Sophos Anti-Virus

User Manual

Novell NetWare

SOPHOS

Sophos Anti-Virus

for NetWare

User Manual
February 1998

This manual documents Sophos Anti-Virus
for NetWare, 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 # masnez0c/980112

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.

Why is virus checking needed for NetWare?

Virus checking is necessary because many PC viruses can infect files on NetWare drives. This is due to the excellent emulation of logical DOS drives under NetWare.

Macro, parasitic, multipartite and companion viruses can all spread across the network.

Boot sector viruses cannot spread across the network. This is because, unlike local workstation drives, NetWare does not allow individual sector addressing through DOS interrupts 25H and 26H or through BIOS interrupt 13H.

Link viruses do not infect files on network drives.

See Sophos' technical report 'Viruses and Anti-Virus Measures on NetWare' for more information on viruses and NetWare.

About SWEEP for NetWare

SWEEP for NetWare is supplied with:

- **The SWEEP NLM (NetWare Loadable Module).** This is used to check files on the file server and provide the InterCheck server function (i.e. on-access scanning for client workstations).
- **SWEEP for DOS.** This can be installed on the server and used by individual users to check their local DOS drives.

Using SWEEP for NetWare to scan files on the file server has two advantages over running SWEEP for DOS from a workstation:

- It does not involve DOS in sweeping, which means that it is not susceptible to the stealth techniques used by many viruses.
- It runs on the file server to scan files stored there, so there is no increase in network traffic.

About InterCheck

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

How to use this manual

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

On-demand scanning

If using SWEEP for on-demand scanning of a file server, read the ‘Installing SWEEP’ and ‘Using SWEEP’ chapters.

On-access scanning for a network

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

More advanced features

If using SWEEP’s more advanced features, read the ‘Configuring SWEEP’ and ‘SWEEP options’ 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’ describes how to install and run SWEEP on a server and how to upgrade SWEEP.

- 'Using SWEEP' describes how to load and unload SWEEP, how to perform immediate and scheduled sweeping, and how to set up virus reporting.
- 'Configuring SWEEP' describes how to configure the immediate, scheduled, real-time and InterCheck modes of operation.
- 'SWEEP options' describes options for administering the configuration file, central checksumming, the virus library, the executables and exclusions lists, and the log file. It also lists SWEEP's command line qualifiers.
- 'Installing InterCheck clients' describes how to install and run InterCheck clients to provide on-access scanning for workstations.
- '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.

Features of Sophos Anti-Virus for NetWare

- Checks NetWare file servers for the presence of all viruses known to Sophos at the time of release, including Macintosh viruses in files stored on the server.
- 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 viruses in parts of files likely to contain a virus, and a 'full sweep' which looks for viruses 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 full scheduling facilities, so SWEEP can be configured to perform regular checks without any further operator action.
- Supports background or priority operation.
- Offers centralised control of anti-virus software, which makes for easy updating.

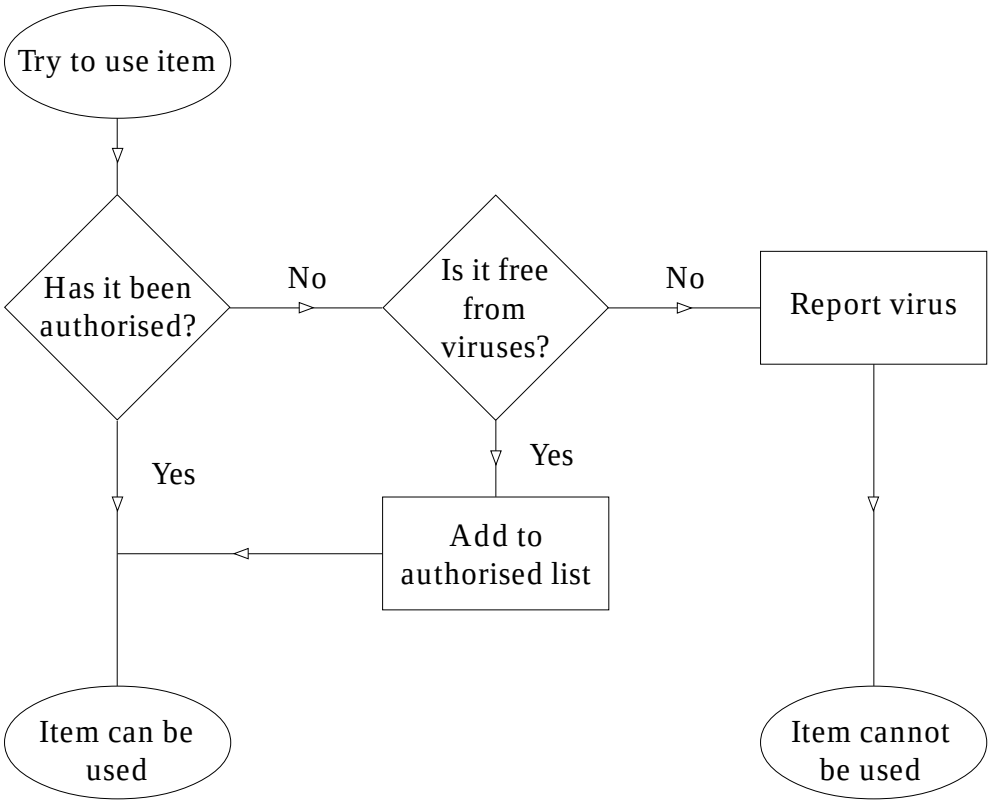
Sophos Anti-Virus is also available for DOS/Windows 3.x, Windows 95, Windows NT (i386 & Alpha AXP), OpenVMS (VAX & Alpha AXP), OS/2 and Banyan VINES.

About InterCheck

This chapter presents an overview of Sophos' InterCheck technology.

What is InterCheck?

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



The InterCheck principle

How are InterCheck and SWEEP related?

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

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

What types of InterCheck client are there?

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

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

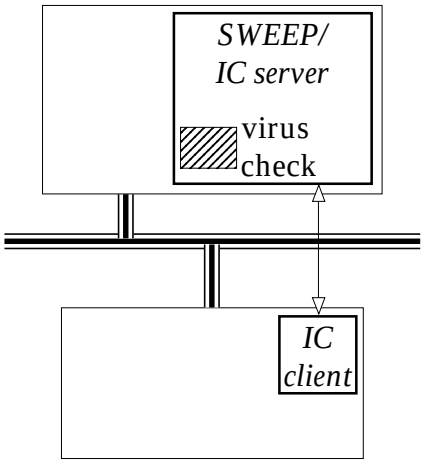
A **stand-alone InterCheck client** does not have to communicate with a remote InterCheck server, and uses a local installation of SWEEP to check for viruses.

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

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

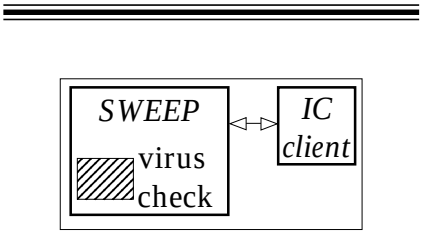
How does InterCheck work?

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

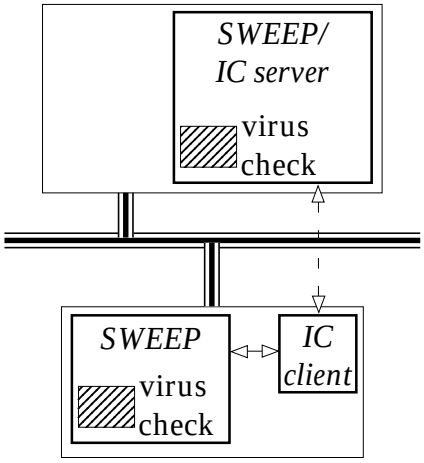


Networked IC client and remote IC server

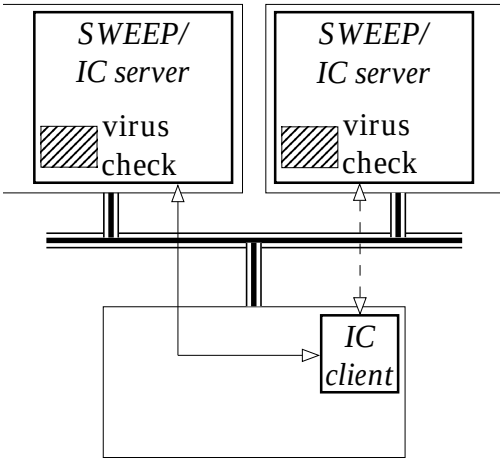
No IC server



Stand-alone IC client with local installation of SWEEP



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



Networked IC client with remote IC server and backup IC server

Different InterCheck client and server configurations

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

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

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

Checksum files

The list of authorised items is called a checksum file.

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

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

Features

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

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

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

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

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

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

Overview of InterCheck installation and configuration

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

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

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

InterCheck server installation and configuration

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

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

Networked InterCheck client installation and configuration

Installation

DOS, Windows, Windows 95 and Macintosh

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

Configuration

DOS, Windows and Windows 95

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

Stand-alone InterCheck client installation and configuration

Installation

DOS/Windows 3.x and Windows for Workgroups

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

Windows 95 and Windows NT

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

Configuration

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

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

Windows NT

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

Installing SWEEP

This chapter describes how to install and run SWEEP on a server and how to upgrade SWEEP.

System requirements

The minimum requirements are:

- NetWare version 3.11 or later.
- At least 4 Mb of available RAM.
- At least 10 Mb of free hard disk space.

The server should be patched to the baseline recommended by Novell. See the Novell Web site at http://support.novell.com/ for details.

Which level of installation?

There are two levels of installation, depending on the functions the user requires:

Installing SWEEP on a file server.
This initial step places the software on a server and enables on-demand scanning of server volumes.

Installing SWEEP as an InterCheck server.
With this further optional set of steps, SWEEP is also enabled to handle requests for on-access scanning from workstations on the network.

The first level is detailed in this chapter. The second is described in the 'Installing InterCheck clients' chapter.

Preparing for file server installation

SWEEP is installed onto the file server **from a workstation**.

Before installation, it is essential to perform a secure boot of the workstation, i.e. boot it from a write-protected virus-free system disk. Failure to do this may spread any virus on the workstation to the file server during the installation process.

Note: For instructions on creating a clean system disk, see 'Creating a clean boot system disk' in the 'Treating viral infection' chapter of the Sophos Anti-Virus user manual for DOS/Windows 3.x.

It is not necessary to restart the file server when installing SWEEP.

Important!

- Switch the workstation PC off.
- Insert a clean, write-protected system disk into drive A:. This disk should also contain the appropriate NetWare client software and LOGIN programs.
- Switch the PC on.
- After the PC has booted, it will display the prompt

  A>

Run the workstation client software from the floppy disk, then run LOGIN **from the floppy disk** with the '/S NUL' command line qualifier under NetWare 3.x or '/NS' qualifier under NetWare 4.x. This will prevent the execution of any login scripts.

If any other NetWare commands are executed, such as MAP, make sure that they are present and run from the floppy disk.

Installing SWEEP on the file server

At a workstation, after secure booting (described above), log in to the file server.

The user installing SWEEP must be able to write to the SYSTEM directory of the file server. This will normally involve logging in with write access rights equivalent to those of SUPERVISOR.

After logging in, insert the Sophos Anti-Virus CD in the workstation's CD-ROM drive (in this example drive D:).

Now copy the SWEEP NLM (NetWare Loadable Module) into the SYSTEM directory of the file server, normally F:\SYSTEM, e.g.:

```
COPY D:\NETWARE\SWEEP.NLM F:\SYSTEM
```

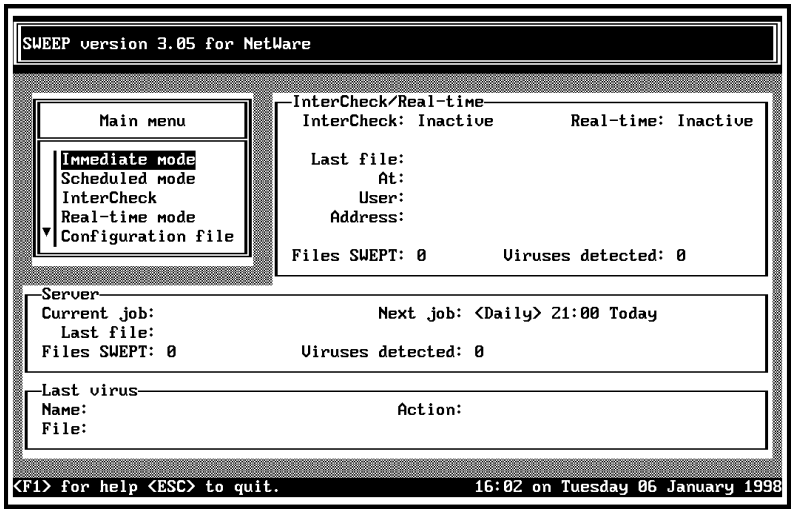
Then at the server console, or by using RCONSOLE from a workstation, enter

```
LOAD SWEEP -DS
```

NetWare 3.x users do not need to use the -DS qualifier, which enables support for NetWare Directory Services.

SWEEP will load and run. Note that the first time it is run, SWEEP may take several seconds to load.

The main menu will be displayed, as shown below:



Note: If a black and white monitor is used, load SWEEP with the -BW command line qualifier:

Testing SWEEP

SWEEP's virus checking can be tested as follows.

At a workstation, use a text editor, such as EDIT, to create a new file containing the test string:

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Take care to key in the string correctly. Save the file as EICAR.COM, then copy it to a server volume.

Now select *Immediate mode* from the *Main menu* on the SWEEP screen. Select *Configuration* to go to the *Immediate Configuration* menu, then select *Files* and specify the directory in which EICAR.COM has been placed. SWEEP should report a virus in the Server and Last virus windows at the bottom of the screen.

Refer to the 'Using SWEEP', 'Configuring SWEEP' and 'SWEEP options' chapters for information on configuring and running the SWEEP NLM.

Installing SWEEP as an InterCheck server

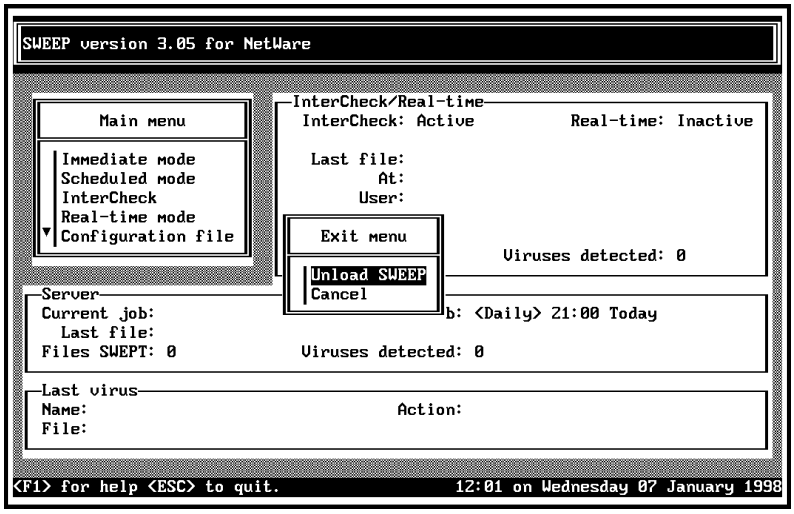
SWEEP can also be used as an InterCheck server to provide on-access scanning for client workstations. For information, see the 'Installing networked InterCheck clients' section of the 'Installing InterCheck clients' chapter.

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, copy the new SWEEP.NLM to the SYSTEM directory of the file server, and then unload and reload SWEEP.

To unload SWEEP, press *Esc* to get to the *Exit menu*.



Select *Unload SWEEP* and press *Enter*, saving the configuration if required.

To load the new version, enter

```
LOAD SWEEP -DS
```

Updating SWEEP when InterCheck is used

If using InterCheck, update SWEEP for DOS on the server after updating SWEEP.NLM. For example, insert the current Sophos Anti-Virus for DOS CD and copy D:/DOS/*.* into the server SWEEP directory.

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

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

Note: The InterCheck client TSR does not require updating.

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

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/).

The IDE files should be saved in a file with an IDE extension, and this should be placed in the server SWEEP directory. The SWEEP NLM will recognise the new IDE file after it is unloaded and reloaded.

Using SWEEP

This chapter describes how to load and unload SWEEP, how to perform immediate and scheduled sweeping, and how to set up virus reporting.

Loading SWEEP

When using SWEEP, all input and screen displays occur at the file server console. SWEEP can therefore be controlled from the server console itself, or (using RCONSOLE) at a workstation attached to the file server.

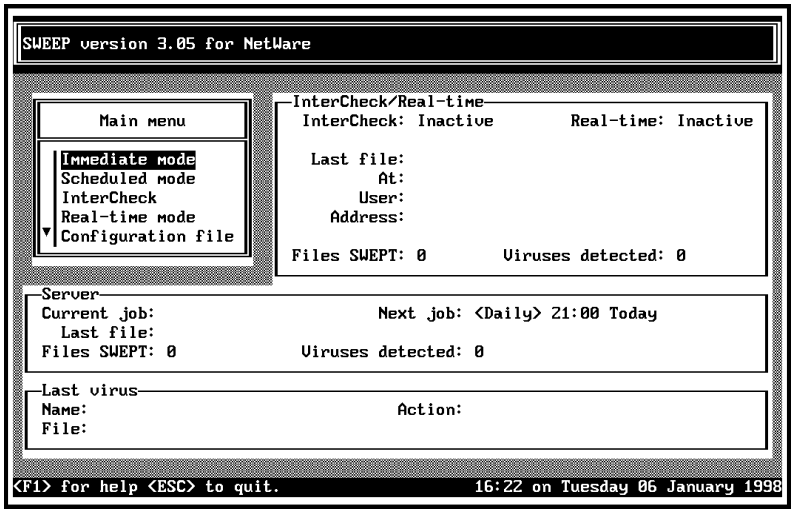
To run SWEEP, enter at the file server console

```
LOAD SWEEP
```

Alternatively, if using a black and white display, load SWEEP with the command

```
LOAD SWEEP -BW
```

The main SWEEP display will be shown.



The main SWEEP display is split into four windows:

- **Main menu**: contains the options to configure the immediate, scheduled, InterCheck and real-time modes, as well as options to administer the configuration file, the checksumming, and other aspects of SWEEP.
- **InterCheck/Real-time display**: shows the status of InterCheck and the real-time mode (*Active* or *Inactive*), information about the last file swept, the total number of files swept, and the total number of viruses detected.
- **Server display**: shows the current immediate or scheduled job, the next scheduled job, the last file, number of files swept and number of viruses detected in immediate and scheduled modes.
- **Last virus display**: shows name and location of the last virus discovered, along with the action taken.

SWEEP's four scanning modes

SWEEP for NetWare has four modes of operation:

- **Immediate mode**: runs SWEEP now.
- **Scheduled mode**: one or more SWEEP sessions are scheduled for particular days and times.

- **InterCheck mode**: SWEEP acts as a server checking files on individual workstations.
- **Real-time mode**: checks files as they are copied to or from the server on which the NLM is loaded.

Every time SWEEP runs an immediate or scheduled job on the server, an entry is made in the SWEEP.LOG file in the server SWEEP directory. This file also contains reports on viruses found or errors.

Navigating through menus

To select an option, position the selection bar on it (using the cursor up / down keys) and press *Enter*.

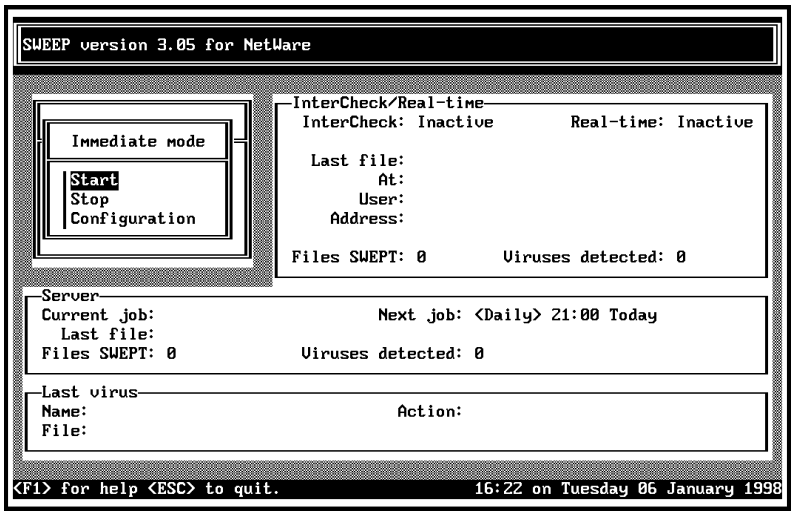
To quit a menu and return to the previous one, press *Esc*.

To add an item to a list (for example days when SWEEP is scheduled to run) press *Ins*. To delete an item from a list, position the selection bar on the item and press *Del*.

Immediate mode

Starting an immediate sweep

To perform an immediate scan of the file server, select *Immediate mode* from the main menu, then *Start*.



SWEEP will check the file server according to the current configuration settings and display all output in the *Server* window, in addition to writing it to the log file and (optionally) sending it to a report file.

Hint: Immediate mode in SWEEP can be selected at load time by using the -I command line argument.

```
LOAD SWEEP -I
```

will load SWEEP and start immediate execution. This enables SWEEP to load and start execution from the AUTOEXEC.NCF file.

Stopping an immediate sweep

To abort the checking process, select *Stop* from the *Immediate mode* menu at any stage.

Configuring immediate sweep

To change the scanning parameters, select *Configuration* from the *Immediate mode* menu. Parameters can be changed while SWEEP is scanning the server, but they will not come into effect until the next scan begins.

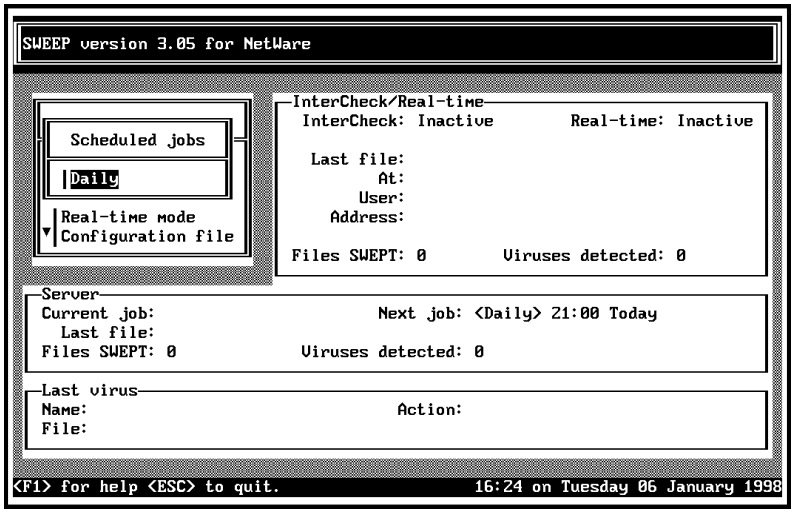
See the 'Configuring SWEEP' chapter for information on immediate sweep configuration options.

Scheduled mode

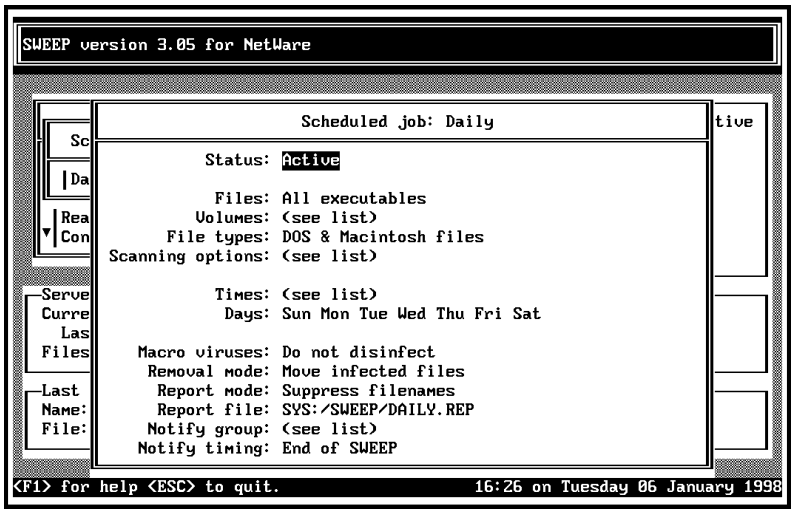
SWEEP can be scheduled to run at predetermined times on specified days of the week. This allows SWEEP to be run at night, for example, or at times when the network is not being used heavily.

Each scheduled job is given a name and the times and days on which it is run. These can be set individually for each job.

Select *Scheduled mode* from the main menu. This will display the names of all scheduled jobs.



Use *Ins* to add new jobs, *Del* to remove jobs from the list and *Enter* to edit / view an existing job.

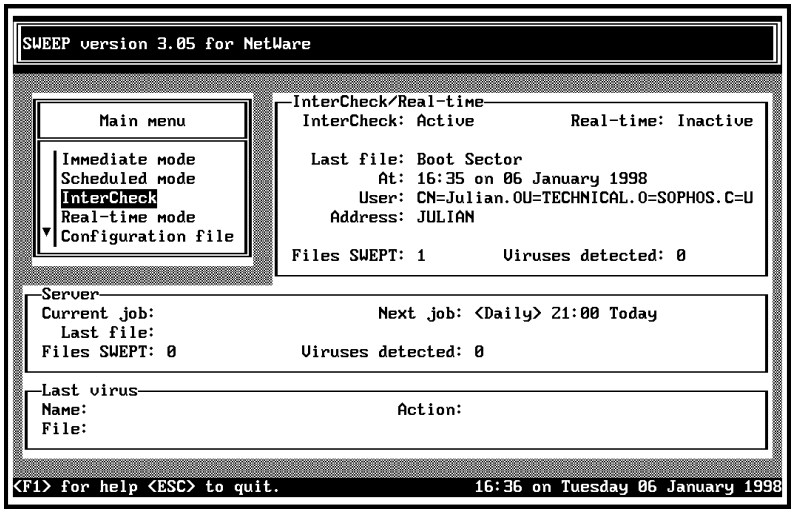


See the 'Configuring SWEEP' chapter for information on the scheduled sweep configuration options.

Note: It is possible to stop a scheduled job at any stage. To do this, select *Stop* from the *Immediate mode* menu.

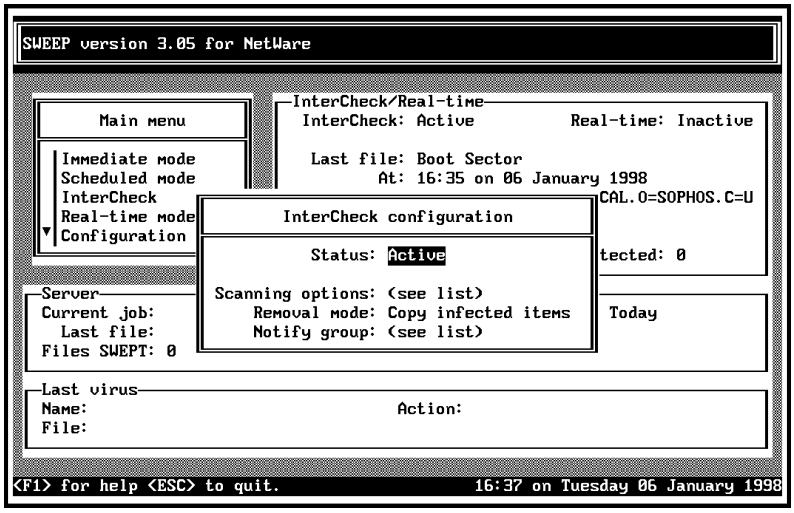
InterCheck mode

The *InterCheck* entry from the main menu is used to control the status and configuration of the InterCheck server.



Activating the InterCheck server

To activate the InterCheck server, select *InterCheck* from the main menu, select *Status* from the *InterCheck configuration* menu, and then select *Active*.



If set to *Active*, InterCheck will process requests by clients.

Important! If the status is set to *Inactive*, workstations running InterCheck will not be able to receive authorisation for new files and disks.

See the ‘Configuring SWEEP’ chapter for information on the InterCheck configuration options.

Real-time mode

Real-time mode provides on-access virus protection on the server, if required.

Whereas the InterCheck client intercepts files as they are accessed by a workstation, real-time scanning intercepts file accesses on the server itself. It is therefore useful where InterCheck is not available or not used on workstations.

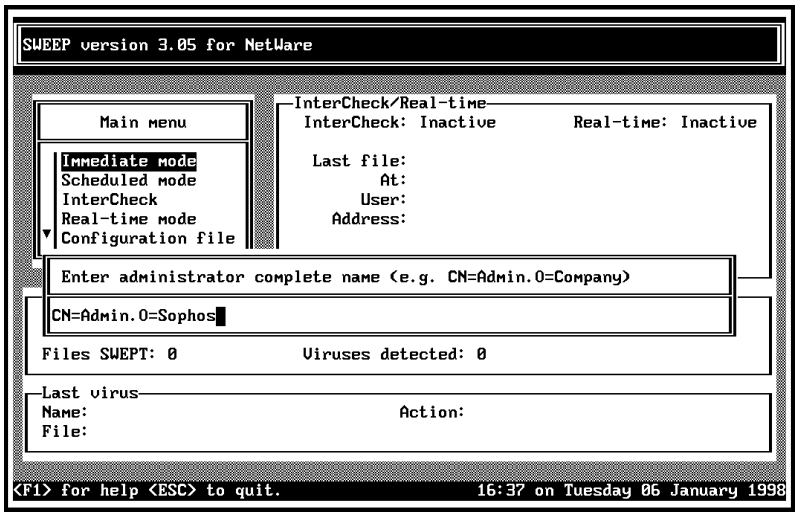
By default, real-time mode is inactive. To activate it, select *Real-time mode* from the main menu and set the Status to *Active*. Note that this adds an overhead to all file system operations on the server.

See the ‘Configuring SWEEP’ chapter for information on the real-time mode configuration options.

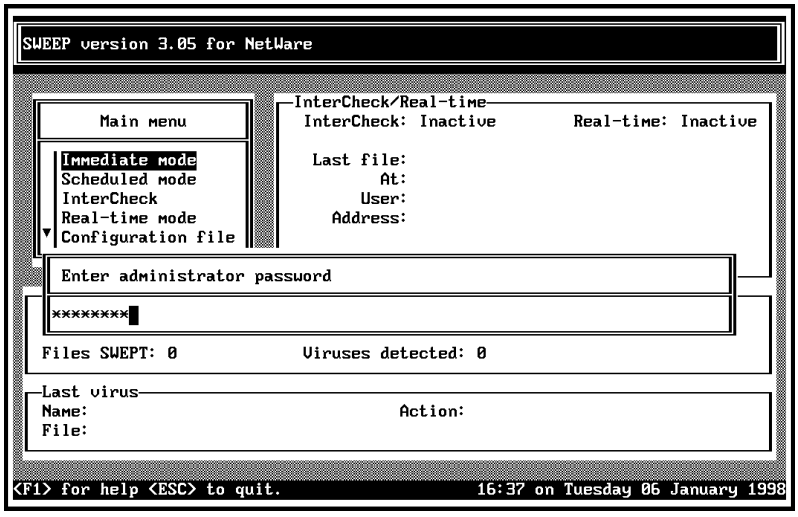
Using NetWare Directory Services for virus reporting

SWEEP for NetWare supports NetWare Directory Services (NDS) on file servers running NetWare 4.x. This allows any user in the NDS tree to be notified about virus incidents, rather than just those in the bindery emulation context, as long as that user has a connection to the server where the virus is found.

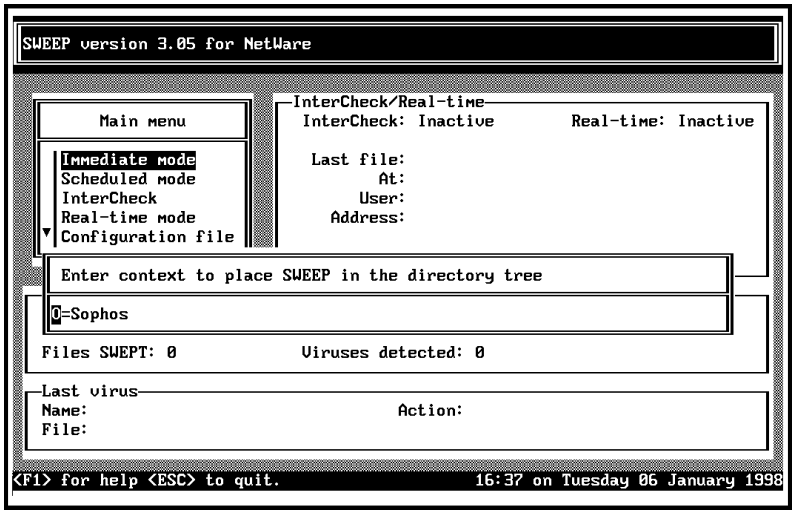
SWEEP must be started with the -DS qualifier to enable this feature. The first time that SWEEP is started in this mode, it will prompt the user for the complete name of an administrator, in this example `CN=Admin.O=Sophos`



followed by the appropriate password



and a context in the directory tree, in this example O=Sophos

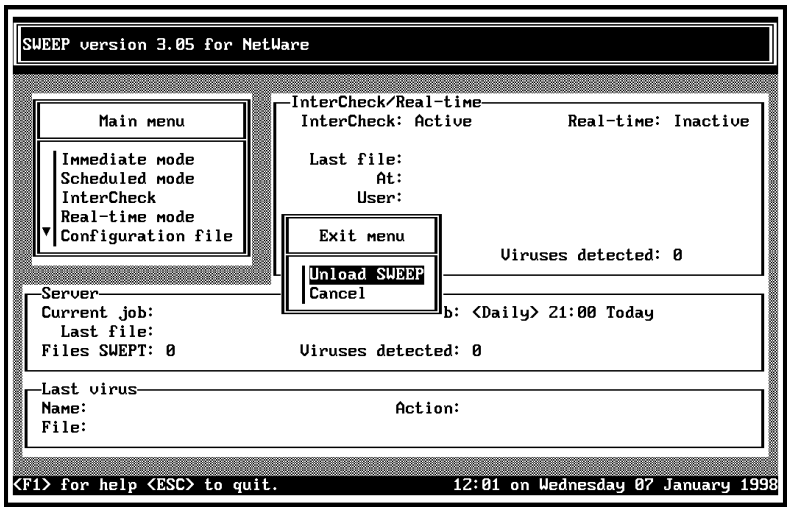


SWEEP uses this to create a new user. The NLM will automatically log in as this user every time SWEEP is subsequently started with the -DS qualifier, enabling it to see the complete NDS tree.

See the 'Notify group' section of the 'Configuring SWEEP' chapter for information on using the NDS tree to select users to notify if a virus is found.

Unloading SWEEP

To quit SWEEP at any stage, press *Esc* repeatedly until the *Exit menu* is displayed. Select *Unload SWEEP* and press *Enter*.

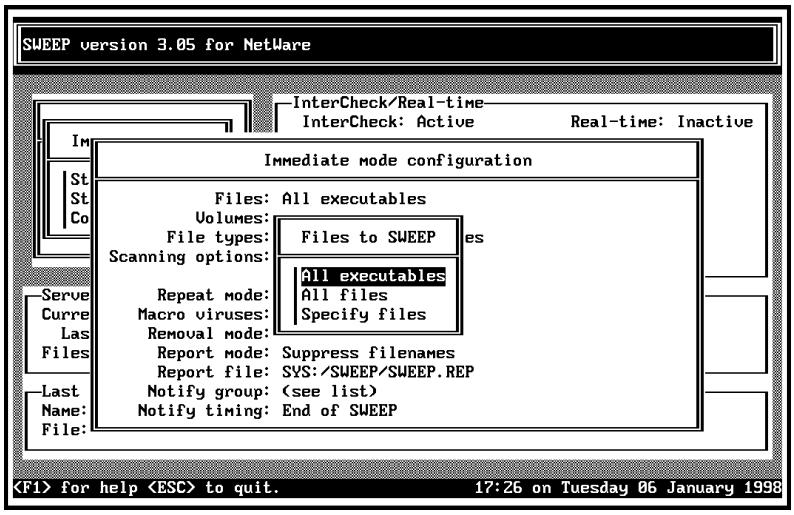


Configuring SWEEP

This chapter describes how to configure the immediate, scheduled, real-time and InterCheck modes of operation.

Files (immediate and scheduled modes)

This allows the user to specify the files or file types that will be virus checked.



All executables

By default, SWEEP checks the following files in all volumes on the file server:

```
*.ADD, *.BID, *.COM, *.DLL, *.DMD,
*.DOC, *.DOT, *.DRV, *.EXE, *.FLT,
*.I13, *.IFS, *.MOD, *.OV?, *.SCR,
*.SYS, *.TSD, *.VSD, *.VXD, *.XL?
```

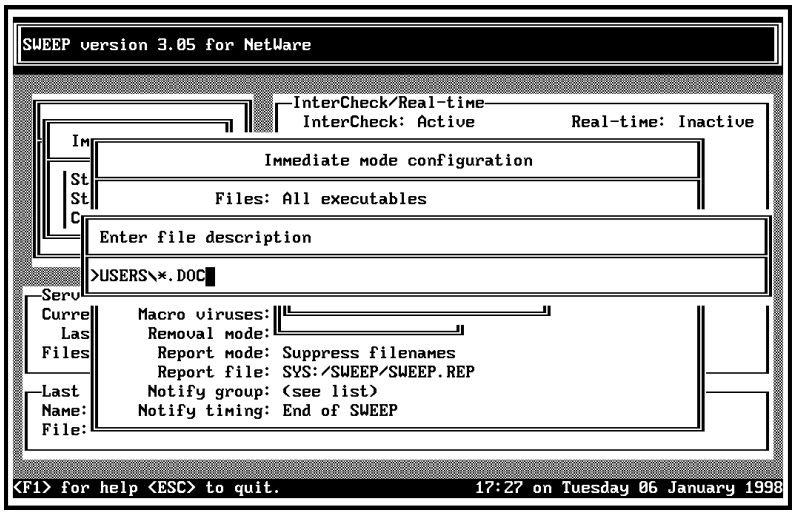
All files

This option will allow sweeping of all files regardless of their extension.

Specify files

Select *Specify files* to allow scanning of a particular set of files. A list of the set of files currently selected will be displayed. Use *Del* to remove file specifications from the list and *Ins* to add new specifications.

When adding new file specifications, an entry such as USERS*.DOC instructs SWEEP to scan all DOC files in the given directory. To scan in the given directory, and all subdirectories below it, use the recursion operator at the start of the entry, e.g. >USERS*.DOC:



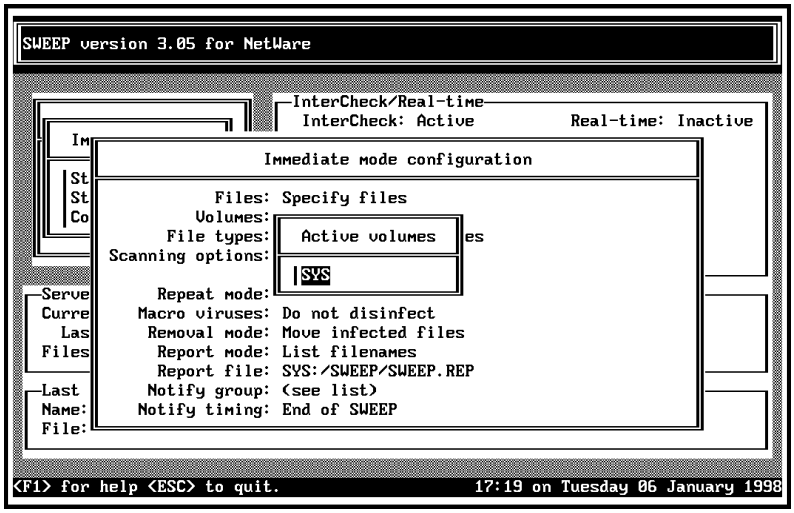
Conventional wildcard characters are supported.

Volumes (immediate, scheduled and real-time modes)

This allows the user to select the volumes to be virus checked.

In immediate and scheduled modes

Selecting *Volumes* will display a list of the volumes that will be checked.

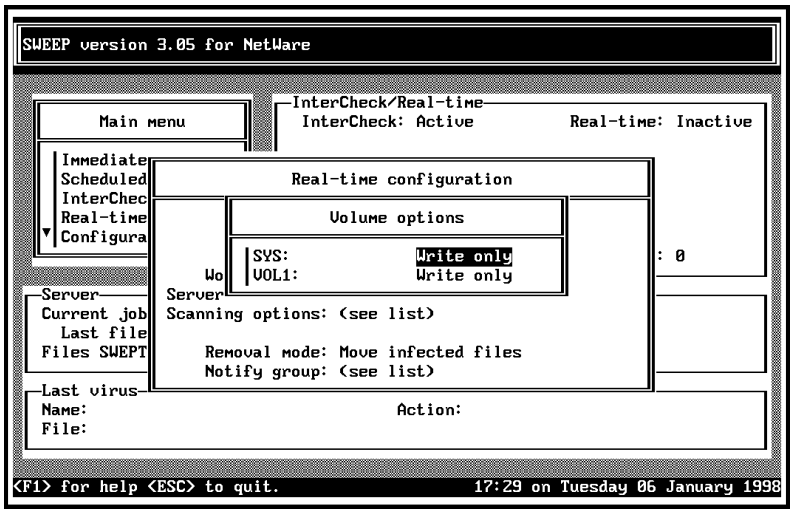


Use *Del* to remove volumes from the list and *Ins* to add new volumes.

By default all mounted volumes will be selected.

In real-time mode

The *Volumes* option from the *Real-time configuration* menu provides three real-time scanning options for each connected volume: write only, read and write, and none.

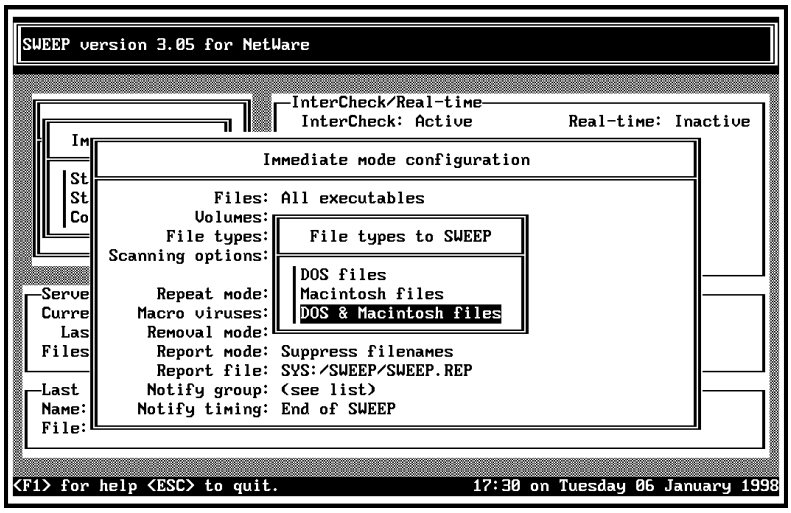


If *Write only* is selected, every time a file on the volume is written to, that file will be checked for

viruses. If *Read and write* is selected, every time a file on the volume is read from or written to (i.e. accessed), that file will be checked for viruses. If *None* is selected, the volume will not use real-time scanning.

File types (immediate and scheduled modes)

It is possible to specify whether SWEEP should examine DOS files for DOS viruses, Macintosh files for Macintosh and macro viruses, or both by selecting the appropriate entry from the *File types* menu.



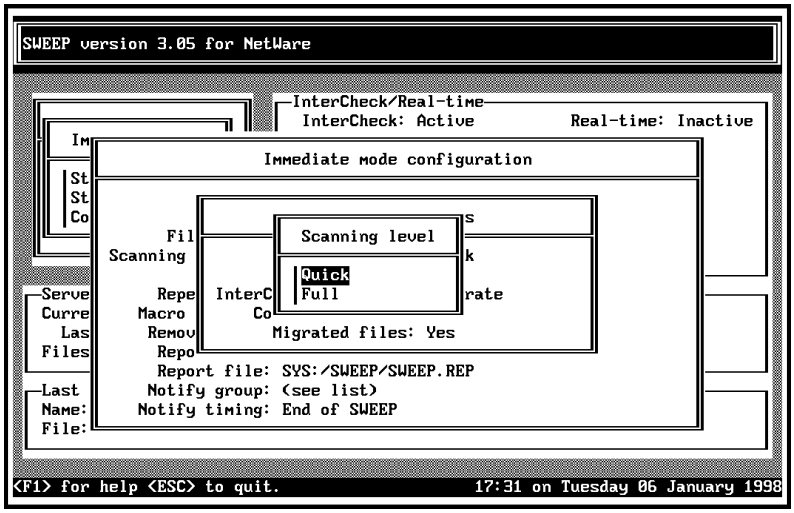
Scanning options (immediate, scheduled, real-time, InterCheck)

Scanning level

The ‘quick’ scanning level only checks the parts of files likely to contain viruses, while the ‘full’ level examines the complete contents of each file.

The ‘full’ level is more secure because it can discover viruses ‘buried’ underneath other code appended to a file, as well as minor virus mutations and corruptions. However, it is much slower, and for normal operation ‘quick’ scanning is generally sufficient.

To choose the level, select *Scanning options* followed by *Scanning level*, then select the required level.

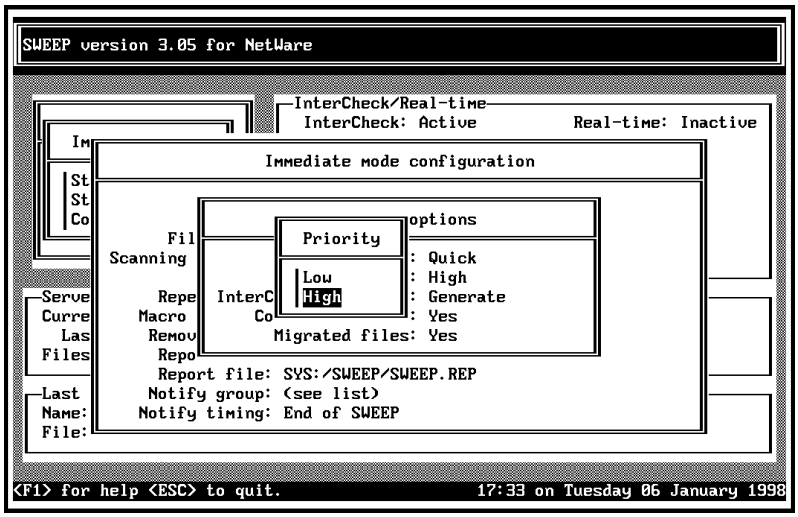


Priority

SWEEP can be set to run at low or high priority. Low priority minimises impact on network performance. High priority maximises scanning speed.

Use low priority when the server is likely to be busy. High priority should be used when clearing up a virus attack, or during periods when the server is underused, for example at night.

To change priority, select *Priority* from the *Scanning options* menu.

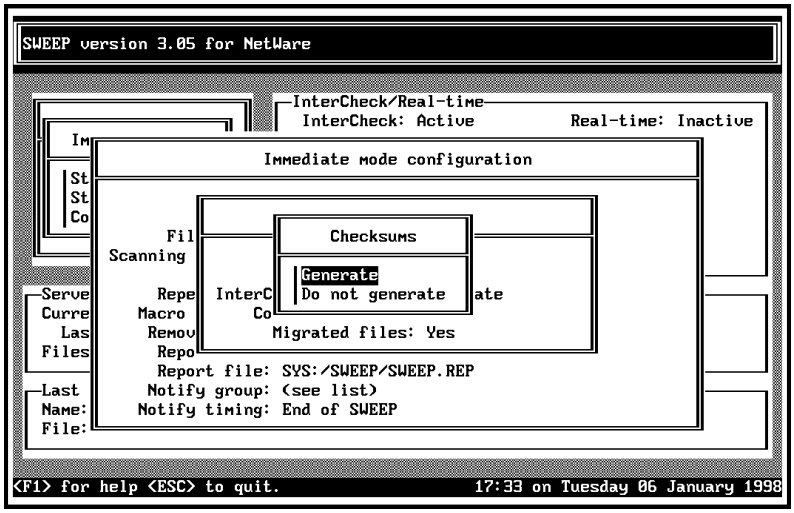


This option is not available in real-time and InterCheck modes.

InterCheck checksums

When SWEEP scans a file on the server and finds it to be virus-free, it can add its InterCheck checksum to the central list, which can then be used by all InterCheck clients connected to the file server. This reduces the number of on-line checking requests by the clients, and therefore reduces overall InterCheck overhead.

Select *InterCheck checksums* from the *Scanning options* menu to configure this setting.

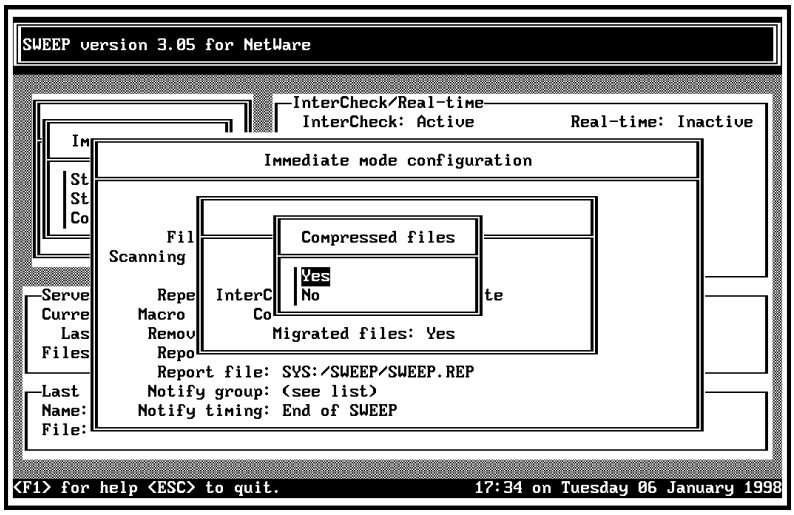


Compressed files

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

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

Select *Compressed files* from the *Scanning options* menu to enable this feature.

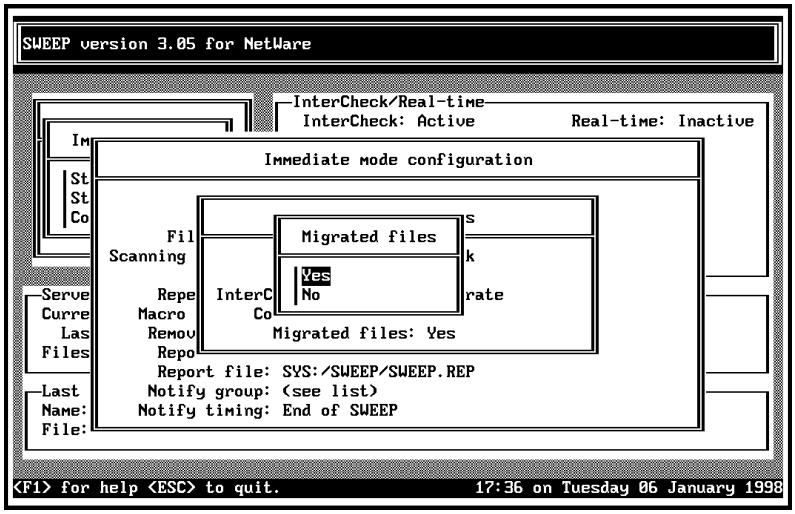


Migrated files

SWEEP can be configured to avoid checking files that have been migrated (i.e. moved to another server or to other media) with Cheyenne's Hierarchical Storage Management system.

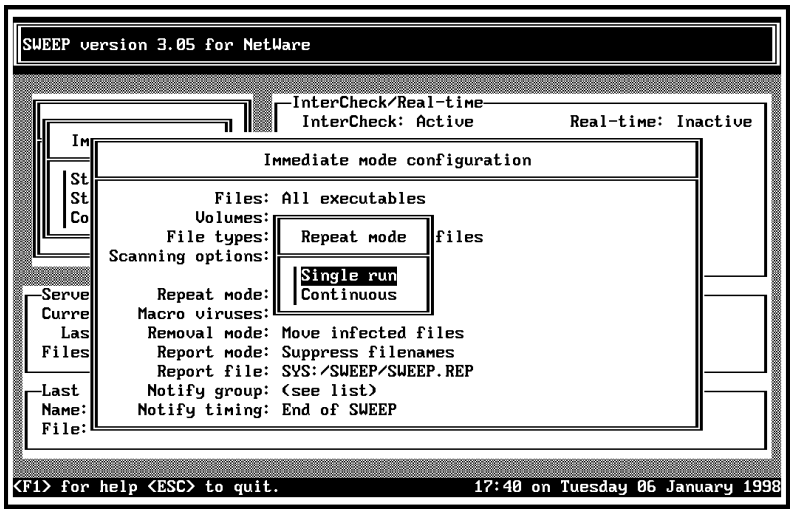
If the *Migrated files* option is set to *Yes*, SWEEP will check a file whether it is migrated or not. If the file is migrated, this will cause it to be demigrated. This is the default setting. If the option is set to *No*, SWEEP passes over migrated files, so that running a virus check will not initiate demigration. Remember that, in this case, SWEEP will not report viruses in these files.

Select *Migrated files* from the *Scanning options* menu to configure this setting.



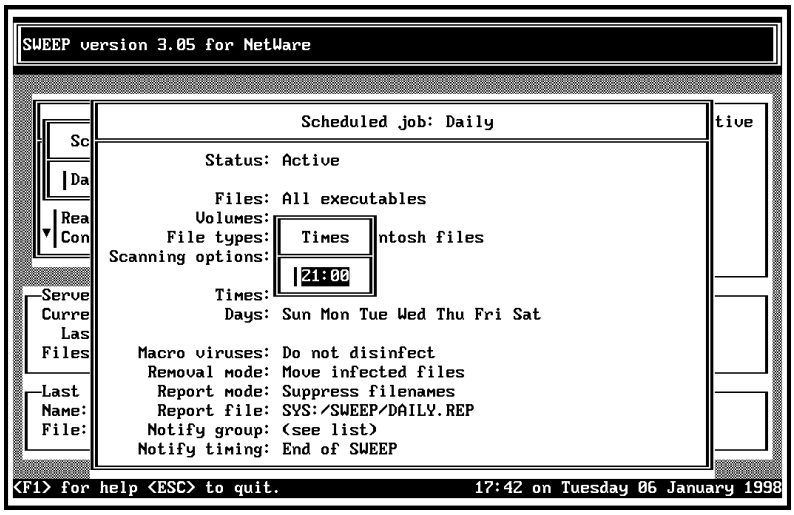
Repeat mode (immediate mode only)

In immediate mode, SWEEP can run either once or continuously as a background process. To change between single and continuous mode, select *Repeat mode* from the *Immediate mode configuration* menu, then select the required mode.



Times (scheduled mode only)

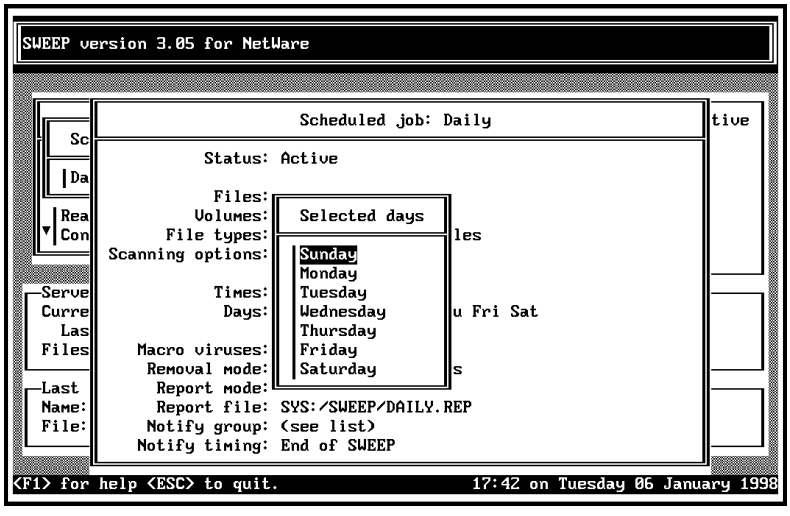
Selecting the *Times* entry displays the specified job's activation times. Use *Del* to remove times from the list and *Ins* to add new times.



The virus check will be performed at every selected time on every selected day.

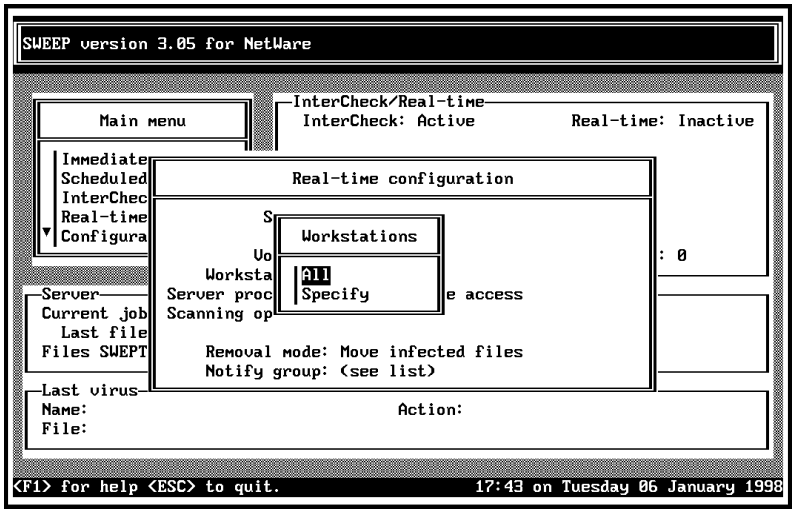
Days (scheduled mode only)

Selecting the *Days* entry displays the specified job's activation days. Use *Del* to remove days from the list and *Ins* to add new days.



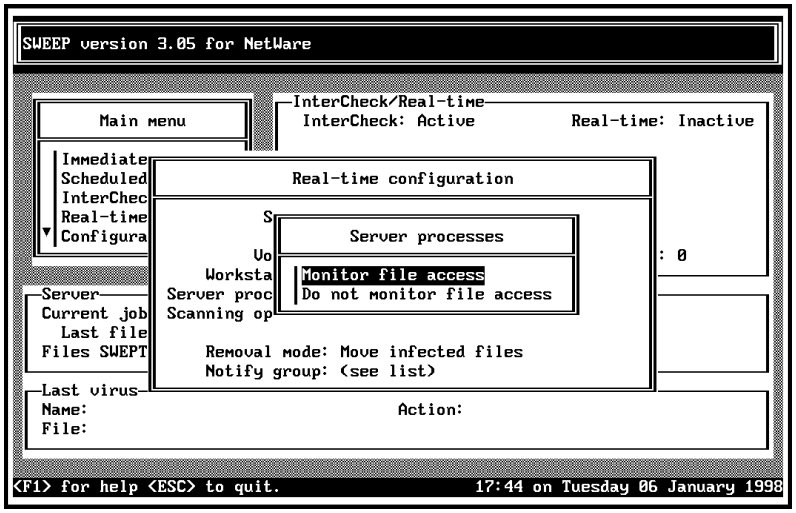
Workstations (real-time mode only)

The *Workstations* option from the *Real-time configuration* menu allows all connected workstations, or only specified workstations, to activate real-time scanning on the server. This allows the activation of real-time scanning to be restricted to workstations, e.g. OS/2 clients, not running InterCheck.



Server processes (real-time mode only)

The *Server processes* option from the *Real-time configuration* menu is used to specify whether processes running on the server activate real-time scanning or not.



Monitor file access

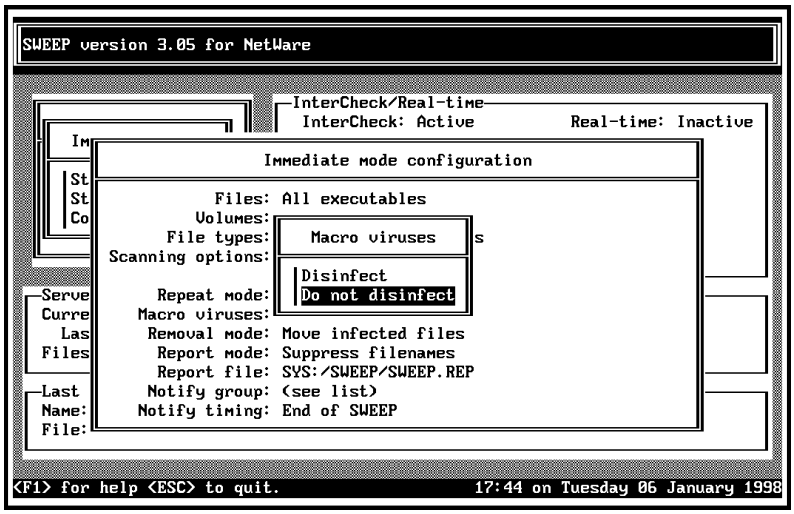
This will activate real-time scanning for all file accesses, whether originating from other processes on the server itself (e.g. by another NLM), or from file operations from outside the server.

Do not monitor file access

This will activate real-time scanning only for file accesses originating from outside the server. This might be useful if, for example, a backup NLM is run on the server.

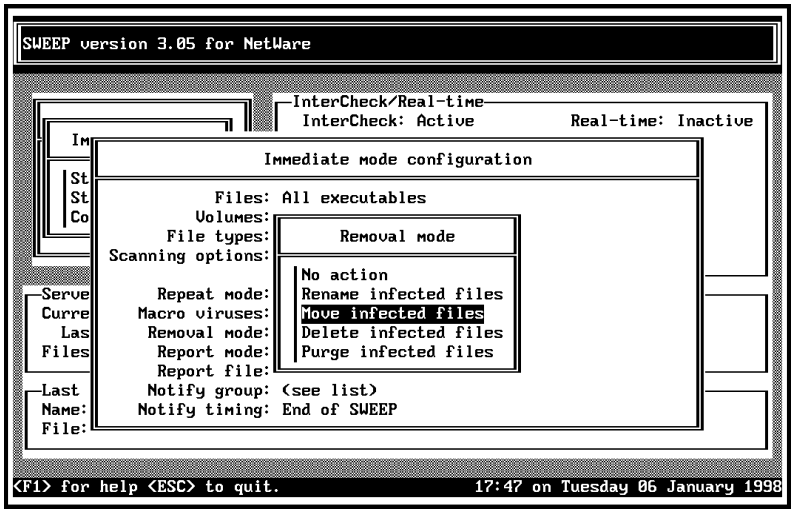
Macro viruses (immediate and scheduled modes)

SWEEP can disinfect documents infected with certain types of macro virus. If disinfection fails, the chosen removal mode (see below) will be applied to selected documents. By default, SWEEP does not disinfect macro viruses.



Removal mode (immediate, scheduled, real-time, InterCheck)

To select the action taken on virus detection, select *Removal mode*, then select the required removal action.



The default action is to move infected files to the server SWEEP\INFECTED subdirectory.

Rename infected files

When renaming of files is selected the last character of the file extension is changed to a digit.

For example INFECTED.COM will be renamed to INFECTED.CO0, or if INFECTED.CO0 already exists, INFECTED.COM will be renamed to INFECTED.CO1 and so on. If more than 10 files with such extensions exist, an error will be reported.

Note that renaming a COM or EXE file to CO0 or EX0 will prevent it from being directly executed by the user.

This option is not available in InterCheck mode.

Move infected files

The infected files are moved to the isolation directory and renamed to have extension 000, 001 etc.

Warning! It is important to set the access rights to this directory so that only authorised users are allowed to examine its contents (see Novell documentation for details on using utilities to set directory rights). This ensures

that it acts as a ‘quarantine area’ from which users can neither recover data nor execute infected objects.

This option is not available in InterCheck mode.

Delete infected files

Note that deleted files can be recovered easily under NetWare.

This option is not available in real-time or InterCheck modes.

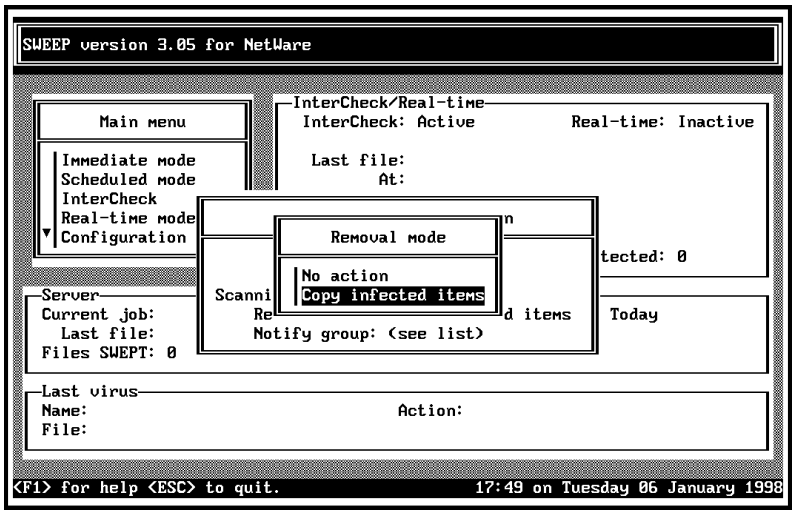
Purge infected files

Once a file has been purged it cannot be recovered.

This option is not available in InterCheck mode.

Copy infected items

When infected items are discovered, they will be copied into the server SWEEP\INFECTED directory for further examination, if this option is selected. Infected file names are made non-executable by setting their extension to a three digit number starting with 000, while infected boot sectors are called BOOT.XXX where XXX is the sequential number of the file, starting with 000.

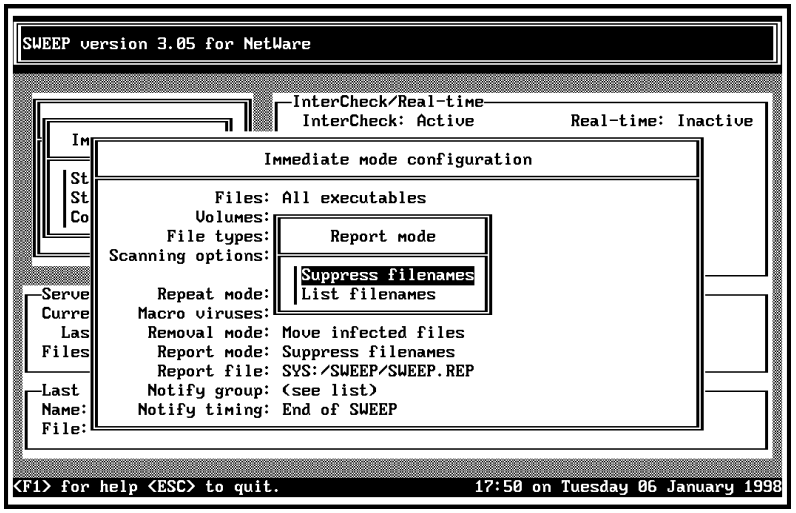


Access rights to the server SWEEP\INFECTED directory should be disabled for all users except the supervisor.

This option is only available in InterCheck mode.

Report mode (immediate and scheduled modes)

Selecting *List filenames* will cause SWEEP to record in the report file the name of every item examined. Otherwise only infected items and errors will be recorded.

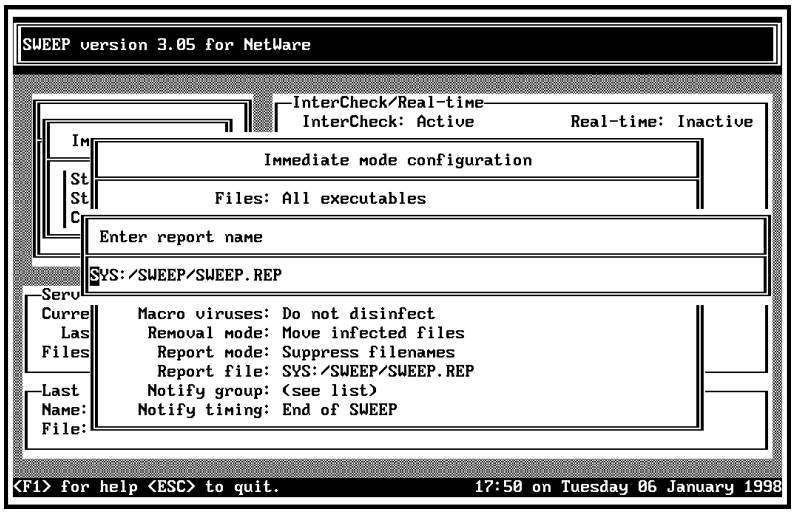


Hint: The *List filenames* option typically produces large report files because the name of every file checked is entered into the report. This option is useful for periodic audit purposes however.

Report file (immediate and scheduled modes)

By default, the report file for immediate scans is SWEEP.REP in the server SWEEP directory, and the file for scheduled scans is given the name of the job, with a .REP extension.

To specify a different report filename, select *Report file*, then enter the required filename.



Notify group (immediate, scheduled, real-time and InterCheck)

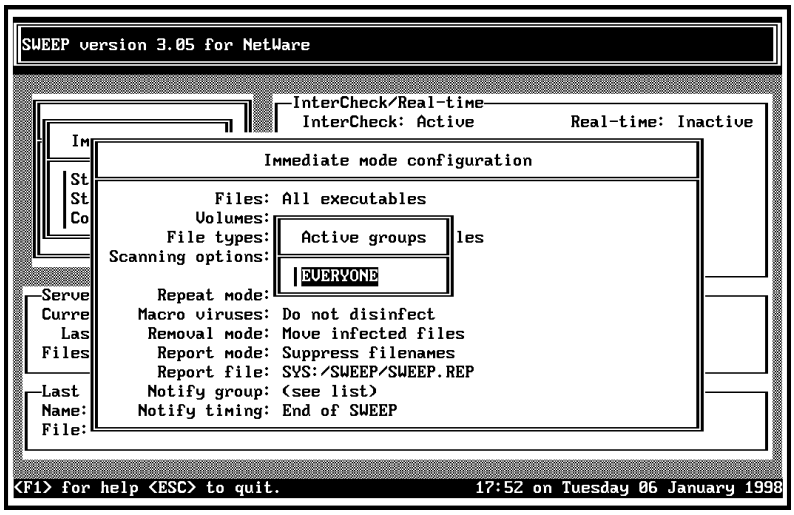
NetWare bindery groups

When SWEEP detects a virus it sends a broadcast message to all members of selected NetWare user groups. Users who are not logged in when the virus is detected are informed the next time they log in. By default, the group EVERYONE is selected if it exists.

It is recommended that a user group such as VIRALERT is created and that all users to be

informed of virus incidents are made members of this group. See Novell NetWare documentation for details of using SYSCON to create user groups and make designated users members of a group.

To select the group to be informed, select *Notify group*. A list of user groups will be displayed.



Use *Del* to remove user groups from the list and *Ins* to add new user groups.

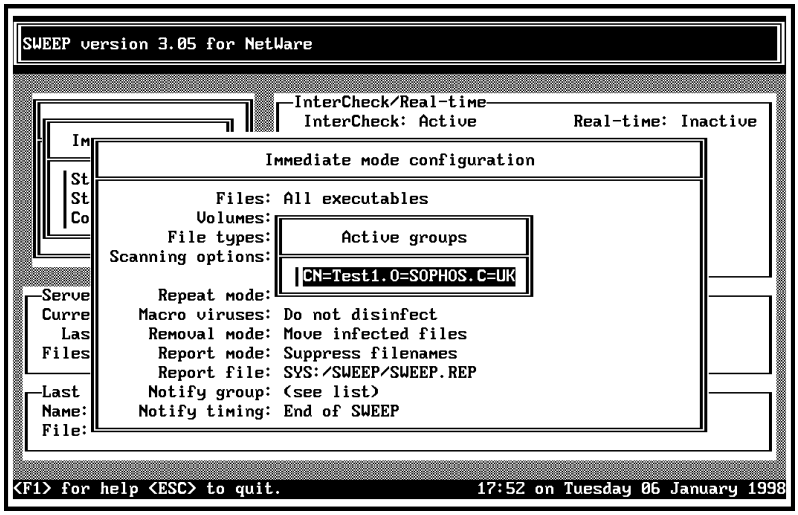
NetWare Directory Services (NDS) groups

Loading SWEEP for NetWare with the -DS qualifier enables support for NetWare Directory Services (NDS) on file servers running NetWare 4.x.

This allows any user in the NDS tree to be notified about virus incidents, rather than just those in the bindery emulation context, as long as that user has a connection to the server where the virus is found. See the ‘Using NetWare Directory Services for virus reporting’ section of the ‘Using SWEEP’ chapter for more information on making NDS groups available to SWEEP for NetWare.

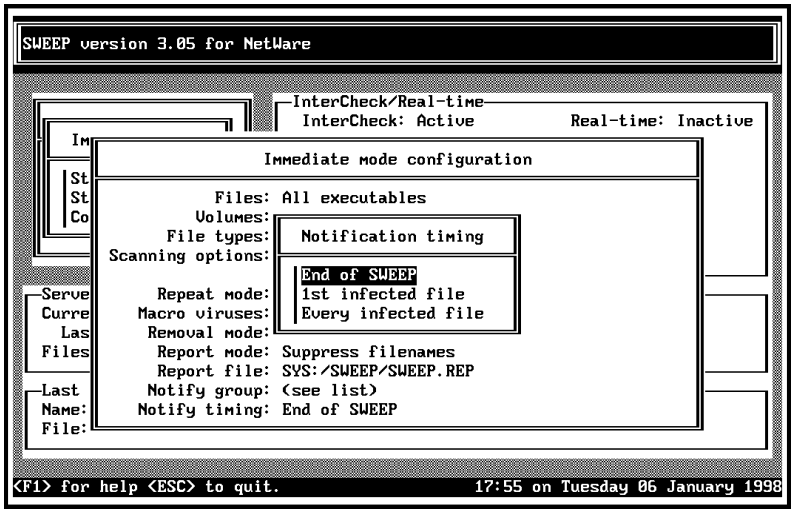
If NDS groups are available, selecting *Notify group* will display the currently selected groups. Use *Del* to remove a highlighted entry, and *Ins* to insert a new group.

If inserting a new group, a list of available groups will be presented. Highlight a group and press *Return* to select it and add it to the list of groups to notify if a virus is found.



Notify timing (immediate and scheduled modes)

Select *Notification timing*, then the time that the groups in *Notify group* will be notified if a virus is found.



Users can be notified of a virus discovery at the end of the SWEEP run (*End of SWEEP* option), on discovery of the first infected file (*1st infected file* option), or on discovery of every infected file (*Every infected file* option).

SWEEP options

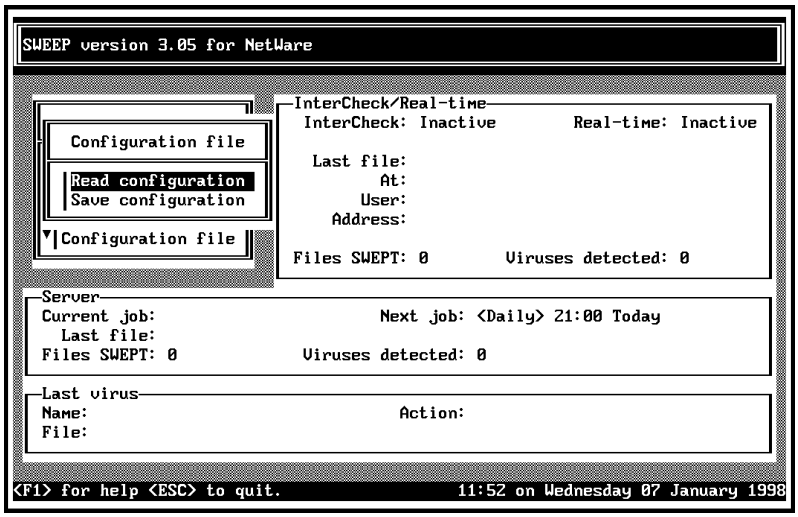
This chapter describes options for administering the configuration file, central checksumming, the virus library, the executables and exclusions lists, and the log file. It also lists SWEEP's command line qualifiers.

Configuration file

The configuration can be saved and will be read in whenever SWEEP is loaded. This is especially useful when installing a new copy of SWEEP because it enables SWEEP to be updated without having to be reconfigured.

Read configuration

To restore a previously saved configuration, select *Configuration file* from the main menu, then select *Read configuration.*



The configuration is read automatically when SWEEP is loaded.

Save configuration

Configuration is saved in the file SWEEP.CFG in the server SWEEP directory.

There are two ways of saving the current configuration:

1. Select *Configuration file* from the main menu, then select *Save configuration*.

or

2. Press *Esc* repeatedly until the *Exit* menu is displayed. Select *Unload SWEEP*. If the configuration has been changed, the *Save configuration* menu will be displayed. Select the desired option.

or

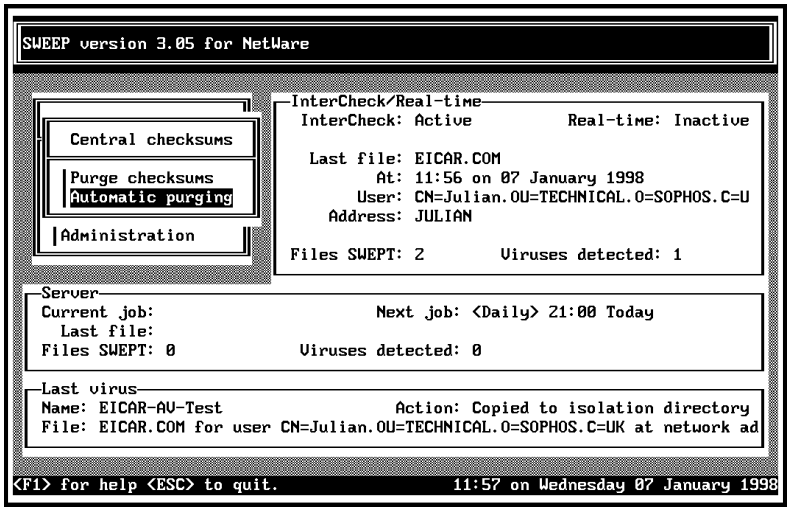
3. Unload SWEEP via the server console.

Central checksums

The *Central checksums* entry is used to administer the central InterCheck checksum file.

The central checksum file can be purged either on demand or automatically. The checksum database should normally be purged every time SWEEP is updated to ensure that the checksum file always represents objects authorised with the most recent version of SWEEP.

Select the *Central checksums* menu from the main menu.

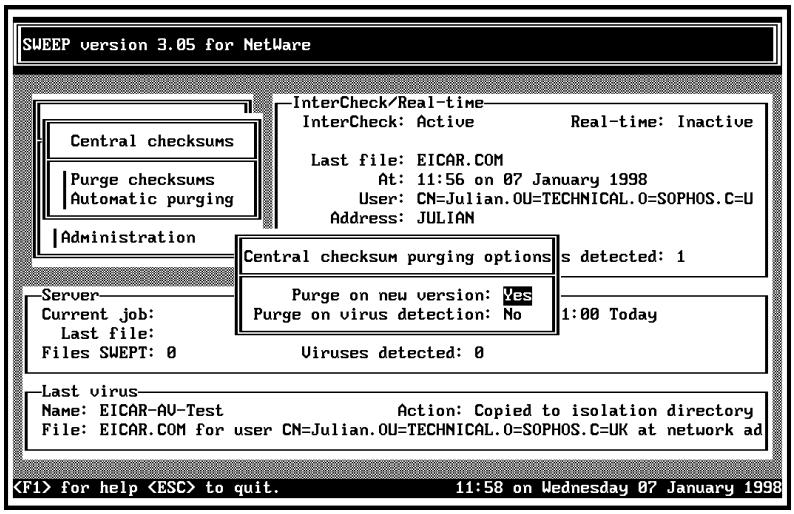


See the 'Checksumming options' section of the 'Configuring InterCheck clients' chapter for more information on InterCheck checksums.

Purge checksums

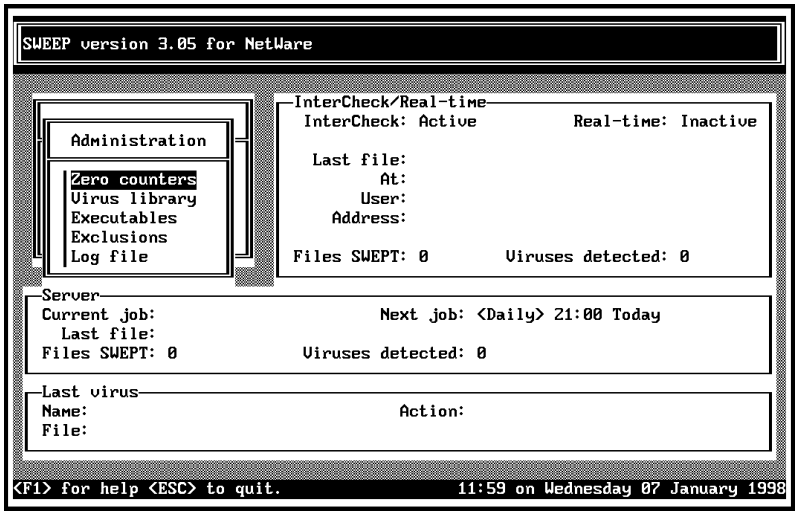
This option will purge the central checksum file.

Automatic purging



The *Purge on new version* option will purge the central checksum file every time the SWEEP NLM is updated, while *Purge on virus detection* will purge the central checksum file every time a virus is detected.

Administration

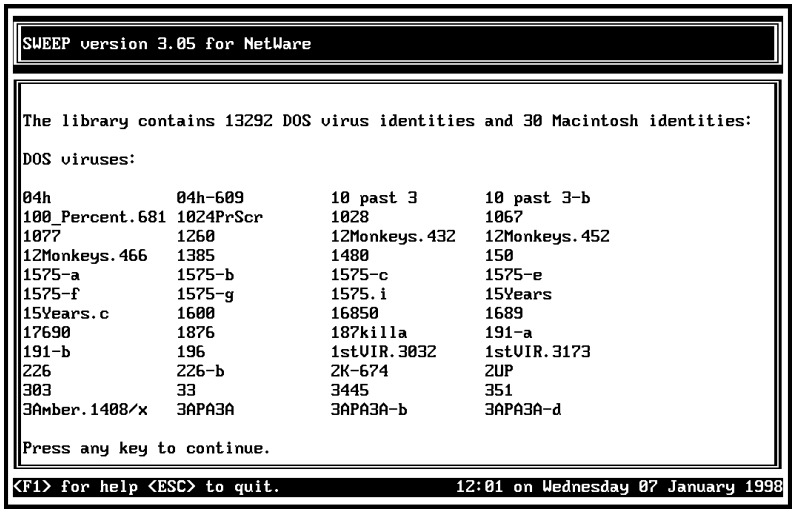


Zero counters

To zero the on-screen counters (such as the number of files checked and viruses detected), select *Zero counter*s from the *Administration* menu.

Virus library

To display a list of the viruses detected by SWEEP, select *Virus library* from the *Administration* menu.



Hint: The virus library can also be used to confirm that virus identities (see the 'Urgent SWEEP updates' section of the 'Installing SWEEP' chapter) have been correctly loaded by SWEEP.

Executables

View/modify

Selecting *Executables* then *View/modify* from the *Administration* menu will display a list of file extensions to be treated as executables by SWEEP. Use *Ins* to insert a new entry and *Del* to delete a highlighted entry. This list is only used if SWEEP is set to check 'All executables' rather than 'All files'.

Set default

This option will replace the existing default list of executable file extensions with those specified by the *View/modify* option.

Exclusions

This option makes it possible to exclude files from virus-checking. Use *Ins* to insert a new entry and *Del* to delete an entry from the list. Files may be specified by the full path (volume, directory and full filename) or by filename only. If filename only is used, files of that name will be excluded regardless of the directory they appear in. Subdirectories cannot be excluded.

Exclusions apply to immediate and scheduled job and real-time scanning, but not to InterCheck.

Log file

View

To display SWEEP's log file, select *Log file* then *View* from the *Administration* menu.

Clear

To clear SWEEP's log file, select *Log file* then *Clear* from the *Administration* menu.

Maximum size

This option allows the maximum size of the log file to be controlled. When the log file exceeds this size, the oldest entries in the file are discarded.

Note: To go directly to the end of the log file, press *Ctrl-PgDn*. On versions of RCONSOLE that do not support this key combination, use *Ctrl-x*.

SWEEP command line qualifiers

-BW Black and white display

If using a black and white or a monochrome display, better contrast should be achieved if SWEEP is started with the -BW qualifier, e.g.

```
LOAD SWEEP -BW
```

-DS NetWare Directory Services

SWEEP for NetWare supports NetWare Directory Services (NDS) on file servers running NetWare 4.x. This allows any user in the NDS tree to be notified about virus incidents, rather than just those in the bindery emulation context, as long that user has a connection to the server where the virus is found.

SWEEP must be loaded with the -DS qualifier to use this feature:

```
LOAD SWEEP -DS
```

See the 'Using NetWare Directory Services for virus reporting' section of the 'Using SWEEP' chapter for information on using the -DS qualifier for the first time, and the 'Notify group' section of the

'Configuring SWEEP' chapter for information on selecting NDS groups for notification.

-I Start immediate sweep

Immediate mode in SWEEP can be selected at load time by using the -I command line argument. For example

```
LOAD SWEEP -I
```

will load SWEEP and start immediate execution. This enables SWEEP to load and start execution from the AUTOEXEC.NCF file, should the supervisor choose to do so.

-WD Use non-standard directory

By default, SWEEP creates and uses the directory SYS:\SWEEP (referred to here as the server SWEEP directory) for all file-based operations. By using the command line qualifier

```
LOAD SWEEP -WD=directory
```

SWEEP can be made to use the directory *directory*.

Important! If this option is used, the client part of InterCheck must be set up to use the same directory.

Installing InterCheck clients

This chapter describes how to install and run InterCheck clients to provide on-access scanning for workstations.

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.

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

There are three steps to take when 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. See the 'Installing the InterCheck server' section below.

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

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

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

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

The 'Advanced options for networked InterCheck clients' section should also be consulted if:

- Using InterCheck on a multiple-server network.
- Using a dedicated server for the InterCheck server.
- Creating groups of InterCheck users.

Installing the InterCheck server

This section assumes that SWEEP.NLM has already been loaded (see the 'Installing SWEEP' chapter).

Log in to the server with SUPERVISOR privileges. Insert the Sophos Anti-Virus CD and at a DOS prompt enter

```
D:\INTERCHK\ICINSTAL
```

where D: is the CD drive.

If there is more than one server on the network, select the desired server from the *Where* menu.

In most situations the default options should be used. To use non-standard options, select the *Options* menu. See the 'Configuring InterCheck clients' chapter for a description of the different options available.

To start the installation, select *Onto file server* from the *Install* menu and follow the instructions.

At the server console, or using RCONSOLE, switch to the SWEEP for NetWare screen, select *InterCheck* from the main menu, and set InterCheck Status to *Active*. The InterCheck server is now ready to process client requests. The other options can initially be left in the default state and configured once the system is operational (see the 'Configuring SWEEP' chapter).

Now follow the instructions for the relevant operating system below.

Installing networked InterCheck clients for DOS and Windows

With a login script

Important! For ease of installation and troubleshooting, it is recommended to create a group of users who will run InterCheck, and add new members gradually, rather than installing InterCheck for every workstation at once. The instructions assume that this will be done.

Note: InterCheck for DOS has been designed to run from the login script and (unlike many TSRs) will not split base memory when loaded in this way.

NetWare 3.x servers

Use SYSCON to edit the system login script to include the following:

```
MAP INS S1:=SYS:SWEEP
IF MEMBER_OF "INTERCHECK" THEN BEGIN
#ICLOGIN
END
```

This will run InterCheck for users in the group INTERCHECK.

NetWare 4.x servers

Edit the login script for the appropriate Organization or Organizational Unit to include the following:

```
MAP INS S1:=SYS:SWEEP
IF MEMBER_OF "INTERCHECK" THEN BEGIN
NOSWAP
#ICLOGIN
END
```

If the NOSWAP command causes problems with other DOS applications run from the login script, such applications should be run before the NOSWAP command.

Without a login script

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

```
MAP I:=Server/Volume:SWEEP
I:\SWEEP\INTERCHK
```

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

Installing networked InterCheck clients for Windows 95

With a login script

See the instructions in the 'With a login script' subsection of the 'Installing 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 in 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.

Installing networked InterCheck clients for Macintosh

Important! Macintosh InterCheck clients, like other InterCheck clients, must be able to read and write to the server SWEEP COMMS directory. However, this is only possible on volumes that support Mac namespace. For existing InterCheck users, this means either adding Mac namespace to the volume where the SWEEP directory is placed, or re-installing the InterCheck files on a volume which already has Mac namespace and using the command

```
LOAD SWEEP -WD=MacVol:SWEEP
```

from the server to run the SWEEP NLM.

If the latter option is adopted, and the old InterCheck server installation is removed, the existing InterCheck client installations must be updated to use the new InterCheck server.

If using the Sophos Anti-Virus CD, locate `Icme400o.img` in the `DiskImgs` folder and use it to make a floppy disk with the utility supplied. At the Macintosh workstation, insert this disk into the floppy drive.

Drag the InterCheck icon from the floppy into the System Folder:Extensions directory and restart the Macintosh.

InterCheck will automatically scan the network for a server running a version of SWEEP when it is required to authorise a file. A valid server is the one that has been selected via the ‘chooser’ and is visible on the Desktop (there can be more than one server connected). If there is no connection to a server running SWEEP or a virus is found, the file will not be authorised and it will be prevented from running.

InterCheck will create an invisible file on the Mac to hold the checksum of every executable which has been run. The first time that an application is run, it will be sent to the server for scanning and if no viruses are found, a checksum will be generated.

Advanced options for networked InterCheck clients

InterCheck on multiple-server networks

If there is more than one file server that workstations can log in to, there are implications for InterCheck.

For some clients, logging into a new server deletes all existing drive mappings, including that used to load InterCheck. In this case, InterCheck will revert to operating as if installed on a stand-alone PC. However, if InterCheck has also been installed on the new server, a new link will be established and full InterCheck functionality will be maintained.

The initial installation of InterCheck automatically approves for use the Novell utility programs (such as LOGIN.EXE). If the user logs out from the server, InterCheck will revert to stand-alone operation, and the user will be able to log back in and resume normal operation.

Using a dedicated SWEEP server

It is possible to route client requests to a file server dedicated to running the SWEEP InterCheck server. To do this, specify the server by name when installing the InterCheck client, e.g. in the login script:

```
MAP INS S1:=SERVER\SYS:SWEEP
#ICLOGIN
```

Creating groups of InterCheck users

Groups of InterCheck users can be specified as described in ‘Installing networked InterCheck clients for DOS and Windows’. Alternatively, to exclude certain users from loading InterCheck, create a group of those users and add these lines to the login script:

```
MAP INS S1:=SYS:SWEEP
IF NOT MEMBER_OF "IEXCLUDE" THEN BEGIN
#ICLOGIN
END
```

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

It is important to ensure that InterCheck is still run from the server whenever the workstation is connected to the network, as described in the 'Installing networked InterCheck clients' section. This ensures that the local copy of InterCheck is updated automatically if the central version on the server is updated.

Starting ICINSTAL

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
```

Clients with no network access

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

```
D:\INTERCHK\ICINSTAL
```

at a DOS prompt, if the CD is in drive D:.

Using ICINSTAL

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

To use non-standard installation options, select the *Options* menu. 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.

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 'Installing 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.

The automated installation program

The InterCheck client for Windows for Workgroups is installed with an automated installation program, which, used with its default settings, will:

- Install the InterCheck client files onto client WFWG workstations, requiring no user input when used with the default settings.
- Use the default preset configuration options, or the configuration options in the configuration file specified by the system administrator on the server.
- Ensure that InterCheck is run every time the workstation is started.
- Ensure that local InterCheck files (including configuration files) are kept up to date.

For information on changing the default settings, and on alternative approaches to installation, see 'Before installing the InterCheck client' below.

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 '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 'Installing manually from the client' below.

Interactive or non-interactive installation?

Both methods of installation can be used interactively. 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.

Enter the lines

```
MAP I:=Server/Volume:Directory
I:\ICLOGIN -A
```

where *Server*, *Volume* and *Directory* are the names of the server, volume and directory containing the InterCheck files respectively.

The next time that Windows is restarted and 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, 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 (Universal Naming Convention) format, removing any dependency on the initial drive mapping. For example

```
MAP I:=Server/Volume:Directory
I:\ICLOGIN -A -U
MAP DEL I:
```

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.

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.

Dealing with viruses

The method used to deal with a virus depends on where that virus is found.

Viruses on the NetWare server

If a virus is found on the NetWare server, see ‘Eliminating viruses on the NetWare server’ below.

Viruses on a workstation

If the InterCheck server finds a virus on an InterCheck client, it should be dealt with on the client workstation. Use the version of SWEEP specific to the workstation’s operating system, or SWEEP for DOS. See the ‘Treating viral infection’ chapter of the relevant Sophos Anti-Virus manual.

Eliminating viruses on the NetWare server

The action taken against viruses found on the file server depends on which kind of item is infected.

Files with macro viruses

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

facility is enabled by selecting *Disinfect* from the *Macro viruses* option in SWEEP's Immediate and/or Scheduled menus (see the 'Macro viruses' section of the 'Configuring SWEEP' chapter). If disinfection fails, the chosen removal mode will be applied to the infected file. By default, SWEEP does not disinfect macro viruses.

Infected executables

It is generally inadvisable to attempt to disinfect infected executables. This is because it is difficult to ensure that the executable has been properly restored after disinfection; it may be unstable which may put valuable data at risk.

Infected executables can be moved to an isolation directory; renamed in such a way that they cannot be executed by users; deleted; purged; or copied with non-executable filenames. See the 'Removal mode' section of the 'Configuring SWEEP' chapter.

Infected boot sectors

NetWare servers are not currently susceptible to boot sector viruses (see the 'Why is virus checking needed for NetWare?' section of the 'About Sophos Anti-Virus' chapter).

Troubleshooting

This section provides answers to some common problems encountered when using Sophos Anti-Virus under NetWare.

Insufficient server memory

The typical server memory requirement for SWEEP.NLM is 4Mb. If the server has insufficient memory it may behave unpredictably.

In 1995 Novell published the 'NetWare 3 and 4 Server Memory Worksheet' to help users calculate the amount of memory needed for their NetWare 3 and 4 servers. This is currently available via the Novell Web site (http://www.novell.com/).

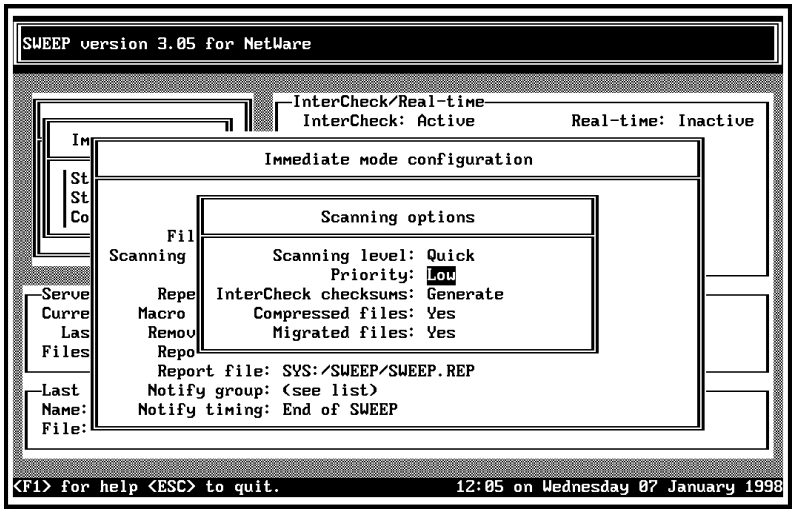
SWEEP abends during loading on NetWare 4.0x

Bindery emulation must be enabled before SWEEP is run on NetWare 4.0x. This is the default setting when NetWare 4.0x is installed.

SWEEP slows down the network

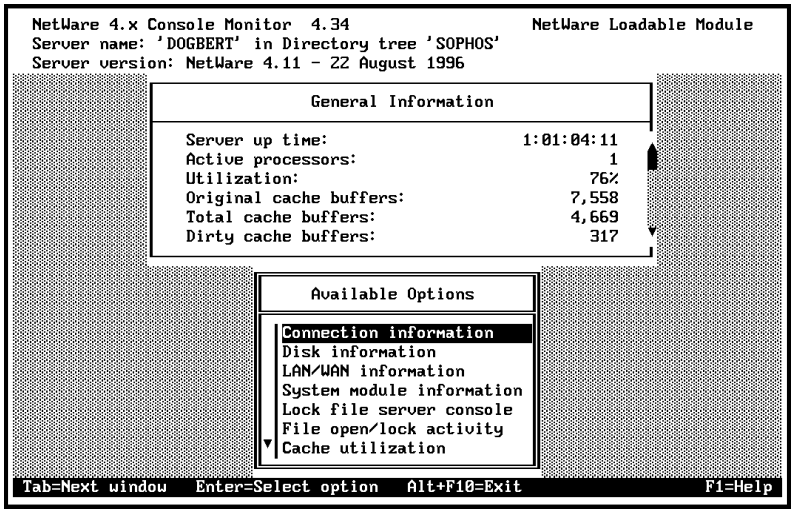
SWEEP can run in high or low priority mode. In high priority mode it may slow down the server noticeably, while in low priority mode the effect on server performance should be negligible. Under some circumstances running in 'quick' mode may have a greater impact on network performance than running in 'full' mode.

If your server slows down considerably, make sure that the priority of running is set to *Low*. This will have to be checked in *Immediate mode configuration* as well as in all scheduled jobs.



MONITOR shows a high percentage of time devoted to SWEEP

The Novell program MONITOR.NLM shows the file server utilisation as a percentage. When the network is idle, this may be 1% or 2%. When SWEEP is started in immediate mode, or while a scheduled SWEEP is running, utilisation may jump to over 70%, which can concern system administrators.



However, SWEEP utilises any processing time **during which the server would otherwise be idle**; if other requests for resources are made, SWEEP will give up those resources to the requesting process.

A high utilisation figure when running SWEEP should not be a cause for concern and will not normally be reflected in any impact on network performance.

Scheduling does not work

Note that if SWEEP is scheduled to run at a predetermined time and day, it must be left loaded. The user must **not** unload the software either via the menu system, or by using the UNLOAD command.

Hint: NetWare is a multi-tasking system which allows several processes to run at the same time. You can switch between screens by pressing *Alt* and *Esc* at the same time.

Unclear text displayed on monitor

Check if the monitor is black and white. If it is, use the -BW command line qualifier when loading SWEEP:

```
LOAD SWEEP -BW
```

InterCheck displays a warning but the keyboard locks

Ensure that KEYB command in AUTOEXEC.BAT is placed **before** InterCheck, as a conflict will otherwise result.

InterCheck does not examine a disk when first accessed

InterCheck intercepts all high-level disk accesses and checks the disk before the first one is allowed to proceed. Disk editors such as *Norton Utilities* access the disk using low level functions which are not

trapped by InterCheck. This may result in an infected disk not being examined by InterCheck and remaining accessible to the disk editor.

Diskless workstations are unusable after logging into new server

Check that InterCheck has been installed on the new server. If it has not been, the InterCheck client will be unable to access the list of checksums and will refuse to execute any programs.

InterCheck client refuses to load high

Check the following:

a) The PC is running DOS 5 or greater

b) An appropriate memory manager, such as EMM386, has been loaded to provide UMB support

c) The line

```
DOS=UMB
```

is present in the CONFIG.SYS file

d) There is a free UMB of sufficient size to load InterCheck TSR

InterCheck may also refuse to load high if the OPTIMIZE program supplied with QEMM modifies the AUTOEXEC.BAT file so that LOGIN is executed using the LOADHI program with options '/r:l /lo'.

Removing the LOADHI from the LOGIN entry in AUTOEXEC.BAT cures the problem.

Windows slows down on startup

When starting Windows, tens of files are executed transparently to the user. If the list of InterCheck checksums gets deleted, every item will be sent to the

server for checking. This may slow down the startup process, but it will happen only once.

Installation of new software slows down

InterCheck will intercept new software while it is being installed on a PC. This slows down the installation process.

On stand-alone PCs the installation may fail due to InterCheck refusing to execute unknown software. If that is the case, remove InterCheck, install the software, and reinstall InterCheck. Then sweep the disk.

InterCheck displays a warning

If InterCheck reports any of the following warning messages

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

it is necessary to use either or both of the configuration options MaxPathLength and MaxAddressLength in the INTERCHK.CFG InterCheck configuration file. These instruct InterCheck to reserve additional memory for subsequent configuration changes. Under normal circumstances these options are not required. For example:

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

MaxPathLength — defines the maximum length of the program and communication directory names that will be supported by InterCheck.

MaxAddressLength 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.

Workstation runs slower after InterCheck is installed

InterCheck will run much more slowly if a disk cache has not been installed.

InterCheck displays a warning that the file must be swept

When the communication between the server and an InterCheck client fails, new programs can no longer be automatically authorised. A message box appears stating that the file must be swept for viruses and access to the program is denied.

The diagnosis depends on whether a 'Server virus scanner is currently unavailable' message appears first, or not.

'Server virus scanner is currently unavailable'

This message is displayed if a fault occurred while communicating with the server or if no answer was received from the server process.

If a 'please wait' message was displayed for more than one minute before the 'Server not available' message was displayed, the client timed out waiting for a response. Try increasing the time-out parameter (ServerTimeout) in the INTERCHK.CFG file.

If a 'please wait' message was displayed for a few seconds before the 'Server not available' message was displayed, the transfer of the program to the server has failed in the middle. Check the amount of space available to the user. There must be sufficient space to

copy the program being checked into the COMMS directory. Under NetWare the amount of space available can be restricted in a number of different ways; the volume may be full, directory restriction may have been imposed or there may be a restriction specific to the current user.

If a 'please wait' message flashes briefly before the 'Server not available' message is displayed, the communication with the server failed almost immediately. The most common reason is that the user does not have write access to the COMMS directory. The user must have Read, Write, File scan, Modify and Erase permission in this directory.

The 'Please scan file for viruses' message appears immediately

This is the expected response when InterCheck is not connected to a network. It means that the client can no longer detect the presence of the server process. The InterCheck client looks for a file called IC.STA in the server SWEEP\COMMS directory. No attempt is made to communicate with the server if this file is not present. There are a number of reasons why InterCheck may not be able to find the IC.STA file.

a) The driver mapping which InterCheck was using to communicate with the server has been deleted or changed. This is normally the drive from which InterCheck is started. In Windows it is possible to enable permanent drive mapping which will be reset on starting Windows, overriding the required mapping.

b) The server process may not be loaded or enabled.

c) InterCheck has been loaded from the fixed disk and has started in stand-alone mode. Normally, to enable the network operation, you need to execute the networked copy of InterCheck. This informs the resident version of InterCheck where the COMMS directory is located.

Testing the client/server communication link

See the 'Testing InterCheck functioning' section of the 'Installing InterCheck clients' chapter for information on testing the client/server communication link.

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. See also the 'Urgent SWEEP updates' section of the 'Installing SWEEP' chapter.

Further help needed

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

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

By email to support@sophos.com

Questions can be sent to Sophos by email. Please include as much information as possible, including SWEEP and InterCheck version, operating system and patch level, 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.

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 booting a microcomputer from a floppy disk.

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

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

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.

Diskless Workstation: A PC which does not contain a floppy disk drive and is connected to a network.

DNS: Domain Name System; the distributed database used to translate human-readable Internet addresses (e.g. 'sophos.com') into numeric IP addresses (e.g. 193.82.145.1). IP addresses are difficult to remember and change if a machine moves, unlike DNS names. Domain names are hierarchical; for example 'elbereth.sophos.com' is the machine 'elbereth' in the network 'sophos', which belongs to the 'com' top-level domain for commercial entities.

DOS: Disk Operating System. See MS-DOS.

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

EXE: The extension given to executable files in MS-DOS. These are similar to COM files, but can contain more than 64K of code and data.

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 Mb 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.

InterCheck: Proprietary Sophos technology which enables a server-based virus scanner to be used for scanning workstations connected to the network.

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

I/O Port: A computer communicates with the outside world through Input/Output (I/O) ports. Examples are the RS-232 serial port and printer ports on a PC.

IP: Internet Protocol; the base level of the TCP/IP system. It is a connectionless, unreliable datagram service. 'Datagram' means that all communications

	are made up of packets; 'connectionless', that each network packet is separate and individually routed; and 'unreliable' means that packets are not guaranteed to get through. An IP packet contains two IP addresses for its source and destination.
IP Address:	A numeric Internet address; a 32-bit binary number, normally written in dotted-decimal notation; e.g. '194.82.145.1'.
LAN:	Local Area Network; a data communications network covering a limited area (up to several kilometres in radius) with moderate to high data transmission speeds.
Link Virus:	A virus which subverts directory entries to point to the virus code.
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.
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.
MS-DOS:	The Disk Operating System sold by Microsoft. It is the most common microcomputer operating system in the world, and operates on the IBM PC.
Multipartite Virus:	A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector viruses and parasitic viruses.

NLM: NetWare Loadable Module; a program which runs as a process on a Novell NetWare file server.

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

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

Partition Table: A 64-bit table found inside the master 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.

TCP: Transmission Control Protocol; a reliable, connection-oriented, stream-type service built on top of IP. IP is too ‘raw’ a protocol for applications to use, so other protocols like TCP sit above it providing additional functionality. TCP provides a two-way data stream, and port numbers in order to differentiate between different TCP connections. Well-known services exist on standard port numbers; SMTP email is on port 21, and HTTP is port 80. Application protocols such as Telnet, FTP and HTTP are built on top of TCP.

Timeout: A logical access control feature which automatically logs-off users of terminals which do not exhibit signs of activity for a certain duration of time.

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.

UMB: Upper Memory Block. DOS=UMB statement in the CONFIG.SYS file specifies that DOS should maintain a link between conventional memory and the upper memory area. This must be specified if programs or device drivers are loaded there.

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.

URL: Universal Resource Locator; a World Wide Web 'address'.

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

F

H

I

Q

R

S

T

U

V

W

X

Z

User comment form

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

Product: _____ Version: ❒.❒❒

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

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

Please indicate any errors found in this software or documentation:

_____

_____

_____

Please give any suggestions for improving the software or documentation:

_____

_____

_____

Name: _____

Position: _____

Organisation: _____

Address: _____

_____

Telephone: _____ Fax: _____

Signed: _____ Date: _____

Australia:

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

Bahrain:

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

Belgium:

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

Brazil:

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

Channel Islands:

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

Croatia:

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

Denmark:

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

Finland:

Oy Protect Data Ab
P.O. Box 48
00931 Helsinki
Finland
Email antti.laaja@dlc.fi
Tel 09 752 521 · Fax 09 7525 2210 · Code +358

France:

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

Germany:

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

Hong Kong:

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

Ireland:

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

Italy:

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

Japan:

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

Malta:

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

Netherlands:

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

Forum Data Security
WG Plein 202
1054 SE Amsterdam
The Netherlands
Email forum_data_security@pi.net
Tel 20 685 3486 · Fax 20 612 9702 · Code +31

New Zealand:

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

Norway:

Protect Data Norge AS
Brobekkveien 80
0583 Oslo
Norway
Email protect_data@oslonett.no
Tel 022 65 64 50 · Fax 022 65 64 58 · Code +47

Poland:

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

Portugal:

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

Singapore:

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

Slovakia:

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

Slovenia:

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

Spain:

Sinutec Data Security Consulting S.L.
Traversera de Gracia 54-56 Entlo. 3 y 4
08006 Barcelona
NIF B-60062502
Spain
Email sinutec@ysi.es
http://www.sinutec.com/
Tel 93 490 70 52 · Fax 93 490 76 04 · Code +34

Sweden:

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

Switzerland:

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

Turkey:

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

United States of America:

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

Uruguay:

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

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

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