Sophos Anti-Virus

User Manual

Windows NT

SOPHOS

Sophos Anti-Virus

for Windows NT

User Manual
October 1997

This manual documents Sophos Anti-Virus
for Windows NT, 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 # maswez0f/970919

This document is also available in electronic form from Sophos.

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

Contents

SWEEP for Windows NT quick start guide

This chapter summarizes the installation process and provides a quick tour of SWEEP. It is aimed at users familiar with both Windows NT and previous versions of SWEEP. Subsequent chapters and the on-line help provide more detailed information.

Installing and starting SWEEP

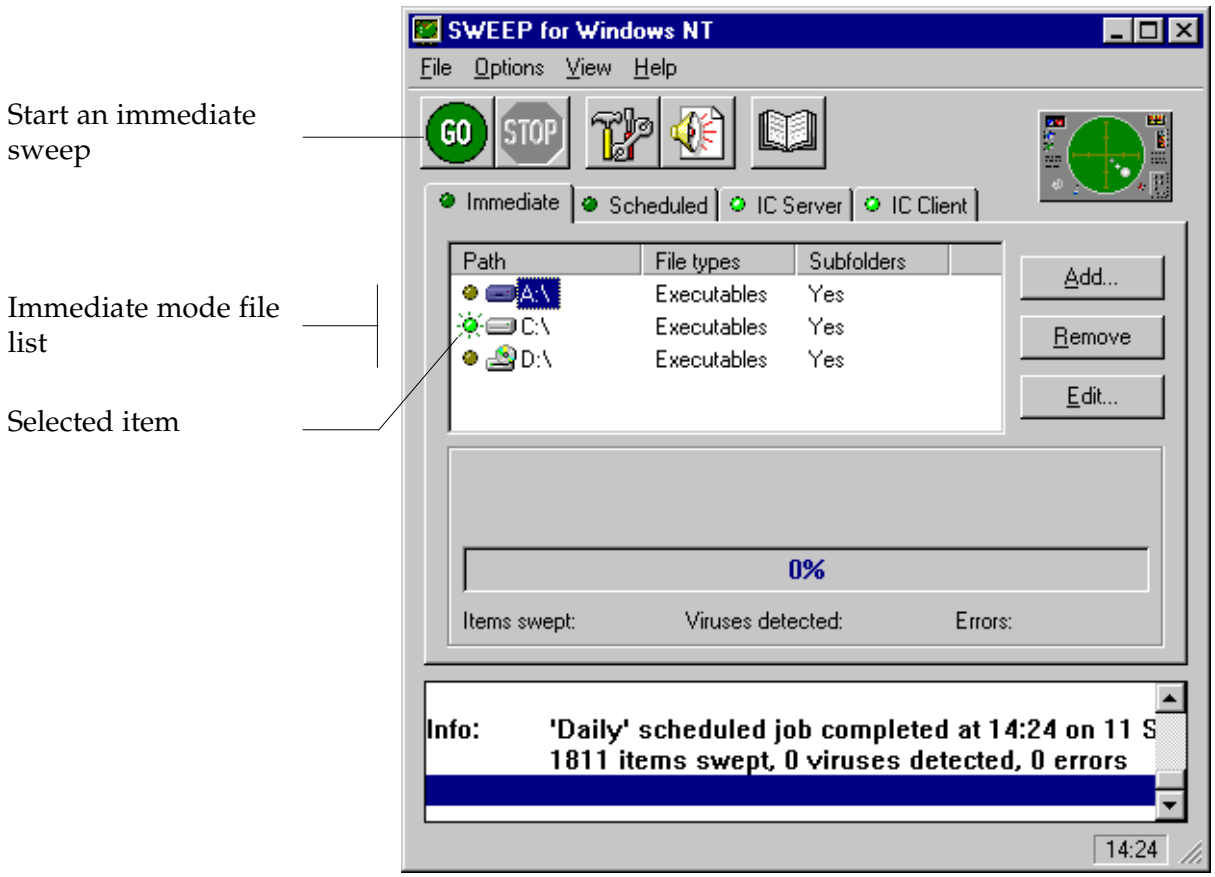
Log in as a user with local Administrator privileges, run SETUP.EXE from the SWEEP for Windows NT installation disk, and follow the SWEEP installation program's instructions.

The 'Local installation/upgrade' will install SWEEP with immediate and scheduled mode facilities enabled. The 'Central installation/upgrade' will place the SWEEP installation program on the file server. Installations made from a central installation can be set to update automatically when the version on the server is updated.

'Enable InterCheck Client' will add InterCheck facilities to this, 'Enable InterCheck Server' will allow the workstation to act as an InterCheck server for other machines on the network, and 'Enable scheduled sweeping of network resources' will enable the scheduled mode to check network drives.

Select the option to run SWEEP as soon as the installation program has finished.

Sweeping local hard drives



By default, the immediate mode file list contains all local drives, with all the local hard drives selected.

To sweep all the selected drives, paths and files, select *Go* from the *File* menu or click the associated *GO* icon.

Sweeping a floppy disk

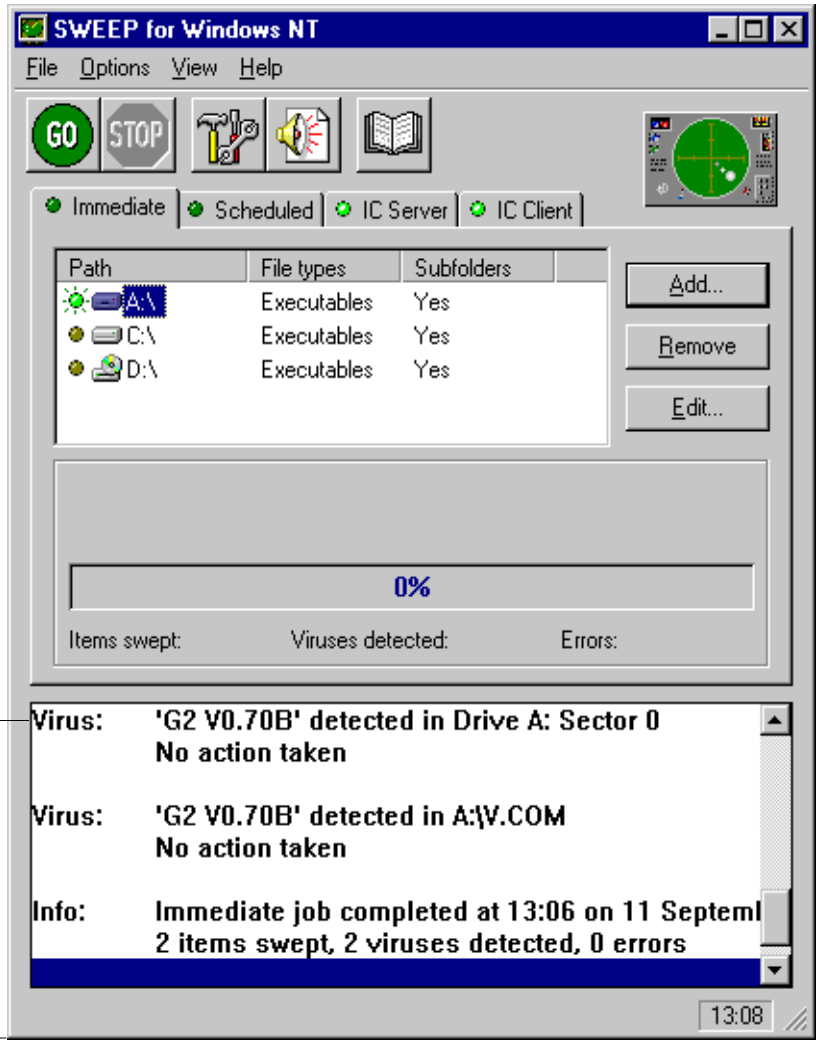
To sweep a floppy disk, insert the disk and double-click on its icon in the file list. Alternatively, deselect the local hard drive(s), select the floppy disk (in this example A:\), and start an immediate sweep as described above.

Finding a virus

If SWEEP discovers a virus - do not panic!

SWEEP will help with the disinfection process, providing features to disinfect infected files and boot sectors automatically.

If SWEEP discovers a virus, a warning will appear at the end of the sweep job and a 'virus detected' entry will appear in the on-screen log:



'Virus detected' entry

Drag lower edge of SWEEP window to expand on-screen log

To display more details about that virus, double-click on the 'virus detected' entry in the on-screen log. This

will display a virus information dialog which includes advice on removing that particular virus (see the 'Information on a particular virus' section of 'The virus library' chapter).

For more information on dealing with a virus, see the 'Treating viral infection' chapter, or SWEEP's on-line help.

About SWEEP

This chapter introduces SWEEP, describes features specific to SWEEP for Windows NT, and helps users identify the most relevant chapters for their needs.

What is SWEEP?

SWEEP offers on-demand, scheduled and (with InterCheck) on-access virus checking, along with automatic reporting and disinfection.

Virus checking for Windows NT

At the time of writing, there are no known Windows NT specific viruses. However, Windows NT machines are subject to virus infection:

- Macro viruses can infect documents on any operating system supported by the relevant application.
- Boot sector viruses can infect PCs irrespective of the operating system they are running. However, many assume they are infecting a DOS machine, which can lead to unforeseen consequences for Windows NT machines.
- DOS viruses can replicate and infect DOS programs running on Windows NT machines.

SWEEP and Windows NT

Under Windows NT, services can be run independently of users, and their access rights do not depend on the logged on user. This affects SWEEP's structure and the way it is installed and run.

SWEEP for Windows NT has two distinct components, with different functions and privileges:

- The SWEEP service.
- The SWEEP Graphical User Interface (GUI).

The SWEEP service

The SWEEP service includes all SWEEP and InterCheck functions along with the scheduler and notification system.

As a Windows NT service, this runs independently of any users and of the GUI, and must log on in its own right, using a service account.

The account that the SWEEP service uses depends on the options selected when installed:

- **If SWEEP is used for sweeping local disks only**, a System account, which is used by default, is sufficient.
- **If SWEEP requires network access** (for scheduled sweeping of the network), a non-System account may be required.

The account used is determined when SWEEP is installed, but can be changed at a later date. See the 'Managing the SWEEP services' section of the 'Installing SWEEP' chapter.

The SWEEP GUI

The SWEEP GUI allows the user to perform immediate mode (i.e. on-demand) virus checking

and, if the GUI user has sufficient privileges, to further control and configure the SWEEP service.

The GUI is not a Windows NT service, and operates with the same privileges as the current user.

Depending on their rights, the user of the GUI may not have access to SWEEP's scheduled mode, InterCheck client mode and InterCheck server mode pages. They may also not be able to access the same items via the immediate (i.e. on-demand) mode as they can via the scheduled mode.

Features of SWEEP for Windows NT

SWEEP for Windows NT:

- Checks local hard disks, floppy disks and networks for the presence of all viruses known to Sophos at the time of SWEEP's 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, and includes a stand-alone InterCheck client for on-access scanning of unknown items.
- Is updated twelve times a year, and 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.
- Detects and disinfects Microsoft Word and Excel macro viruses.
- Provides automatic updating for networked PCs.
- 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 virus fragments in every part of every file.

- Is easy to use, and easily integrated into complex virus-checking applications, such as the automated unattended checking of file servers.
- Features an 'immediate mode' which allows checking on demand, along with a 'scheduled mode' which allows multiple scheduled jobs to be configured for automatic operation, even when no-one is logged in to the machine.
- Can notify network managers of the discovery of a virus automatically, via the event log, network messages, and SMTP email.
- Includes an extensive on-line virus information database.
- Is a 32-bit application and is fully Windows NT compliant.

How to use this manual

This manual is organised into the following chapters:

- 'SWEEP for Windows NT quick start guide' summarizes the installation process and provides a quick tour of SWEEP.
- 'About SWEEP', this chapter.
- 'About InterCheck' presents an overview of Sophos' InterCheck technology.
- 'Installing SWEEP' describes how to install and upgrade SWEEP.
- 'Using SWEEP' shows how to start SWEEP, start an immediate sweep, change the items to be included in immediate and/or scheduled jobs, activate the InterCheck server and InterCheck client, close down the SWEEP GUI, and use the InterCheck monitor.

- 'Configuring SWEEP' introduces the configuration options used by the immediate, scheduled and InterCheck modes.
- 'SWEEP alert message options' describes the options available for notifying users of SWEEP activity.
- 'SWEEP options' describes the options available through the *File*, *Options* and *View* menus.
- 'The virus library' details the on-line virus library.
- 'Installing InterCheck clients' describes how to install and run InterCheck clients.
- 'Configuring InterCheck clients' describes the configuration of InterCheck clients running under Windows 95, Windows for Workgroups, Windows 3.x, and DOS.
- 'CLI SWEEP for Windows NT' documents the Command Line Interface (CLI) version of SWEEP for Windows NT.
- 'Treating viral infection' describes SWEEP for Windows NT's automatic disinfection facility and other mechanisms for dealing with viruses.
- 'Troubleshooting' provides answers to some common problems which can be encountered when using SWEEP.
- 'On-screen log messages' contains information about the on-screen log messages.

The chapters to be consulted depend on the use(s) to which SWEEP will be put:

On-demand scanning of local workstations only

If using SWEEP for Windows NT simply to check a local disk for viruses, it should be sufficient to read the 'SWEEP for Windows NT quick start guide'.

On-access scanning

If using SWEEP for on-access scanning of files, read the 'About InterCheck' and 'Installing SWEEP' chapters.

More advanced features

If configuring SWEEP and using its more advanced features, read the 'Using SWEEP', 'Configuring SWEEP' and 'SWEEP options' chapters.

Centralised distribution of SWEEP

If using a file server installation for the centralised distribution, scheduling and upgrading of SWEEP, read the 'Installing SWEEP', 'Using SWEEP', 'Configuring SWEEP' and 'SWEEP options' chapters.

On-access scanning for a networked environment

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

Command line SWEEP

If installing and using the command line version of SWEEP for Windows NT, read the 'CLI SWEEP for Windows NT' chapter.

General information

For further information, read 'The virus library', 'Treating viral infection', 'Troubleshooting', and 'On-screen log messages' chapters.

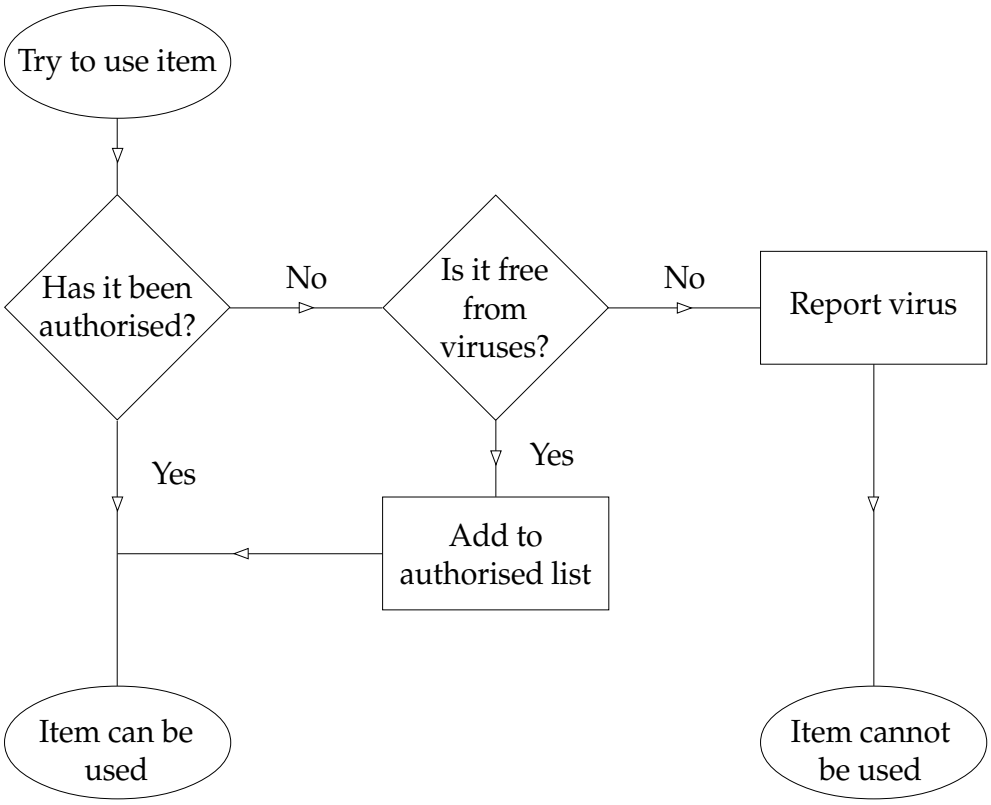
Note that much of the material in this manual is available via the on-line help system. Also note that, unless otherwise specified, references to SWEEP for Windows NT refer to the GUI version of SWEEP for Windows NT.

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.

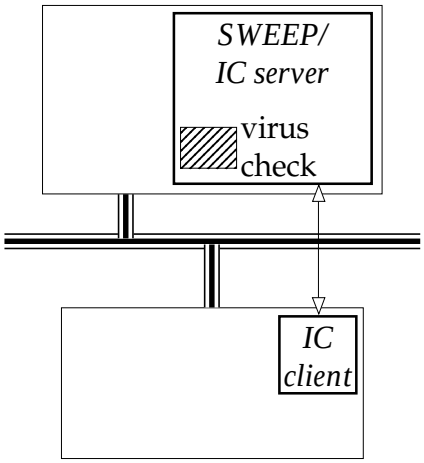
A **stand-alone InterCheck client** does not have to communicate with a remote InterCheck server, and uses a local installation of SWEEP to check for viruses.

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.

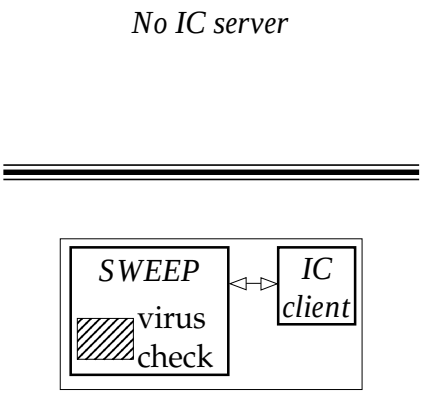
Either way, InterCheck is the most efficient way of protecting users from viruses: each item is checked for viruses only once, unless it is modified, in which case it is rechecked.

How does InterCheck work?

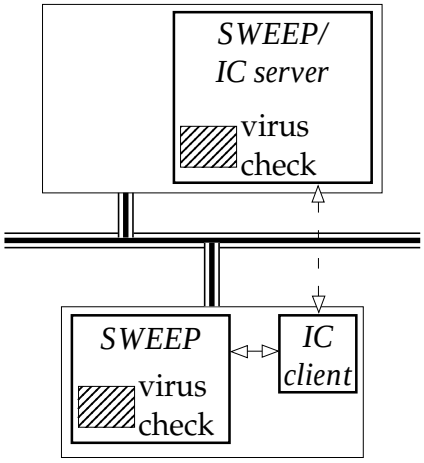
The InterCheck client software monitors all file and disk accesses. Whenever an item is accessed, it is



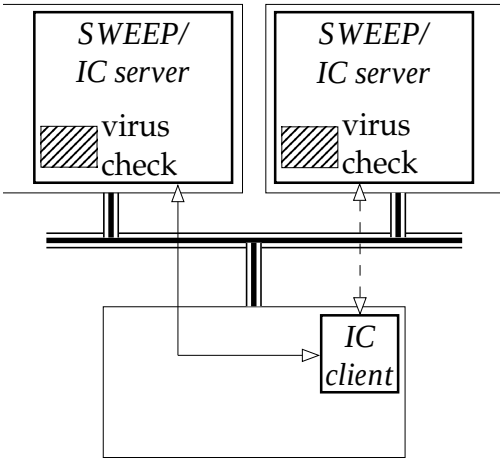
Networked IC client and remote IC server



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 checks with a 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 and CD-ROMs.

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, OS/2 & Banyan VINES

See the SWEEP for Windows NT, NetWare, OpenVMS, OS/2 and Banyan VINES user manuals (i.e. the InterCheck server's SWEEP user manual) respectively.

DOS

See the SWEEP for DOS user manual.

Networked InterCheck client installation and configuration

Installation

DOS, Windows, Windows 95 & Macintosh

See the 'Installing InterCheck clients' chapter of the InterCheck server's SWEEP user manual.

Configuration

DOS, Windows & Windows 95

See the 'Configuring InterCheck clients' chapter of the InterCheck server's SWEEP user manual.

Stand-alone InterCheck client installation and configuration

Installation

DOS/Windows 3.x & Windows for Workgroups

See the 'Installing InterCheck clients' chapter of the InterCheck server's SWEEP user manual.

Windows 95 & Windows NT

See the 'Installing SWEEP' chapters of the SWEEP for Windows 95 and SWEEP for Windows NT user manuals respectively.

Configuration

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

See the 'Configuring InterCheck clients' chapter in the InterCheck server's SWEEP user manual, and also in the SWEEP for Windows 95 user manual.

Windows NT

See the 'Configuring SWEEP' chapter of the SWEEP for Windows NT user manual.

Installing SWEEP

This chapter describes how to install and upgrade SWEEP for Windows NT.

System requirements

The minimum requirements to use SWEEP for Windows NT are:

- An Intel 386, or an Alpha AXP based computer.
- Microsoft Windows NT 3.51 or later. For systems running Windows NT 3.1-3.5 see the 'CLI SWEEP for Windows NT' chapter.
- 6 Mb of free hard disk space on an Intel machine, or 8 Mb on an Alpha machine.

Preparing to install SWEEP

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

Local or central installation?

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

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

1. The SWEEP installation files are placed on a file server.

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

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

Which features should be installed?

SWEEP for Windows NT can be installed with any, all or none of the following optional features:

InterCheck support

InterCheck allows on-access checking of all files (see the 'About InterCheck' chapter).

The **InterCheck client** will check all files accessed on the workstation. It does not require a separate InterCheck server.

The **InterCheck server** is needed only if SWEEP is to be used as an InterCheck server by networked InterCheck clients on remote, non-NT machines. For information on installing networked InterCheck clients, see the 'Installing InterCheck clients' chapter.

Scheduled network access

Enables SWEEP to run scheduled sweeps of files on remote machines. Note that immediate sweeps of such files can be performed without selecting this option.

Automatic upgrading

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

Starting the SWEEP installation program

Log in as a user with local Administrator privileges, insert the SWEEP for Windows NT installation disk into the floppy disk drive, and run SETUP.

Note: If performing Stage 2 of central installation (from file server to workstation), run SETUP from the central installation.

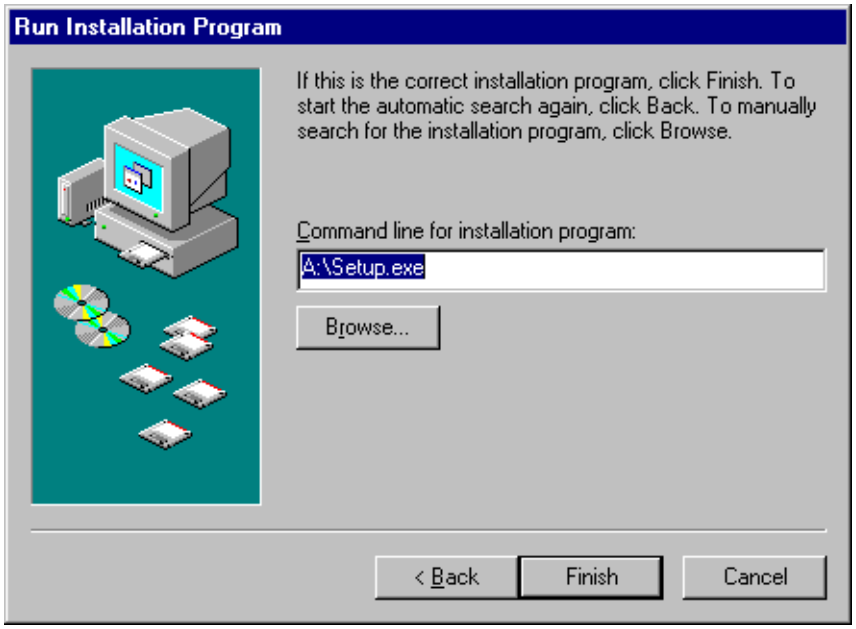
To run SETUP under Windows NT 4:

Click Windows NT *Start*, click *Settings*, followed by *Control Panel*.

Double-click the *Add/Remove Programs* icon in the Control Panel.

On the *Install/Uninstall* tab, click *Install*.

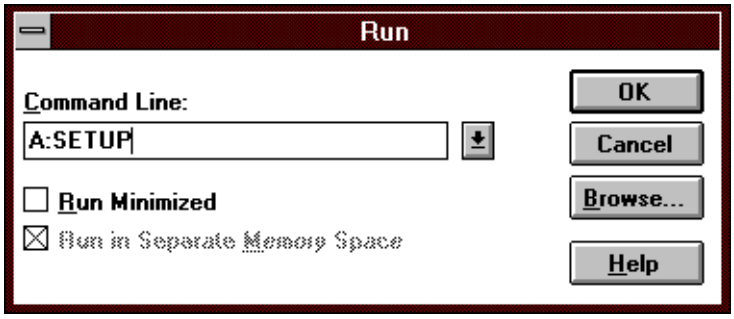
The SWEEP installation program is called SETUP.EXE.



Click *Finish* to accept this and start the SWEEP installation program.

To run SETUP under Windows NT 3.51:

Select *Run* from the Program Manager's *File* menu and enter the command line



to start the SWEEP installation program.

Installing SWEEP

The sections below give step-by-step instructions for:

- **Local installation of SWEEP from floppy disk**

  Read this if installing SWEEP from floppy disk to a single workstation or stand-alone PC.

- **Central installation of SWEEP**

  Read this if placing SWEEP on a file server and then installing it from the server to workstations. This allows easy centralised distribution and automatic updating.

Each step below corresponds to a screen presented by the installation program, and each screen is described fully in the 'Installation options' section below.

Local installation from floppy disk

Start the installation program from the installation disk, as described in the 'Starting the SWEEP installation program' section above.

1. **Installation type**

   Select 'Local installation/upgrade'.

2. **Folder selection**

   Choose the installation disk as the SWEEP source folder. The destination folder is the folder on the local hard disk where SWEEP will be installed.

3. **InterCheck support and scheduled network access**

   Install SWEEP with InterCheck client, InterCheck server and/or scheduled sweeping of network resources, as required (see the 'Installation options' section).

4. **SWEEP service account details**

   Applies only if scheduled sweeping of network resources was selected in 'InterCheck support and

network access'. Enter domain name, user name and password for the SWEEP service (see the 'Installation options' section).

Central installation

Stage 1: From floppy disk to file server

Start the installation program from the installation disk, as described in the 'Starting the SWEEP installation program' section above.

1. **Installation type**

   Select 'Central installation/upgrade'.

2. **Folder selection**

   Choose the installation disk as the SWEEP source folder. The destination folder, e.g. I:\SWEEP\NTinst, is the folder on the network drive where the SWEEP installation files will be copied. This folder must be visible to users.

3. **SWEEP installation options**

   Set the default installation options (see the 'Installation options' section). These will appear selected in subsequent installations of SWEEP, at which point they can be changed.

4. **Auto-upgrade mode**

   Applies only if 'Auto-upgrade' was selected in 'SWEEP installation options'. Set the default installation options. These will appear selected in subsequent installations of SWEEP, at which point they can be changed.

Stage 1 of the central installation places the SWEEP installation files on the file server. Stage 2 is necessary to provide a functioning SWEEP installation on workstations.

Stage 2: From file server to workstation

On the workstation, start the SWEEP installation program from the central installation.

1. **Folder selection**

   The SWEEP source folder is the folder to which the SWEEP installation files were copied (see Stage 1). The destination folder is the folder on the local hard disk where SWEEP will be installed.

2. **InterCheck support and scheduled network access**

   Select InterCheck client, InterCheck server and/or scheduled sweeping of network resources, as required (see the 'Installation options' section).

3. **SWEEP service account details**

   Applies only if scheduled sweeping of network resources was selected in 'InterCheck support and network access'. Enter domain name, user name and password for the SWEEP service (see the 'Installation options' section).

4. **SWEEP installation options**

   Select 'Auto-upgrade' and/or 'Prevent removal', as required (see the 'Installation options' section).

5. **Auto-upgrade service account details**

   Applies only if 'Auto-upgrade' was selected in 'SWEEP installation options'. Enter a domain name, user name and password for the upgrade account (see the 'Installation options' section).

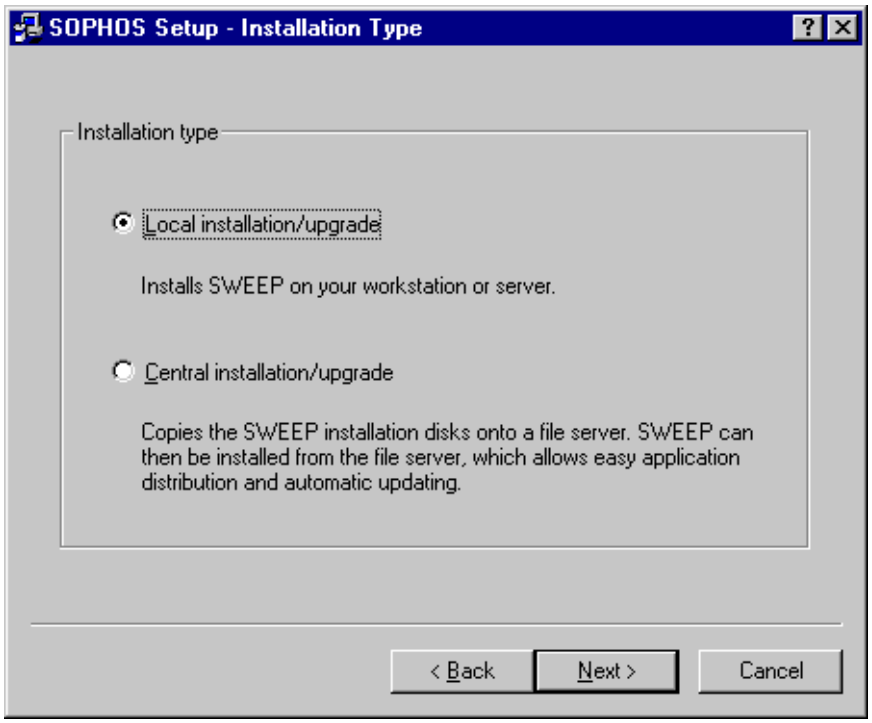
6. **Auto-upgrade mode**

   Applies only if 'Auto-upgrade' was selected in 'SWEEP installation options'. Select the 'Non-interactive' or 'Interactive' mode as required (see the 'Installation options' section).

Installation options

This section describes all the options presented by the installation program. It should normally be used in conjunction with the 'Installing SWEEP' section above.

Installation type



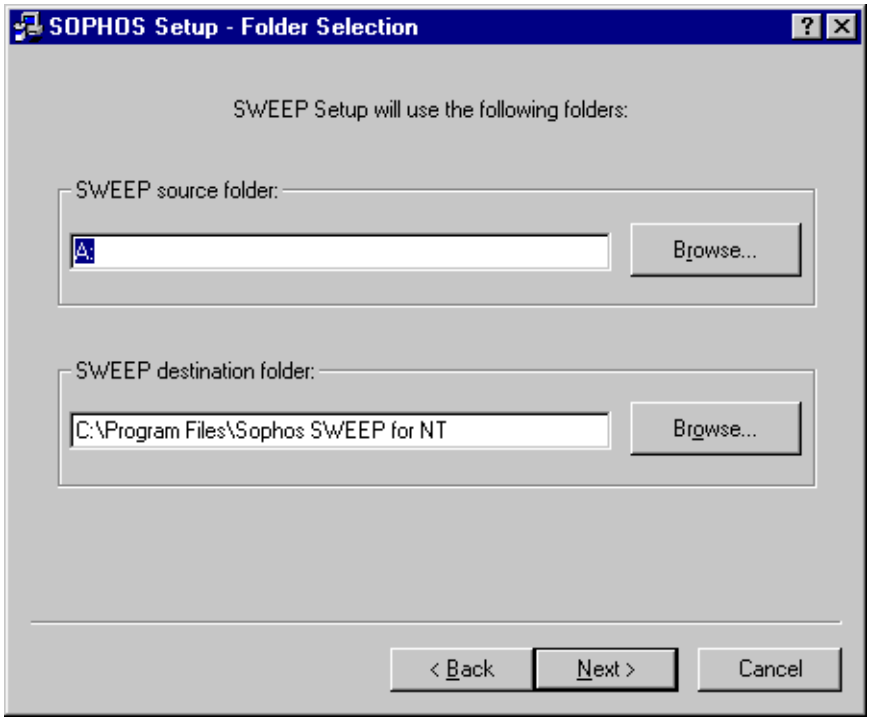
Local installation/upgrade

Installs SWEEP to a stand-alone PC or a single workstation.

Central installation/upgrade

Places the SWEEP installation files on a file server, from where subsequent installations can be made. This allows easy centralised distribution and automatic updating.

Folder selection



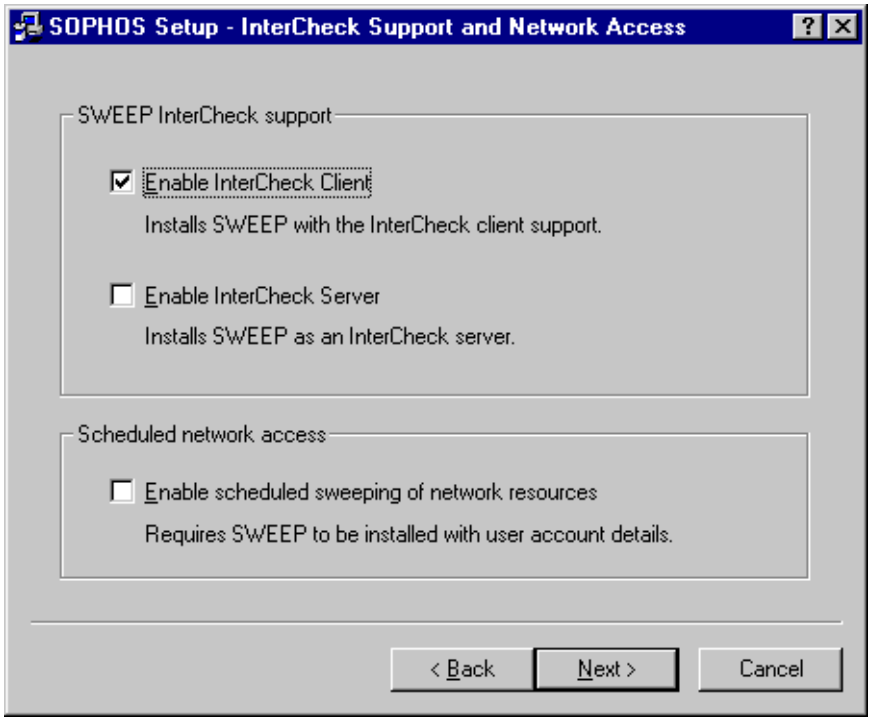
SWEEP source folder

This is the location of the SWEEP installation program - either the installation disk or, if performing Stage 2 of a central installation, the SWEEP installation folder on a network drive.

SWEEP destination folder

If 'Local installation/upgrade' was selected, this is the folder where SWEEP will be installed. If 'Central installation/upgrade' was selected, this is where the central installation files will be copied.

InterCheck support and scheduled network access



Enable InterCheck Client

If installed and active, the Windows NT InterCheck client will automatically check all files accessed on the workstation. This does not require an InterCheck server. See the 'Using SWEEP' and 'Configuring SWEEP' chapters for more information.

Enable InterCheck Server

If installed and active, the InterCheck server will provide virus-checking services for InterCheck clients installed on other, non-NT machines on the network. See the 'About InterCheck', 'Installing InterCheck clients' and 'Configuring InterCheck clients' chapters for more information. Note that this option requires the SWEEP for DOS and InterCheck disks as well as the SWEEP for Windows NT disks.

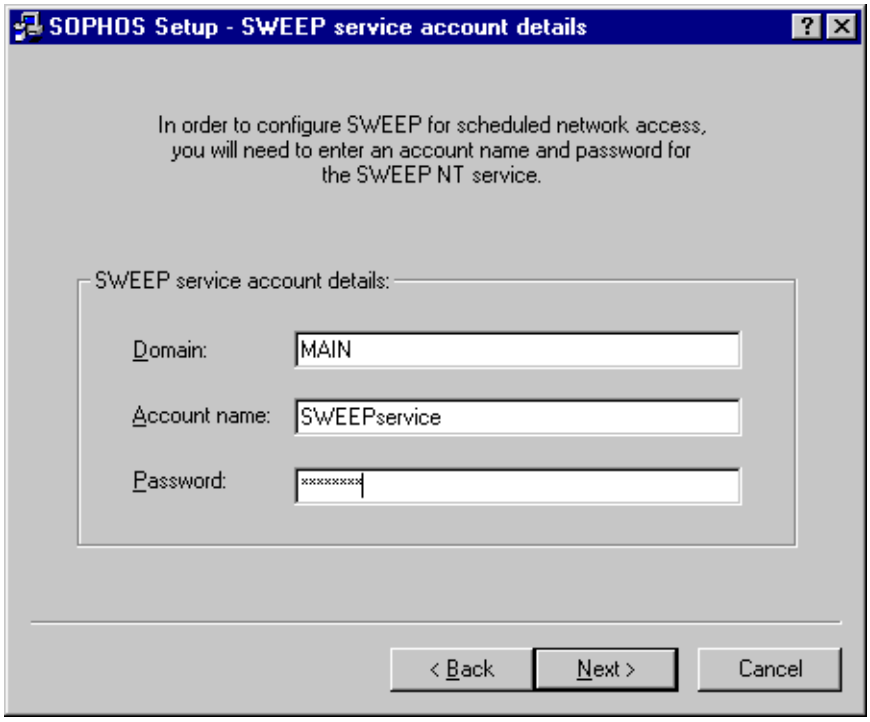
Enable scheduled sweeping of network resources

If this is selected, it will allow SWEEP's scheduler to access files on remote machines. Note that immediate sweeps of networked resources can be performed without selecting this option.

Note: The SWEEP scheduler uses the same account as the SWEEP service and not that of the user operating the SWEEP GUI. Thus it has the same network access rights as the SWEEP service. See the 'SWEEP and Windows NT' section of the 'About SWEEP' chapter.

SWEEP service account details

This screen is presented only if 'Enable scheduled sweeping of network resources' is selected in 'InterCheck support and network access'.

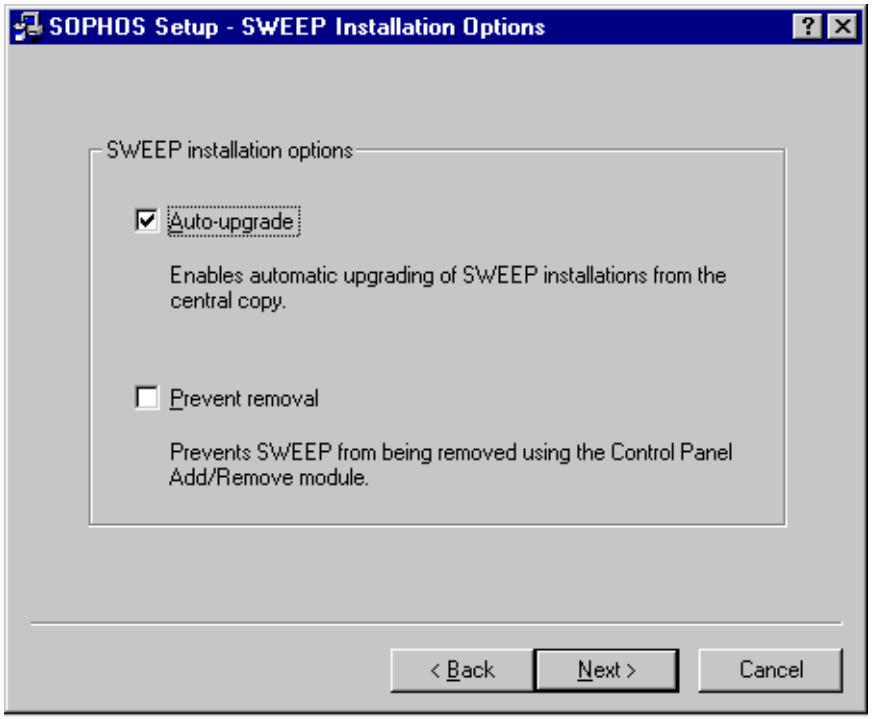


The SWEEP service requires a domain (or the local workstation) name, a user account name and a password. This user should have local Administrator

privileges. It is recommended that a special domain account be used (see the 'Managing the SWEEP services' section). Note that the account can be changed later.

SWEEP installation options

These options are presented only if SWEEP is installed centrally.



Note: In central installation Stage 1 (floppy disk to file server), selecting these options only sets defaults for subsequent installations. In Stage 2 (file server to workstation), they can be changed.

Auto-upgrade

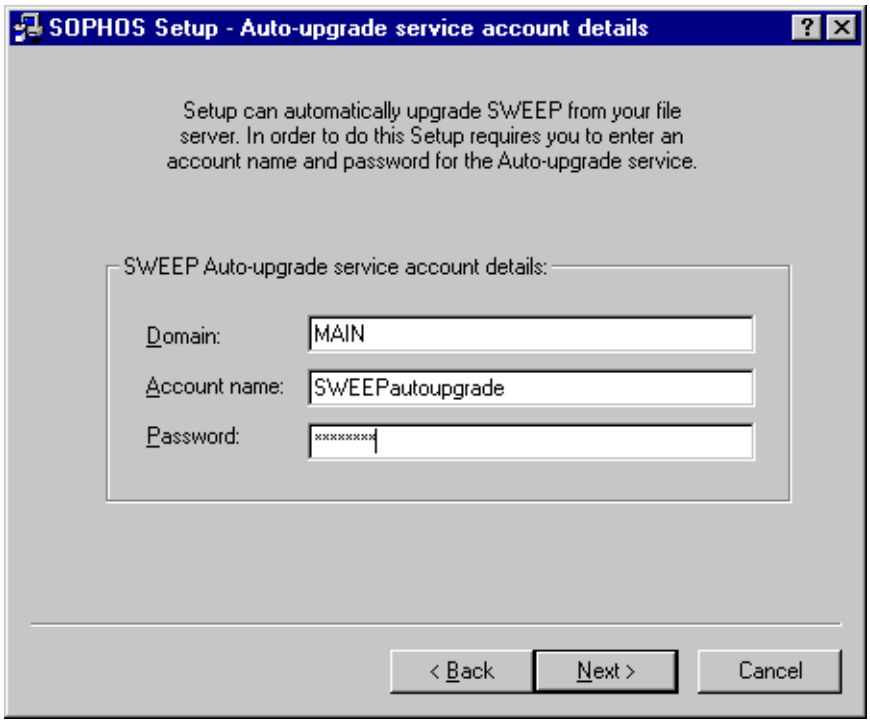
If this is selected, installations made from the file server will be upgraded automatically whenever the version on the file server is upgraded.

Prevent removal

If this is selected, installations made from the file server cannot be removed via an uninstall icon, and Windows NT 4 will not list SWEEP in *Add/Remove Programs* from the Control Panel.

Auto-upgrade service account details

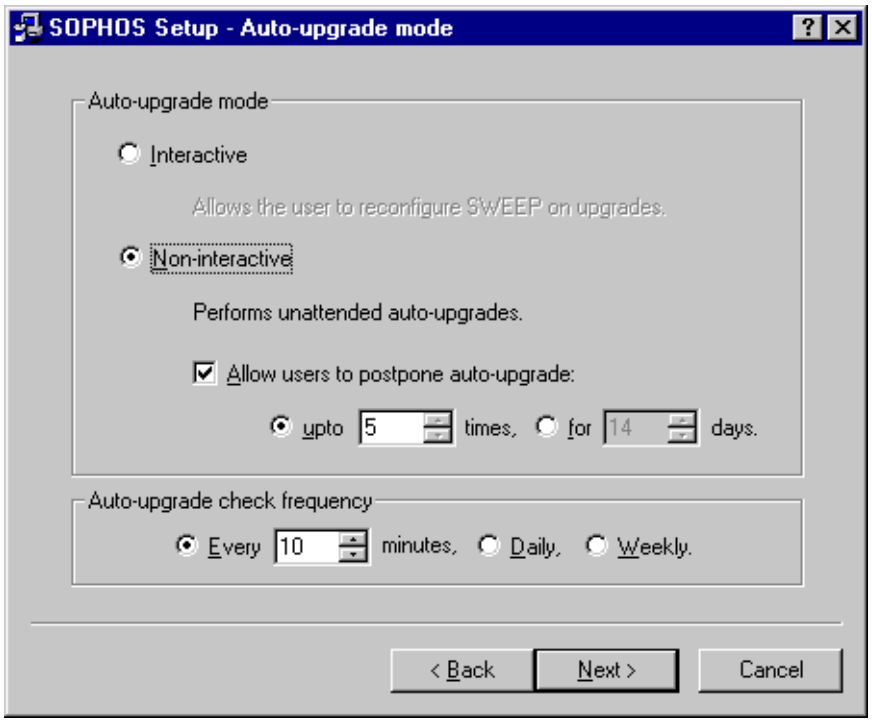
This screen is presented only if 'Auto-upgrade' is selected in central installation Stage 2 (from file server to workstation).



SWEEP's auto-upgrade service requires a domain (or the local workstation) name, a user account name and password. This user must have sufficient rights to log in to the network and read the files in the installation directory. It is recommended that a special domain account be used (see the 'Managing the SWEEP services' section). Note that the account can be changed later.

Auto-upgrade mode

This screen is presented only if SWEEP is installed centrally and 'Auto-upgrade' is selected.



Note: In central installation Stage 1 (floppy disk to file server), selecting these options only sets defaults for subsequent installations. In Stage 2 (file server to workstation), they can be changed.

Interactive

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

Non-interactive

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

Allow users to postpone Auto-upgrade

If 'Non-interactive' upgrading was selected, users may be allowed to postpone the upgrade a specified number of times, or for a specified period of time. This is the recommended option.

Auto-upgrade check frequency

This option sets the frequency with which the installation of SWEEP will check the file server for a newer version of SWEEP.

Upgrading SWEEP

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

SWEEP's upgrade facility makes installing these upgrades simple.

There are two approaches to upgrading SWEEP:

1. **Local upgrade**

   Upgrades SWEEP on a single workstation or stand-alone PC.

2. **Central upgrade**

   Places the upgraded SWEEP installation files on a file server, from where automatic upgrades can be made.

The sections below give step-by-step instructions on how to perform each type of upgrade. Each step corresponds to a screen described in the 'Installation options' section, except where indicated.

Local upgrade

Start the installation program on the update disk, as described in the 'Starting the SWEEP installation program' section above, and close down the InterCheck monitor and SWEEP GUI if prompted.

1. **Installation type**

   Select 'Local installation/upgrade'.

2. **Update options** (see 'Update options' in the 'Upgrade options' section below).

   Select 'Upgrade existing installation' or 'New installation' as required.

3. **Folder selection**

   Choose the installation disk as the source folder. The destination folder is the folder on the hard disk where SWEEP will be installed. If 'Upgrade exisiting installation' was selected, the destination folder cannot be changed.

4. **InterCheck support and network access**

   Confirm or change the options selected when SWEEP was last installed or upgraded.

Central upgrade

Start the installation program on the update disk, as described in the 'Starting the SWEEP installation program' section above.

1. **Installation type**

   Select 'Central installation/upgrade'.

2. **Folder selection**

   Choose the installation disk as the source folder. The destination folder is the network folder where the central installation files will be placed.

3. **SWEEP installation options**

   Choose ‘Auto-upgrade’ and/or ‘Prevent removal’ as required.

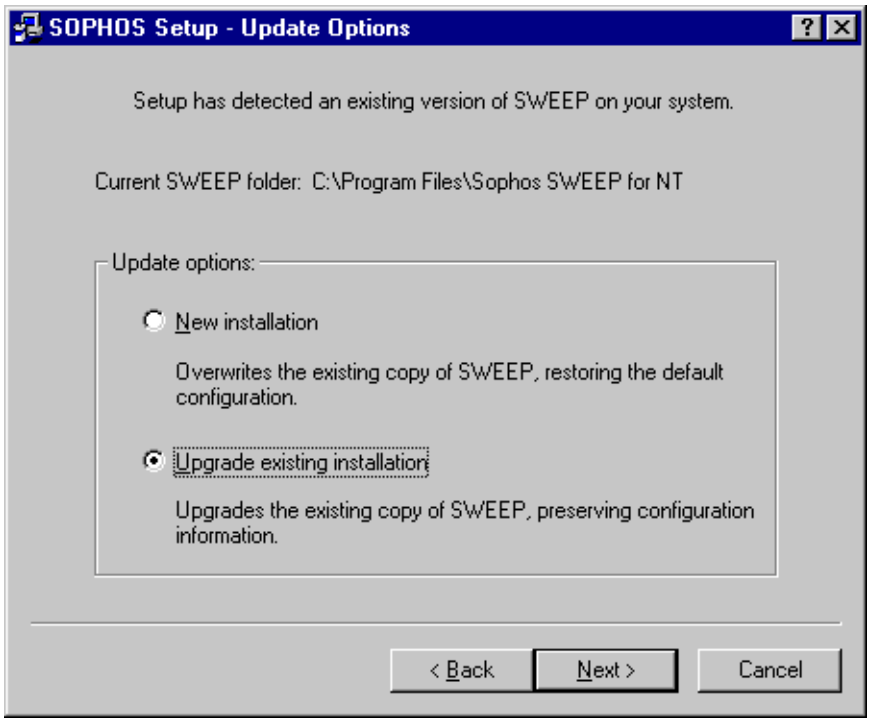
4. **Auto-upgrade mode**

   Applies only if ‘Auto-upgrade’ was selected. Confirm or change default options.

If ‘Auto-upgrade’ was selected in Stage 2 of the central installation, the workstation installations of SWEEP will be upgraded automatically.

Upgrade options

Update options



New installation

Overwrites the existing version of SWEEP and restores the default configuration.

Upgrade existing installation

Upgrades SWEEP, preserving configuration.

Note: If 'Upgrade existing installation' is selected, the 'Folder selection' screen will appear, but the destination folder can not be changed. This is because the new version of SWEEP has to be installed in the same folder as the old in order to retain the old configuration settings.

Urgent SWEEP updates

Viruses are detected using Sophos' proprietary Virus Description Language (VDL). VDL identities for the detection and disinfection of viruses can be encoded as IDE (identitity) files which consist entirely of printable ASCII characters. New identities can be faxed, emailed or downloaded from Sophos' Web site (http://www.sophos.com/). Save the VDL update in an ASCII file with an IDE extension (e.g. NEWVIRUS.IDE), and place it in the SWEEP folder.

Centralised distribution of IDE files

With a central installation of SWEEP with 'Auto-upgrade' enabled, the IDE file can be placed in the SWEEP central installation folder on the file server. The workstation installations will receive the new IDE file the next time they are automatically upgraded, and the local checksum files will also be purged.

IDE files and the Windows NT InterCheck client

A new IDE file introduced to an installation of the SWEEP for Windows NT InterCheck client will not be recognised until the SWEEP service is stopped and restarted. The local checksum file should be purged manually.

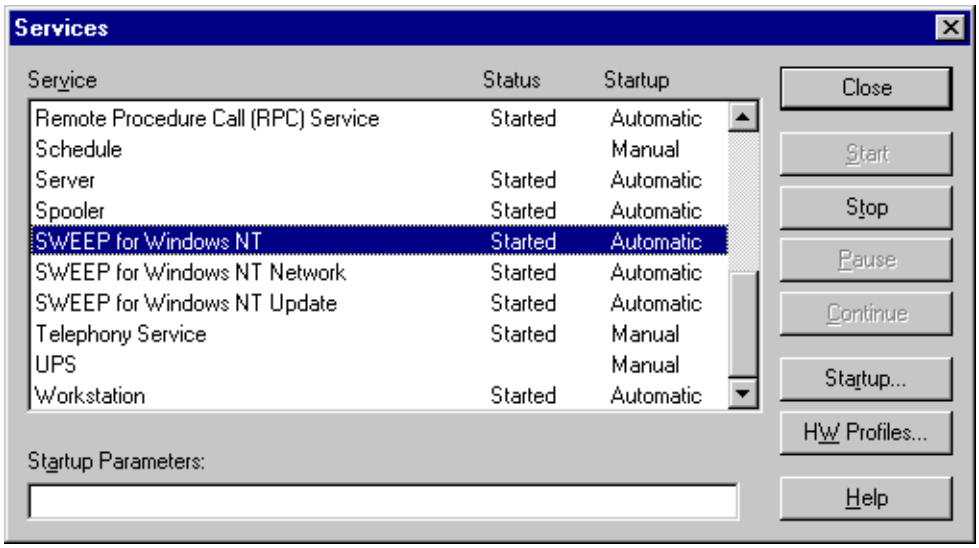
Managing the SWEEP services

The SWEEP service accounts can be changed, and SWEEP services can be stopped and restarted via the Services dialog. It is necessary to restart the SWEEP service after adding a new IDE file, for example.

Open the Windows NT Control Panel, and double-click the *Services* icon

Services

to display the Services dialog.



Note: It is recommended that special domain accounts be created for the user specified SWEEP accounts described below. See the Windows NT documentation for information on creating user accounts. The user specified SWEEP accounts should have the 'Password never expires' option selected and the 'User must change password on next logon' option deselected.

SWEEP for Windows NT (user specified) service

This service is used to run SWEEP independently of the GUI.

Its user account determines which parts of the network can be accessed by scheduled sweeps, and is initially entered in the 'SWEEP service account details' dialog during installation. The specified user should have local Administrator privileges.

SWEEP for Windows NT Network (user specified) service

This service is used to store the account required to access the network.

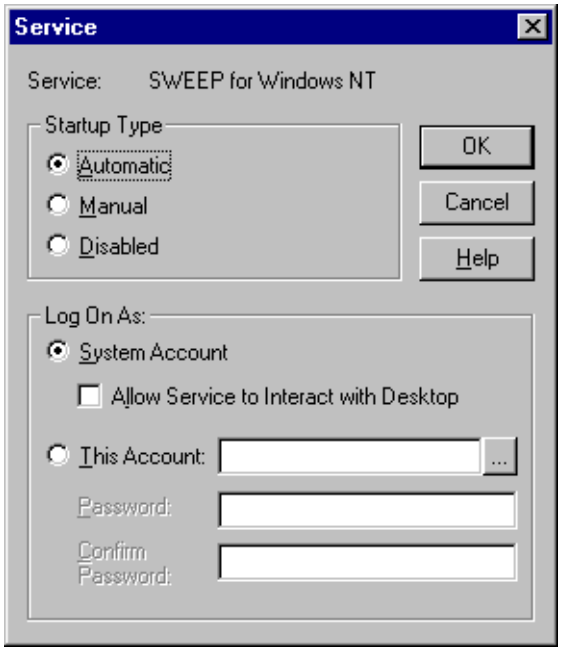
It is used by the auto-upgrade facility and the InterCheck logging messaging module. Its account details are initially entered in the 'Auto-upgrade service account details' dialog during SWEEP installation. This service account should have access to the SWEEP areas on the network.

SWEEP for Windows NT Update service

This service is used to perform the auto-upgrade. Its service account is set to 'System' by the installation program and should not be changed by the user.

Changing service user accounts

Double-click on the relevant entry in the Services dialog to display its Service dialog.



The 'Log On As' section can be used to set the account name and password. The service has to be stopped and restarted for any changes to take effect.

Stopping and restarting the SWEEP services

To stop and restart a SWEEP service, highlight the service on the Services dialog, press the *Stop* button, and then press the *Start* button.

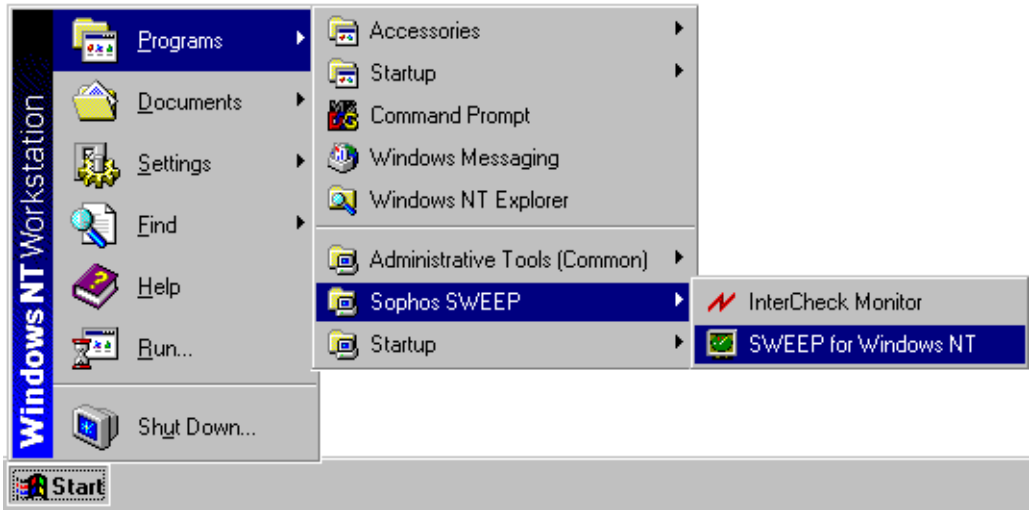
Using SWEEP

This chapter shows how to start SWEEP once it has been installed, start an immediate sweep, change the items to be included in immediate and/or scheduled jobs, activate the InterCheck server and InterCheck client, close down the SWEEP GUI, and use the InterCheck monitor.

Starting SWEEP

Under Windows NT 4

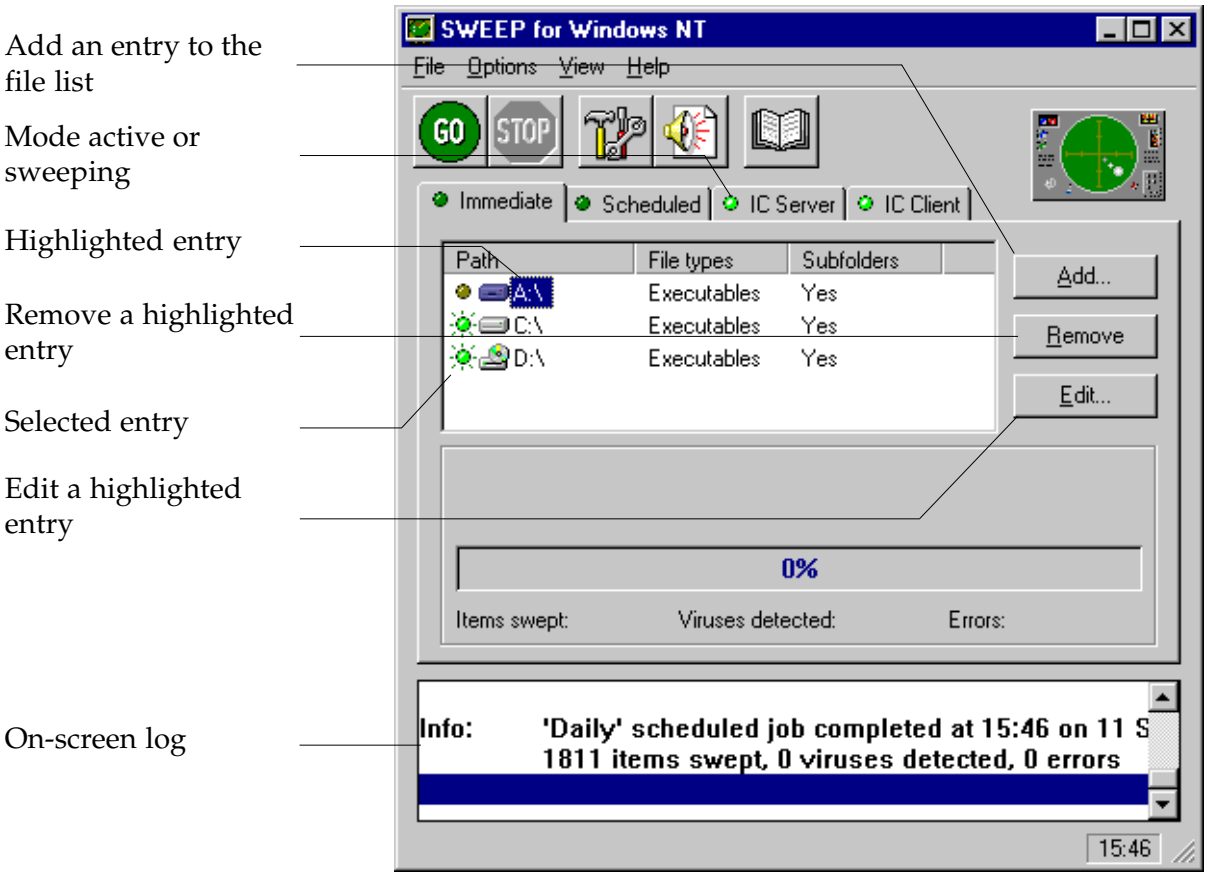
Click *Start*, click *Programs*, click the *Sophos SWEEP* folder, and then click the *SWEEP for Windows NT* icon.



Under Windows NT 3.51

The SWEEP installation program creates a program group called Sophos SWEEP. Open this program group and double-click the *SWEEP for Windows NT* icon.

Overview of the SWEEP display



The main SWEEP display contains:

- The menu and toolbar. The icons in the toolbar provide short-cuts to commonly used menu options.
- The immediate, scheduled, InterCheck server, and InterCheck client mode tabbed pages. The immediate mode page is displayed on start-up,

and contains the file list along with the progress indicator for immediate operation. The scheduled and InterCheck tabbed pages will not be available if the user running the GUI is not an Administrator. The IC client and IC server tabbed pages will not be available if SWEEP was not installed as an InterCheck client and InterCheck server respectively. A light on the left of each tab is illuminated when that mode is active or performing a sweep.

- The on-screen log. This contains information about the current session, along with (if the user running the GUI is an Administrator) all the scheduled and InterCheck log messages reported since the service was started.

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

Immediate mode

Starting an immediate sweep

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

or click the associated *GO* icon:

Hint: To sweep any individual item in the immediate mode display, double-click on its icon in the file list.

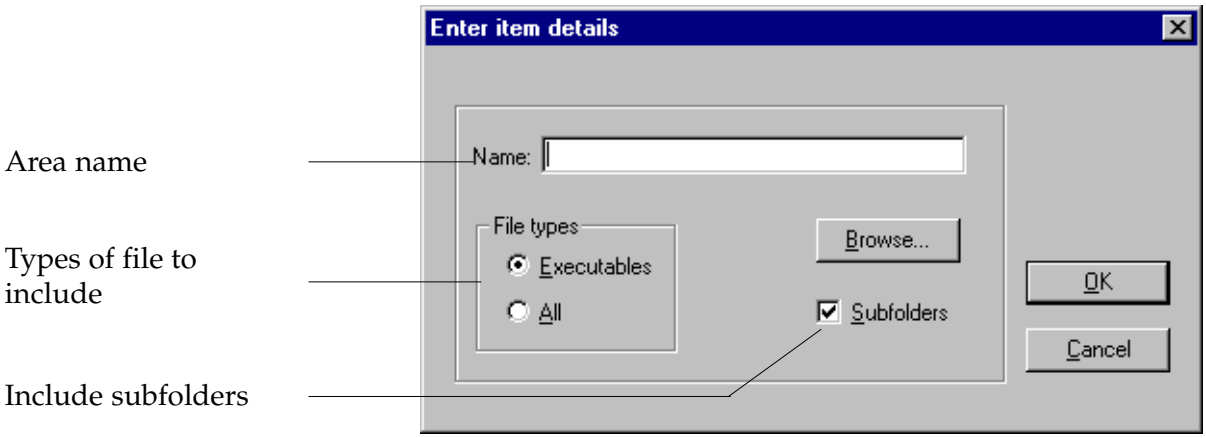
Default immediate mode file list

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

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

Adding new items for immediate sweep

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



Area name

Specifies the drive, folder or filename to be swept. Both mapped and UNC path names can be entered. Wildcards can also be included. *Browse* can be used to select from a list of available items.

File types

Only those files defined as executables will be swept, unless the 'All' file types option is selected. See the 'Executables' section of the 'SWEEP options' chapter

for information on changing the files defined as executables.

Subfolders

Subfolders will be swept if this option is selected.

Removing items from immediate sweep

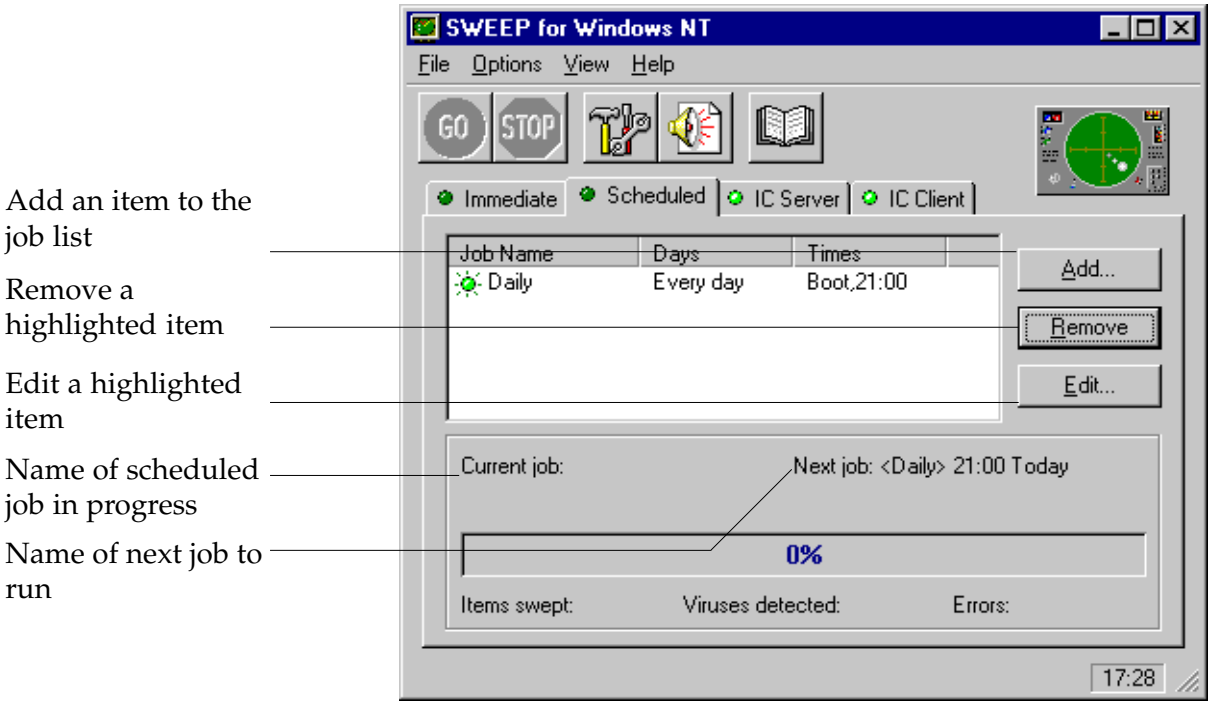
Highlight the name of the path to be removed and click *Remove*. An entry in the file list is highlighted by clicking on the path name.

Editing an item for immediate sweep

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

Scheduled mode

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



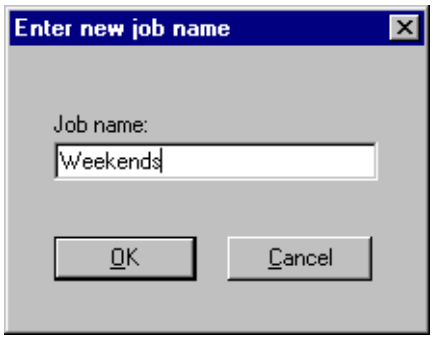
Default scheduled mode job list

By default, a job named 'Daily' is created. Unless it is deselected or removed from the job list, this job will sweep the system at 21.00 every day and also every time that the SWEEP service is started (normally when the machine is booted).

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

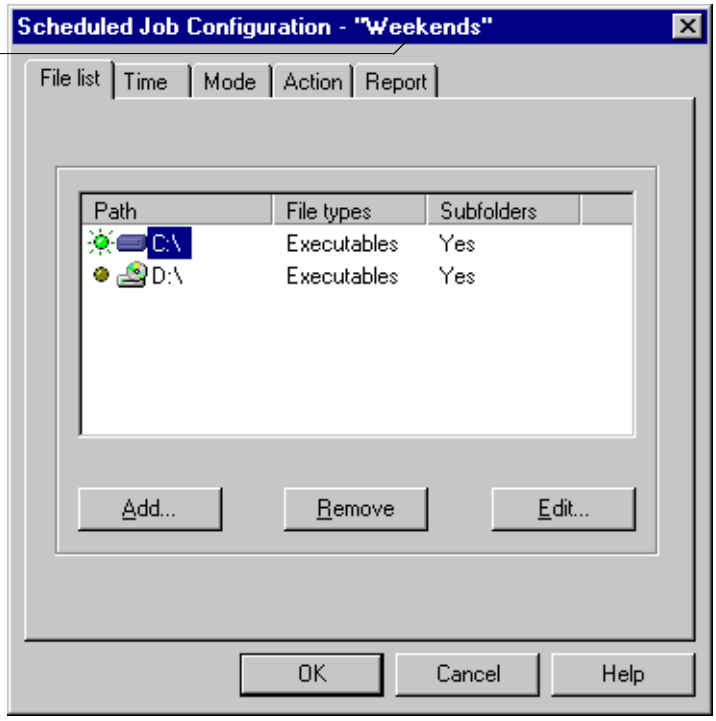
Adding a new scheduled job

To add a new scheduled job, press *Add* on the scheduled mode page. You will be prompted for a job name:



You will then be presented with the scheduled mode configuration page.

Scheduled job name



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

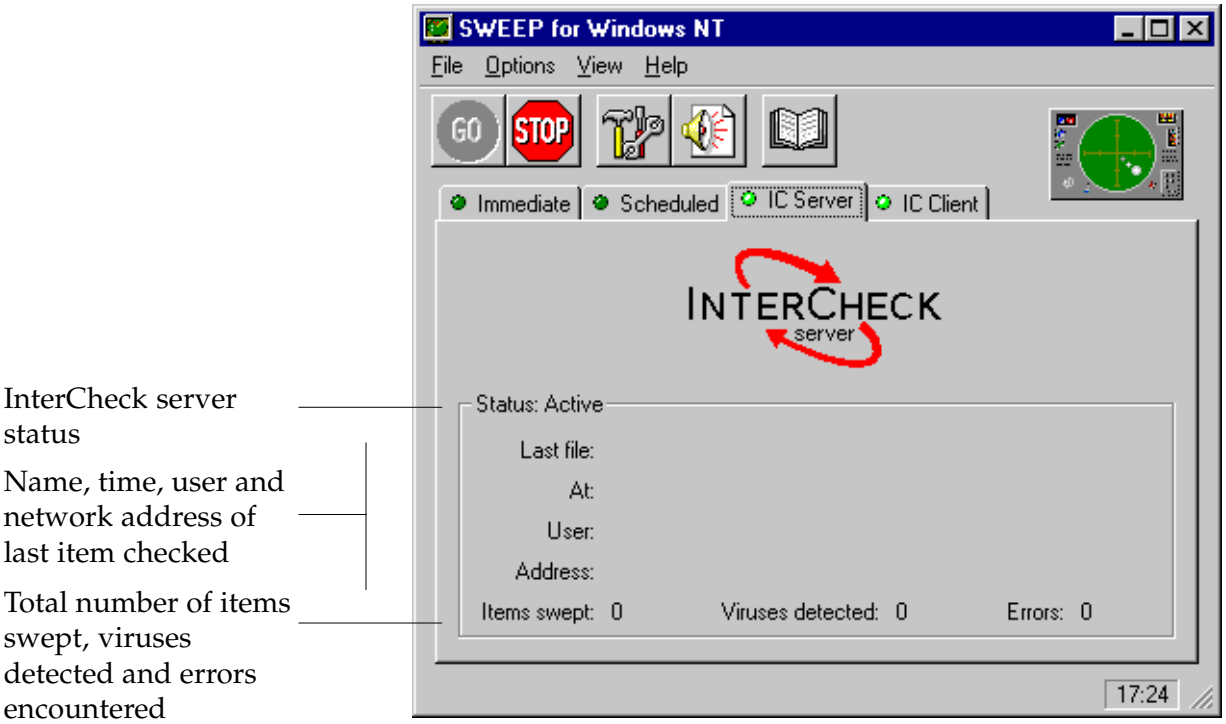
Removing a scheduled job

Highlight the name of the job to be removed on the scheduled mode page and click *Remove*.

Editing a scheduled job

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

InterCheck server mode

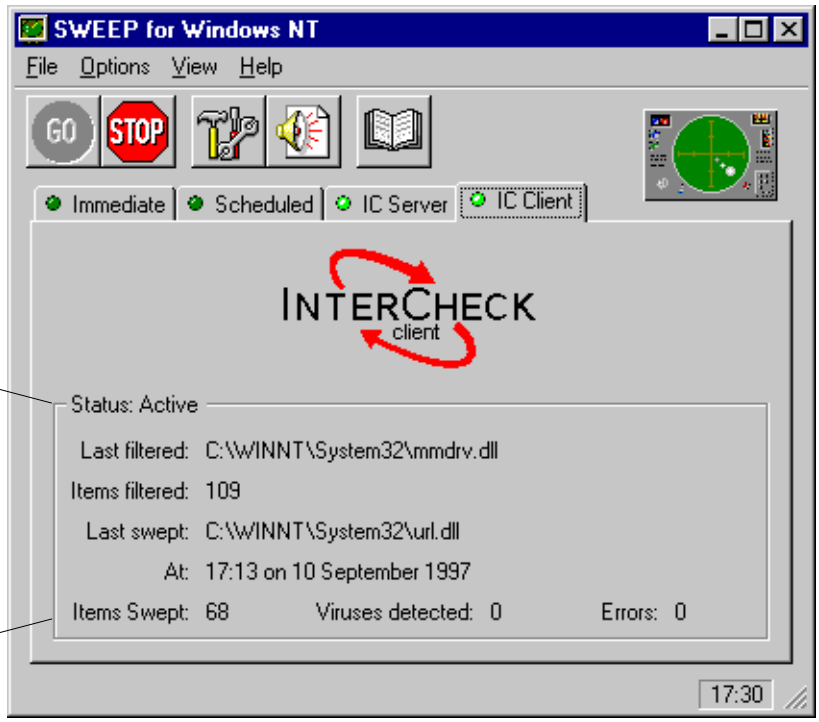


The InterCheck server display shows the status of the InterCheck server (either active or inactive), the name, time, user and network address of the last item sent to the InterCheck server for checking, along with totals of the number of items swept, viruses detected and errors encountered.

Activating the InterCheck server

By default, the InterCheck server (if installed) will be active. If the server status is shown as inactive, it will not be able to service requests from InterCheck clients. To activate an inactive InterCheck server, select the IC server tabbed page and then either select *Go* from the file menu or click the *GO* icon.

InterCheck client mode



InterCheck client status

Name of last item and total number of items checked by client

Name and time of last item swept by SWEEP

Total number of items swept, viruses detected and errors encountered

The InterCheck client display shows the status of the InterCheck client (either active or inactive), the name of the last item filtered (i.e. the last item checked against the list of authorised items by the InterCheck client), the name and time of the last item swept (i.e. the last item not in the list of authorised items and therefore checked for viruses by SWEEP), along with totals of the number of items filtered, items swept, viruses detected and errors encountered.

Activating the InterCheck client

By default, the InterCheck client (if installed) will be active. If the client status is shown as inactive, the InterCheck client will not check items as they are accessed on the workstation PC. To activate an inactive InterCheck client, select the IC client tabbed page and then either select *Go* from the file menu or click the *GO* icon.

Closing down the SWEEP GUI

Select *Exit* from the *File* menu to close down the SWEEP GUI.

Any immediate sweeps in progress will be terminated. However, as long as the underlying SWEEP service is still active, any scheduled jobs, the InterCheck server, and the InterCheck client will continue to operate.

Note: Closing down the SWEEP GUI does not shut down the SWEEP service. The service will also remain active even if the user logs off the Windows NT system.

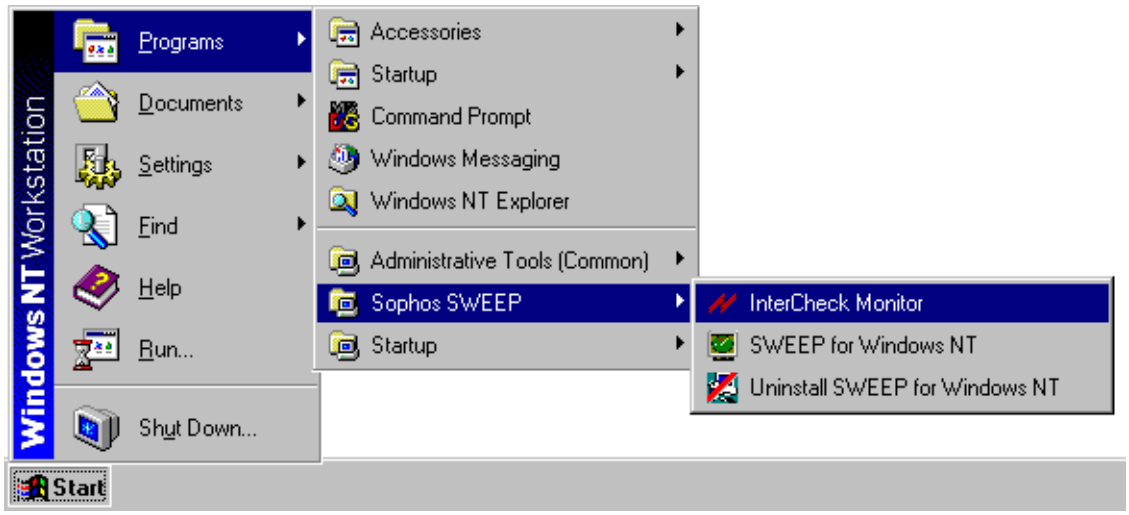
Using the InterCheck monitor

Starting the InterCheck monitor

By default, the InterCheck monitor will be launched on Windows NT start-up if the InterCheck client is installed.

To start the InterCheck monitor under Windows NT 4 at any other time:

Click *Start*, click *Programs*, click the *Sophos SWEEP* folder, and then click *InterCheck Monitor*.



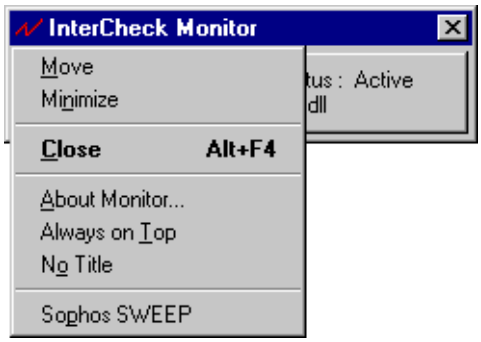
While active, the InterCheck monitor can be displayed by double-clicking its icon in the right-hand corner of the Windows NT taskbar.

Overview of the InterCheck monitor display

The InterCheck monitor displays the total number of items filtered (i.e. the items checked against the list of authorised items by the InterCheck client), the status of the InterCheck client (either active or inactive), and the name of the last item filtered.

Using the InterCheck monitor

Click the upper left hand corner of the InterCheck monitor window title bar to display a list of options.



Minimize

If selected, the InterCheck monitor window will be minimized.

Always on Top

If selected, the InterCheck monitor window will remain above all other windows.

No title

If selected, the InterCheck monitor window title bar will disappear. To restore the title bar, double-click inside the InterCheck monitor window.

Sophos SWEEP

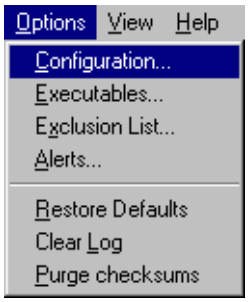
Select *Sophos SWEEP* to start SWEEP for Windows NT.

Configuring SWEEP

This chapter introduces the configuration options used by the immediate, scheduled and InterCheck modes of operation.

About configuring SWEEP

Select *Configuration* from the *Options* menu

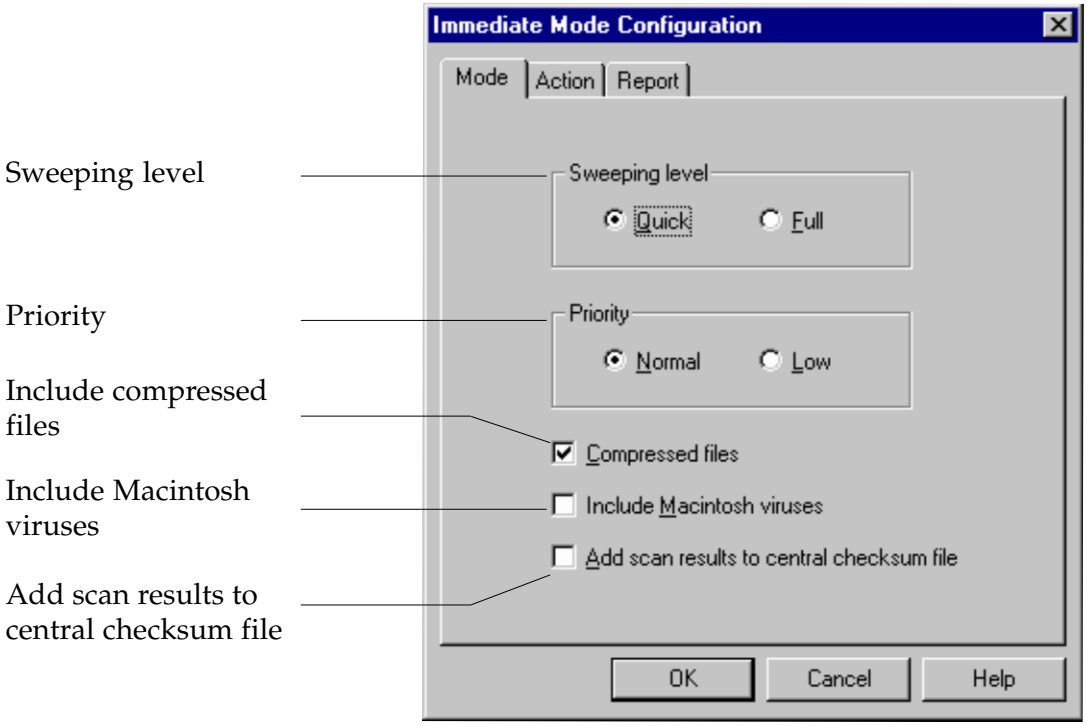


or click the associated icon

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

Note: Immediate, scheduled, IC client and IC server modes are configured independently.

Sweeping mode (immediate, scheduled, IC client & IC server modes)



Sweeping level

The 'quick' sweeping 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, 'full' sweeping level is much slower, and for normal operation 'quick' sweeping is generally sufficient.

Priority

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

This option is not available in IC client mode.

Compressed files

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

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

Include Macintosh viruses

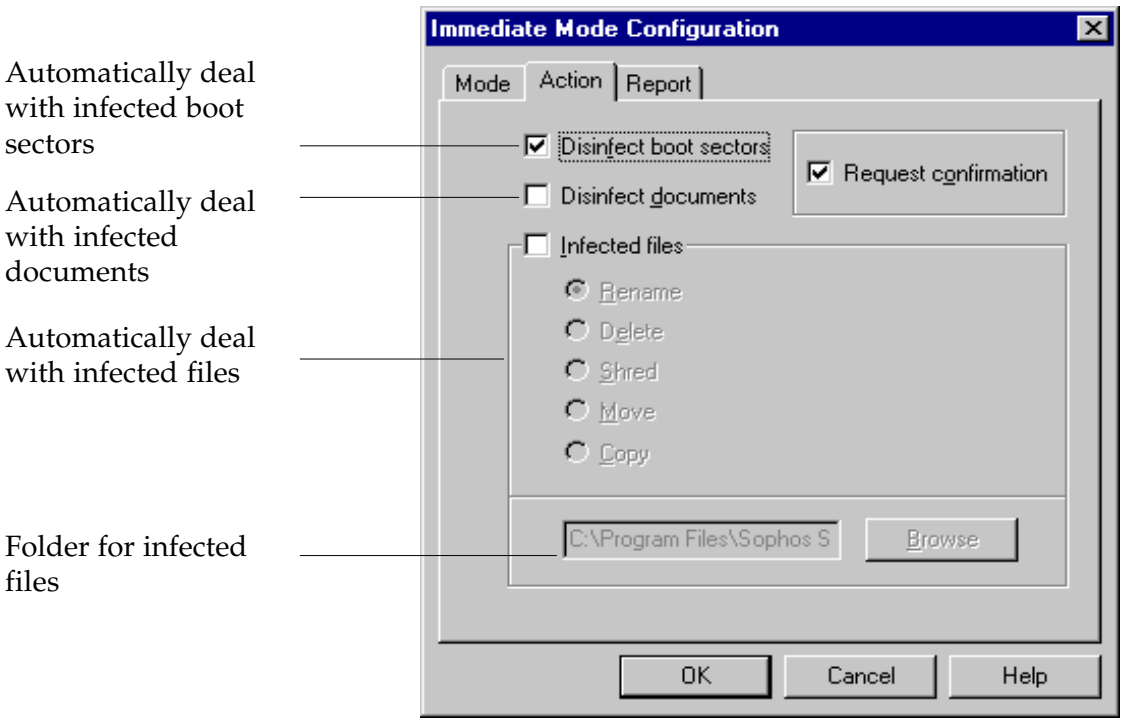
SWEEP for Windows NT is capable of looking for viruses inside Macintosh files. SWEEP will check any executable Macintosh files it finds irrespective of their file extension, even if SWEEP is set to check only (DOS) executable file types.

Add scan results to central checksum file

Any file found to be virus-free can be checksummed and added to the server's central checksum file. Networked InterCheck clients can use this central checksum file in addition to their own local checksum file, thereby eliminating the need for multiple checking and authorisation of identical items.

This option is not available in IC client mode.

Action on virus detection (immediate, scheduled & IC server modes)



Disinfect boot sectors

SWEEP can disinfect most boot sector viruses from floppy disks. SWEEP for Windows NT will not automatically disinfect a hard disk's boot sector. See the 'Treating viral infection' chapter for information on manually disinfecting boot sectors. See the on-line virus library for specific details on individual viruses.

This option is not available in IC server mode.

Disinfect documents

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

This option is not available in IC server mode.

Infected files

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

Note that the only option available in IC server mode is to copy infected files.

Request confirmation

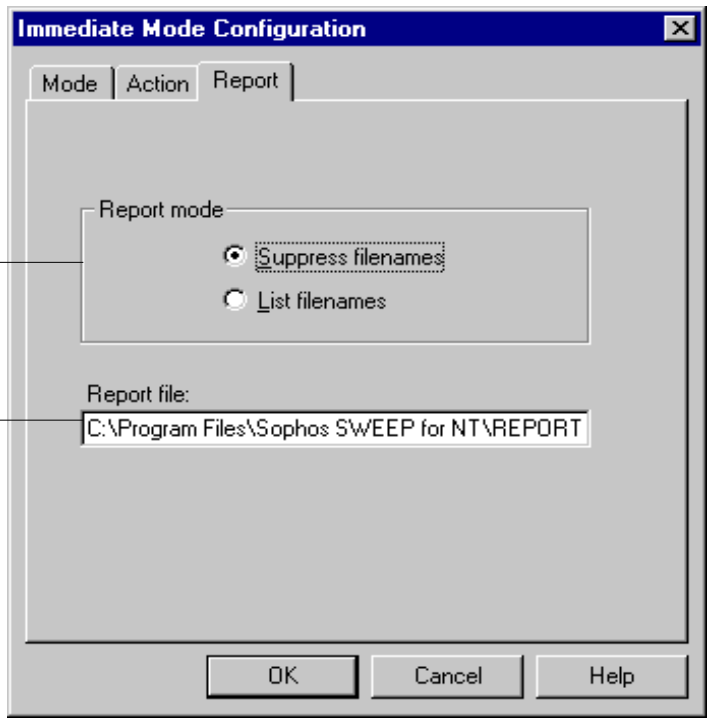
If this option is selected, SWEEP will ask for confirmation before proceeding with any action that involves changing infected items (i.e. disinfecting boot sectors, disinfecting documents, and renaming, deleting, shredding and moving infected files).

This option is only available in immediate mode, where it is enabled by default.

Reporting results (immediate & scheduled modes)

What to include in the report

Where to save the report



The report file contains information about individual immediate or scheduled jobs, and is aimed at the user. It is generated in addition to the continuous log file, which is aimed at the Administrator.

Note that the report file is written as the GUI user for immediate sweeps and as the service user for scheduled sweeps (see the 'SWEEP and Windows NT' section of the 'About SWEEP' chapter).

Report mode

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

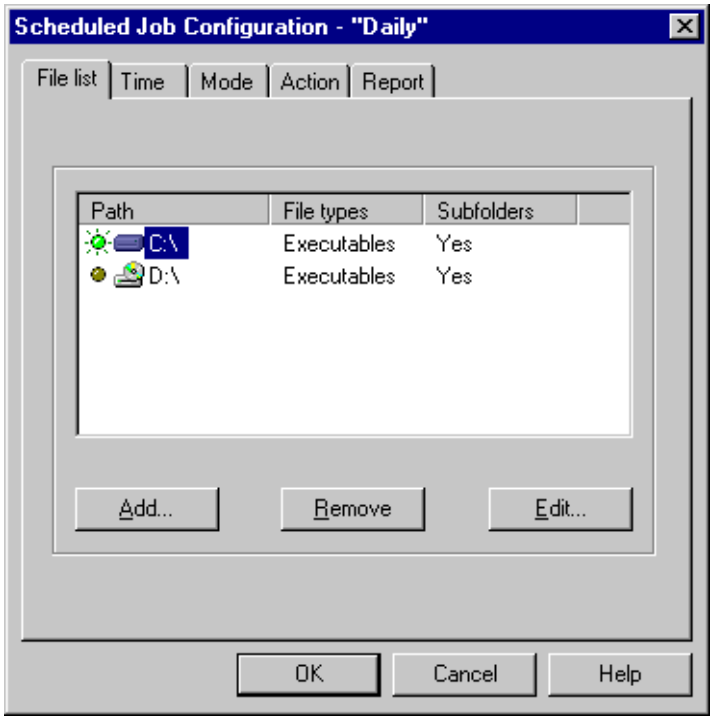
Report file

The report file will be saved to disk.

File list (scheduled mode only)

File list, functionally equivalent to the immediate mode file list

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

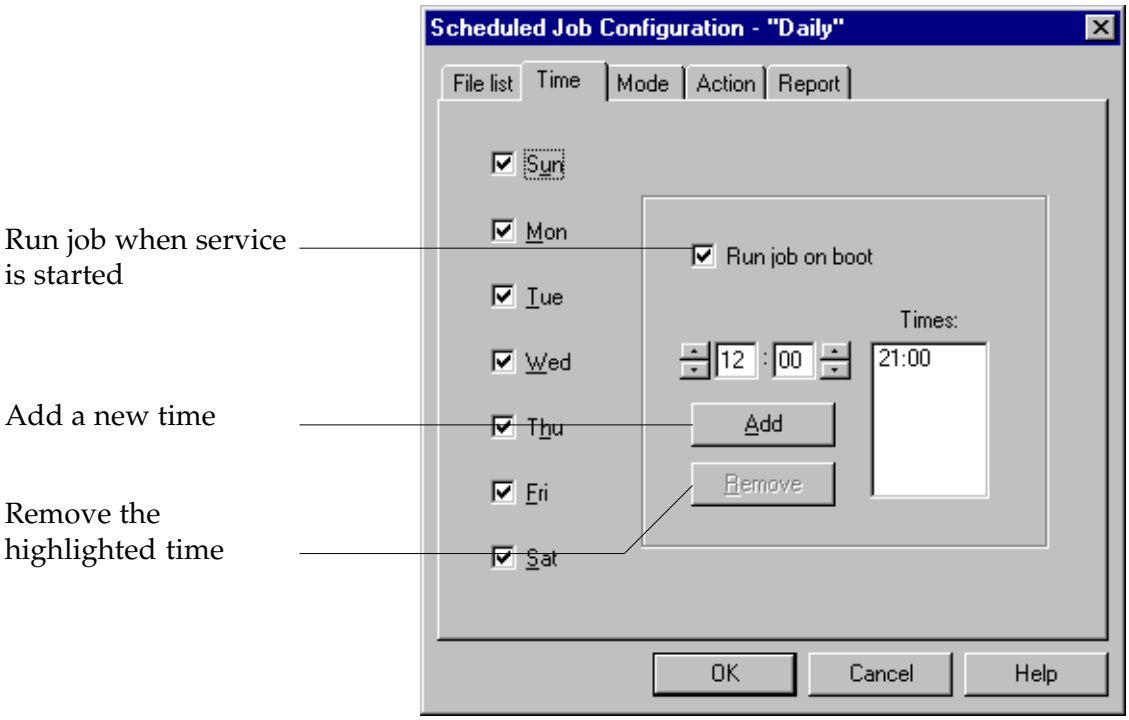


The scheduled mode file list is similar to the immediate mode file list, but specifies the files to be swept in a scheduled job. The default scheduled mode file list is the same as that for immediate mode, except that local floppy drives are not listed.

Note that the files available for sweeping in the scheduled mode might not be the same as those available in the immediate mode. This is because the scheduled sweep runs with the SWEEP service's user rights, which might not be the same as those of the current SWEEP GUI user. See the 'Managing the SWEEP services' section of the 'Installing SWEEP' chapter.

It is recommended that networked resources are referred to by UNC names because mapped drives are only available when a user is logged in to the machine. The browse control will only show those files and folders to which the scheduled SWEEP service has access.

Time (scheduled mode only)



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

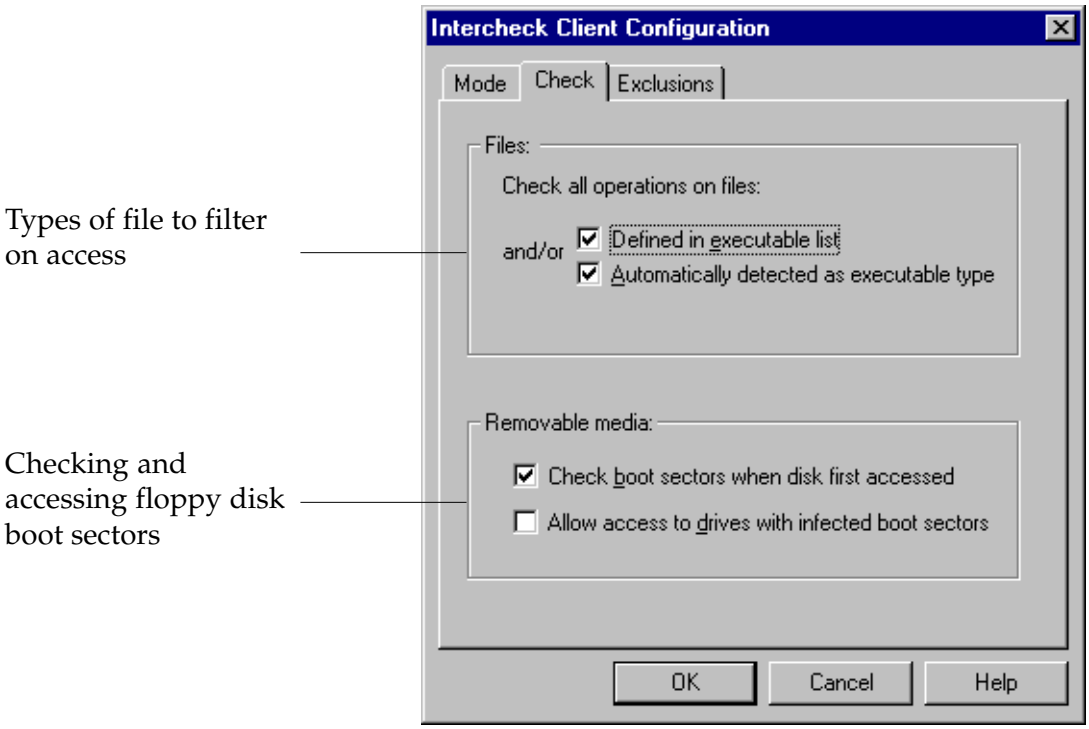
Add time

To add a time, set the time, press *Add* and click *OK*.

Run job on boot

This option forces SWEEP to run that job whenever the SWEEP service is started, such as when the Windows NT machine is booted.

Check (IC client mode only)



Files

Check all operations on files

'Defined in executable list' will check those files defined as executables, via *Executables* from the *Options* menu. 'Automatically detected as executable type' examines all files accessed, irrespective of their extension, looking at the structure of the file to determine whether they should be checked. The 'Automatically detected as executable type' option is primarily for determining whether a file is an OLE document which should be checked for macro viruses, such as a Word document which might not have the extension DOT or DOC. Windows programs are also detected in this manner.

Removable media

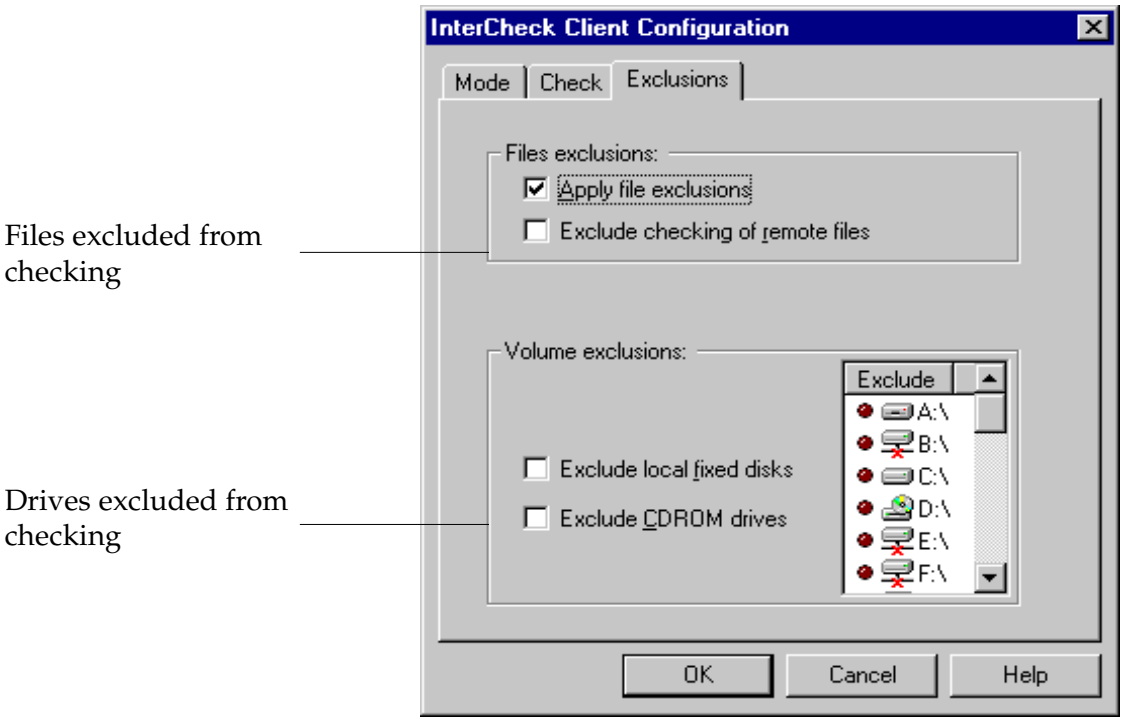
Check boot sectors when disk first accessed

By default, the InterCheck client checks the boot sectors of all removable media when they are first used.

Allow access to drives with infected boot sectors

If selected, the InterCheck client will allow access to drives with infected boot sectors. This option has been provided to allow files to be copied off a floppy disk infected with a boot sector virus. Note that a boot sector virus will only infect a computer if that computer is booted from the infected disk.

Exclusions (IC client mode only)



File exclusions

Apply file exclusions

The file exclusions are specified by *Exclusion List* from the *Options* menu.

Exclude checking of remote files

If selected, the InterCheck client will not check files on network drives.

Volume exclusions

The volume exclusions display shows a list of all possible drive mappings, irrespective of whether the mapping is valid for a particular user, although unmapped drives for the current user will be marked. None of the selected drives will be checked by the InterCheck client.

Exclude local fixed disks

This option excludes all local fixed disks, irrespective of whether they are specified in the volume exclusions display.

Exclude CDROM drives

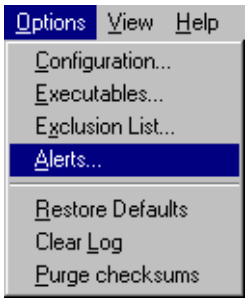
This option excludes all CD-ROM drives, irrespective of whether they are specified in the volume exclusions display.

SWEEP alert message options

This chapter describes the options available for notifying users of SWEEP activity.

About SWEEP alert message options

Select *Alerts* from the *Options* menu



or click the associated icon

to display the notification configuration pages.

There are five notification control pages: Event logging, Network messaging, SMTP email, Desktop messaging and InterCheck logging. Each shares a number of common features: disable notification, job specification, and notification level.

Disable notification

The form of notification whose control page is currently selected can be turned off.

Job specification

If the 'All jobs' option is selected, all configuration options for that form of notification will apply to the immediate mode, all scheduled jobs, and (where available) the InterCheck modes.

The 'Specific jobs' option allows the immediate mode, each individual scheduled job and the InterCheck modes to have different notification configuration settings. If a specific job is not explicitly configured, it will inherit the settings of the <default> job.

This option is not available on the Desktop Messaging control page.

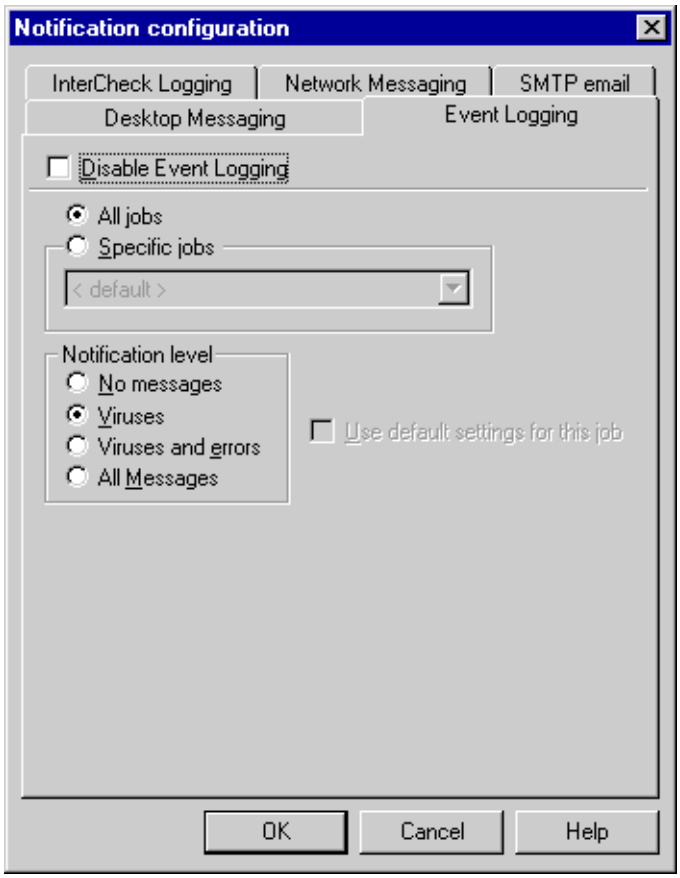
Notification level

There are three forms of notification message that can appear in the alerts: virus detected messages, error messages, and general information messages such as the time a job was started. The alerts can include none of these, just the virus messages, the virus and error messages, or all three forms of message.

The notification level setting will not affect the level of information placed in the report file, the on-screen log or the log file.

This option is not available on the Desktop Messaging control page.

Event logging



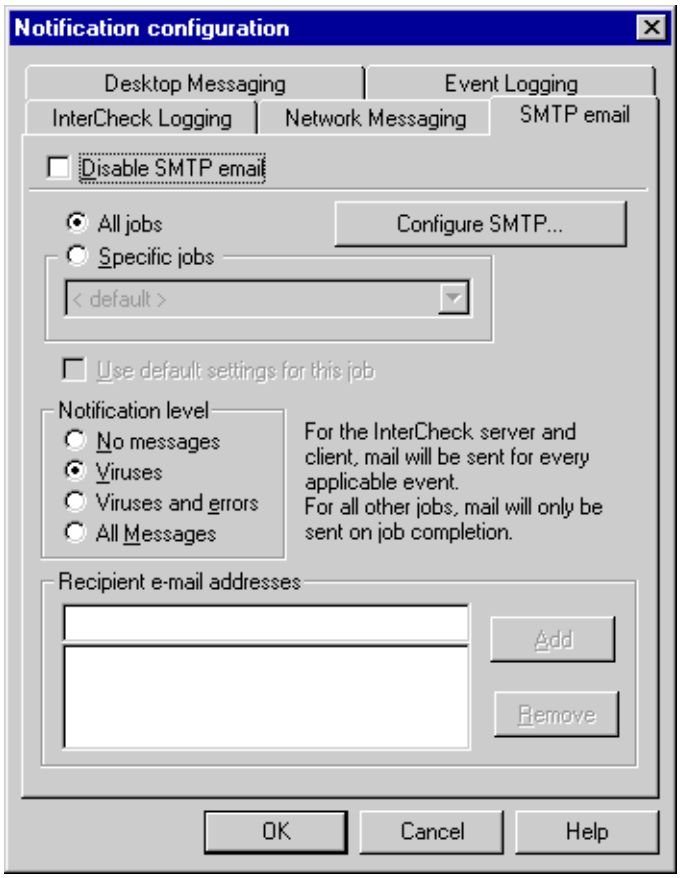
If event logging is enabled, SWEEP will record the specified level of information for the specified jobs in the Windows NT Application event log.

Network messaging

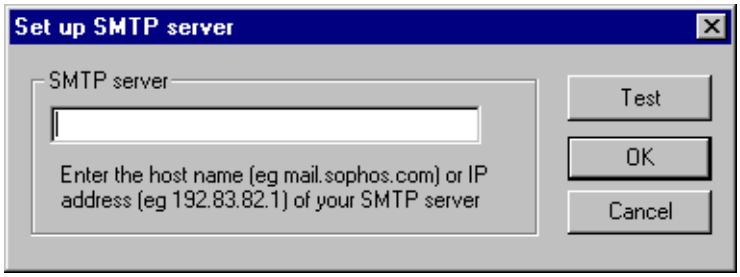
This will cause SWEEP to send a network message to the named machines or users. Note that only one machine can be notified under each name, so if a user name is specified, and that user is logged on to two machines, they will only receive the message at the first machine. This is due to limitations in the Lan Manager messaging system. For this reason it is recommended to use machine names as recipients rather than user names.

Note also that in order for Windows 95 or Windows for Workgroups PCs to receive messages, they must be running the WinPopup application.

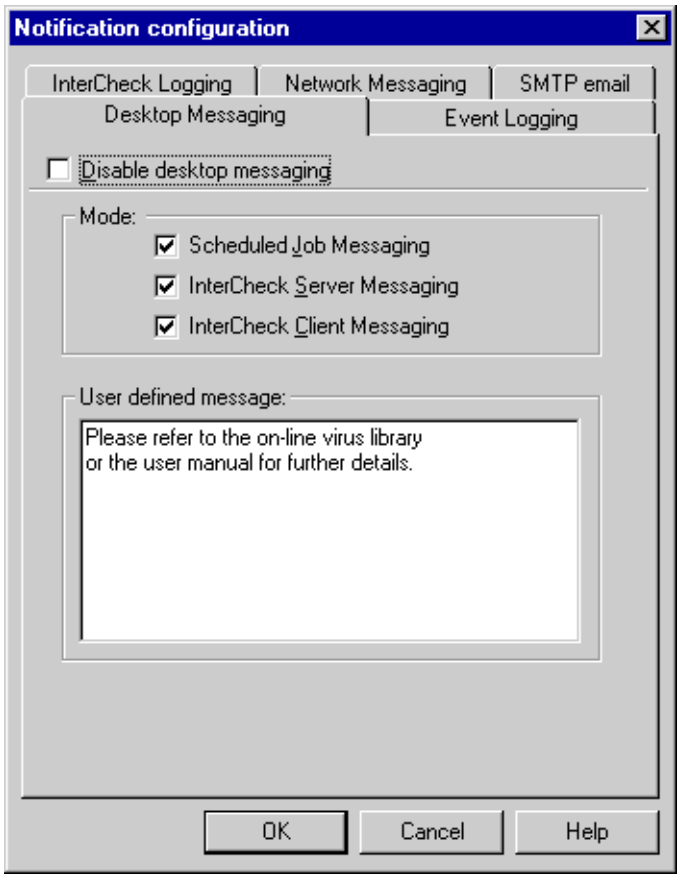
SMTP email



The email addresses of the recipients of the notification messages can be added and removed. Click *Configure SMTP* to enter the host name or IP address of the SMTP server:



Desktop messaging



The Desktop Messaging option controls the message displayed on discovery of a virus when the GUI is not active.

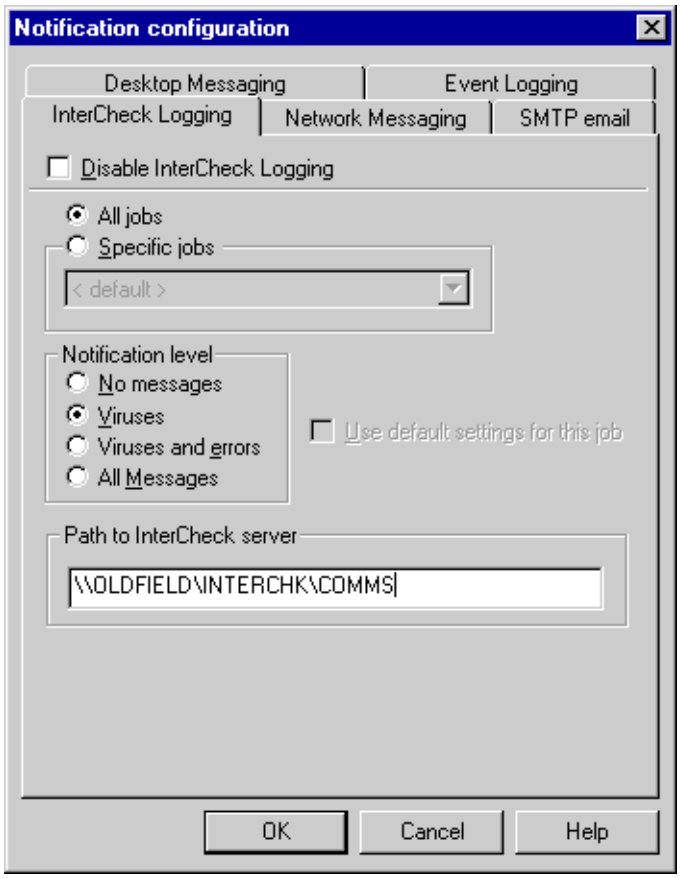
Mode

The user defined message can be displayed in scheduled, InterCheck server and/or InterCheck client mode(s).

User defined message

The user defined message will be added to the end of the standard virus detected message.

InterCheck logging



Path to InterCheck server

Stand-alone InterCheck clients can send log messages to the COMMS directory of a remote InterCheck server. Specify a UNC path name, e.g.

```
\\ServerName\INTERCHK\COMMS
```

SWEEP needs a user account to log in to the network. It will use the same account that the auto-upgrade facility uses to check for newer versions of SWEEP (see the 'Auto-upgrade service account details' section of the 'Installing SWEEP' chapter). This account can be changed (see the 'Managing the

SWEEP services' section of the 'Installing SWEEP' chapter for more information).

Messages will be logged by the remote InterCheck server and may generate additional alerts.

SWEEP options

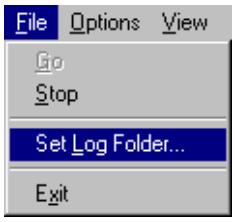
This chapter describes the options available through the *File*, *Options* and *View* menus.

Set log folder

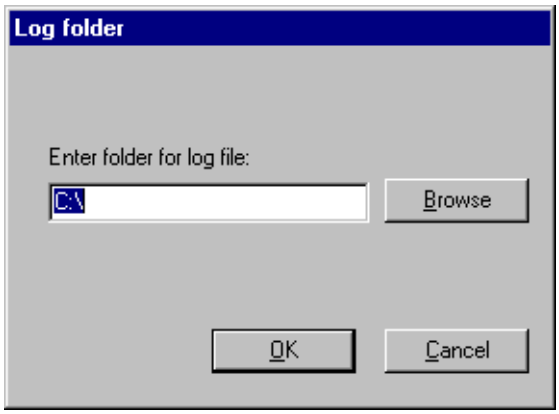
SWEEP maintains a continuous log of all of its activity. This log file contains administrative messages along with the messages described in the 'On-screen log messages' chapter, and is aimed at the Administrator. It is generated in addition to the report file, which is aimed at the user (see the 'Reporting results' section of the 'Configuring SWEEP' chapter).

Note that the log file is written as the SWEEP service user and not as the GUI user.

The location of the log file can be specified by the *Set Log Folder* option from the *File* menu.



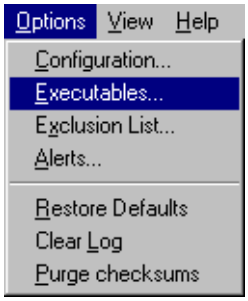
By default the log file will be saved in the SWEEP directory, but this can be changed:



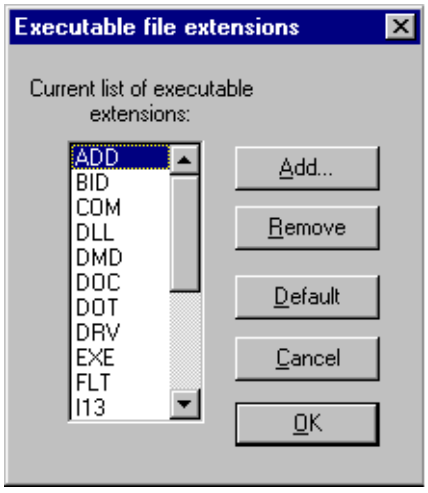
It is recommended that networked resources are referred to by UNC names because mapped drives are only available when a user is logged in to the machine. The browse control will only show those files and directories to which SWEEP has access.

This option is only available to Administrators.

Executables

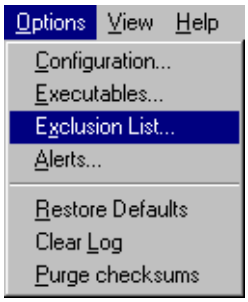


The list of file extensions to be treated as executables by SWEEP can be edited with this option. This list is only used if SWEEP is set to check 'executable' rather than 'all' file types. See also the 'File types' subsection of the 'Immediate mode' section of the 'Using SWEEP' chapter.

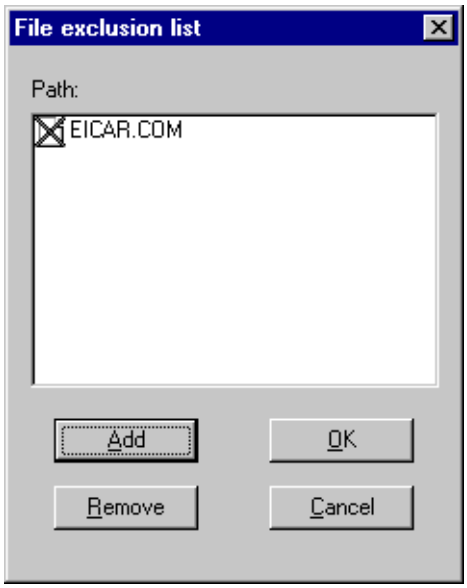


This option is only available to Administrators.

Exclusion list

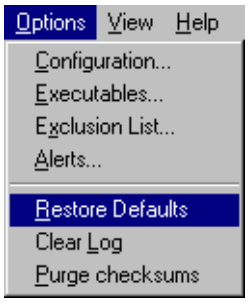


The exclusion list contains the specific files to be excluded from all SWEEP operations.



This option is only available to Administrators.

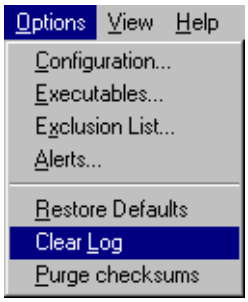
Restore defaults



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

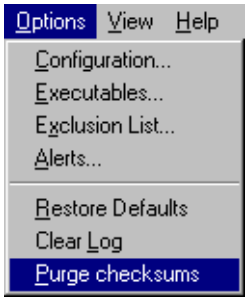
For non-Administrators, this will affect only their own immediate sweep settings.

Clear log



The on-screen log provides a record of activity in the current session, and of all the scheduled and InterCheck mode activity since the service was started. The on-screen log also reflects the information that is appended to the continuous log file on disk. The *Clear log* option clears the on-screen log, but does not affect the continuous log file on disk.

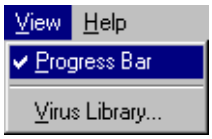
Purge checksums



SWEEP for Windows NT maintains two checksum files: the central checksum file contains the items authorised by the InterCheck server for use by networked InterCheck clients, and the local checksum file contains the items authorised by the Windows NT InterCheck client. Selecting *Purge checksums* will clear both checksum files.

This option is only available to Administrators.

Progress bar



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

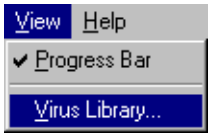
Note that the progress bar is set separately for immediate and scheduled modes.

The virus library

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

Starting the virus library

Select *Virus Library* from the *View* menu

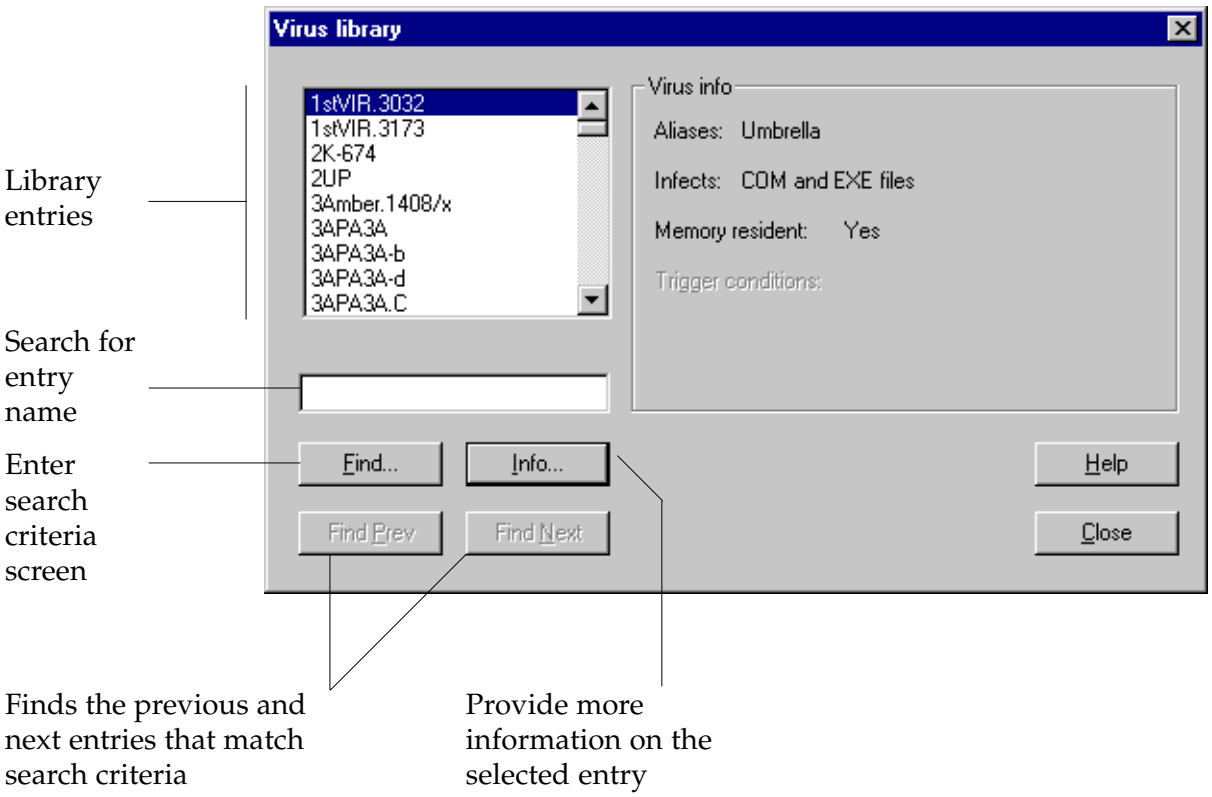


or click the associated icon

to start the on-line virus library.

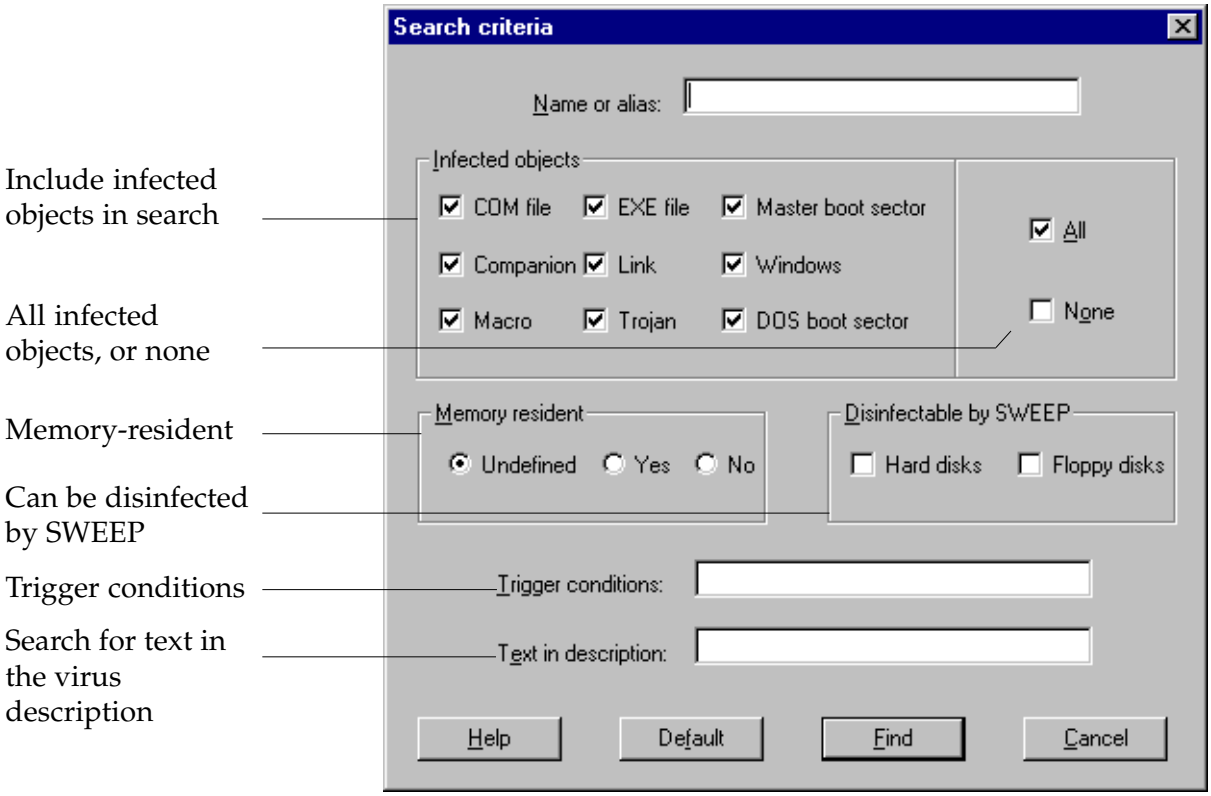
Hint: When SWEEP discovers a virus, double-click on the 'virus detected' entry in the on-screen log to go straight to the relevant library entry.

Information on a particular virus



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

Searching for a particular virus



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

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

Infected objects

Viruses can attach themselves to COM and EXE files; they can infect the master boot sector or the DOS boot sector; companion viruses place the virus code in a COM file with the same name as the EXE file; link viruses subvert directory entries to point to the virus code; Windows viruses affect Windows executables; and macro viruses place viral macros inside Microsoft Word and Excel documents. Trojan horses are not

viruses, but are programs which provide unanticipated and undesired side-effects when executed.

Memory-resident

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

Disinfectable by SWEEP

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

Trigger conditions

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

Text in description

The 'Text in description' option will search for a string which appears in the information about that virus.

Installing InterCheck clients

This chapter describes how to install and run InterCheck clients.

Note: For information on installing the stand-alone Windows 95 and Windows NT InterCheck clients, see the 'Installing SWEEP' chapter of the SWEEP for Windows 95 or SWEEP for Windows NT manual.

Which kind of InterCheck client?

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

Networked InterCheck clients

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

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

Stand-alone InterCheck clients

Stand-alone InterCheck clients do not require a remote InterCheck server, and use a local installation of SWEEP for virus checking. They offer faster initial authorisation of files, create less network traffic, and

can also be used on stand-alone workstations or workstations not always connected to the network.

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

Installing networked InterCheck clients

Before installing networked InterCheck clients:

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

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

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

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

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

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

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

Now consult the following instructions for the relevant operating system.

Networked InterCheck clients for DOS and Windows

With a login script

Locate the users' login batch file (see the Windows NT documentation), and include the following:

```
NET USE I: \\ServerName\INTERCHK
I:\ICLOGIN
```

where I: can be any unused drive letter, and *ServerName* is the name of the server on which SWEEP is installed.

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

Without a login script

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

For example, with a Windows NT server enter the line

```
NET USE I: \\ServerName\INTERCHK
```

in the login script, or with a NetWare server enter the line

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

in the login script, or with a Banyan VINES server enter the line

```
SETDRIVE I "InterCheck@Vanye@Server"
```

in the user profile.

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

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

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

Networked InterCheck clients for Windows 95

With a login script

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

Without a login script

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

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

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

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

Networked InterCheck clients for Macintosh

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

At the Macintosh workstation, insert the 'InterCheck' 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.

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 SWEEP for Windows NT and SWEEP for Windows 95 manuals 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 'InterCheck' disk into the floppy disk drive, and enter

```
A:ICINSTAL
```

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

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 'Networked InterCheck clients for DOS and Windows' subsection of the 'Installing networked InterCheck clients' section.

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

Before installing the InterCheck client

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

Configuring the InterCheck client

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

Automatic or manual installation?

There are two ways to run the installation program:

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

Interactive or non-interactive installation?

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

Installing automatically from a login script

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

For example, with a Windows NT server enter the lines

```
NET USE I: \\ServerName\Directory
I:\ICLOGIN -A
```

or with a NetWare server 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. With a Banyan VINES server, run ICLOGIN with the -A option from the user profile. For example

```
SETDRIVE I "InterCheck@Vanye@Servers"
POSTLOGIN /DOS I:\SWEEP\ICLOGIN -A
POSTLOGIN /WIN95 I:\SWEEP\ICLOGIN -A
```

if InterCheck@Vanye@Servers is the file service on the file server that contains the InterCheck files.

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

Alternatively, if a permanent mapping to a drive is not required or not possible, 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, on a Windows NT server

```
NET USE I: \\ServerName\directory
I:\ICLOGIN -A -U
NET USE I: /DELETE
```

or on a NetWare server

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

The -U option may not have any effect with a Banyan VINES server because some Banyan VINES clients do not currently support UNC drive names.

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. Note that this will not work with Banyan VINES file servers.

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 SWEEP for Windows NT user manual.

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 a local copy of SWEEP 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 SWEEP for DOS user manual.

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 if the server SWEEP supports it, but 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 option 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.

CLI SWEEP for Windows NT

This chapter documents the Command Line Interface (CLI) version of SWEEP for Windows NT. Unless otherwise specified, all references to SWEEP or SWEEP for Windows NT in this chapter refer to the CLI version.

System requirements

The minimum requirements to use SWEEP for Windows NT are:

- An Intel 386, or an Alpha AXP based computer.
- Microsoft Windows NT 3.1 or later.
- 3 Mb of free hard disk space.

Installing SWEEP in stand-alone mode

Install SWEEP in stand-alone mode if InterCheck server functionality is not required.

Installing SWEEP

Log in as a user with Administrator privileges. Insert the SWEEP for Windows NT disk into the drive. Select *Run* from the Program Manager's *File* menu and enter

```
A:SETUP
```

The setup program will create a common program group and an icon for the application. If SWEEP

needs to be reconfigured later, press *Alt+Enter* when the SWEEP icon is highlighted and edit the command line options.

Running SWEEP

To check all hard disks present on the system either double-click on the SWEEP icon or type

```
NTSWEEP
```

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

```
NTSWEEP A:
```

Installing SWEEP in InterCheck server mode

Install SWEEP in InterCheck server mode if InterCheck server functionality is required. This is easiest to do at the server itself.

Note: It is preferable to use the GUI version of SWEEP to do this, because SWEEP will then run as a Windows NT service, i.e. independently of users.

Initial installation

Log in as a user with Administrator privileges.

Open a command line box. Insert the ICONTROL diskette into drive A: and run NTICINST:

```
A:NTICINST PathName
```

where *PathName* is the full path of the directory into which SWEEP will be installed, for example:

```
A:NTICINST C:\SWEEP
```

Follow the on-screen instructions.

Setting up share permissions

In File Manager, select the drive and directory into which SWEEP has just been installed. From the *Disk* menu, select *Share As*. In the Shared Directory dialog box, type

```
INTERCHK
```

in the Share Name field. Click on *Permissions* and ensure that *Everyone* has at least *Change* access to this share. Click on *OK* on each box to create the share.

The InterCheck users should also have change access to the COMMS and LISTS directories, and no access to the INFECTED directory.

Creating the configuration file

Open a command line box and type

```
CD PathName
```

where *PathName* is the same as selected above.

Type

```
ICONTROL
```

to start ICONTROL, then exit ICONTROL. This creates a marker file required by SWEEP.

Starting the InterCheck server

To start the InterCheck server, enter at a Command Prompt

```
NTSWEEP -ICS
```

SWEEP is now ready to process InterCheck requests from clients on remote machines.

Controlling the InterCheck server

This is accomplished by running ICONTROL.EXE (for DOS) or ICW.EXE (for Windows).

Updating SWEEP

SWEEP is updated monthly.

If using InterCheck, on the server press *Alt* and *Tab* until the InterCheck server window is active. Press *Ctrl-C* to stop the InterCheck server. If using Event Viewer, exit from it.

On the server, use File Manager or the COPY command to copy the whole contents of the new 'SWEEP for Windows NT' disk to the directory where SWEEP is installed (usually \SWEEP). If using InterCheck, copy the contents of the new 'SWEEP for DOS' disk to this directory too. It is not necessary to update the INTERCHK or ICONTROL files.

At the Command Prompt, type:

```
NTSWEEP
```

SWEEP will load and run. Alternatively, to restart the InterCheck server, type:

```
NTSWEEP -ICS
```

Using SWEEP

Checking the hard disk

Enter the command

```
NTSWEEP
```

SWEEP will check all hard drives on the system. SWEEP can be interrupted by pressing *Esc* at any time.

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

```
NTSWEEP D: E:
```

If SWEEP discovers any viruses, it will display a message box at the end of the run and sound a bell. To clear the warning, press *Enter* or click *OK*. Viruses which have been discovered will be displayed in the SWEEP box.

Checking multiple floppy disks

Run SWEEP using the command

```
NTSWEEP -MU A:
```

SWEEP will prompt the user to insert each floppy disk to be checked. Press *Esc* to terminate the process.

Checking file servers

SWEEP can be used to check file server logical drives over a network. On most networks it is necessary to be logged in as an Administrator or have **read** rights equivalent to those of an Administrator.

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

```
\PAGEFILE.SYS
%SystemRoot%\SYSTEM32\CONFIG\APPEVENT.EVT
%SystemRoot%\SYSTEM32\CONFIG\DEFAULT
%SystemRoot%\SYSTEM32\CONFIG\DEFAULT.LOG
%SystemRoot%\SYSTEM32\CONFIG\SAM
%SystemRoot%\SYSTEM32\CONFIG\SAM.LOG
%SystemRoot%\SYSTEM32\CONFIG\SECEVENT.EVT
%SystemRoot%\SYSTEM32\CONFIG\SECURITY
%SystemRoot%\SYSTEM32\CONFIG\SECURITY.LOG
%SystemRoot%\SYSTEM32\CONFIG\SOFTWARE
%SystemRoot%\SYSTEM32\CONFIG\SOFTWARE.LOG
%SystemRoot%\SYSTEM32\CONFIG\SYSEVENT.EVT
%SystemRoot%\SYSTEM32\CONFIG\SYSTEM
```

```
%SystemRoot%\SYSTEM32\CONFIG\SYSTEM.ALT
%SystemRoot%\SYSTEM32\CONFIG\%USERNAME000
%SystemRoot%\SYSTEM32\CONFIG\%USERNAME000.LOG
```

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

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

SWEEP is capable of scanning files which have read access removed by their owner without changing either the owner or altering the discretionary access control list for those files.

What if SWEEP reports a virus or virus fragment?

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

The screen output will look something like this:

```
SWEEP virus detection utility
Version 3.00
Copyright (c) 1989,97 Sophos Plc, Oxford

System time 15:20:36, System date 10 September 1997
This issue includes viruses known to Sophos up to 01 August 1997

Quick Sweeping 3 areas for 11749 viruses.
Press Esc to quit.

>>> Virus 'G2 V0.70B' found in sector 0 of drive A:
>>> Virus 'G2 V0.70B' found in file A:\V.COM
1 file (1.5 Kbytes) swept in 0 minutes and 1 second
at 1536 bytes/second.
2 viruses were discovered.
1 file out of 1 was infected.

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

Scheduling SWEEP

SWEEP can be scheduled to check the local drives on a regular basis using the Windows NT AT command. For example, the following instruction will cause SWEEP to be executed at midnight each day and place the output in the file SWEEP.LOG:

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

It is important to specify the '/interactive' parameter to the AT command, and the -NK parameter to NTSWEEP. Adding the -A command line parameter to the NTSWEEP command will cause the log to be appended to by each successive use of SWEEP.

The log file or the Windows NT Event Log should be examined regularly to determine whether files are infected. All filenames used should be specified with full paths. Windows NT scheduled tasks are persistent, which means that if the machine is rebooted the tasks will still be there.

The AT command can be used to list the tasks scheduled on your system:

```
AT
```

Note that the schedule service must be started on the machine before scheduled tasks can be set up. This is done by entering the command

```
NET START SCHEDULE
```

or from the 'Services' section of the Control Panel.

For more information on the use of the Windows NT Schedule Service, consult the Windows NT documentation.

What does SWEEP check?

By default, SWEEP looks for viruses in:

- All files defined as executables, i.e. COM, DLL, DOC, DOT, EXE, OV?, SYS and XL? files on all local hard disk drives.
- Logical sector 0 of all local hard disk drives (operating system boot sectors).
- Physical sector 1 of hard disk devices (master boot sectors).

Additional (or different) areas or file types can be specified from the command line or by creating an area file. If this is done, all default settings will be overridden unless the -AS qualifier is added to the command line.

The syntax for describing areas to be checked is described in the following sections.

Specifying items to be checked in the area file

The area file must reside in the current drive and subdirectory when SWEEP is run. The default area file is called SWEEP.ARE, although the -AF qualifier can be used to specify another name.

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

For example, the area file may contain

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

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

Note: The | symbol is the Windows NT 'pipe' operator and is not the same as 1 (digit) or l (character).

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

```
NTSWEEP A: D:
```

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

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

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

```
NTSWEEP -AD=A
```

then SWEEP will check

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

All local hard disk drives can be specified with the entry

```
*:
```

and this operator also accepts file specifications, so for example

```
*:\*.SYS
```

will sweep all SYS files in the root directory of every drive. This also works with the exclusion operator (see below).

Universal Naming Convention (UNC) names can also be used in the area file. For example

```
\\ACCOUNTS\ADMIN\"All Executables"
```

will sweep all the files with executable extensions in the \\ACCOUNTS\ADMIN share and all subdirectories thereof.

Files

Particular file types and areas can be specified in the area file using the normal Windows NT descriptions. For example

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

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

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

```
C:*.ABC
```

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

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

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

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

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

To check all executable files specify

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

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

Excluding files

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

For example

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

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

For example

```
<FOO.EXE   ; file FOO.EXE will be excluded
           ; in whatever drive and
           ; directory it may appear
<C:FOO.EXE ; FOO.EXE will be excluded in
           ; drive C:'s current directory
<\J\FOO.EXE; FOO.EXE will be excluded
           ; if found in the \J directory
           ; of the current drive
<J\FOO.EXE ; FOO.EXE will be excluded if
           ; found in the J subdirectory
           ; of the current directory on
           ; the current drive
```

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

Hint: To exclude complete directories, specify the full directory path, excluding the tail \. For example

```
<\FOODIR
```

Disk sectors

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

Sectors can be referred to in two ways: as *logical* sectors or as *absolute* sectors. A *logical* sector number refers to the position of the sector within a particular drive or partition. This is useful when referring to the

partition boot sector, which is logical sector 0 of the partition. The *absolute* specification of a sector is in terms of its physical position on the specified device. While more complex than a logical sector number, it allows any sector on the disk to be specified. This is important for checking the *master boot sector*, which can be found at absolute sector 0.

Logical Sectors

To specify a logical sector or set of sectors, use the '`|`' symbol. It is also possible to specify a byte or group of bytes to be checked in each sector (e.g. if it contains variable information). The format of the specification is

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

where

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

`ssector` is the first logical sector to be checked

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

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

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

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

For example

```
C:|0
```

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

```
C:|0 10
```

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

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

```
|*
```

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

Absolute Sectors

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

The format of the specification is

```
+drive sector
```

where

`drive` is the disk drive number

`sector` is the sector number

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

For example

```
+80 1
```

specifies that sector 1 on the first fixed disk should be checked.

To check master boot sectors on all hard drives, specify

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

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

Sweeping with new identities

To upgrade SWEEP 'in-the-field', send a copy of the suspected virus to Sophos. We will analyse it and send back the '*identity*' which describes it in VDL (Virus Description Language). Using a text editor, create the file NAME.IDE (where NAME is the virus name, e.g. TREMOR.IDE) and type in the identity, which normally consists of about 20 hexadecimal digits. This can be faxed, emailed, or downloaded from the Sophos Web site. Identities contain a checksum which is verified by SWEEP.

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

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

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

Sweeping with new patterns

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

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

where

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

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

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

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

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

For example, SWEEP.PAT may contain

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

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

```
NTSWEEP A:
```

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

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

```
NTSWEEP C: -F
```

Running SWEEP at different priorities

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

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

```
NTSWEEP -PR=H
```

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

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

```
NTSWEEP -PR=L
```

This makes SWEEP run only when Windows NT would otherwise be idle.

Running SWEEP from batch files

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

SWEEP returns:

0 If no errors are encountered and no viruses found.

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

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

3 If viruses or virus fragments are discovered.

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

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

```
GOTO END
:FISHY
ECHO Something has been discovered
:END
```

This batch file will print

```
Something has been discovered
```

if SWEEP discovers a virus,

```
Some error has occurred
```

in the event of an error, or

```
No problems
```

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

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

Running SWEEP continuously

SWEEP can be configured to run continuously in the background. To do this, write a batch file which will restart SWEEP after the scan is completed. For example

```
:SWEEP
C:\SWEEP\NTSWEEP -P=C:\SWEEP\SWEEP.LOG -A -PR=L
GOTO SWEEP
```

The command line argument

```
-PR=L
```

forces SWEEP to run at a low priority level so that the impact on server performance is reduced. The command can be executed from the Startup program group.

Customising the 'Viruses found' report

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

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

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

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

Event logging

Whenever SWEEP is run, it will automatically update the Windows NT Application event log. This feature can be disabled by using the -NE command line qualifier.

In order to cut down the number of messages written to the log, use the -QE command line qualifier, which will cause only error messages and virus alerts to be written.

Note: The System event log is not updated if SWEEP is run from a floppy disk.

MAPI interface

SWEEP can mail a copy of the report when it is run by using MAPI. Use the -MI command line qualifier to specify the profile and password (-MI=<profile>,<password>) from which mail will be sent. The mail will be sent to the alias *sweepers*.

For example:

```
NTSWEEP -MI=ian,fish
```

If the account and the password are not specified, mail will be sent from an account with the name and password *'sweep'*.

If SWEEP is run in InterCheck server mode, the mail is sent on every logged event, such as a virus discovery.

MAPI profiles which use Microsoft Mail as their transport will not function in service mode, i.e. when SWEEP is run from the AT scheduler.

Automatic virus handling

SWEEP can deal with viruses in two ways: disinfection or removal.

Virus disinfection

The removal of some boot sector viruses from hard disks and most macro viruses from Word documents can be performed by using the disinfection capability built into SWEEP. To enable disinfection, the command line qualifier -DI must be used

```
NTSWEEP C: -DI
```

Use the -DIB qualifier to disinfect only boot sectors, and the -DID qualifier to disinfect only documents.

Disinfection of hard disks is normally preferable to virus removal, as described in the next section.

Virus removal

SWEEP has facilities to disable some viruses while the infected system is running.

If the virus is in an executable file, it can be disabled by deleting the infected file. Use the command line qualifier -REMOVEF:

```
NTSWEEP -REMOVEF
```

-REMOVEF is useful because it only affects infected files, which can be done on network drives from a workstation. -REMOVEF does not require Windows NT to be shut down.

If the command line qualifier -RS is specified as well as -REMOVEF, infected files will be positively overwritten (shredded) instead of simply being deleted. Note that this makes them unrecoverable.

In either case, the user will be asked whether each file should be removed or not, and whether each boot sector should be disabled. If the -NOC command line qualifier is used, however, SWEEP will not ask for confirmation before removal is performed. Use this qualifier with care!

-REMOVE has the same effect as -REMOVEF, but tries to clean up system areas as well. If the virus is in the boot sector or other system area, use -REMOVE, which is described in greater detail in the 'SWEEP command line qualifiers' section.

Important! -REMOVE disables infected boot sectors (both master boot sectors and Windows NT boot sectors) by modifying them in such a way that if a disabled machine is bootstrapped, it will merely hang.

Full sweep

By default, 'quick sweep' is enabled. This checks only those parts of files likely to contain viruses and is marginally less secure than checking the entire contents of files.

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

```
NTSWEEP -F B:
```

will perform a full sweep of drive B:.

SWEEP command line qualifiers

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

```
NTSWEEP -?
```

The command format is

```
NTSWEEP d1 ... dn f1 ... fn q1 ... qn
```

where

`d1` to `dn` are the drives which will be checked (A:, B:, C: etc.) and '*:' denotes all hard drives

`f1` to `fn` are descriptors of files checked

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

For example

```
NTSWEEP A: C:
```

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

@file Command line qualifiers from an external file

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

```
-P="Sweep Log.TXT"
-NS -A -EX=COM,DLL,SYS
```

entering

```
NTSWEEP @EXAMPLE.TXT
```

would have the same effect as the command

```
NTSWEEP -P="Sweep Log.TXT" -NS -A -EX=COM,DLL,SYS
```

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

-? Help

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

-6 62 seconds

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

-A Append report

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

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

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

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

-AD=<drive> Area file default

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

For example

```
NTSWEEP -AD=X
```

would assume that all areas refer to drive X:.

-AF=<filename> Area file

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

See also the 'Specifying items to be checked in the area file' section above.

-ALL Sweep all files

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

```
\>*.*
```

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

For example

```
NTSWEEP A: -ALL
```

will check all files on drive A:.

Warning! This is a slow process which can cause false positives.

-AS Sweep standard areas

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

For example

```
NTSWEEP SUSPFILE.EXE -AS
```

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

-CC Central checksumming

The -CC qualifier will cause SWEEP to generate a central checksum list for use with InterCheck. It will only work if SWEEP is installed as an InterCheck server. The InterCheck clients will use the central checksum file as well as their own local checksum files. Any file scanned and found to be virus-free by SWEEP will be checksummed and the checksum added to the central file. This feature works in InterCheck server mode (initiated with the -ICS qualifier) and standard SWEEP mode (including background or start-up sweeps).

To add files held on another server to the central checksum file, sweep it over the network from the server with the central checksum file. It is not possible to update a central checksum file held on one server from another.

The -CC qualifier serves no purpose on non-InterCheck servers.

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

SWEEP may be placed in the common Startup folder; however it may not be desirable to perform the system check every time Windows NT is booted. The -D qualifier allows the user to specify either the probability with which SWEEP will actually proceed to check the system, or the day of the week on which the system should be checked.

For example

```
NTSWEEP -D=MONDAY
```

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

Alternatively

```
NTSWEEP -D=20
```

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

See also the -DE command line qualifier.

-DA Display areas

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

-DE Daily execution

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

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

For example

```
NTSWEEP -DE
```

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

For example

```
NTSWEEP -DE=SWEEP.DA1
```

-DI Disinfect

This command line qualifier enables SWEEP to perform automatic disinfection of some boot sector viruses and some macro viruses.

See also the 'Automatic virus handling' section and the -DIB and -DID command line qualifiers.

-DIB Disinfect boot sectors

Use the -DIB qualifier to disinfect only boot sectors.

-DID Disinfect documents

Use the -DID qualifier to disinfect only documents.

-DL Display library

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

-DN Display names of files as they are scanned

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

-ELA Write log messages to the Application event log

SWEEP will write log messages to the Application event log by default.

-ELS Write log messages to the System event log

If this command line qualifier is specified, SWEEP will write log messages to the System event log rather than the Application event log. For this feature to work, SWEEP must be or have once been executed by an Administrator on the machine.

-EV=<machine> Remote event log

This qualifier forces SWEEP to write event log messages to the specified remote machine in addition to the machine SWEEP is running on.

-EX=<extensions> Executable extensions

The extensions of files that SWEEP normally treats as executables are COM, DLL, DOC, DOT, EXE, OV?, SYS and XL?. This can be changed with the -EX command line qualifier.

For example

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

will remove DLL files from the list of executable files and

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

will add the VXD extension.

-F Full sweep

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

See also the 'Full sweep' section above.

-FM=<file> Specify message file

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

The default filename of MESSAGEFILE is 'SWEEP.MSG'.

For example

```
NTSWEEP -FM=MY_MSG.TXT
```

specifies the file 'MY_MSG.TXT'.

-FS File server

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

-ICS[=<servername>] InterCheck server mode

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

For example

```
NTSWEEP -ICS=Server_1
```

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

-MAC Macintosh virus scanning

The use of the -MAC qualifier will force SWEEP to scan Macintosh files for viruses as well as the standard PC viruses. This feature should be used either with -ALL qualifier or with a file specification of *.*, because otherwise SWEEP will only scan files with the standard executable extensions. For example

```
NTSWEEP -MAC *.* -REC
```

will scan all files in the current directory and its subdirectories for both Macintosh and PC viruses.

When used in conjuction with -ICS, the InterCheck server will also scan files for Macintosh viruses.

-MI=<account>,<password> mail interface

This enables the sending of a copy of the SWEEP report via MAPI. It logs on to mail with the profile and password specified and sends the report to the alias *sweepers*.

If no profile and password are specified, SWEEP will perform the operation using *sweep* as both the profile and password.

For example

```
NTSWEEP -MI=IAN,FISH
```

Note that this option does not work when SWEEP is run as a service, e.g. when run from NTSweepLoader or as an AT scheduled job.

-MSG=<name>[,<name2>,...]

This will cause SWEEP to send a network message to the named machines or users. Note that only one machine can be notified under each name, so if a user name is specified, and that user is logged in to two machines, they will only receive the message at the first machine. This is due to limitations in the Lan Manager messaging system. For this reason it is recommended to use machine names as recipients.

Note also that in order for Windows 95 or Windows for Workgroups PCs to receive messages, they must be running the WinPopup application.

-MU Check multiple disks

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

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

```
NTSWEEP -MU A:
```

When prompted, insert a disk in drive A: and press any key to start checking it. Once that disk has been checked, insert another disk into drive A: when prompted, and press any key to start checking.

This will continue until *Esc* is pressed to interrupt the checking or until SWEEP detects one or more viruses.

-NAB Do not check boot sectors

This prevents SWEEP from attempting to check the boot sectors. It is used to avoid the 'Could not read' error message when used (e.g. in the system login script) by someone without Administrator privileges.

-NAF Do not read file with areas to be checked

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

-NAP Do not use internal virus patterns

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

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

-NAS Do not check standard areas

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

Note: The area file (normally SWEEP.ARE) must reside on the current drive and in the current subdirectory.

-NB No bell

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

-NCI Do not check identities

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

-NDI Do not disinfect infected items

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

-NE No event log

SWEEP makes an entry in the event log every time that it is run and when it is stopped. This command line qualifier prevents this. See also the -QE, -ELA and -ELS qualifiers.

Events are not logged if SWEEP is run from floppy disk.

-NEM Do not use the emulator

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

-NI No interrupting

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

-NK No key to continue

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

-NOC No confirmation before virus removal

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

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

Warning! Use this qualifier with care!

-NS Not silent

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

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

-NTW No Temp Warning

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

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

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

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

For example

```
NTSWEEP -P=SEC.DOC
```

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

-PAT=<Hex> Pattern specification

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

If found, such patterns are reported as 'Command line 1' etc.

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

For example

```
NTSWEEP -F -PAT=23f78172bca918e1
```

-PD Pause on discovery of a match

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

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

-PR=H|L Priority

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

```
NTSWEEP -PR=H
```

specifies high priority, while

```
NTSWEEP -PR=L
```

specifies low priority.

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

-Q Quick sweep

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

-QE Suppress informational entries to event log

SWEEP makes an entry in the event log every time that it runs and when it is stopped. If this command line qualifier is used, only error messages and virus alerts will be written. See also the -ELA, -ELS and -NE qualifiers.

-REC Recursive search

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

For example

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

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

-REMOVE Remove viruses on discovery

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

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

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

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

For example

```
NTSWEEP -REMOVE
```

or

```
NTSWEEP -REMOVE -RS -NOC
```

See also the 'Virus removal' section.

-REMOVEF Remove infected files

As -REMOVE, except that infected boot sectors are not disabled. This is especially useful if it is inconvenient to boot Windows NT from floppy disk.

-RS Remove viruses by positively overwriting them

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

Disabling of boot sectors is not affected.

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

For example

```
NTSWEEP -REMOVE -RS
```

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

See also the 'Virus removal' section.

-S Silent running without displaying checked areas

By default, SWEEP does not display the areas it is checking onthe screen. The qualifier -S is equivalent

to this default mode, and is the opposite of the -NS qualifier.

-SC Scan inside compressed files

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

Note: This option is not necessary to sweep files on NTFS volumes which have the Windows NT compression attribute set.

-SS Super silent running

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

-WC Warn if compressed files are encountered

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

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

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

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

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

Treating viral infection

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

Automatic disinfection

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

SWEEP for Windows NT can:

- Disinfect documents infected with certain types of macro viruses.
- Disinfect floppy disks infected with boot sector viruses.
- Deal with infected executable files.

Manual disinfection

In some cases, for example when automatic disinfection is deselected, or a hard disk boot sector is infected, manual disinfection may be necessary.

The exact manual disinfection process may also depend upon the specific virus, so consult SWEEP's virus library before attempting disinfection.

Hint: When SWEEP discovers a virus, double-click on the 'virus detected' entry in the on-screen log for advice.

Important! If in doubt, please contact Sophos' technical support before performing any of the operations described here.

Creating a clean DOS boot disk

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

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

```
FORMAT A: /S
```

Copy HIMEM.SYS, EMM386.EXE, FDISK.EXE, SYS.COM (not to be used on Windows NT), DEBUG.EXE, SMARTDRV.EXE, SCANDISK.EXE (or CHKDSK.EXE for MS-DOS 5 and before), and FORMAT.COM onto the disk. HIMEM.SYS is an Extended Memory (XMS) driver which allows SWEEP to use all the PC's memory thereby improving performance. SMARTDRV.EXE is a disk caching program which improves SWEEP's performance by minimising the amount of disk access required when traversing the directory structure of a disk.

Create a CONFIG.SYS file with the following lines:

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

Create an AUTOEXEC.BAT with the following lines:

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

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

If a computer becomes infected, use the clean boot disk to boot the computer. This will ensure that various items on the computer can be examined through a 'clean' operating system, giving the virus no chance to employ hiding techniques.

Manual disinfection of infected boot sectors

The process for manually disinfecting a boot sector virus depends on whether the virus is a master boot sector virus or a partition boot sector virus, and whether it is on a hard disk or a floppy disk.

Boot sector viruses on the hard disk

If the hard disk is infected with a boot sector virus, SWEEP for Windows NT will not be able to disinfect it automatically. Before attempting manual disinfection, it is advisable to backup any important data contained on the hard disk.

Master boot sector virus

Reboot the PC with a clean boot disk. Use SWEEP for DOS to disinfect the virus, e.g. with the command

```
SWEEP -DI
```

Alternatively, **reboot the PC with a clean boot disk**, check that the contents of the infected drive are visible (e.g. with `DIR`), and replace the master boot sector with the command

```
FDISK /MBR
```

If the contents of the hard disk are not visible after a clean boot, contact Sophos' technical support for advice. Some boot sector viruses do require additional action for full recovery. For example, the

OneHalf virus encrypts the boot sector so that it is only readable when the virus is in memory.

Partition boot sector virus

Infected partition boot sectors on Windows NT machines usually require specialist attention. Most viruses are written for DOS, and therefore assume the machine has a DOS boot sector instead of a partition boot sector. Contact Sophos' technical support for advice.

Boot sector viruses on floppy disks

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

Manual disinfection of infected executable files

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

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

Manual disinfection of infected documents

When dealing with infected documents, it is not necessary to reboot from a clean system disk. However, it is important to ensure that the application that created the document is not open when disinfection is attempted.

In some cases it is possible to manually edit the macros from the infected document using the relevant application. However, some macro viruses

now operate a form of stealth to prevent users from doing this. For example, *Winword/ShareFun* prevents the use of the Tools/Macro and File/Templates menu option. Please consult Sophos' technical support before attempting to perform manual disinfection of macro viruses.

Recovering from virus side-effects

Recovery from virus side-effects depends on the virus. In the case of innocuous viruses such as *Cascade*, recovery from side-effects is not necessary, while in the case of a virus such as *Michelangelo*, recovery will usually involve the restoration of a complete hard disk.

Some viruses, such as *Winword/Wazzu* gradually make minor changes to users' data. This sort of corruption (e.g. the removal of the word 'not' from a sentence in a Word file) can be very hard to detect and highly undesirable.

The most important thing when recovering from virus side-effects is the existence of **sound backups**. Original executables should be kept on write-protected disks, so that any infected programs can easily be replaced by the original clean versions.

Sometimes it is possible to recover data from disks damaged by a virus. Sophos can also supply utilities for repairing the damage caused by some viruses. Contact Sophos' technical support for advice.

After disinfection

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

- Uncover and close the loopholes which allowed the virus to enter the organisation.

- Inform any possible recipients of infected disks outside the organisation that they may be affected by the virus.
- In the UK, inform the *Computer Crime Unit* of *New Scotland Yard* in London about the attack (Tel 0171 230 1177, Fax 0171 230 1275).

Troubleshooting

This chapter provides answers to some common problems which can be encountered when using SWEEP. See also the 'On-screen log messages' chapter for details of individual error messages.

Incorrect access rights (NTFS)

The Administrator account should have full control of all the directories SWEEP creates. Everyone must have the following access rights:

\SWEEP	Read and execute
\SWEEP\COMMS	Read, write and execute
\SWEEP\INFECTED	No access
\SWEEP\LISTS	Read, write and execute
\SWEEP\REPORTS	Read, write and execute to their own report files

The SWEEP installation program will assign these rights automatically. However, if they are changed, SWEEP may, for example, be unable to start InterCheck or to open the log or report files.

If problems do occur, log in as the local Administrator and amend the access rights using the Windows NT Explorer (see the Windows NT documentation).

Note that the COMMS and REPORTS directories are only created if SWEEP is installed as an InterCheck server.

SWEEP runs slowly

Full sweep

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

Checking all files

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

Network drives selected

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

Progress bar selected

If the progress bar is selected, SWEEP will have to count all the items that are to be swept. This can take several minutes on large network drives.

InterCheck server runs slowly

A high volume of requests from networked InterCheck clients will slow the InterCheck server.

Files waiting to be checked are stored in the InterCheck server's COMMS directory. Note that a network can have more than one InterCheck server, and that some networked InterCheck clients could be run as stand-alone InterCheck clients.

Auto-upgrades fail to happen

The SWEEP for Windows NT Network service may be registered as an account which does not have sufficient rights to access SWEEP's central installation directory. See the 'Managing the SWEEP services' section of the 'Installing SWEEP' chapter for more information. The central installation directory must also have the SETUP.EXE and WSWEEPNT.CFG files present.

SWEEP service fails to start

Ensure that the password for the SWEEP for Windows NT service account is still valid, and that the service has not been disabled. See the 'Managing the SWEEP services' section of the 'Installing SWEEP' chapter for more information.

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 you are ever in doubt, contact Sophos' technical support for advice.

To decrease the chance of false positives:

- Only sweep executables.
- Perform a 'quick sweep' rather than a 'full sweep'.

New viruses

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

If a virus unknown to SWEEP is suspected, please send Sophos a sample and a description as soon as possible. If it is a virus, SWEEP must be updated as soon as possible. When the virus has been analysed (which may take from 10 minutes to a few days), we will fax or email the IDE file which can be used to update SWEEP. The latest IDE files can also be downloaded from the Sophos Web site.

Virus not disinfected

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

- Check that 'disinfect documents' is selected (see the 'Action on virus detection' section of the 'Configuring SWEEP' chapter).
- If dealing with a disk or removable media, make sure that it is not write-protected.
- If dealing with files on an NTFS volume, make sure that SWEEP has sufficient access rights.

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

See also the 'On-screen log messages' 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.

On-screen log messages

There are three categories of message that can appear in the on-screen log and the log file. The first type contains administrative messages such as the SWEEP version number, the times that jobs are started and stopped, and information about the number of viruses detected during each job. The second type occurs when a virus or virus fragment is detected and contains the virus name, where it was found, and information about the action taken. The third type alerts the user to other problems encountered during the job. This chapter describes the virus detected messages and the error messages.

Note: The italicized sections in the messages below indicate information that varies.

Virus detected messages

Double-clicking on a line with a virus name will display more information about that virus.

```
Virus:   'virus name' detected in location
         Action
```

SWEEP's 'virus detected' message contains the name and the location of the virus. The *location* will be one of either:

filename
Drive *drive name*: Sector *sector number*
Disk *disk* Cylinder *cylinder* Head *head* Sector *sector*

The *action* will depend on the settings on the Action tab of the Configuration page (see the 'Configuring SWEEP' chapter), and will be one of the following:

`No action taken`

No action will be taken if SWEEP has been configured not to disinfect boot sectors or documents, and not to rename, delete, shred, move or copy any infected files.

`File deleted`

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

`File renamed to` *`filename`*

The *filename* will be the old name with the file extender changed to a number. For example, if a virus was named VIRUS.EXE it would be renamed to VIRUS.000, or VIRUS.001 if there was already a file called VIRUS.000, and so on.

`File shredded`

The infected file has been deleted and cannot be recovered.

`File moved to` *`new location`*

The *new location* is the location specified in the Action tab of the Configuration option.

`File copied to` *`new location`*

The *new location* is the location specified in the Action tab of the Configuration option.

`Error` *`problem`*

The *problem* will be one of either:

```
deleting file
renaming to filename
```

`shredding file`
`moving to` *`location`*
`copying to` *`location`*

The file could not be deleted/renamed/shredded/moved/copied. If the infected file was found on a floppy disk, check that the disk is not write-protected.

Important! The infected file will remain unchanged and may be able to infect other disks and files.

`Has been disinfected`

SWEEP for Windows NT can automatically disinfect, or remove, certain boot sector viruses on floppy disks if the 'disinfect boot sector' option has been selected. SWEEP for DOS will be required to disinfect a hard disk boot sector. SWEEP can also automatically remove the viral macros from documents infected with certain types of macro viruses.

`Error: Disinfection failed`

SWEEP was unable to disinfect the boot sector. See the 'Treating viral infection' chapter for advice on disinfecting a boot sector.

Important! The infected disk will remain unchanged and may be able to infect other disks and files.

`Virus:` '*`virus name`*' `detected in` *`location`*
`InterCheck request at` *`time`*
`User` *`user`*
`Node` *`network address`*
`Action`

This is InterCheck's 'virus detected' message. It contains the name and location of the virus, along with the time it was discovered, the name and network address of the user who found it, and a summary of the action taken. The *`action`* depends on the settings on the Action tab on the InterCheck Configuration page (see the 'Configuring SWEEP' chapter), and will be one of either:

```
        No action taken
        File copied to new location
        Error copying to location
```

These are the same as the equivalent SWEEP 'virus found' actions.

```
Virus:  report source report:
        Message
        At time
        User user
        Node network address
```

The *report source* will be either SWEEP or InterCheck, indicating whether the report comes from the InterCheck client software or from SWEEP for DOS running on the InterCheck client machine. The *message* contains the text of the report.

```
Virus fragment: 'virus name' detected in location
        No action taken
```

The 'virus fragment detected' message contains the name and location of the virus fragment. The *location* will be one of either:

filename
Drive *drive name*: Sector *sector number*
Disk *disk* Cylinder *cylinder* Head *head* Sector *sector*

SWEEP does not remove virus fragments. See 'Virus fragment reported' in the 'Troubleshooting' chapter.

Error messages

```
Error:  InterCheck report:
        Message
        At time
        User user
        Node network address
```

This is an error reported by the InterCheck client software. The description of the error will be contained in the *message*.

```
Error:   Invalid InterCheck request received in file filename
         At time
         User user
```

If the InterCheck server receives an InterCheck request and does not recognise it as such, then it will issue this error message. If this error occurs on a regular basis there may be a fundamental problem with the InterCheck installation.

```
Error:   Corrupted InterCheck request received in file filename
         At time
         User user
```

Every InterCheck request sent from the client to the server is protected by a checksum. If the InterCheck server receives a request with a bad checksum it will issue this error message. If this error occurs on a regular basis there may be a fundamental problem with the InterCheck installation.

```
Warning: InterCheck version is newer than this version of SWEEP.
         Please upgrade this copy of SWEEP.
```

This error message arises when the InterCheck server receives an InterCheck request from a newer version of the InterCheck client than it knows about. The solution is to upgrade SWEEP.

```
Error:   Could not start InterCheck.
         Could not open InterCheck marker file filename
         At time
```

InterCheck requires read and write access to its COMMS folder (normally a subfolder of the SWEEP folder called COMMS) to be able to communicate with the InterCheck clients.

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

The file called *filename* was on the list of files to be swept, but could not be opened for examination. Check that the file is not in use or already open.

`Error: Could not read filename`

The file called *filename* was on the list of files to be swept, but could not be read. This might indicate that the file or the disk is corrupt.

`Error: Sector size of drive drive is too large`

SWEEP will only currently sweep disk sectors of 2k or less. It is highly unlikely that your machine will ever contain sectors larger than this.

`Error: Could not open report file filename/folder`

The filename and folder of the report file are specified on the Report tab of the Configuration page (see the 'Configuring SWEEP' chapter). SWEEP will not be able to open the report file if its filename is not valid, or if it does not have sufficient access rights to the folder. Note that the report file is written as the current GUI user for immediate sweeps and as the service user for scheduled sweeps.

```
Error:  Log file filename could not be opened.
        Log data will not be saved.
```

The location of the log file is specified with the *Set Log Folder* option from the *File* menu (see the 'SWEEP options' chapter). SWEEP will not be able to open the log file if it does not have sufficient access rights to the folder. Note that the log file is written as the service user and not as the GUI user.

Glossary

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

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.

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.

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

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.

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

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

Macro Virus: A virus which uses macros in a data file to become active in memory and attach itself to other data files. Unlike conventional viruses, macro viruses can be written relatively easily with little specialist knowledge, and can also attain a degree of platform independence.

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

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

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

NTFS: NT File System; the Windows NT file system.

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

Polymorphic Virus: Self-modifying encrypting virus.

SMTP: Simple Mail Transport Protocol; the delivery system for Internet email.

Trojan Horse: A computer program whose execution would result in undesired side-effects, generally unanticipated by the user.

UNC: Universal Naming Convention; a standard system for naming network drives, e.g. the UNC directory \\MAIN\USERS\ would refer to the USERS directory on the server called MAIN.

VDL: Virus Description Language; a proprietary Sophos language used to describe virus characteristics algorithmically. It has extensive facilities to cope with polymorphic viruses.

Index

L

M

N

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 plemounier@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
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 crypsys@pi.net
http://www.pi.net/~crypsys/
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 715878 · Fax 02 715894 · 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

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