Configuring Sophos Anti-Virus

This section shows the options which you can configure. These options are all available from the Options and View menu on Sophos Anti-Virus toolbar located on the **GUI**.

Configuration options

Mode
Action
Report
File List
Time
Check (Windows NT only)
Exclusions (Windows NT only)

Alert options

InterCheck logging (Windows NT only)
Desktop messaging
Event logging (Windows NT only)
Network messaging(Windows NT only)
SMTP email
MAPI email (Windows 95/98 only)

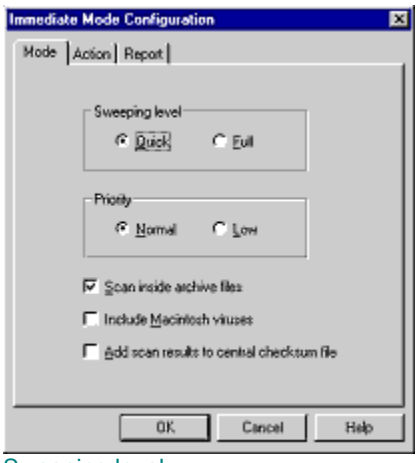
Other options

Executables
Exclusion list
Restore defaults
Clear log
Purge checksums (Windows NT only)
Security (Windows NT only)
Progress bar

Mode page

Mode

This configuration page allows you to configure the scanning activity of Sophos Anti-Virus. It is available for all tabbed pages available in the main Sophos Anti-Virus interface.



Sweeping level
Priority
Scan inside archive files
Include Macintosh viruses (Windows NT only)

Add scan results to central checksum file (Windows NT only)

Back to **Configuration menu**

subheadings within **mode**

Sweeping level

Quick and Full scanning levels are available.

Quick checks only those parts of each file that are likely to contain viruses. For normal operation, Quick scanning should be sufficient.

Full examines all the contents of each file. Full is more secure as it can discover viruses buried beneath code attached to a file, virus mutations and corruptions.

Note: Full is slower than the Quick option.

Choose Quick or Full scan.

Back to **Mode**

Back to **Configuration menu**

Priority

To minimise the impact of Sophos Anti-Virus on the performance of your system, you can set it to run at Low priority. This setting will however increase the time Sophos Anti-Virus takes to scan the system.

Choose high or low priority.

Back to **Mode**

Back to **Configuration menu**

Scan inside archive files

Sophos Anti-Virus is capable of looking for viruses inside compressed files.

Note: InterCheck provides automatic protection from viruses in files which have been compressed because access to every unrecognised item (e.g. a newly decompressed file) is only granted after that item has been checked for viruses.

Place a check in the box if you want Sophos Anti-Virus to scan the contents within compressed files.

Back to **Mode**

Back to **Configuration menu**

Include Macintosh viruses (Windows NT only)

Sophos Anti-Virus for Windows NT is capable of looking inside Macintosh files. If this option is enabled, Sophos Anti-Virus checks *all* executables irrespective of their file extensions.

Place a check in the box if you want Sophos Anti-Virus to scan Macintosh files.

Back to **Mode**

Back to **Configuration menu**

Add scan results to central checksum file (Windows NT only)

Any file Sophos Anti-Virus declares safe can be added to the central **checksum** file. Workstations that run InterCheck from the file server will use this file as well as their own local checksum file. This approach eliminates multiple checks and authorisations of identical files.

Place a check in the box if you want Sophos Anti-Virus to add clean files to the central checksum file.

Note: This option is only available if InterCheck has been installed.

Back to **Mode**

Back to **Configuration menu**

ACTION PAGE

Action

The Action configuration page is available for all tabbed pages (excluding the SAVI tabbed page) located on the Sophos Anti-Virus **GUI**. Some configuration pages will have particular Action options greyed out.

Disinfect boot sectors
Disinfect documents
Infected files

Request confirmation

Back to **Configuration menu**

subheadings within Action page

Disinfect boot sectors

There are two types of boot sectors:

Floppy disk boot sectors

Sophos Anti-Virus can disinfect most boot sector viruses found on floppy disks.

Hard disk boot sectors

Sophos Anti-Virus will *not* automatically disinfect them. You need to disinfect hard disk boot sectors manually. See manual disinfection

Place a check in the box ‘Disinfect boot sectors’ to deal with infected boot sectors.

Back to **Action**

Back to **Configuration menu**

Disinfect documents

Sophos Anti-Virus can disinfect certain infected documents (files that contain **macros**).

If the document disinfection fails, the infected document will be dealt with like any other infected file found on your system. See Infected files.

Place a check in the box beside ‘Disinfect documents’ if you want Sophos Anti-Virus to deal with infected documents. See manual disinfection.

Back to **Action**

Back to **Configuration menu**

Infected files

An infected file can be made safe in several ways:

- renaming or moving will reduce the likelihood of someone running an infected executable. These options will *not* purge the file.
- deleting or **shredding** will ensure the file cannot accidentally be opened or executed. Shredding is the most secure option. These options destroy the file.

Place a check in the box beside ‘Infected files’ and select the action you want Sophos Anti-Virus to take. See manual disinfection.

Back to **Action**

Back to **Configuration menu**

Request confirmation

Sophos Anti-Virus can request confirmation prior to proceeding with any action that involves changing infected items.

This option is only available for the Immediate job. It is enabled by default.

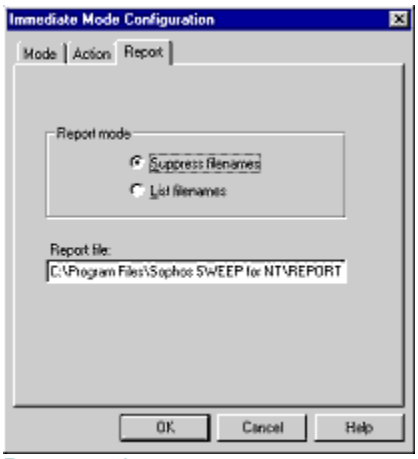
Back to **Action**

Back to **Configuration menu**

Report page

Report

This page can be configured by users, allowing them to create a log of their Scheduled and Immediate scanning activity.



Report mode
Report file

Back to **Configuration menu**

subheadings within report page

Report mode

Choose ‘Suppress filenames’ to avoid logging examined items.

Choose ‘List filenames’ to log all scanned items.

Back to **Report**

Back to **Configuration menu**

Report file

By default, the report file is found in the Sophos Anti-Virus folder under Reports. This location can be changed by the user, if desired.

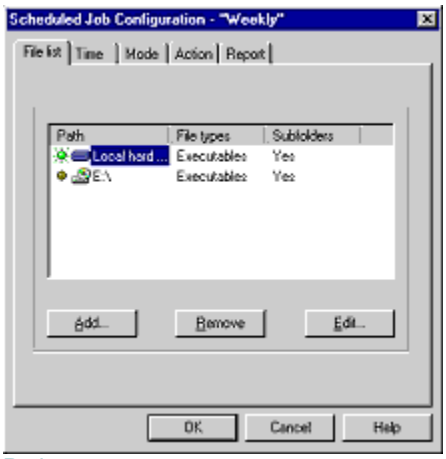
Back to **Report**

Back to **Configuration menu**

File List

File list

The file list shows the drives, directories and files that can be scanned on demand (immediate and scheduled jobs). The list can be specified by the user.



Path
File types
Subfolders

Back to **Configuration menu**

subheadings within File list page

Path

Path shows the location of the files or directories you want to scan.

Back to **File List**
Back to **Configuration menu**

File types

File types can be either Executables or All files.

Back to **File List**
Back to **Configuration menu**

Subfolders

If you want the subfolders of the items in the Path scanned, place a check in the box beside Subfolders.

Back to **File List**
Back to **Configuration menu**

Time page

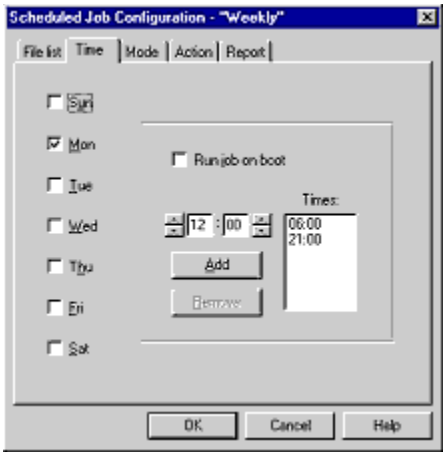
Time

Sophos Anti-Virus can be configured to schedule jobs at particular times on specific days of the week.

Add time

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

By default, Sophos Anti-Virus carries out a virus check whenever the computer is booted and at 21:00 daily for Windows NT or at 13:00 for Windows 95/98.



Run job on boot

Back to **Configuration menu**

subheadings within Time page

Run job on boot (Windows NT only).

Place a tick in the box beside ‘Run job on boot’ to set the highlighted job to scan every time your computer is booted.

Back to **Time**

Back to **Configuration menu**

Check page

Check (Windows NT only)

This page allows you specify which file types InterCheck will check.

Files
Removable media

Back to **Configuration menu**

Files

Place a check in the box beside ‘Defined in executable list’ to check files defined as executables. See Executables.

Place a check in the box beside ‘Automatically detected as executable type’ to check files likely to be executable according to their structure and irrespective of their extensions.

Back to **Check**

Back to **Configuration menu**

Removable media

Place a check in the box beside ‘Check boot sectors when disk first accessed’ if you want InterCheck to check the boot sectors of all removable media when they are first used.

Place a check in the box beside ‘Allow access to drives with infected boot sectors’ if you want access to these infected drives. This option is allows you to copy files off a floppy disk infected with a boot sector virus.

IMPORTANT! Do not boot a computer with an infected disk. This action may infect your computer.

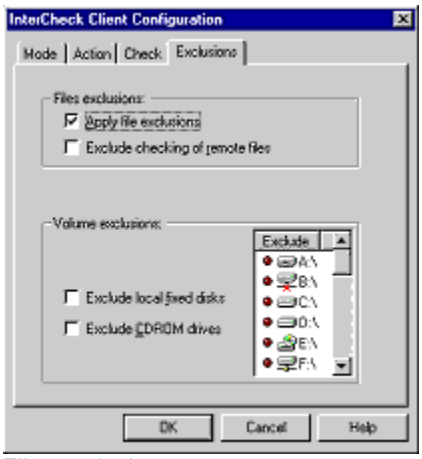
Back to **Check**

Back to **Configuration menu**

Exclusions page

Exclusions (Windows NT only)

This configuration page is available when the IC Client tabbed page is selected. You can select the files to exclude from InterCheck checking.



Files exclusions
Volume exclusions

Back to **Configuration menu**

Files exclusions

Place a check in the box beside ‘Apply file exclusions’ to inform InterCheck to not scan those files excluded from Immediate and Scheduled jobs. The Exlcusions list is found under the Options menu item.

Place a check in the box beside ‘Exclude checking of remote files’ to exclude files located on networked drives.

Back to **Exclusions**

Back to **Configuration menu**

Volume exclusions

Displayed is a list of all possible **drive mappings**, irrespective of whether the mapping is valid for a particular use. InterCheck will NOT check any of the selected drives.

Place a check in the box beside ‘Exclude local fixed disks’ to exclude all local fixed disks, irrespective of whether they are specified in the volume exclusions display.

Place a check in the box beside ‘Exclude CDROM drives’ to exclude all CD drives, irrespective of whether they are specified in the Volume exclusions display.

Back to **Exclusions**

Back to **Configuration menu**

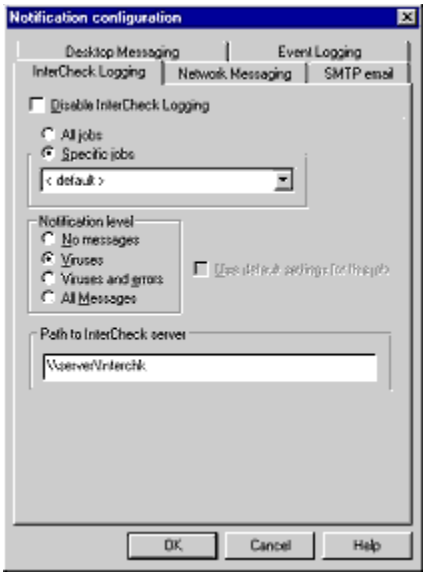
Alerts: InterCheck logging

InterCheck logging (Windows NT only)

Workstations can send messages to the COMMS directory of an InterCheck Server.

Messages will be logged on the InterCheck Server and may generate additional alerts.

This option can be tailored for specific jobs (i.e. you can specify which type of message is recorded for each job).



Notification level
Path to InterCheck Server

Back to **Configuration menu**

Path to InterCheck server

You must specify a **UNC** path name

For example:

```
\\ServerName\INTERCHK\COMMMS
```

Back to **InterCheck logging**

Back to **Configuration menu**

Alerts: desktop

Desktop messaging

For Windows NT, Desktop Messaging controls the messages displayed when a virus is discovered when the **GUI** is not active,.

For Windows 95/98, Desktop messaging is not available if the GUI is not active.

Notification level
User defined message

Back to **Configuration menu**

Alerts: notification level

Notification level

Select the appropriate notification level.

No messages

Viruses

Viruses and errors

All messages

Back to **Configuration menu**

User defined message

Any message added here by the user will be added to the end of the standard virus detected message.

Back to **Desktop messaging**
Back to **Configuration menu**

Alerts: Event logging

Event logging (Windows NT only)

Event Logging allows the administrator to specify the type of notification added to the Windows NT Event Log.

This option can be tailored for specific jobs (i.e. you can specify which type of message is recorded for each job).

Notification level

Back to **Configuration menu**

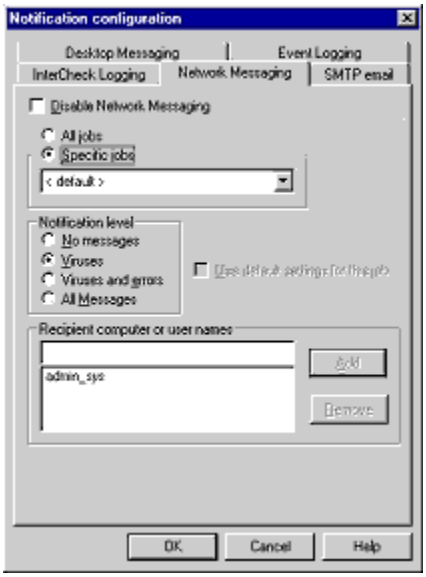
Alerts: network messaging

Network messaging (Windows NT only)

You can configure Sophos Anti-Virus to send a network message to named computers and usernames.

This option can be tailored for specific jobs (i.e. you can specify which type of message is recorded for each job).

Note: Windows 95/98 users networked to a Windows NT server will have to run WinPopup application in order to receive messages.



Notification level

Recipient computer or user names

Back to **Configuration menu**

Recipient computer or user names

Due to limitations in the LAN Manager messaging system, only one message is delivered per computer name or username. So, even if a username is logged into several computers, only the first computer will receive the message.

As a result, we recommend you enter computer names rather than usernames.

Back to **Network messaging**

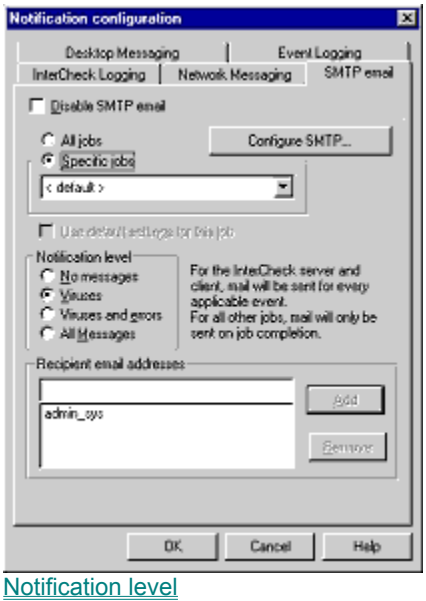
Back to **Configuration menu**

Alerts: SMTP

SMTP email

You can add and remove the email addresses for the recipients of the notification messages. Click Configure **SMTP** to enter the host name or **IP** address of the SMTP server.

This option can be tailored for specific jobs (i.e. you can specify which type of message is recorded for each job).



Notification level

Recipient email addresses

Configure SMTP

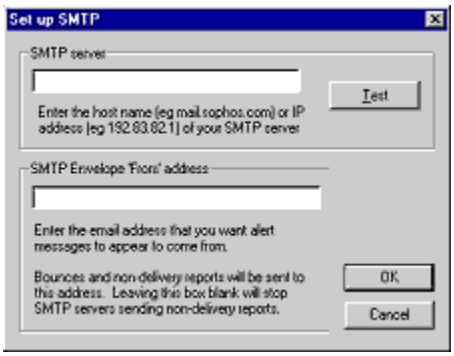
Back to **Configuration menu**

Recipient email addresses

You can add and remove the email addresses for the recipients of the notification messages.

Back to **Configuration menu**

Configure SMTP



SMTP server

You can enter the **IP** address of your **SMTP** server here.

SMTP envelope “From” address

Enter the address you want the notification messages to appear to come from. Consider that a recipient might want to reply to a notification message, so select an address for a mailbox that will be checked regularly.

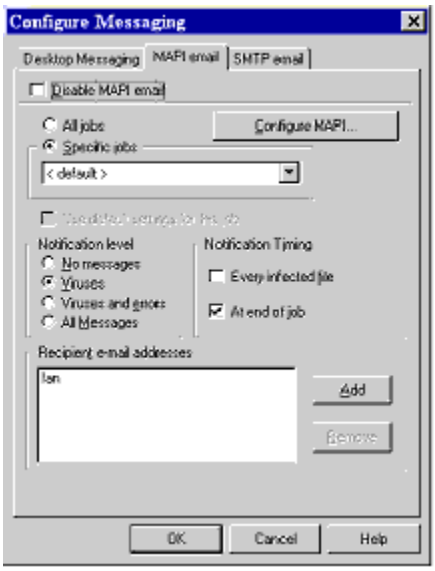
Back to **SMTP email**

Back to **Configuration menu**

MAPI email (Windows 95/98 only)

MAPI email creates, manipulates, transfers, and stores e-mail messages.

When Sophos Anti-Virus detects one or more viruses, the MAPI email option can send a notification message.



Notification level

Recipient email addresses

Notification Timing

Back to **Configuration menu**

Notify timing

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

Back to **MAPI email**

Back to **Configuration menu**

Other Dialogues

Executables

This list shows which types of executables will be scanned by Sophos Anti-Virus if the configuration is set to scan executable files only. The current list of executables can be modified.

Back to **Configuration menu**

Exclusion list

Enter any files you want to exclude from all Immediate and Scheduled jobs. InterCheck will also have these files excluded by default.

To not include the exclusion list in the InterCheck settings, go to the Exclusion configuration page . Remove the check in the box' Apply file exclusions'.

Note: Available from the IC Client tabbed page only

Back to **Configuration menu**

Restore defaults

This option will set all Sophos Anti-Virus settings back to their defaults after requesting confirmation.

Note: Performing this change will destroy all Scheduled jobs.

For the user, this option will affect only their own Immediate scanning settings. For Windows NT, administrator rights are needed to restore defaults.

Back to **Configuration menu**

Clear log

The **On-screen log** provides a record of activity in the current session and a record of all the scheduled and , for Windows NT users, InterCheck 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.

Back to **Configuration menu**

Purge checksums (Windows NT only)

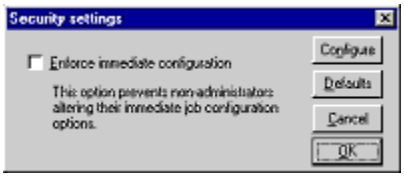
Two **checksum** files can be maintained: the central checksum file (items authorised by the InterCheck server for use on workstations) and the local checksum file (items authorised by the local installation of InterCheck).

Both these checksum files will be purged if this option is performed.

Back to **Configuration menu**

Security (Windows NT only)

Place a check in the box beside Enforce immediate configuration if you want to prevent users (non-administrators) from changing their Immediate job configuration.



Click Configure if you want to change any settings of the Administrator Defined User Mode Configuration.

Back to **Configuration menu**

Progress bar

The progress bar is a visual aid, showing how much of the current job has been completed.

Sophos Anti-Virus has to count the items to be scanned before it can display the progress bar correctly. As a result, scanning time can be increased.

On large network drives, time can be saved by disabling this option. Any Sophos Anti-Virus jobs that are already running will be unaffected.

Note: The progress bar is set separately for Immediate and Scheduled tabbed pages.

Back to **Configuration menu**

About alert messaging

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

Disable notification

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

Job specification

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

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

Notification level

There are four levels of notification to choose from:

No message; virus detected message; virus detected and error messages; or all messages, including information such as the time a job as started.

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

InterCheck logging

Desktop messaging

Event logging

Network messaging

SMTP email

Back to **Configuration menu**

Use SAV

Sophos Anti-Virus main interface

The Sophos Anti-Virus **GUI** consists of icons, **tabbed pages**, and an On-screen log.

If you click on any of the icons below, a pop-up description will appear.



Up to five tabbed pages can appear on the GUI. They represent the different scanning modes available.Click on any of the links to jump to more information about that tabbed page:

Immediate tabbed page

Scheduled tabbed page

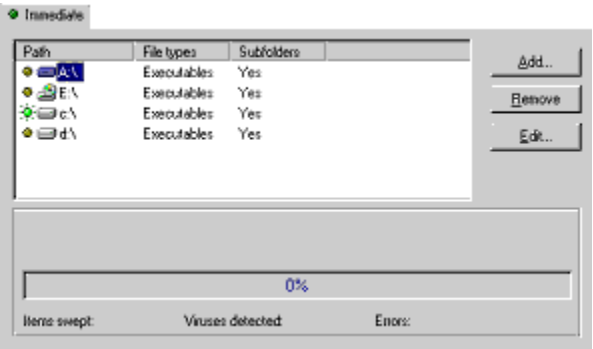
IC Server tabbed page(NT only)

IC Client tabbed page(NT only)

SAVI tabbed page

The On-screen log contains information about the current session, along with (if you are logged on as an administrator) all the scheduled and InterCheck log messages reported since the service was started.

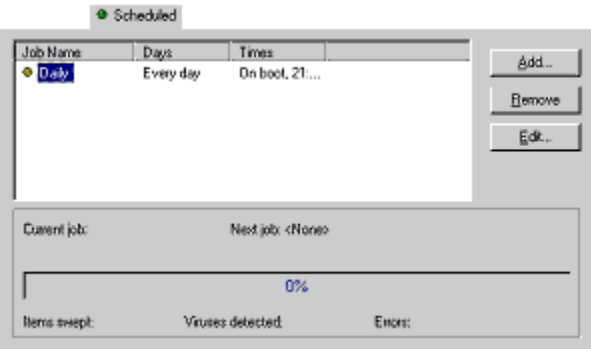
Immediate tabbed page



The Immediate mode is displayed on start-up. You can add an item by clicking Add. You can remove or edit the entries within the **File List** by highlighting a particular item and clicking the Remove or Edit button as appropriate. The **active lights** show currently selected items for scanning.

Back to **Sophos Anti-Virus GUI**

Scheduled tabbed page



By default, Sophos Anti-Virus carries out a virus check whenever the computer is booted and at 21:00 daily for Windows NT and at 13:00 for Windows 95/98.
You can add a scheduled job by clicking Add. You can remove or edit a scheduled scan within the **File List** by highlighting a particular job and clicking the Remove or Edit button. The **active lights** show which jobs are currently selected items for scanning.
Specify the files or directories to be scanned at File List tabbed page and the scanning times at the Time tabbed page.

Note: The scheduled tabbed page is always available for Windows 95/98 users and for users logged on as administrators using Windows NT.

Back to **Sophos Anti-Virus GUI**

IC Server tabbed page (Windows NT only)

The InterCheck Server, a component of Sophos Anti-Virus that is normally run on a file server, collects and logs virus reports from networked workstations running Sophos Anti-Virus.
InterCheck Server also provides on-access scanning for those workstations configured to run networked installations of InterCheck.
This tabbed page shows whether the InterCheck Server is active and gives details of scanning activity.

Administrators can start, stop and configure the InterCheck Server.

Note: Ensure that InterCheck Server has been installed.

Back to **Sophos Anti-Virus GUI**

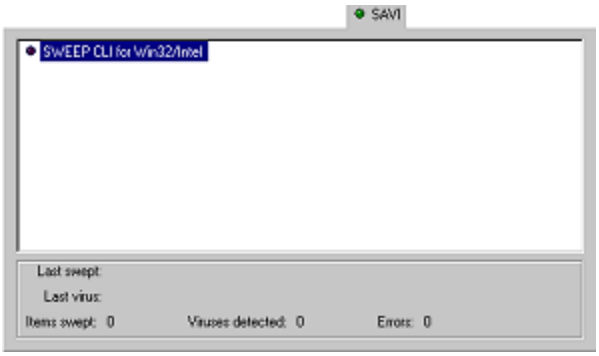
IC Client tabbed page (Windows NT only)

InterCheck, a component of Sophos Anti-Virus, ensures that unknown files (e.g. programs, documents, email attachments or Internet downloads) and disks cannot be accessed until they are checked for viruses.
This tabbed page shows whether the InterCheck Client is active and gives details of scanning activity. Administrators can start, stop and configure the InterCheck Client.

Note: Ensure that InterCheck Client has been installed.

Back to **Sophos Anti-Virus GUI**

SAVI tabbed page (Windows NT only)



If an administrator has at any time run a third party application which uses SAVI (Sophos Anti-Virus Interface), another tabbed page will appear. This tabbed page lists SAVI aware applications and displays runtime information.

Back to **Sophos Anti-Virus GUI**

Sophos

Sophos Plc was founded as an electronic design partnership in 1980, moved into data security in 1985, and is now a world leader in the development of anti-virus and data security software. At the centre of this success is a reputation for innovative and sophisticated products backed by quality support.

All Sophos products are designed, manufactured and supported by the company, which exports world-wide through a network of subsidiaries and international distributors. These products include:

- Sophos Anti-Virus, comprising SWEEP for on-demand scanning and InterCheck for on-access scanning.
- D-FENCE disk authorisation and encryption software.
- VACCINE checksumming virus detection system.
- E-DES file encryption package for DOS and Windows.

Sophos Anti-Virus

Contact Sophos

Sophos Anti-Virus

Sophos Anti-Virus can perform the following:

on-demand scanning

scheduled scanning

on-access scanning

automatic reporting

disinfection

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.
- InterCheck checks each item as you try to access it and grants access only if it is virus-free.

Back to **Sophos**

Contact technical support

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

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

By email to support@sophos.com

Questions can be sent to Sophos by email. Please include as much information as possible, including SWEEP and InterCheck version (a version number accompanies each release), operating system and patch level, and the exact text of any error messages.

By telephone on +44 1235 559933

Sophos offers 24-hour, 365-day telephone technical support.

Contact Sophos

World Wide Web

www.sophos.com.

Email

General Enquiries
enquiries@sophos.com

Sales Enquiries
sales@sophos.com

Technical support:
support@sophos.com

Phone and Fax

UK and international:
Phone +44 1235 559933
Fax +44 1235 559935

Australia:
Phone +02 9212 1600
Fax +02 9212 1788

France:
Phone 01 46 92 24 42
Fax 01 46 92 24 00

Germany:
Phone 06136 91193
Fax 06136 911940

USA:
Phone 781 213 3456
Fax 781 213 54661

Postal addresses

Sophos Plc, UK:
The Pentagon, Abingdon Science Park, Abingdon, Oxfordshire, OX14 3YP, England.

Sophos Pty Ltd:
Level 4, 725 George Street, Sydney, NSW 2000, Australia.

Sophos Plc, France:
2, Place de la Défense, BP 240, 92053 Paris la Défense, France.

Sophos GmbH, Germany:
Am Hahnenbusch 21, D-55268 Nieder-Olm, Germany.

Sophos Inc, USA:
50-S Audubon Road, Wakefield, MA 01880, USA.

Back to **Sophos**

Troubleshooting

Troubleshooting

This section provides answers to some common problems which can be encountered when using Sophos Anti-Virus.

Auto-updating fails to happen

Updated files are not in central directory

Ensure that the **central update** is made to the central installation directory on the file server where local installations of Sophos Anti-Virus will look for updates.

Insufficient rights to installation directory

Auto-upgrading uses the SWEEP for Windows NT Network service. This service needs to be registered as an account which has sufficient rights to access Sophos Anti-Virus's central installation directory. See the 'Managing the SWEEP services' chapter of the Sophos Anti-Virus for Windows NT manual, which is located on the CD under Documentation. The central installation directory must also have the SETUP.EXE and WSWEEPNT.CFG files present.

Note: This section is for Windows NT users only.

Back to **Troubleshooting**

False positives

Sophos Anti-Virus may very occasionally report a virus in a file that is not infected. Indeed, some polymorphic viruses are deliberately written to look like normal programs.

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

To decrease the chance of false positives:

- Only check executables. See Executables.
- Perform a ‘quick sweep’ rather than a ‘full sweep’. See Sweeping level.

Back to **Troubleshooting**

InterCheck Server runs slowly (Windows NT only)

A high volume of virus-checking requests from workstations will slow the InterCheck Server. Files waiting to be checked are stored in the InterCheck Server's COMMS directory.

Note: A network can have more than one InterCheck Server, and InterCheck can be run locally on some or all workstations rather than from the file server.

Back to **Troubleshooting**

New viruses

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

If a virus unknown to Sophos Anti-Virus is suspected, please send Sophos a sample and a description as soon as possible. If it is a virus, Sophos Anti-Virus 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.

Back to **Troubleshooting**

SWEEP runs slowly

Full sweep

The speed difference between Full and Quick scanning depends on the configuration of your machine, but typically Quick level is 5 to 10 times faster than Full option. Sophos Anti-Virus will run on Quick by default.

Checking all files

By default, Sophos Anti-Virus will check only files defined as executables. If Sophos Anti-Virus is checking all files, the process will take longer.

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, Sophos Anti-Virus will have to count all the items that are to be scanned. This job can take several minutes on large network drives.

Back to **Troubleshooting**

Virus fragment reported

The report of a virus fragment indicates that a part of a file matches a 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 virus. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active.

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 Sophos Anti-Virus will report ‘Virus fragment’ rather than ‘Virus’. A corrupted virus cannot spread.

If a virus fragment is reported, contact Sophos technical support for advice.

Back to **Troubleshooting**

Virus not disinfected

Sophos Anti-Virus may report that a virus has not been disinfected. In this case:

- Check that 'Disinfect documents' is selected.
- If dealing with a disk or removable media, make sure that it is not write-protected.
- If dealing with files on an **NTFS** volume, make sure that SWEEP has sufficient access rights.

Note: Sophos Anti-Virus will not disinfect a virus fragment, because it has not found an exact virus match.

Back to **Troubleshooting**

On-screen log messages

Virus detected messages

DoubleClicking on a line with a virus name will display more information about that virus.

- 'virus name' detected in **location**
  No action taken
- 'virus name' detected in location
  File deleted
- 'virus name' detected in location
  File renamed to filename
- 'virus name' detected in location
  File shredded
- 'virus name' detected in location
  File moved to new location
- 'virus name' detected in location
  File copied to new location
- 'virus name' detected in location
  Error action
- 'virus name' detected in location
  Has been disinfected
- 'virus name' detected in location
  Error: Disinfection failed
- 'virus name' detected in **location**
  InterCheck request at time
  User user
  Node network address
  No action taken
- 'virus name' detected in location
  InterCheck request at time
  User user
  Node network address
  File copied to new location
- **report source** report:
  Message
  At time
  User user
  Node network address
- 'virus name' detected in location
  InterCheck request at time
  User user
  Node network address
  Error copying to location

Error messages

- **InterCheck report:**:
  Message
  At time
  User use
  Node network address
- **Invalid InterCheck request received in file:**
  file
  At time
  User user
- **Corrupted InterCheck request received in file:**
  file
  At time
  User user
- **InterCheck version is newer than this version of SWEEP:**
  Please upgrade this copy of SWEEP.
- **Could not start InterCheck:**
  Could not open InterCheck marker file filename
  At time
- **Could not open filename:**
- **Could not read filename:**
- **Sector size of drive is too large:**
- **Could not open report file filename /directory:**
- **Log file filename could not be opened:**
  Log data will not be saved.
- **Password protected file:**
- **Could not allocate memory for *filename/folder*:**

React with virus warning

Virus disinfection

If Sophos Anti-Virus reports a virus, disinfection facilities are available:

Automatic disinfection

Manual disinfection

Automatic disinfection

In most cases, Sophos Anti-Virus can deal with infected items automatically, provided that it is configured properly. See the Action tabbed page for more information.

Sophos Anti-Virus can

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

Back to **Virus disinfection**

Manual disinfection

In some cases, where automatic disinfection is deselected or a boot sector is infected, manual disinfection may be necessary.

The exact manual disinfection process may also depend upon the specific virus, so consult the Sophos Virus Library before attempting disinfection.

Boot sector

Master boot sector virus on hard disk

Partition boot sector virus on hard disk

Boot sector virus on floppy disk

Executables

Viruses in executables

Documents

Viruses in documents

Back to **Virus disinfection**

Master boot sector virus on hard disk

If the hard disk is infected with a boot sector virus, Sophos Anti-Virus will *not* be able to disinfect it automatically. Ensure that you back up all important data contained on the hard disk.

Reboot the computer with a clean boot disk. Use Sophos Anti-Virus for DOS/Windows 3.x to disinfect the virus e.g. with the command

```
SWEEP -DI
```

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

```
FDISK /MBR
```

If the contents of the hard disk are not visible after a clean boot, contact Sophos technical support for advice. Some boot sector viruses require additional action for full recovery. For example, the *OneHalf* virus encrypts the boot sector so that it is only readable when the virus is in memory.

Back to **Manual disinfection**

Back to **Virus disinfection**

Partition boot sector virus on hard disk

Infected partition boot sectors occasionally require specialist attention. Most viruses are written for DOS and assume the machine has a DOS boot sector instead of a partition boot sector. Contact Sophos technical support for advice.

Back to **Manual disinfection**

Back to **Virus disinfection**

Boot sector viruses on floppy disk

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

Back to **Manual disinfection**

Back to **Virus disinfection**

Viruses in executables

Attempting to disinfect infected executables is generally inadvisable as it is impossible to ensure that the executable has been properly restored after disinfection. The executable may be unstable, putting the valuable data at risk.

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

Back to **Manual disinfection**

Back to **Virus disinfection**

Viruses in documents

You do not need to reboot from a clean boot disk when disinfecting documents.

Important! Ensure that the application that created the infected document is not open when disinfection is attempted.

In some instances, you can manually edit the macros from the infected document using the relevant application. Some **macro** viruses now operate a form of stealth to prevent users from editing a macro. For example, *Winword/ShareFun* prevents the use of the Tools/Macro and File/Templates menu option.

Contact Sophos technical support before attempting to manually disinfect the macro viruses.

Back to **Manual disinfection**

Back to **Virus disinfection**

Recovery from side-effects

Side-effects depend entirely on the virus. Innocuous viruses (*Cascade*) need no recovery while some viruses (*Michelangelo*) involve restoration of the complete hard disk.

Some viruses (*Winword/Wazzu*) will alter your data gradually. These types of changes can be very hard to detect and highly undesirable.

Sound backups are key when recovering from virus side-effects. Originals should be kept on write-protected disks, so any infected programs can easily be replaced by the original clean versions.

Recovering data from virus-damaged disks is occasionally possible. Utilities are available at Sophos. Please contact Sophos technical support.

Back to **Manual disinfection**

Back to **Virus disinfection**

Checksum

A value calculated from item(s) of data which can be used by a recipient to verify that the data has not been altered. Usually 32 or 64 bits long.

GUI

Graphical User Interface The main Sophos Anti-Virus screen from which you can perform on-demand scanning.

Shredding

A very secure type of file deletion that overwrites the contents of the file.

No messages

If selected, no messages will be sent.

Viruses

If selected, only virus messages will be sent.

Viruses and errors

If selected, virus and error messages will be sent.

All messages

If selected, all messages will be sent.

UNC

Universal Naming Convention: a standard system for naming network drives.

STMP

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

IP

Internet Protocol; an internet standard the user applies when communicating with a web application.

On-screen log

Contains information about the current session. The administrator can also have all the scheduled and InterCheck log messages reported since the service was started.

Log file

Contains a continuous log of all of Sophos Anti-Virus activity. This log file contains administrative messages.

Drive mapping

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.

Tabbed Pages

Found on the Sophos Anti-Virus GUI, tabbed pages show the various scanning facilities used by SWEEP and InterCheck.

On-demand scanning

Allows the user to scan items for known viruses.

Scheduled scanning

cans items for known viruses at scheduled times on specified days.

On-access scanning

Occurs automatically, ensuring that each item has been checked for known viruses before it is accessed.

Automatic reporting

Sends alerts when a known virus or a virus fragment is found.

Disinfection

Disinfection of certain items occurs automatically, if selected by the user.

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.

Central update

Places the updated installation files onto a file server, from where working local installations can be updated automatically.

NTFS

NT File System; the file system on Windows NT.

Sophos Virus Library icon

Click this icon to open the Sophos Virus Library for information on viruses and disinfection.

Macro

Instructions in a data file used to carry out program commands automatically. They generally have access to a substantial range of functions such as opening, manipulating and closing of files.

Go icon

Click this icon to scan all selected items in the file list.

Stop icon

Click this icon to stop a scan.

Configuration icon

Click this icon to get to the configuration options.

Alerts icon

Click this icon to get to the alert (notification) options.

Sophos Virus Library icon

Click this icon to launch the Sophos Virus Library. If the icon is greyed out on the GUI, the Sophos Virus Library cannot be located.

File list

Shows the drives, paths and files that can be scanned on demand. The list can be specified by the user.

Active light

means that an item has been selected for scanning.

means that an item has not been selected for scanning.

On-screen log pop-up virus detected messages

Double-clicking on a line with a virus name will display more information about that virus. Sophos Anti-Virus's 'virus detected' message contains the name and location of the virus, followed by information about the action taken.

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 hexadecimal address

No action will be taken if Sophos Anti-Virus 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 extension 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 page.

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

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.

Sophos Anti-Virus can automatically disinfect, or remove, certain boot-sector viruses on floppy disks if the ‘disinfect boot sector’ option has been selected. Sophos Anti-Virus for DOS/Windows 3.x will be required to disinfect a hard disk boot sector. SWEEP can also automatically remove the viral macros from documents infected with certain types of macro viruses.

Sophos Anti-Virus was unable to disinfect the boot sector. See the manual for more information.

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

The ‘virus fragment detected’ message contains the name and location of the virus fragment. The *location* will be one of either:
filename `filename`
Drive `drive name`: Sector `sector number`
Disk `disk` Cylinder `cylinder` Head `head` Sector `sector`

Sophos Anti-Virus does not remove virus fragments.

The report source will be either SWEEP or InterCheck, indicating whether the report comes from the InterCheck software or from Sophos Anti-Virus for DOS/Windows 3.x running on the InterCheck on a local workstation.

The message contains the text of the report.

On-screen log pop-up error messages

This is an error reported by the InterCheck software.

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

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

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

This error message arises when the InterCheck server receives an InterCheck request from a newer and thus incompatible version of the local installation of InterCheck. The solution is to upgrade SWEEP.

InterCheck requires read and write access to its COMMS directory (normally a sub-directory of the SWEEP directory called COMMS) to be able to communicate with the local installation of InterCheck.

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

SWEEP will only currently scan disk sectors of 2kb 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 scans and as the service user for scheduled scans.

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. For Windows NT, note that the log file is written as the service user and not as the GUI user.

If a file is corrupt, this error message suggests that Sophos Anti-Virus encountered a document containing macros some or all of which were corrupt. If a file was encrypted, this error message suggests that Sophos Anti-Virus encountered a password protected document and could not scan it.

About InterCheck

InterCheck

InterCheck, a component of Sophos Anti-Virus, ensures that unknown files (e.g. programs, documents, email attachments or Internet downloads) and disks cannot be accessed until they are checked for viruses.

InterCheck splits the task of file authorisation into two processes:

Monitoring all file and disk accesses

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

Scanning unknown items

If InterCheck does not recognise an item, it sends it for scanning. If the item is virus-free, it is added to the list of authorised items (checksum file) and access is granted. From then on, access to this item is granted immediately unless it has been modified. However, if a virus is found, InterCheck denies access, so the workstation cannot be infected.

Local and networked installations of InterCheck

Local and networked installations of InterCheck

There are two types of InterCheck installation:

Local InterCheck

Local InterCheck has all files scanned on the local machine. It offers fast authorisation of files and can be used on machines not always connected to the network.

Local InterCheck is available for Windows NT, Windows 95/98, Windows for Workgroups and DOS/Windows 3.x workstations.

Networked InterCheck

Networked InterCheck sends unknown files to the InterCheck server on a remote machine for scanning. It is easy to administer and uses few system resources on the workstation.

Networked InterCheck is available for Windows 95/98, DOS/Windows 3.x and Macintosh workstations.

See the appropriate link for InterCheck installation you require:

InterCheck for Windows NT workstations

InterCheck for Windows 95/98 workstations

InterCheck for non-NT workstations on an NT network

Back to **InterCheck**

InterCheck for Windows NT workstations

InterCheck for Windows NT (the Windows NT IC Client) is incorporated in the Sophos Anti-Virus for Windows NT software, and performs all on-access scanning locally.

Running InterCheck

InterCheck for Windows NT starts automatically each time Windows NT is started, before any network connections are made.

InterCheck does not require user input during normal operation. It does not display Requesting authorisation messages.

Back to **Local and networked installations of InterCheck**

Back to **InterCheck**

InterCheck for non-Windows NT workstations on a Windows NT network

Sophos Anti-Virus for Windows NT can provide centralised on-access scanning for non-NT workstations connected to a Windows NT server.

Ensure that the InterCheck server is installed and configure the workstations to run Local or networked installations of InterCheck from the file server.

Note: Many platforms can run local installations of InterCheck. Contact Sophosfor more details.

Back to **Local and networked installations of InterCheck**

Back to **InterCheck**

InterCheck for Windows 95/98 workstations

InterCheck for Windows 95/98 is incorporated in the Sophos Anti-Virus for Windows 95/98 software and performs all scanning locally.

Note: Windows 95/98 workstations on a network can run networked InterCheck, if desired. For details, see *the InterCheck Advanced User Guide* on the Sophos Anti-Virus CD.

Running InterCheck

InterCheck starts automatically each time Windows 95/98 is started, before any network connections are made. InterCheck does not require user input during normal operation.

Back to **Local and networked installations of InterCheck**

Back to **InterCheck**

About InterCheck Server

InterCheck Server

The InterCheck Server, a component of Sophos Anti-Virus that is normally run on a file server, collects and logs virus reports from networked workstations running Sophos Anti-Virus.

InterCheck Server also provides on-access scanning for those workstations configured to run networked installations of InterCheck.

The administrator can choose the level of information sent by the workstations to the COMMS directory of an InterCheck server for logging.

USING: what is?

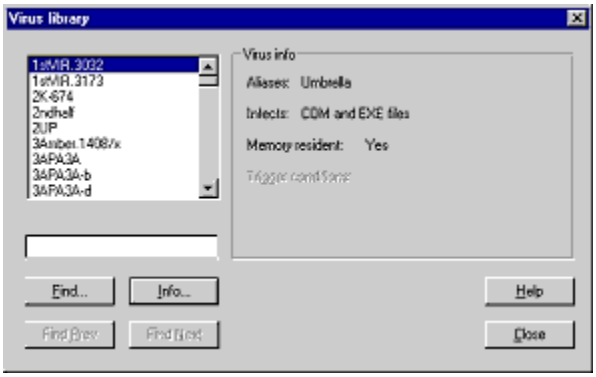
What is the Sophos Virus Library?

The Virus Library holds names and relevant information about viruses. The information contains virus descriptions, virus aliases, trigger conditions, which files are at risk and whether or not SWEEP can disinfect the infected files.

Search where virus name is known
Search where virus name is unknown
Why can’t I find a particular virus?
How do I narrow or widen my search?

USING: How do I?

How do I search for a known virus?



Search where virus name is known

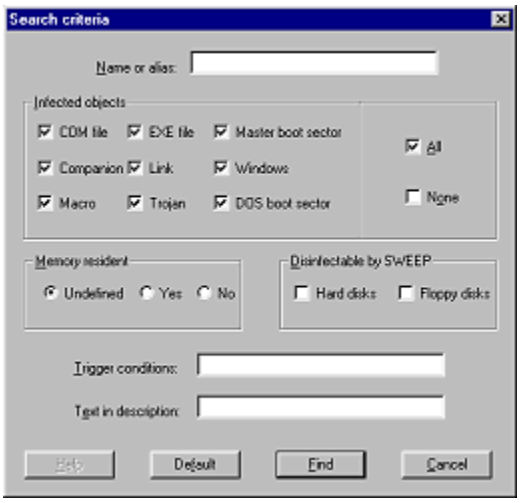
To find out information about a known virus, enter the virus name (or the first few letters of the virus name) in the text box. The virus list will highlight the first virus name (in alphabetical order) that matches your entry. If the highlighted virus was not the one you intended, use the *Find Prev* and *Find Next* buttons to locate the virus — more than one virus may contain the letters you entered.

Important! Sometimes, prefixes are placed before virus names. Ensure that you click *Find Next* until the library locates the name of a particular virus (e.g. the Melissa virus is stored under WM97/Melissa as it infects Word 97 documents).

Once the virus is located, ensure that it is highlighted. In the *Virus info* dialog, an abstract of the virus is available. For more information about the virus, you can click the *Info…* button, or double-click on the virus name.

Back to **main page**

How do I search for an unknown virus?



Search where virus name is unknown

If a virus name is unknown, click the *Find* button, which will open the *Search criteria* dialog.

Here, you can enter letters that you know are in the virus name, you can specify which types of objects the virus infects, whether it is memory resident or not, whether SWEEP can disinfect it or not, any trigger conditions you are aware of , or any descriptive text. These fields are made available to help you narrow your search. They do **not** all have to be filled in.

Once you complete entering the relevant information, click the *Find* button. The virus list will highlight the first virus name (in alphabetical order) that matches your entry. If the highlighted virus was not the one you intended, use the *Find Prev* and *Find Next* buttons to locate the virus — more than one virus may have the letters or characteristics you specified.

Important! Sometimes, prefixes are placed before virus names. Ensure that you click *Find Next* until the library locates the name of a particular virus (e.g. the Melissa virus is stored under WM97/Melissa as it infects Word 97 documents).

If your search was unsuccessful, return to the *Search criteria* dialog and edit your search criteria.

Once the virus is located, ensure that it is highlighted. In the *Virus info* dialog, an abstract of the virus is available. For more information about the virus, you can click the *Info…* button, or double-click on the virus name.

Back to **main page**

How do I narrow or widen my search?

Narrowing a search

If too many virus names that match a partial virus name entry are available, click the *Search* button, which will open the *Search criteria* dialog. By adding any extra information, the search can eliminate similar names that do not meet the correct criteria.

Search where virus name is unknown

Widening a search

If your search did not locate a particular virus name, change the specifications in your search by eliminating some specified criteria. If you know the virus name only in part, eliminate the other criteria and attempt a search with only the partial name. From here, you can add one criterion at a time.

If you are certain that a virus name you are aware of cannot be located in the list, please contact Technical Support at Sophos.

Phone +44 1235 559933
Fax +44 1235 559935

Email support@sophos.com

Back to **main page**

USING: Why can't I?

Why can't I find a particular virus?

It may be that your virus name search is too wide or narrow. See How do I narrow or widen my search? for more information.

If you are certain that a virus name you are aware of cannot be located in the list, please contact Technical Support at Sophos.

Phone +44 1235 559933
Fax +44 1235 559935

Email support@sophos.com

Back to **main page**

Glossary

This section displays links to the Sophos Anti-Virus glossary pages.

Glossary A - H

Boot sector:	Part of the operating system which is first read into memory from disk when a PC is switched on (booted). The program stored in the boot sector is then executed, which in turn loads the rest of the operating system into memory from the system files on disk.
Boot sector virus:	A type of computer virus which subverts the initial stages of the booting process. A boot sector virus attacks either the master boot sector or the DOS boot sector.
Booting-up:	A process carried out when a computer is first switched on or reset, where the operating system software is loaded from disk.
Checksum:	A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered. Usually 32 or 64 bits long.
Compressed file:	See File Compression.
DOS:	Disk Operating System. See MS-DOS.
DOS boot sector:	The boot sector which loads DOS into PC RAM and starts its execution. Common point of attack by boot sector viruses.
File compression:	The compacting of a file through the process of recoding its bit structure into a shorter form.

Back to **Glossary main page**

Glossary I - P

IDE:	The extension given to a file containing a virus identity encoded with Sophos' Virus Description Language (VDL). It will appear as a string of ASCII characters.
InterCheck:	Proprietary Sophos technology which ensures that unknown files and disks cannot be accessed until checked for viruses.
InterCheck server:	The component of InterCheck (q.v.) that provides centralised logging, reporting and updating, and, for certain networked workstations, on-access scanning.
IP address:	A numeric Internet address; a 32-bit binary number, normally written in dotted-decimal notation; e.g. '194.82.145.1'.
Macro virus:	A virus which uses macros in a data file to become active in memory and attach itself to other data files. Unlike conventional viruses, macro viruses can be written relatively easily with little specialist knowledge, and can also attain a degree of platform independence.
Mapped directory path:	A network drive known by its locally mapped name, e.g. the UNC directory path \\MAIN\USERS\ might be mapped to F:\ on one particular computer on the network.
Master boot sector:	The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the PC is booted. It contains the partition table as well as the code to load and execute the boot sector of the 'active' partition. It is a common point of attack by boot sector viruses.
Memory-resident virus:	A virus which stays in memory after it has been executed and infects other objects when certain conditions are fulfilled. Non-memory-resident viruses are active only while an infected application is running.
MS-DOS:	The Disk Operating System sold by Microsoft. It is the most common microcomputer operating system in the world, and operates on the IBM PC.
Multipartite virus:	A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector viruses and parasitic viruses.
NTFS:	NT File System; a Windows NT file system.
Polymorphic virus:	Self-modifying encrypted virus.

Back to **Glossary main page**

Glossary Q - Z

SMTP:	Simple Mail Transport Protocol; the delivery system for Internet email
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
TSR:	Terminate and Stay Resident; a term used to describe an MS-DOS program which remains in memory after being executed. A TSR can be re-activated either by a specific sequence of keystrokes, or at some specific time, or by some specific signal from an I/O port.
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).

Back to **Glossary main page**