Sophos Anti-Virus

User Manual

OS/2

SOPHOS

Sophos Anti-Virus

for OS/2

User Manual
March 2001

Contents

Installing Sophos Anti-Virus

Using Sophos Anti-Virus (GUI)

Using Sophos Anti-Virus (CLI)

Updating Sophos Anti-Virus

Protecting non-OS/2 workstations

Dealing with viruses

Other information

Read this first

1. Before you install Sophos Anti-Virus, follow the steps in the 'Creating an emergency disk set' chapter.
2. Choose the kind of installation you require:

   For multiple, networked OS/2 machines, follow the steps in 'Installation on a network'.

   For a single OS/2 computer, follow the steps in 'Installation on a single machine'.
3. This manual describes how to use Sophos Anti-Virus for OS/2 via two different interfaces.

   If using the **Graphical User Interface (GUI)**, read the 'Using Sophos Anti-Virus (GUI)' chapters shown in the contents list.

   If using the **Command Line Interface (CLI)**, read the 'Using Sophos Anti-Virus (CLI)' chapters shown in the contents list.
4. This manual also describes how to use Sophos Anti-Virus to provide scanning and central virus reporting for any non-OS/2 machines on the network.

   See the 'Protecting non-OS/2 workstations' chapters shown in the contents list.

About Sophos Anti-Virus

This chapter introduces Sophos Anti-Virus and describes its key features.

What is Sophos Anti-Virus?

Sophos Anti-Virus offers on-demand, scheduled and on-access virus checking, automatic reporting and disinfection for individual PCs and entire networks.

How does it work?

Sophos Anti-Virus divides virus checking between two components:

- **SWEEP** provides immediate and scheduled scanning of all disks, files and documents, and
- **InterCheck** checks each item as you try to access it, and grants access only if it is virus-free.

About Sophos Anti-Virus for OS/2

Sophos Anti-Virus for OS/2 can check OS/2 machines for DOS, OS/2, Windows and macro viruses. It can be used:

- From the Graphical User Interface (GUI).
- From the command line.

Whichever is used, the functionality is the same.

Sophos Anti-Virus for OS/2 can also be used as an InterCheck Server. This can provide server based virus reporting and on-access scanning (InterCheck) for non-OS/2 client workstations.

About InterCheck

InterCheck ensures that unknown items (e.g. programs, documents, email attachments or internet downloads) cannot be used until checked for viruses.

Important! InterCheck can be run on most workstations, but not currently on OS/2.

How does InterCheck work?

InterCheck splits the task of file authorisation into two processes:

Monitoring all file and disk accesses

Whenever a user attempts to access an item, InterCheck compares it with a list of authorised items. If a match is found, access is permitted; if not, the item is scanned for viruses.

Scanning unknown items

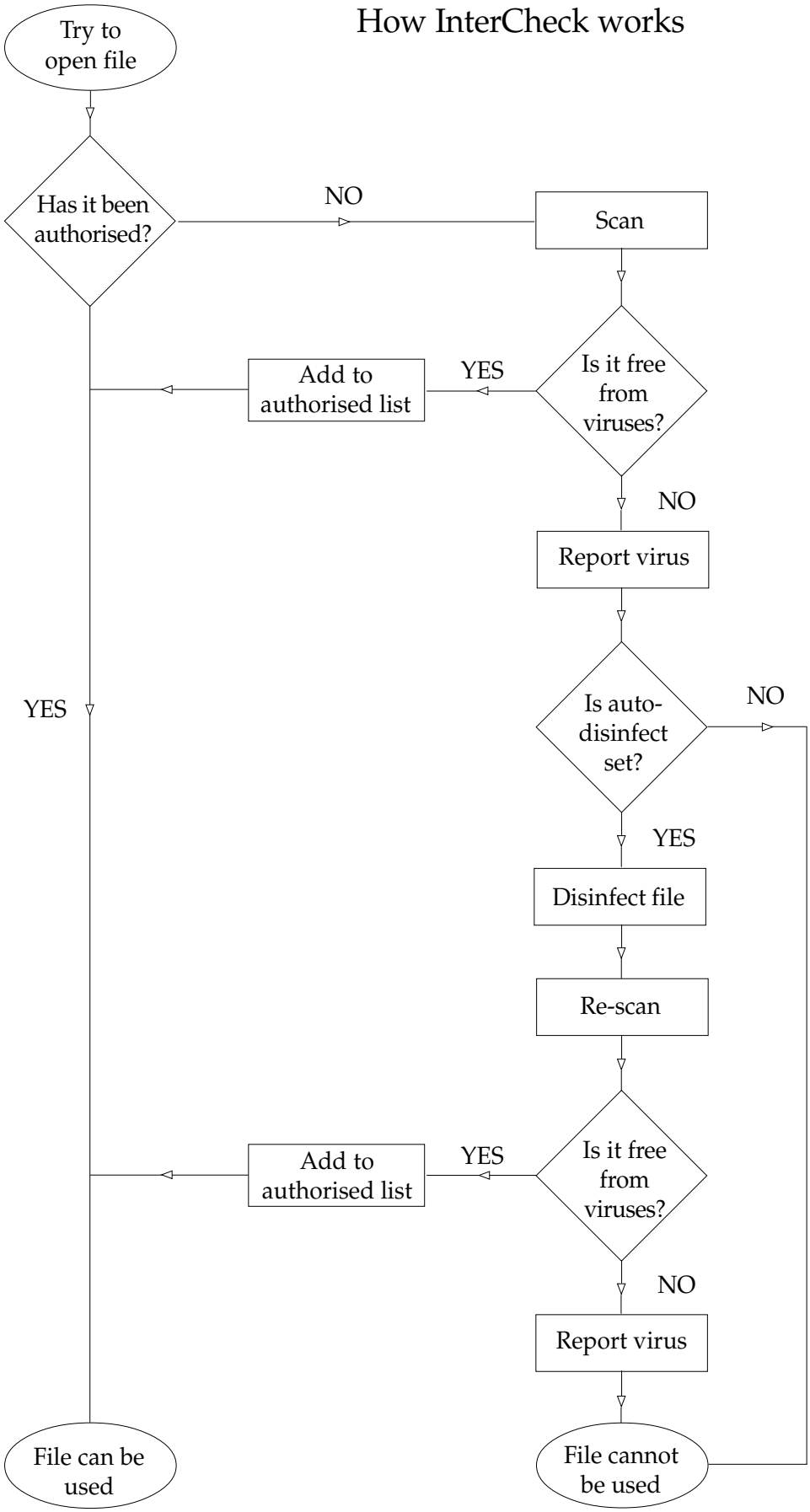
InterCheck sends any unknown item for scanning.

If the item is virus-free, it is added to the list of authorised items (checksum file) and access is granted. Unless the item is modified, users can subsequently access it without further authorisation.

If a virus is found, InterCheck reports the virus and denies access. However, if automatic disinfection* has been set up, any item that can be disinfected (documents or floppy disk boot sectors) is cleaned and scanned again. If the item is now virus-free, access can go ahead.

* Automatic disinfection is not available for all platforms.

How InterCheck works



Creating an emergency disk set

This chapter describes how to create a set of emergency disks. You will need these if ever you have to disinfect computers manually.

Creating emergency disks

You should create:

- An OS/2 Utility disk set.
- Emergency SWEEP disks.

Note: Some versions of the OS/2 documentation refer to the Utility disks as Startup diskettes.

You can find instructions on how to make an OS/2 Utility disk set in the OS/2 documentation. You should reserve a set to form part of your emergency kit.

You create emergency SWEEP disks by using the special disk creation program supplied.

Make sure that all source disks are virus-free and that all disks are created on a virus-free machine.

Preparation

To make an OS/2 emergency disk set you need:

1. A Sophos Anti-Virus CD.
2. An OS/2 Utility floppy disk set.
3. Three blank (or reusable) floppy disks. They will be reformatted if necessary.

Write-protect your OS/2 and Sophos Anti-Virus floppy disks before starting.

Extracting the disk creation program

First you extract the disk creation program from an archive on the Sophos Anti-Virus CD.

Note: If the OS/2 computer has no CD drive, follow the steps in 'Appendix: Making floppy disk sets'. Then go to 'Running the disk creation program' below.

Insert the Sophos Anti-Virus CD in an OS/2 computer.

Change to a directory on the hard disk where you can make a temporary sub-directory. For example:

```
C:
cd\temp
```

Enter

```
F:\diskimgs\esdos2
```

where F: is the CD drive.

Running the disk creation program

This creates a sub-directory called esdos2. Change to this directory

```
cd esdos2
```

Then enter

```
mkstand -U:A -T:A
```

Creating an 'Emergency OSWEEP' disk

The computer prompts you for one of the OS/2 Utility disks. Insert the relevant disk and press *Enter*.

After a few more seconds the computer asks for a target floppy disk. Insert the first target floppy disk and press *Enter*. If the disk is not blank you are asked if you want to continue. Enter *Y* to format it first.

When the disk has been written, remove it from the drive and label it 'Emergency OSWEEP'. Press *Enter*.

Creating 'Emergency Virus Data' disks

The computer prompts you to place the second target floppy disk in drive A:.

Insert the second blank disk and press *Enter*. If the floppy is not blank, you are asked if you want to clear it. The virus data is then written to the disk.

When finished remove it from the drive and label it 'Emergency Virus Data Disk 1 of 2'. Press *Enter*.

The computer prompts you to insert the third target floppy disk in drive A:.

Insert the disk and press *Enter*.

When the data has been copied, remove the disk and label it 'Emergency Virus Data Disk 2 of 2'. Press *Enter*.

The computer announces the completion of the disk generation process.

Checking the new emergency disks

You are now asked if you want to scan the newly created disks. Sophos recommends that you do so. Enter *Y* and insert the disks when prompted. When all the disks have been checked, press *Esc*.

When your disks have been scanned, write-protect them and place them, together with the clean OS/2 Utility disk set, in a secure place.

Emergency disk creation qualifiers

For all processes the relevant command qualifiers are:

-P	Update SWEEP files on existing emergency floppy disks.
-T:x	Use drive x for target disks.
-U:x	Use drive x for OS/2 Utility disks.
-?	Help text.

Installation on a network

This chapter describes how to use a 'central installation' to install Sophos Anti-Virus for OS/2 across a network.

For details of how to provide central reporting and on-access scanning for non-OS/2 clients, see 'Installing an OS/2 InterCheck Server'.

Before installation

Before you install Sophos Anti-Virus, you should prepare emergency disks. See the 'Creating an emergency disk set' chapter.

About central installation

You install Sophos Anti-Virus on multiple OS/2 computers as follows:

1. Install the setup files in a central location, e.g. the OS/2 server, and add the latest virus identities.
2. Install Sophos Anti-Virus on the workstations by running the setup program from these central files.

Central installation

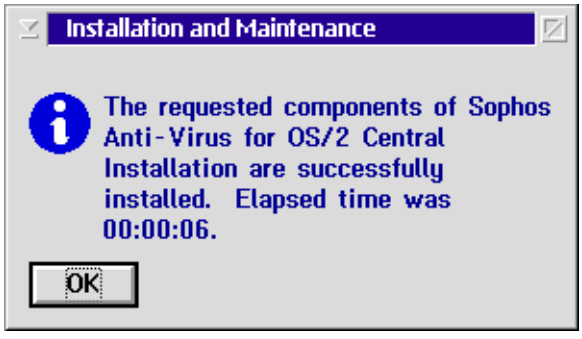
Insert the Sophos Anti-Virus CD in the server. At a command prompt, enter:

```
F:\OS_2\SETUP -CENTRAL -INSTPATH=C:\SAVCID
```

if F: is the CD drive and C:\SAVCID is the directory where the installation will be made.

Note: If the OS/2 server has no CD drive, follow the steps in 'Appendix: Making floppy disk sets' and then run the copy of SETUP on the server.

Click *OK*. Setup makes an installation to the OS2INST folder in the central installation directory. When file copying is complete, you see the screen below.



A message appears in the command window

```
Creating central configuration ...
```

When the central configuration has been completed, the message changes to

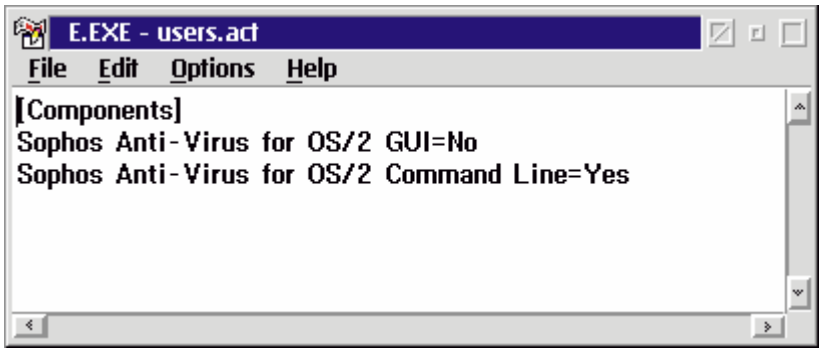
```
Creating central configuration ... Done.
```

Now you may need to modify the central installation files, depending on which version of Sophos Anti-Virus you want to install on workstations later.

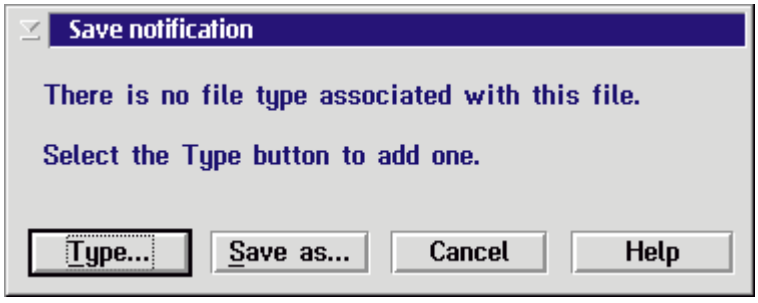
If you want the command-line version, you do not need to make any changes.

If you want the GUI (Graphical User Interface) version, go to the central installation directory and open the action file USERS.ACT with the 'E' text editor

```
C:
CD \SAVCID\OS2INST
E USERS.ACT
```



In the second line, change No to Yes. Then select **File | Save**.



Click the **Type ...** button.

Select Plain Text. Click Set.

If you install the command-line version, you can use the procedure above to upgrade to the GUI version at any time.

Next we recommend that you create an alias for the central installation directory if you can (only the domain administrator can do so).

For instance, at the command prompt, enter

```
NET ALIAS SAVCID \\<Servername> C:\SAVCID\OS2INST
```

where

SAVCID is the alias name

<Servername> is the server

C:\SAVCID\OS2INST is the directory to be aliased.

If you have an internet connection, you should now download the latest virus identities from the Sophos website.

If you do not have an internet connection, go straight to the 'Workstation installation' section.

Adding the latest virus identities

If you have an internet connection, you should download the latest virus identities (IDE files). These protect you against virus threats that have appeared since the current version of Sophos Anti-Virus was compiled.

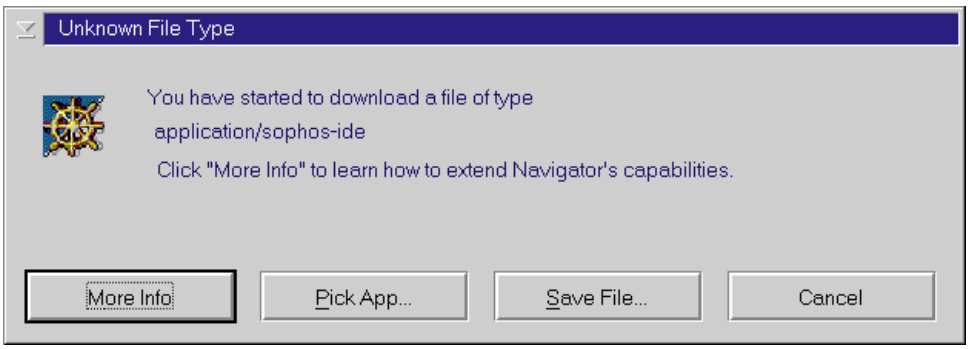
Go to the Sophos website, www.sophos.com.

Look in the Downloads menu and select Latest virus identities (www.sophos.com/downloads/ide).

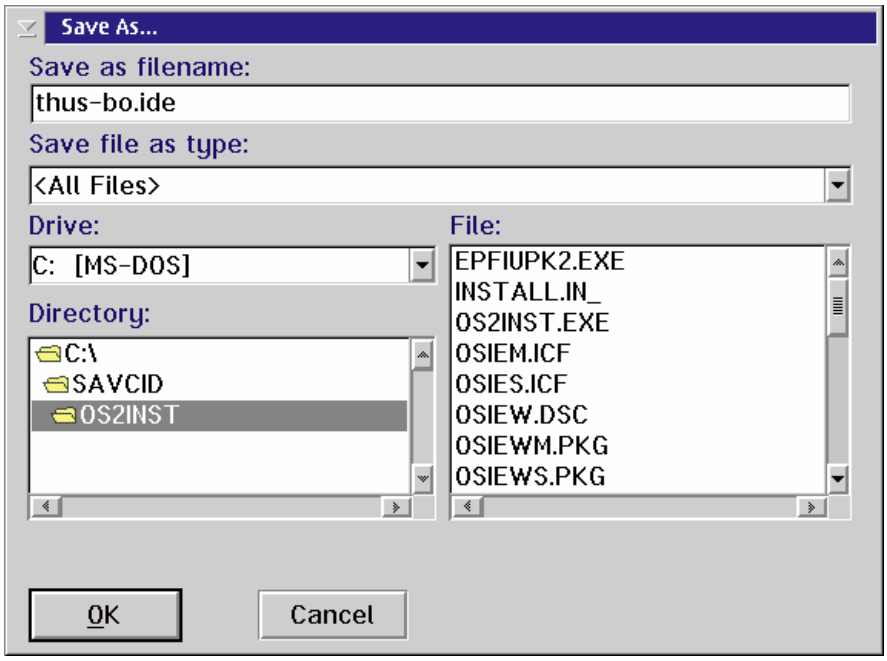
You can download IDE files one at a time or, if you have an unzip program on your computer, all at once.

To download each file individually, go to the list of IDE files and click on the filename in the Download column.

You will see the screen below.



Click *Save File.*



Save the file in the central installation directory, C:\SAVCID\OS2INST. Click *OK.*

To download all the files at once, click *Download Zip*. Save the Zip file to your hard disk. Then unzip the IDE files to the C:\SAVCID\OS2INST folder.

Now you install Sophos Anti-Virus on the workstations.

Workstation installation

To install Sophos Anti-Virus on workstations, you run the setup program from the central installation directory (CID). The easiest way to do this is to place a command in the workstations' login script.

In the login script, enter a line to map a drive:

```
NET USE S: SAVCID
```

You should always map the same drive to the CID. This is because each workstation stores the path and will look for updates under the drive letter first used.

Then enter a setup command like this:

```
S:\SETUP -A -START -COE
```

This will run setup from the CID automatically.

At a random time, between ten minutes and one hour after the script runs, Sophos Anti-Virus will be installed to C:\SAV on the workstation and (if the GUI is installed) will be started automatically.

Setup activity will be logged in SAVSETUP.LOG in \OS2\INSTALL on the drive from which OS/2 was started (usually C:) .

You can use further parameters to specify the source or destination files and the timing of installation or updating. For details, see the 'SETUP command line qualifiers' section.

Note: You can also use this command to update a workstation with an existing, manual installation of Sophos Anti-Virus. Any -INSTPATH qualifier is overridden by the existing directory.

SETUP command line qualifiers

You can prefix all qualifiers with a hyphen or a slash.

For help, use the -?, -H or -HELP qualifier.

There are qualifiers to specify:

- Installation type.
- Source and target directories.
- Scheduling of installation and CID-locking.
- Removal of Sophos Anti-Virus.
- Error messages and reporting.

Installation type

-A or -AUTO

Perform an automatic installation or update from a central installation directory.

-ACTION

Specify the 'action file' used when installing or updating Sophos Anti-Virus on workstations from a central installation. This is a text file which determines which components of Sophos Anti-Virus are installed (GUI or command-line version only).

The default action file created during central installation is USERS.ACT in the central installation directory (CID). It contains the lines

```
[Components]
Sophos Anti-Virus for OS/2 GUI=No
Sophos Anti-Virus for OS/2 Command Line=Yes
```

Change No to Yes in the second line to ensure that the GUI will be installed.

Enter No in both lines if you want to have Sophos Anti-Virus removed from workstations.

The -ACTION qualifier lets you make different kinds of installations for different users. When you put the SETUP command in users' login scripts, simply use a different -ACTION value for different users.

-CENTRAL

Perform the operation on the central installation directory (CID) instead of the workstation. By default, this creates or updates the CID.

-CLOSE

Close the currently running background (automatic) setup program.

-UPDATE

Marks the central installation directory (CID) as updated, so that workstations will update from it.

You should run SETUP with this qualifier in the CID when IDE (virus identity) files are added to it. See 'Updating Sophos Anti-Virus with new virus identities' in the 'Updating a network' chapter.

You should not use this qualifier when updating the CID using the -CENTRAL qualifier.

-FULL

The -FULL qualifier is used when updating the central installation directory with virus data files other than IDE files, e.g. a new VDL.DAT.

-FULL recreates the central installation directory's configuration file, SWEEPOS2.CFG. This ensures that the configuration file accurately reflects the contents of the CID, and that workstations will transfer precisely the files needed to update them. -FULL can be used only with -UPDATE.

See 'Updating Sophos Anti-Virus with new virus identities' in the 'Updating a network' chapter.

-START

If Sophos Anti-Virus is running when an update is performed, it is stopped. When updating is complete, Sophos Anti-Virus is restarted. If -START is used, Sophos Anti-Virus will be started even if it was not running before.

Source and target directories

-SRCPATH=directory

Specifies the source directory, i.e. the directory containing the files to be installed. When updating from a central installation directory (CID), the CID already used will be the source directory. Otherwise, the default is the directory from which SETUP is run.

-INSTPATH=directory

Specifies the directory to which files are to be installed. This applies to new installations, not to updates. The default directory for a workstation installation is C:\SAV.

Scheduling and CID locking

-MINDELAY=n

Sets the minimum delay for an automatic install or update to n minutes. The install or update will take place at a random time between the minimum and maximum delay times (see -MAXDELAY).

The default is 10 minutes.

-MAXDELAY=n

Sets the maximum delay for an automatic install or update to n minutes. The install or update will take place at a random time between the minimum delay time (see -MINDELAY) and the maximum delay time. The random time is different on each workstation in order to spread the network load of updating.

The default is 60 minutes.

-PERIOD=n

SETUP locks the CID when updating it or using it to update workstations. If a lock cannot be placed immediately, SETUP retries at random intervals. This qualifier sets the maximum interval to n minutes. The default is 1 minute.

-TIMEOUT=n

SETUP locks the central installation directory (CID) when updating it or using it to update workstations. If a lock cannot be placed immediately, SETUP retries repeatedly until it times out. This qualifer sets the timeout to n minutes. The default is 10 minutes. See also -PERIOD.

-ONCE

Only attempt an automatic installation or update once. Unless this qualifier is used, SETUP will repeatedly check the central installation directory to see whether a further update is needed.

-LOCKLIMIT=n

Sets the maximum period for which SETUP can lock the central installation directory. Zero means no limit. The default is 20 minutes.

Removal of Sophos Anti-Virus

-REMOVE

Remove the product. The product removed is the workstation installation of Sophos Anti-Virus unless the -CENTRAL qualifer is used.

-CLEAR

If Sophos Anti-Virus for OS/2 files are deleted, SETUP -REMOVE can fail. The program will warn that the product cannot be deleted because it is not installed. Settings can then be left in the user profile. SETUP -REMOVE -CLEAR clears these settings. SETUP -CENTRAL -REMOVE -CLEAR clears the settings for a central installation.

You will have to delete Workplace Shell objects (the icons and the entry in Startup which starts SWEEP on system start) manually if they remain after removing Sophos Anti-Virus. See the OS/2 documentation for instructions.

Error messages and reporting

-LOG=filename

Specifies a file that SETUP will use to log messages. The default is SAVSETUP.LOG in \OS2\INSTALL on the drive from which OS/2 was started (usually C:) .

-LOGLVL=<Error level>

Sets the level of error and other messages written to the log file. See the 'Error levels' section for details.

The default setting is WARNING, which means that minor problems that do not stop updating, as well as more serious errors, are written to the log file.

-REPORTER=filename

Specifies a command file to be used for reporting errors. This is useful for automatic updates, which display no errors on screen. The command file would usually e-mail a message to a system administrator.

There are seven parameters:

%1 Machine name (%HOSTNAME% or else "Unknown")
%2 Date
%3 Time
%4 Message
%5 SETUP log file
%6 Installer error log file
%7 Installer history log file

-REPLVL=<Error level>

Sets the level of error and other messages reported by a program called with the -REPORTER qualifier. See the 'Error levels' section for details.

The default is CORRECTED, which means that corrected, uncorrected and fatal errors are reported.

-DMY

If an error-reporting command is used (see -REPORTER), the date will be passed to it in the format dd/mm/yyyy.

-MDY

If an error-reporting command is used (see -REPORTER), the date will be passed to it in the format mm/dd/yyyy.

-YMD

If an error-reporting command is used (see -REPORTER), the date will be passed to it in the format yyyy/mm/dd.

-DISPLVL=<Error level>

Sets the level of error and other messages to be displayed on screen. See the 'Error levels' section for details. The default setting is ERROR, which means that errors that can make an operation fail and more serious errors are displayed.

-ERRLOG=filename

Specifies the filename of the Installer's error-logging file.

-HISTLOG=filename

Specifies the filename of the Installer's history-logging file.

-COE or -CONTERR

Continue on error. An automatic installation or update will continue running even if an error occurs (unless you use the -ONCE qualifier).

Error levels

This section lists the different levels of error messages and the methods used for reporting.

Error levels

Error messages and other messages are classified by level. There are five levels. In increasing order of severity, these are as follows:

INFO	Information. No action required.
WARNING	A small problem was detected but SETUP was able to continue.
CORRECTED	An error was detected but has been corrected, at least for the current operation. The condition causing the error requires attention.
ERROR	The operation (install, update or remove) may not have been completed successfully.
FATAL	The operation has not been completed successfully. SETUP could not continue running, even if -COE (continue on error) was specified.

Reporting methods

Errors are reported in three ways.

On screen

If the SETUP information file can be found, the appropriate page is displayed. Otherwise, a text message appears on screen. No messages are displayed in automatic mode.

In a log file

You can use the -LOGLVL qualifier to set the level of messages that will be logged. The default is WARNING.

By calling a reporting program

You can use the -REPORTER qualifier to specify a program to report errors.

You can set the level of messages reported by using the -REPLVL qualifier. The default is CORRECTED.

Installation on a single machine

This chapter describes how to install SWEEP, the on-demand component of Sophos Anti-Virus, on a single machine.

For details of how to provide central reporting and on-access scanning for non-OS/2 clients, see 'Installing an OS/2 InterCheck Server'.

System requirements

- OS/2 Warp 3 or later.
- 4 Mb hard disk space (CLI version).

  6 Mb hard disk space (GUI version).

If intending to use InterCheck on-access scanning:

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

Before installation

Before you install Sophos Anti-Virus, you should prepare emergency disks. See the 'Creating an emergency disk set' chapter.

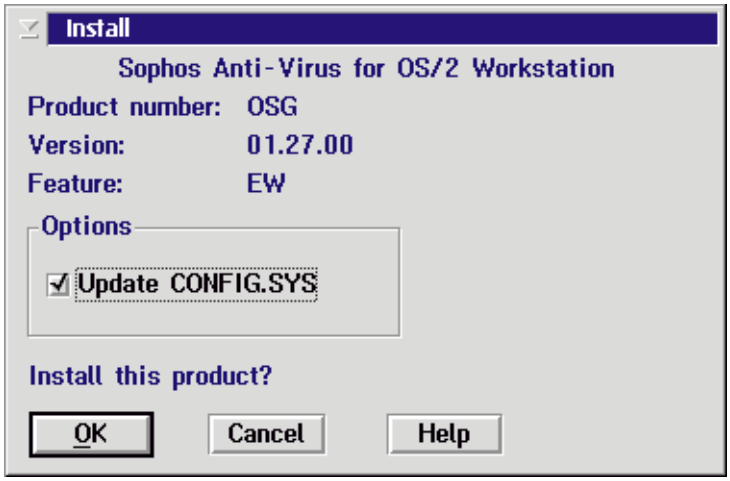
Installation

Insert the Sophos Anti-Virus CD into the disk drive. Open an OS/2 command prompt and enter

```
F:\OS_2\INSTALL
```

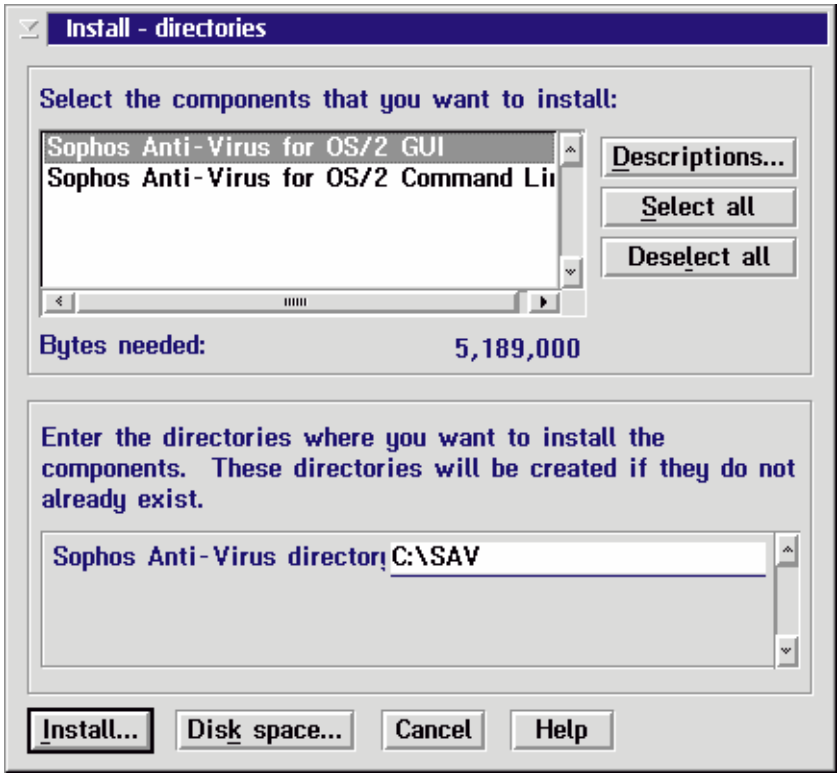
where `F:` is the CD-ROM drive.

Note: If the computer has no CD drive, follow the steps in 'Appendix: Making floppy disk sets' and then run the copy of INSTALL on the hard disk.



By default, the configuration file CONFIG.SYS will be updated. If the 'Update CONFIG.SYS' option is deselected, a trial version of the configuration file is created instead. Click *OK* to proceed.

Next you choose which version of Sophos Anti-Virus to install.



Select 'Sophos Anti-Virus for OS/2 GUI' to install SWEEP with the Graphical User Interface. If you do this, you can also use SWEEP from the command line.

Select 'Sophos Anti-Virus for OS/2 Command Line' to install the command-line version only. If you do this, you can easily upgrade to the GUI version later.

Note: You can click on *Disk space* to check how much space is available on local drives.

Then enter the directory where SWEEP will be installed, e.g. `C:\SAV`.

Finally, click *Install*.

Restart the machine when prompted. The Sophos Anti-Virus folder appears on the desktop.

If you have an internet connection, download the latest virus identities from the Sophos website (www.sophos.com/downloads/ide) and place them in the directory where SWEEP was installed.

Using Sophos Anti-Virus

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

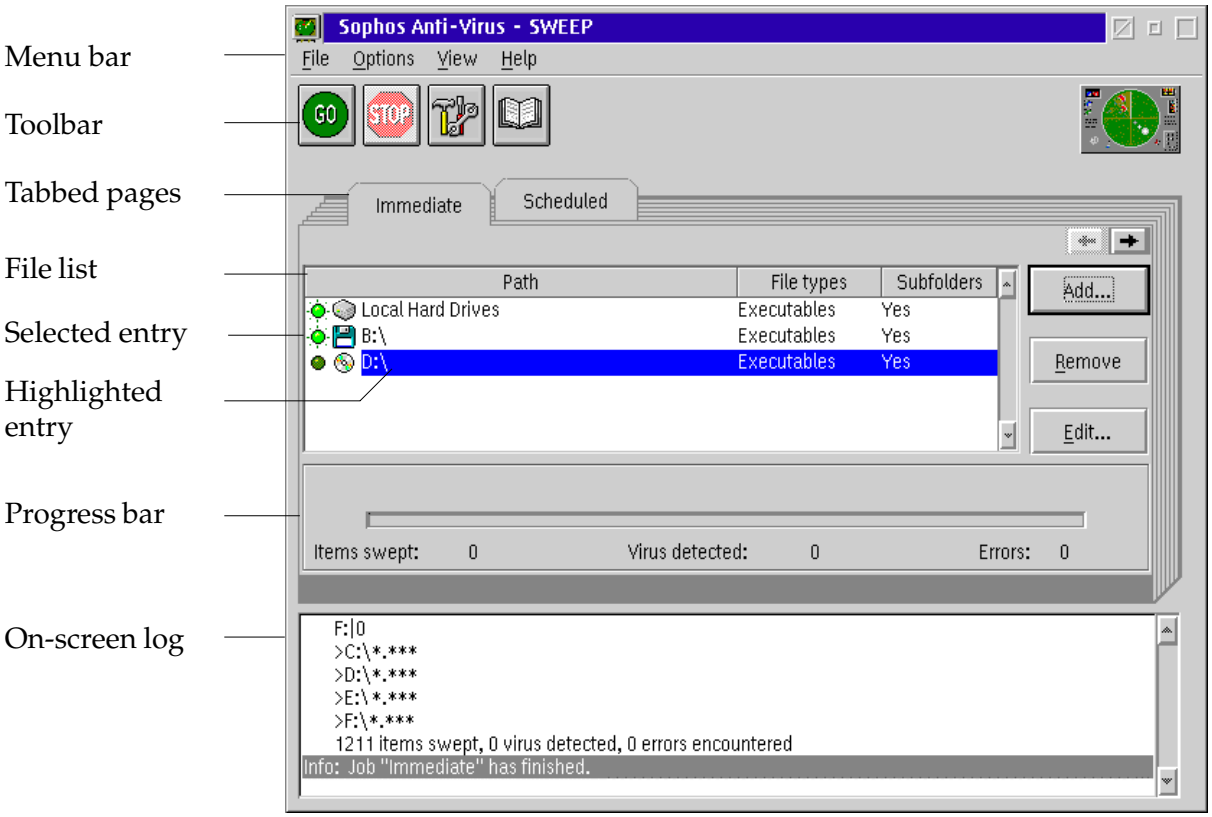
Starting SWEEP

To start SWEEP, locate the Sophos Anti-Virus folder on the desktop and open it.

This displays the Sophos Anti-Virus icons. To open the Sophos Anti-Virus window, from which scans can be run, double-click on the icon below.

Note: To scan the machine immediately, click on the 'Scan this computer with Sophos Anti-Virus' icon.

Overview of the Sophos Anti-Virus display



At the 'Sophos Anti-Virus - SWEEP' screen, you can run immediate or scheduled scans, configure Sophos Anti-Virus and find information about viruses.

Icon toolbar

The icons provide short-cuts to commonly used menu options.

Starts scanning.

Interrupts scanning.

Lets you configure the immediate or scheduled job.

Displays the virus library.

Tabbed pages

There is a tabbed page for each scanning mode:

Immediate for scanning on demand.

Scheduled for scanning automatically at set times.

Path list

On the Immediate mode page, the path list shows items that can be scanned. An illuminated light to the left of an entry indicates selected entries. Toggle this light to select or deselect items.

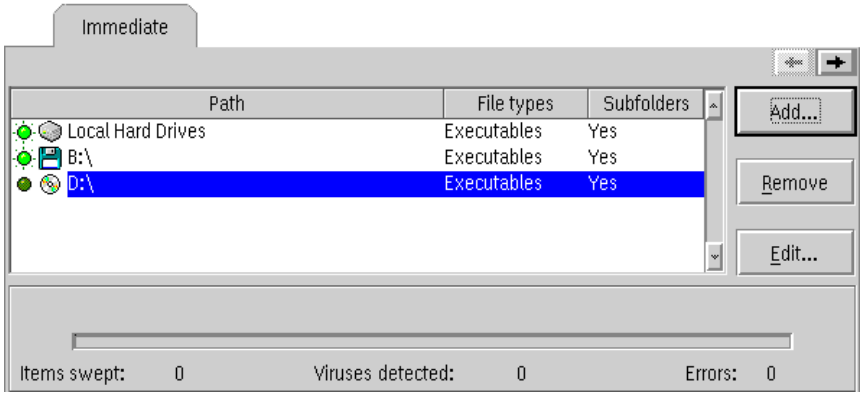
On the Scheduled page, this is replaced by the scheduled job list.

On-screen log

This contains information about the current session, along with all log messages since SWEEP was started. Double-clicking on a virus name here displays details of the virus and how to deal with it.

Immediate scanning

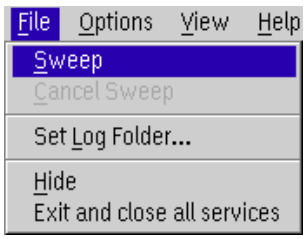
The immediate mode page is displayed on start-up. To view it at other times, click on the Immediate tab.



The path list shows the drives, paths and files that can be scanned on demand. An illuminated light to the left of an entry indicates selected entries. Toggle this light to select or deselect items.

Starting an immediate scan

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



Alternatively, click the *GO* icon.

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

Stopping a scan

To stop scanning at any time, click the *STOP* icon.

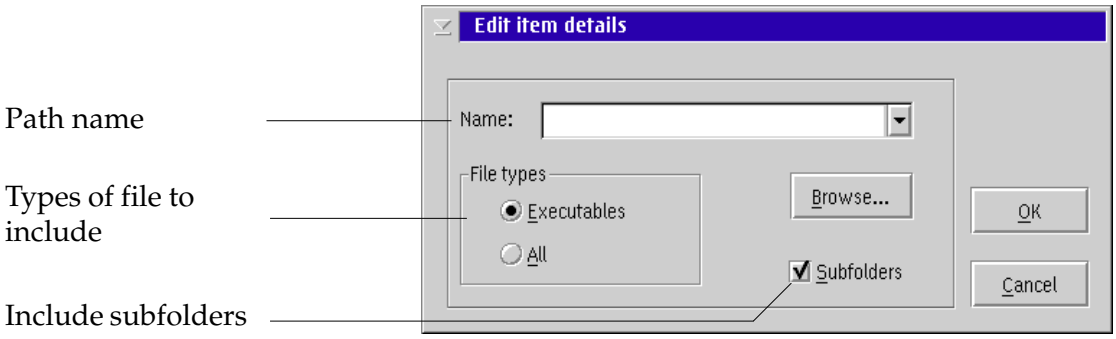
Default immediate mode file list

By default, local hard drives are displayed on the immediate mode page and marked as selected.

See the 'Configuring Sophos Anti-Virus' chapter for information on immediate mode configuration settings.

Adding new items for immediate scanning

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



Path name

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

File types

Only those files defined as executables will be scanned, unless 'All' is selected. See the 'Executables' section of the 'Further options' chapter for information on changing the files defined as executables.

Subfolders

Subfolders will be scanned if this option is selected.

Editing an item for immediate scanning

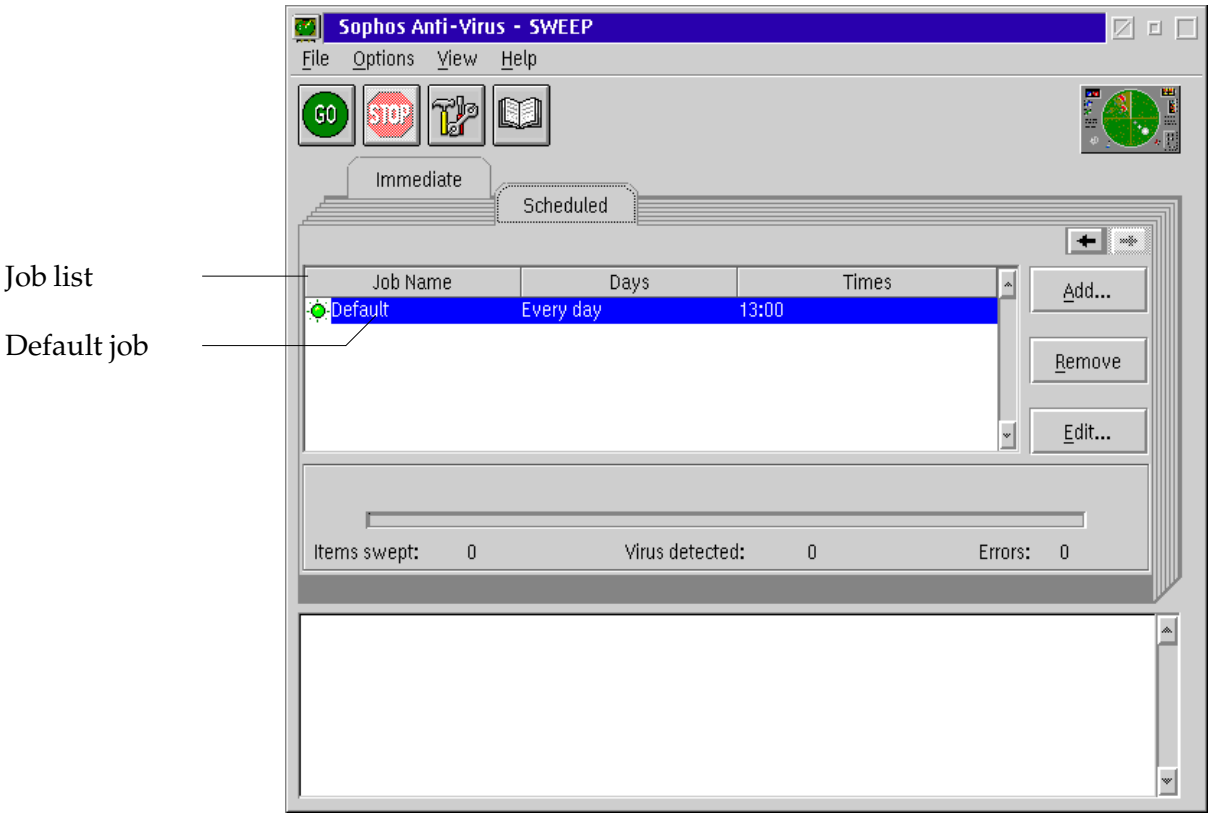
To edit an entry in the path list, highlight the name of the path to be edited and click *Edit*. This will display the item details dialog, as described in the 'Adding new items for immediate scanning' section above.

Removing items from immediate scanning

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

Scheduled scanning

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

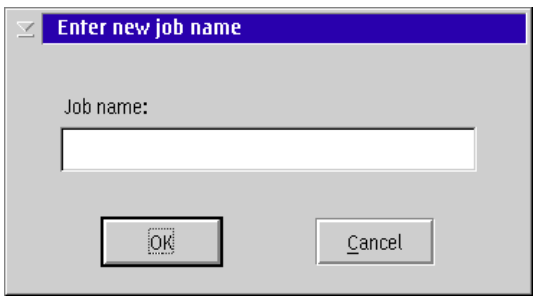


Default scheduled job list

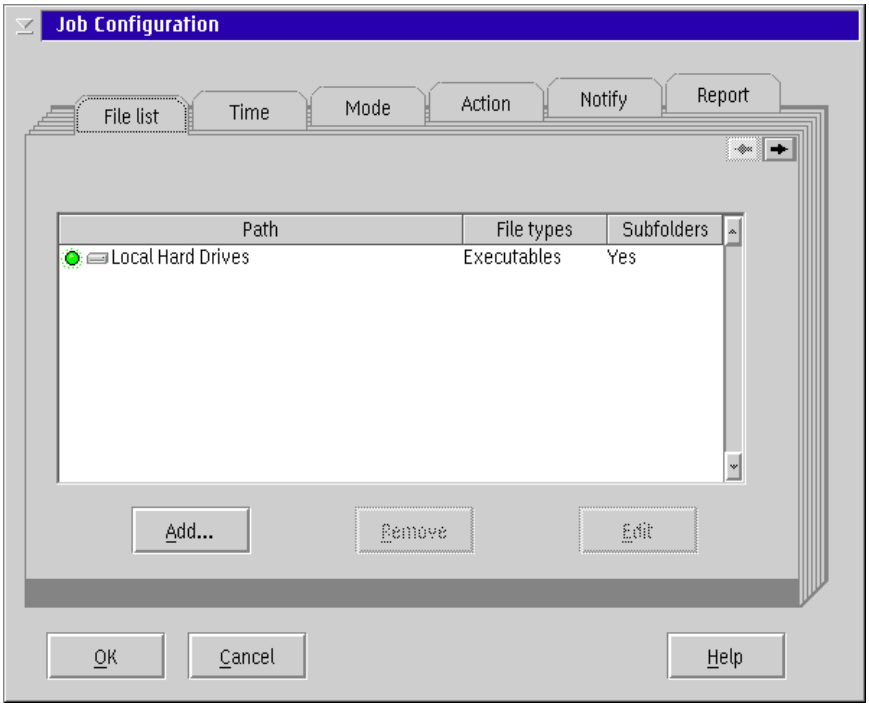
By default, a job named 'Default' is created, which is configured to scan all local hard drives. See below for details of how to modify or remove this job.

Adding a new scheduled job

To add a new scheduled job, click *Add* on the scheduled mode page. SWEEP prompts for a job name.



The job configuration pages will then appear.



Specify the items to be scanned at the File list tabbed page, and then the scanning times at the Time tabbed page. Click *OK* to accept the settings for the new job. See the 'Configuring Sophos Anti-Virus' chapter for more information on the scheduled mode configuration settings.

Editing a scheduled job

Highlight the name of the job to be edited and click *Edit*, or double-click on the job's entry. This will display the job configuration pages as described in the 'Adding a new scheduled job' section above.

Removing a scheduled job

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

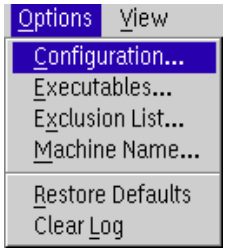
Configuring Sophos Anti-Virus

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

About configuration

To display the job configuration pages for the immediate mode or for a highlighted job in the scheduled job list:

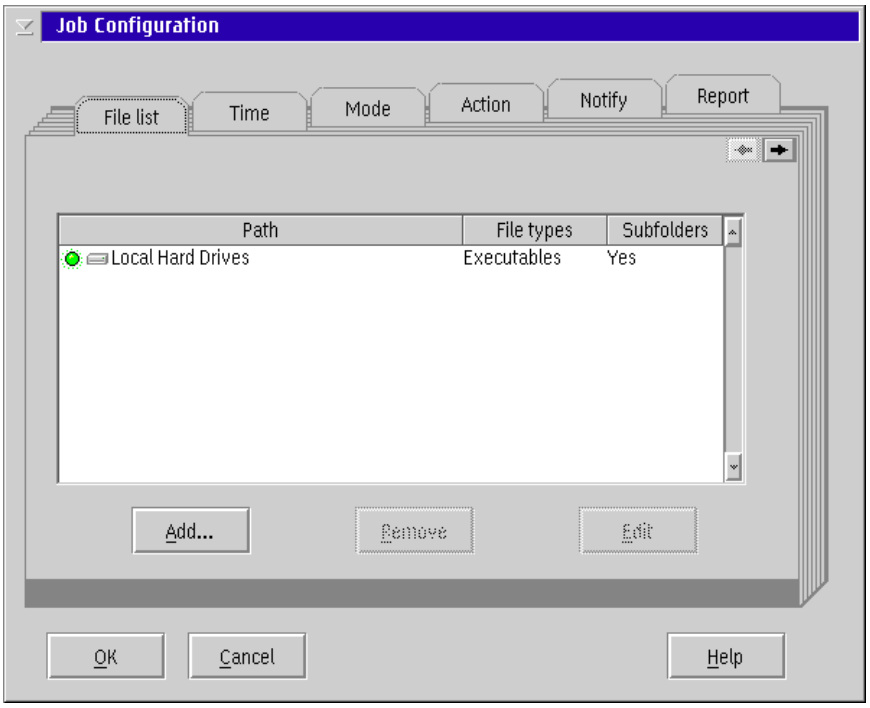
Select *Configuration* from the *Options* menu.



Alternatively, click the configuration icon.

Note: Some configuration pages apply to scheduled jobs only.

File list (scheduled mode only)



The File list page is used to specify the items to be included in scheduled scans.

It is used in the same way as the file list window in the immediate mode page.

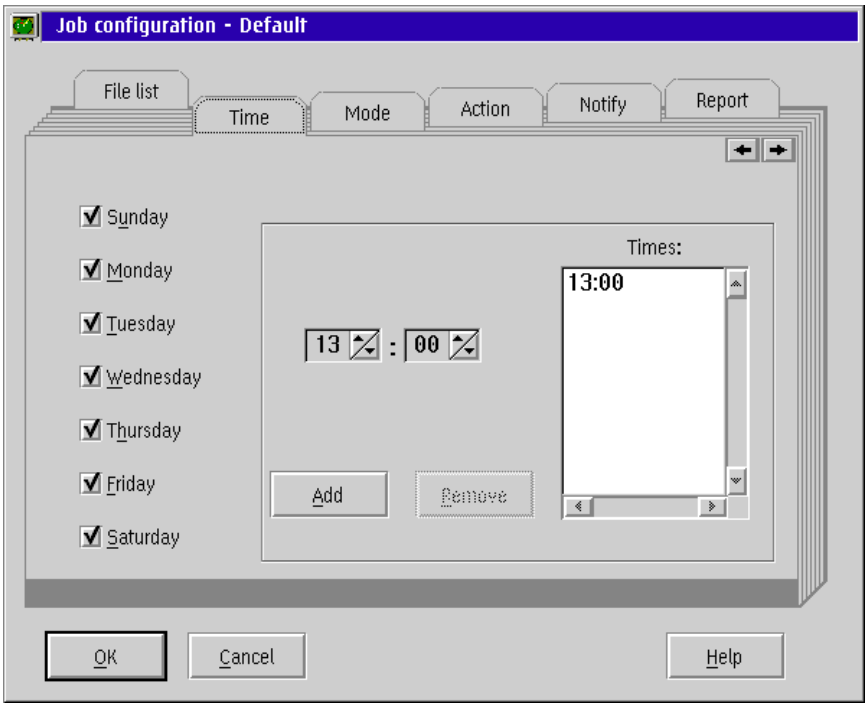
To add items to the list, click *Add* and specify an item or items in the item details dialog.

To remove an item, highlight it and click *Remove*.

To edit an item, double-click on it, or highlight it and click *Edit*, and specify the settings in the item details dialog.

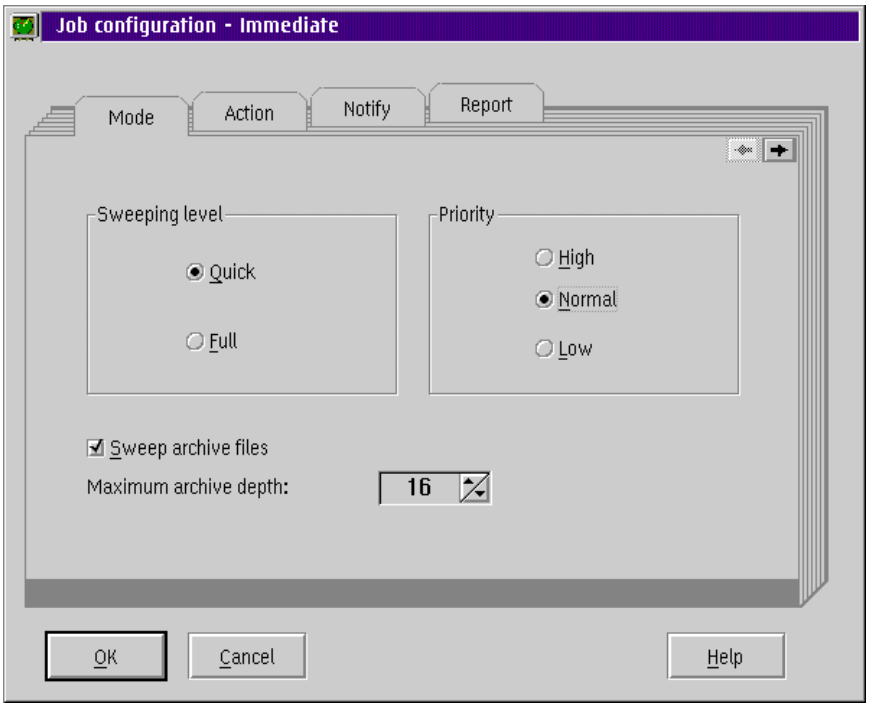
Note: The 'Path', 'File types' and 'Subfolders' settings are described in the 'Adding new items for immediate scanning' sub-section of the 'Immediate scanning' section of the 'Using Sophos Anti-Virus' chapter.

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.

Mode



Sweeping level

The 'Quick' sweeping level checks only the parts of a file likely to contain viruses, and is sufficient for normal operation.

The 'Full' level examines the complete contents of each file. It is more secure because it can discover viruses 'buried' under other code appended to a file, as well as minor virus mutations and corruptions. However, it is much slower than 'Quick' operation.

Priority

'High' priority gives SWEEP precedence over any other applications being run.

'Normal' priority gives SWEEP the same priority as other applications.

'Low' priority reduces the impact on system performance by ensuring that SWEEP will perform scans only when the system is otherwise idle.

Sweep archive files

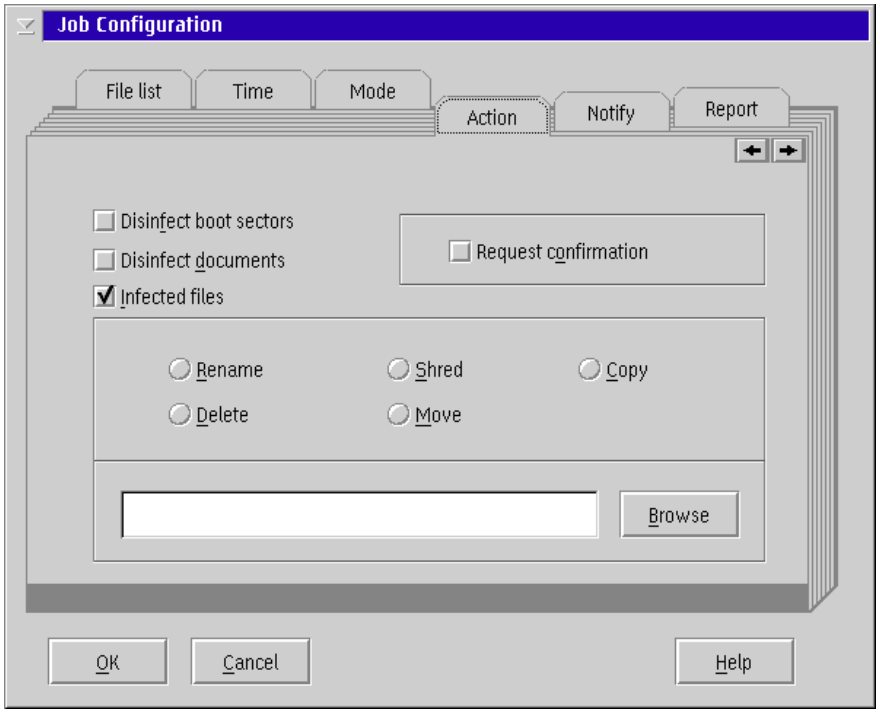
Select this option if you want SWEEP to look for viruses inside archive files.

The archive types that can be checked include: ZIP, ARJ, RAR, UUE, GZIP, TAR, CMZ. See the readme file for the latest details.

SWEEP can also check archive files 'nested' within archive files. Use 'Maximum archive depth' to set the number of levels of nested files (between 0 and 32) which SWEEP will check. The default is 16.

Note: Sophos Anti-Virus will not recognise archives which are nested to a greater depth than the maximum set here and will not check inside them.

Action



Disinfect boot sectors

SWEEP can disinfect boot sectors on floppy and hard disks automatically. Note that a hard disk can not be disinfected if any files on it are active. If disinfection of a hard disk fails, follow the instructions for manual disinfection in the 'Treating viral infection' chapter.

Disinfect documents

SWEEP can remove the viral macros from documents infected with certain types of macro virus.

If disinfection fails, the infected file will be dealt with in the same way as any other infected file (see 'Infected files' below).

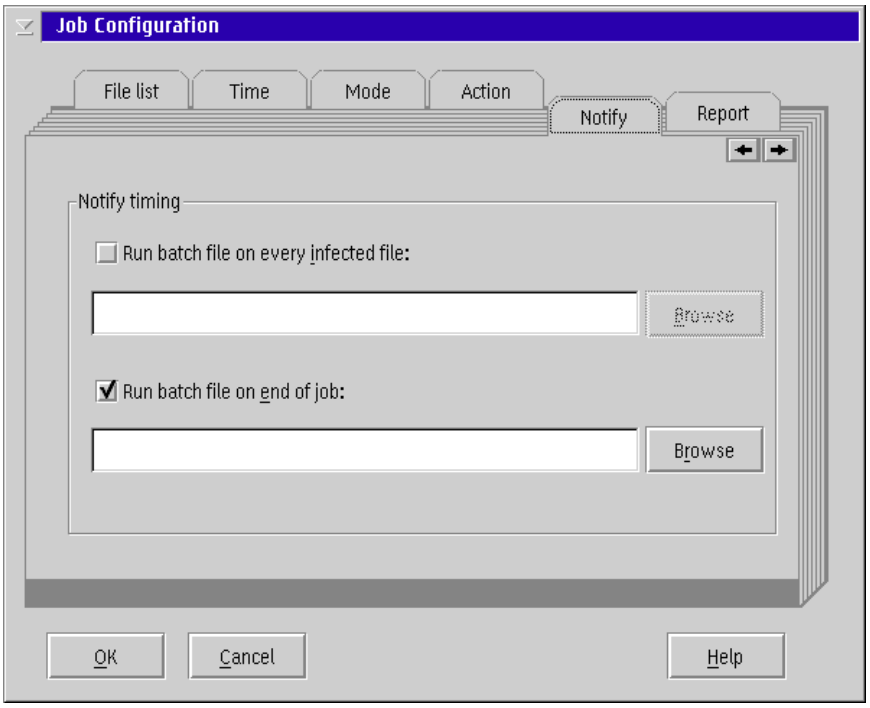
Infected files

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

Request confirmation

If this is selected, SWEEP will ask the user to confirm that it should take action on any infected items it may find. The request is made before each immediate scan. This option is not available for scheduled jobs.

Notify



SWEEP can notify users of virus finds. To do this, it runs a batch file **after each infected item is found** or **at the end of the job** in which the viruses are found**,** or both. There are separate batch files for the two forms of notification.

To create these file(s), open a text editor and create a batch file.

The following parameters can be used in the first batch file (run after each infected item):

%1 machine name
%2 job name
%3 virus name
%4 location

The following parameters can be used in the second batch file (run at the end of the job):

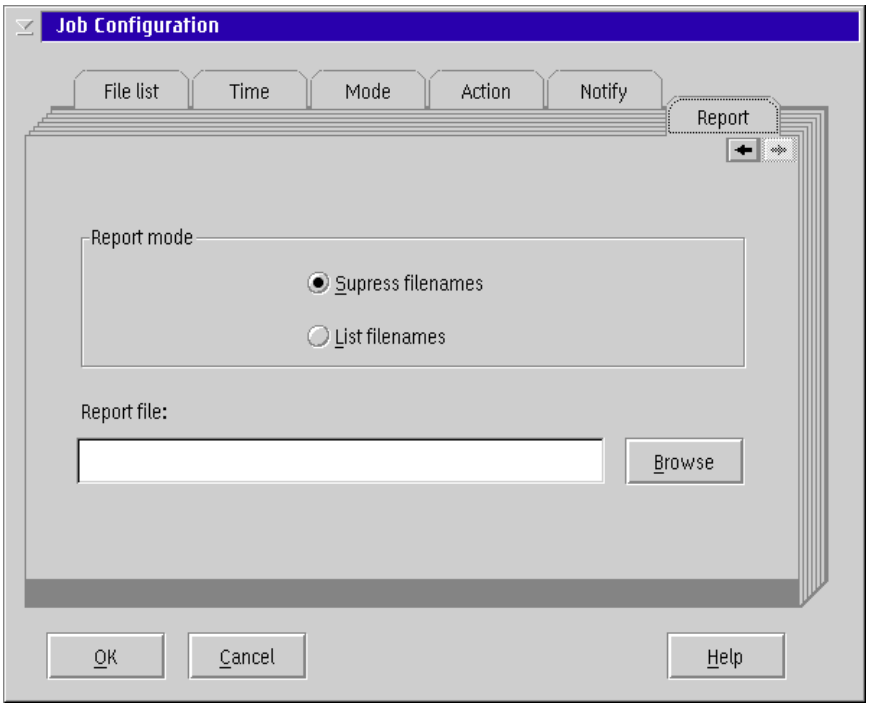
`%1` machine name
`%2` job name
`%3` items (number of items scanned)
`%4` viruses (number of viruses found)
`%5` errors
`%6` report file

Notify timing

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

Use the browser to specify the batch file that will be run.

Report



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

Report mode

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

Report file

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

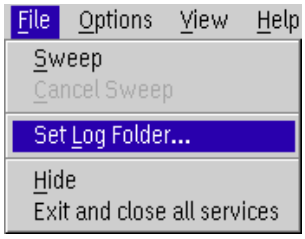
Further options

This chapter describes further options available from the *File*, *Options* and *View* menus, and lists the SWEEP command line qualifiers.

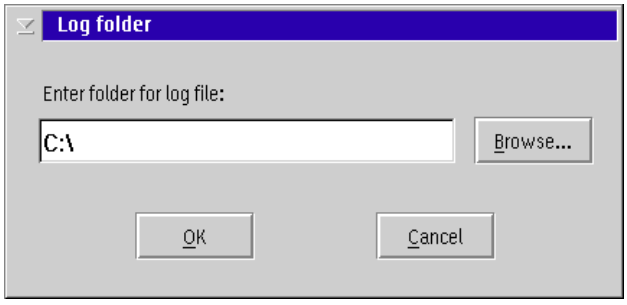
Set log folder

SWEEP maintains a continuous log of all its activity. This log file contains administrative messages along with on-screen messages.

By default the log file will be saved in the directory to which Sophos Anti-Virus was installed (the default is C:\SAV). This can be changed by selecting *Set Log Folder* from the *File* menu.

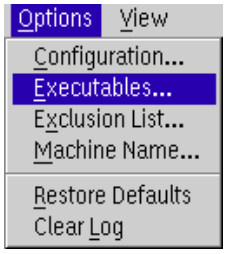


Specify a directory at the 'Log folder' dialog.

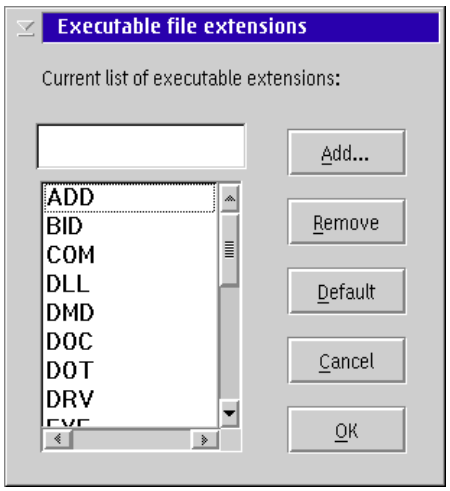


Executables

To edit the list of file extensions treated as executables, select *Executables* from the *Options* menu.



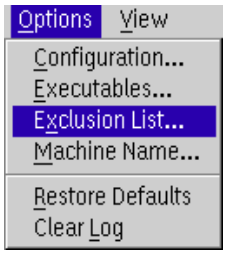
Then specify extensions in the dialog box.



This list is used only if SWEEP is set to check 'executable' rather than 'all' file types. See also 'File types' in the 'Adding new items for immediate scanning' sub-section of the 'Immediate scanning' section of the 'Using Sophos Anti-Virus' chapter.

Exclusion list

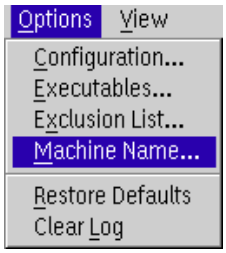
The exclusion list contains the specific files to be excluded from all SWEEP operations. To edit it, select *Exclusion list* from the *Options* menu.



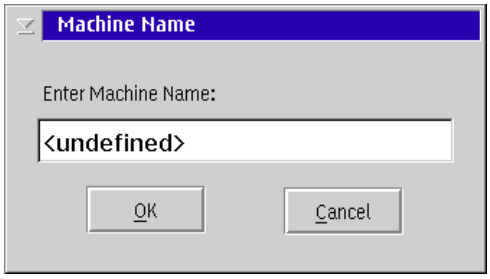
Then add or remove items in the 'Exclusion list' dialog.

Machine name

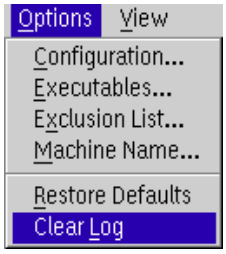
If SWEEP is configured to notify other users of virus finds, it is useful to identify the machine where the virus has been found. To enable SWEEP to do this, select *Machine Name* from the *Options* menu.



Enter a name in the 'Machine Name' dialog.

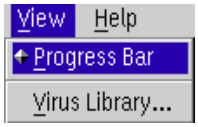


Clear log



The on-screen log provides a record of activity in the current session and reflects the information that is appended to the continuous log file. This option clears the on-screen log but does not affect the continuous log file on disk.

Progress bar



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

Note: This option is set separately for immediate and scheduled modes. The progress bar is enabled or disabled for each scheduled job individually.

SWEEP command line qualifiers

Certain command line qualifiers can be used to configure scanning and reporting.

Either '-' or '/' can be used when entering an option, i.e. /AUTO and -AUTO are identical.

-AUTO

Starts scanning when SWEEP is started, using the most recent configuration set at the Immediate tabbed page.

-EXEJOB <jobname>

Starts the scheduled job named <jobname> when SWEEP is started instead of waiting until the scheduled time.

The -EXEJOB and -AUTO options cannot both be used; if both are included in the command line, -AUTO will be ignored.

-CLOSE

Closes both the window and the background scheduler.

If SWEEP is not running, errorlevel 1 is returned. All other options are ignored.

-CF<config file>

Specifies a name and path for the configuration file.

If the program cannot open the file, SWEEP will be started with default options, and on exit will try to create a configuration file with the given path and filename.

-NOWIN

Starts the background scheduler only.

-LOGPATH <path>

Allows the user to alter the stored (or default) location of the log file, SWEEP.LOG. The new path will be stored in the configuration file.

-REPORTPATH<path>

Allows the user to enter a default path for the (job) report files. This path will be used when no path is entered for a report file in the appropriate dialog.

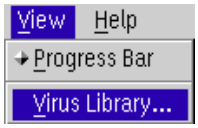
The virus library

This chapter describes the use of the on-line virus library.

Note: This facility is available only via the GUI.

Starting the virus library

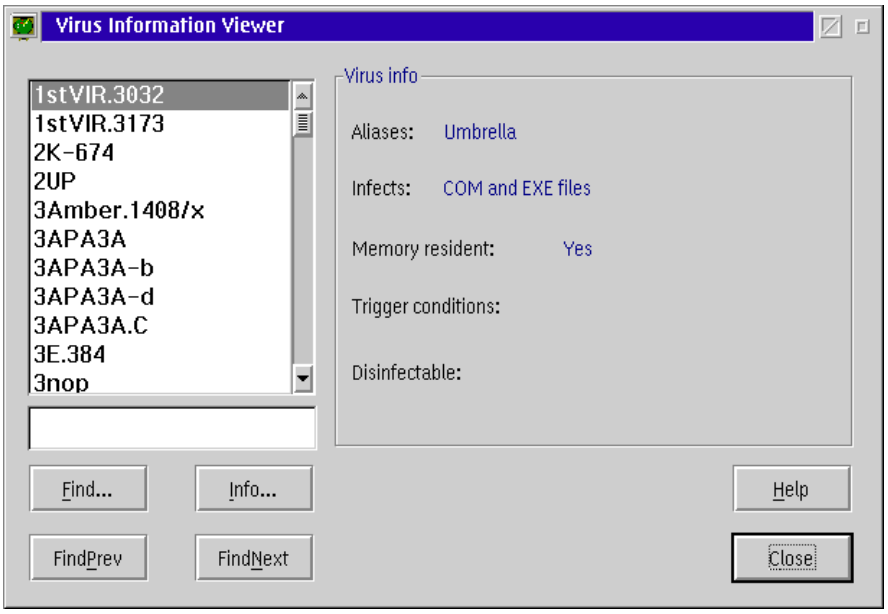
Select *Virus Library* from the *View* menu



or click the associated icon

to start the on-line virus library.

Finding information on a virus



To find details of a virus, enter the virus name (or part of the name) in the text box. In the list, the first name that matches your entry will be highlighted. If this name is not the one you intended, use the *Find Prev* and *Find Next* buttons to locate the right virus.

Note: Many virus names have prefixes indicating the platform or application they infect, e.g. *Melissa* is listed under *WM97/Melissa* as it infects Word 97 documents. Make sure you click *Find Next* until the right name appears.

Basic information about the highlighted virus appears in the 'Virus info' box.

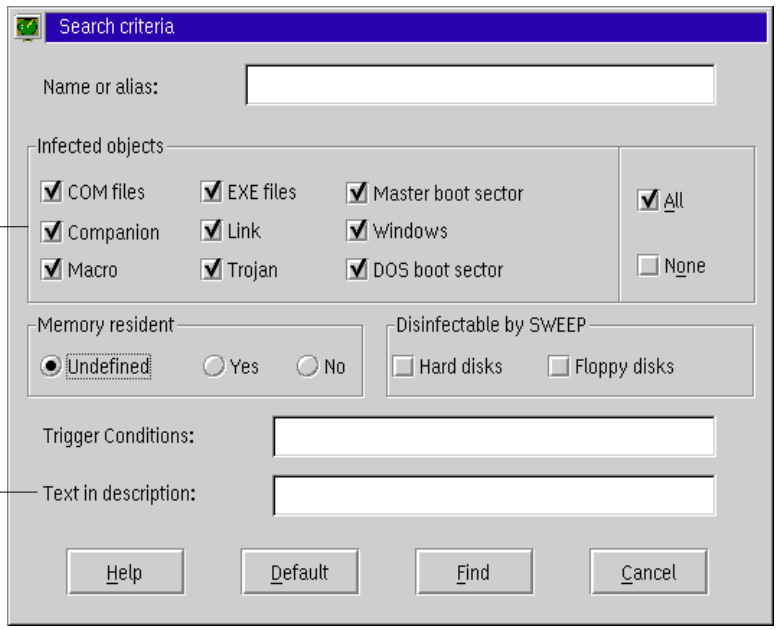
For more information, including advice on disinfection, click *Info ...* or double-click the virus name.

Searching for an unknown virus

You can search for viruses with certain characteristics. In the 'Virus Information Viewer', click *Find* to open the 'Search criteria' screen:

Search according to the kind of objects infected

Search for text in the virus description



Enter criteria in one or more of the sections (described below). Then click the *Find* button. This returns you to the 'Virus Information Viewer' and highlights the first entry that matches your criteria. If it is not the one you intended, use the *Find Prev* and *Find Next* buttons to locate other possible matches.

Infected objects

In this section, you can specify which areas or files the virus infects.

Viruses can place themselves in **COM and EXE files**, 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.

Macro viruses place viral macros inside Microsoft Word, Excel, PowerPoint, Access, Office 95 and Office 97 documents.

Trojan horses are not viruses, but programs which provide unanticipated side-effects when run.

You can also use the checkboxes to include 'All' or 'None' of these categories in your search.

Memory-resident

In this section, you can specify whether the virus you are searching for is memory-resident or not. Memory-resident viruses stay in memory after they are executed and infect other objects when certain conditions are fulfilled.

Disinfectable by SWEEP

Check these boxes to include in the search viruses which can be removed from hard and/or floppy disks.

Trigger conditions

In this text box, you can enter conditions (e.g. a certain time or date) that will trigger a virus's side-effects.

Text in description

In this text box, you can enter a text string which appears in the information about the virus you are searching for.

Using CLI Sophos Anti-Virus

This chapter describes how to run SWEEP from the command line on workstations or on a file server.

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

What will SWEEP check?

By default, SWEEP will look for viruses in:

- More than thirty types of files identified by their filename extension.
- Logical sector 0 of all local hard disk drives.
- Physical sector 1 of hard disk devices 80 to 83 Hex.

Different areas or file types can be specified, as described in the 'Configuring CLI Sophos Anti-Virus' chapter.

Scanning level

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

Virus checking with SWEEP

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

Checking hard disks

Enter the command

```
OSWEEP
```

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

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

```
OSWEEP D: E:
```

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

Checking floppy disks

Run SWEEP using the command

```
OSWEEP -MU A:
```

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

Checking file servers

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

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

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

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

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

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

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

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

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

Running SWEEP on a file server

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

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

Scheduling

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

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

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

Background Operation

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

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

The SWEEP option

```
-PR=L
```

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

following line should be added to the startup command file

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

where RUNSWEEP.CMD is the command file.

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

What if SWEEP reports a virus or virus fragment?

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

The screen output will look something like this

```
SWEEP virus detection utility
Version 3.29
(c) 1989,2000 Sophos Ltd, Oxford

Please wait ...
System time 18:10:05, System date 11 January 2000

Virus library date 03 January 2000 (47327 viruses)

Quick Sweeping

Press Esc to quit.

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

Please send infected samples to Sophos for analysis.

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

Customising the ‘Viruses found’ report

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

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

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

Virus removal with SWEEP

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

Configuring CLI Sophos Anti-Virus

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

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

Specifying what SWEEP will check

Users can specify which items SWEEP will check by using either

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

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

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

Specifying items to be checked in the command line

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

```
OSWEEP ISVIRUS.BIN
```

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

```
OSWEEP D: E:
```

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

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

Specifying items to be checked in SWEEP.ARE

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

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

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

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

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

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

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

```
OSWEEP A: D:
```

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

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

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

```
OSWEEP -AD=A
```

then SWEEP will check

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

Specifying files to be checked in SWEEP.ARE

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

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

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

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

```
C:*.ABC
```

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

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

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

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

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

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

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

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

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

Excluding files from checking

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

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

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

For example

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

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

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

```
<\NU.EXE
```

and SWEEP is started with the command line qualifier

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

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

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

in the SWEEP.ARE file.

Specifying disk sectors to be checked in SWEEP.ARE

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

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

Specifying Logical Sectors to be checked

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

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

where

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

`ssector` is the first logical sector to be checked

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

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

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

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

For example

```
C:|0
```

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

```
C:|0 10
```

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

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

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

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

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

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

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

```
|*
```

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

Specifying Absolute Sectors to be checked

To specify an absolute sector, use the '+' symbol followed by the drive number, the cylinder (or 'track') number, the head (or 'side') number and the sector

number within that cylinder. The first floppy disk drive in the system is number 0, the second is number 1, and so on. The first physical hard disk drive is number 80, the second is number 81 and so on. It is also possible to specify a byte or group of bytes to be checked in the sector (for example if the sector contains variable information).

The format of the specification is

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

where

`drive` is the disk drive number

`cylinder` is the cylinder number

`head` is the head number

`sector` is the sector number

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

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

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

For example

```
+80 0 0 1
```

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

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

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

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

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

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

Full sweep

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

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

Running SWEEP at different priorities

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

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

```
OSWEEP -PR=H
```

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

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

```
OSWEEP -PR=L
```

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

Error codes returned by SWEEP

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 a corrupt or password protected file is encountered, or if some error preventing further execution is discovered.

3 If viruses or virus fragments are discovered.

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

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

This batch file will print

```
Something has been discovered
```

if SWEEP discovers a virus,

```
Some error has occurred
```

in the event of an error, or

```
No problems
```

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

Extended error codes

A different set of error codes will be returned if SWEEP is run with the -EEC command line qualifier.

0 No errors have occurred and no viruses have been found.

8 Survivable errors have occurred.

12 Archive files have been found and decompressed.

16 Archive files have been found and not decompressed.

20 Viruses have been found and disinfected.

24 Viruses have been found and not disinfected.

32 OSWEEP has failed an integrity check.

36 Unsurvivable errors have occurred.

40 Execution has been interrupted.

Scanning with new virus identities

SWEEP can be updated to check for specific new viruses. See 'Updating Sophos Anti-Virus with new virus identities' in the 'Updating a network' or 'Updating a single machine' chapter for details.

Scanning 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 format

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

where

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

`Hex1` etc. are pattern bytes in hexadecimal, 2 hex 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 15 characters and a pattern can be up to 24 bytes long.

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

For example, SWEEP.PAT may contain

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

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

```
OSWEEP A:
```

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

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

```
OSWEEP C: -F
```

Virus disinfection and removal

Common boot sector viruses can be removed from hard and floppy disks, and macro viruses from documents, by using SWEEP's built-in disinfection capability. To enable this, the system must be shut down and restarted, and the command line qualifier -DI must be used

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

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

See also the 'Treating viral infection' chapter.

SWEEP command line qualifiers

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

```
OSWEEP -?
```

The command format is

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

where

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

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

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

For example

```
OSWEEP A:
```

will SWEEP the floppy disk in drive A: while

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

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

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

@file Command line qualifiers from an external file

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

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

when the file SWEEP.CM contains

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

is equivalent to

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

Command files compared with .ARE files

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

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

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

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

-? Help

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

-6 62 seconds

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

-A Append report

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

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

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

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

-AD=<drive> Area file default

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

For example

```
OSWEEP -AD=X
```

would assume that all areas refer to drive X.

-AF=<filename>Area file

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

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

-ALL Scan all files

In order to scan all files on a disk instead of just the executable files, specify the -ALL command line

qualifier. This is equivalent to creating a SWEEP.ARE file which contains

```
\>*.*
```

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

For example

```
OSWEEP A: -ALL
```

will recursively sweep all files on drive A:.

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

-ARCH=n

This qualifier allows SWEEP to scan inside archive files. The archive types scanned include ZIP, GZIP, RAR, ARJ, CMZ, and TAR.

By default, SWEEP will unpack 16 levels of 'nested' archive files (i.e. archive files within archive files). If you want to change this setting, use -ARCH=n, where n is the maximum number of levels. The number n can be between 0 and 32.

-AS Scan standard areas

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

For example

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

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

-CI Check integrity

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

-D=<day | percentage> Day or Percentage

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

For example

```
OSWEEP -D=MONDAY
```

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

Alternatively

```
OSWEEP -D=20
```

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

Note: See also the -DE command line qualifier.

-DA Display areas

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

-DE Daily execution

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

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

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

For example

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

-DI Disinfect

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

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

See the 'Treating viral infection' chapter.

-DIB

Use the -DIB qualifier to disinfect only boot sectors.

-DID

Use the -DID qualifier to disinfect only documents.

-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.

-EEC Use extended set of error codes

This qualifier directs SWEEP to use an extended set of eror codes. For details, see the 'Error codes returned by SWEEP' section of this chapter.

-EX=<extensions> Executable extensions

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

For example

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

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

-F Full SWEEP

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

See also the 'Full sweep' section.

-FM Specify message file

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

For example

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

specifies the file 'MY_MSG.TXT'.

-FS File server

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

See also 'Checking file servers' in the 'Virus checking with SWEEP' section of the 'Using CLI Sophos Anti-Virus' chapter.

-ICI InterCheck INI file

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

For example

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

would specify SECOND.INI as the initialisation file.

-ICS [=<servername>] InterCheck Server mode

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

For example

```
OSWEEP -ICS=Server_1
```

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

-MU Check multiple disks

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

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

```
OSWEEP -MU A:
```

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

-NAF Do not read file with areas to be checked

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

-NAP Do not use internal virus patterns

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

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

For example

```
OSWEEP -NAP -F
```

-NAS Do not check standard areas

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

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

-NB No bell

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

-NCI Do not check identities

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

-NE Do not use the emulator

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

-NI No interrupting

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

-NK No key to continue

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

-NOC No confirmation before virus removal

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

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

Warning! Use this qualifier with care!

-NP Do not display full pathname

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

Using the -NP qualifier will mean that SWEEP will only record the names of the files it checks instead.

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

-NS Not silent

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

-NTW No Temp Warning

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

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

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

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

For example

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

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

-PD Pause on discovery of a match

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

-PR Priority

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

```
OSWEEP -PR=H
```

specifies high priority, while

```
OSWEEP -PR=L
```

specifies low priority.

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

-Q Quick sweep

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

-REC Recursive search

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

For example

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

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

-REMOVE Remove viruses on discovery

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

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

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

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

For example

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

See the 'Virus disinfection and removal' section.

-REMOVEF Remove infected files

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

```
OSWEEP -REMOVEF
```

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

See the 'Virus disinfection and removal' section.

-RS Remove viruses by positively overwriting them

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

Disabling of boot sectors is not affected.

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

For example

```
OSWEEP -REMOVE -RS
```

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

See the 'Virus disinfection and removal' section.

-S Silent running without displaying checked areas

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

-SC Scan inside compressed files

By default, SWEEP looks for viruses inside files compressed by using dynamic compression utilities PKLite, LZEXE and Diet.

This command line qualifier is the equivalent of the default.

-SS Super silent running

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

Updating the emergency disk set

This chapter describes how to update your emergency disks. You should do this before you update Sophos Anti-Virus each month.

Preparation

When you update your emergency disks, you need:

- The emergency disks to be updated. You should write-enable these.
- The Sophos Anti-Virus CD.

Updating the disk set

Extracting the disk update program

First you extract the disk creation program from an archive on the Sophos Anti-Virus CD.

Note: If the OS/2 computer has no CD drive, follow the steps in 'Appendix: Making floppy disk sets'. Then go to 'Running the disk update program' below.

Insert the Sophos Anti-Virus CD in an OS/2 computer.

Change to a directory on the hard disk where you can make a temporary sub-directory. For example:

```
C:
cd\temp
```

Enter

```
F:\diskimgs\esdos2
```

where F: is the CD drive.

Running the disk update program

This creates a sub-directory called esdos2. Change to this directory

```
cd esdos2
```

Then enter

```
mkstand -P -T:A
```

Updating the 'Emergency OSWEEP' disk

The computer asks for your 'Emergency OSWEEP' floppy disk.

Write-enable and insert the 'Emergency OSWEEP' disk and press *Enter*.

The emergency SWEEP programs are written to it. When the disk has been updated, remove it from the drive and mark it with the date it was updated.

Press *Enter*.

Updating the 'Emergency Virus Data' disks

The computer prompts you for your 'Emergency Virus Data' disks.

Write-enable and insert your first 'Emergency Virus Data' disk and press *Enter.* The new virus data is written to it. When finished, remove it from the drive and mark it with the date it was updated.

You are prompted for another disk.

Write-enable and insert the disk and press *Enter.*

When finished, remove the disk and label it. Press *Enter*. The computer announces the completion of the update process.

Scanning the updated disks

You will now be asked if you want to scan the newly updated disks. Sophos recommends that you do so.

Run SWEEP on the disks, placing them in the target drive as prompted.

When all disks have been scanned replace them, with your clean OS/2 Utility disk set, in your secure place.

You can now update Sophos Anti-Virus.

Updating a network

This chapter describes how to update Sophos Anti-Virus using a central installation. It also explains how to restore a previous version of Sophos Anti-Virus and how to add new virus identities between updates.

About central updates

Updating Sophos Anti-Virus across your network involves two steps.

1. The central installation on the server is updated from the Sophos Anti-Virus CD or download.
2. The workstations detect the new version of Sophos Anti-Virus and update automatically.

Before you update

Before you update Sophos Anti-Virus, you should update your emergency disks, as described in the 'Updating the emergency disk set' chapter.

You should also delete any virus identities you have added to the central installation directory. Then download the latest virus identities from the Sophos website and place them in the central installation folder.

Central updating

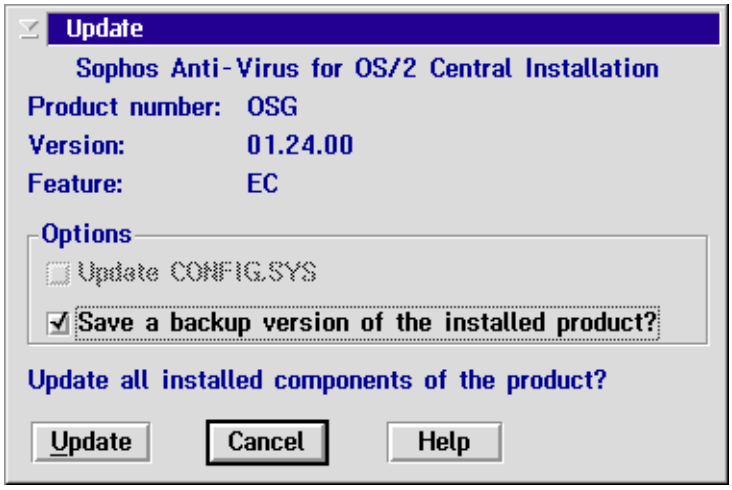
Insert the Sophos Anti-Virus CD in the server where you previously made a central installation. At a command prompt, enter:

```
F:\OS_2\SETUP -CENTRAL
```

where F: is the CD drive.

Note: If the OS/2 server has no CD drive, follow the steps in 'Appendix: Making floppy disk sets' and then run the copy of SETUP on the server.

If any workstations are currently updating from the CID, there will be a delay before SETUP can modify the CID. Each time SETUP attempts to access the CID, it will print a dot on the command line.



At the 'Update' screen, you can choose to save a backup of the version of Sophos Anti-Virus currently installed. A backup lets you restore the existing version if you stop the update or if the update goes wrong.

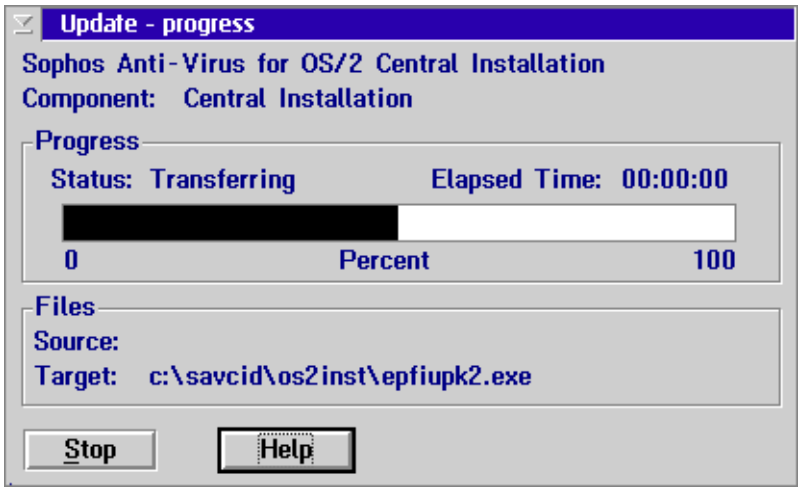
If your CID is on a **non-OS/2** machine, e.g. a Windows NT server, you may be unable to use the backup option successfully.

You do not need to specify which directory will be updated. SETUP will automatically update the existing CID.

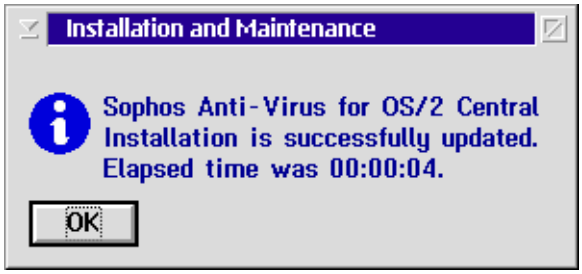
Click *Update*.

If you have chosen not to save a backup, you will be prompted to confirm your choice.

You then see the update in progress.



When the central installation has been updated, you see the screen below.



Workstations update automatically when they detect the updated software in the central installation.

Restoring a previous version

You can restore a previous version of Sophos Anti-Virus.

Restoring a central installation

To restore a previous version in the central installation directory (CID), update the CID from the CD or floppy disk set for that version. All the files needed in the CID will be copied from the source, whatever their date and time.

As IDE files are added to the CID manually, they are not deleted automatically when you restore a previous version. Nor will any deleted IDEs be restored.

You should delete any IDEs in the CID manually.

Restoring a workstation installation

To restore a previous version on a workstation that uses auto-updating, restore the CID as described above.

All the changes in the CID, including IDE files, are reflected on the workstation when it next updates from the CID.

Updating Sophos Anti-Virus with new virus identities

This section describes how to update Sophos Anti-Virus with new virus identities (IDEs), which are used to detect viruses that appear between regular updates.

You can download the latest IDEs from the Sophos website:

www.sophos.com/downloads/ide

Place the IDE files in the central installation directory (CID) on the server, e.g. C:\SAVCID\OS2INST.

Before the workstations can update themselves with the new IDEs, you have to mark the central installation as 'updated'.

Run SETUP from the CID with the -UPDATE and (optionally) -FULL qualifiers, e.g.

```
C:\SAVCID\OS2INST\SETUP -UPDATE -FULL
```

The -FULL qualifier ensures that workstations transfer precisely the files needed.

If any workstations are currently updating from the central installation directory, there will be a delay before SETUP can modify it. When the CID has been marked as updated, the workstations update with the new IDEs automatically.

You should remove IDE files when they are no longer needed. See the Sophos website for information on which IDEs are needed for each version of Sophos Anti-Virus.

Updating a single machine

This chapter describes how to update Sophos Anti-Virus on a single machine. It also describes how to add new virus identities between regular updates.

For information on updating the InterCheck components, see the 'Installing an OS/2 InterCheck Server' chapter.

Regular updates

Registered users of Sophos Anti-Virus are sent updates in the first week of every month, or can download updates from the Sophos website.

Before you update

Before you update Sophos Anti-Virus, you should update your emergency disks. See the 'Updating the emergency disk set' chapter.

Updating SWEEP

If updating SWEEP on a server with Local Security installed, log in as an Adminstrator first. If the OS/2 InterCheck Server is running, stop it by selecting its window and typing *Esc*.

Insert the Sophos Anti-Virus CD and enter

```
F:\OS_2\UPDATE
```

where `F:` is the CD-ROM drive.

Note: If the computer has no CD drive, follow the steps in 'Appendix: Making floppy disk sets' and then run the copy of UPDATE on the hard disk.

The 'Update' screen appears.

'Update CONFIG.SYS' will update the configuration file. If this is deselected, a trial configuration file is created instead.

'Save a backup version of the installed product' saves a backup so that the earlier version of SWEEP can be restored if needed.

Finally, click *Update*.

The setup program will update the components you have installed (i.e. the GUI or CLI version of Sophos Anti-Virus).

If you have an internet connection, you should now download the latest virus identities from the Sophos website (http://www.sophos.com/downloads/ide) and place them in the folder where SWEEP is installed (for details, see below).

If running an InterCheck Server, restart it. For details of how to start or restart the InterCheck Server, see the 'Installing an OS/2 InterCheck Server' chapter.

Updating Sophos Anti-Virus with new virus identities

Users can add new 'virus identities' (IDEs), which SWEEP uses for virus detection, at any time.

New identities can be downloaded from the Sophos website (http://www.sophos.com/downloads/ide).

Loading new IDEs

Copy the IDE files into the directory containing OSWEEP.EXE.

Exit from any scan in progress and then run SWEEP.

If the OS/2 InterCheck Server is installed, it must be stopped and restarted (see the 'Installing an OS/2 InterCheck Server' chapter).

How to confirm that IDEs have been loaded

Select *About Sweep ...* from the *Help* menu. Click on *More*. The IDE files should be listed under 'Version Information'.

The IDE files loaded are also listed in the SWEEP log file if one has been specified.

Protecting non-OS/2 workstations

This chapter gives an overview of how to protect **non-OS/2 workstations** on an OS/2 based network.

Protecting non-OS/2 workstations

You can use Sophos Anti-Virus to protect all the workstations on your network, whichever operating system they run. There are two steps:

1. Install an OS/2 InterCheck Server

This allows workstations to report to the file server and can provide server based on-access scanning for those workstations that require it.

See the 'Installing an OS/2 InterCheck Server' chapter.

2. Install Sophos Anti-Virus on workstations

There are two ways to provide virus-checking on workstations.

For Windows NT, Windows 95/98 and Windows 3.x workstations, you install and run a 'native' version of Sophos Anti-Virus on each workstation. Virus checking is performed locally but reports are sent to the InterCheck Server.

For DOS workstations, you run InterCheck on-access scanning from the file server. All virus checking is performed by the InterCheck Server.

See the 'Installing Sophos Anti-Virus on non-OS/2 clients' chapter.

Installing an OS/2 InterCheck Server

This chapter describes how to install an OS/2 InterCheck Server to provide central reporting and/or remote on-access scanning from workstations.

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

Information on **installing Sophos Anti-Virus on workstations**, so that they can send reports and (if necessary) requests for scanning to the InterCheck Server, can be found in the 'Installing Sophos Anti-Virus on non-OS/2 clients' chapter.

Software required

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

- SWEEP for OS/2 (`\OS_2\*.*`).
- SWEEP for DOS (`\DOS\*.*`).
- InterCheck for DOS, Windows, Windows 95/98 (`\INTERCHK\*.*`).
- ICONTROL (`\TOOLS\ICONTROL\*.*`).

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

About InterCheck Server installation

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

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

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

InterCheck and Peer Servers

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

The procedure for installing an InterCheck Server is summarized below and detailed on the pages that follow.

Summary of the installation procedure

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

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

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

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

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

Procedure for installing the InterCheck Server

1. Log in to the InterCheck Server host

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

2. Create directories on the server

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

Create the directories

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

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

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

Enter

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

where F: is the CD drive.

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

4. Copy the SWEEP for DOS and InterCheck files

Enter

```
I:
CD\INTERCHK
COPY F:\DOS\*.*
COPY F:\INTERCHK\*.*
```

where F: is the CD drive.

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

5. Create required subdirectories

Type

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

6. Create and populate a group ICUSERS

A group ICUSERS must be created and populated with all the users who are to run the InterCheck client software, i.e. to run InterCheck from the server. Another name can be used instead of ICUSERS if desired. This group is needed so that access rights for the InterCheck directories can be assigned to it. It may be desirable for privileged users running the DOS or Windows LAN clients not to be forced to run the InterCheck client, in case the client software interferes with critical management operations when the InterCheck Server is not running. Normally, though, the group ICUSERS should include the group USERS.

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

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

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

7. Create an alias for access to the INTERCHK directory

Type

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

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

8. Grant access rights to directories

Type

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

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

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

9. Create a login script

See the 'Installing Sophos Anti-Virus on non-OS/2 clients' chapter, where there are instructions on creating a login script for each platform.

10a. Create a desktop icon for ICW

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

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

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

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

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

10b. Create a desktop icon for ICONTROL

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

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

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

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

The session type may be DOS Full Screen or DOS Window according to your preference. Finally the program Title (in the General settings page) should be set to 'InterCheck Server Controller' or some similar description. You may now close the settings notebook for ICONTROL and the Templates and OS/2 System folders.

11. Configure the InterCheck Server and Client software

InterCheck Server

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

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

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

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

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

At this stage, the IC Server option in the main menu bar should be highlighted. Press the *Enter* key. A menu will appear showing various options including

List and Exit. Type L to select List. A small box will appear showing a path. Press the *Enter* key.

Now a larger box will appear with the title

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

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

```
I:\SWEEP
```

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

A box will appear with the title

```
Save changes before exiting?
```

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

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

First type I to select Infected, then enter the path

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

of the directory INFECTED created at step 5.

Press the *Enter* key to enter the path. Then type C to select Comms, then enter the path

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

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

You have now finished creating the initial version of the SWEEPIC.INI file. You can either leave ICONTROL running for later operations, or exit from it by pressing the *Esc* key, then the *Enter* key. Further information on ICONTROL may be found in the 'Controlling the InterCheck Server' chapter.

InterCheck Client

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

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

You can run InterCheck without any further configuration.

However, if you want to configure InterCheck, see the Sophos Anti-Virus user manual for the workstation platform (e.g. Windows 95/98), or the 'Configuring InterCheck clients' chapter of the 'InterCheck Advanced User Guide'. All manuals are available on the Sophos Anti-Virus CD or website.

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

12. Place InterCheck Server startup in system startup command file

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

The InterCheck Server program is OSWEEP.EXE, which is also used for normal checking of file systems. However, it is started with a special command line.

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

However, in order to test the InterCheck installation, the InterCheck Server may be started by entering

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

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

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

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

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

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

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

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

Configuring the InterCheck Server

This is performed with ICW or ICONTROL, as described in the 'Controlling the InterCheck Server' chapter.

Updating the InterCheck Server

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

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

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

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

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

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

Note: Workstations that run InterCheck from the file server do not require updating.

Updating Sophos Anti-Virus with new virus identities

See 'Updating Sophos Anti-Virus with new virus identities' in the 'Updating a single machine' chapter for details.

Note that the OS/2 InterCheck Server must be stopped and restarted when making urgent updates.

Installing Sophos Anti-Virus on non-OS/2 clients

This chapter describes how to install Sophos Anti-Virus on **non-OS/2 workstations** on your OS/2 network.

Note: For full details of installation and configuration, see the manual for the appropriate version of Sophos Anti-Virus.

About installation on non-OS/2 workstations

First, ensure that an InterCheck Server has been installed, as described in the 'Installing an OS/2 InterCheck Server' chapter. Then install Sophos Anti-Virus on the workstations.

On Windows NT/2000 or Windows 95/98 workstations, you install Sophos Anti-Virus for Windows NT/2000 or Windows 95/98 on each workstation. Virus checking is performed locally but reports are sent to the InterCheck Server.

On DOS or Windows 3.1x workstations, you install InterCheck on-access scanning from the server. Virus checking is performed by the InterCheck Server.

Note: These are the recommended forms of installation. For details of alternative ways to provide on-access protection, see the 'InterCheck Advanced User Guide' on the Sophos Anti-Virus CD or website.

Windows NT or 2000 workstations

Installation is carried out at a **Windows NT or 2000** workstation or file server on the network.

Insert the Sophos Anti-Virus CD into the CD drive. The CD will auto-start. Select 'Quick Installation' to start the setup program.

Note: If auto-start is not enabled, open the Win32/I386/WinNT or Win32/AXP/WinNT folder and run Setup.exe.

At the 'Installation Type' screen, select 'Central installation'.

At the 'Folder Selection' screen, select a central folder in which to place the installation files.

You can also specify auto-updating at the setup screens. Note that choices made at this stage only set defaults. When working installations are made on the workstations, these can be changed.

Then, **at each Windows NT or 2000 workstation**, run Setup.exe from the central folder.

At the 'InterCheck Support and Network Access' screen, ensure that 'Enable InterCheck client' is selected.

Remember that Sophos Anti-Virus for Windows NT or 2000 should be updated each month.

Note: If you are installing Sophos Anti-Virus on a large number of workstations, you may wish to use the SAVADMIN program in the Tools\SAVADMIN directory on the Sophos Anti-Virus CD.

For full details, see the installation section of the Sophos Anti-Virus for Windows NT or 2000 manual.

Windows 95/98 workstations

You can install Sophos Anti-Virus on Windows 95/98 workstations across the network.

Installation is carried out at a Windows 95/98 PC visible to other users.

Insert the Sophos Anti-Virus CD, which will auto-start. Select 'Quick Installation' to start the setup program.

At the 'Installation Type' screen, select 'Central installation' and 'InterCheck for Windows 95/98'. At the 'Folder Selection' screen, select a central folder in which to place the installation files.

Workstation installations can be made from these installation files either manually or automatically.

Manual installation

At each workstation, run Setup.exe from the folder on the server where the installation files were placed.

Automatic installation

Workstation installations can be made from the central installation automatically via a login script.

In the workstation's login script enter

```
\\ServerName\INTERCHK\W95inst\Setup -INL -A
```

where *ServerName* is the file server and INTERCHK the share in which the installation files were placed.

Remember that Sophos Anti-Virus for Windows 95/98 should be updated each month.

DOS workstations

To protect DOS workstations, you run Sophos InterCheck from the file server, with or without a login script.

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

With a login script

Each user who will run InterCheck should have a drive assignment to the InterCheck alias set in their login profile. Using the example names used in the 'Installing an OS/2 InterCheck Server' chapter, this assignment will assign drive I: to the alias ICHK.

Each user should have a login script containing

```
I:\ICLOGIN
```

Note: If the IBM DOS network client will not restore network connections automatically when the user logs in, use the following shortcut. Instead of assigning the drive I: in the user's login profile, insert the following in the user's login script:

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

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

Without a login script

Each user should execute the commands below, either manually or in their AUTOEXEC.BAT startup command file, after starting the IBM client software and logging in:

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

Windows 3.1x workstations

This section assumes that the IBM LAN Server network client for Windows 3.1x has been installed on the Windows workstations.

To protect Windows 3.1x workstations, you run Sophos InterCheck from the server.

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

Users log in before starting Windows

If users log in under DOS, before Windows has started, see the 'DOS workstations' section above.

Users log in after starting Windows

For users who log in after starting Windows, the procedure is as follows.

Note: Each user who will run InterCheck has a drive assignment to the InterCheck alias set in their login profile. Using the example names used in the 'Installing an OS/2 InterCheck Server' chapter, this assignment will assign drive I: to the alias ICHK.

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

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

A windowed display will appear. If you have more than one hard disk, select the desired drive from the *Where* menu.

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

```
I:\COMMS
```

and type <Return> to enter this information.

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

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

```
SWEEPVXDLOAD=YES
```

Note: You will need to update your installation each month by running ICINSTAL.

Testing communications with the InterCheck Server

Where workstations send files to the InterCheck Server for checking (e.g. Windows 3.1x workstations), it is useful to test communications.

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. InterCheck will interpret this as the creation of an executable type file and will send the file to the server for checking.

Controlling the InterCheck Server

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

Introduction to ICONTROL

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

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

The ICONTROL programs are copied to the InterCheck Server as part of the InterCheck Server installation process (see the 'Installing an OS/2 InterCheck Server' chapter).

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

ICONTROL for Windows

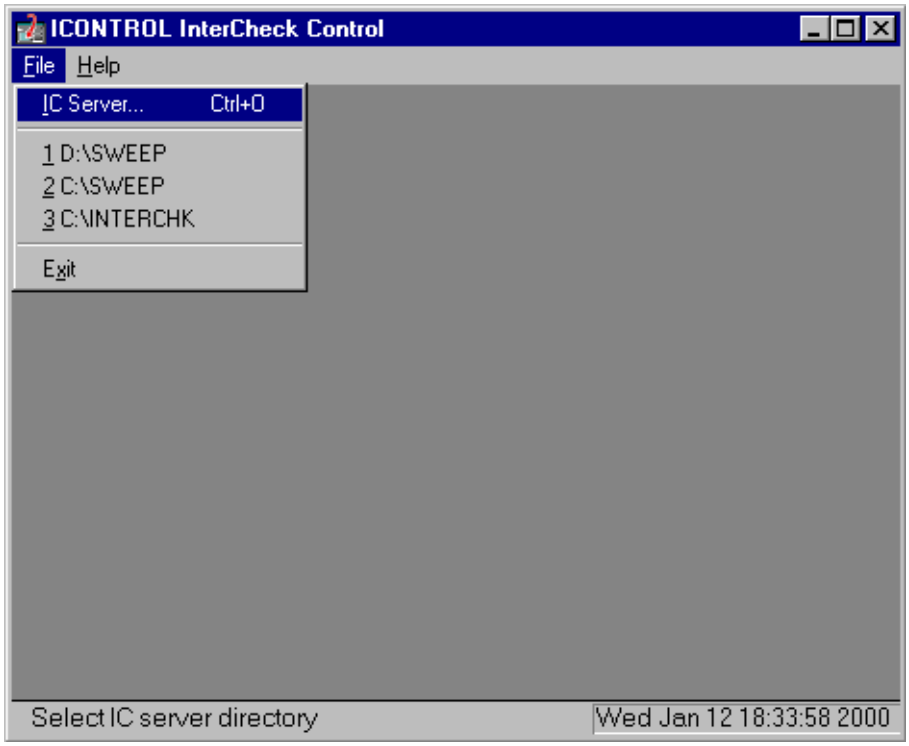
Starting ICONTROL

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

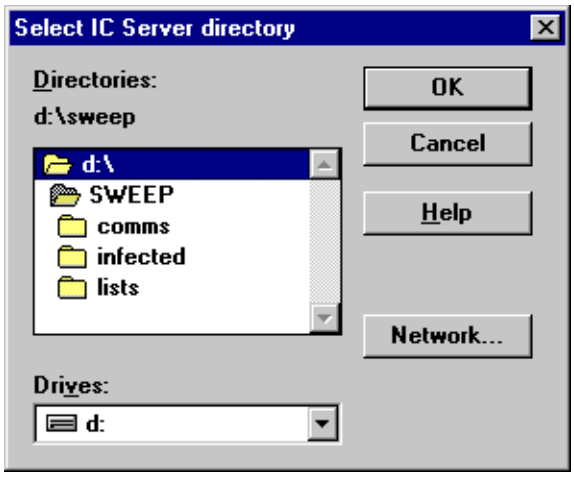
Note that ICW.EXE can be placed in, and launched from, a Windows 3.x Program Group or the Windows 95 Taskbar in the same way as any other Windows executable.

Selecting the InterCheck Server

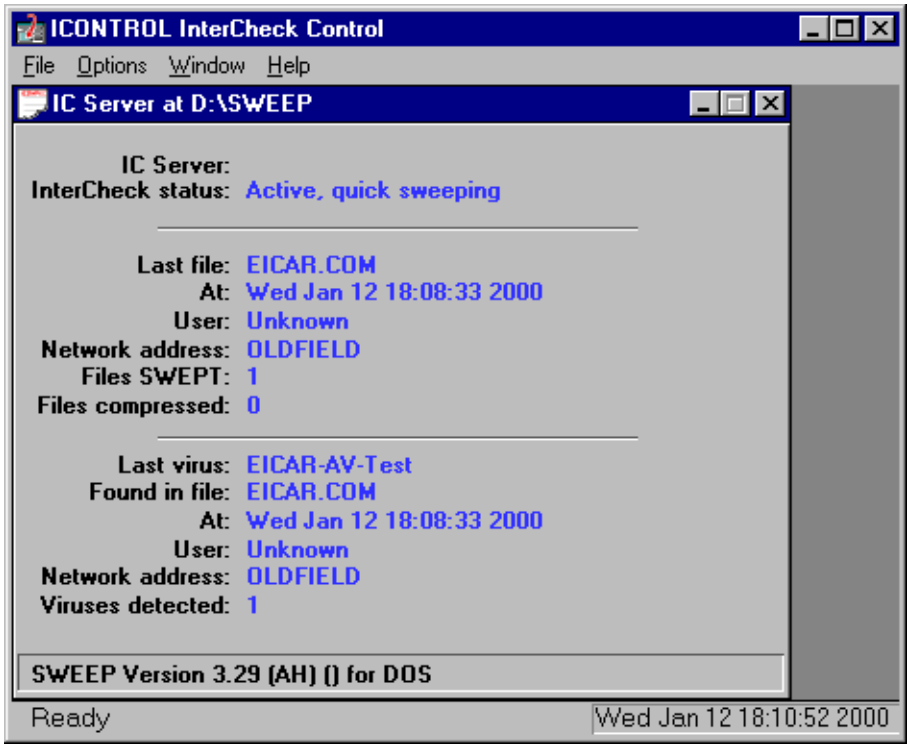
Choose *IC Server* from the *File* menu.



Select an InterCheck Server working directory.



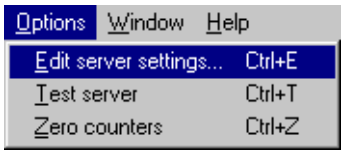
When the directory is specified ICONTROL will display the current status of the InterCheck Server that is running at that location.



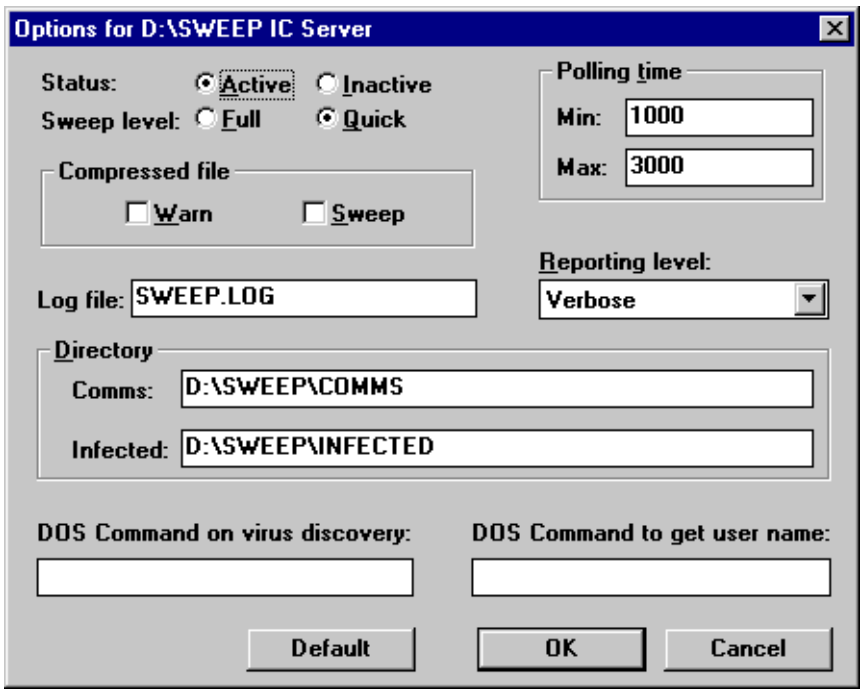
Other InterCheck Servers can be monitored by selecting them via the *File* menu. Unlike ICONTROL for DOS, ICONTROL for Windows can monitor multiple servers at the same time.

Setting InterCheck Server options

You can configure the InterCheck Server by selecting *Edit server settings* from the *Options* menu.



The options operate on the InterCheck Server whose status window is currently selected.



Status

Set the *Status* to active or inactive. The default is active.

Sweep level

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

Compressed file

SWEEP automatically scans files which have been compressed using PKLite, LZEXE and Diet. The Compressed file options in ICONTROL are no longer used.

Polling time

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

Log file

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

Reporting level

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

Directory

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

The locations of these directories are set during the system installation (see the 'Installing an OS/2 InterCheck Server' chapter), and it is unlikely that they will have to be changed subsequently.

DOS command on virus discovery

An OS/2 command file can be executed when a virus is found. Notification can be sent to a user, workstation or group.

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

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

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

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

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

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

DOS command to get user name

An OS/2 command file can be executed when the owner of a file has to be determined.

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

The appropriate system utility should be used to return the name of the owner of that file, and this

name should be written to the file SWEEP.USR in the same directory as the InterCheck Server.

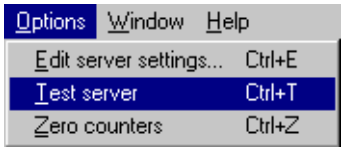
Note: IBM LAN Server does not provide a mechanism for obtaining the userid of the file owner, so this command is not used for LAN Server networks.

Default

Select this to set the options to their default values.

Testing communications

You can test the communication between ICONTROL and the selected InterCheck Server. Select *Test server* from the *Options* menu.

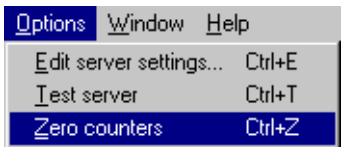


The test server dialog is displayed and updated throughout the process until the outcome is displayed.

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

Zeroing counters

You can zero the viruses found and files swept counters on the selected InterCheck Server. Select *Zero counters* from the *Options* menu.



ICONTROL for DOS

Starting ICONTROL

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

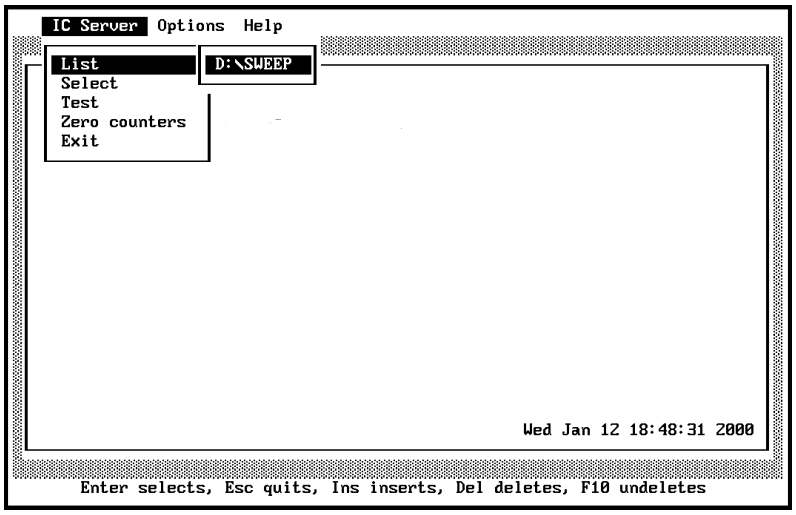
```
D:\SWEEP\ICONTROL
```

to start ICONTROL.

Selecting the InterCheck Server

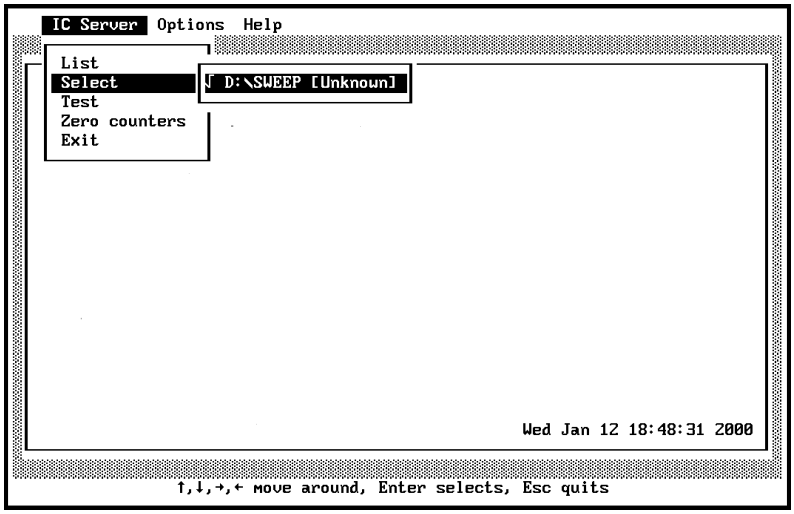
You can control one or more InterCheck Server processes using ICONTROL under DOS, although only one can be selected and monitored at one time.

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

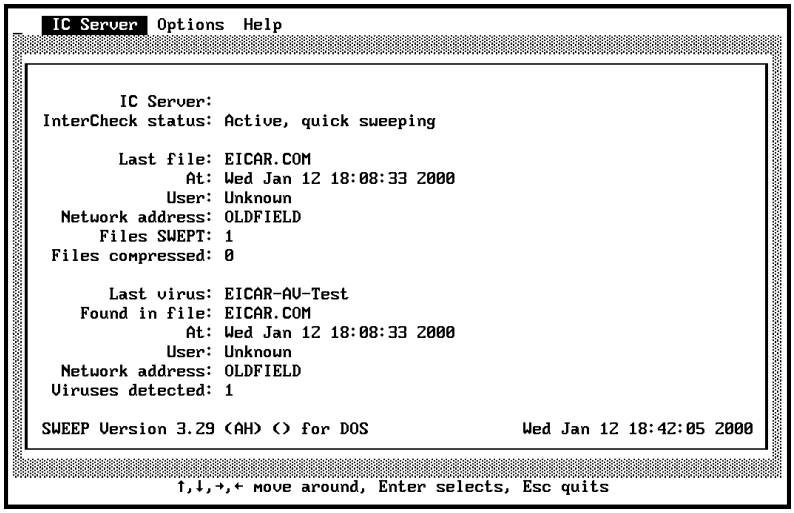


If there is no entry with the correct drive and path, press *Insert* and enter the details, or press *Enter* to edit an existing entry.

Use the *Select* option from the *IC Server* menu to select an InterCheck Server (from the list defined in the *List* option) for monitoring and controlling.



If the selected SWEEP is running in InterCheck Server mode, and no menus are 'hanging' off the top bar, ICONTROL will start to monitor SWEEP and update the main ICONTROL display.



The main ICONTROL display shows the InterCheck Server status (active, inactive or unknown), last file scanned, total files scanned, number of compressed files, last virus detected, and total viruses detected.

Testing communications

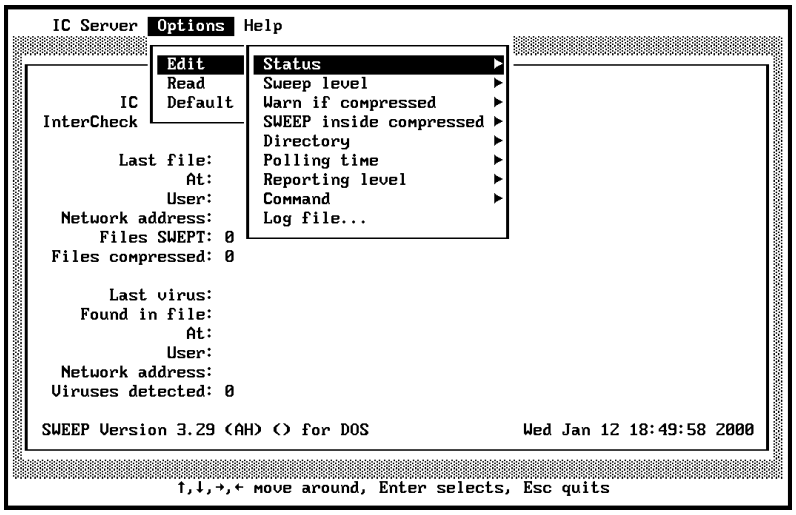
You can test communication between ICONTROL and the selected InterCheck Server. Select *Test* from the *IC Server* menu. See 'Testing communications' in the 'ICONTROL for Windows' section above.

Zeroing counters

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

Setting InterCheck Server options

To configure the InterCheck Server, select *Edit* from the *Options* menu.



You can set parameters such as scanning level, polling times and reporting levels. These parameters are equivalent to those in the *Options* menu of ICONTROL for Windows (see the 'ICONTROL for Windows' section above).

Restoring last saved options

Select *Read* from the *Options* menu to set the options to those specified in the InterCheck Server configuration file, i.e. restore them to their last saved values.

Restoring default options

Select *Defaults* from the *Options* menu to set the options to their default values.

Command line qualifiers

-BW Display in black and white

Forces display for a black and white monitor.

-CFG=<file> Name of configuration file

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

-CO Colour monitor

Forces display for a colour monitor.

-MO Monochrome monitor

Forces display for a monochrome monitor.

-P.. Path through menus

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

```
ICONTROL -P120^04
```

1 Selects *Options* menu.

2 Selects *Default*.

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

^ Escapes to the top menu bar.

0 Selects *IC Server* menu.

4 Selects *Exit* to exit from ICONTROL.

Treating viral infection

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

Recovery from a virus attack

Recovery from a virus attack involves two stages:

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

Eliminating viruses

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

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

If using SWEEP from the GUI (Graphical User Interface), specify automatic disinfection at the Job Configuration pages. See the 'Action' section of the 'Configuring Sophos Anti-Virus' chapter.

If using SWEEP from the command line, or if automatic disinfection is deselected, consult the sections below. These explain how to prepare for disinfection and how to deal with each kind of infected item.

Preparing to deal with viral infection

Before attempting to deal with infected boot sectors, shut down the system and restart it in stand-alone mode, as described in the 'Running programs stand-alone' section below.

This may also be necessary to deal with infected executable files which are locked, such as some system files.

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

What you will need

You will need the following for stand-alone working:

- A set of OS/2 Utility disks.
- The 'Emergency OSWEEP' disk.
- The 'Emergency Virus Data' disks you have created.

These are the disks created before Sophos Anti-Virus was first installed (see the 'Creating an emergency disk set' chapter).

Running programs stand-alone

1. If OS/2 is already running, shut it down.
2. Boot OS/2 from the OS/2 Utility disk set. Follow the on-screen instructions. When booting is finished, the A: prompt appears. Remove the OS/2 Utility disk.

Dealing with boot sector viruses on the hard disk

There are two ways to deal with boot sector viruses on the hard disk: disinfection or replacing the boot sector.

Disinfection

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

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

Place the 'Emergency OSWEEP' disk in the A: drive.

At a command prompt, type

```
A:\OSWEEP -DI -CI
```

Press *Enter*.

The -DI qualifier instructs SWEEP to disinfect any infected items. -CI checks the integrity of the copy of SWEEP on the 'Emergency OSWEEP' disk.

After checking program integrity, the computer will ask for the virus data disk. Remove the 'Emergency OSWEEP' disk and place the first virus data disk in drive A:. You will be prompted for the second virus data disk.

The computer is scanned for boot sector and file viruses. Boot sectors are disinfected and infected executables are reported (see the 'Dealing with infected executable files' section).

When disinfection is complete, re-boot OS/2 from the hard disk and scan the whole computer for infected documents.

Important! SWEEP must be run directly from the 'Emergency OSWEEP' disk. Otherwise disinfection will fail.

Replacing the boot sector

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

Follow the steps in the 'Running programs stand-alone' section above. Check that the contents of the infected drive are visible (e.g. with DIR).

Important! If the contents of the hard disk are not visible, contact Sophos technical support for advice. Some boot sector viruses require additional action for full recovery.

To overwrite the master boot sector:

Ensure the last OS/2 Utility Disk is in the drive. Enter:

```
FDISK /NEWMBR
```

or, in the case of Warp Server for e-business

```
LVM /NEWMBR
```

To overwrite the OS/2 boot sector:

Locate the OS/2 Utility disk containing the file SYSINSTX.COM.

- For Warp 3 and Warp Server v4, this will be the third of the three Utility disks.
- For Warp 4 (Merlin) and Warp Server for e-business, this will be the first of the four Utility disks.

Insert this disk in drive A: and enter a command such as:

```
SYSINSTX C:
```

Dealing with boot sector viruses on floppy disk

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

Disinfection

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

Place the 'Emergency OSWEEP' disk in the A: drive.

At a command prompt, type

```
A:\OSWEEP A: -DI -MU
```

The computer will ask for the virus data disk. Remove the 'Emergency OSWEEP' disk and insert the first virus data disk. You will be prompted for the second virus data disk.

Boot sectors are disinfected and infected executables are reported (see the 'Dealing with infected executable files' section).

When disinfection is complete, re-boot OS/2 from the hard disk and scan the whole computer for infected documents.

Reformatting

Follow the steps in the 'Running programs stand-alone' section above. Copy the valuable data from the infected disk to a clean destination (it is safe to copy files if the PC has been clean booted) and reformat the infected disk.

Dealing with infected executable files

Attempting to disinfect executables is inadvisable because it is impossible to ensure that executables are properly restored after disinfection. Restored files may be unstable, putting valuable data at risk.

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

Locate all the infected executables and delete them using

```
OSWEEP -REMOVEF
```

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

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

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

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

Dealing with infected documents

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

To disinfect a document file, use a command such as

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

In some cases, it is possible to manually edit the macros from the infected document using the relevant application. However, some macro viruses now operate a form of stealth to prevent users from doing this. For example, *Winword/ShareFun* prevents the use of the Tools/Macro and File/Templates menu options. Please consult Sophos technical support before attempting to perform manual disinfection of macro viruses.

Boot Manager

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

If the OS/2 Boot Manager is infected:

Follow the steps in the 'Running programs stand-alone' section.

Ensure the last OS/2 Utility Disk is in the drive. Then use the OS/2 FDISK (or LVM) utility to delete and reinstall the Boot Manager. Detailed instructions are in IBM's OS/2 documentation.

Recovering from virus side-effects

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

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

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

Sometimes data can be recovered from disks damaged by a virus. Sophos can also supply utilities for repairing the damage caused by some viruses. Contact Sophos technical support for advice.

After disinfection

After a virus attack, consider the following measures:

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

Troubleshooting

This chapter provides answers to common problems.

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 depends on the configuration of the machine and the sizes of the files being examined, but typically the 'quick' level is 5 to 10 times faster than the 'full'.

See the 'Mode' section of the 'Configuring Sophos Anti-Virus' chapter (if using the GUI version), or the 'Full Sweep' section in the 'Configuring CLI Sophos Anti-Virus' chapter (if using the command line version).

Checking archive files

If checking of archive files is selected, every archive will be unpacked to the depth specified. Scanning may therefore take much longer than if this option is not selected.

Checking all files or all sectors

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

Virus fragment reported

The report of a virus fragment indicates that part of a file matches part of a virus. There are two 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 virus fragment is reported, contact Sophos technical support for advice.

False positives

SWEEP may very occasionally report a virus in a file that is not infected. This may happen if a sequence of bytes in a normal program matches part of a known virus (some polymorphic viruses deliberately include code resembling that in normal programs).

If in doubt, contact Sophos technical support for advice.

To decrease the chance of false positives:

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

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 website.

Further help needed

On the website 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 website.

By email to support@sophos.com

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

By telephone on +44 1235 559933

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

Appendix: Making floppy disk sets

This chapter describes the steps you need to take if you want to install Sophos Anti-Virus on an OS/2 computer without a CD drive.

What to do if you are a floppy disk user

If you want to install Sophos Anti-Virus on a computer with no CD drive, you must:

- Copy the necessary files (which are in archive form) from the Sophos CD onto floppy disks.
- Extract the files from floppy disk onto the OS/2 computer and run them.

Follow the instructions overpage.

Making floppy disks

At a computer that does have a CD drive, insert the Sophos Anti-Virus CD.

Enter

```
F:
cd\diskimgs
```

where F: is the CD drive.

To copy the program for creating emergency disks, you enter

```
cpesdos2 A: format
```

where A: is the floppy disk drive.

You are prompted to enter floppy disks. If the disks are not blank, they will be formatted (after confirmation).

To copy the Sophos Anti-Virus installation program, you enter

```
cpsavos2 A: format
```

where A: is the floppy disk drive.

You are again prompted to enter floppy disks.

When disk creation has finished, use the disks as described in the next section.

Using the floppy disks

Take the floppy disks to the machine where you are going to make emergency disks or install Sophos Anti-Virus.

Change to a directory on the hard disk where you can make a temporary sub-directory. For example:

```
C:
cd\temp
```

To extract the program that creates emergency disks, insert the floppy disk 'esdos2.exe'. Enter

```
A:\esdos2
```

This creates a sub-directory called esdos2. Change to this directory

```
cd esdos2
```

Then run the `mkstand` program, as described in the 'Creating an emergency disk set' chapter.

To extract the Sophos Anti-Virus installation program, insert the floppy disk 'savos2'. Enter

```
A:\savos2
```

This creates a sub-directory called savos2. Change to this directory

```
cd savos2
```

Then run the setup program, as described in the 'Installation on a network' or 'Installation on a single machine' chapter.

Glossary

ASCII: American Standard Code for Information Interchange; the standard system for representing letters and symbols.

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

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

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

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

Checksum: A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered.

CMD: The extension given to 'command' file names in OS/2. A command file may be written in the OS/2 scripting language REXX, or may simply contain a series of OS/2 commands. STARTUP.CMD is a special command file which is executed whenever OS/2 is started, and can be used to configure OS/2 to a user's requirements.

COM: The extension given to a type of executable file in MS-DOS. A COM file is similar to an EXE file, but can only contain up to 64K of code and data.

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 Boot Sector: The boot sector which loads the BIOS and DOS into PC RAM and starts their execution.

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

Extended DOS Partition: An area of the hard disk assigned to DOS. It is usually subdivided into logical disks. The first logical disk can be made bootable though this is not usual.

FAT: File Allocation Table; a mnemonic term used by the MS-DOS operating system (and others) to describe the part of a disk which contains information describing the physical location on the disk of the chains of clusters forming the files stored on that disk.

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

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

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

IDE: The extension given to a file containing a virus identity encoded with Sophos's Virus Description Language (VDL). It will appear as a string of ASCII characters.

InterCheck: Proprietary Sophos technology which ensures that unknown files and disks cannot be accessed until checked for viruses.

InterCheck Server: Component of InterCheck (q.v.) that provides central reporting and, for certain networked workstations, on-access scanning.

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

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

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

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

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

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

Memory-resident Virus: A virus which stays in memory after it has been executed and infects other objects when certain conditions are fulfilled. Non-memory-resident viruses are active only while an infected application is running.

MS-DOS: The Disk Operating System sold by Microsoft. It operates on the IBM PC.

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

OS/2: An operating system for 80386+ based IBM compatibles. It allows true multi-tasking.

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

Partition Table: A 64-bit table found inside the master boot sector on hard disks which contains information about the starting and ending of up to four partitions on the hard disk. The partition table also contains information on the type of the partition, e.g. DOS partition, Unix partition etc.

Polymorphic Virus: Self-modifying encrypting virus.

Primary DOS Partition: A portion of the hard disk assigned exclusively to DOS. It is usually the bootable partition for DOS.

Stealth Virus: A virus which hides its presence from the PC user and anti-virus programs, usually by trapping interrupt services.

SWEEP: The component of Sophos Anti-Virus that provides immediate and scheduled virus scanning and disinfection.

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

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

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

Virus Identity: An algorithm describing various characteristics of a virus and used for virus recognition. Sophos describe viruses using the proprietary Virus Description Language (VDL).

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

Index

Q

R

S

T

U

V

W

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

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

Tel +44 1235 559933 • Fax +44 1235 559935

14.02.2001

Technical support hotline:

Email support@sophos.com

UK:	**Tel (+44) 1235 559933 (24 hrs)**
USA:	**Tel (+1) 781 213 3456**
Australia:	**Tel (+61) 2 8217 7111**
France:	**Tel (+33) 1 41 99 94 40**
Germany:	**Tel (+49) 6136 91193**