Sophos Anti-Virus

User Manual

DOS/Windows 3.x

SOPHOS

Sophos Anti-Virus

for DOS/Windows 3.x

User Manual
February 1998

This manual documents Sophos Anti-Virus
for DOS and Windows 3.x, 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 # masdez0j/971218

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.

SWEEP can be used on its own to scan workstations or file servers; the use of InterCheck is optional.

About SWEEP

SWEEP for DOS can be used in two ways:

- Through the menu-based utility SW.
- By specifying command line qualifiers.

The former is simpler to use, and allows most options to be configured, while the latter gives greater flexibility and control.

SWEEP for DOS and networks

Sophos produces 'native' virus-checking software for Windows NT, Windows 95, NetWare, OpenVMS, OS/2 and Banyan VINES. However, on other systems, SWEEP for DOS can be used to:

- Check the file server.
- Act as an InterCheck server.

In these cases, SWEEP for DOS can be run either on a 'soft PC' on the server, or on a dedicated workstation.

This allows InterCheck to be implemented on PC networks such as AIX, AS/400, HP-UX, LANtatsic, NetWare Lite, OSF/1, Solaris, UNIX and WFWG.

About InterCheck

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

Features of Sophos Anti-Virus

- 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, while urgent updates can 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, Excel and Office 97 macro viruses.
- Offers two levels of security, allowing a ‘quick sweep’ which looks for virus identities in parts of files likely to contain a virus, and a ‘full sweep’ which looks for virus fragments in every part of every file.
- Is easy to use, and easily integrated into complex virus-checking applications, such as the automated unattended checking of file servers.
- Includes an extensive on-line virus information database.

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 on a workstation

If using SWEEP for on-demand scanning on a workstation, read ‘Installing SWEEP’.

On-access scanning on a workstation

If using SWEEP and InterCheck for on-demand and on-access scanning on a workstation, read the ‘Installing SWEEP’ and ‘About InterCheck’ chapters.

More advanced features

If using SWEEP’s more advanced features, read the ‘Using SWEEP with SW’ or the ‘Using SWEEP from the command line’ and ‘Configuring SWEEP’ chapters, as well as the installation chapter.

Scheduled scanning on a network

If using SWEEP for scheduled scanning via the AT utility (available only to those with a file server licence), read the ‘Scheduling SWEEP’ chapter, as well as the chapters on SWEEP installation and use.

Providing on-access scanning for a network

If using SWEEP and InterCheck to provide on-access scanning on networks for which Sophos does not offer a ‘native’ server based on-access scanner, read the ‘About InterCheck‘, ‘Installing SWEEP as an InterCheck server’, ‘Installing InterCheck clients’, ‘Controlling the InterCheck server’ and ‘Configuring InterCheck clients’ chapters.

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’ shows how to install SWEEP on a workstation, how to install InterCheck on-access scanning for a workstation, how to install SWEEP on a file server, and how to upgrade SWEEP.
- ‘Using SWEEP with SW’ describes the use of SWEEP with the SW menu-based user interface.
- ‘Using SWEEP from the command line’ introduces the basics of using SWEEP from the command line.
- ‘Configuring SWEEP’ describes how to specify which items SWEEP will check and how to

customise virus reporting. It also details the SWEEP command line qualifiers.

- 'Scheduling SWEEP' describes how to schedule SWEEP with the AT utility supplied on the ICONTROL disk.
- 'Installing SWEEP as an InterCheck server' shows how to install SWEEP as an InterCheck server and how to upgrade this installation.
- 'Installing InterCheck clients' describes how to install and run InterCheck clients.
- 'Controlling the InterCheck server' describes how to control SWEEP for DOS running as an InterCheck server.
- 'Configuring InterCheck clients' describes the configuration of InterCheck clients running under Windows 95, Windows for Workgroups, Windows 3.x and DOS.
- 'Treating viral infection' describes how to deal with a virus once it has been discovered.
- 'Troubleshooting' provides help with possible problems.

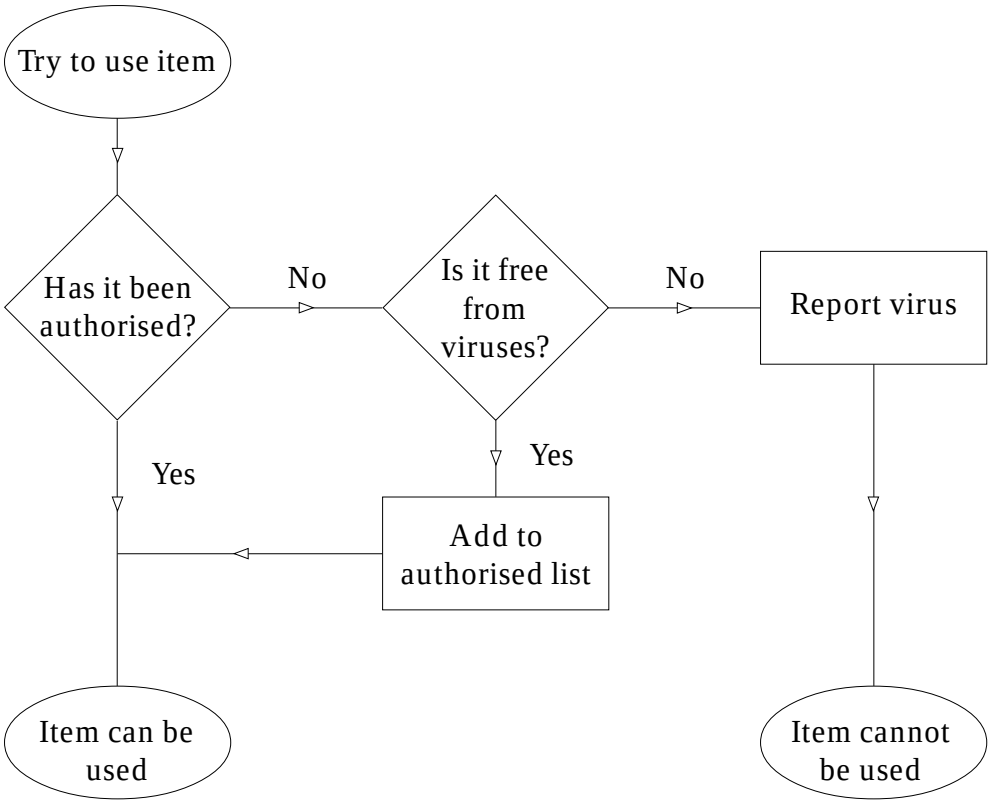
In addition, the 'Glossary' contains explanations of some technical terms used in this guide.

About InterCheck

This chapter presents an overview of Sophos' InterCheck technology.

What is InterCheck?

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



The InterCheck principle

How 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.

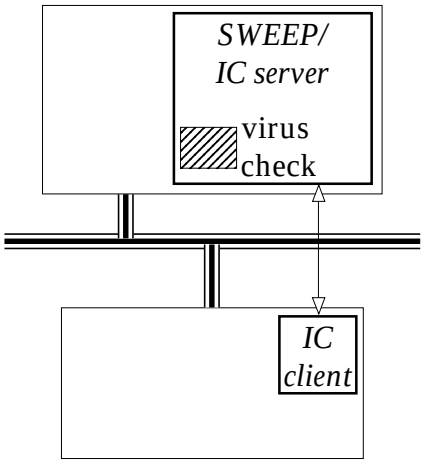
A **stand-alone InterCheck client** does not have to communicate with a remote InterCheck server, and uses a local installation of SWEEP to check for viruses.

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.

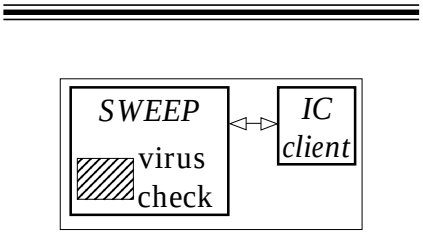
How does InterCheck work?

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

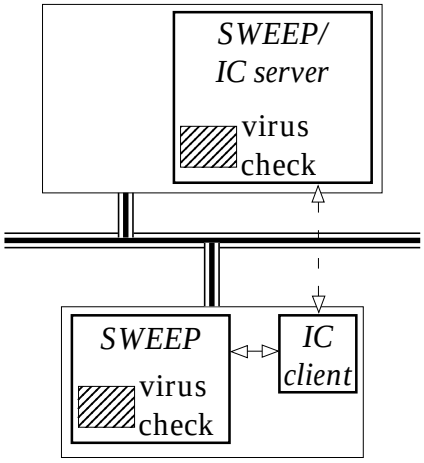


Networked IC client and remote IC server

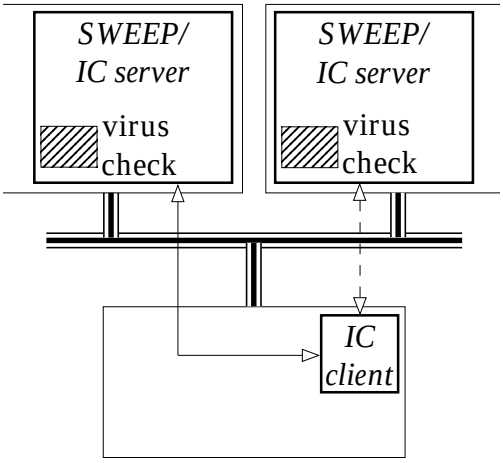
No IC server



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 shows how to install SWEEP on a workstation, how to install InterCheck on-access scanning for a workstation, how to install SWEEP on a file server, and how to upgrade SWEEP.

Important! Instructions refer to Sophos Anti-Virus floppy disks. If using a Sophos Anti-Virus CD, either make Sophos Anti-Virus floppy disks with the utility supplied, or use the DOS directory on the CD.

System requirement

The minimum system requirement is:

- MS-DOS version 3.1 or later.

Which kind of installation?

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

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

Installing SWEEP and stand-alone InterCheck on a workstation.
This enables on-access as well as on-demand scanning of a workstation. Note that the procedure for installing stand-alone InterCheck on-access scanning also installs SWEEP.

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. See the 'Installing SWEEP as an InterCheck server' chapter.

The first three types of installation are described in the sections below.

Before installing SWEEP

Before installing SWEEP **on a DOS workstation**, it is recommended to check that the workstation is virus-free. This is done by running SWEEP directly from floppy disk, and requires:

- The SWEEP floppy disk.
- A write-protected system floppy disk.

The workstation must be booted from a write-protected, virus-free system floppy disk, or some stealth viruses may not be detected. For instructions on creating a clean floppy disk, see 'Creating a clean DOS boot disk' in the 'Treating viral infection' chapter.

Switch the PC off and insert the write-protected system floppy disk in drive A:. Switch the power on.

Wait until the PC boots and displays the prompt

```
A>
```

Take the system floppy disk out and insert the SWEEP floppy disk. Now enter the command

```
SWEEP *:
```

SWEEP will scan the local hard drives.

If SWEEP finds a virus, do not panic. Consult the 'Treating viral infection' chapter.

Installing SWEEP on a workstation

On-demand scanning of a workstation, and any files it can access, is provided by installing SWEEP.

The procedure depends on whether SWEEP is to be installed under DOS or Windows.

Under DOS

First, virus-check the PC as described in 'Before installing SWEEP' above.

Then either copy all files from the SWEEP floppy disk into a directory on the hard disk, or run the INSTALL utility. To start the INSTALL utility, insert the installation floppy disk into drive A: and type

```
A:INSTALL
```

Under Windows

First, virus-check the PC as described in 'Before installing SWEEP' above, and then

1. Start Windows and open the Windows Program Manager.
2. Insert the SWEEP for DOS floppy disk in the disk drive.
3. Choose *Run* from the *File* menu in Program Manager.
4. If using the A: drive, enter

   ```
   A:SETUP
   ```

   in the Run dialog box.
5. Enter or confirm the target directory for the SWEEP files. The installation utility will copy the files and create the SW icon.
6. To start SW, double-click this SW icon.

Installing SWEEP and stand-alone InterCheck on a workstation

On-access scanning of a workstation is provided by an InterCheck client. There are two types:

The **stand-alone InterCheck client** performs scanning locally. This reduces network traffic, offers faster initial authorisation of files, and makes it suitable for workstations not always connected to the network. Installation on a DOS/Windows workstation is described below. This also installs a copy of SWEEP.

For stand-alone clients on Windows for Workgroups workstations connected to a network, see the 'Installing InterCheck clients' chapter.

The **networked InterCheck client** sends files to a remote InterCheck server for scanning, and is suitable for large networks. Installation is described in the 'Installing InterCheck clients' chapter of the Sophos Anti-Virus user manual for the InterCheck server.

Stand-alone InterCheck client for DOS/Windows

The stand-alone InterCheck client is installed using the ICINSTAL facility. This is started and used as described below.

Note: The user is prompted to load SWEEP as part of the procedure.

Starting ICINSTAL

The procedure for starting ICINSTAL depends on whether the workstation has access to a network.

For clients with no network access

Insert the InterCheck disk into the floppy disk drive, and enter

```
A:ICINSTAL
```

at a DOS prompt, if the InterCheck disk is in drive A:.

For clients with network access

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
```

Using ICINSTAL

If there is 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.

Please note that when InterCheck first installs, the whole disk is swept for viruses. This may take several minutes depending on the size of the disk drive.

Starting InterCheck when not connected to the network

ICINSTAL installs a local copy of InterCheck on the workstation and modifies the AUTOEXEC.BAT to load INTERCHK.EXE on startup.

Note: Ensure that InterCheck is run from the server whenever the workstation is connected to the network. If this is done, the local copy of InterCheck is updated automatically when the central version on the server is updated.

Installing SWEEP on a file server

On-demand scanning can be made available to all users on the network by installing SWEEP on a file server (if the licence allows this).

To do this, copy all files from the SWEEP floppy disk into a publicly accessible read-only area on the server.

Note: When installing under NetWare do **not** mark SWEEP.EXE as execute-only, because the software needs to load overlays when run.

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. When an update is received:

If using SWEEP only, follow the steps in the 'Installing SWEEP on a workstation' or 'Installing SWEEP on a file server' sections above.

If using a stand-alone InterCheck client on the workstation, follow the steps in the 'Installing SWEEP and stand-alone InterCheck on a workstation' section above. This updates SWEEP and InterCheck.

If using SWEEP as an InterCheck server, see the 'Updating SWEEP used as an InterCheck server' section of the 'Installing SWEEP as an InterCheck server' chapter.

Urgent SWEEP updates

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

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

Each IDE file should be placed in a file with an IDE extension in the SWEEP directory. SWEEP will then load the new virus identities when restarted.

Using SWEEP with SW

This chapter describes the use of SWEEP with the SW menu-based user interface.

Starting SW

Important! Before running anti-virus software, it is essential to ensure that no viruses are memory-resident. This is achieved by 'secure booting', as described in the 'Secure booting' section of the 'Using SWEEP from the command line' chapter.

Failure to boot securely may result in some stealth viruses not being detected on disk.

After secure booting, the PC will display the prompt

```
A>
```

SW can now be run. Insert the SWEEP floppy disk into the A: drive, type SW and press *Enter*:

```
A> SW
```

Overview of the SW display

SW can be driven using either keyboard or mouse.

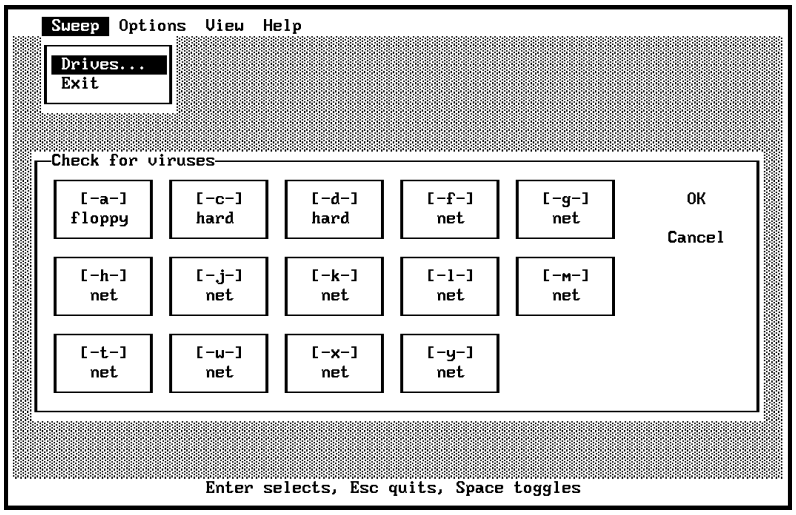
Keyboard The bottom bar on the screen shows the function of particular keys at any time.

Mouse The mouse can be used either to click on a selected object or to 'point and drag' menu entries. The latter

technique is especially useful for quick navigation through the menus.

Using SW

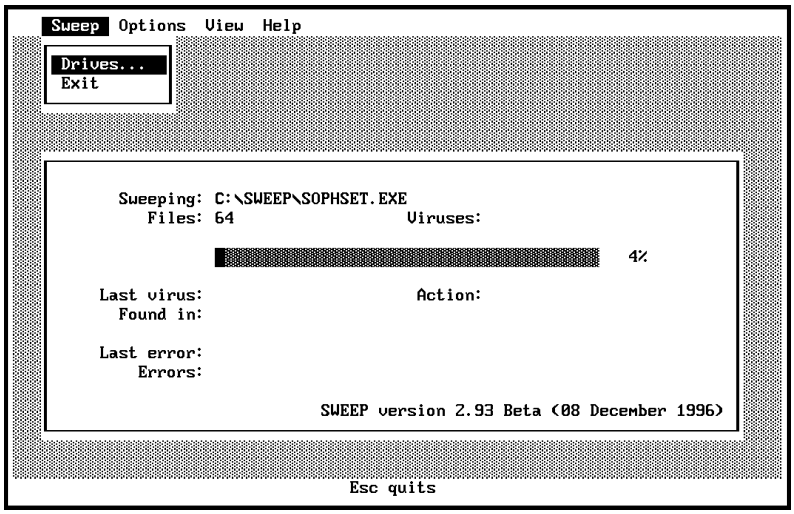
By default, SW will display the list of drives:



Double-clicking on a drive will start sweeping it immediately.

Use the cursor keys to move the cursor over the drive to check, and press the spacebar to select or deselect the drive. The mouse can also be used to select the drive(s) to check.

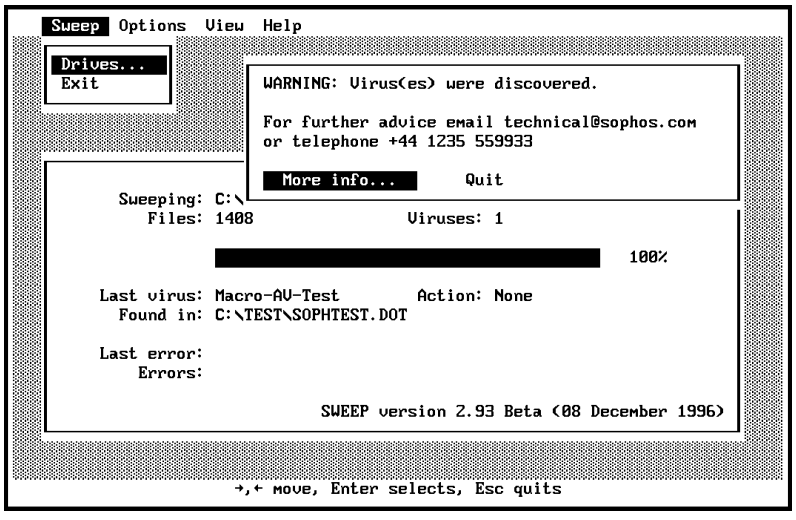
Once all the drives have been specified, press *Return* or click *OK* to start sweeping:



Finding a virus

If SWEEP discovers a virus - do not panic!

SWEEP will display a warning message:

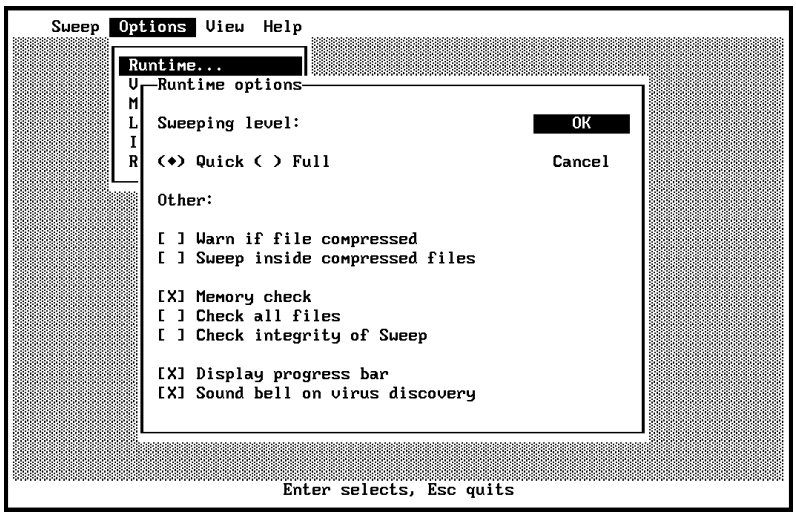


Select *More info* to display the virus database entry for the last virus found. This entry will include advice on removing that particular virus. See the 'Virus library' section below for more information on the virus library.

Note: The message displayed when a virus is found can be customised. See the 'Message if virus found' section below for more information.

For more information on dealing with a virus, see the 'Treating viral infection' chapter.

Runtime options



Sweeping level

For everyday use, the 'quick sweep' mode offers excellent security. The 'full sweep' mode gives a still higher level of security because it examines the complete contents of files and can, for example, discover viruses 'buried' underneath other code appended to a file.

See also the '-Q Quick sweep' and '-F Full sweep' sections of the 'Configuring SWEEP' chapter.

Warn if file 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 (note that InterCheck will trap the closing of files as they are

decompressed and send them to the server automatically for checking). SWEEP can warn if it encounters any of these files, but by default it does not.

See also the '-WC Warn if compressed files are encountered' section of the 'Configuring SWEEP' chapter.

Sweep inside compressed files

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.

See also the '-SC Scan inside compressed files' section of the 'Configuring SWEEP' chapter.

Memory check

By default, SWEEP will check memory for memory-resident viruses before each sweep is performed.

See also the '-ME Check memory' and '-NM No memory check' sections of the 'Configuring SWEEP' chapter.

Check all files

Only those files defined as executables will be swept, unless the *Check all files* option is selected. The extensions treated as executables are COM, DLL, DOC, DOT, EXE, OV?, SYS and XL?. Note that SWEEP will automatically detect whether files contain macros (and are thus vulnerable to macro virus infection) irrespective of their file extension.

See also the '-ALL Sweep all files' section of the 'Configuring SWEEP' chapter.

Check integrity of SWEEP

If this option is selected, the SWEEP executable (SWEEP.EXE) will be checked before each sweep is performed. A change in the contents of SWEEP.EXE may indicate the presence of a virus or some other form of data corruption.

See also the '-CI Check integrity' section of the 'Configuring SWEEP' chapter.

Display progress bar

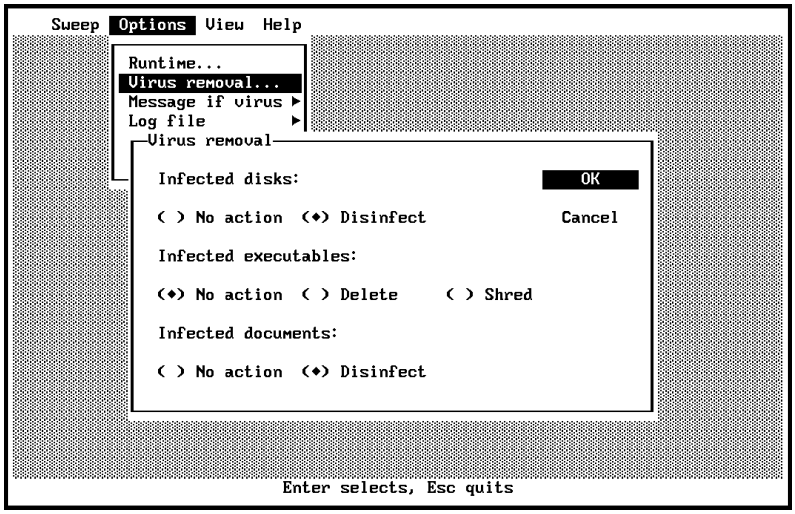
In order to display the progress bar, SWEEP has to count all the items to be swept before starting the virus check. On large network drives this can take a significant length of time, which can be saved by disabling this option.

Sound bell on virus discovery

By default, SWEEP will sound a bell if a virus is found.

See also the '-NB No bell' section of the 'Configuring SWEEP' chapter.

Virus removal



Infected disks

SWEEP can automatically disinfect most boot sector viruses from infected floppy and hard disks.

Infected documents

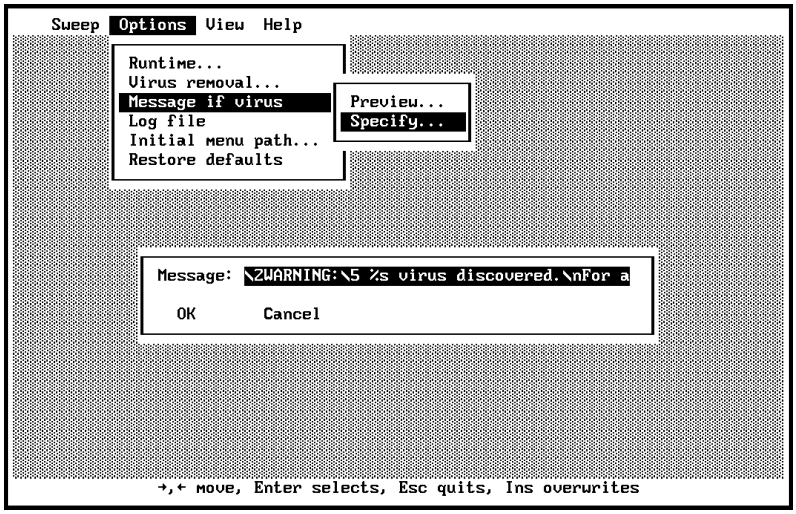
SWEEP can remove the viral macros from documents infected with certain types of macro viruses. If document disinfection fails, the infected file will be dealt with in the same way as any other infected file.

Infected executables

If an infected executable is found, the file can be deleted or shredded. Shredding is a more secure type of file deletion that overwrites the contents of the file.

Message if virus found

The message displayed when a virus is found can be customised. Select *Message if virus* then *Specify* from the *Options* menu to specify the message.



The first occurrence of %s in the text will be replaced by the name of the last virus found, while \n will produce a new line. To embolden parts of the message, start the emphasized text with \2 and end with \5. Select *Message if virus* then *Preview* from the *Options* menu to view the message.

Log file

SWEEP can create a log file of activity. To specify the location of the log file, select *Log file* then *Specify* from the *Options* menu. To view its contents, select *Log file* then *View*. To empty it, select *Log file* then *Clear*.

Initial menu path

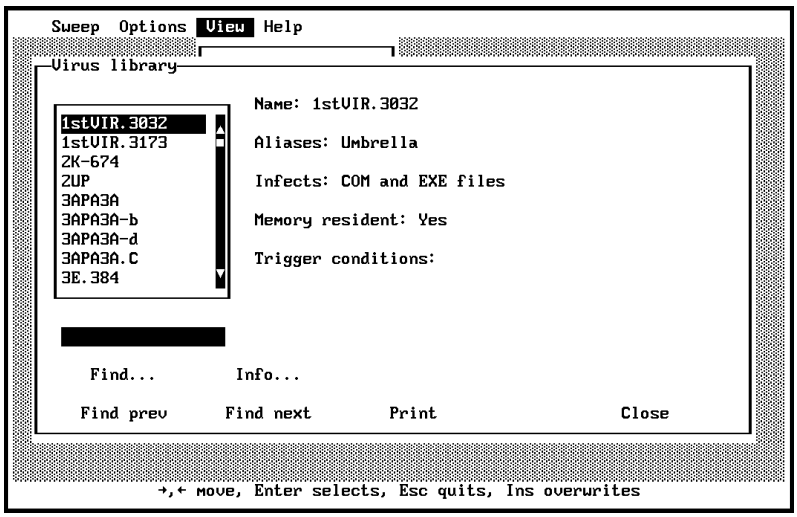
Select *Initial menu path* from the *Options* menu to specify the menu which will be displayed when SW is started. The default initial path is represented by the string '00', because the *Drives* option from the *Sweep* menu is the first entry in the first menu (see the '-P.. Path through menus' section below). Enter a different string to display a different menu on start-up, e.g. to display *Virus library* from the *View* menu on start-up, enter '20' to specify the third menu's first option.

Restore defaults

Select *Restore defaults* from the *Options* menu to restore the default SW options.

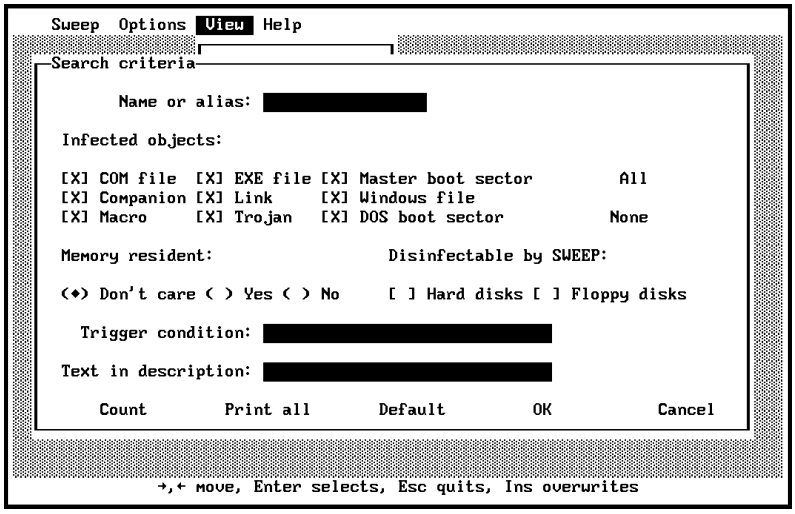
Virus library

Select *Virus library* from the *View* menu to open the virus library.



Searching for a particular virus

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



Infected objects

Some viruses infect **COM** or **EXE files**. Others infect the **master boot sector** or the **DOS boot sector**. **Companion viruses** place the virus code in a COM file with the same name as the EXE file. **Link viruses** subvert directory entries to point to the virus code. **Windows viruses** affect Windows executables and **macro viruses** place viral macros inside documents capable of containing macro sequences. **Trojan horses** are not viruses, but programs which provide unanticipated and undesired side effects when executed.

Memory-resident

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

Disinfectable by SWEEP

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

Trigger conditions

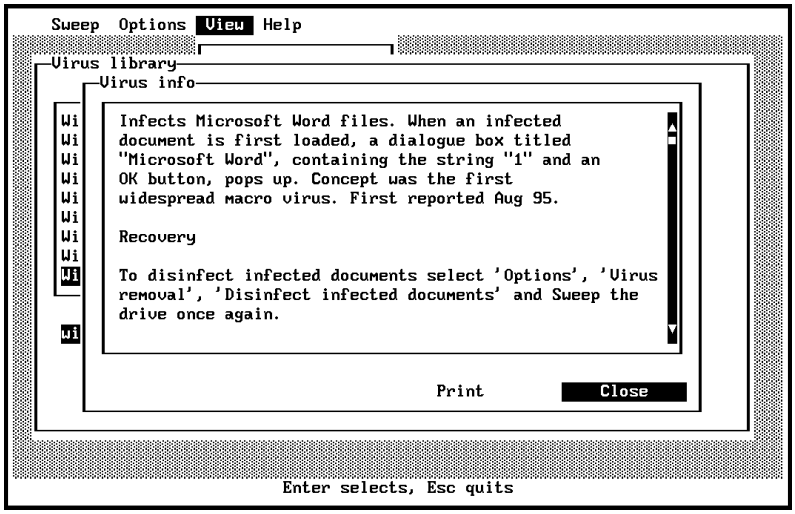
Many viruses require specific conditions, such as a certain time or date, in order to exhibit side-effects.

Text in description

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

Information on a particular virus

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



SW command line qualifiers

-BW Display in black and white

Some black and white monitors appear to the PC as colour, resulting in an unclear output in SW. This is especially apparent on some LCD screens. To force SW to output black and white text use -BW.

```
SW -BW
```

Note: -BW is **not** the same as the -MO command line qualifier.

-INI=<name> Specify SW configuration file

SW stores the configuration options, such as the drives selected and the runtime options, in an INI file. This is normally called SW.INI and stored in the directory from which SW is run, but an alternative name and path can be specified.

See also the -SW=<path> command line qualifier.

-MO Display in monochrome

This option should be used only with the old MDA (Monochrome Display Adapter) screens. If used on a CGA, EGA or VGA screen, the display will remain blank.

-P.. Path through menus

This qualifier can be used to specify the selection of options in the SW menu structure. **0 selects the first option, 1 the second etc.** For example

```
SW -P32
```

will choose option 4 and then option 3 (i.e. the *Command line qualifiers* option from *Help* menu).

'^' is equivalent to the user pressing *Esc*, '@C' to *Alt-C*, '\r' to *Enter* and '\b' to *Backspace*, while '?' allows the user to make a selection.

Menu options can also be referred to by their keyboard shortcuts. For example

```
SW -PVV\rWinword/Concept
```

would select the V*irus library* from the V*iew* menu, and would enter 'Winword/Concept' as the search string.

-SW=<path> Specify location of SWEEP

If SWEEP.EXE is not located in the same directory as SW.EXE, use the -SW=<path> command line qualifier to specify the correct path.

For example, if SWEEP.EXE is in the F:\SOPHOS subdirectory and SW is being run from drive C:, enter

```
SW -SW=F:\SOPHOS\SWEEP.EXE
```

See also the -INI=<file> command line qualifier.

Using SWEEP from the command line

This chapter introduces the basics of using SWEEP from the command line.

Secure booting

Important! Before running anti-virus software, it is essential to ensure that no viruses are memory-resident. This is achieved by 'secure booting', i.e. executing only code that is known to be virus-free during booting-up. For this a write-protected, clean system floppy disk is needed (see 'Creating a clean DOS boot disk' in the 'Treating viral infection' chapter).

Failure to boot securely may result in some stealth viruses not being detected on disk.

Securely booting stand-alone PCs

Important! Switch the PC off. Do **not** use *Ctrl-Alt-Del* because this is intercepted by some viruses.

Insert a clean, write-protected system floppy disk into drive A:.

Switch the PC on and let it boot from the floppy. After the PC has booted, it will display the prompt

```
A>
```

SWEEP can now be run.

Using a memory manager

If SWEEP does not find extended or expanded memory, it will create a 'swap' file on the hard disk. To increase the sweeping speed, install the extended or expanded **memory manager**. For example, to use extended memory, insert the following line into CONFIG.SYS:

```
DEVICE=HIMEM.SYS
```

and copy the HIMEM.SYS onto the floppy. When the PC is next booted, extended memory will be available to SWEEP.

Using other device drivers

In most cases there is no need to load any other device drivers in order to sweep disks. However, if the system needs to load any device drivers, such as ANSI.SYS, or to execute any software on startup, the file CONFIG.SYS must refer to copies of the drivers held on drive A:. In addition, any software executed on startup through AUTOEXEC.BAT must also be present on the floppy disk.

CONFIG.SYS normally refers to other files, which are loaded into memory before the system is started, using statements such as

```
DEVICE=filename
```

Clean copies of all these files should be transferred onto the floppy disk and CONFIG.SYS on the floppy disk should be modified, if necessary, to ensure that it refers to the files on the floppy disk, rather than the original copies on the hard disk. For example, any statements in CONFIG.SYS, such as

```
DEVICE=C:\DOS\ANSI.SYS
```

should be modified to read

```
DEVICE=ANSI.SYS
```

to ensure that all of the operating system is loaded from the write-protected floppy disk.

Securely booting a Novell NetWare workstation

This section describes the procedure for the secure booting of a Novell NetWare 3.11 workstation before sweeping the file server.

Important! Switch the workstation off.

Insert a clean, write-protected, system floppy disk into drive A:. This floppy disk should also contain the NETx, IPX and LOGIN programs, as well as an extended or expanded memory manager (see 'Using a memory manager' above).

Switch the PC on, and wait for the prompt

```
A>
```

Run IPX from the floppy disk, followed by NETx. Then run LOGIN **from the floppy disk** with the '/S NUL' command line qualifier. This will prevent the execution of both system and user login scripts. Enter

```
LOGIN /S NUL USERNAME
```

to log in to the network. If there is a need to execute any other NetWare programs, make sure that they are present and run from the floppy disk.

Note that users can only check directories to which they have access. In order to access all subdirectories on a server, it is necessary to log in with **read** rights equivalent to those of SUPERVISOR.

Booting a workstation connected to other networks

A similar process should be followed for other networks, so that a supervisor can log in without executing any DOS programs stored on the file server.

What should you check?

SWEEP can be used to check floppy disks, hard disks, network drives and memory. It is normal to check the hard disk first and then any suspect floppy disks.

Note: SWEEP cannot find viruses in files which have been modified in any way from the original. See the 'Checking compressed files' section of the 'Configuring SWEEP' chapter as well as the -SC and -WC command line qualifiers.

Checking the hard disk

After performing a secure boot, drive A: will be the current drive and the system will display the prompt

```
A>
```

Take the system floppy disk out and insert the SWEEP floppy disk. Run SWEEP from the floppy disk using the command

```
SWEEP C:
```

SWEEP will check drive C:. To interrupt SWEEP press *Esc* at any time. Any viruses discovered are listed on the screen.

To check all hard drives type

```
SWEEP *:
```

Checking floppy disks

After performing a secure boot, drive A: will be the current drive and the system will display the prompt

```
A>
```

Take the system floppy disk out and insert the SWEEP floppy disk. Run SWEEP using the command

```
SWEEP -MU
```

SWEEP will prompt for the floppy disks to be checked.

Checking file servers

SWEEP can be used to check file server drives.

Important! It is important to establish a network user with read rights before checking the network. Some viruses infect files at the moment of 'file open' request to DOS. If the user performing the checking has write rights to all files, and such a virus is resident in memory, **all files on the server will be infected after sweeping the server**.

Boot up and log into the server securely, as described in the 'Secure booting' section. The system will display the prompt

```
A>
```

Take the system floppy disk out and insert the SWEEP floppy disk. Run SWEEP from the floppy disk using the command

```
SWEEP <drive1> <drive2> ... <driven>
```

For example, to check drives F: and G:, use the command

```
SWEEP F: G:
```

Most networks do not allow examination of the boot sectors of file servers. Thus, when sweeping a file server drive, boot sectors will not be checked. Furthermore, on most networks, some files (normally .SYS) are not readable and SWEEP will report an error after trying to open them. When sweeping a file server drive, by default .SYS files are not checked. Any other unreadable files can be excluded by quoting them, preceded by the exclusion operator, in the SWEEP.ARE file. For more information see the 'What does SWEEP check?' section.

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.

There is no loss of security in not checking these files, as they contain data and not executable code. They cannot be infected by a virus.

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 a small chance that the virus has been matched by a legitimate, virus-free program. If in doubt, contact Sophos’ technical support for advice. The screen output will look like this:

```
SWEEP virus detection utility
Version 3.04
Copyright (c) 1989,97 Sophos Plc, Oxford, England

System time 10:44:43, System date 10 December 1997
Virus library date 01 December 1997 (12998 viruses)

Quick Sweeping
Press Esc to quit

>>> Virus 'Form' found in abs sector 1, drive 00 (floppy disk)
    head 0, cyl 0
0 files swept in 0 minutes and 4 seconds.
1 virus was discovered.
0 files out of 1 were infected.

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

The shaded line above indicates the discovery of the virus ‘Form’. A virus is reported in the line which starts with ‘>>>’ followed by either ‘Virus’ or ‘Virus fragment’. In the above example no files were infected because Form is a boot sector virus.

For information on dealing with viruses, see the ‘Treating viral infection’ chapter.

What does SWEEP check?

By default, SWEEP looks for viruses and virus fragments in the following areas:

- All memory used by programs and viruses.
- All COM, DLL, DOC, DOT, EXE, OV?, SYS and XL? files on the specified disk.
- Logical sector 0 of the specified disk.
- First data sector of the partition (except when running under DOS version 4 or above).
- Physical sector 1 of hard disk devices 80 to 83 Hex (internal hard disks).

Note: SWEEP automatically detects whether files contain macros (and are thus vulnerable to macro virus infection) irrespective of their file extension.

Note: In most cases these default settings are sufficient and there is no need to check any extra items.

To specify additional (or different) areas, or file types, use the command line or create a file called SWEEP.ARE. The syntax for describing areas to be checked is described in the ‘Configuring SWEEP’ chapter.

To display items checked by SWEEP, use the -DA command line argument:

```
SWEEP -DA
```

Configuring SWEEP

This chapter describes how to specify which items SWEEP will check, how to check compressed files, and how to customise virus reporting. It also details the SWEEP command line qualifiers.

Specifying what SWEEP will check

The files or areas to be checked by SWEEP can be specified from the command line (as described in this section), or in an area file (as described in the 'Specifying what SWEEP will check with SWEEP.ARE' section below).

Specifying drives to be checked

To check the current drive only, do not specify any drives in the command line. Issue the command

```
SWEEP
```

To check one or more drives, specify them in the command line. For example, to check drives C: and D:, use

```
SWEEP C: D:
```

Note: If one or more drives are specified, SWEEP will **not** check the current drive in addition to these.

To specify all hard drives for checking, use the '*:' command line qualifier:

```
SWEEP *:
```

Hint: This is useful when the number of hard drives is unknown, e.g. when invoking SWEEP from a file server to check all workstation hard drives.

Specifying files to be checked

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

```
SWEEP ISVIRUS.BIN
```

Make sure that any symbols used do not conflict with the PC-DOS meaning. For example, do not use the recursion symbol '>' in the command line, because it means redirection in PC-DOS.

If one or more items are specified in the command line, SWEEP will check only these items.

Specifying what SWEEP will check with SWEEP.ARE

Items to be checked can be specified in an area file (SWEEP.ARE).

This must reside in the current drive and subdirectory when you run SWEEP. For example, if the current drive and directory is C:\PROGS, SWEEP.ARE must reside on the C: drive in the directory C:\PROGS.

SWEEP.ARE can contain a list of files, sectors and memory regions to be checked. This file can be edited as required. The syntax for describing areas to be checked is given in the following sections.

Example of a SWEEP.ARE file

For example, SWEEP.ARE may contain

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

which will check the DOS boot 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 DOS 'pipe' operator and is not the same as 1 (digit) or l (character).

The default drive in the command line can be overridden by using the -AD command line qualifier. For example, to check drive A: while SWEEP is on drive C: you would type

```
SWEEP -AD=A:
```

If the drive is not specified, the default drive will be used. For example, if SWEEP.ARE contains

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

and the command

```
SWEEP -AD=A:
```

is issued, then SWEEP would check

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

in addition to the standard areas on drive A:.

Specifying files to be checked with SWEEP.ARE

Particular file types and areas can be specified in SWEEP.ARE using the normal DOS 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 specified directory, should be searched.

For example, if the entry

```
C:*.ABC
```

is specified, and the current directory of 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 directory C:\MYAREA\MYFILES and all its subdirectories.

Note: See also the -REC command line qualifier.

To check all executables

To check all executable files (COM, DLL, DOC, DOT, EXE, OV?, SYS, XL?) 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

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.

If the name of a file is specified **without a path**, all files or directories with that name will be excluded. For example

```
<ALL.EXE ; will not be examined
```

will not examine the file ALL.EXE in any subdirectory in which it is found, e.g. files C:\EXE\ALL.EXE, C:\FIX\DEVELOP\ALL.EXE etc.

Excluding a directory will exclude all files and subdirectories of that directory.

Important! The drive, path and file name of the included and excluded items must be **identical**. For example, if the user specifies

```
C:\>*.COM
```

to be examined and excludes

```
<\WS.COM
```

the file 'C:\WS.COM' will still be examined. To exclude it, specify

```
<C:\WS.COM
```

Likewise, if the specification is

```
\>*.EXE
```

and the current drive is C:, specifying

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

means that SWEEP will still examine 'NU.EXE' in the root directory. To exclude it, specify

```
<\NU.EXE
```

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

```
SWEEP -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 checked with 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 DOS boot sector, as they contain executable program code which many viruses attack. A floppy disk has only a DOS boot sector.

Sectors can be referred to in two ways: as *logical* sectors or *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 DOS 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, the absolute sector at cylinder 0, head 0, sector 1 and logical sector 0 are the same physical sector.

Logical Sectors

To specify a particular logical sector or set of sectors, use the '|' symbol (the DOS pipe operator). You can also 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, e.g. 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.

Specifying 'F' as `ssector` will check the first data sector of the drive.

For example

```
C:|F
```

will check the first data sector of the drive C:.

Note: This sector needs to be checked only on DOS versions prior to version 5.0, due to the way that the system files are loaded during the boot process.

In addition, the '`|*`' specification can be used:

```
|*
```

This checks all 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.**

Absolute Sectors

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 made 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 disks 80 to 83 Hex, specify

```
"All master boot sectors"
```

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

Specifying memory ranges for checking

Intelligent memory checking (i.e. only memory used by programs and viruses) is enabled by default, but can be explicitly specified in SWEEP.ARE by

```
"All memory"
```

or by using the -ME command line qualifier:

```
SWEEP -ME
```

Intelligent memory checking is less prone to false positives than checking all 640K of base memory.

Other areas of memory can be checked for the presence of virus fragments. To specify memory ranges, use the '[' symbol.

The format of the specification is

```
[segment:sbyte ebyte]
```

where

`segment` is the memory segment (assumed to be 0000 if not specified)

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

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

Note that all values are in **hexadecimal** format.

For example

```
[0000:0000 00FF]
```

specifies that bytes 0000 to 00FF hex within segment 0000 should be checked.

In addition, the following specification can be used:

```
[*]
```

This checks all 640K of base memory. The [*] qualifier can be specified in the command line. For example

```
SWEEP [*]
```

Note: Checking all 640K of base memory can cause false positives. This is especially common when more than one anti-virus product is used and one of these does not encrypt (or scramble) virus fragments held in memory. A similar situation can occur if a virus is successfully removed from the hard disk, and SWEEP is run immediately afterwards. The remnant of the virus may still be present in system buffers and will be flagged if memory is checked. This does **not** necessarily mean that the virus is active in memory.

Checking compressed files

If InterCheck is being used on client workstations, users are automatically protected from infection, and compressed files are checked as described in the 'Checking compressed files automatically' section.

If InterCheck is not being used, users should follow the instructions in the 'Checking compressed files using SWEEP' section.

The approach depends on the kind of compressed files encountered:

- **Statically compressed files**, such as those compressed with PKZIP, ARC etc., consist simply of compressed data. No known viruses infect statically compressed files after compression.
- **Dynamically compressed files**, such as those compressed with PKLITE, LZEXE etc., consist of compressed data and a program to compress that data. The data can be infected before compression, while the decompression program can be infected at any time after compression.

Note: Some utilities allow compression of whole drives. A separate section, 'Checking dynamically compressed drives' explains how to deal with these.

Checking compressed files automatically

If InterCheck is running on client workstations, compressed files will be dealt with as follows:

Statically compressed files

InterCheck will trap the closing of files as they are decompressed (with PKZIP, ARC etc.) and send them to the server automatically for checking.

Dynamically compressed files

By default, InterCheck will check the decompression program only. However, for files compressed with

PKLITE, LZEXE and Diet, the InterCheck server can be enabled to scan the compressed data also. See the Sophos Anti-Virus user manual for the InterCheck server.

Checking compressed files using SWEEP

Statically compressed files

Statically compressed files should be decompressed on an isolated PC and checked with SWEEP.

Dynamically compressed files

By default, SWEEP will check the decompression program only. However, for files compressed with PKLITE, LZEXE and Diet, it can be configured to check the compressed data also.

Use the -SC command line qualifier. For example:

```
SWEEP A: -SC
```

Use this facility with care, as SWEEP's scanning speed will be reduced.

Configuring SWEEP to warn of compressed files

SWEEP can be configured to warn when it encounters compressed files.

Use the -WC command line qualifier. For example:

```
SWEEP A: -WC
```

SWEEP will report files compressed with ARC, ARJ, BOO, LZH, PAK, ZIP, ZOO, PKLite, ARJ self extract, LX 0.9X, LHarc, TopSpeed CRUNCH, PKARCK, BSA, LARC, LH, LZEXE, Diet and Cruncher, but will not decompress them.

Use this facility with care, as SWEEP's scanning speed will be reduced.

Checking dynamically compressed drives

Some utilities allow transparent dynamic compression of whole drives. These will not be accessible if the user boots up from a standard system floppy disk, as is usually the case before using SWEEP.

This section shows how to create system disks that make it possible to access and virus check drives compressed with *Drivespace* (supplied with MS-DOS 6), *Stacker* and *Superstor*.

Drives compressed with Drivespace (MS-DOS 6)

To create a bootable floppy disk use

```
FORMAT A: /S
```

while *Drivespace* compression is active.

As well as the two hidden system files (IBMBIO.SYS and IBMSYS.SYS or similar), the operating system automatically creates a third file DBLSPACE.BIN which contains the compression code.

After booting from such a system floppy disk, the compressed drive can be accessed and checked for viruses as normal.

Drives compressed with Stacker

Stacker uses a device driver which is loaded through CONFIG.SYS. So the procedure is as follows:

1. Format a bootable DOS system floppy disk using

   ```
   FORMAT A: /S
   ```

2. Copy the file C:\STACKER\STACKER.COM to the floppy disk.
3. Copy the file C:\STACKER\SSWAP.COM to the floppy disk.

4. The file CONFIG.SYS on the hard disk should have two lines which refer to STACKER and look like:

```
DEVICE=C:\STACKER\STACKER.COM C:\STACKVOL.DSK
DEVICE=C:\STACKER\SSWAP.COM C:\STACKVOL.DSK /SYNC
```

   These lines should be copied into CONFIG.SYS on the floppy disk, but the references to C:\STACKER should be replaced with A:\. The above file would read:

```
DEVICE=A:\STACKER.COM C:\STACKVOL.DSK
DEVICE=A:\SSWAP.COM C:\STACKVOL.DSK /SYNC
```

   It is important that no other parts of those lines are changed.

After booting from such a system disk, the compressed drive can be accessed and checked for viruses as normal.

Drives compressed with Superstor

1. Create a bootable floppy disk using the command

   ```
   FORMAT A: /S
   ```

2. The files SSTORDRV.SYS and DEVSWAP.COM should be copied to the floppy. The CONFIG.SYS file on the floppy should contain

   ```
   DEVICE=A:\SSTORDRV.SYS
   DEVICE=A:\DEVSWAP.COM
   FILES=20
   BUFFERS=20
   ```

After booting from such a system disk, the compressed drive can be accessed and checked for viruses as normal.

Full or quick sweeping

By default, ‘quick sweep’ is enabled. This checks only those parts of files likely to contain viruses and is

marginally less secure than checking the entire contents of files.

A ‘full sweep’ is available as an option. This checks the entire file contents and can be selected with the command line argument -F. For example, specifying

```
SWEEP -F B:
```

will perform a full sweep of drive B:.

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 when SWEEP is run. For example, if the current drive and directory is C:\PROGS and drive A: is being checked using the command

```
SWEEP 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). Thus, the -F command line qualifier must be used. For example

```
SWEEP C: -F
```

Running SWEEP from batch files

SWEEP returns error codes that can be tested by using the DOS '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 are 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' DOS command. For example

```
@ECHO OFF
SWEEP -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.

Remember that IF ERRORLEVEL means 'if level is greater or equal' to the specified value.

Customising the 'Viruses Found' report

SWEEP will produce a warning if it discovers one or more viruses. This warning can be customised, for example

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

by placing the appropriate text in the file SWEEP.MSG in the current directory.

To specify a different file name use the -FM command line qualifier.

Note that SW can also display a customised warning when SWEEP discovers viruses: see the 'Message if

virus found' section of the 'Using SWEEP with SW' chapter.

Virus disinfection

Common boot sector viruses can be removed from hard and floppy disks, and macro viruses from documents, by using SWEEPs built-in disinfection capability. To enable disinfection, the command line qualifier -DI must be used

```
SWEEP C: -DI
```

For a list of viruses which SWEEP can disinfect, consult the on-line virus database in SW (see the 'Virus library' section of the 'Using SWEEP with SW' chapter). For more information on disinfection, see the 'Treating viral infection' chapter.

SWEEP command line qualifiers

SWEEP accepts certain command line qualifiers to control and/or automate the sweeping process. These qualifiers are described in the following subsections, or can be listed using

```
SWEEP -?
```

The command format is

```
SWEEP drive1 ... driven file1 ... filen q1 ... qn
```

where

`drive1` to `driven` are the drives which will be checked (A:, B:, C: etc.) and '*:' denotes all hard drives

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

`q1` to `qn` are command line qualifiers (all beginning with either a hyphen '-' or a slash '/')

For example

```
SWEEP A: C:
```

will SWEEP the floppy disk in drive A: and hard drive C:.

@file Command line qualifiers from an external file

SWEEP can obtain its command line qualifiers from an external text file. For example, if a file called EXAMPLE.TXT contained the following text

```
*:
```

entering

```
SWEEP @EXAMPLE.TXT
```

would SWEEP all hard drives on the PC.

This feature is normally used to avoid exceeding command line length limitations.

-? Help

SWEEP will display all command line qualifiers along with 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 -6 command line qualifier.

-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, for example

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

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

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 current drive, unless they have an explicitly stated drive.

For example

```
SWEEP -AD=D:
```

would assume that all areas refer to drive D:.

-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

```
SWEEP A: -ALL
```

will check all files on drive A:.

Warning! This is a slow process which can cause false positives. It can also cause problems on file servers when SWEEP tries to open files already in use.

-AS Sweep standard areas

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

For example

```
SWEEP SUSPFILE.EXE -AS
```

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

-CI Check integrity

This command line qualifier causes SWEEP to perform an extra-stringent integrity check of SWEEP.EXE before executing (this is in addition to the standard integrity check). A change in the contents of SWEEP.EXE may indicate the presence of a virus or some other form of data corruption. Note that if a stealth virus is present in memory, as well as on SWEEP.EXE, no change in the integrity of SWEEP.EXE will be detected.

For example

```
SWEEP -CI
```

-D=<day|percentage> Execute only on day or percentage of times

SWEEP may be placed in the AUTOEXEC.BAT 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

```
SWEEP -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, e.g. MO for Monday, TU for Tuesday and so on.

Alternatively

```
SWEEP -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.

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.

For example

```
SWEEP -DA
```

-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 in the current directory.

For example

```
SWEEP -DE
```

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

For example

```
SWEEP -DE=sweep.da1
```

-DI Disinfect

This command line qualifier enables SWEEP to perform automatic disinfection of some boot sector and macro viruses. 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 will not actually check for them.

-DN Display names of files as they are scanned

This displays 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 are COM, DLL, DOC, DOT, EXE, OV?, SYS and XL?. This can be changed with the -EX command line qualifier.

For example

```
SWEEP -EX=COM,DOC,DOT,EXE,OV?,SYS,XL?
```

will remove DLL files from the list of executable files, and

```
SWEEP -EX=COM,DLL,DOC,DOT,EXE,OV?,SYS,VXD,XL?
```

will add the VXD extension.

-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.

For example

```
SWEEP -F
```

See also the ‘Full or quick sweeping’ section above.

-FM=<file> Specify message file

SWEEP will output the contents of the file specified with -FM=MESSAGEFILE to the screen if it discovers any 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

```
SWEEP -FM=MY_MSG.TXT
```

specifies the file ‘MY_MSG.TXT’.

-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

```
SWEEP -ICS -ICI=SECOND.INI
```

would specify SECOND.INI as the initialisation file.

-ICS[=<servername>] InterCheck server mode

This command line qualifier places SWEEP into InterCheck server mode. The name of the server is optional, and if it is not supplied the machine name is used.

For example

```
SWEEP -ICS=Server_1
```

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

-IF InterCheck file deletion

After a virus is discovered on a workstation, it may be desirable to purge the InterCheck checksum file (e.g. if the workstation has been infected after booting from a floppy, bypassing InterCheck). With the -IF qualifier, the InterCheck server will do this, so that all files will have to be rechecked. The option is not enabled by default.

For example

```
SWEEP -ICS -IF
```

-ME Check memory

By default, SWEEP will check memory for viruses. This qualifier is only necessary after memory checking has been switched off with the -NM command line qualifier.

-MU Check multiple disks

This allows the user to check a succession of floppy disks in a drive without reloading SWEEP.EXE every time.

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

```
SWEEP -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 the checking.

This will continue until *Esc* is pressed to interrupt the checking.

-NAF Do not read file with areas to be checked

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

-NAP Do not use internal virus patterns

By default, SWEEP will check for virus patterns built in by Sophos. With this command line 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 command line qualifier.

For example

```
SWEEP -NAP -F
```

-NAS Do not check standard areas

By default, SWEEP will check standard areas defined at compile time. Use this command line qualifier to prevent these areas from being checked (for example, if the areas to be checked have been defined 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 or virus fragment, 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.

-NDI Do not disinfect infected items

SWEEP will only try to disinfect infected items if the -DI command line qualifier is specified, so the -NDI qualifier is only necessary after a -DI has been used. This might, for example, be in a batch file or within a file specified by @file.

-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 lead to some polymorphic viruses not being found.

-NI No interrupting

Execution of SWEEP can normally be interrupted by pressing *Esc* or *Ctrl-C*. 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 -NK command line qualifier.

-NM No memory check

By default, SWEEP performs an intelligent memory check. If this command line qualifier is used, the memory is not checked.

-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

```
SWEEP -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.

For example, the output after entering

```
SWEEP -NS -NP
```

might include

```
Examining area 4: C:"All executables"
CONFIG.SYS
MSDOS.SYS
COMMAND.COM
IO.SYS
```

-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.

For example, the output after entering

```
SWEEP -NS
```

might include

```
Examining area 4: C:"All executables"
      C:\CONFIG.SYS
      C:\MSDOS.SYS
      C:\COMMAND.COM
      C:\IO.SYS
```

Note: This will also affect the information that is placed the security report, if such a report is to be created.

-NTW No Temp Warning

SWEEP will perform a check to ensure that either the TEMP or TMP environment variables point to a valid path in which SWEEP can create temporary files. A warning will be issued if this check fails. The -NTW option disables this feature.

-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

```
SWEEP -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 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 command line qualifier.

For example

```
SWEEP -PAT=23f78172bca918e1 -F
```

-PB Display progress bar

This qualifier enables SWEEP to display a progress bar.

Note: To do this, SWEEP has to count all the items to be swept before starting, so that a sweep takes slightly longer than otherwise. On very large network drives, this can have a significant impact on performance.

-PD Pause on discovery of a match

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

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.

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

For example

```
SWEEP 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

```
SWEEP -REMOVE
```

or

```
SWEEP -REMOVE -RS -NOC
```

-REMOVEF Remove infected files

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

-REMOVEB Disable infected boot sectors

As -REMOVE, except that infected files are not removed.

-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

```
SWEEP -REMOVE -RS
```

Note: Files overwritten when this option is used cannot be recovered.

-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 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: All files on disk (not just *.COM, *.EXE etc.) will be checked if the -WC command line qualifier is specified. This process can be very slow and is not recommended for file server drives.

Note: 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

```
SWEEP A: -WC
```

Scheduling SWEEP

This chapter describes how to schedule SWEEP with the AT utility.

Note: The AT utility is available only to users with DOS file server (site) licences.

Why schedule SWEEP?

Scheduling SWEEP makes it possible to carry out virus-checking at convenient times, for example when the network load is low.

Setting up a schedule in AT.INI

The SWEEP schedule and commands are defined in the AT.INI file.

The AT.INI must reside in the current directory of the current drive when AT.EXE is run. An alternative path and file can be specified in the command line when AT.EXE is started.

AT.INI is a text file containing two types of entries:

- **Action entries** specify what should happen.
- **Time entries** specify when it should happen. Time entries always specify the timing of the preceding Action entries.

Action entries start in the first column, while Time entries start with one or more *Spaces* or *Tabs*.

An example of an AT.INI file

For example, AT.INI could contain:

```
ECHO Meeting
  9:30 Mon,Thu
ECHO Lunch
  12:30 Mon,Tue,Wed,Thu,Fri
```

This would display 'Meeting' at 09:30 every Monday and Thursday and 'Lunch' every week day at 12:30.

Action entries in the AT.INI file

Action entries can start any DOS command, program or a batch file, and are passed on to the system exactly as entered in AT.INI.

It is possible to specify more than one Action entry to be associated with a Time entry. For example:

```
ECHO Here is a DIR at 09:00
DIR C:
  09:00 Mon
```

would cause the display of the text and the execution of the DIR command at 9:00 a.m. every Monday.

Important! No command executed by the AT command should require keyboard input since no further scheduled commands will be executed until the offending command terminates. When launching SWEEP, use the -NK command line qualifier, which prevents it from asking for user input.

For example

```
SWEEP F: -NK -P=SWEEP.LOG
  07:00
  19:00
```

would start SWEEP at 7:00 and 19:00 every day, storing the output in SWEEP.LOG file.

Time entries in the AT.INI file

Time entries refer to the preceding Action entries. A time entry must start with a *Tab* and consists of an (optional) time followed by an optional day or date.

Time is specified in 24-hour format and wildcard characters (?) are allowed. For example

```
ECHO Hello!
  7:00 Mon
  12:00 Mon,Tue,Wed,Thu,Fri
  ??:30
ECHO It's my birthday today!
  22/4
ECHO I am 30 today!
  22/4/98
```

would display ‘Hello!’ at 7:00 on Monday, at 12:00 on all workdays and at 30 minutes past each hour. It would also display ‘It's my birthday today!’ every 22nd April, while on 22nd April 1998 it would (also) display ‘I am 30 today’.

If a ‘+’ follows the time, it means ‘at that time or later’. For example:

```
ECHO Dinner
  19:00+
```

would display ‘Dinner’ when AT is executed at any time between 19:00 and 23:59.

Time entries can also contain a date, which may contain wildcards. For example:

```
SEND "It's the 5th!" TO EVERYBODY
  0:00 5/?/98
```

would execute the command ‘SEND’ at 0:00 on the 5th of every month during 1998.

Dates are specified in European style, i.e. day, month, year. Months can be spelled out, e.g. January, but the first 3 characters must be given.

Comments in the AT.INI file

Any entry can contain comments after ';' which are ignored. For example

```
; This is a comment
ECHO Good evening! ; a greeting
  19:00
```

Starting the scheduler

Important! AT.EXE must be running in order to execute scheduled commands. This is normally accomplished by running it as a background task within Windows or on a soft PC on the server.

To invoke AT, type 'AT' at the DOS command line. For example

```
C:> AT
```

AT command will read the AT.INI file at startup as well as whenever AT.INI is modified. This allows you to edit AT.INI in one Window while AT is running in the second one. When the new AT.INI is saved, AT will reread it and modify the scheduled events accordingly.

AT checks the syntax of AT.INI whenever it is read. If AT.INI is edited, it is possible to check that the syntax is right: simply save the file and run AT. If AT does not complain, the syntax is correct.

AT Command line qualifiers

AT command line qualifiers can be specified in the command line. For example

```
AT -SS MYFILE.INI
```

The qualifiers are as follows.

-NOW Execute all events now

When this is used, AT will execute all events from AT.INI file immediately. This option is used for testing.

-NP No pause

By default, the AT command waits until a scheduled event occurs. If the user wishes to check if any events are scheduled and not wait until a scheduled event occurs, the -NP qualifier is used.

For example, insert the command

```
AT -NP
```

in AUTOEXEC.BAT and edit the AT.INI file in the root directory to contain

```
ECHO Happy Christmas!
  25/12
```

AT will print out the message on 25th December and continue to execute the rest of the commands in AUTOEXEC.BAT.

-SS Super Silent mode

If this command line qualifier is used, AT will not display anything on the screen until a scheduled event occurs.

-? Display command line qualifiers

This causes AT to display command line qualifiers.

<filename> Alternative to AT.INI

It is possible to specify an alternative file which will be used instead of AT.INI by placing it in the command line. For example:

```
AT MYAT.INI
```

Example setup

This example shows how to set up SWEEP to check network drives F: and G: automatically every day at 07:00, 13:00 and 19:00 plus 22:00 on Fridays.

This will be done within Windows (the PC must, of course, be left on 24 hours per day).

The report will be sent to F:\REP\SWEEP.LOG and if SWEEP discovers a virus, the SUPERVISOR will be paged (providing the system supports the PAGE command).

SWEEP.EXE and AT.EXE are assumed to be in the F:\SWEEP directory.

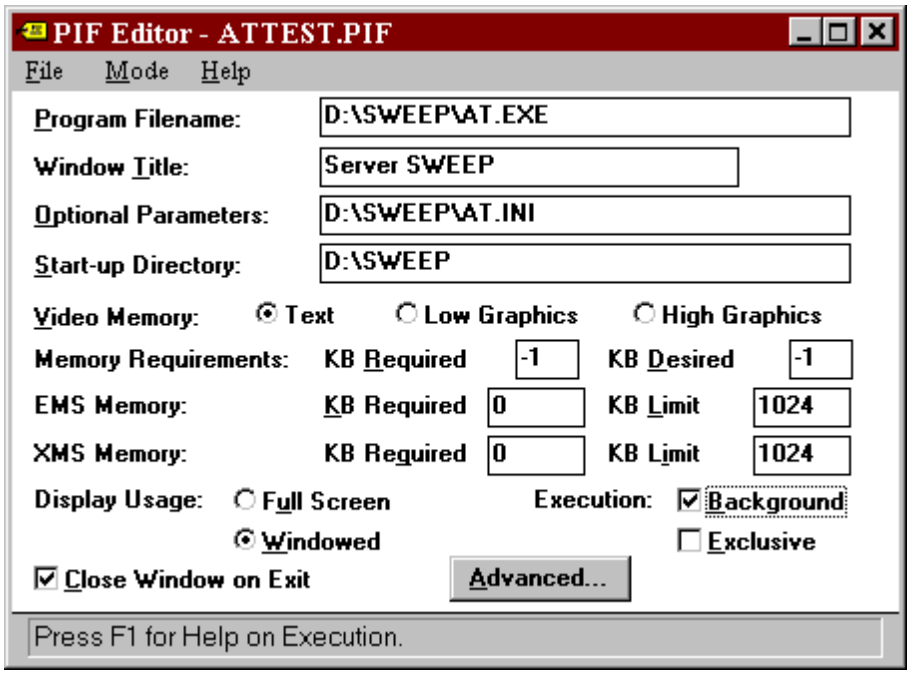
Using a text editor, edit F:\AT.INI to contain the following text:

```
F:\SWEEP\MYSCAN.BAT
  07:00
  13:00
  19:00
  22:00 Fri
```

Create and edit the file F:\SWEEP\MYSCAN.BAT to contain the following commands:

```
SWEEP F: G: -NK -P=F:\REP\SWEEP.LOG
IF ERRORLEVEL 3 GOTO VIRUS
GOTO END
:VIRUS
PAGE SUPERVISOR "Virus alert!"
:END
```

From within Windows use the PIF editor to create the file AT.PIF with the following specifications:

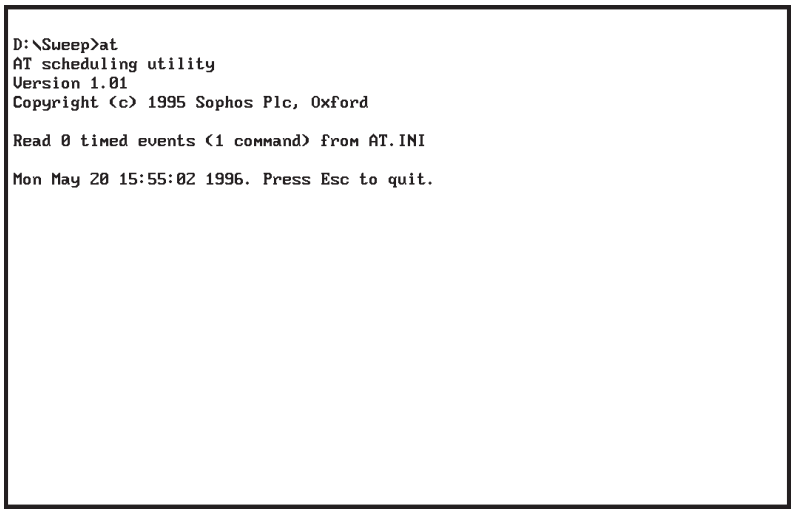


Save the file.

Open *StartUp* group in Windows.

Using File manager pick up AT.PIF and drag it to the *StartUp* group.

Test the correct functioning of AT by double clicking on it. This should start the AT command and the DOS box will show the current time and date.



When the next scheduled event is due, AT will load SWEEP and execute it.

Since the icon has been placed in the *StartUp* group, the scheduled process will be restarted automatically whenever Windows is started.

Installing SWEEP as an InterCheck server

This chapter shows how to install SWEEP as an InterCheck server and how to upgrade this installation.

Important! Instructions refer to Sophos Anti-Virus floppy disks. If using a Sophos Anti-Virus CD, either make Sophos Anti-Virus floppy disks with the utility supplied, or use the DOS directory on the CD.

Why install SWEEP as an InterCheck server?

Installing SWEEP for DOS as an InterCheck server enables on-access scanning of connected workstations that are configured as InterCheck clients.

This is necessary only on networks for which Sophos Anti-Virus does not offer a 'native' InterCheck server, e.g. networks with **Windows for Workgroups, Windows 95, LANtastic, NetWare Lite** and **UNIX (NFS) file servers**.

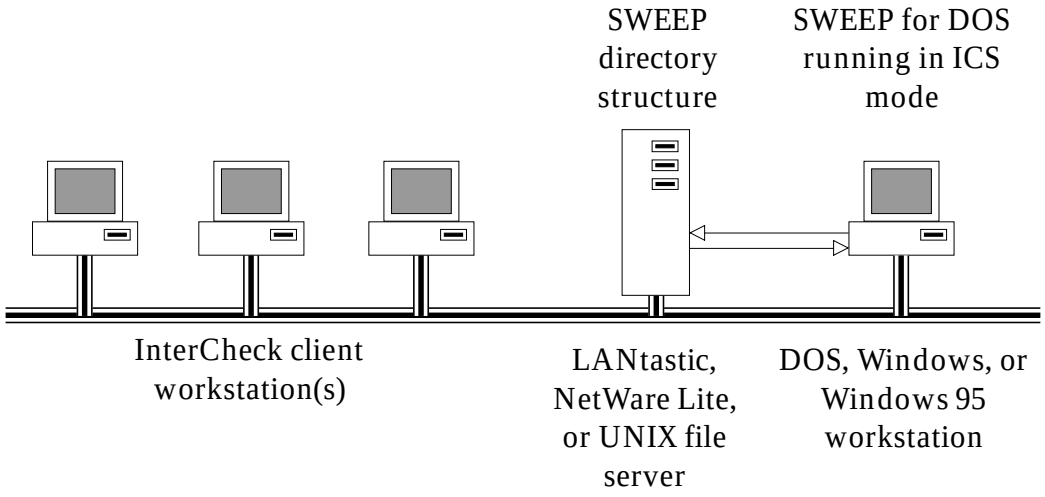
Summary of the installation procedure

This section summarizes the installation procedure. Specific instructions for different operating systems appear in the sections below.

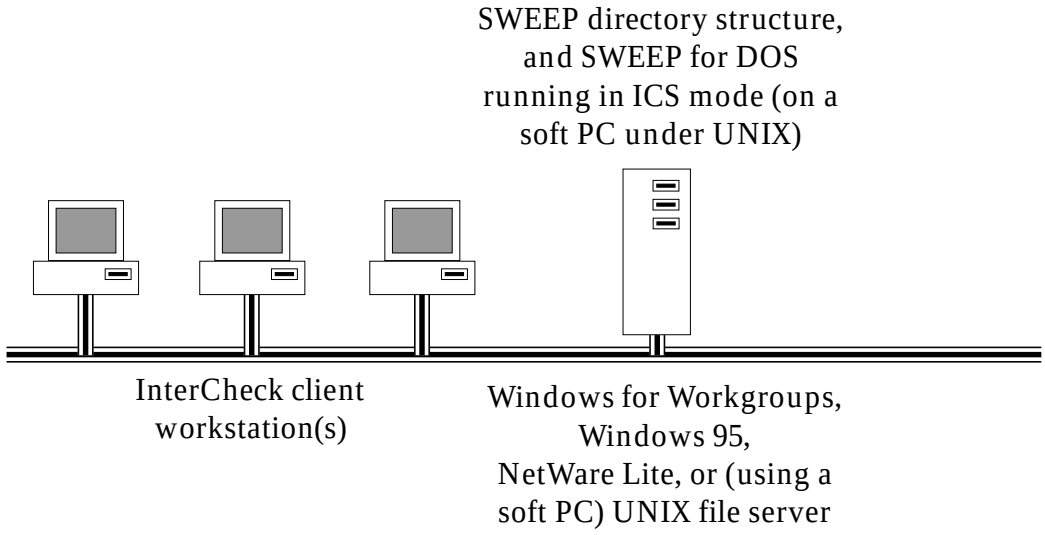
The main steps

1. Create the SWEEP directory structure on the file server, and copy the SWEEP for DOS, InterCheck and ICONTROL floppy disks to these directories.

2. Create the InterCheck configuration files in the SWEEP directory.
3. Set the access rights to the SWEEP directory structure (see 'The SWEEP directory structure' and the operating system specific instructions).
4. Run SWEEP for DOS in InterCheck server mode from that directory. This can be done from a dedicated workstation connected to the file server, or from the file server itself. The latter option, if available, will decrease network traffic.



InterCheck server running on a dedicated workstation



InterCheck server running on the file server

The SWEEP directory structure

The SWEEP directory structure consists of the main SWEEP directory and the following subdirectories:

COMMS	Used for communication between InterCheck clients and the server.
INFECTED	Used for storing infected items for later analysis.
LISTS	Used for keeping the checksum files when clients are diskless workstations.

All versions require the DOS utility SHARE installed on the server and the workstations. Note that Windows 95 uses SHARE by default. If in doubt as to whether SHARE is present, use a text editor to examine AUTOEXEC.BAT. If SHARE is not present, insert the line

```
SHARE
```

immediately after the PATH statement, save AUTOEXEC.BAT and reboot the computer.

Installing the InterCheck server on Windows for Workgroups and Windows 95 servers

Setting up the directories

From a DOS prompt, set up the following directories on a drive that is visible to the client workstations:

```
MD \SWEEP
MD \SWEEP\COMMS
MD \SWEEP\INFECTED
MD \SWEEP\LISTS
```

The contents of the SWEEP for DOS, InterCheck and ICONTROL floppy disks should be copied into the \SWEEP directory, for example by entering

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

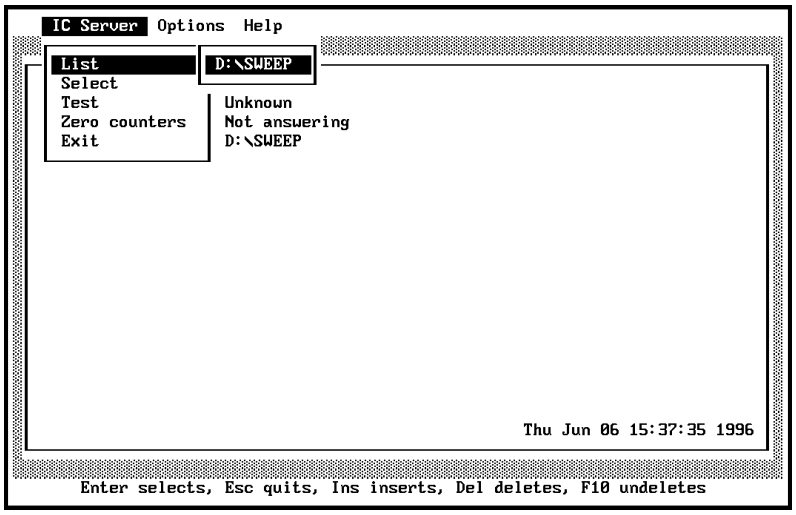
with each disk in drive A: in turn.

Creating the configuration files

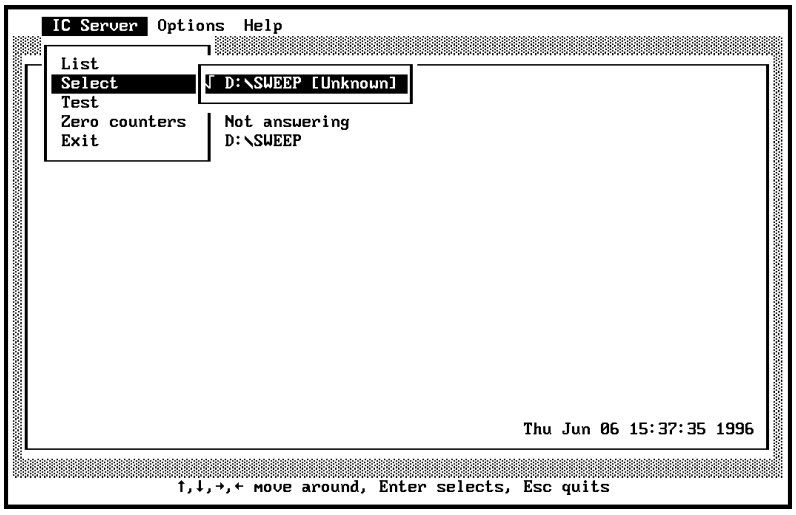
Make the \SWEEP directory current and start ICONTROL, for example by entering at a DOS prompt

```
CD \SWEEP
ICONTROL
```

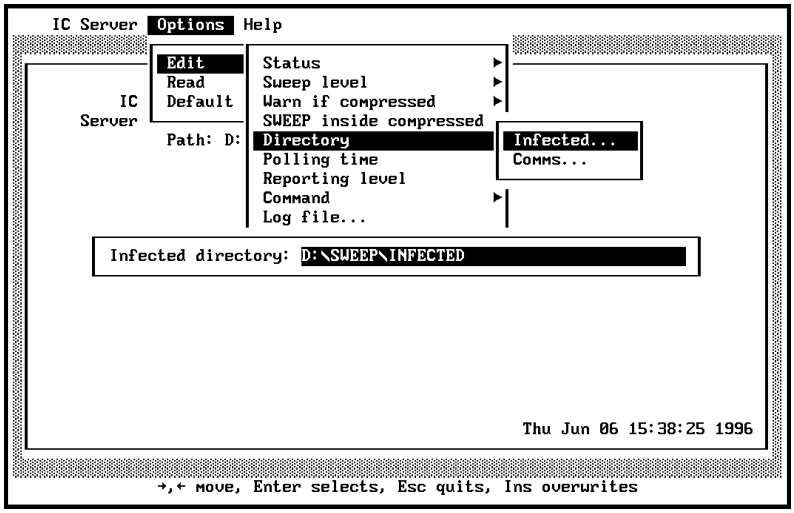
Select *List* from the *IC Server* menu. This should contain the correct drive and path of the \SWEEP directory.



Select *Select* from the *IC Server* menu and confirm that the same path is selected while the server name is shown as [Unknown].



From the *Options* menu select *Edit*, followed by *Directory* and then *Infected*.



Check that the correct drive and path of the INFECTED directory is specified. Repeat the operation with the COMMS directory.

Select *Exit* from the *IC Server* menu and save the ICONTROL configuration changes.

Using a text editor, create the INTERCHK.CFG (InterCheck client configuration) file in the SWEEP directory. Insert the lines

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

and save the file. See the 'Configuring InterCheck clients' chapter for further configuration options.

Setting the access rights

This is not relevant when SWEEP for DOS is running as an InterCheck server under DOS, Windows 3.x, Windows for Workgroups or Windows 95.

Starting the InterCheck server

The SWEEP directory contains a Program Information File called ICSERVER.PIF (originally

from the ICONTROL floppy disk), which contains the following settings:

Program Filename:	\SWEEP\SWEEP.EXE
Window Title:	IC Server
Optional Parameters:	-ICS=*ServerName*
Start-up Directory:	\SWEEP
Memory Requirements:	KB Required: -1
Display Usage:	Windowed
Execution:	Background, Non-exclusive

Background priority (advanced options): 100

Windows for Workgroups

ICSERVER.PIF can be executed at any time to start SWEEP for DOS in InterCheck server mode.

To start the InterCheck server when the Windows machine starts Windows, pick up ICSERVER.PIF in File Manager and drag it to the *StartUp* group.

Select the ICSERVER icon by single-clicking it, then select *File* followed by *Properties*. If *Run Minimised* is selected, the server process will be represented by an icon instead of a full DOS box. Under *Description* enter 'IC Server'.

Restart Windows and verify that the 'IC Server' box appears with SWEEP running in it.

Windows 95

Under Windows 95, the ICSERVER.PIF file will appear in Explorer as a shortcut to an MS-DOS program. This shortcut can be executed in the normal way to start SWEEP for DOS in InterCheck server mode, and can be placed in the Windows 95 Taskbar or Startup folder or on the Desktop.

Controlling the InterCheck server

This is performed with ICONTROL, as described in the 'Controlling the InterCheck server' chapter.

Stopping the InterCheck server

To terminate the ICSERVER process:

Windows for Workgroups

Click on the ICSERVER icon (or box if it is already displayed) and press *Esc*.

Windows 95

Press *Esc* while the SWEEP DOS box is active.

Installing the InterCheck server on a LANtastic file server

Setting up the directories

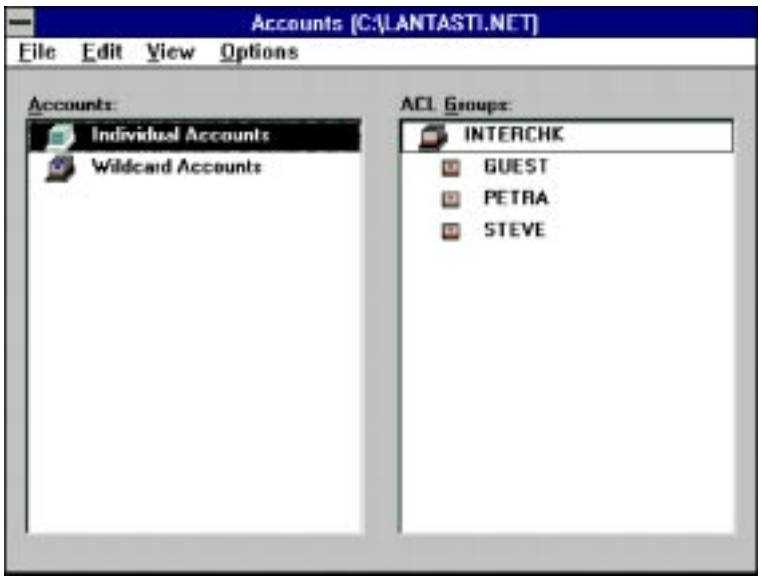
On the server, create a directory called SWEEP and subdirectories of this called COMMS, INFECTED and LISTS.

Copy the contents of the SWEEP for DOS floppy disk, the InterCheck floppy disk and the ICONTROL floppy disk into the SWEEP directory.

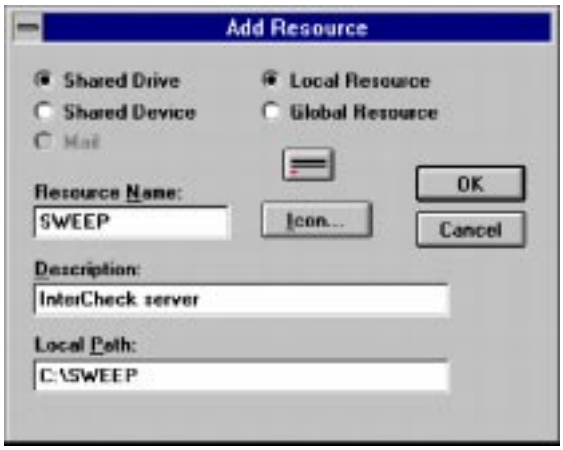
Setting the access rights

Before InterCheck services can be provided, an INTERCHK ACL group must be created using the LANtastic Network Manager.

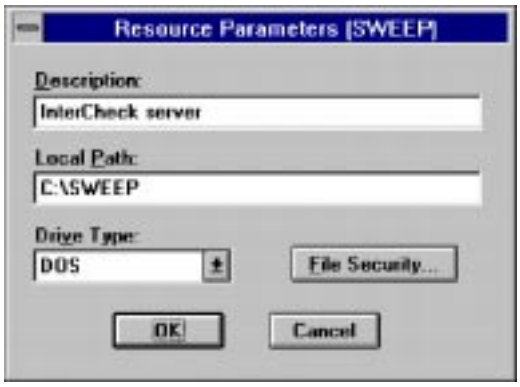
All users who will use InterCheck should be added to this ACL group.



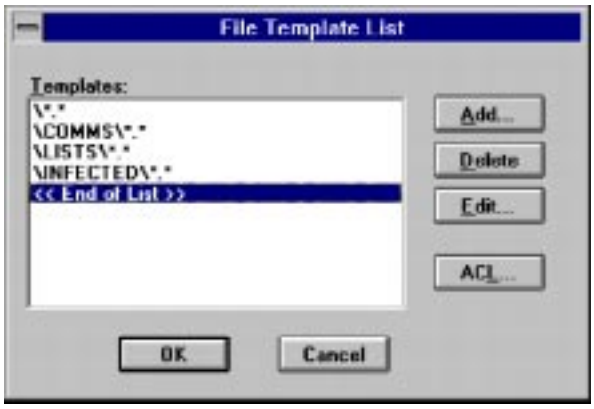
Using the resources option from the LANtastic Network Manager, create a shared drive local resource called SWEEP. The local path for the resource should point to the SWEEP directory on the InterCheck server.



Once the resource has been created, modify it.



Select File Security and add the following templates:



The ACL for each template should be:

	INTERCHK	**Other users**
.	RLE	<NONE>
\COMMS*.*	Default	<NONE>
\INFECTED*.*	<NONE>	<NONE>
\LISTS*.*	Default	<NONE>

In a multi-server network, an INTERCHK ACL group and a global resource for SWEEP can be defined on each server not running an InterCheck server process. Each global resource should specify a server that is running the InterCheck server process. InterCheck users should be placed in each INTERCHK ACL group.

Creating the configuration files

Make the \SWEEP directory current and start ICONTROL, for example by entering at a DOS prompt

```
CD \SWEEP
ICONTROL
```

Select *List* from the *IC Server* menu. This should contain the correct drive and path of the \SWEEP directory.

Select *Select* from the *IC Server* menu and confirm that the same path is selected while the server name is shown as [Unknown].

From the *Options* menu select *Edit*, followed by *Directory* and then *Infected*.

Check that the correct drive and path of the INFECTED directory is specified. Repeat the operation with the COMMS directory.

Select *Exit* from the *IC Server* menu and save the ICONTROL configuration changes.

An INTERCHK.CFG configuration file must be created in the same directory. The minimum contents of this file should be:

```
[InterCheckGlobal]
Exclude=CONFIG.SYS
CommsDirectory=W:\COMMS
```

See the 'Configuring InterCheck clients' chapter for further configuration options.

All users who log in to the InterCheck server must use the same drive letter to map to the SWEEP directory on the server. This drive should be the same as the one in the INTERCHK.CFG file:

```
NET USE W: \\intercheck_one\sweep
```

Starting the InterCheck server

From a DOS prompt, change to the drive and directory containing the InterCheck files, and enter:

```
SWEEP -ICS=ServerName
```

where *ServerName* is the name for the InterCheck server.

Controlling the InterCheck server

This is performed with ICONTROL, as described in the 'Controlling the InterCheck server' chapter. However, the 'DOS command on virus discovery' and 'DOS command to get user name' ICONTROL options are dependent on the InterCheck server operating system.

Command on virus discovery

Use the NET SEND command inside a batch file similar to:

```
NET SEND * "<text>" * <user>
```

where <user> is the user to be notified. For example:

```
NET SEND * "Virus %1 discovered at %3" * supervisor
```

would send the above message to the supervisor in case of a virus discovery.

Command to get user name

LANtastic does not provide a mechanism for obtaining the userid of the file owner.

Stopping the InterCheck server

At the DOS prompt where SWEEP for DOS is running in InterCheck server mode, press *Esc*.

Installing the InterCheck server on a NetWare Lite file server

Setting up the directories

On the server, create a directory called SWEEP and subdirectories of this called COMMS, INFECTED and LISTS.

Copy the contents of the SWEEP for DOS floppy disk, the InterCheck floppy disk and the ICONTROL floppy disk into the SWEEP directory.

Creating the configuration files

Run ICONTROL once to create a SWEEPIC.INI.

In the SWEEP directory create a text file INTERCHK.CFG containing the two following lines:

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

See the ‘Configuring InterCheck clients’ chapter for further configuration options.

Setting the access rights

Log in to the network as supervisor, then run the NET program. Select *Supervise the Network* then *Network Directories*.

Press *Ins* to add a new shared directory.

In the next menu box, select the name of the server on which SWEEP has just been installed. Press *Enter*.

Enter a name for this network share, e.g. INTERCHK, then press *Enter*.

In the next dialog box, enter the full pathname of the SWEEP directory created earlier. Ensure that the default access rights are set to ALL. No users will need nondefault rights.

Press *Esc* and select *Yes* to confirm that this new setting is to be saved. The new network directory should appear in the list.

Press *Esc* repeatedly to exit the NET program.

Starting the InterCheck server

It is recommended that the InterCheck server is run on the NetWare Lite server on which the software is installed. This will minimise network traffic.

Running the InterCheck server on the NetWare Lite server

Change directory to the SWEEP directory, and start the InterCheck server by typing

```
SWEEP -ICS=ServerName
```

where *ServerName* is the name for the InterCheck server.

Running the InterCheck server on a NetWare Lite client

Map a drive to the INTERCHK network directory:

```
NET MAP drive: INTERCHK
```

Make that drive current.

Use a text editor such as DOS EDIT to check the SWEEPIC.INI file. Ensure that the lines beginning InfectedDirectory and CommsDirectory read as follows:

```
InfectedDirectory=drive:\INFECTED
CommsDirectory=drive:\COMMS
```

Start the InterCheck server by issuing the command

```
SWEEP -ICS=ServerName
```

where *ServerName* is the name for the InterCheck server.

Windows issues

The InterCheck server will run under Windows on a NetWare Lite Server and a NetWare Lite Client. Bear in mind, though, that a machine running the InterCheck server in a Windows DOS box will not be protected itself. Individual DOS sessions can be protected by running InterCheck after starting, but no Windows files will be automatically checked on that machine. Make sure that the PIF associated with the server task has the Background execution box set.

Clients that run InterCheck before entering Windows will have full InterCheck protection.

Controlling the InterCheck server

This is performed with ICONTROL, as described in the 'Controlling the InterCheck server' chapter. However, the 'DOS command on virus discovery' and 'DOS command to get user name' ICONTROL options are dependent on the InterCheck server operating system.

Command on virus discovery

The suggested batch file is:

```
NET SEND "InterCheck Alert: Server ServerName" UserName
```

where *ServerName* is the name of the NetWare Lite server on which the InterCheck server is running, and *UserName* is the name of the user who should

receive these alerts. It is possible to specify multiple user names.

There is a limit of 30 characters in a NetWare Lite message. If that is exceeded, the NET SEND program asks for confirmation before sending a truncated version of the message. On an unattended server, this will cause the InterCheck system to seize up.

Command to get user name

This is not possible in any greater depth than is provided by the InterCheck client. NetWare Lite is a DOS based utility and as such stores no information about file ownership.

Stopping the InterCheck server

At the DOS prompt where SWEEP for DOS is running in InterCheck server mode, press *Esc*.

Installing the InterCheck server on a UNIX (NFS) file server

Note: To install the InterCheck server on a UNIX machine, a PC NFS daemon which supports file locking is required.

Setting up the directories

The following procedure assumes that the UNIX directory exported as a network drive is /export/pc.

InterCheck needs to run as a user; hence it is necessary to create the user *interchk*. Procedures for this differ depending on the operating system version. Having created the user *interchk*, log in as *root* and enter:

```
mkdir /export/pc/sweep
cd /export/pc/sweep
mkdir comms
mkdir infected
mkdir lists
```

Copy the contents of the SWEEP for DOS floppy disk, the InterCheck floppy disk and the ICONTROL floppy disk into the /export/pc/sweep directory.

Creating the configuration files

Run ICONTROL once to create a SWEEPIC.INI.

In the SWEEP directory create a text file INTERCHK.CFG containing the two following lines:

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

See the 'Configuring InterCheck clients' chapter for further configuration options.

Setting the access rights

From a PC connected to the network log in as *interchk*. Access privileges to the four directories should apply to all users of InterCheck and should be set as follows:

	Owner	**Group**	**World**
/sweep	rwx	rx	rx
/sweep/comms	rwx	rwx	rwx
/sweep/infected	rwx	-	-
/sweep/lists	rwx	rwx	rwx

To do this, log in as *interchk*, and enter:

```
su interchk
chmod 755 /export/pc/sweep
chown interchk /export/pc/sweep
cd /export/pc/sweep
chmod 777 comms
chmod 700 infected
chmod 777 lists
```

Make sure that the NFS file lock daemon is loaded and that PCs mount NFS directories using file locking.

Starting the InterCheck server

There are two ways in which SWEEP for DOS can be run as an InterCheck server: in a DOS emulator on the UNIX server, or on a dedicated DOS workstation connected to the UNIX server. The former option will minimise network traffic.

Running the InterCheck server on the UNIX server

In a DOS emulator on the UNIX machine, change directory to the SWEEP directory.

Start the InterCheck server by typing

```
SWEEP -ICS=ServerName
```

where *ServerName* is the name for the InterCheck server.

Running the InterCheck server on a UNIX client

On a client PC, map a drive to the SWEEP network directory and make that drive current.

Use a text editor such as DOS EDIT to check the SWEEPIC.INI file. Ensure that the lines beginning InfectedDirectory and CommsDirectory read as follows:

```
InfectedDirectory=drive:\INFECTED
CommsDirectory=drive:\COMMS
```

where *drive* is the name of the mapped drive. Start the InterCheck server by issuing the command

```
SWEEP -ICS=ServerName
```

where *ServerName* is the name for the InterCheck server.

Controlling the InterCheck server

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

However, the 'DOS command on virus discovery' and 'DOS command to get user name' ICONTROL options are dependent on the InterCheck server operating system.

Command on virus discovery

NFS does not provide a simple universal mail system for sending messages to users. Notification of designated users is system-dependent.

Command to get user name

Derivation of the name of the userid of the file owner is best accomplished by using the PC-NFS command LS.EXE in combination with a small 'C' program. The user name is written to the file F:\SWEEP\SWEEP.USR:

```
LS -L %1 | NAME >F:\SWEEP\SWEEP.USR
```

The program name.c is:

```
#include <stdio.h>

#define NAME_STARTING_CHAR 14

void main() {

      int i,c;

      for(i=0;i<NAME_STARTING_CHAR;i++) (void)getchar();
      while ((c=getchar())!=' ') putchar(c);
}
```

name.c should be compiled using a DOS C compiler.

Stopping the InterCheck server

At the DOS prompt where SWEEP for DOS is running in InterCheck server mode, press *Esc*.

Installing the InterCheck clients

When SWEEP has been installed as an InterCheck server, there is a further step to take before

workstations on the network can benefit from on-access scanning. This is the installation of the InterCheck client software, which identifies files not previously scanned and sends them to the InterCheck server. For instructions, see the 'Installing InterCheck clients' chapter.

Updating SWEEP used as an InterCheck server

In an InterCheck system, the only items that need to be updated are the DOS SWEEP executables held on the server. The client software on the workstations is updated automatically.

To update SWEEP:

1. Copy the contents of the latest SWEEP disk into the SWEEP directory on the server, as described in the relevant 'Setting up the directories' section above.
2. Stop the InterCheck server, as described in the relevant 'Stopping the InterCheck server' section above.
3. Restart SWEEP in InterCheck server mode, as described in the relevant 'Starting the InterCheck server' section above.

InterCheck services will be resumed immediately.

Installing InterCheck clients

This chapter describes how to install and run InterCheck clients.

Note: For information on installing the stand-alone Windows 95 and Windows NT InterCheck clients, see the Sophos Anti-Virus user manuals for Windows 95 and Windows NT.

Important! Instructions refer to Sophos Anti-Virus floppy disks. If using a Sophos Anti-Virus CD, either make Sophos Anti-Virus floppy disks with the utility supplied, or use the DOS directory on the CD.

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, Windows 95 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, DOS/Windows 3.x, and Windows for Workgroups workstations. See the 'Installing stand-alone InterCheck clients' section below.

Installing networked InterCheck clients

Before installing networked InterCheck clients:

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

   This installs the InterCheck server and makes the InterCheck files available for installation.

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 the 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. Note that 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 and Windows

With a login script

Locate the users' login batch file and include the following:

```
I:\ICLOGIN
```

where I: is mapped to the directory on the server in which SWEEP is installed.

InterCheck will start on the client workstation when it logs in to the network.

Without a login script

Ensure that the directory on the file server that contains the InterCheck files is permanently mapped to a DOS drive.

Execute the DOS InterCheck executable (INTERCHK.EXE) after the workstation has made a connection to the network, for example by adding the line

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

to the workstation's AUTOEXEC.BAT file if the InterCheck executables are stored in I:\SWEEP.

Networked InterCheck clients for Windows 95

With a login script

See the instructions in the 'With a login script' subsection of the 'Networked InterCheck clients for DOS and Windows' section above.

Without a login script

Execute the Windows 95 InterCheck executable (ICWIN95.EXE) after the workstation has made a connection to the network.

InterCheck cannot be started with AUTOEXEC.BAT under Windows 95, but it can be placed in the Startup folder to make it start automatically every time Windows 95 is started.

To do this, select *Settings* and then *Taskbar* from the Windows 95 Start menu. Click the *Start Menu Programs* tab and then the *Add* button.

Enter the location of the network copy of the ICWIN95.EXE program into the dialog box, and click *Next*. Then select a folder to place the new shortcut in. Select *StartUp* and then *Next*. Finally, select *Finish* to add ICWIN95.

Networked InterCheck clients for Macintosh

The Macintosh 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

See the installation instructions in 'Stand-alone InterCheck client for DOS/Windows' in the 'Installing InterCheck on-access scanning for a workstation' section of the 'Installing SWEEP' chapter.

Stand-alone InterCheck clients for Windows for Workgroups

For Windows for Workgroups (WFWG) workstations which log in to the network **after** starting Windows, follow the installation procedure below.

For WFWG workstations that log in to the network **before** starting Windows, see the 'Networked InterCheck clients for DOS and Windows' subsection of the 'Installing networked InterCheck clients' section.

For WFWG workstations that are not connected to a network, see the 'Starting ICINSTAL' subsection of the 'Stand-alone InterCheck clients for DOS/Windows' section.

Before installing the InterCheck client

Before installing the InterCheck client on WFWG workstations which log in to the network after starting Windows, there are three issues to consider:

Configuring the InterCheck client

If changes are to be made to the way the InterCheck client is configured, they must be entered in the InterCheck configuration file (INTERCHK.CFG) before installation. Otherwise, InterCheck will be installed with the default configuration. See the 'Configuring InterCheck clients' chapter for more information.

Automatic or manual installation?

There are two ways to run the installation program:

1. Automatically from a login script. This can be used to install the InterCheck client without having to visit each individual workstation. See the 'Installing automatically from a login script' section below.
2. Manually from each client. This approach is generally used when no login script is available. See the 'Installing manually from the client' section below.

Interactive or non-interactive installation?

Both methods of installation can be used interactively, as described in the 'Interactive installation' section below. This might be necessary if an individual client configuration is non-standard, or if the users require more control over the installation and update process. See the 'Interactive installation' section below.

Installing automatically from a login script

Run ICLOGIN with the -A option from the workstation's login script.

For example

```
I:\ICLOGIN -A
```

if the DOS drive I: is mapped to the directory on the server that contains the InterCheck files.This must be a permanent drive mapping.

The next time that the workstation logs in to the network, the login program will instruct Windows for Workgroups to run the InterCheck installation program. The installation program will install InterCheck to the local machine, and then automatically start the InterCheck client.

Alternatively, if a permanent mapping to a drive is not required or not possible, and if the file server supports UNC (Universal Naming Convention), use ICLOGIN with the -U command line qualifier and then remove the connection to the drive. The -U option makes ICLOGIN translate all the drive specifications to UNC format, removing any dependency on the initial drive mapping.

Installing manually from the client

On the client workstation, select *Run* from the Windows for Workgroups *File* menu and enter

```
I:\ICSETUPW.EXE
```

if the DOS drive I: is mapped to the directory on the server that contains the InterCheck files. This must be a permanent drive mapping.

Alternatively, if a permanent connection to a DOS drive is not available or not desired, enter in the Run dialog box

```
\\servername\directory\ICSETUPW.EXE
```

where *servername* and *directory* are the names of the server and the directory containing the InterCheck files.

The installation program will copy all the InterCheck client files to a directory called C:\INTERCHK on the client workstation. After a successful installation, it will restart the workstation and then start the InterCheck client.

Interactive installation

There are two ways of running ICSETUPW interactively:

1. Include the lines

```
[InstallOptions]
InteractiveInstall=1
```

in the InterCheck configuration file (INTERCHK.CFG) and run ICSETUPW. This is the only way of achieving interactive installation when a login script is used.

2. Run ICSETUPW.EXE with the -I command line qualifier. For example, if installing manually from the client, select *Run* from the *File* menu and enter

   ```
   ICSETUPW -I
   ```

When the installation program is run from a login script in interactive mode, the next time that the workstation logs in to the network the installation program will be presented to the user. The user is given the option of postponing the installation.

When the installation program is run either from a login script or manually from the client, the user is given the option to abort the process at all stages. The installation program will step through the configuration options available. No modifications will be made on the workstation until the user clicks *Finish* on the last page. The installation program will then copy all the InterCheck client files to the specified directory on the client workstation. It will then restart the workstation and start the InterCheck client.

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 configure and control SWEEP for DOS 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 DOS, Banyan VINES or 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 SWEEP as an 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

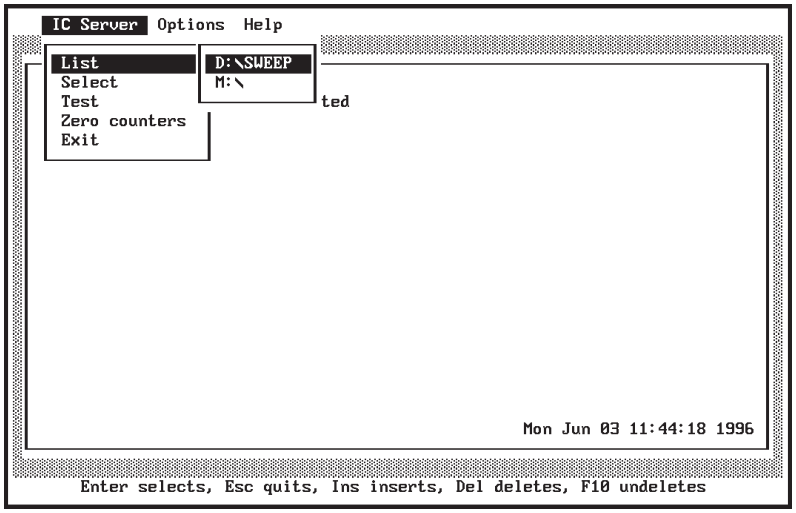
```
D:\SWEEP\ICONTROL
```

to start ICONTROL.

Selecting the InterCheck server

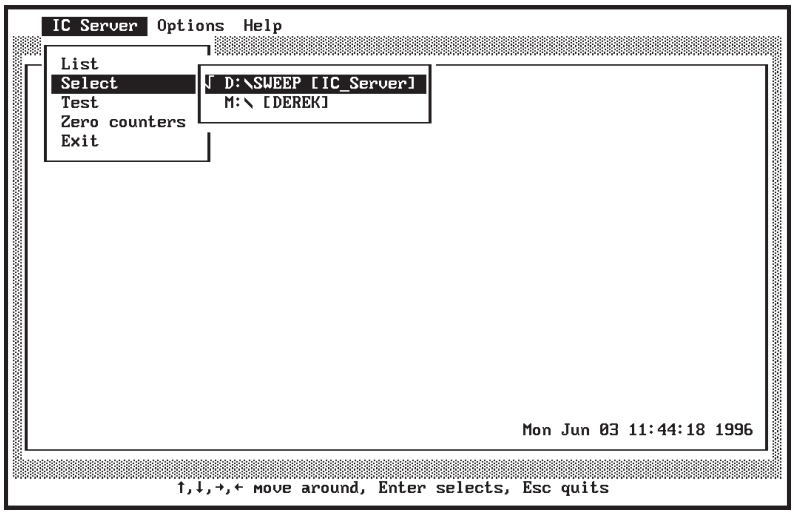
One or more InterCheck server processes can be controlled using ICONTROL under DOS, although only one InterCheck server can be selected and hence monitored at one time.

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

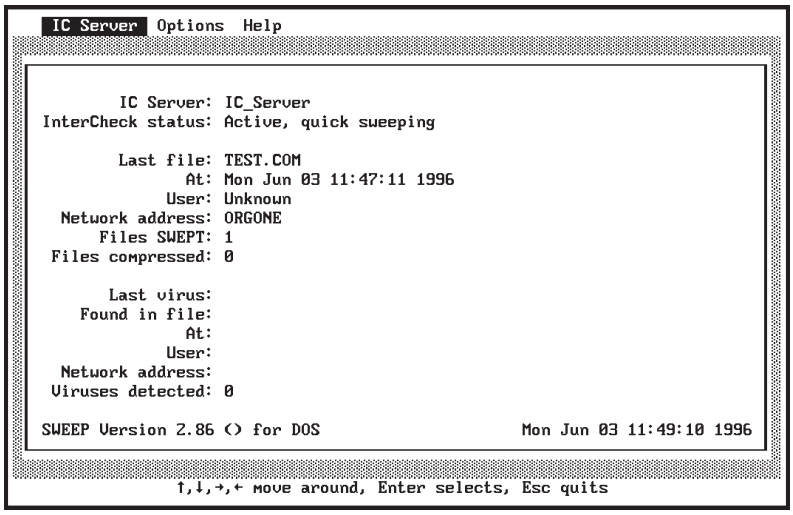


If there is no entry with the correct drive and path, press the *Insert* key and enter the appropriate details, or press *Enter* to edit an existing entry.

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

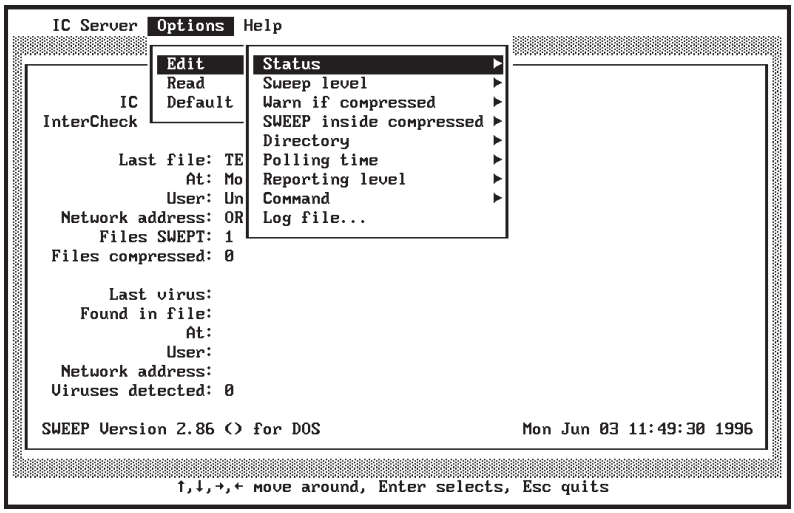
Select *Test* from the *IC Server* menu to test the communication between ICONTROL and the selected InterCheck server. The test server dialog is displayed and updated throughout the process until the outcome is displayed.

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, because 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 SWEEP as an

InterCheck server' chapter), and it is unlikely that they will have to be changed subsequently. Note also that they cannot be changed if a Banyan VINES InterCheck server is being used.

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 a DOS or 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 version 3 does not provide a mechanism for obtaining the userid of the file owner.

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

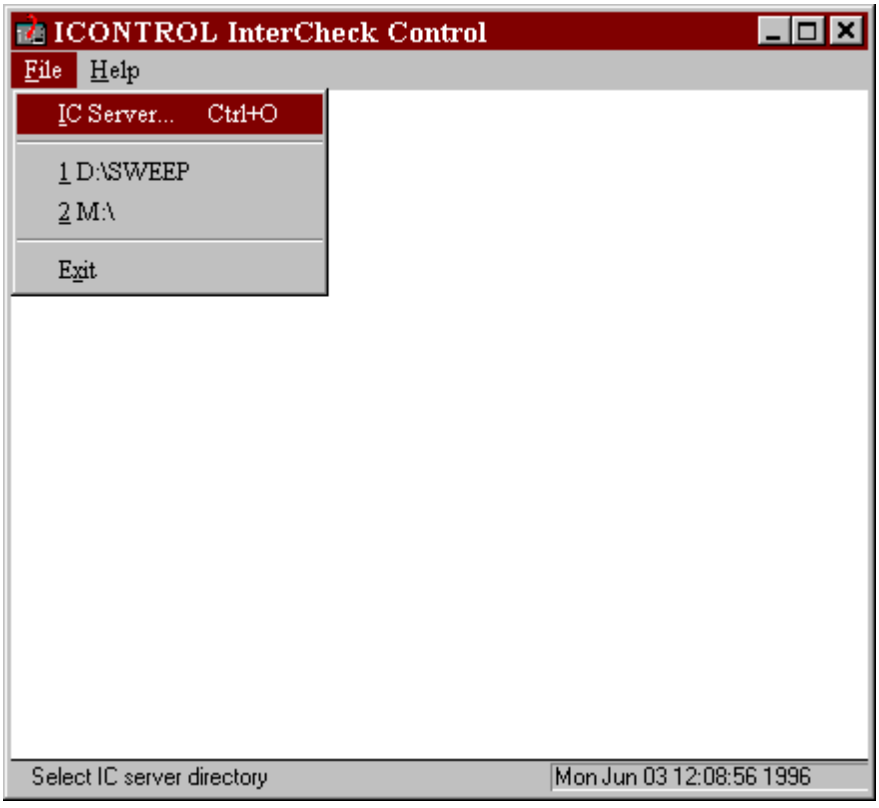
Starting ICONTROL

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

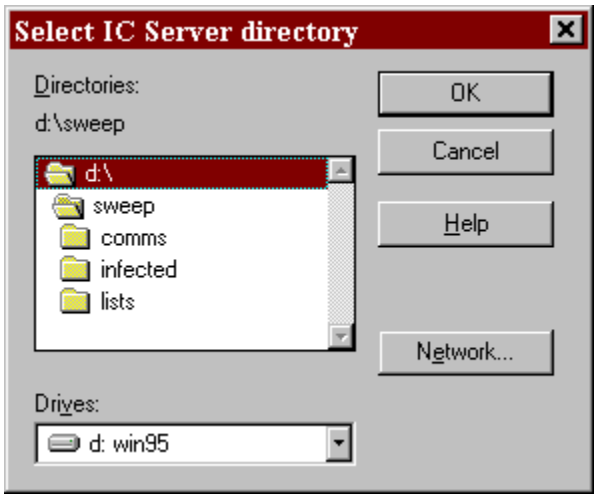
Note that ICW.EXE can be placed in, and launched from, a Windows 3.x Program Group or the Windows 95 Taskbar in the same way as any other Windows executable.

Selecting the InterCheck server

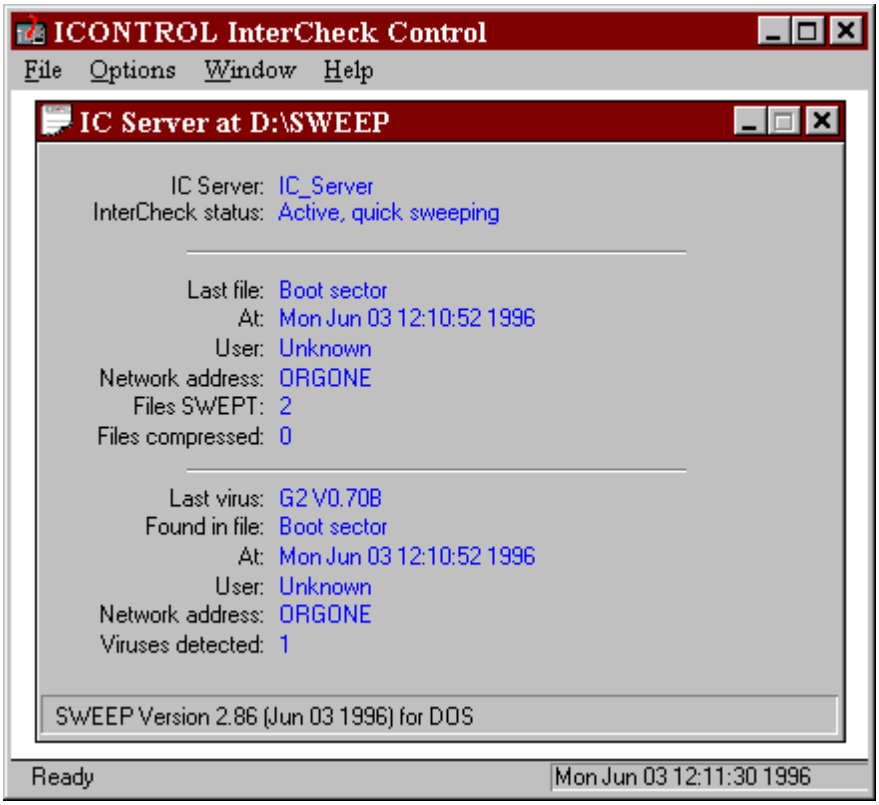
Choose *IC Server* from the *File* menu



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

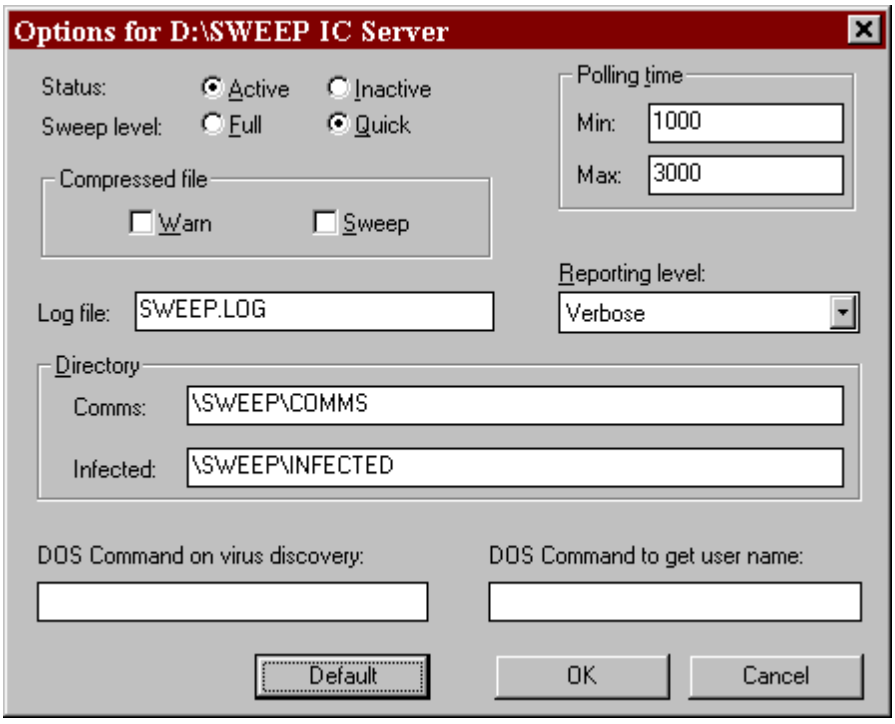
for DOS, ICONTROL for Windows can monitor multiple servers at the same time.

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'.

Starting a SWEEP InterCheck server automatically

SWEEP can be started as an InterCheck server automatically by ICONTROL for Windows under Windows 3.1, Windows for Workgroups and Windows 95. This is not available in OS/2.

ICONTROL will load SWEEP.EXE as an InterCheck server in hidden mode if the ICW.INI file (stored in the WINDOWS or WIN95 directory) contains an entry such as the following under the [Application Settings] section:

```
ICServer=D:\SWEEP\SWEEP.EXE, -ICS=ServerName, D:\SWEEP
```

All three parameters must be stated. The first parameter specifies the SWEEP executable which will be run in server mode, the second specifies the command line qualifier SWEEP.EXE needs to start in InterCheck server mode, and the third specifies the working InterCheck server path.

The directory from which SWEEP is run in InterCheck server mode must contain a SWEEPIC.INI file and must not contain a file called SWEEPIC.RES. SWEEPIC.INI will ensure that the InterCheck server can be run, while the absence of SWEEPIC.RES means that there are no InterCheck servers already running in that directory.

The InterCheck server loading time is almost the same as the time for which the ICONTROL introductory dialog is displayed. Shortly after this

dialog closes the resident InterCheck server status should be displayed.

Under OS/2 the auto InterCheck server launch will be ignored (even with the ICW.INI ICServer entry supplied).

ICONTROL should not be forced to run a resident InterCheck server with a working directory on a remote workstation, for example:

```
[Application Settings]
ICServer=D:\SWEEP\SWEEP.EXE, -ICS=ServerName, Q:\SWEEP
```

where Q: is a drive on a networked workstation and D: local hard disk. This is because the InterCheck server run on a local machine might have difficulty reading from and writing to its working directory on the remote PC.

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. The -A and -U options are described in more detail in the 'Installing InterCheck clients' chapter.

-? 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 by SWEEP.

Additional information on PC viruses can be found in Sophos' *Data Security Reference Guide*.

Recovery from a virus attack

Recovery from a virus attack involves two stages:

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

Eliminating viruses

SWEEP's automatic disinfection facilities, or DOS 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.

Note: For greater protection, SWEEP will not perform disinfection if it detects a virus active in memory. It is always advisable to reboot from a clean disk, as recommended in the sections below.

Creating a clean DOS boot disk

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

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

```
FORMAT A: /S
```

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

Create a CONFIG.SYS file with the following lines:

```
DEVICE=A:\HIMEM.SYS
DEVICE=A:\EMM386.EXE
DOS=HIGH
FILES=15
BUFFERS=40
```

Create an AUTOEXEC.BAT with the following lines:

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

Make the floppy disk write-protected (to ensure that it cannot become infected with a virus), and label it with the operating system for which it was created.

If a computer becomes infected, use the clean boot disk to boot the computer. This will ensure that

various items on the computer can be examined through a 'clean' operating system, giving the virus no chance to employ hiding techniques.

Dealing with infected boot sectors on the hard disk

Infected boot sectors on hard disk can either be disinfected with SWEEP or have their boot sectors replaced with a clean one:

1. Disinfection

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

Boot the PC with a clean boot disk. Use SWEEP for DOS to disinfect the virus with the command

```
SWEEP -DI
```

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

2. Replacing the boot sector

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

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

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

```
FDISK /MBR
```

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

```
SYS C:
```

If using the SYS command to overwrite a DOS boot sector virus, it is essential that the clean boot disk was for the same version of DOS as the infected PC.

Also, if the infected PC is not a DOS machine, the SYS command should not be used because it is operating system specific.

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 infected boot sectors on floppy disk

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

1. Disinfection

Boot the PC with a clean boot disk. Then use SWEEP for DOS to disinfect the virus, with the command

```
SWEEP A: -DI
```

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

To scan and disinfect a number of floppy disks, use the command

```
SWEEP A: -DI -MU
```

SWEEP will prompt for each disk to be inserted in turn. It is important to check all floppy disks which have been used in infected machines, because just one infected disk which goes unchecked can cause re-infection.

2. Reformatting

Alternatively**, boot 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 booted from a clean boot disk), and reformat the disk using

```
FORMAT A:
```

if the disk is in drive A:.

Disinfection of infected executable files

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

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

Disinfection of infected documents

SWEEP can automatically disinfect documents infected with certain types of macro viruses.

It is not necessary to reboot from a clean system disk, but it is important to ensure that the application that created the document is not open when disinfection is attempted. Use the command

```
SWEEP -DI
```

In some cases it is also possible to 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 this.

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

After a virus attack:

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

Troubleshooting

This chapter provides answers to some common problems which can be encountered when using SWEEP.

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, but typically the quick level is 5 to 10 times faster than the full. See also ‘Sweeping level’ in the ‘Runtime options’ section of the ‘Using SWEEP with SW’ chapter, and ‘Full or quick sweeping’ in the ‘Configuring SWEEP’ chapter.

No extended or expanded memory

If SWEEP does not find extended or expanded memory, it will create a ‘swap’ file on the hard disk or on a network drive. To increase the sweeping speed, install the extended or expanded memory manager. For example, to use extended memory, insert the following line into CONFIG.SYS:

```
DEVICE=HIMEM.SYS
```

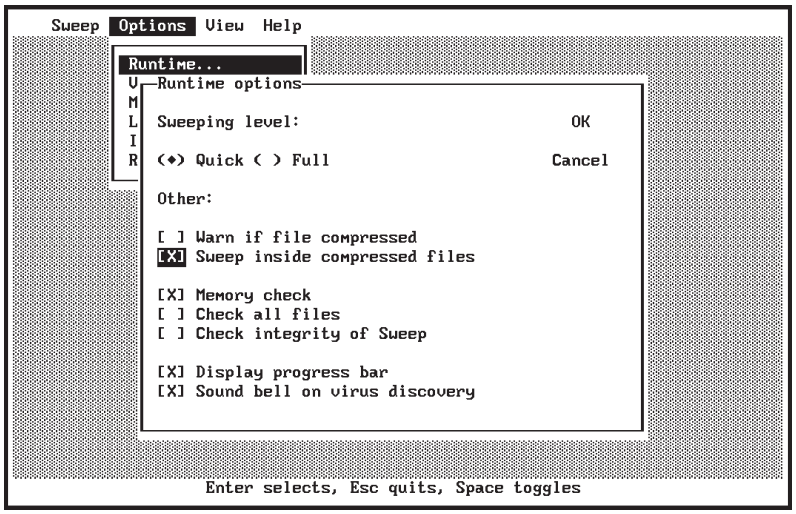
and copy the HIMEM.SYS onto the floppy. When the PC is next booted, extended memory will be available to SWEEP.

If a PC is being used which either does not have extended or expanded memory (e.g. an 8086-based machine) the location of the swap file can be specified by setting the TMP environment variable. For example, type

```
SET TMP=C:
```

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

By default, SWEEP will only check files defined as executables. If SWEEP is checking all files, it will take longer than if only executable files are being checked.

All files can be checked by using the command line qualifier -ALL or by including a descriptor such as

```
>\*.*
```

in the SWEEP.ARE file.

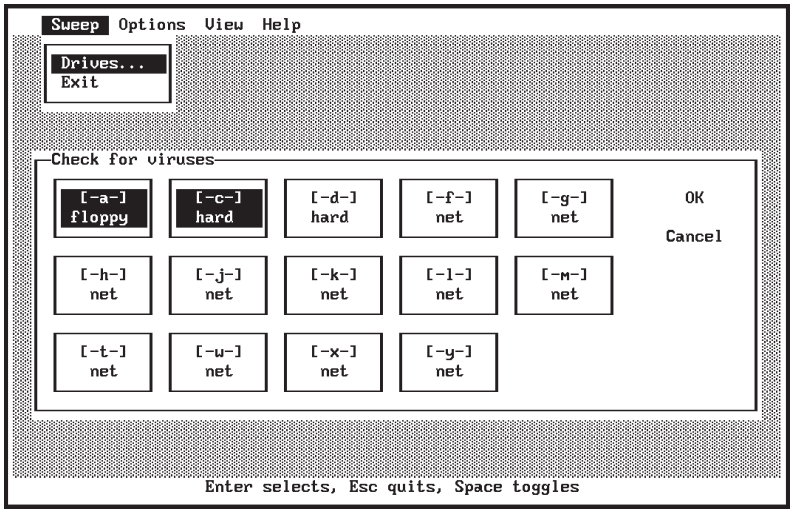
Similarly, if checking all sectors is selected, SWEEP will take a long time to run.

Network drives

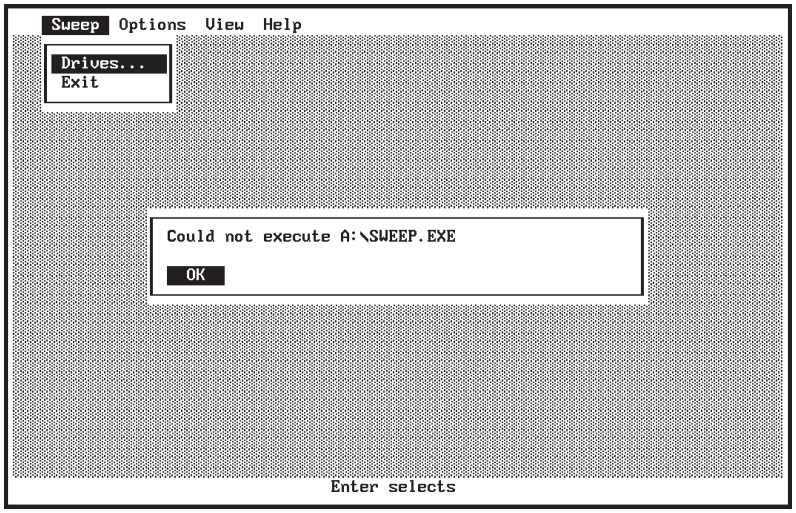
Some network drives will be much larger than a local hard disk, and so will take significantly longer to check. Most network interfaces provide much slower access than a local hard disk, which can reduce speed further still.

Multiple drives selected in SW

When selecting drives to be checked in SW, it is possible to specify more than one drive inadvertently. In the following example, both drives A: and C: have been specified. To SWEEP only drive A:, deselect drive C: by clicking on it before starting the SWEEP.



Could not run SWEEP.EXE



When running SW from floppy disk to check disks in the same drive, do not remove the SWEEP disk until prompted to insert the first disk to be checked.

Out of memory

Apart from the conventional memory, SWEEP also uses extended memory, expanded memory or disk space during its execution. If it runs out of memory, it will produce a message to that effect.

Non-conventional memory requirement is currently about 340K, but this may increase in the future.

Network Error: file in use

If a network file is already open when SWEEP tries to examine it, a message similar to the following will be displayed and the execution of SWEEP will be interrupted:

```
Network Error: file in use during OPEN A FILE.  File = F:\ARCHLOG\00000041.REC
Abort, Retry?
```

If a file is to be accessible to several processes at the same time, it must be marked as 'shareable' by using the NetWare utility *FILER*.

Alternatively, SWEEP can be instructed to ignore these messages and continue execution by using the -NI command line qualifier:

```
SWEEP -NI
```

The above error usually occurs when either the -ALL or -WC options are used.

Text unclear on a black and white monitor

Some black and white monitors appear to the PC as colour, resulting in an unclear output in SW. This is especially apparent on some LCD (Liquid Crystal Display) screens. To force SW to output black and white text use the -BW command line qualifier:

```
SW -BW
```

Display remains blank

Check that the -MO (monochrome) command line qualifier has not been used. -MO should be used only with the old MDA (Monochrome Display Adapter) screens. If used on a CGA, EGA or a VGA screen, the display will remain blank.

Could not open file F:\PUBLIC\SWEEP.EXE

This error message appears if SWEEP is run from a NetWare file server after being set as an execute-only attribute.

To remedy the problem, delete SWEEP.EXE on the network and reinstall it from the distribution disk.

Users cannot access InterCheck server

Users must have the following access rights to the SWEEP InterCheck server directories:

\SWEEP	Read access
\SWEEP\COMMS	Read and write access
\SWEEP\LISTS	Read and write access
\SWEEP\INFECTED	No access

for the InterCheck client software to function correctly.

To check the correct access rights have been assigned, go to the InterCheck client workstation(s) and try to create files in the above directories. It should not be possible to create files in the SWEEP directory while it should be possible to create and delete files in the COMMS and LISTS directories.

For information on setting access rights under specific operating systems, see the relevant 'Setting the access rights' section in the 'Installing SWEEP as an InterCheck server' chapter'.

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.

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.

Using a normal text editor, create a VIRUSNAM.IDE file (where 'VIRUSNAM' is the name of the virus) in the same directory as SWEEP and SWEEP will be able to recognise the new virus when it is next run.

Stealth viruses

Stealth viruses such as *4K* and *Joshi* actively hide themselves from anti-virus software. If the virus is memory-resident, SWEEP will not discover its presence inside the files (although it will probably discover it in memory). To avoid this problem, perform a secure boot so that the virus cannot become memory-resident in the first place.

Further help

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, 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.

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

Boot Protection: Method used to prevent bypassing security measures installed on a hard disk by boot a microcomputer from a floppy disk.

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.
Cache:	High-speed data storage used to hold data retrieved from a slow device. Using a cache increases the overall performance of a system.
Checksum:	A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered. Usually 32 or 64 bits long.
COM:	The extension given to a type of executable file in MS-DOS. A COM file is similar to an EXE file, but can only contain up to 64K of code and data. In operating systems other than DOS, the extension COM can have a different significance.
Companion Virus:	A virus which 'infects' EXE files by creating a COM file with the same name which contains the virus code. It exploits the DOS property that if two programs with the same name exist, the operating system will execute a COM file in preference to an EXE file.
Compressed File:	See File Compression.
Conventional Memory:	The bytes of PC memory addressable by the 8086 instruction set.
DOS:	Disk Operating System. See MS-DOS and PC-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.
Expanded Memory:	PC memory which conforms to the industry standard specification EMS (Expanded Memory Specification), and enables the CPU to access more than 640K of memory.
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.
Extended Memory:	Memory in PCs which lies above 1 MByte in a 80286 (or above) machine.
False Negative:	An existent event reported as non-existent, e.g. the absence of a virus when the virus is present.

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

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.

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.

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.

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

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

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

Logic Bomb: A program modification which causes damage when triggered by some condition such as the date, or the presence or absence of data.

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 boot. 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.

Menu-driven: Software which presents the user with a fixed 'menu' of command choices, often requiring only a single key or mouse button depression to select the required option.

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. See also PC-DOS.

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

Operating System: The computer program which performs basic housekeeping functions such as maintaining lists of files, running programs etc. PC operating systems include MS-DOS and OS/2, while minicomputer and mainframe operating systems include UNIX, VMS and MVS.

OS/2: An operating system for 80286+ 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.

PC-DOS Microcomputer operating system originally used by IBM for its PCs. It is functionally identical to MS-DOS.

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 bootstrap 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.

UNIX: UNIX is a multi-user operating system, developed by AT&T. Several versions of UNIX exist, which do not all achieve compatibility with each other.

VDL:	Virus Description Language; a proprietary Sophos language used to describe virus characteristics algorithmically. It has extensive facilities to cope with polymorphic viruses.
Virus Identity:	An algorithm describing various characteristics of a virus and used for virus recognition. Sophos describe viruses using the proprietary Virus Description Language (VDL).
Virus Pattern:	A sequence of bytes extracted from a virus and used for virus recognition.
WAN:	Wide Area Network; a set of computers that communicate with each other over long distances.

Index

E

F

H

I

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/