virus Description Language, see VDL
virus library 65–68
searching for a virus 67
starting 65
virus information 66

W

WAN 122
Wide Area Network, see WAN
Windows 95
Control Panel 76
Explorer 70
StartUp folder 64
Windows viruses 67

X

XL files 79, 92

Z

ZIP 53
ZOO 53

User comment form

We welcome your comments and suggestions on our software and documentation. They help us to provide you with better products. Please fax this form to +44 1235 559935. Comments about this manual can also be emailed to <publications@sophos.com>.

Product: ________________________________ Version: ❒.❒❒

Documentation:	Excellent	Good	Fair	Poor
Accuracy	❒	❒	❒	❒
Completeness	❒	❒	❒	❒
Clarity	❒	❒	❒	❒
Page layout	❒	❒	❒	❒

Software:	Excellent	Good	Fair	Poor
Ease of use:	❒	❒	❒	❒
Ease of installation:	❒	❒	❒	❒
Overall assessment:	❒	❒	❒	❒

Please indicate any errors found in this software or documentation:

____

____

____

Please give any suggestions for improving the software or documentation:

____

____

____

Name: ____

Position: ____

Organisation: ____

Address: ____

____

Telephone: ______________________ Fax: ______________________

Signed: ______________________ Date: ______________________

Australia:

Doctor Disk
Level 7
418A Elizabeth Street
Surry Hills NSW 2010
Australia
Email sales@drdisk.com.au
http://www.drdisk.com.au/
Tel 02 9281 2099 · Fax 02 9281 9740 · Code +61

Bahrain:

International Information Systems
PO Box 3086
Flat 31, Building 123 Block 320
Exhibition Road
Manama
Bahrain
Tel 293821, 292040 · Fax 293408 · Code +973

Belgium:

Software Marketing Group
rue E. Van Ophemstraat 40
B-1180 Brussels
Belgium
Email pbuysse@netdirect.be
Tel 02 376 57 42 · Fax 02 376 09 85 · Code +32

Brazil:

Datasafe Produtos de Informática e Serviços Ltda
Rua Santa Justina, 336 Gr. 108
Itaim
04545-041 Sao Paolo SP
Brazil
Email datasafe@originet.com.br
Tel 011 822 1129 · Fax 011 822 1129 · Code +55

Channel Islands:

Softek Services Ltd
20 Peter Street
St Helier
Jersey
JE2 4SP
Email sales@softek.co.uk
http://www.softek.co.uk/
Tel 01534 811182 · Fax 01534 811183 · Code +44

Croatia:

Qubis d.o.o.
Nova Cesta 1
10000 Zagreb
Croatia
Email qubis@zg.tel.hr
Tel 01 391461 · Fax 01 391294 · Code +385

Denmark:

Lamb Soft & Hardware
Lille Strandstraede 14
1254 Copenhagen K
Denmark
Email info@lamb-soft.dk
http://www.lamb-soft.dk/
Tel 3393 4793 · Fax 3393 4793 · Code +45

Finland:

Oy Protect Data Ab
PL 21
FIN-00701 Helsinki
Finland
Email karlerik.heimonen@protectdata.fi
http://www.protectdata.fi/
Tel 09 7525 2440 · Fax 09 7525 2210 · Code +358

France:

Racal-Datacom S.A.
18 Rue Jules Saulnier
93206 Saint-Denis Cedex
France
Email infos@racal-datacom.fr
Tel (1) 49 33 58 00 · Fax (1) 49 33 58 33 · Code +33

Germany:

NoVIR DATA
Hochofenstrasse 19-21
23569 Lübeck
Germany
Email 100141.2044@compuserve.com
Tel 0451 306 066 · Fax 0451 309 600 · Code +49

Hong Kong:

Racal-Datacom Limited
Sun House
181 Des Voeux Road
Central Hong Kong
Email w_chu@racal.com.hk
Tel 28158633 · Fax 28158141 · Code +852

Ireland:

Renaissance Contingency Services Ltd.
The Mews
15 Adelaide Street
Dun Laoghaire
Co Dublin
Ireland
Tel 01 280 9410 · Fax 01 280 8302 · Code +353

Italy:

Telvox s.a.s.
Via F.lli Cairoli 4-6
40121 Bologna
Italy
Email telvox.teleinf@bologna.nettuno.it
http://www.nettuno.it/fiera/telvox/telvox.htm
Tel 051 252 784 · Fax 051 252 748 · Code +39

Japan:

Computer Systems Engineering Co. Ltd.
23-2 Maruyamacho
Aletsusa Bldg.
Shibuya-ku
Tokyo 150-0044
Japan
Email pws@cseltd.co.jp
http://www.cseltd.co.jp/sweep/
Tel 03 3463 5633 · Fax 03 3496 7477 · Code +81

Malta:

Shireburn Co. Ltd.
Carolina Court
Guze Cali Street
Ta'Xbiex, Msd 14
Malta
Email info@shireburn.com
http://www.shireburn.com/
Tel 319977 · Fax 319528 · Code +356

Netherlands:

CRYPSYS Data Security
P.O. Box 542
4200 AM Gorinchem
The Netherlands
Email info@crypsys.nl
http://www.crypsys.nl/
Tel 0183 62 44 44 · Fax 0183 62 28 48 · Code +31

Forum Data Security
WG Plein 202
1054 SE Amsterdam
The Netherlands
Email info@forum-ds.nl
http://www.forum-ds.nl/
Tel 20 685 3486 · Fax 20 612 9702 · Code +31

New Zealand:

Wang New Zealand Ltd
P O Box 6648
Wellington
New Zealand
Email sophos@wang.co.nz
Tel 04 382 0100 · Fax 04 385 6067 · Code +64

Norway:

Protect Data Norge AS
Brobekkveien 80
0583 Oslo
Norway
Email pdn@protect.no
http://www.protect.no/
Tel 022 071500 · Fax 022 071501 · Code +47

Poland:

Safe Computing Ltd.
ul. Targowa 34
03-733 Warszawa
Poland
Email info@safecomp.com
http://www.safecomp.com/
Tel 022 6198956 · Fax 022 6700756 · Code +48

Portugal:

Década Informática s.a.
Apt. 7558
Estr. Lisboa/Sintra, Km 2,2
2720 Alfragide
Portugal
Email amandio.sousa@decada.mailpac.pt
Tel 01 471 2045 · Fax 01 471 2191 · Code +351

Singapore:

Racal Electronics (S) Pte. Ltd.
26 Ayer Rajah Crescent #04-06/07
Singapore 139944
Email sales@racal.com.sg
http://www.racal.com.sg/
Tel 779 2200 · Fax 778 5400 · Code +65

Slovakia:

Protect Data Slovakia
Kukolova 1
831 07 Bratislava
Slovak Republic
Email protectd@ba.sanet.sk
Tel 07 541 1527 · Fax 07 541 2210 · Code +421

Slovenia:

Sophos d.o.o.
Zwittrova 20
8000 Novo mesto
Slovenia
Email slovenia@sophos.com
Tel 068 322977 · Fax 068 322975 · Code +386

Spain:

Sinutec Data Security Consulting S.L.
Traversera de Gracia 54-56 Entlo. 3 y 4
08006 Barcelona
NIF B-60062502
Spain
Email sinutec@ysi.es
http://www.sinutec.com/
Tel 3-414.49.19 · Fax 3-202.14.25 · Code +34

Sweden:

Protect Datasäkerhet AB
Humlegardsgatan 20, 2tr
Box 5376
102 49 Stockholm
Sweden
Email info@protect-data.se
http://www.protect-data.se/
Tel 08 459 54 00 · Fax 08 459 54 10 · Code +46

Switzerland:

Performance System Software SA
Rue Jean-Pelletier 6
1225 Chene-Bourg
Geneva
Switzerland
Email jlt@pss.ch
http://www.pss.ch/
Tel 022 860 1030 · Fax 022 349 4775 · Code +41

Turkey:

Logic Bilgisayer Ltd
Esentepe Cad. Techno Centre 10/2
Mecidiyekoy
Istanbul
Turkey
Tel 0212 212 3664 · Fax 0212 212 3669 · Code +90

United States of America:

ACT
7908 Cin-Day Rd, Suite W
West Chester
Ohio 45069
USA
Email farrell@altcomp.com
http://www.altcomp.com/
Tel 513 755 1957 · Fax 513 755 1958 · Code +1

Uruguay:

Datasec
Patria 716
Montevideo 11300
Uruguay
Tel 02 7115878 · Fax 02 7115894 · Code +598

Sophos Plc • The Pentagon • Abingdon Science Park • Abingdon • OX14 3YP • England • Tel 01235 559933 • Fax 01235 559935
Sophos Inc • 18 Commerce Way • Woburn • MA 01801 • USA • Tel 781 932 0222 • Fax 781 932 0251
Sophos GmbH • Am Hahnenbusch 21 • D-55268 Nieder-Olm • Germany • Tel 06136 91193 • Fax 06136 911940

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