## Viruses and Windows NT

At the time of writing, there are no known Windows NT specific viruses. However, Windows NT is widely used on file servers for DOS-based workstations and is therefore a target for DOS viruses which can replicate and infect DOS programs on Windows NT machines. Windows NT allows the running of DOS programs, and so a virus attached to a DOS program can also run. Even though the ability of many DOS based parasitic viruses to infect other programs, especially Windows NT specific programs, is restricted, the side effects are still likely to function. In addition, most boot sector viruses are PC viruses, rather than DOS viruses, and as such will be able to infect PCs irrespective of the operating system they are running. Furthermore, macro viruses will infect documents on any operating system supported by the relevant application.

## How SWEEP can help

Computer viruses often include side-effects, which can range from the relatively harmless to the decidedly malicious. Viruses can spread widely before these side-effects are seen, so it is vital to detect and eliminate them as soon as possible. This is SWEEP's main purpose.

SWEEP for Windows NT:

- Checks local hard disks, floppy disks and networks for the presence of all viruses known to Sophos at the time of SWEEP's release, including Macintosh viruses in the files stored on the server.
- Is updated twelve times a year, and urgent updates can be distributed by fax or email or downloaded from the Sophos web site.
- Easily detects polymorphic viruses using Sophos' advanced Virus Description Language (VDL) and a built-in code emulator.
- Scans inside compressed files.
- Detects Microsoft Word and Excel macro viruses.
- Incorporates Sophos' proprietary InterCheck client-server virus detection technology, which allows the use of server-based software for checking workstations.
- Offers two levels of security, allowing a 'quick sweep' which looks for virus identities in parts of executables likely to contain a virus, and a 'full sweep' which looks for virus patterns in every part of every executable.
- Is easy to use, yet easily integrated into complex virus-checking applications, such as the automated unattended checking of file servers.
- Features an 'immediate mode' which allows checking on demand, along with a 'scheduled mode' which allows multiple scheduled jobs to be configured for automatic operation, even when no-one is logged in to the machine.
- Can notify network managers of the discovery of a virus automatically, via the event log, network messages, and SMTP email.
- Includes an extensive on-line virus information database.
- Is a 32-bit application and is fully Windows NT compliant.

SWEEP is also available for DOS/Windows, Windows 95, Novell NetWare, OpenVMS (VAX & Alpha AXP), OS/2 and Banyan VINES.

# SWEEP and Windows NT services

Access to all objects on a Windows NT system is controlled, and all processes must have a Security Identifier (SI) in order to execute. Without an SI it would be impossible to authorise the use of files by a process, memory or any other part of the Windows NT system. Under normal use, a process inherits the SI of its parent, so any process started interactively by a user will have the same SI as that user.

A Windows NT service is a program that operates independently of users, and runs even when no users are logged in to the system. However, services must still be authenticated and login in their own right. By default, new services login using a System account, which is a built-in security account for system processes. The System account has access to all local resources but does not have any rights to access shares on remote computers.

SWEEP has two main components: the SWEEP service engine which includes all SWEEP and InterCheck functionality along with the scheduler, and the Graphical User Interface for the SWEEP service engine. It is important to distinguish between the two. The SWEEP engine can be running as a service independently of any users, even if the interface is not running. The GUI interface allows a specific user to control the SWEEP engine, depending on their user privileges. The SWEEP scheduler will have the same file access rights as the SWEEP service, even when accessed through the SWEEP GUI. Therefore, if you wish to use the SWEEP scheduler to sweep networked files, you will not be able to use the System account, but will have to use an account having both rights to read the networked resources to be checked as well as local Administrator rights. The account used by the SWEEP service is determined when SWEEP is installed, but can be changed at a later date.

# Updating SWEEP

*Updating SWEEP*

Registered users of SWEEP are sent updated SWEEP disks in the first week of every month. SWEEP for Windows NT’s ‘auto-upgrade’ facility makes installing these upgrades simple.

*Urgent SWEEP updates*

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

Centralised distribution of IDE files

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

IDE files and the InterCheck client

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

# Using SWEEP

## Overview of the SWEEP display

*The menu and toolbar*

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

*The immediate, scheduled and InterCheck mode tabbed pages*

The immediate, scheduled, InterCheck server, and InterCheck client mode tabbed pages. The immediate mode page is displayed on start-up, and contains the file list along with the progress indicator for immediate operation. The scheduled and InterCheck tabbed pages will not be available if the user running the GUI is not an Administrator. The IC Client and IC Server tabbed pages will not be available if SWEEP was not installed as an InterCheck client and InterCheck server respectively.

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

*On-screen log*

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

## Immediate mode

*Starting an immediate sweep*

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

Any other individual item in the immediate mode display can be swept by double-clicking on its icon in the file list.

*Default immediate mode file list*

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

*Adding new items for immediate sweep*

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

- path name
- file types
- subfolders

*Removing items from immediate sweep*

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

*Editing an item for immediate sweep*

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

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

Only those files defined as executables will be swept, unless the ‘All’ file types option is selected.

Subfolders will be swept if this option is selected.

## Scheduled mode

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

*Default scheduled mode job list*

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

*Adding a new scheduled job*

To add a new scheduled job, press *Add* on the scheduled mode page. You will be prompted for a job name, and will then be presented with the scheduled mode configuration page as described in Configuring SWEEP.

*Removing a scheduled job*

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

*Editing a scheduled job*

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

## InterCheck server mode

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

### *Activating the InterCheck server*

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

## InterCheck client mode

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

### *Activating the InterCheck client*

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

## Closing down the SWEEP GUI

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

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

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

## SWEEP services

Open the Windows NT Control Panel and double-click the *Services* icon to display the Services dialog.

*SWEEP for Windows NT*

This is the SWEEP service used to run SWEEP independently of the graphical user interface. The user account used by this service determines what parts of the network can be accessed by scheduled sweeps.

*SWEEP for Windows NT Network*

This account is used by the SWEEP auto-upgrade facility to check for newer versions of SWEEP on the network. It is also used by the InterCheck logging messaging module to access the InterCheck server’s COMMS directory.

*Changing the SWEEP service user accounts*

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

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

*Starting and stopping the SWEEP service user accounts*

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

## Using the InterCheck monitor

*Starting the InterCheck monitor*

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

To start the InterCheck monitor under Windows NT 4 at any other time, click *Start*, click *Programs,* click the *Sophos SWEEP* folder, and then click *InterCheck Monitor*.

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

*Overview of the InterCheck monitor display*

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

*Using the InterCheck monitor*

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

- Always on Top: if selected, the InterCheck monitor window remain above all other windows.
- No title: if selected, the InterCheck monitor window title bar will disappear. To restore the title bar, double-click inside the InterCheck monitor window.
- Sophos SWEEP: select *Sophos SWEEP* to start SWEEP for Windows NT.

## Configuring SWEEP

*About configuring SWEEP*

Select *Configuration* from the *Options* menu or click the associated icon to call up the configuration page for the mode whose tabbed page is currently displayed.

Immediate, scheduled, IC Client and IC Server modes are configured independently.

*Sweeping mode (immediate, scheduled, IC Client & IC Server modes)*

- sweeping level
- priority
- compressed files
- include Macintosh viruses
- add scan results to central checksum file

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

- disinfect boot sectors
- disinfect documents
- infected files
- request confirmation

*Reporting results (immediate & scheduled modes)*

The report file contains information about individual immediate or scheduled jobs, and is aimed at the user. It is generated in addition to the continuous log file, which is aimed at the administrator. Note that the report file is written as the GUI user for immediate sweeps and as the service user for scheduled sweeps.

- report mode
- report file

*File list (scheduled mode only)*

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

Note that the files available for sweeping in the scheduled mode might not be the same as those available in the immediate mode. This is because the scheduled sweep runs with the SWEEP service's user rights. The login user of the SWEEP service is determined when SWEEP is installed, and might not be the same as the current user. It is recommended that networked resources are referred to by UNC filenames because mapped drives are only available when a user is logged in to the machine. The browse control will only show those files and directories to which the scheduled SWEEP service has access.

*Time (scheduled mode only)*

SWEEP can be configured to run at particular times on specific days of the week, for example, once a day on weekdays and twice a day at weekends.

- run job on boot

*Check (IC Client mode only)*

- files
- removable media

*Exclusions (IC Client mode only)*

- files exclusions
- volume exclusions

The ‘quick’ sweeping level only checks the parts of files likely to contain viruses, while the ‘full’ level examines the complete contents of each file. The ‘full’ level is more secure because it can discover viruses ‘buried’ underneath other code appended to a file, as well as minor virus mutations and corruptions. However, ‘full’ sweeping level is much slower, and for normal operation ‘quick’ sweeping is generally sufficient.

To minimise SWEEP’s impact on system performance it can be set to run at ‘low’ priority. This will increase the time taken to sweep the system. This option is not available in IC Client mode.

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

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

Any file found to be virus-free can be checksummed and added to the server’s central checksum file. Networked InterCheck clients can use this central checksum file in addition to their own local checksum file, thereby eliminating the need for multiple checking and authorisation of identical items. This option is not available in IC Client mode.

SWEEP can disinfect most boot sector viruses from floppy disks. SWEEP for Windows NT will not disinfect a hard disk's boot sector. To disinfect a hard disk boot sector, boot from a clean floppy disk and use the CLI version of SWEEP. See the on-line virus library for specific details on individual viruses. This option is not available in IC Server mode.

SWEEP can remove the viral macros from documents infected with certain types of macro viruses. If the document disinfection fails, the infected file will be dealt with in the same way as any other infected file. This option is not available in IC Server mode.

If an infected file is found, there are several actions that can be taken to make that file safe. Renaming or moving an executable file should prevent it from being run, but deleting or shredding the file will ensure that it cannot be accidentally executed. Shredding is a more secure type of file deletion that overwrites the contents of the file. Note that the only option available in IC Server mode is to copy infected files.

If this option is selected, any action that involves changing infected items (i.e. disinfecting boot sectors, disinfecting documents, and renaming, deleting, shredding and moving infected files) will ask for confirmation before proceeding. This option is only available in immediate mode, where it is enabled by default.

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

The report file will be saved to disk.

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

Check all operations on files: By default, the InterCheck client will check all files opened. ‘Defined in executable list’ will check those files defined as executables, via *Executables* from the *Options* menu. ‘Automatically detect as executable type’ checks all files accessed, irrespective of their extension, looking at the structure of the file to determine whether they should be checked. The ‘Automatically detect as executable type’ option is primarily for determining whether a file is an OLE document which should be checked for macro viruses, such as a Word document which might not have the extension DOT or DOC.

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

Allow access to drives with infected boot sectors: If selected, the InterCheck client will allow access to drives with infeced boot sectors. This might be useful to enable files to be copied off a floppy disk infected with a boot sector virus. Note that a boot sector virus will only infect a computer if that computer is booted from the infected disk.

Apply file exclusions: The file exclusions are specified by *Exclusion List* from the *Options* menu.
Exclude checking of remote files: If selected, the InterCheck client will not check files on network drives.

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

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

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

## SWEEP alert message options

*About SWEEP alert message options*

Select *Alerts* from the *Options* menu or click the associated icon to display the notification configuration pages.

Each notification control page shares a number of common features: disable notification, job specification, and notification level.

*Event logging*

- disable notification
- job specification
- notification level

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

*Network messaging*

- disable notification
- job specification
- notification level
- recipient computer

*SMTP e-mail*

- disable notification
- job specification
- notification level
- recipient e-mail

*Desktop messaging*

- disable notification
- mode
- message

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

*InterCheck logging*

- disable notification
- job specification
- notification level
- path to InterCheck server

SWEEP needs a user account to log in to the network. It will use the same account that the auto-upgrade facility uses to check for newer versions of SWEEP, or if one is not set it uses the SYSTEM account. See Changing the SWEEP service user accounts for more information on changing the user account.

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

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

If the ‘All jobs’ option is selected, all configuration options for that form of notification will apply to the immediate mode, all scheduled jobs, and (where available) the InterCheck mode. The ‘Specific jobs’ option allows the immediate mode, each individual scheduled job and the InterCheck mode to have different notification configuration settings. If a specific job is not explicitly configured, it will inherit the settings of the <default> job.

There are three forms of notification message that can appear in the alerts: virus found messages, error messages, and general information messages such as the time a job was started. The alerts can include none of these, just the virus messages, the virus and error messages, or all three forms of message. The notification level setting will not affect the level of information placed in the report file, the on-screen log or the log file.

This will cause SWEEP to send a network message to the named machines or users. Note that only one machine can be notified under each name, so if a user name is specified, and that user is logged on to two machines, they will only receive the message at the first machine. This is due to limitations in the Lan Manager messaging system. For this reason it is recommended to use machine names as recipients rather than user names. Note also that in order for Windows 95 or Windows for Workgroups PCs to receive messages, they must be running the WinPopup application.

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

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

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

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

```
\\ServerName\SWEEP\COMMS
```

## The virus library

*Starting the virus library*

Select *Virus Library* from the *View* menu or click the associated icon to start the on-line virus library.

*Information on a particular virus*

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

*Searching for a particular virus*

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

- infected objects
- memory resident
- disinfectable by SWEEP
- trigger conditions
- text in description

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

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

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

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

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

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

# SWEEP options

## Set log folder

SWEEP maintains a continuous log of all of its activity. This log file contains administrative messages along with the messages described in Virus detected messages and Error messages, and is aimed at the administrator. It is generated in addition to the report file, which is aimed at the user.

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

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

By default the log file will be saved in the root folder of the first local hard drive, but this can be changed by clicking *Set Log Folder* from the *File* menu.

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

This option is only available to administrators.

### Executables

The list of file extensions to be treated as executables by SWEEP can be edited with this option. This list is only used if SWEEP is set to check ‘executable’ rather than ‘all’ file types.

This option is only available to administrators.

### Exclusion list

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

This option is only available to administrators.

### Restore defaults

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

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

### Clear log

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

### Progress bar

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

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

# Treating viral infection

### Establishing a clean environment for disinfection

A virus can be eliminated from the memory of an infected PC by switching the PC off and booting from an uninfected (and preferably write-protected) system disk. This is called performing a secure bootstrap or a clean boot, and is essential to providing a safe environment from which the disinfection process can begin.

Assuming the computer’s memory is free from viruses, it is safe to move or copy infected files.

### Treating infected floppy disks

If a virus is discovered on a floppy disk that has just been received, then it is relatively easy to deal with.

Infected files and documents can be automatically renamed, deleted, shredded, moved or copied if SWEEP has been configured to do so.

Floppy disks infected with boot sector viruses can normally be disinfected automatically by SWEEP. However, if SWEEP does not disinfect the boot sector, data can be safely copied off the disk and the disk reformatted. Formatting a floppy disk destroys all the data that is stored on it, including any viruses.

The source of the infected disk should then be established to locate any other infected disks.

*Important!* If just one infected floppy escapes disinfection other disks and PCs could be reinfected.

*Note:* It is advisable to preserve a clearly marked infected floppy for analysis and evidence.

## Treating infected hard disks

If SWEEP discovers a virus on a hard disk, it is likely that the infection is widespread and considerably more work may be required to recover from the virus attack. The first step is to identify all infected PCs and disks.

The next step involves stopping the virus from spreading. Infected PCs should be disconnected from the network and all disk interchange between PCs suspended.

After the virus outbreak has been contained, the recovery process can begin. The virus has to be eliminated from all the infected floppy disks, as described above, as well as from infected hard disks.

If the hard disk only contains infected files, then these can be dealt with as described above.

However, if the boot sector of the hard disk is infected, then SWEEP for Windows NT will not disinfect it. You should use the DOS version of SWEEP after a clean boot. See the DOS SWEEP user manual for more details, or contact Sophos' technical support.

## After disinfection

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

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

# Troubleshooting

## SWEEP runs slowly

*Full sweep*

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

*Checking all files*

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

*Network drives selected*

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

*Progress bar selected*

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

### False positives

When SWEEP reports a virus pattern or identity match, it has almost certainly discovered a virus. However, there is a small chance that the contents of a virus-free program may be identified as a virus. This is due to the fact that polymorphic viruses (which change their appearance on every infection) are deliberately written to look like normal programs.

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

Options and actions which increase the chance of false positives are:

- Sweeping all files.
- Full sweeping.

## False negatives

A false negative is the opposite of a false positive, i.e. the event in which SWEEP fails to report a virus in an infected file.

*Unknown viruses*

Any virus-specific software will discover only those viruses which were known to the manufacturer at the time of software release. If you suspect you have discovered a virus unknown to SWEEP, please send Sophos a sample as soon as possible. There is a good chance that the virus is ‘in the wild’ and the sooner that it gets incorporated into SWEEP, the better.

You can also upload the infected sample onto our secure bulletin board (+44 1235 559936) or our ftp site (ftp.sophos.com). When the virus has been analysed (which may take from 10 minutes to a few days), we will fax or email you the IDE file which can be used to update SWEEP.

# On-screen log messages

### Virus detected messages

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

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

Virus:  'virus name' detected in location
        File deleted

Virus:  'virus name' detected in location
        File renamed to filename

Virus:  'virus name' detected in location
        File shredded

Virus:  'virus name' detected in location
        File moved to new location

Virus:  'virus name' detected in location
        File copied to new location

Virus:  'virus name' detected in location
        Error action

Virus:  'virus name' detected in location
        Has been disinfected

Virus:  'virus name' detected in location
        Error: Disinfection failed

Virus:  'virus name' detected in location
        InterCheck request at time
        User user
        Node network address
        No action taken

Virus:  'virus name' detected in location
        InterCheck request at time
        User user
        Node network address
        File copied to new location

Virus:  'virus name' detected in location
        InterCheck request at time
        User user
        Node network address
        Error copying to location

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

## Error messages

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

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

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

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

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

Error:  Could not open filename

Error:  Could not read filename

Error:  Sector size of drive drive is too large

Error:  Could not open report file filename/directory

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

# On-screen log pop-up virus detected messages

This is SWEEP’s ‘virus detected’ message. It contains the name and the location of the virus. The ‘virus detected’ message will be followed by information about the action taken. This action will depend on the settings on the Action tab of the Configuration page.

The *location* will be one of either:

*filename*
Drive *drive name*: Sector *sector number*
Disk *disk* Cylinder *cylinder* Head *head* Sector *sector*
Memory block at address *8 digit hex address*

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

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

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

The infected file has been deleted and cannot be recovered.

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

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

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

The *action* will be one of either:

```
deleting file
renaming to filename
shredding file
moving to location
copying to location
```

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

SWEEP for Windows NT can automatically disinfect, or remove, certain boot-sector viruses on floppy disks if the ‘disinfect boot sector’ option has been selected. SWEEP for DOS will be required to disinfect a hard disk boot sector.

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

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

This is InterCheck’s ‘virus detected’ message. It contains the name and location of the virus, along with the time it was discovered, the name and network address of the user who found it, and a summary of the action taken. The action depends on the settings on the Action tab on the InterCheck Configuration page.

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

The *message* contains the text of the report.

# On-screen log pop-up error messages

This is an error reported by the InterCheck client software.

The description of the error will be contained in the `message`.

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

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

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

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

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

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

SWEEP will only currently sweep disk sectors of 2k or less. It is highly unlikely that it will ever encounter larger sectors.

SWEEP needs to allocate memory for the report if it is to send it to the users on the notification list. If the report is too big then SWEEP will not be able to load it into memory to send it. The report file can become very large if it is configured to list every file that it examines.

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

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

## What is InterCheck?

SWEEP with InterCheck technology offers on-access virus checking, while SWEEP alone offers on-demand checking. InterCheck ensures that unknown files (e.g. programs, documents, email attachments or Internet downloads) and disks cannot be used until checked for viruses.

InterCheck splits the task of virus detection between a client and a server. The **InterCheck client** determines whether items on the client workstation should be checked for viruses, while in a networked environment the **InterCheck server** performs the actual virus checks where necessary.

There are two main types of InterCheck client: networked and stand-alone. A **networked InterCheck client** exists on a separate machine from the InterCheck server, and communicates with it over the network. A **stand-alone InterCheck client** does not have to communicate with a remote InterCheck server, and uses a local installation of SWEEP to check for viruses.

A networked InterCheck client is easier to administer and uses fewer system resources on the client workstations. A stand-alone InterCheck client generally offers faster initial authorisation of files, and can also be used on machines not always connected to the network. Either way, InterCheck is the most efficient way of protecting users from viruses - each item is checked for viruses only once, unless it is modified in which case it is rechecked.

### How does InterCheck work?

The InterCheck client software monitors all file and disk accesses. Whenever an item is accessed, it is compared with a list of authorised items. If a match is found the access is permitted. If a match is not found, the networked InterCheck client sends a copy of the item to the InterCheck server for checking, while the stand-alone InterCheck client checks with a local installation of SWEEP.

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

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

## Features

### Complete cover

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

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

### Performance

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

### Automatic reporting

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

### Easy administration

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

### Portable PCs

InterCheck clients can continue to provide the same levels of protection even when a PC is not connected to the network.

## Overview of InterCheck installation and configuration

Networked InterCheck clients require a separate InterCheck server. This involves installing SWEEP and the InterCheck software on the file server, and running SWEEP in InterCheck server mode. Networked InterCheck clients are currently available for DOS, Windows 3.x, Windows for Workgroups, Windows 95 and Macintosh workstations.

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

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

*InterCheck server installation and configuration*

**Windows NT, NetWare, OpenVMS, OS/2 & Banyan VINES**

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

**DOS**

See the SWEEP for DOS InterCheck Supplement.

*Stand-alone InterCheck client installation*

**Windows 3.x & Windows for Workgroups**

See the ‘Installing InterCheck clients’ chapter of the InterCheck server user manuals.

**Windows 95 & Windows NT**

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

*Networked InterCheck client installation*

**DOS, Windows 3.x, Windows for Workgroups, Windows 95 & Macintosh**

See the ‘Installing InterCheck clients’ chapter of the InterCheck server user manuals.

*Stand-alone InterCheck client configuration*

**Windows 3.x, Windows for Workgroups & Windows 95**

See the ‘Configuring InterCheck clients’ chapter in the InterCheck server user manuals, and also in the SWEEP for Windows 95 user manual.

**Windows NT**

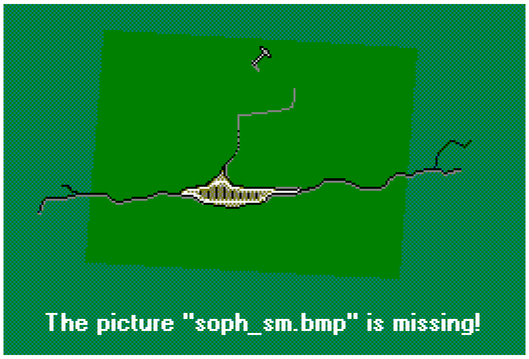
See the ‘Configuring SWEEP’ chapter of the SWEEP for Windows NT user manual.

*Networked InterCheck client configuration*

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

See the ‘Configuring InterCheck clients’ chapter of the InterCheck server user manuals.

# About Sophos Plc.



Sophos Plc was founded in 1980, moved into data security in 1985, and is now a world leader in the development of software for data security and computer virus detection. At the centre of this success is a reputation for innovative and sophisticated products backed by quality support. Sophos currently exports to 27 countries through a network of international distributors.

All Sophos products are designed, manufactured and supported at our base near Oxford in England. These products include:

- "SWEEP" virus detection utility.
- "D-FENCE" disk authorisation software.
- "VACCINE" checksumming virus detection system.
- "EDS" file encryption package for DOS and Windows.

# Contacting Sophos

**Email**

General enquiries:
enquiries@sophos.com

Sales enquiries:
sales@sophos.com

Technical support:
support@sophos.com

Comments on manuals, on-line help, etc.:
publications@sophos.com

**Sophos Plc, UK**

Phone +44 1235 559933

Fax +44 1235 559935

Sophos Plc.
The Pentagon
Abingdon Science Park
Abingdon
OX14 3YP
England

**Sophos Inc, USA**

Phone +1 617 932 0222

Fax +1 617 932 0251

Sophos Inc.
18 Commerce Way
Woburn
MA 01801
USA

**BBS** +44 1235 559936

**FTP** ftp.sophos.com

**WWW** http://www.sophos.com/

## What is a computer virus?

A computer virus ‘infects’ programs and disks by attaching copies of itself to them:

- A boot-sector virus will infect the boot sector of disks.
- Parasitic, companion, link and macro viruses infect files.
- Multi-partite viruses can infect both files and boot sectors.

A PC or disk is said to be infected if it contains an infected boot sector and/or one or more infected files. A PC’s memory is said to be infected if it contains some form of memory resident virus.

There are three ways in which a PC and a PC’s memory can become infected:

- The PC is bootstrapped from a disk infected with a boot-sector or multi-partite virus.
- An infected program file is executed, e.g. by issuing its filename as a command at the command prompt, or by double-clicking its icon within Windows.
- A file infected with a macro virus is loaded into the application which ‘executes’ the relevant macro language.

See Sophos’ *Data Security Reference Guide* for more information on viruses.