Sophos Anti-Virus

User Manual

OS/2

SOPHOS

Sophos Anti-Virus

for OS/2

User Manual
February 1998

This manual documents Sophos Anti-Virus
for OS/2, 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 # masoez02/980115

This document is also available in electronic form from Sophos.

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

Contents

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.

About SWEEP and OS/2

There are a small number of OS/2 specific viruses. Although most viruses are written for DOS, these can still replicate and infect DOS programs held on OS/2 based PCs. In addition, macro viruses can infect documents held on OS/2 based PCs.

SWEEP for OS/2 is virus-specific and will check OS/2 based computers for DOS, OS/2, Windows and macro viruses.

About InterCheck

For an introduction to InterCheck, see the separate ‘About InterCheck’ chapter.

How to use this manual

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

On-demand scanning

If using SWEEP for on-demand scanning, read ‘Installing SWEEP’ and ‘Using SWEEP’.

On-access scanning for a network

If using SWEEP and InterCheck to provide on-access scanning for networked workstations, read the ‘About InterCheck‘, ‘Installing the InterCheck server’, ‘Installing InterCheck clients’, ‘Controlling the InterCheck server’ and ‘Configuring InterCheck clients’ chapters.

More advanced features

If using SWEEP’s more advanced features, read the ‘Configuring SWEEP’ chapter.

General information

For further information, read the ‘Treating viral infection’ and ‘Troubleshooting’ chapters.

Summary of each chapter

This manual is organised into the following chapters:

- ‘About Sophos Anti-Virus’, this chapter.
- ‘About InterCheck’ presents an overview of Sophos’ InterCheck technology.

- 'Installing SWEEP' describes how to install SWEEP on a workstation or a file server, how to run SWEEP for the first time, and how to upgrade SWEEP.
- 'Using SWEEP' describes how to run SWEEP for routine virus checking and how to run SWEEP on a file server.
- 'Configuring SWEEP' describes how to specify items to be checked by SWEEP and how to run SWEEP at different priorities. It also lists the SWEEP command line qualifiers.
- 'Installing the InterCheck server' describes how to install SWEEP as an InterCheck server in order to handle requests for on-access scanning from workstations.
- 'Installing InterCheck clients' describes how to install and run InterCheck clients on workstations.
- 'Controlling the InterCheck server' describes how to control SWEEP running as an InterCheck server.
- 'Configuring InterCheck clients' describes the configuration of InterCheck clients running under DOS, Windows 3.x and Windows 95.
- 'Treating viral infection' provides advice on removing a virus.
- 'Troubleshooting' provides help with possible problems.

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

Features of Sophos Anti-Virus

Sophos Anti-Virus for OS/2 is supplied with Sophos Anti-Virus for DOS and for Windows 95. It:

- Checks local hard disks, floppy disks and network drives for the presence of all viruses known to Sophos at the time of release.

- Incorporates Sophos' proprietary InterCheck client-server virus detection technology, which allows the use of server-based software for checking workstations.
- Is updated twelve times a year with the latest virus information. Urgent updates can also be distributed by fax or email, or downloaded from the Sophos Web site.
- Easily detects polymorphic viruses using Sophos' advanced Virus Description Language (VDL) and a built-in code emulator.
- Scans inside compressed files.
- Detects and disinfects Microsoft Word and Excel macro viruses.
- Offers two levels of security, allowing a 'quick sweep' which looks for viruses in parts of files likely to contain a virus, and a 'full sweep' which looks for viruses in every part of every executable.
- Is easy to use, yet easily integrated into complex virus-checking applications, such as the automated unattended checking of file servers.
- Can be scheduled with the aid of utilities supplied with the network software, so SWEEP can be configured to perform regular checks without any further operator action.
- Can be set to run in the background and as a low, medium or high priority operation.

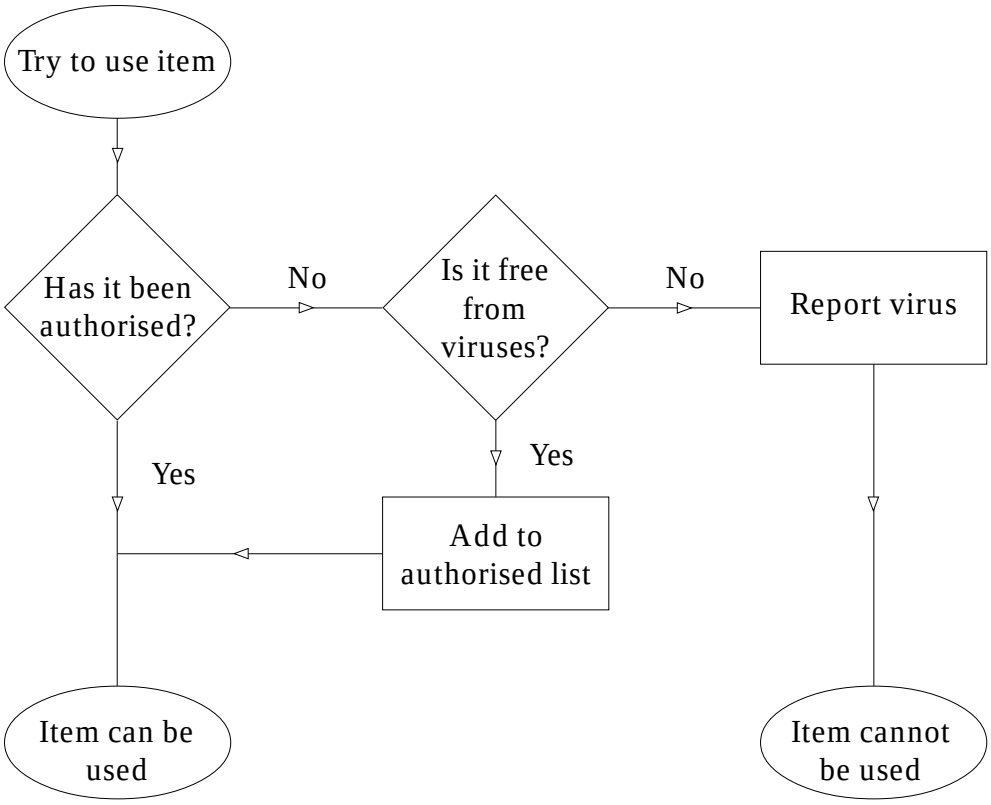
Sophos Anti-Virus is also available for Windows NT (i386 and Alpha AXP), Novell NetWare, OpenVMS (VAX and Alpha AXP) and Banyan VINES.

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 are InterCheck and SWEEP related?

Used alone, SWEEP offers on-demand virus checking; combined with InterCheck technology it also offers on-access checking.

InterCheck splits the task of virus detection between a client and a server. The **InterCheck client** determines whether items on the client workstation should be checked for viruses, while the **InterCheck server** (or a local installation of SWEEP) performs the actual virus checks where necessary.

What types of InterCheck client are there?

There are two main types of InterCheck client: networked and stand-alone.

A **networked InterCheck client** exists on a separate machine from the InterCheck server, and communicates with it over the network.

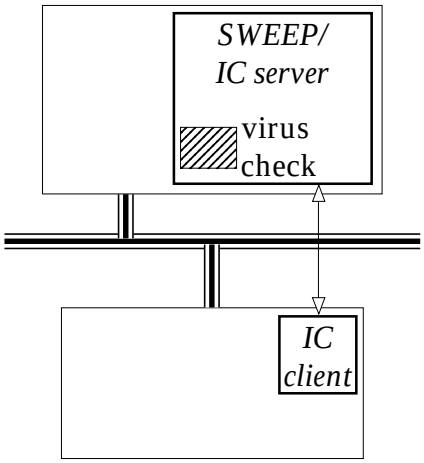
A **stand-alone InterCheck client** does not have to communicate with a remote InterCheck server, and uses a local installation of SWEEP to check for viruses.

A networked InterCheck client is easier to administer and uses fewer system resources on the client workstations. A stand-alone InterCheck client generally offers faster initial authorisation of files, and can also be used on machines not always connected to the network.

Either way, InterCheck is the most efficient way of protecting users from viruses: each item is checked for viruses only once, unless it is modified, in which case it is rechecked.

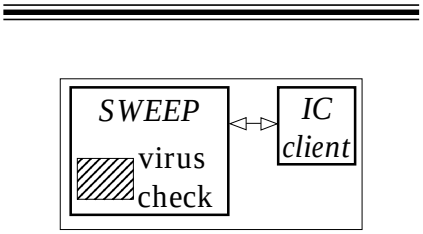
How does InterCheck work?

The InterCheck client software monitors all file and disk accesses. Whenever an item is accessed, it is

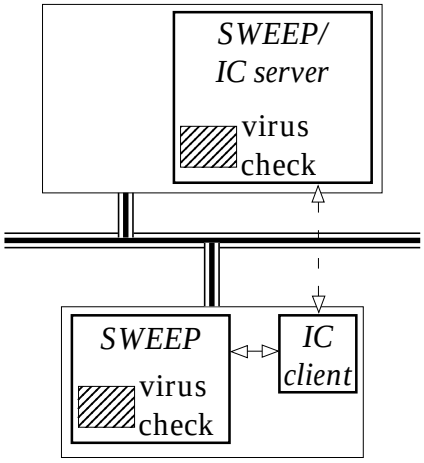


Networked IC client and remote IC server

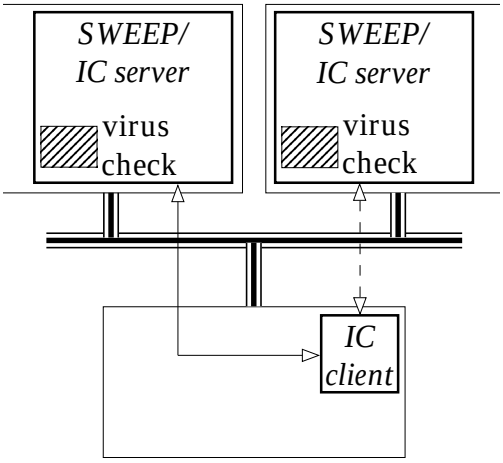
No IC server



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

compared with a list of authorised items. If a match is found, the access is permitted. If a match is not found, the networked InterCheck client sends a copy of the item to the InterCheck server for checking, while the stand-alone InterCheck client performs the checking by using the local installation of SWEEP.

If the item is found to be clean, it is added to the list of authorised items and the access is allowed to continue. Any further accesses of this item are then completed without the need for further authorisation, unless it is modified, in which case authorisation is again automatically requested.

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

Checksum files

The list of authorised items is called a checksum file.

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

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. The process of 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 continue to provide the same levels of 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

Native InterCheck server functionality is currently included in SWEEP for NetWare, Windows NT (Intel and Alpha), OpenVMS (VAX and Alpha), DOS, OS/2 and Banyan VINES. SWEEP for DOS can also be used to provide InterCheck server functionality for other operating systems.

Networked InterCheck clients require a separate InterCheck server. This involves installing SWEEP and the InterCheck software on the file server, and running SWEEP in InterCheck server mode. Networked InterCheck clients are currently available for DOS, Windows, Windows 95 and Macintosh workstations.

Stand-alone InterCheck clients do not require an InterCheck server. In the case of Windows 95 and Windows NT, the stand-alone InterCheck clients are installed as part of the SWEEP installation process. Stand-alone InterCheck clients are currently available for DOS/Windows 3.x, Windows for Workgroups, Windows 95 and Windows NT (Intel and Alpha) workstations.

InterCheck server installation and configuration

Windows NT, NetWare, OpenVMS, DOS, OS/2 and Banyan VINES

See the Sophos Anti-Virus user manuals for Windows NT, NetWare, OpenVMS, DOS, OS/2 and Banyan VINES (i.e. the Sophos Anti-Virus user manual for the InterCheck server) respectively.

Networked InterCheck client installation and configuration

Installation

DOS, Windows, Windows 95 and Macintosh

See the 'Installing InterCheck clients' chapter of the Sophos Anti-Virus user manual for the InterCheck server.

Configuration

DOS, Windows and Windows 95

See the 'Configuring InterCheck clients' chapter of the Sophos Anti-Virus user manual.

Stand-alone InterCheck client installation and configuration

Installation

DOS/Windows 3.x and Windows for Workgroups

See the 'Installing InterCheck clients' chapter of the Sophos Anti-Virus user manual for the InterCheck server.

Windows 95 and Windows NT

See the 'Installing SWEEP' chapter of the Sophos Anti-Virus user manuals for Windows 95 and Windows NT respectively.

Configuration

DOS/Windows 3.x, Windows for Workgroups and Windows 95

See the 'Configuring InterCheck clients' chapter of the Sophos Anti-Virus user manual.

Windows NT

See the 'Configuring SWEEP' chapter of the Sophos Anti-Virus user manual for Windows NT.

Installing SWEEP

This chapter describes the installation options and shows how to install SWEEP on a workstation or on a file server, how to run SWEEP for the first time, and how to update SWEEP.

System requirements

The minimum requirements are:

- An Intel 286 (or higher) based computer.
- OS/2 1.1 or later (excluding OS/2 2.0).
- 1 Mb to 3 Mb of hard disk space.

If intending to use InterCheck:

- IBM LAN Server software version 2 or higher. If LAN Server versions 2 or 3 are used, apply the latest corrective service to server and clients.

Which kind of installation?

Important! There are three different forms of installation, depending on the functions the user requires:

Installing SWEEP on a workstation.
This enables on-demand scanning of a workstation.

Installing SWEEP on a file server.
This makes on-demand scanning available to all users on the network.

Installing SWEEP as an InterCheck server.
This allows SWEEP to offer on-access scanning to other workstations on the network.

The first two are described here. For the third, see the 'Installing the InterCheck server' chapter.

Installing SWEEP

On a workstation

To install SWEEP on a workstation, insert the Sophos Anti-Virus CD in the CD drive and copy SWEEP to the hard disk:

```
MD C:\SWEEP
CD C:\SWEEP
COPY H:\OS_2\OSWEEP.EXE C:
```

where H: is the drive letter of the CD drive.

It is a good idea to include the path (`C:\SWEEP` in this example) in the `PATH` environment variable.

On a file server

If the licence covers installation of SWEEP on a file server, it can be installed there and made available to all stations on the network. To do this, copy the OS_2\OSWEEP.EXE file from the Sophos Anti-Virus CD to a publicly accessible area on the file server.

Running SWEEP for the first time

To check all hard disks on the system, type

```
OSWEEP
```

To check a single drive, specify its drive letter. For example to check a flopy disk in drive A:, type

```
OSWEEP A:
```

For full information on using SWEEP, see the 'Using SWEEP' and 'Configuring SWEEP' chapters.

Updating SWEEP

Registered users of SWEEP are sent updates in the first week of every month, or can download updated versions from the Sophos Web site.

If updating SWEEP for OS/2 on a server with Local Security installed, log in as an Adminstrator first.

Make sure SWEEP is not running in any session. If the OS/2 server is running, stop it by selecting its window and typing *Esc*. Then copy the contents of the OS_2 folder on the Sophos Anti-Virus CD into the SWEEP directory. Restart the InterCheck server if necessary (see the 'Installing the InterCheck server' chapter).

Urgent SWEEP updates

SWEEP can be updated 'in-the-field' to take into account new viruses discovered between monthly updates.

Sophos can supply new virus identities, which SWEEP will use for virus detection, as IDE (identity) files which consist entirely of printable ASCII characters. New identities can be faxed, emailed or downloaded from the Sophos Web site (http://www.sophos.com/).

Save the new identity in an ASCII file with an IDE extension (e.g. NEWVIRUS.IDE) and place it in the SWEEP directory. If the OS/2 InterCheck server is installed, it must be stopped and restarted (see the 'Installing the InterCheck server' chapter).

When SWEEP is run, there will be an increase in the number of viruses that SWEEP looks for. If the virus library is displayed (`SWEEP -DL`) the new virus will be included in it.

There is no limit on the number of IDE files that SWEEP can handle.

Important! ***.IDE files must reside on the same drive and in the same subdirectory as OSWEEP.EXE**.

Note: New virus identities are added to subsequent monthly updates of SWEEP, so the IDE files quickly become redundant and may be removed. SWEEP will warn if IDE files more than ninety days old are still present.

Using SWEEP

This chapter describes how to use SWEEP for routine virus checking and how to run SWEEP on a file server.

Note: This chapter describes SWEEP run with its default settings. In many cases, these will offer sufficient protection. However, for information on the options available, see the ‘Configuring SWEEP‘ chapter.

What will SWEEP check?

By default, SWEEP will look for viruses in:

- All 386, 3GR, ADD, COM, CPL, DLL, DMD, DOC, DOT, DRV, EXE, FLT, FON, FOT, I13, IFS, MOD, OV?, SCR, SYS, VXD and XL? files on all local hard disk drives.
- Logical sector 0 of all local hard disk drives.
- Physical sector 1 of hard disk devices 80 to 83 Hex.

Different areas or file types can be specified, as described in the ‘Configuring SWEEP’ chapter.

Sweeping level

By default, SWEEP performs a ‘quick sweep’, which checks only those parts of files likely to contain viruses. This is slightly less secure than a ‘full sweep’, which checks the entire file contents. To specify a ‘full sweep’, see the -F qualifier in the ‘Configuring SWEEP’ chapter.

Virus checking with SWEEP

SWEEP can be used to check hard disks, floppy disks and network drives for viruses.

Checking hard disks

Enter the command

```
OSWEEP
```

SWEEP will check all hard drives present on the system. It is possible to interrupt SWEEP by pressing *Esc* at any time.

To check particular hard drives, use their letters. For example:

```
OSWEEP D: E:
```

If SWEEP discovers any viruses it displays a red warning screen at the end of the run and sounds a bell. To clear the warning, press any key. Viruses which have been discovered will then be displayed.

Checking floppy disks

Run SWEEP using the command

```
OSWEEP -MU A:
```

SWEEP will prompt the user to insert floppy disks to be checked.

Checking file servers

SWEEP can be used to check file server logical drives over a network. On most networks it is necessary to be logged in as a supervisor or have read rights equivalent to those of a supervisor (the latter is more secure if the workstation itself is infected).

Most networks do not allow the boot sectors of file servers to be examined. Under OS/2 version 1.2 and later SWEEP determines automatically which drives

are network drives to which such restrictions apply. Under all versions of OS/2 from 1.1 onwards, SWEEP can be forced to treat all drives in a SWEEP run as network drives by using the -FS command line qualifier.

On most networks, some files are not readable and SWEEP will report an error after trying to open them. SWEEP automatically avoids the files

```
\EA#DATA.#SF
\WP#ROOT.#SF
\OS2\SYSTEM\SWAPPER.DAT
```

on all drives (note that the # symbol above represents the space character).

Any files can be exempted from examination by quoting them, preceded by the **exclusion operator**, in the SWEEP.ARE file. For more information see the 'What will SWEEP check?' section and the 'Configuring SWEEP' chapter.

A quick way of finding 'unreadable' files on the file server is to run SWEEP and note the names of any file(s) which could not be opened.

Important! Maximum effectiveness is obtained by running SWEEP on the file server itself in stand-alone mode. For instructions on disinfecting a system in stand-alone mode, see the 'Treating viral infection' chapter.

Running SWEEP on a file server

This section gives instructions for running SWEEP on a LAN Server or LAN Manager file server.

SWEEP for OS/2 can be installed on a file server as an integral part of an anti-virus strategy. Although SWEEP does not contain any network-specific features, the LAN server environment encourages the use of different techniques for controlling the operation of the virus scanner.

Scheduling

SWEEP can be scheduled to run on a regular basis using the AT command, provided by the Network Operating System. For example, the following instruction will run SWEEP at midnight each day and place the output in the file SWEEP.LOG:

```
AT 00:00 /E:M,T,W,Th,F,S,Su "C:\SWEEP\OSWEEP -P=C:\SWEEP\SWEEP.LOG"
```

The red 'alert' screen will be displayed if SWEEP detects a virus and the log file should then be examined to determine which files are infected. Full pathnames must be specified. The instruction can be added to the startup command file so that it will be automatically executed every time the server is started.

Background Operation

SWEEP can be configured to run continually as a background process. A command file is required to restart SWEEP after the scan has completed. The following is a simple example file which continually runs SWEEP until a virus is detected:

```
@ECHO OFF
:START
C:\SWEEP\OSWEEP -PR=L-P=C:\SWEEP\SWEEP.LOG
IF ERRORLEVEL 3 GOTO VIRUS_FOUND
GOTO START
:VIRUS_FOUND
```

The SWEEP option

```
-PR=L
```

changes the priority of the scan to low, so that the impact on server performance is reduced. It is not advisable to run the command file as a detached process since it cannot easily be monitored or terminated. The command should be run in the background instead. To ensure the command file is executed every time the server is started the

following line should be added to the startup command file

```
START /MIN RUNSWEEP.CMD
```

The command file can easily be customised to take additional actions when a virus is encountered.

What if SWEEP reports a virus or virus fragment?

If SWEEP reports a virus or virus fragment, it has almost certainly discovered a virus. However, there is always a small chance that the virus or virus fragment has been matched by a virus-free program. If in doubt, telephone Sophos' technical support for advice.

The screen output will look something like this

```
SWEEP virus detection utility
Version 3.04
(c) 1989,97 Sophos Ltd, Oxford

Please wait ...
System time 18:39:54, System date 16 December 1997

Virus library date 01 December 1997 (12988 viruses)

Quick Sweeping

Press Esc to quit.

Elapsed time 00:03
>>> Virus 'G2 v0.70B' found in file E:\OS2SWEEP\TEST\V.EX
18 files swept in 0 minutes and 7 seconds.
1 virus was discovered.
1 file out of 18 was infected.

Please send infected samples to Sophos for analysis.

For advice email technical@sophos.com or telephone +44 1235 559933.
```

Customising the 'Viruses found' report

SWEEP's 'Viruses found' warning can be customised, for example:

```
Contact MIS Immediately on Ext 4321
```

by placing text in the file SWEEP.MSG in the current directory. To specify a different file name, use the -FM command line qualifier.

Virus removal with SWEEP

SWEEP has facilities to disable some viruses while the infected system is running. See the ‘Treating viral infection’ chapter.

Configuring SWEEP

This chapter describes how to specify items to be checked by SWEEP, how to run SWEEP at different priorities, how to run SWEEP from batch files, and how to use SWEEP with new virus patterns. It also lists all the SWEEP command line qualifiers.

Note: For information on SWEEP's default settings, see the 'What will SWEEP check?' section of the 'Using SWEEP' chapter.

Specifying what SWEEP will check

Users can specify which items SWEEP will check by using either

- The command line, or
- An area file, SWEEP.ARE.

The command line allows the user to specify drives, directories, files or drive sectors. It can also include qualifiers (listed in this chapter).

The SWEEP.ARE file allows the user to specify what will be swept in greater detail, down to the level of a byte or group of bytes.

Specifying items to be checked in the command line

Items to be checked can be specified in the command line. For example, to check the file ISVIRUS.BIN type

```
OSWEEP ISVIRUS.BIN
```

or to check all executable files on drives D: and E: type

```
OSWEEP D: E:
```

Make sure that any symbols used do not conflict with the OS/2 meaning. For example, do not use the recursion symbol '>' in the command line, as it means redirection in OS/2.

Note: When the items to be checked are specified, all default settings will be overridden unless the -AS qualifier is added to the command line.

Specifying items to be checked in SWEEP.ARE

Items to be checked can be specified in an area file, SWEEP.ARE. This must reside in the current drive and subdirectory. For example, if the current drive and directory is C:\PROGS, SWEEP.ARE must reside on the C: drive in the directory C:\PROGS.

Note: When the items to be checked are specified, all default settings will be overridden unless the -AS qualifier is added to the command line.

The SWEEP.ARE file can be edited as required. The syntax for describing areas to be checked is given in the following sections. For example, SWEEP.ARE may contain

```
D:|0
D:>*.EXE
D:>*.OVL
+81 0 0 1
```

which will check the bootstrap sector on drive D:, all EXE and OVL files on drive D: and physical sector 1 on the second hard disk.

Note: The | symbol is the OS/2 'pipe' operator and is not the same as 1 (one) or l (letter l).

Drives can also be specified in the command line. For example, to check drives A: and D: while SWEEP is on drive C:, type

```
OSWEEP A: D:
```

Note that a default drive can precede any areas defined in the SWEEP.ARE file *which do not already specify a drive*. For example, if SWEEP.ARE contains

```
*.*
D:|0
```

and the user issues the command (see -AD command line qualifier for a full explanation)

```
OSWEEP -AD=A
```

then SWEEP will check

```
A:*.*
D:|0
```

Specifying files to be swept in SWEEP.ARE

Particular file types and areas can be specified in SWEEP.ARE using the normal OS/2 descriptions. For example

```
C:\*.ABC
```

will make SWEEP examine all files with extension .ABC in the root directory of drive C:.

The *recursion operator* '>' can be used to specify that all subdirectories, as well as the current directory, should be searched. For example, if the entry

```
C:*.ABC
```

is specified, and the disk in drive C: contains two subdirectories, **only the current directory** will be searched for ABC files. On the other hand, if the entry

```
C:>*.ABC
```

is specified, not only the current directory but also both subdirectories will be searched for ABC files. Similarly, if the entry

```
C:\MYAREA\MYFILES\>*.ABC
```

is specified, the search will cover the subdirectory C:\MYAREA\MYFILES and all its child directories.

Remember that the more files specified, the longer it will take to check the system.

To check all executable files (COM, EXE, OV?, SYS, DLL, DRV, IFS, etc.) specify

```
C:"All executables"
```

Sweeping is about 30% faster than when each group is specified individually. The drive specification (C: in above example) is optional.

Excluding files from sweeping

Certain files or directories can be excluded from sweeping, by preceding the description with the '<' exclusion operator. For example

```
C:\>*.EXE
<C:\DONOT.EXE ; will not be examined
```

will recursively search all EXE files except DONOT.EXE in the root directory of drive C:. If the name of a file **without a drive or path** is specified, all files or directories with that name will be excluded.

For example

```
<FOO.EXE
  ; file FOO.EXE will be excluded
  ; in whatever drive and
  ; directory it may appear
<C:FOO.EXE
  ; FOO.EXE will be excluded in
  ; the current directory of
  ; drive C
```

```
<\J\FOO.EXE
  ; FOO.EXE will be excluded if
  ; found in the \J directory of
  ; the current drive
<J\FOO.EXE
  ; FOO.EXE will be excluded if
  ; found in the J subdirectory
  ; of the current directory on
  ; the current drive
```

Note: Wildcard characters **cannot** be used with the exclusion operator.

Any exclusion descriptors which contain the '\' symbol and do not specify a drive will have the drive specified in the -AD command line qualifier inserted. For example, if SWEEP.ARE contains

```
<\NU.EXE
```

and SWEEP is started with the command line qualifier

```
OSWEEP -AD=C:
```

the file which will be excluded will be C:\NU.EXE. This is equivalent to entering

```
<C:\NU.EXE
```

in the SWEEP.ARE file.

Specifying disk sectors to be swept in SWEEP.ARE

At a lower level than the file structure, disks are organised into 'sectors'. The most important of these are the 'master boot sector' and the 'partition boot sector', as they contain executable program code which many viruses attack. A floppy disk has only a partition boot sector.

Sectors can be referred to in two different ways: as *logical* sectors or as *absolute* sectors. A *logical* sector number refers to the position of the sector within a

particular drive or partition. This is useful when referring to the partition boot sector, which is logical sector 0 of the partition. The *absolute* specification of a sector is in terms of the cylinder, head and sector of its physical position on the specified device. While more complex than a logical sector number, it allows any sector on the disk to be specified. This is important for checking the master boot sector, which can be found at cylinder 0, head 0, sector 1. On hard disks this sector is not accessible using a logical sector number. On floppy disks, absolute sector 0,0,1 and logical sector 0 are the same physical sector.

Specifying Logical Sectors to be swept

To specify a particular logical sector or set of sectors, use the '|' symbol (the OS/2 pipe operator). It is also possible to specify a byte or group of bytes to be checked in each sector (for example if the sector contains variable information). The format of the specification is

```
drive | ssector esector sbyte ebyte
```

where

`drive` is the drive letter, eg. C: (optional)

`ssector` is the first logical sector to be checked

`esector` is the last logical sector to be checked (optional)

`sbyte` is the first byte to be checked (optional)

`ebyte` is the last byte to be checked (optional)

Note that all values must be in **decimal** format.

For example

```
C:|0
```

specifies that the whole of logical sector 0 on drive C: should be checked, whereas

```
C:|0 10
```

specifies that a check should be taken of logical sectors 0 to 10 inclusive, and

```
C:|0 10 271 275
```

specifies further that in each of the logical sectors 0 to 10, only bytes 271 to 275 inclusive should be checked.

The following specification would check logical sector 15 on drive A:, checking only byte number 536 within that sector:

```
A:|15 15 536
```

Note that the start- and end-sectors have been specified the same.

In addition, the following can be used on all drives except network drives:

```
|*
```

This checks all disk sectors within the current logical disk, and should be used with care, because it may find virus fragments in deleted files, and might cause false positives.

Specifying Absolute Sectors to be swept

To specify an absolute sector, use the '+' symbol followed by the drive number, the cylinder (or 'track') number, the head (or 'side') number and the sector number within that cylinder. The first floppy disk drive in the system is number 0, the second is number 1, and so on. The first physical hard disk drive is number 80, the second is number 81 and so on. It is also possible to specify a byte or group of bytes to be checked in the sector (for example if the sector contains variable information).

The format of the specification is

```
+drive cylinder head sector sbyte ebyte
```

where

`drive` is the disk drive number

`cylinder` is the cylinder number

`head` is the head number

`sector` is the sector number

`sbyte` is the first byte to be checked (optional)

`ebyte` is the last byte to be checked (optional)

Note that all values must be in **hexadecimal** format.

For example

```
+80 0 0 1
```

specifies that sector 1 of cylinder 0, head 0 on the first fixed disk (usually drive C:) should be checked, whereas

```
+1 0 0 1 23 1B7
```

specifies that a check should be taken of bytes 23 hex to 1B7 hex inclusive on sector 1 of cylinder 0, head 0 on the second floppy-disk drive (usually drive B:).

To check master boot sectors on drives 80 to 83 Hex, specify

```
C:"All master boot sectors"
```

If a particular drive is not present, no error message is produced.

Full sweep

By default, ‘quick’ sweep is enabled. This checks only those parts of files likely to contain viruses and is marginally less secure than a ‘full’ sweep, which checks the entire contents of files.

A ‘full’ sweep can be selected with the command line qualifier -F. See the ‘Command line qualifiers’ section.

Running SWEEP at different priorities

When SWEEP is run, it is scheduled by OS/2 to run with the same priority as any other OS/2 application, such as a word processor. Network servers run at a high priority in order to achieve rapid response.

SWEEP should be run in high priority mode if a virus is suspected on your system and the user wishes to run SWEEP as soon as possible and as fast as possible, without shutting the system down. Use the command line qualifier -PR=H.

```
OSWEEP -PR=H
```

This will run SWEEP with the same high priority as the network software, but at a lower priority than any real-time processes.

SWEEP should be run in low priority (lower than any other task) if the user wishes to check constantly for virus presence, without affecting the system performance. Use the command line qualifier -PR=L.

```
OSWEEP -PR=L
```

This makes SWEEP run only when OS/2 would otherwise be idle.

Running SWEEP from batch files

SWEEP returns error codes that can be tested by using the 'IF ERRORLEVEL' command in batch files. This enables automatic action to be taken if SWEEP discovers an abnormal condition. SWEEP returns:

0 If no errors are encountered and no viruses found.

1 If the user interrupts the execution by pressing *Esc*.

2 If some error preventing further execution is discovered or if compressed files have been found when using the -WC command line qualifier.

3 If viruses or virus fragments are discovered.

Hint: These return values can be tested by using the 'IF ERRORLEVEL' command. For example

```
@ECHO OFF
OSWEEP -NK
IF ERRORLEVEL 3 GOTO FISHY
IF ERRORLEVEL 1 GOTO SOMEERR
ECHO No problems
GOTO END
:SOMEERR
ECHO Some error has occurred
GOTO END
:FISHY
ECHO Something has been discovered
:END
```

This batch file will print

```
Something has been discovered
```

if SWEEP discovers a virus,

```
Some error has occurred
```

in the event of an error, or

```
No problems
```

if nothing is discovered. The -NK command line qualifier tells SWEEP not to pause for a key if viruses are discovered.

Sweeping with new virus identities

SWEEP can be updated to check for specific new viruses. See 'Urgent SWEEP updates' in the 'Installing SWEEP' chapter for details.

Sweeping with new patterns

The range of patterns checked by SWEEP can be extended by creating a file called SWEEP.PAT containing the patterns in the following format:

```
Name Hex1 Hex2 ... Hexn ; Comments
```

where

`Name` is the pattern name (no spaces allowed)

`Hex1` etc. are pattern bytes in hexadecimal, 2 hexadecimal digits per byte, most significant nibble first

`; Comments` are any comments after the ';'

Pattern bytes can be separated by spaces or tabs. A name can contain up to 16 characters and a pattern can be up to 24 bytes long.

If the line starts with a space or a tab, the pattern will have the name 'Noname n' where n is a number from 0 upwards.

For example, SWEEP.PAT may contain

```
ABC_Virus 26 83 88 9c 9f f9 f0 23
HAL_Virus ABCDEF0123456789 ; comment
```

Important! **SWEEP.PAT must reside in the current drive and subdirectory**. For example, if the current drive and directory is C:\PROGS and drive A: is being checked using the command

```
OSWEEP A:
```

then SWEEP.PAT must reside on the C: drive in the directory C:\PROGS.

Note: SWEEP looks for patterns only when it is run in 'full sweep' mode ('quick sweep' is the default). The -F qualifier must be specified. For example

```
OSWEEP C: -F
```

Virus disinfection and removal

Common boot sector viruses can be removed from hard and floppy disks, and macro viruses from documents, by using SWEEP's built-in disinfection

capability. To enable this, the system must be shut down and restarted, and the the command line qualifier -DI must be used

```
A: OSWEEP C: -DI
```

SWEEP can also be used to delete infected executables while the system is running. This is done with the -REMOVEF qualifier.

For full information, see the 'Treating viral infection' chapter.

SWEEP command line qualifiers

SWEEP accepts certain optional command line qualifiers to control and/or automate the sweeping process. These can be used to customise the working of SWEEP to individual requirements. The qualifiers are described in the following subsections, or can be listed using

```
OSWEEP -?
```

The command format is

```
OSWEEP drive file1 ... filen qua1 ... quan
```

where

`drive` is the optional default drive which will be checked (A:, B:, C: etc.) and '*:' denotes all local hard drives

`file1` to `filen` are descriptors of files checked

`qua1` to `quan` are command line qualifiers (all beginning with either a hyphen '-' or a slash '/')

For example

```
OSWEEP A:
```

will SWEEP the floppy disk in drive A: while

```
OSWEEP -P=ALL.LOG -NS
```

will SWEEP all local hard disks, listing each file in the file ALL.LOG.

Note: Command files can contain any number of items per line (up to the maximum number of characters permitted per line)

@file Command line qualifiers from an external file

SWEEP can obtain its command line qualifiers from an external text file. For example:

```
OSWEEP @SWEEP.CM E:
```

when the file SWEEP.CM contains:

```
-NS -NK
C: D:
-P=SWEEP.LOG
```

is equivalent to

```
OSWEEP -NS -NK C: D: -P=SWEEP.LOG E:
```

Command files compared with .ARE files

Both .ARE files and command files can contain the symbols '<' (exclusion), '>' (subdirectory recursion) and '|' (logical sector specification.

.ARE files contain exactly one item per line; command files can contain any reasonable number.

Command files can contain qualifiers (-NS, -NK etc.); .ARE files cannot.

.ARE files can contain specifications containing spaces, e.g. +80 0 0 1, 'All executables', and comments; command files cannot.

-? Help

SWEEP will display all command line qualifiers and a short description of their function.

-6 62 seconds

The 62 seconds time stamp is used as a signature by several viruses. It is also used by several backup programs, **which can result in false alarms**. SWEEP does not check for this identity by default, but can be made to, by using the command line qualifier '-6'.

-A Append report

By default, any security report written to a file by SWEEP will be overwritten by a subsequent report written to a file of the same name. Specifying the -A qualifier in the command line, e.g.

```
OSWEEP -A -P=FOO.REP
```

directs SWEEP to append the new report to the old file FOO.REP, rather than overwriting the old report with the new one.

If this is used in an automatic process, this file should be pruned from time to time to stop it taking up ever more disk space, especially if the -NS command line qualifier is used.

-AD=<drive> Area file default

Any files or areas listed in the SWEEP.ARE file are assumed to be in the specified drive, unless they have an explicitly stated drive.

For example

```
OSWEEP -AD=X
```

would assume that all areas refer to drive X.

-AF=<filename>Area file

The default area file is called SWEEP.ARE. The -AF qualifier can be used to specify a different name.

See also the 'Specifying items to be checked in SWEEP.ARE' section above.

-ALL Sweep all files

In order to sweep all files on a disk instead of just the executable files, specify the -ALL command line qualifier. This is equivalent to creating a SWEEP.ARE file which contains

```
\>*.*
```

It thus specifies a recursive search of all files (rather than just executable files) from the root directory of the current drive.

For example

```
OSWEEP A: -ALL
```

will recursively sweep all files on drive A:.

Note: This is a slow process which can cause false positives.

-AS Sweep standard areas

If an area to be swept is specified in the command line, SWEEP will not check standard areas (master boot sector, OS/2 boot sector etc.). With the -AS command line qualifier, standard areas will be checked as well.

For example

```
OSWEEP SUSPFILE.EXE -AS
```

will sweep SUSPFILE.EXE as well as the standard areas.

-CI Check integrity

This qualifier causes SWEEP to check the integrity of OSWEEP.EXE before executing. A change in the contents of OSWEEP.EXE may indicate the presence of a virus or some other form of data corruption.

-D=<day|percentage> Day or Percentage

SWEEP may be incorporated into the STARTUP.CMD file; however it may not be desirable to perform the system check every time the computer is switched on. The -D qualifier allows you to specify either the probability with which SWEEP will actually proceed to check the system, or the day of the week on which the system should be checked.

For example

```
OSWEEP -D=MONDAY
```

will only run SWEEP when invoked on a Monday. The day of the week can be abbreviated to a minimum of two letters, eg. MO for Monday, TU for Tuesday and so on.

Alternatively

```
OSWEEP -D=20
```

will make SWEEP check the system on average 20 times out of every 100 times that SWEEP is invoked. The number specified must be an integer between 0 and 100.

Note: See also the -DE command line qualifier.

-DA Display areas

This command line qualifier will list all areas to be checked by SWEEP, but will not actually check them.

-DIB

Use the -DIB qualifier to disinfect only boot sectors.

-DID

Use the -DID qualifier to disinfect only documents.

-DE Daily execution

This command line qualifier will check whether SWEEP has already been executed that day and if it has, it will not be executed again.

The file SWEEP.DAY is created on the current drive and directory.

A different file can be specified by including '=filename' after the -DE command line qualifier.

For example

```
OSWEEP -DE=SWEEP.DA1
```

-DI Disinfect

This command line qualifier enables SWEEP to perform automatic disinfection of some boot sector viruses and some macro viruses. If using it, always make sure that SWEEP is being used after having booted from a clean, write-protected system disk.

Important! Note that virus disinfection will not work if the boot sector has already been disabled by using the -REMOVE command line qualifier.

See the 'Treating viral infection' chapter.

-DL Display library

This command line qualifier will display the names of all viruses to be searched for by SWEEP, but not actually check them.

The file VIRPATS.LST on the SWEEP disk contains descriptions of viruses detected by SWEEP. You can PRINT it using the command

```
PRINT VIRPATS.LST
```

-DN Display names of files as they are scanned

This will display files being checked. The display consists of the time followed by the item being checked.

-EX=<extensions> Executable extensions

The extensions of files that SWEEP normally treats as executables can be changed with the -EX command line qualifier. See the 'What will SWEEP check?' section of the 'Using SWEEP' chapter for the default list of file extensions.

For example

```
OSWEEP -EX=EX1,EX2
```

will replace the list of extensions with the EX1 and EX2 file types.

-F Full SWEEP

By default, SWEEP checks only those parts of files likely to contain viruses. A 'full' sweep examines the complete contents of each file and can be specified by using this command line qualifier. Note that a 'full sweep' is much slower than a 'quick sweep'.

See also the 'Full sweep' section.

-FM Specify message file

SWEEP will output the contents of the file specified with -FM=MESSAGEFILE to the screen if it discovers one or more viruses and the file MESSAGEFILE exists. This facility can be used to customise virus recovery procedures. The default file name of MESSAGEFILE is SWEEP.MSG.

For example

```
OSWEEP -FM=MY_MSG.TXT
```

specifies the file 'MY_MSG.TXT'.

-FS File server

Use the -FS command line qualifier if using SWEEP to check a file server over a network. This qualifier prevents checking of the boot sectors (which most networks do not allow).

See also the 'Checking file servers' section of the 'Using SWEEP' chapter.

-ICI InterCheck INI file

When SWEEP is used as an InterCheck Server, this command line qualifier can specify a different initialisation file from the default SWEEPIC.INI.

For example

```
OSWEEP -ICI=SECOND.INI
```

would specify SECOND.INI as the initialisation file.

-ICS [=<servername>] InterCheck Server mode

This command line qualifier places SWEEP into the InterCheck Server mode. The name of the server is optional.

For example

```
OSWEEP -ICS=Server_1
```

would start SWEEP in InterCheck server mode with a server called Server_1.

-MU Check multiple disks

Hint: This command line qualifier allows the user to check a succession of disks in a drive without reloading SWEEP.EXE every time.

For example, to check multiple disks in drive A: type

```
OSWEEP -MU A:
```

When prompted, insert a disk in drive A: and press any key to start checking it. Once that disk has been checked, insert another disk into drive A: when prompted, and press any key to start checking. This will continue until *Esc* is pressed to interrupt the checking, or SWEEP detects one or more viruses.

-NAF Do not read file with areas to be checked

By default, SWEEP will try to open the file SWEEP.ARE and read from it the names of any areas to be checked. Use this qualifier if SWEEP is not required to check the areas defined in SWEEP.ARE.

-NAP Do not use internal virus patterns

By default, SWEEP will check for virus patterns built in by Sophos. With this qualifier it will not use these patterns. The only patterns then detected will be those in SWEEP.PAT and on the command line. SWEEP will still search for virus identities.

SWEEP looks for patterns only when performing a full sweep, which is specified by the -F qualifier.

For example

```
OSWEEP -NAP -F
```

-NAS Do not check standard areas

By default, SWEEP will check standard areas defined at compile time. Use this qualifier to prevent these areas from being checked (for example, if the areas to be checked have been specified in SWEEP.ARE).

Note: SWEEP.ARE must reside on the current drive and in the current subdirectory.

-NB No bell

When SWEEP discovers a virus fragment or a virus, it sounds a bell. This can be disabled using the -NB command line qualifier.

-NCI Do not check identities

SWEEP normally searches for identities. This can be disabled using the -NCI command line qualifier.

-NE Do not use the emulator

SWEEP finds various polymorphic viruses by emulating the environment in which the virus code would normally execute, thereby making the virus decrypt and reveal itself. Disabling this emulator will speed SWEEP up, but may result in some polymorphic viruses not being found.

-NI No interrupting

Execution of SWEEP can normally be interrupted by pressing *Esc* or *Ctrl-Break*. If this command line qualifier is used, execution cannot be interrupted.

-NK No key to continue

If SWEEP discovers one or more viruses or virus fragments, it pauses at the end of the security report and asks for a key to be pressed before continuing. To skip this, use the command line qualifier option -NK.

-NOC No confirmation before virus removal

SWEEP will not ask for confirmation before deleting an infected file or disabling an infected boot sector, if this command line qualifier is used.

This qualifier has no effect unless -REMOVE is also specified.

Warning! Use this qualifier with care!

For example

```
OSWEEP -REMOVE -NOC
```

-NP Do not display full pathname

If SWEEP has been set to display the names of the areas which are checked, it will normally display the full path of the files it checks (see the -NS qualifier). Using the -NP qualifier will mean that SWEEP will only record the names of the files it checks instead.

Note: This will also affect the information placed in the security report created by the -P option.

-NS Not silent

By default, SWEEP does not display the names of areas which are checked. Using this command line qualifier will cause each area to be displayed as it is checked.

-NTW No Temp Warning

SWEEP will perform a check to ensure that the TEMP or TMP environment variable specifies a valid path to which SWEEP can write temporary files. A warning will be issued if this check fails. The -NTW option disables this check.

-P[=<file | device>] Print security report

This command line qualifier directs SWEEP to produce a report of the areas checked. SWEEP outputs this report to the device PRN, if the qualifier is used as -P (not followed by =).

Alternatively, the report can be directed to a particular file or device using the qualifier as -P=.

For example

```
OSWEEP -P=SEC.DOC
```

directs SWEEP to write its security report to the file SEC.DOC.

-PAT=<Hex> Pattern specification

Patterns can be specified in the command line using this qualifier. This may be useful in order to check for a particular pattern as a 'one-off'. The pattern must be specified as a string of hexadecimal digits without any blanks as separators and can be up to 24 bytes (48 hexadecimal characters) long. If found, such patterns are reported as 'Command line 1' etc.

SWEEP looks for patterns only when performing a 'full sweep', which is specified by the -F qualifier.

For example

```
OSWEEP -F -PAT=23f78172bca918e1
```

-PD Pause on discovery of a match

SWEEP will pause whenever it discovers a matching pattern and wait for a keystroke before continuing, if this command line qualifier is used.

Note: If -WC is specified at the same time, SWEEP will pause whenever it discovers a compressed file and will wait for a keystroke before continuing. See the -WC command line qualifier for further details.

-PR Priority

By default, SWEEP runs with the priority of any other standard OS/2 task such as a word processor. This qualifier can be used to increase or decrease this priority:

```
OSWEEP -PR=H
```

specifies high priority, while

```
OSWEEP -PR=L
```

specifies low priority.

High priority is a little below that of real-time tasks, while low priority is equivalent to idle-time priority.

-Q Quick sweep

By default, SWEEP will perform a 'quick sweep'. This qualifier is only necessary after the default mode is switched off. This might have been done, for example, in a batch file or in a file specified by @file.

-REC Recursive search

This command line qualifier directs SWEEP to search directories below the ones specified in the command line.

For example

```
OSWEEP C:\*.DLL C:\SIMULATI\*.SYM -REC
```

will search all .DLL files on the disk starting from the root directory (\) as well as all .SYM files from the \SIMULATI directory downwards.

-REMOVE Remove viruses on discovery

This qualifier directs SWEEP to delete any infected files and disable any infected boot sectors.

The -RS command line qualifier can be used in conjunction with -REMOVE to ensure that the file is positively overwritten rather than simply deleted.

Confirmation will be requested before any item is deleted or disabled unless the -NOC qualifier is also used.

Disabling of boot sectors is done by substituting the first two bytes pointed to by the initial JMP instruction with a JMP-to-itself instruction. Note that after disabling a boot sector, the virus fragment may still be there, but the virus will be totally inactive.

For example

```
OSWEEP -REMOVE -RS -NOC
```

See the 'Virus disinfection and removal' section.

-REMOVEF Remove infected files

As -REMOVE, except that infected boot sectors are not disabled. For example

```
OSWEEP -REMOVEF
```

This is especially useful if it is inconvenient to boot OS/2 from floppy disk.

See the 'Virus disinfection and removal' section.

-RS Remove viruses by positively overwriting them

SWEEP will remove any infected files by positively overwriting them instead of just deleting them, if this command line qualifier is used.

Disabling of boot sectors is not affected.

-RS has no effect unless -REMOVE or -REMOVEF is also specified.

For example

```
OSWEEP -REMOVE -RS
```

Note: Files overwritten when this option is used canot be recovered.

See the 'Virus disinfection and removal' section.

-S Silent running without displaying checked areas

By default, SWEEP does not display on the screen the areas it is checking. The qualifier -S is equivalent to this default mode, and is the opposite of the -NS qualifier.

-SC Scan inside compressed files

SWEEP looks for viruses inside files compressed by using dynamic compression utilities PKLite, LZEXE and Diet if this command line qualifier is used.

-SS Super silent running

SWEEP will not display anything (not even the copyright message) unless a virus is found, if this command line qualifier is used.

-WC Warn if compressed files are encountered

SWEEP cannot currently find viruses in files which have been modified in any way from the original. This includes files in ZIP, ARC, ZOO and other static compression formats.

However, SWEEP is capable of looking for viruses inside files compressed using the dynamic compression utilities PKLite, LZEXE and Diet (use the -SC command line qualifier).

Using -WC will cause SWEEP to warn if any compressed files are found on the disk.

Note: Files created by 'disk doublers' such as Stacker can be swept without the use of the -WC qualifier, provided that the 'disk doubler' is running.

If the -PD qualifier is specified at the same time as -WC, SWEEP will pause when it finds a compressed file and will wait for a keystroke before continuing.

For example

```
OSWEEP A: -WC -PD
```

Installing the InterCheck server

This chapter describes how to install SWEEP as an InterCheck server in order to handle requests for on-access scanning from workstations.

Information on **using the InterCheck server** can be found in the 'Controlling the InterCheck server' chapter.

Information on **installing the InterCheck clients**, which allow workstations to send files to the server for scanning, can be found in the 'Installing InterCheck clients' chapter.

Software required for InterCheck

The following software components from Sophos are required to make up the InterCheck software system:

- SWEEP for OS/2 (`\OS_2\*.*`).
- SWEEP for DOS (`\DOS\ENG\*.*`).
- InterCheck for DOS, Windows, Windows 95 (`\INTERCHK\*.*`).
- ICONTROL (`\TOOLS\ICONTROL\*.*`).

Users with the Sophos Anti-Virus CD can find these items in the paths indicated.

Users with Sophos Anti-Virus on floppy disk will have disks containing each of these items.

About InterCheck server installation

This section describes installation of the InterCheck software on an IBM LAN Server network.

Installation is described in terms of command line commands to LAN Server, because these are applicable to all versions of the LAN Server product. Equivalent commands may be issued through the LAN Server Administration program, where it exists. However, these operations vary considerably from one version of LAN server to another, so this approach is not described in detail here.

Both Basic and Advanced versions of IBM LAN Server are supported. HPFS386 is supported, with or without Local Security on the server.

InterCheck and Peer Servers

The OS/2 InterCheck Server is designed to be installed on file servers configured as members of domains. It can also be installed on Peer Servers, provided that the Peer Server is either OS/2 Warp Connect or OS/2 Warp Version 4. In this case, InterCheck will support a 'workgroup'. Reduced performance will be obtained from InterCheck installed on a Peer Server, compared with that given by a full file server belonging to a domain.

Summary of the installation procedure

The installation procedure is summarized below, and then explained in detail on the following pages.

1. Log in with Administrator privileges to the file server which will host the InterCheck Server.

2. Create directories on the server:

SWEEP	for SWEEP for OS/2, InterCheck Server and ICONTROL.
INTERCHK	for the InterCheck client and SWEEP for DOS.

3. Copy the ICONTROL and SWEEP for OS/2 files to the SWEEP directory.
4. Copy the SWEEP for DOS and the InterCheck files to the INTERCHK directory.
5. Create subdirectories

   ```
   INTERCHK\COMMS
   INTERCHK\LISTS
   INTERCHK\INFECTED
   ```

6. Using the User Profile Manager, create a group ICUSERS. Add all users who are to run InterCheck clients to this group.
7. Create an alias ICHK for the INTERCHK directory.
8. Grant access rights to the directories created in steps 2 and 5.
9. Create a login script. Arrange for all members of the group ICUSERS to run it.
10. (Optionally) create a desktop icon for ICONTROL.
11. Configure the InterCheck client and server software. This creates an initial configuration sufficient to start the InterCheck software and to test client-server communications.
12. Alter STARTUP.CMD to run SWEEP for OS/2 in InterCheck Server mode. (If Local Security is enabled on the file server, the file PRIVINIT.CMD will be altered instead of STARTUP.CMD).

Procedure for installing the InterCheck server

1. Log in to the InterCheck server host

The InterCheck server may be hosted by any file server on the domain. It is necessary to log in with full administrator privileges.

2. Create directories on the server

The exact locations and names of the master directories are unimportant. They do not even have to be on the same drive. For simplicity, these instructions suppose that the master directories are created in the root directory of drive I: on the server. This drive I: can use any file system (FAT or HPFS).

Create the directories:

```
MD I:\SWEEP
MD I:\INTERCHK
```

If there is already a directory for SWEEP for OS/2, this can be used wherever I:\SWEEP is specified in these instructions.

3. Copy the ICONTROL and SWEEP for OS/2 files

Users with the Sophos Anti-Virus CD should enter:

```
I:
CD\SWEEP
COPY H:\TOOLS\ICONTROL\*.*
COPY H:\OS_2\*.*
```

where H: is the CD drive.

Users with Sophos Anti-Virus floppy disks should mount the ICONTROL floppy disk in drive A:. and type

```
I:
CD \SWEEP
COPY A:*.*
```

Mount the SWEEP for OS/2 floppy disk in drive A: and type

```
COPY A:*.*
```

Important! In future, always copy the monthly SWEEP for OS/2 updates into this directory I:\SWEEP.

4. Copy the SWEEP for DOS and InterCheck files

Users with the Sophos Anti-Virus CD should enter

```
I:
CD\INTERCHK
COPY H:\DOS\ENG\*.*
COPY H:\INTERCHK\*.*
```

where H: is the CD drive.

Users with Sophos Anti-Virus floppy disks should mount the SWEEP for DOS floppy disk in drive A: and type:

```
I:
CD \INTERCHK
COPY A:*.*
```

Mount the InterCheck floppy disk in drive A: and type

```
COPY A:*.*
```

Important! In future, always copy the monthly SWEEP for DOS updates into this directory I:\INTERCHK.

5. Create required subdirectories

Type

```
MD COMMS
MD LISTS
MD INFECTED
```

6. Create and populate a group ICUSERS

A group ICUSERS must be created and populated with all the users who are to run the InterCheck client software. Another name can be used instead of ICUSERS if desired. This group is needed so that access rights for the InterCheck directories can be assigned to it. It may be desirable for privileged users running the DOS or Windows LAN clients not to be

forced to run the InterCheck client, in case the client software interferes with critical management operations when the InterCheck server is not running. Normally, though, the group ICUSERS should include the group USERS.

Note: It is permissible to use the group USERS instead of creating a group ICUSERS. In this case, this step may be omitted, and the group USERS may be used instead of ICUSERS in step 8.

The group ICUSERS can be created and populated in the usual way using the IBM LAN Server User Profile Management tool. Alternatively, commands may be used, for example

```
NET GROUP /ADD ICUSERS /COMMENT:"InterCheck Users"
NET GROUP /ADD ICUSERS user1
```

7. Create an alias for access to the INTERCHK directory

Type

```
NET ALIAS ICHK \\SERVER I:\INTERCHK /WHEN:STARTUP /UNLIMITED
```

where SERVER is the name of the server where InterCheck is being installed. Another alias name may be used instead of ICHK if desired.

8. Grant access rights to directories

Type

```
NET ACCESS I:\INTERCHK /ADD ICUSERS:R
NET ACCESS I:\INTERCHK\COMMS /ADD ICUSERS:RWC
NET ACCESS I:\INTERCHK\LISTS /ADD ICUSERS:Y
```

The directory I:\INTERCHK\INFECTED should be accessible only by administrators, since it can contain virus-infected files detected by the InterCheck server.

Access to the directory I:\SWEEP by clients is not required for the operation of InterCheck. Its access rights are at the discretion of the network administrator.

9. Create a login script

See the instructions for creating login scripts in the 'Installing networked InterCheck clients' section of the 'Installing InterCheck clients' chapter.

10a. Create a desktop icon for ICW

If WIN-OS/2 is installed, perform this step and omit step 10b.

ICW is a Windows program which can be run in an Enhanced Compatibility Mode WIN-OS/2 session. The recommended ways to create an item to run ICW are described here.

Open the OS/2 System folder on the Desktop, and open the Templates folder within it. Drag an object from the Program template to the Desktop. Fill in the settings fields thus:

Path and file name: I:\SWEEP\ICONTROL.EXE
Parameters: (Leave blank)
Working directory: I:\SWEEP

Move to the Session settings page, and set the WIN-OS/2 full screen, WIN-OS/2 window and Separate session attributes according to your preference. Press the *WIN-OS/2 settings* button, select *WIN-OS/2 settings* and press *OK*. Ensure that the WIN_RUN_MODE setting is selected, then select 3.1 Enhanced Compatibility. Press the *Save* button at the bottom of the window. Move to the General settings page and give the object a title such as 'InterCheck Sever Controller'.

10b. Create a desktop icon for ICONTROL

If WIN-OS/2 is not installed, perform this step instead of 10a.

ICONTROL is a DOS program which can be run in a DOS session. The recommended way to create an icon to run ICONTROL is described here.

Open the OS/2 System folder on the Desktop, and open the Templates folder within it. Drag an object from the Program template to the Desktop. Fill in the settings fields thus:

Path and file name: I:\SWEEP\ICONTROL.EXE
Parameters: (leave blank)
Working directory: I:\SWEEP

The session type may be DOS Full Screen or DOS Window according to your preference. Finally the program Title (in the General settings page) should be set to 'InterCheck Server Controller' or some similar description.

You may now close the settings notebook for ICONTROL and the Templates and OS/2 System folders.

11. Configure the InterCheck client and server

InterCheck Client

The InterCheck client software is configured by the file I:\INTERCHK\INTERCHK.CFG which must be created. The first version of this file should contain the following two lines:

```
[InterCheckGlobal]
Exclude=CONFIG.SYS
```

You can add further lines at any time as described in the 'Configuring InterCheck clients' chapter.

Note that INTERCHK.CFG configures the operation of all InterCheck clients. Therefore altering it is a task for network administrators, not users.

InterCheck Server

The InterCheck server software is configured by the file I:\SWEEP\SWEEPIC.INI which is created and maintained by the ICW or ICONTROL programs.

ICONTROL and ICW are functionally equivalent: ICW runs under Windows or WIN-OS/2, and ICONTROL runs under DOS. Because not all OS/2 servers are configured with WIN-OS/2, this setup step will be carried out with ICONTROL.

ICONTROL runs in a DOS session, which may be either windowed or full-screen. To start the program, type at a DOS command prompt

```
I:
CD \SWEEP
ICONTROL
```

The program will check the configuration and then display its main screen. An error box may appear on the main screen: if it does, press the *Esc* key.

At this stage, the IC Server option in the main menu bar should be highlighted. Press the *Enter* key. A menu will appear showing various options including List and Exit. Type L to select List. A small box will appear showing a path. Press the *Enter* key.

Now a larger box will appear with the title:

```
IC server drive/dir:
```

Enter into this box the path where the InterCheck client software was installed, e.g.

```
I:\SWEEP
```

and press the *Enter* key. Press the *Esc* key to exit from the small box. Type X to exit from ICONTROL.

A box will appear with the title

```
Save changes before exiting?
```

and the YES choice should be highlighted. Press the *Enter* key to exit from ICONTROL. At this point the file I:\SWEEP\SWEEPIC.INI will be written by ICONTROL. However, the information in it is not yet complete.

Now start ICONTROL again. Type the letter O to obtain the Options menu, then E to select Edit, then D to select Directory. At this point you will have a sub-menu with the items Infected and Comms.

First type I to select Infected, then enter the path

```
I:\INTERCHK\INFECTED
```

of the directory INFECTED created at step 5. Press the *Enter* key to enter the path. Then type C to select Comms, then enter the path

```
I:\INTERCHK\COMMS
```

of the COMMS directory created at step 5. Press the *Enter* key to enter the path. Now press the *Esc* key three times to dismiss the menus.

You have now finished creating the initial version of the SWEEPIC.INI file. You can either leave ICONTROL running for later operations, or exit from it by pressing the *Esc* key, then the *Enter* key.

Further information on the use of the ICONTROL program may be found in the 'Controlling the InterCheck Server' chapter.

12. Place InterCheck server startup in system startup command file

The configurations in step 11 **must** be completed before carrying out this step.

The InterCheck server program is the same program OSWEEP.EXE that is used for normal checking of file systems. However, it is started with a special command line.

It is necessary to start this program each time the server machine is booted. This is most easily done by placing the InterCheck server startup command in the system startup command file.

However, in order to test the InterCheck installation, the InterCheck server may be started by issuing the command

```
I:\SWEEP\OSWEEP -ICS
```

from the administrator session in which steps 1-11 were carried out. When the tests are satisfactory, the startup command file can be edited.

For an IBM LAN server running the **Basic LAN Server**, and for an **Advanced LAN Server where Local Security is not enabled**, the file where this command is to be inserted is STARTUP.CMD located in the root directory of the OS/2 boot drive. The recommended command is

```
START I:\SWEEP\OSWEEP -ICS
```

For an IBM LAN server running the **Advanced LAN Server with Local Security enabled**, the file where the command is to be inserted is PRIVINIT.CMD located in the root directory of the OS/2 boot drive. The recommended command is

```
START PRIV I:\SWEEP\OSWEEP -ICS
```

Further information on automatic startup can be found in the IBM LAN Server Network Administrator Reference manual.

Note: The InterCheck server can **not** be started from a RUN= command in the CONFIG.SYS file, because it displays status information on the screen.

Configuring the InterCheck server

This is performed with ICW or ICONTROL, as described in the ‘Controlling the InterCheck server’ chapter.

Updating SWEEP used as an InterCheck server

Registered users of SWEEP are sent updates in the first week of every month, or can download updated versions from the Sophos Web site.

If updating SWEEP for OS/2 on a server with Local Security installed, log in as an Adminstrator first.

Make sure SWEEP is not running in any session. If the OS/2 server is running, stop it by selecting its window and typing *Esc*. Then copy the contents of the OS_2 folder on the Sophos Anti-Virus CD into the SWEEP directory. Restart the InterCheck server.

Update SWEEP for DOS on the server after updating SWEEP for OS/2, e.g. by copying the contents of the \DOS\ENG folder on the Sophos Anti-Virus CD into the INTERCHK directory.

Do not forget to update SWEEP on any stand-alone PCs which are not connected to the network.

When the InterCheck client detects a new version of SWEEP, it will automatically scan the workstation, which will take a few minutes.

Note: The InterCheck client TSR does not require updating.

Make sure that the two executables (SWEEP.NLM and SWEEP.EXE) are suitably protected against modification by normal users.

Urgent SWEEP updates

See ‘Urgent SWEEP updates’ in the ‘Installing SWEEP’ chapter for details. Note that the OS/2 InterCheck server must be stopped and restarted when making urgent updates.

Installing InterCheck clients

This chapter describes how to install and run InterCheck clients.

Note: For the installation of stand-alone Windows 95 and Windows NT InterCheck clients, see the Sophos Anti-Virus manual for Windows 95 or Windows NT.

Which kind of InterCheck client?

There are two kinds of InterCheck clients: networked and stand-alone (see the 'About InterCheck' chapter).

Networked InterCheck clients

Networked InterCheck clients require a remote InterCheck server, and communicate with it over the network. They can be easier to install and administer, and use less disk space and fewer system resources, than stand-alone InterCheck clients.

This option is available for DOS, Windows 95, Windows 3.x and Macintosh workstations. See 'Installing networked InterCheck clients' below.

Stand-alone InterCheck clients

Stand-alone InterCheck clients do not require a remote InterCheck server, and use a local installation of SWEEP for virus checking. They offer faster initial authorisation of files, create less network traffic, and can also be used on stand-alone workstations or workstations not always connected to the network.

This option is available for Windows NT, Windows 95 and DOS/Windows 3.x. See the 'Installing stand-alone InterCheck clients' section below.

Installing networked InterCheck clients

This section describes the installation of networked InterCheck clients in an IBM LAN Server network. Before installation:

1. **Install SWEEP and InterCheck on the file server.**

   This is described in the 'Installing the InterCheck server' chapter.

2. **Decide whether to run InterCheck with a login script or without.**

   If the client workstation has a login script, this can be used to run the InterCheck executable from the SWEEP directory on the file server. This is the easiest way to install and run a networked InterCheck client. See the 'With a login script' subsection for the relevant operating system.

   If the workstation does not have a login script, or if the user wants to start InterCheck at any time after it has logged in to the network, the InterCheck executable can be run without a login script. See the 'Without a login script' subsection for the relevant operating system.

3. **Inform users that InterCheck is being installed.**

   When users next log in to the network after the InterCheck client has been installed, SWEEP will be run to check the programs on their workstation. This may take a few minutes, but it only happens once and reduces subsequent levels of client-server communication. InterCheck can be configured to achieve a balance between 'start-up' and 'run-time' sweep times (see the 'Configuring InterCheck clients' chapter).

Now consult the following instructions for the relevant operating system.

Networked InterCheck clients for DOS

This section assumes that the IBM LAN Server network client for DOS (IBM DOS Lan Requester or IBM DOS LAN Services) has been installed on the DOS workstations.

With a login script

Each user who will run an InterCheck client should have a drive assignment to the InterCheck alias set in their login profile. Using the same example names as those used in the 'Installing the InterCheck Server' chapter, this assignment will assign drive I: to the alias ICHK.

Each user should have a login script containing the command

```
I:\ICLOGIN
```

Note: If the IBM DOS network client will not restore network connections automatically when the user logs in, the following shortcut may be used:

Instead of assigning the drive I: in the user's login profile, insert the following two lines in the user's login script:

```
NET USE I: ICHK
I:\ICLOGIN
```

These lines may be placed in a single common command file which is referenced by CALL commands in the users' login scripts.

Without a login script

Each user should execute the commands below, either manually or in their AUTOEXEC.BAT startup

command file, after starting the IBM client software and logging in:

```
NET USE I: ICHK
I:\INTERCHK
```

Networked InterCheck clients for Windows 95

This section assumes that the IBM LAN Server network client for Windows 95 has been installed on the Windows 95 workstations.

Each user who will run an InterCheck client should have a drive assignment to the InterCheck alias set in their login profile. Using the example names used in the 'Installing the InterCheck Server' chapter, this assignment will assign drive I: to the alias ICHK.

With a login script

Each user should have a login script containing the command

```
I:\ICWIN95
```

Without a login script

Each user should execute the following command, either manually or automatically from the Windows 95 Startup folder.

```
I:\ICWIN95
```

Networked InterCheck clients for Windows 3.x

This section assumes that the IBM LAN Server network client for Windows 3.x has been installed on the Windows workstations.

Note: Networked InterCheck clients for Windows 3.x cannot be installed without a login script.

The installation procedure depends on whether users log in under DOS, before Windows has started, or under Windows.

Users log in before starting Windows

If users log in under DOS, before Windows has started, see the 'Networked InterCheck clients for DOS' section above.

Users log in after starting Windows

If users log in under Windows, two kinds of installation are possible:

1. An OS/2 InterCheck server on a remote machine is used for scanning and virus reporting. Follow the instructions below in full.
2. Scanning is carried out by copies of SWEEP on each workstation, but viruses are reported over the network to the OS/2 InterCheck server. Follow the instructions below, but omit stage 2.

Each user who will run an InterCheck client should have a drive assignment to the InterCheck alias set in their login profile. Using the example names used in the 'Installing the InterCheck Server' chapter, this assignment will assign drive I: to the alias ICHK.

Each user should have a login script containing the command

```
I:\INTERCHK
```

Stage 1

Log in under DOS as a user who does not run a login script (e.g. an administrator) and type

```
NET USE I: ICHK
I:
ICINSTAL
```

A windowed display will appear.

If you have more than one hard disk, select the desired drive from the *Where* menu.

Set the COMMS directory by selecting *Communications directory* from the *Options* menu. Enter

```
I:\COMMS
```

and type <Return> to enter this information.

To start the installation, select *Onto hard disk* from the *Install* menu and follow the instructions. Then exit from the program.

Stage 2

Edit the file `\INTERCHK\INTERCHK.CFG` on the workstation to delete the line

```
SWEEPVXDLOAD=YES
```

Networked InterCheck clients for Macintosh

The Macintosh InterCheck client is currently only supported by SWEEP for NetWare and SWEEP for Windows NT.

Installing stand-alone InterCheck clients

To install stand-alone InterCheck clients, follow the instructions for the relevant operating system.

Stand-alone InterCheck clients for Windows NT and Windows 95

These are installed as part of the SWEEP installation process. See the 'Installing SWEEP' chapter of the Sophos Anti-Virus user manuals for Windows NT and Windows 95 respectively.

Stand-alone InterCheck clients for DOS/Windows 3.x

Note: When InterCheck first installs, the whole disk is scanned. This can take several minutes, depending on the size of the disk.

Clients with network access

The installation procedure depends on whether the user logs in after starting Windows, or before.

User logs in after starting Windows

Follow the instructions in the 'Users log in after starting Windows' subsection of the 'Networked InterCheck clients for Windows 3.x' section, but omit stage 2.

User logs in before starting Windows

Ensure that the directory on the file server that contains the InterCheck files is mapped to a DOS drive. At a DOS prompt on the workstation, change to that drive and enter

```
ICINSTAL
```

If you have more than one hard disk, select the desired drive from the *Where* menu.

To use non-standard installation options, select the *Options* menu. The options correspond to those described in the 'Configuring InterCheck clients' chapter.

To start the installation, select *Onto hard disk* from the *Install* menu and follow the instructions.

Clients with no network access

Insert the Sophos Anti-Virus CD into the CD drive, and enter

```
H:\INTERCHK\ICINSTAL
```

at a DOS prompt, where H: is the CD drive.

Or, if using floppy disks, insert the 'InterCheck' floppy disk into the floppy disk drive and enter

```
A:ICINSTAL
```

at a DOS prompt, where A: is the floppy disk drive.

If you have more than one hard disk, select the desired drive from the *Where* menu.

To use non-standard installation options, select the *Options* menu. These options correspond to those described in the 'Configuring InterCheck clients' chapter.

To start the installation, select *Onto hard disk* from the *Install* menu and follow the instructions.

Testing InterCheck functioning

It is often useful to test the communication link between a client and the server. This can be done very simply by creating a file called TEMP.SYS and entering some random text. Use a text editor such as EDIT under DOS, or Notepad under Windows and Windows 95. InterCheck will interpret this as the creation of an executable type file and will send the file to the server for checking.

Controlling the InterCheck server

This chapter describes how to control SWEEP for OS/2 running as an InterCheck server.

Introduction to ICONTROL

SWEEP running as an InterCheck server provides InterCheck services on any network capable of emulating a logical drive to PCs connected to it.

SWEEP for OS/2 running in InterCheck server mode can be configured and monitored remotely by using ICONTROL for DOS or Windows software. Note that the ICONTROL for DOS program (ICONTROL.EXE) is functionally equivalent to the ICONTROL for Windows program (ICW.EXE).

The ICONTROL programs are copied to the InterCheck server as part of the InterCheck server installation process (see the 'Installing the InterCheck server' chapter).

ICONTROL can be run on a remote machine with a drive mapped to the directory on the server containing ICONTROL, or it can be run on the server itself. Write access to the directory ICONTROL is required if any changes to its configuration are to be made.

ICONTROL for DOS

Starting ICONTROL

If the directory D:\SWEEP contains the InterCheck executables, enter at a DOS prompt

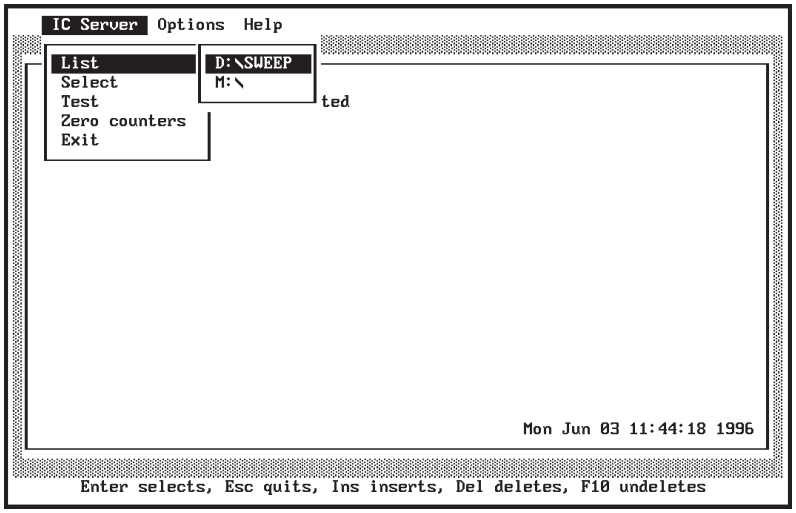
```
D:\SWEEP\ICONTROL
```

to start ICONTROL.

Selecting the InterCheck server

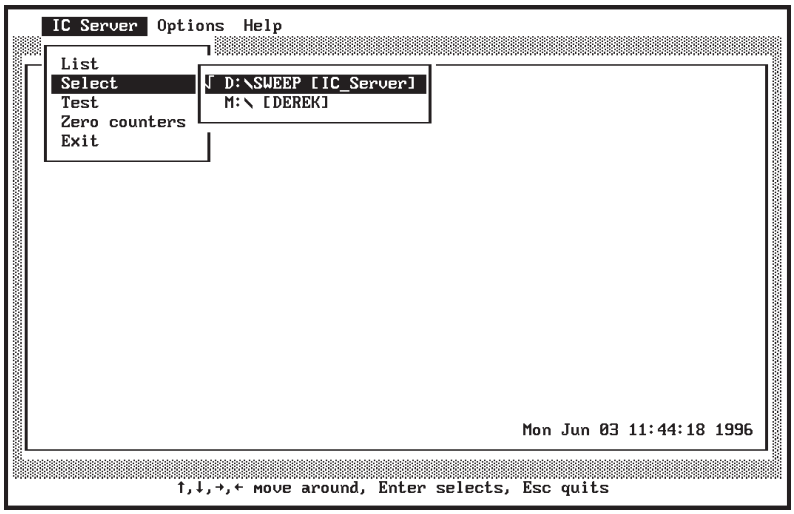
One or more InterCheck server processes can be controlled using ICONTROL under DOS, although only one InterCheck server can be selected and hence monitored at one time.

From the *IC Server* menu select *List* to specify the drive and directory from which SWEEP is running in InterCheck server mode.

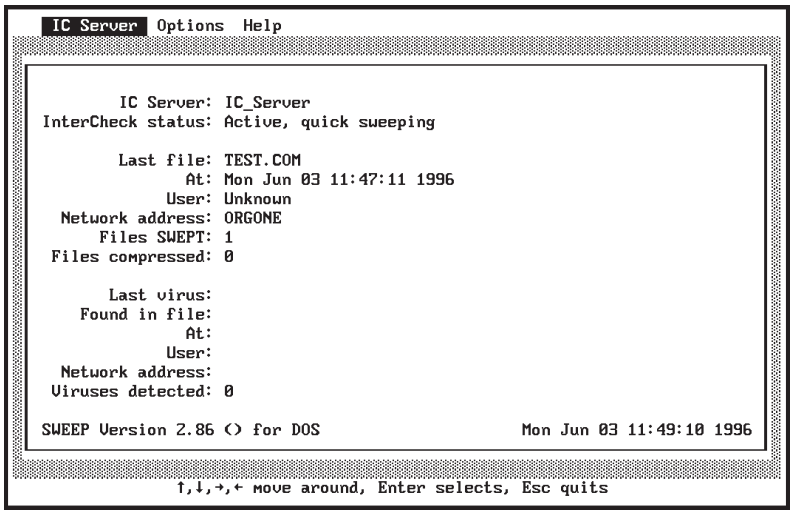


If there is no entry with the correct drive and path, press the *Insert* key and enter the appropriate details, or press *Enter* to edit an existing entry.

The *Select* option from the *IC Server* menu is used to specify the InterCheck server (from the list defined in the *List* option) that is selected for monitoring and controlling.



Assuming that the selected InterCheck server SWEEP is running in InterCheck server mode, and that no menus are 'hanging' off the top bar, ICONTROL will start to monitor SWEEP and update the main ICONTROL display once a server is selected with *Select*.



The main ICONTROL display shows the name of the selected InterCheck server, along with its status (active, inactive or unknown), information about the last file swept, the total number of files swept, the number of compressed files, information about the last virus detected, and the total number of viruses detected.

Testing communications

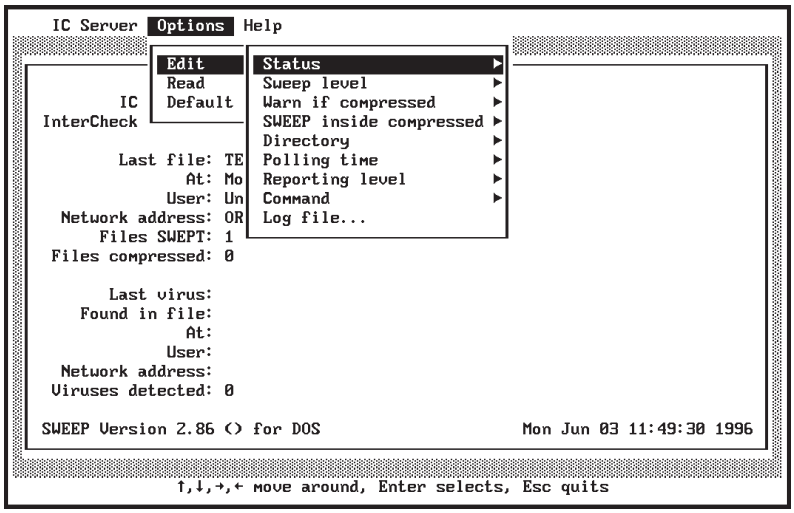
Select *Test* from the *IC Server* menu to test the communication between ICONTROL and the selected InterCheck server. The test server dialog is displayed and updated throughout the process until the outcome is displayed.

The test takes approximately six seconds to complete when the InterCheck server is communicating correctly; otherwise the process will time out after 15 seconds.

Zeroing counters

Select *Zero counters* from the *IC Server* menu to zero the viruses found and files swept counters on the selected InterCheck server.

ICONTROL for DOS options



Edit

Status

The InterCheck server will be able to process requests from InterCheck clients if it is active; otherwise it will not. The server is active by default.

Sweep level

The sweeping level can be set to ‘full sweep’ or ‘quick sweep’. The quick sweep checks only the parts of files likely to contain viruses, while the full sweep examines the full contents of each file. For normal operation quick sweeping is sufficient, and this is the default option.

Warn if compressed

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. SWEEP can warn the user if it encounters any of these files, but by default it does not. InterCheck provides automatic protection from viruses in files which have been compressed, as access to every unrecognised item (e.g. a newly decompressed file) is only granted after that item has been checked for viruses.

SWEEP inside compressed

SWEEP is capable of finding viruses in files which have been compressed using the dynamic compression utilities PKLite, LZEXE and Diet. By default SWEEP will not check inside these compressed files.

Directory

This option allows the location of the INFECTED and COMMS directories on the currently selected InterCheck server to be specified. The COMMS directory is used for communication between InterCheck clients and the server, and the INFECTED directory is used for storing infected items for later analysis.

The locations of these directories are set during the system installation (see the ‘Installing the InterCheck server’ chapter), and it is unlikely that they will have to be changed subsequently.

Polling time

The maximum and minimum polling times are the maximum and minimum times the InterCheck server waits between successive searches of the COMMS directory. Increasing the values will tend to reduce server load slightly, but will increase delays experienced by the InterCheck client software. It is recommended that this option is only used if performance problems are encountered.

Reporting level

This controls the level of detail recorded in the continuous SWEEP log file. The options range from None (the least information) to Verbose (the most).

Command

If an OS/2 InterCheck server is used, a DOS command can be executed when a virus is found, or when the owner of a file has to be determined. Notification can be sent to a user, workstation or group.

The command file may contain other commands at the discretion of the system manager, for example to activate a third party email or paging system to store and forward the notification.

The **'DOS command on virus discovery'** is passed six parameters:

1. Virus name.
2. User name.
3. Time and date of virus discovery.
4. The location of the virus (either a filename or 'Boot_sector').
5. Network Identification Code of the workstation.
6. Name of the server making the report.

Note that all individual parameters have blanks replaced by underscores to allow correct processing by DOS. For example, the 'Dark Avenger' virus would be passed on as 'Dark_Avenger'.

An example of a batch file processing the discovery of a virus might be

```
@ECHO Virus %1 discovered at %3
```

The **'DOS command to get user name'** is passed one parameter in the command line: the full file name.

The appropriate system utility should be used to return the name of the owner of that file, and this name should be written to the file SWEEP.USR in the same directory as the SWEEP InterCheck server.

Note: IBM LAN Server does not provide a mechanism for obtaining the userid of the file owner, so this command is not used for LAN Server networks.

Log file

This option sets the name and location of the continuous SWEEP log file.

Read

This sets the options to those specified in the InterCheck server configuration file, i.e. it restores them to their last saved values.

Default

This sets the options to their default values.

Command line qualifiers

-BW Display in black and white

Forces display for a black and white monitor.

-CFG=<file> Name of configuration file

The default ICONTROL configuration file is called SWEEPIC.INI and is stored in the same directory as ICONTROL. A different path and name can be specified with the -CFG option.

-CO Colour monitor

Forces display for a colour monitor.

-MO Monochrome monitor

Forces display for a monochrome monitor.

-P.. Path through menus

This qualifier can be used to pre-define the selection of menu options. 0 selects the 1st option, 1 the 2nd option etc. '^' is equivalent to the user pressing *Esc* while '?' allows the user to make a selection. In the example

```
ICONTROL -P120^04
```

1 Selects *Options* menu.

2 Selects *Default*.

0 Enters *OK* on 'Initialise options to default values?' dialog.

^ Escapes to the top menu bar.

0 Selects *IC Server* menu.

4 Selects *Exit* to exit from ICONTROL.

ICONTROL for Windows

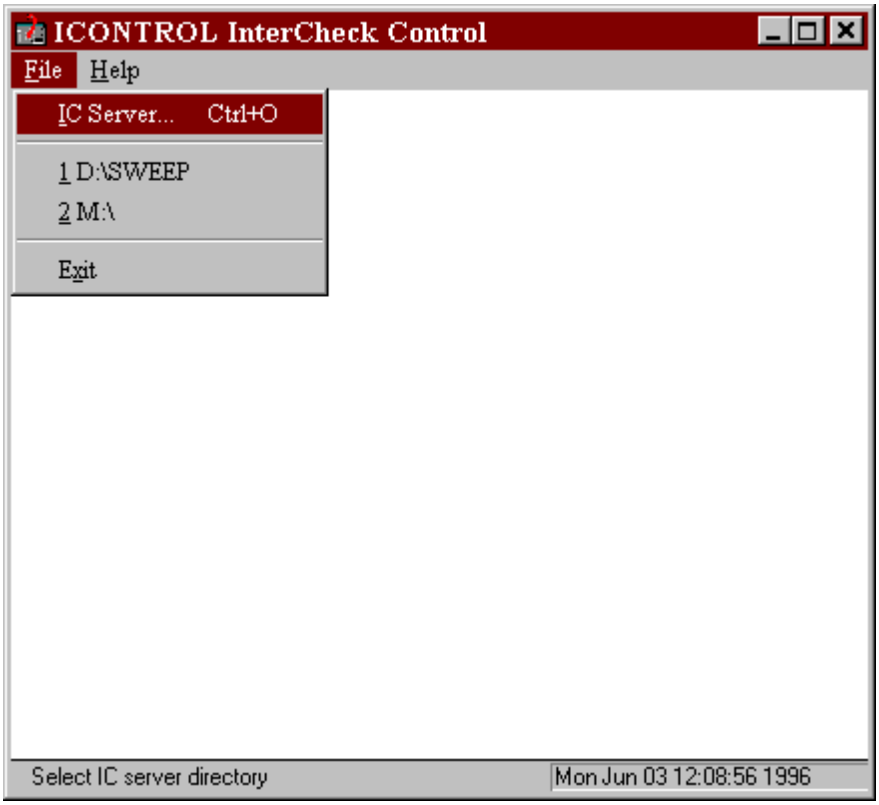
Starting ICONTROL

Use File Manager or Explorer to locate the InterCheck files on the network. Start ICONTROL by double clicking on ICW.EXE.

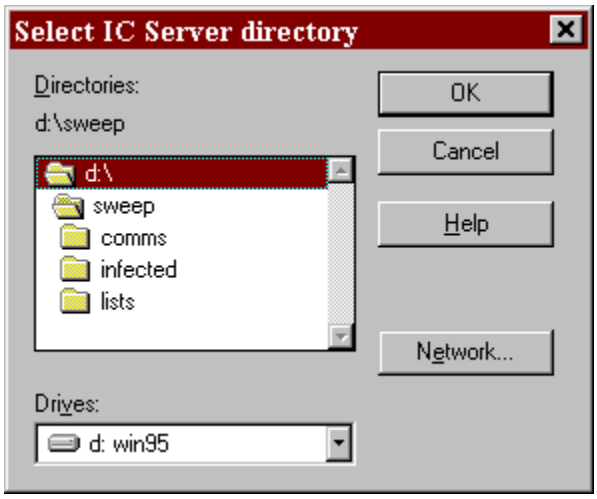
Note that ICW.EXE can be placed in, and launched from, a Windows 3.x Program Group or the Windows 95 Taskbar in the same way as any other Windows executable.

Selecting the InterCheck server

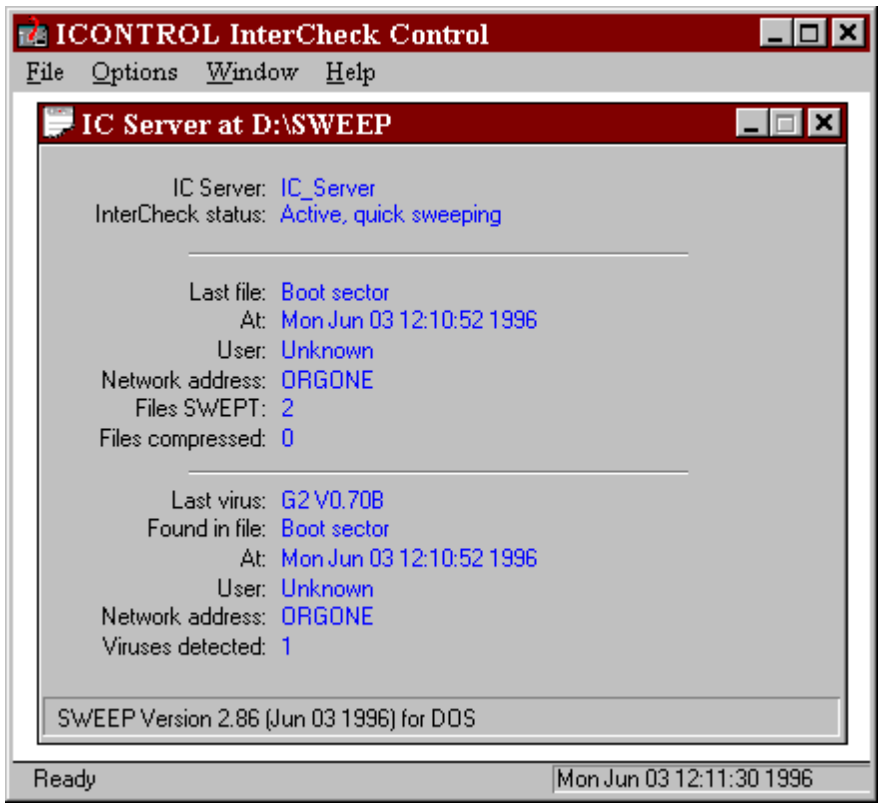
Choose *IC Server* from the *File* menu



and select an InterCheck server working directory



When the directory is specified ICONTROL will display the current status of the InterCheck server that is running at that location, for example:



Other InterCheck servers can be monitored by selecting them via the *File* menu. Unlike ICONTROL

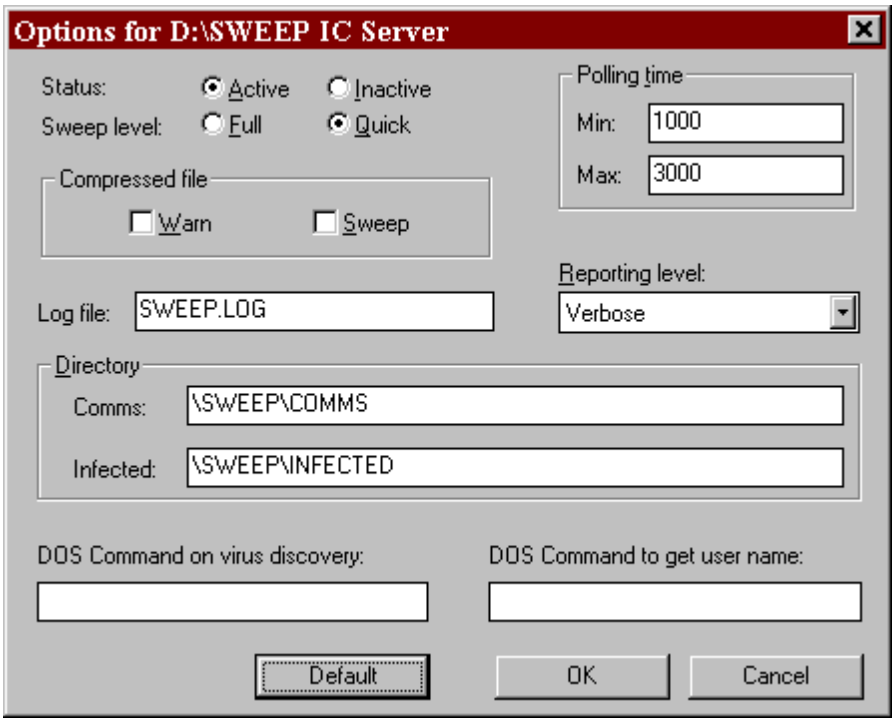
for DOS, ICONTROL for Windows can monitor multiple servers at the same time.

ICONTROL for Windows options

The following options will operate on the InterCheck server whose status window is currently activated / selected.

Edit server settings

You can set parameters such as the minimum and maximum polling times, reporting levels etc. in SWEEP by selecting *Edit server settings* from the *Options* menu:



These parameters are equivalent to those set from the *Options* menu of the DOS ICONTROL (see the 'ICONTROL for DOS options' section above).

Test server

See the ‘Testing communications’ sub-section of ‘ICONTROL for DOS’.

Zero counters

See the ‘Zeroing counters’ sub-section of ‘ICONTROL for DOS’.

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.

DestinationDirectory=<path>

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

```
DestinationDirectory=C:\INTERCHK\COMMS
```

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

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.

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?
```

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 executable 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 (as described in the ‘Installing InterCheck clients’ chapter) 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.

ICLOGIN command line qualifiers

This section describes the command line qualifiers that can be used with ICLOGIN to start the InterCheck client from a login script.

-? Help

Displays the version number.

-A Automatic Windows installation

Initiates the automatic Windows installation.

-U Use UNC

Uses UNC (Universal Naming Convention) when running or installing InterCheck.

Treating viral infection

This chapter describes how to deal with a virus once it has been discovered.

Recovery from a virus attack

Recovery from a virus attack involves two main stages:

1. Elimination of the virus from infected areas.
2. Recovery from any virus side-effects.

Eliminating viruses

SWEEP's automatic disinfection facilities, or OS/2 commands, can deal with many virus attacks:

- **Infected boot sectors** can be disinfected (in some cases) or neutralised.
- **Infected files** can be deleted.
- **Infected documents** can be disinfected.

The sections below explain how to prepare for disinfection and how to deal with each kind of infected item.

Preparing to deal with viral infection

Before attempting to deal with infected boot sectors or files, the system must be shut down and restarted in stand-alone mode, as described in the 'Running programs stand-alone' and 'Running SWEEP stand-alone' sections below.

When dealing with infected documents, this is not necessary. Follow the steps in the section 'Dealing with infected documents'.

Requirements for stand-alone working

The following materials should be at hand for stand-alone working:

The **OS/2 boot floppy disks**. For the various versions of OS/2 these are:

- OS/2 1.x: the first floppy disk of the installation kit.
- OS/2 2.x and OS/2 3.x: the first two floppy disks of the kit (or the two disks if the kit is on CD).
- OS/2 4.x: the three floppy disks of the kit.

The **SWEEP for OS/2** release floppy disk or CD.

It is recommended to prepare in advance an emergency kit consisting of copies of all the above floppy disks, and place it in a secure place ready for use. The OS/2 DISKCOPY command can be used to create the copies. The copies MUST be made on a machine known to be free of viruses. Ideally, the copies will be reserved for dealing with virus problems.

Note: The floppy disk set created by the OS/2 Warp 'Create utility diskettes' utility is unsuitable for this emergency kit. Only the installation floppy disks are suitable.

If handling an infection on a computer which is not equipped with a CD drive, SWEEP will be needed on floppy disk.

Those who do not receive SWEEP on floppy disk can copy SWEEP from CD to a floppy disk in advance with the command

```
COPY H:\OS_2\*.* A:
```

where H: is the CD drive. Store this floppy disk with the others in the emergency kit.

At this time it is a good idea to locate the following IBM utility programs and to note their locations. These can usually be found in the locations indicated:

- SYSINSTX.COM (on the first OS/2 boot floppy disk).
- FDISK.COM (on the last OS/2 boot floppy disk).

Running programs stand-alone

1. If OS/2 is already running, shut it down in the usual way.
2. Boot OS/2 from the installation floppy disk(s). After the last floppy disk has been read, one of two screens appears:
   - A request to load the OS/2 CD.
   - A 'Welcome to OS/2' screen.

   Start an OS/2 command session by pressing *Esc* for OS/2 1.x and OS/2 2.x, or *F3* for OS/2 3.x and OS/2 4.x.
3. **If intending to run FDISK or SYSINSTX**, remove the OS/2 boot floppy disk and insert the appropriate floppy disk (which was located during the preparations above). Then enter the required command.

   If intending to run SWEEP, follow the steps in the next section.

Running SWEEP stand-alone

The exact OSWEEP command line will depend on the operation to be carried out. The examples in this section show the most common case.

First, boot OS/2 according to steps 1 and 2 in 'Running programs stand-alone'.

Then follow the instructions below, depending on whether SWEEP is run from CD or floppy disk.

If the computer has a CD drive and SWEEP is on CD:

Leave the last OS/2 boot floppy disk in the floppy disk drive.

Load the Sophos Anti-Virus CD into the CD drive and run SWEEP with a command such as

```
H:\OS_2\OSWEEP -DI C:
```

where H: is the CD drive and C: is the drive to be disinfected.

Unless SWEEP reports an error, remove the floppy disk from its drive and start OS/2 for normal operations in the usual way.

If SWEEP is on floppy disk and the computer has two floppy disk drives:

Leave the last OS/2 boot floppy disk in drive A:.

Load the SWEEP floppy disk into drive B: and run SWEEP with a command such as

```
B:\OSWEEP -DI C:
```

where C: is the drive to be disinfected.

Unless SWEEP reports an error, remove the floppy disks from their drives and start OS/2 for normal operations in the usual way.

If SWEEP is on floppy disk and the computer has only one floppy disk drive:

It is necessary to swap several times between the SWEEP floppy disk and last OS/2 boot floppy disk:

a) Enter an OSWEEP command as though using drive B:, for example

```
B:\OSWEEP -DI C:
```

where C: is the drive to be disinfected.

b) OS/2 will ask for the floppy disk for drive B:

Remove the OS/2 boot floppy disk from the drive and keep it handy. Insert the SWEEP for OS/2 floppy disk into drive A:.

Select the *Retry* option.

c) OS/2 will ask for the floppy disk for drive A:

Remove the SWEEP floppy disk from the drive and keep it handy. Replace the OS/2 boot floppy disk into the drive.

Select the *Retry* option.

d) OS/2 will ask for the floppy disk for drive B:

Remove the OS/2 boot floppy disk, and replace the SWEEP floppy disk.

Select the *Retry* option.

SWEEP should now finish loading from floppy disk and should run.

Unless SWEEP reports an error, remove the floppy disk from its drive and start OS/2 for normal operations in the usual way.

e) If another command is entered after SWEEP has finished, OS/2 will probably ask for the floppy disk for drive A: again. If it does, remove the SWEEP floppy disk and replace the OS/2 boot floppy disk.

Select the *Retry* option.

Dealing with boot sector viruses on the hard disk

Disinfection

This is the preferred approach. Before attempting this, it is advisable to backup any important data on the hard disk.

Follow the steps in the 'Running SWEEP stand-alone' section above. The examples in that section show the necessary SWEEP commands: it is only necessary to substitute the disk drive letters appropriate to the particular computer.

Important! SWEEP **must** be run directly from the CD or floppy disk and **not** from a copy on the hard disk. Otherwise disinfection will fail.

This will also disinfect any infected documents that SWEEP is capable of disinfecting.

Replacing the boot sector

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

Follow the steps in the 'Running programs stand-alone' section above. 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 /NEWMBR
```

and the **OS/2 boot sector** can be overwritten with a command such as

```
SYSINSTX C:
```

The programs FDISK and SYSINSTX can be accessed in the way described in the 'Running programs stand-alone' section.

Important! If the contents of the hard disk are not visible after a clean boot, contact Sophos' technical support for advice. Some boot sector viruses do require additional action for full recovery. For example, the *OneHalf* virus encrypts the boot sector so that it is only readable when the virus is in memory.

Dealing with boot sector viruses on floppy disk

Floppy disks with infected boot sectors can either be disinfected with SWEEP or reformatted.

1. Disinfection

Follow the steps in the 'Running SWEEP stand-alone' section above. Instead of the command shown in the examples, use

```
B:\OSWEEP B: -DI -MU
```

and insert the infected disk(s) when prompted by SWEEP. If running SWEEP from CD the command is

```
H:\OS_2\OSWEEP B: -DI -MU
```

This will also disinfect any infected documents SWEEP is capable of disinfecting.

2. Reformatting

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

Dealing with 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 using

```
OSWEEP -REMOVEF
```

and restore clean versions from the original installation disks, a clean PC, or sound backups.

-REMOVEF affects infected files only, and can be used on network drives from the workstation. It does not require OS/2 to be shut down, unless a file to be removed is actively in use (e.g. an OS/2 system file).

If the -RS qualifier is specified as well, infected files will be positively overwritten rather than simply deleted. This makes them irrecoverable.

In either case, the user is asked to confirm that each file should be removed, unless the -NOC (No confirmation before virus removal) qualifier is used.

Dealing with 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.

To disinfect a document file, use a command such as

```
OSWEEP FILE.DOC -DI
```

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.

Dual Boot and Boot Manager

Almost all known viruses execute in DOS mode. However, OS/2 systems with Dual Boot or Boot Manager configured are vulnerable to attack whilst DOS is running. For example, the common virus *Form* can damage the Boot Manager.

For maximum protection against viral infection of these systems, SWEEP for OS/2 should be run in preference to SWEEP for DOS. SWEEP for OS/2 can detect infections of the Boot Manager; SWEEP for DOS cannot.

The usual method of virus removal is as follows. **Follow the steps in the 'Running SWEEP stand-alone' section above.** The examples in that section show the necessary SWEEP commands: substitute the disk drive letters appropriate for the computer.

If the OS/2 Boot Manager is infected, an alternative approach is to **follow the steps in the 'Running programs stand-alone' section**, and use the OS/2 FDISK utility to delete and reinstall the Boot Manager. Detailed instructions are in IBM's OS/2 documentation.

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 from the most recent backups.

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 two further 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 Sophos Anti-Virus for OS/2.

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 machine and the sizes of the files being examined, but typically the ‘quick’ level is 5 to 10 times faster than the ‘full’.

See the ‘Full sweep’ section and the -F and -Q command line qualifiers in the ‘Configuring SWEEP’ chapter.

Checking compressed files

If checking of compressed files is selected, SWEEP has to examine every file on the system, which may take much longer than if this option is not selected. Likewise, if sweeping inside compressed files is selected, SWEEP has to examine each file twice, as well as decompressing it in between.

Checking all files or all sectors

If SWEEP has been configured to check all files, it will take longer than if only checking executable files. Similarly, if checking all sectors is selected, SWEEP will take a long time to run.

Virus fragment reported

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

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. SWEEP is able to take advantage of such similarities in its search for virus fragments. See the ‘New viruses’ section below.

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 normally 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'.

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.

Further help needed

On the Web site at http://www.sophos.com/

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

By email to support@sophos.com

Questions can be sent to Sophos by email. Please include as much information as possible, including SWEEP and InterCheck version, operating system and patch level, the command line used to run OSWEEP and the exact text of any error messages.

By telephone on +44 1235 559933

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

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.

Backup: A copy of computer data that is used to recreate data that has been lost, mislaid, corrupted or erased.

BAT: The extension given to 'batch' file names in MS-DOS. A batch file contains a series of MS-DOS commands, which can be executed by using the name of the file as a command. AUTOEXEC.BAT is a special batch file which is executed whenever a PC is switched on, and can be used to configure the PC to a user's requirements.

Boot Sector Virus: A type of computer virus which subverts the initial stages of the booting 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.

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.

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.

CMD: The extension given to 'command' file names in OS/2. A command file may be written in the OS/2

	scripting language REXX, or may simply contain a series of OS/2 commands. STARTUP.CMD is a special command file which is executed whenever OS/2 is started, and can be used to configure OS/2 to a user's requirements.
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.
Device Driver:	A program used to 'handle' a hardware device such as a screen, disk, keyboard etc. This allows the operating system to use the device without knowing specifically how the device performs a particular task.
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.
EXE:	The extension given to executable files in MS-DOS. These are similar to COM files, but can contain more than 64K of code and data.
Extended DOS Partition:	An area of the hard disk assigned to DOS. It is usually subdivided into logical disks. The first logical disk can be made bootable though this is not usual.
FAT:	File Allocation Table; a mnemonic term used by the MS-DOS operating system (and others) to describe the part of a disk which contains information describing the physical location on the disk of the chains of clusters forming the files stored on that disk.
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.

HPFS: High Performance File System; a file system used by OS/2 .

ID: An identification code, username, identification card or an identification token.

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 enables a server-based virus scanner to be used for scanning workstations connected to the network.

Interrupt: A mechanism by which a process can attract the immediate attention of the CPU, usually in order to serve an urgent request from an external device. The interrupt table on 8086 microprocessors occupies the bottom 1K of RAM.

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.

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

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

	'active' partition. 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.
OS/2:	An operating system for 80386+ based IBM compatibles. It allows true multi-tasking.
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.
Partition Table:	A 64-bit table found inside the master boot sector on hard disks which contains information about the starting and ending of up to four partitions on the hard disk. The partition table also contains information on the type of the partition, e.g. DOS partition, UNIX partition etc.
Polymorphic Virus:	Self-modifying encrypting virus.
Primary DOS Partition:	A portion of the hard disk assigned exclusively to DOS. It is usually the bootable partition for DOS.
Stealth Virus:	A virus which hides its presence from the PC user and anti-virus programs, usually by trapping interrupt services.
SYS:	The extension given to system file names in MS-DOS. An example is the file CONFIG.SYS which sets up various configuration parameters for the operating system on power-up.

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: Sometimes explicitly referred to as a computer virus, a program which makes copies of itself in such a way as to 'infect' parts of the operating system and/or application programs. See Boot Sector Virus and Parasitic Virus.

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

W

X

Z

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
Tel 3393 4793 · Fax 3393 4793 · Code +45

Finland:

Oy Protect Data Ab
P.O. Box 48
00931 Helsinki
Finland
Email antti.laaja@dlc.fi
Tel 09 752 521 · 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
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 forum_data_security@pi.net
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 protect_data@oslonett.no
Tel 022 65 64 50 · Fax 022 65 64 58 · 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 93 490 70 52 · Fax 93 490 76 04 · 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/