SOPHOS

sophos anti-virus

Mac OS 8 or 9

User manual

For network and single users

About this manual

This user manual explains how to use Sophos Anti-Virus for Mac OS 8 or 9 and how to configure

■ virus scanning

■ virus alerts

■ disinfection

■ reporting

■ logging.

The manual also provides help in resolving common problems.

If you are using Mac OS X, refer instead to the *Sophos Anti-Virus Mac OS X user manual*.

For information on the installation, initial setup, updating or uninstallation of Sophos Anti-Virus, see the *Sophos Anti-Virus Mac OS 8 or 9 on a network installation guide* or the *Sophos Anti-Virus Mac OS 8 or 9 single user installation guide*.

Sophos documentation is published on the Sophos CD each month and at www.sophos.com/support/docs/

Technical support

UK (24 hours):	(+44) 1235 559933	support@sophos.com
USA (24 hours):	(+1) 888 767 4679	supportus@sophos.com
Australia (24 hours):	(+61) 2 9409 9111	support@sophos.com.au
France:	(+33) 1 40 90 20 90	support@sophos.fr
Germany (24 hours):	(+49) 6136 91193	support@sophos.de
Italy:	(+39) 02 662810 0	support@sophos.it
Japan (24 hours):	(+81) 45 227 1800	support@sophos.co.jp
Singapore (24 hours):	(+65) 6776 7467	supportasia@sophos.com

FAQs and virus information are available on the Sophos website
www.sophos.com

If you contact technical support, provide as much information as possible, including Sophos software version number(s), operating system(s) and patch level(s), and the exact text of any error messages.

Contents

Using Sophos Anti-Virus

Using the Sophos Anti-Virus window

Disinfection

1 Using the Sophos Anti-Virus window

The section contains the following information about using Sophos Anti-Virus on both standalone and networked Macintoshes.

- Overview of the Sophos Anti-Virus window (section 1.1).

- How to run immediate scans (section 1.2).

- Information about InterCheck (section 1.3).

1.1 Overview of the Sophos Anti-Virus window

1.1.1 Opening the Sophos Anti-Virus window

To open the **Sophos Anti-Virus** window, locate the Sophos Anti-Virus folder created on the workstation during installation. If the default settings were used, this folder is in the root of the startup disk.
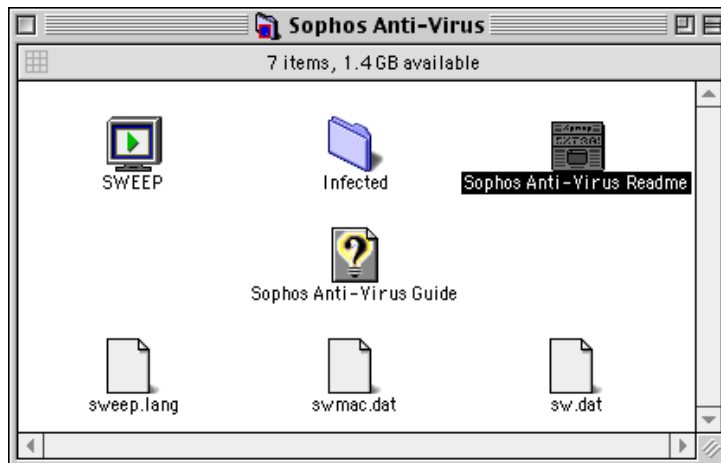
Double-click **SWEEP**.

The **Sophos Anti-Virus** window is displayed.

1.1.2 Features of the Sophos Anti-Virus window
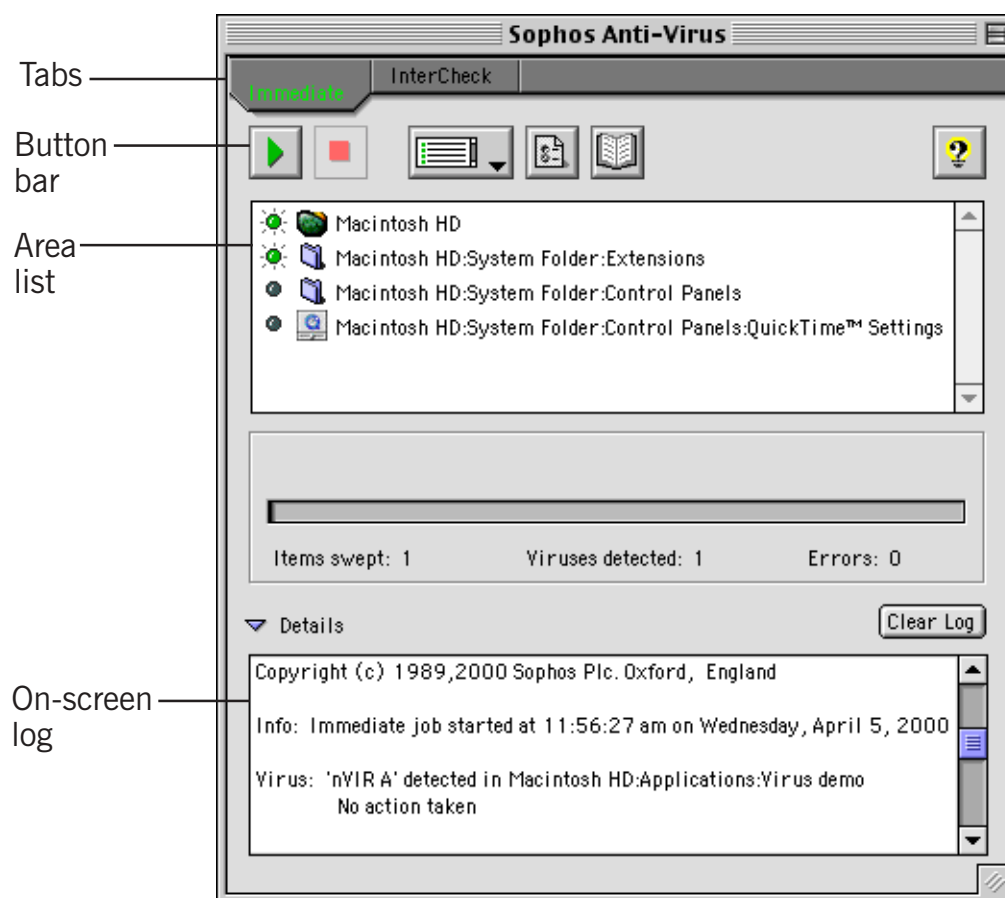
The features of the **Sophos Anti-Virus** window are described below.

Tabs

There is a tabbed page for each type of scan.

- ■ **Immediate** for on-demand scanning.

- ■ **InterCheck** for on-access scanning.

On networked Macintoshes where InterCheck has not been installed, the status on the InterCheck tabbed page is 'Not installed'.

Button bar

▶ Starts scanning.　■ Ends scanning.

▦ Enables you to determine what an immediate scan should check.

▦ Opens a dialog box in which you configure Sophos Anti-Virus.

▦ Connects you to Sophos Virus analyses on the Sophos website.

▦ Opens the help system.

You can also access these functions via the menus or keyboard short-cuts.

Area list

The area list appears only on the **Immediate** tabbed page.

The area list shows items that can be scanned. An illuminated indicator light next to an item shows that it is currently chosen to be included in a scan. Toggle this light to include or exclude the item.

On-screen log

To open the log, click **Details** at the bottom of the window.

The log shows all scans performed, viruses found and errors encountered during the current session. This information is also added to the continuous log (see section 3.10).

To clear the on-screen log, click **Clear Log**.

1.1.3 Closing the Sophos Anti-Virus window

To close the **Sophos Anti-Virus** window, press ⌘-Q.

1.2 How to run immediate scans

1.2.1 Starting an immediate scan

To run an immediate scan, first ensure that the **Immediate** tabbed page is selected.

To scan **all enabled items** (i.e. items selected for scanning) in the area list, click the **Start** button.

To scan **an individual item** in the area list, whether enabled or not, double-click that item.

Drag and Drop scanning

To scan an item without adding it to the area list, drag it from the **Finder** window onto the **Start** button.

Interrupting scanning

To stop scanning at any time, click the **Stop** button.

1.2.2 Adding new items to the area list

By default, all local hard disk(s) and network volumes are included in the area list and are shown as enabled. The area list can be modified as described below.

You can add items to the area list in one of two ways.

Drag and Drop

Select a disk, folder or file and drag it onto the area list. Drag and Drop is the only way to add an individual file.

From the Area list button

1. Click the **Area list** button.

2. Select **Add** from the pop-up menu. A browser window is displayed.

3. Select an item and click the **Select** button below the browser windows.

1.2.3 Removing items from the area list

You can remove an item in one of two ways.

Drag and Drop

Click on the item in the area list to highlight it.

Then drag the item to the Trash or use ⌘-X.

From the Area list icon

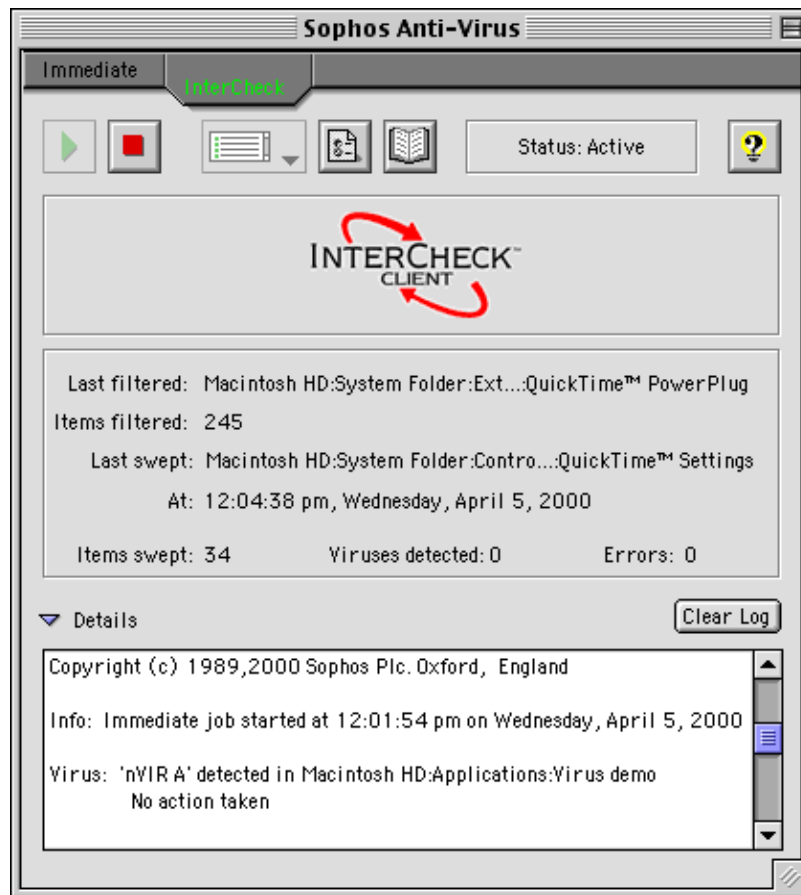Click on an item in the area list to highlight it. Click the **Area list** button

and select **Remove** from the pop-up menu.

1.3 About InterCheck on-access scanning

Once installed, InterCheck on-access scanning is active by default. To monitor, activate or de-activate it, click the **InterCheck** tab.

The **InterCheck** tabbed page displays:

- Status of InterCheck (active, inactive or not installed).

- Last filtered, i.e. last item intercepted and compared with the list of authorised items.

- Items filtered, i.e. number of items intercepted.

- Last swept, i.e. last item scanned for viruses.

- Total items scanned, viruses found and errors.

1.3.1 Activating or de-activating on-access scanning

You can start or stop InterCheck at any time by clicking the **InterCheck** tabbed page, then clicking the **Start** or **Stop** buttons in the button bar.

2 Disinfection

This section provides some general information about disinfection. ***It does not explain how to disinfect a computer of specific viruses***, as disinfection methods are varied and can be virus-specific.

❗ It is recommended that you get information about the virus (see below), then either use the Sophos website for help with disinfection or contact Sophos technical support.

2.1 Getting information about the virus

If Sophos Anti-Virus reports a virus, first isolate the infected computers from the network and internet.

Write down the name of the virus, then, from an uninfected computer, look up its virus analysis on the Sophos website. The virus analysis search page is located at www.sophos.com/virusinfo/analyses.

The analysis tells you what types of file the virus infects, and provides information about disinfection. It may also include a link to detailed disinfection instructions.

If there are no instructions, or if the virus analysis tells you to seek advice, contact Sophos technical support.

2.2 Recovering from virus side-effects

Recovery from virus infection depends on how the virus infected the computer. Some viruses leave you with no side-effects to deal with, others may have such extreme side-effects that you have to restore a hard disk or replace the BIOS in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect. It is therefore very important that you read the virus analysis on the Sophos website, and check documents carefully after disinfection.

Sound backups are crucial. You should keep original executables on write-protected disks so that infected programs can easily be replaced. If you did not have them before you were infected, create or obtain them in case of future infections.

Sometimes you can recover data from disks damaged by a virus. Sophos can supply utilities for repairing the damage caused by some viruses. Contact Sophos technical support for advice.

Configuration

Setting preferences

Other menu options

3 Setting preferences

This section describes the configuration options available for scanning, disinfection, reporting, virus notification, central updating, and managing the log file. They are all located in the **SAV Preferences** dialog box.

To open the **SAV Preferences** dialog box, click the **Preferences** button (it does not matter which tabbed page is selected at the time).

**Alternatively**, on the **Edit** pull-down menu, choose **Preferences**.

To configure preferences for an item listed under **Configuration**, click it, then change the options in the right-hand pane.

The following subsections list each item in turn and explain its configuration options.

3.1 Immediate Mode – Scanning Options

Enables you to choose whether Sophos Anti-Virus should scan inside archive files and whether it should look for non-Macintosh viruses during immediate scanning.
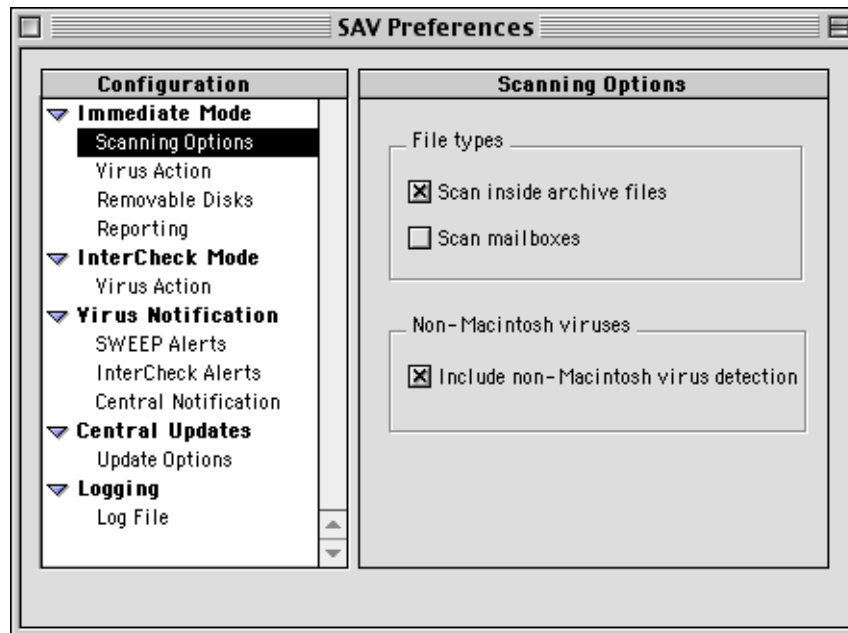
Archive Files

Enables Sophos Anti-Virus to scan inside archive files, including ARJ, Binhex, BZip2, GZIP, InstallShield CAB, LHA, LHZ, MacBinary, RAR, RAR3, RedHat Package Manager (RPM), Stuffit, TAR, Unix archive, Zip. See the readme file for a list of the archive types that can be scanned.

Mailboxes

Enables Sophos Anti-Virus to scan emails and attachments in Outlook Express mailboxes.

Non-Macintosh viruses

This enables Sophos Anti-Virus to detect non-Macintosh viruses, as well as Macintosh and macro viruses.

Non-Macintosh viruses cannot infect Macintoshes but can infect any non-Macintosh machines on the network.

3.2 Immediate Mode – Virus Action

Enables you to specify how Sophos Anti-Virus will deal with infected items found during an immediate scan (e.g. attempt disinfection).
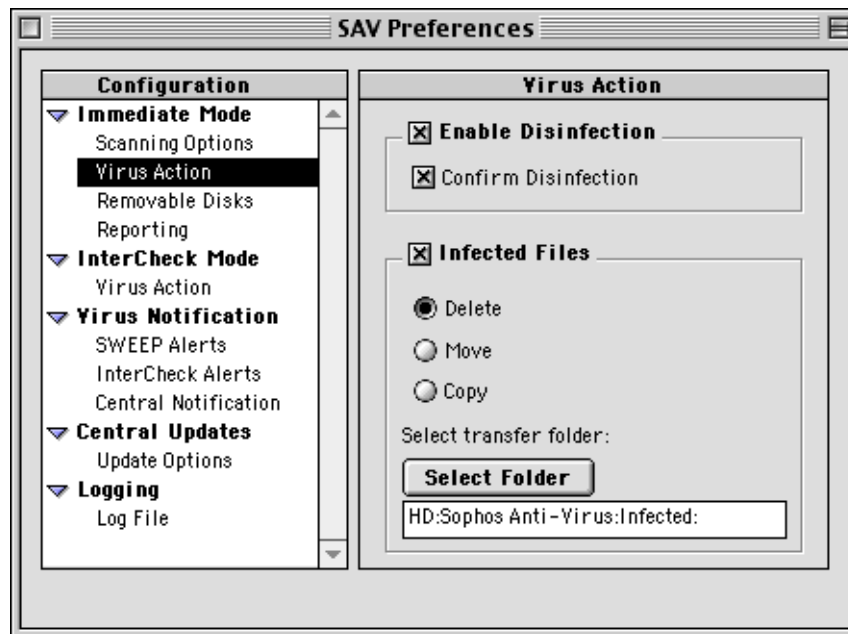
Enable Disinfection

If this option is selected, Sophos Anti-Virus will attempt to disinfect infected items it finds during immediate scanning.

If **Confirm Disinfection** is selected, Sophos Anti-Virus will prompt for confirmation before it attempts disinfection. This helps you locate and check the file for corruption after disinfection.

Infected Files

Prevents you from accessing infected files that cannot be disinfected. **Delete** files, **Move** them to prevent them being run, or **Copy** them to a specified folder for further analysis.

Click **Select Folder** to specify the folder where infected files should be moved or copied.

🛈 **Even if you click Delete, Sophos Anti-Virus does not delete infected mailboxes.**

3.3 Immediate Mode – Removable Disks

Enables you to configure Sophos Anti-Virus to scan removable disks.
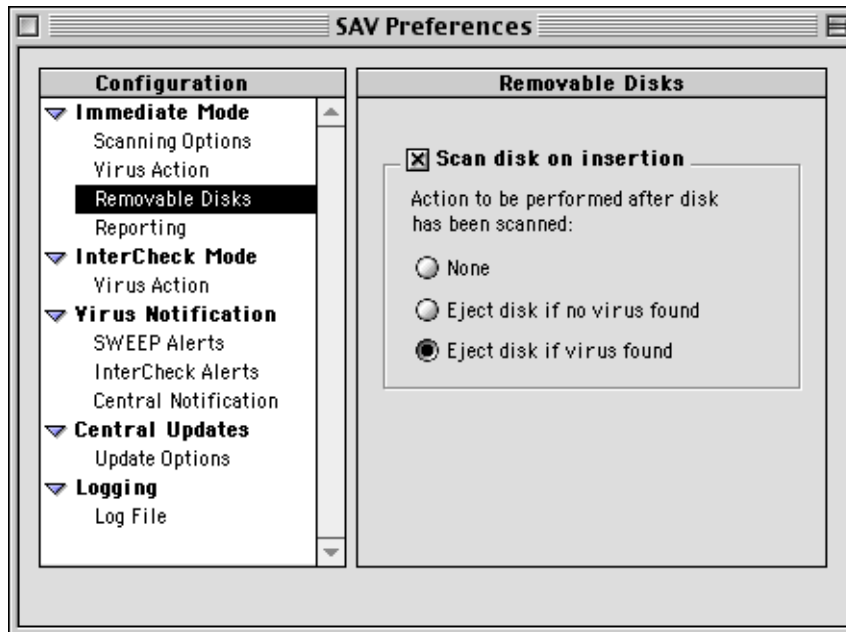
Scan disk on insertion

Configures Sophos Anti-Virus to scan removable disks when they are inserted in the computer. This only works when the **Sophos Anti-Virus** window is open.

You can specify the action that Sophos Anti-Virus will take after scanning the disk.

There are three options:

■ **None**
No action is taken.

■ **Eject disk if no virus found**
The disk is ejected automatically if no virus is found.

■ **Eject disk if virus found**
The disk is ejected automatically if a virus is found.

3.4 Immediate Mode – Reporting

Enables you to configure the level of reporting carried out after an immediate scan.

Sophos Anti-Virus also maintains a continuous log of all scanning activity (see section 3.10).
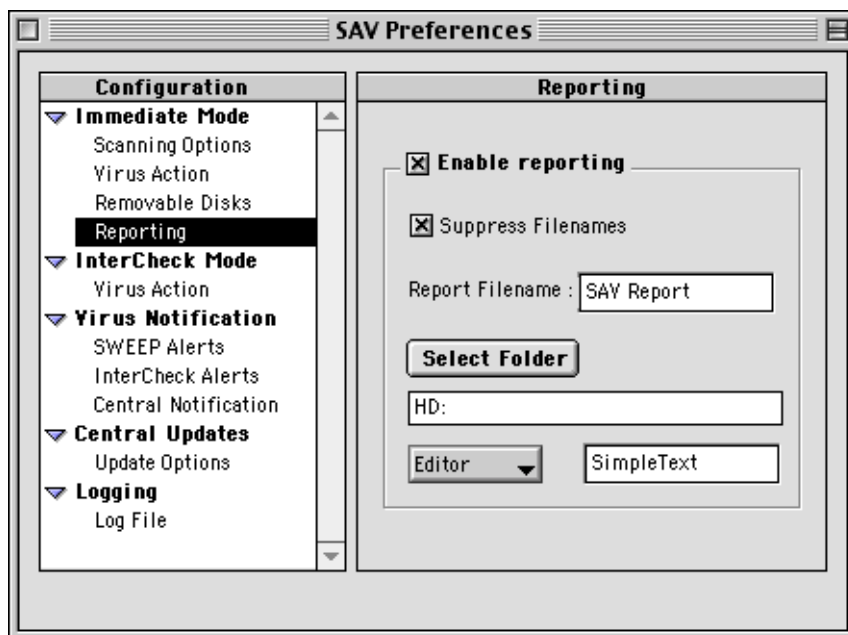
Enable reporting

Enables Sophos Anti-Virus to generate a report file each time an immediate scan is run.

By default, Sophos Anti-Virus will report infected files only. If **Suppress Filenames** is deselected, it will report all files scanned.

Type the name of the report in the **Report Filename** text box. The default name is SAV Report. This file is overwritten each time an immediate scan is run, unless a new filename is chosen for each report.

Click **Select Folder** to specify where the report file should be stored. The default is the root of the hard disk.

Click **Editor** to choose the text editor with which the report file should be opened. The default is SimpleText.

3.5 InterCheck Mode – Virus Action

Enables you to specify how Sophos Anti-Virus will deal with infected items found during an on-access scan by InterCheck (e.g. attempt disinfection).
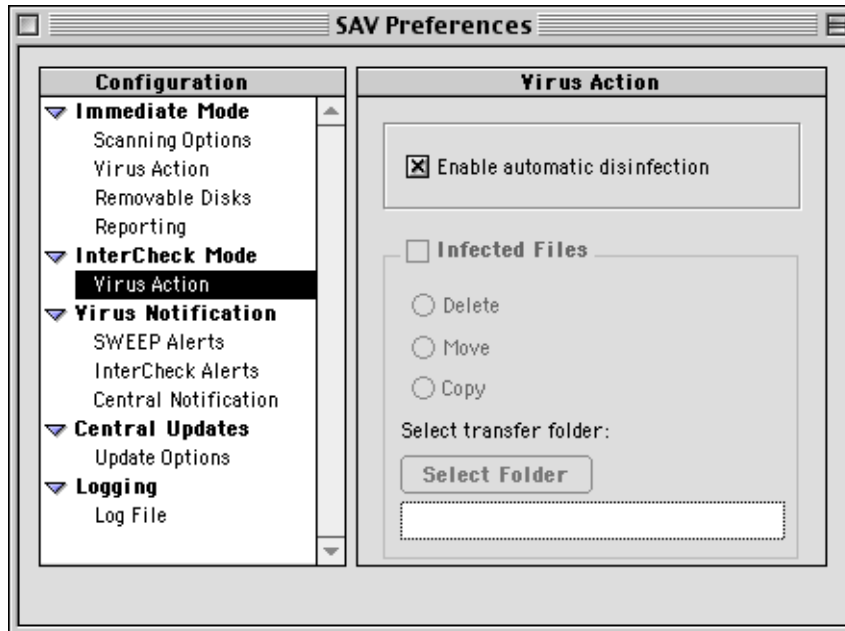

Enable automatic disinfection

This enables automatic disinfection of documents or boot sectors found during on-access scanning.

The other options on this page are not available for InterCheck.

3.6 Virus Notification – SWEEP alerts

Enables you to configure virus and error reports sent as a result of an immediate scan.

? **SWEEP** is a less common name for the component of Sophos Anti-Virus that carries out immediate scanning.
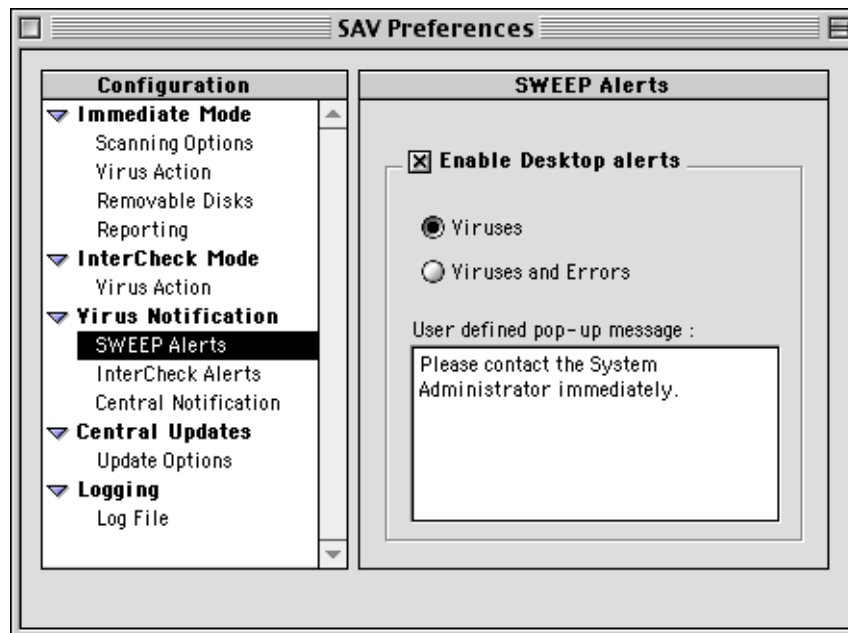
Enable Desktop alerts

Select this to enable Sophos Anti-Virus to display alerts in a pop-up box if a virus is discovered (or an error occurs) at the end of an immediate scan.

There are two levels of alert:

■ **Viruses**
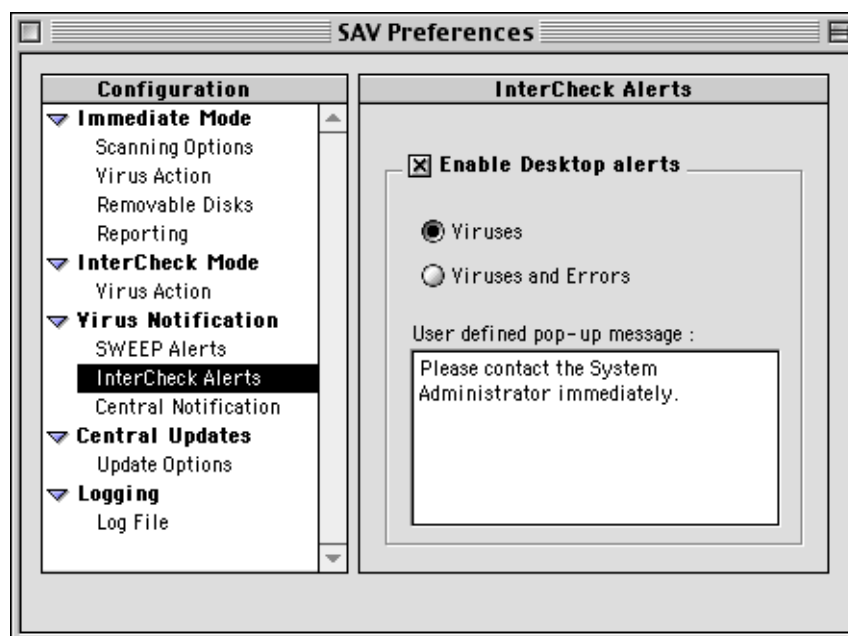Sophos Anti-Virus warns the user that a virus has been found.

■ **Viruses and errors**
Virus warnings and error messages are both displayed.

Define the text of the message in the **User defined pop-up message** text box.

3.7 Virus Notification – InterCheck Alerts

Enables you to configure virus and error reports sent as a result of InterCheck on-access scanning.

Enable Desktop alerts

Select this to enable InterCheck to display alerts in a pop-up box if a virus is discovered (or an error occurs) as the user tries to access an infected file.

There are two levels of alert:

■ **Viruses**
Sophos Anti-Virus warns the user that a virus has been found.

■ **Viruses and errors**
Virus warnings and error messages are both displayed.

Define the text of the message in the **User defined pop-up message** text box.

3.8 Virus Notification – Central Notification

Enables you to specify a location on the network to which virus alerts can be sent.

This location must be a computer on the network running a version of Sophos Anti-Virus that supports InterCheck Server, on which InterCheck Server has been installed. See the Sophos Anti-Virus user manual for the relevant platform.
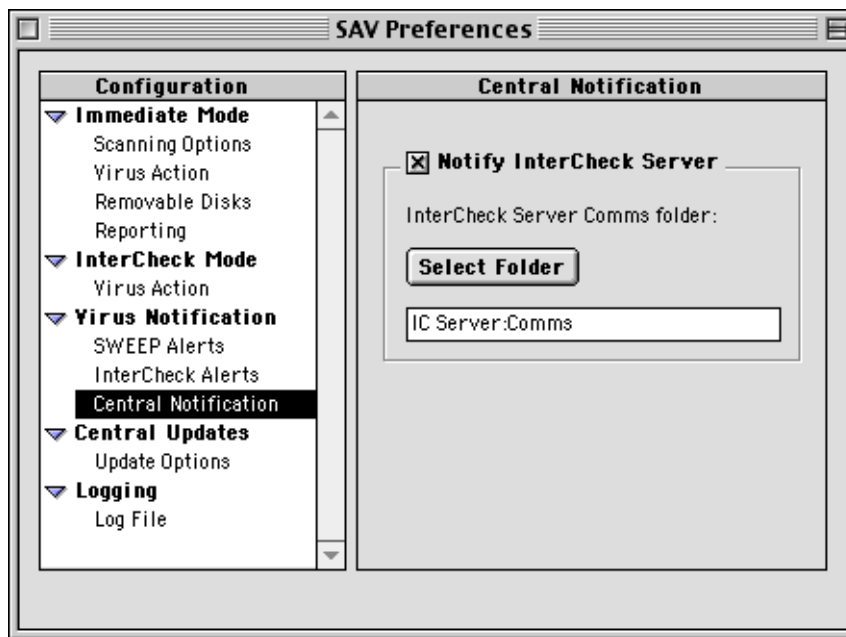
Notify InterCheck Server

Enables virus reports to be sent to an InterCheck Server on the network.

Click **Select Folder** to tell the computer where on the network this folder is located. Choose the Comms folder in your InterCheck Server installation (i.e. the folder containing the ic.sta file).

3.9 Central Updates – Update Options

Enables you to specify the location of the central installation directory (CID) that the computer should check for updates each time it is restarted. Macintosh workstations are automatically configured with this information during installation.

However, if the Macintosh CID is located on a Macintosh server, you must configure Sophos Anti-Virus on the server to update automatically from the CID.
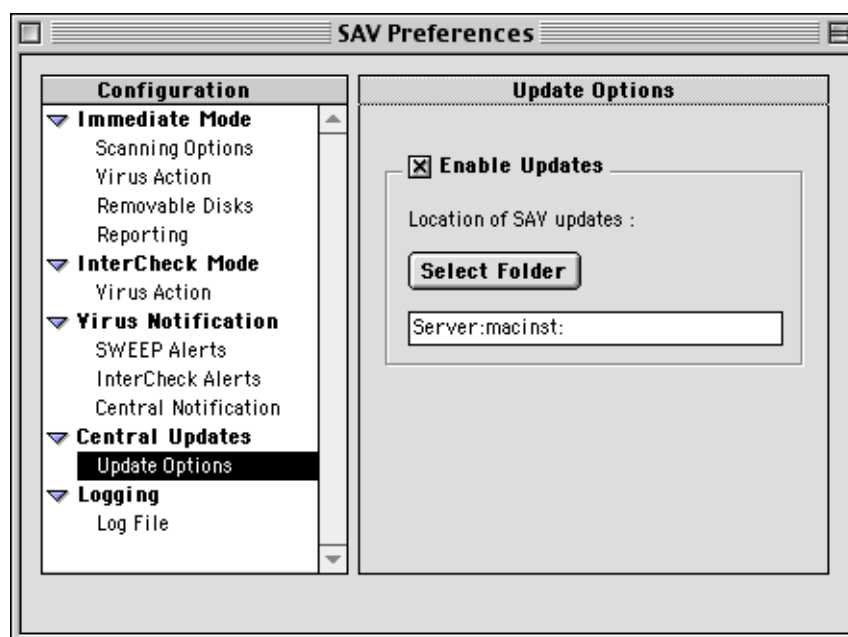
Enable Updates

Select **Enable Updates** to switch on automatic updating of Sophos Anti-Virus on the workstation. This option is enabled by default on Macintosh computers on which Sophos Anti-Virus was installed from the CID.
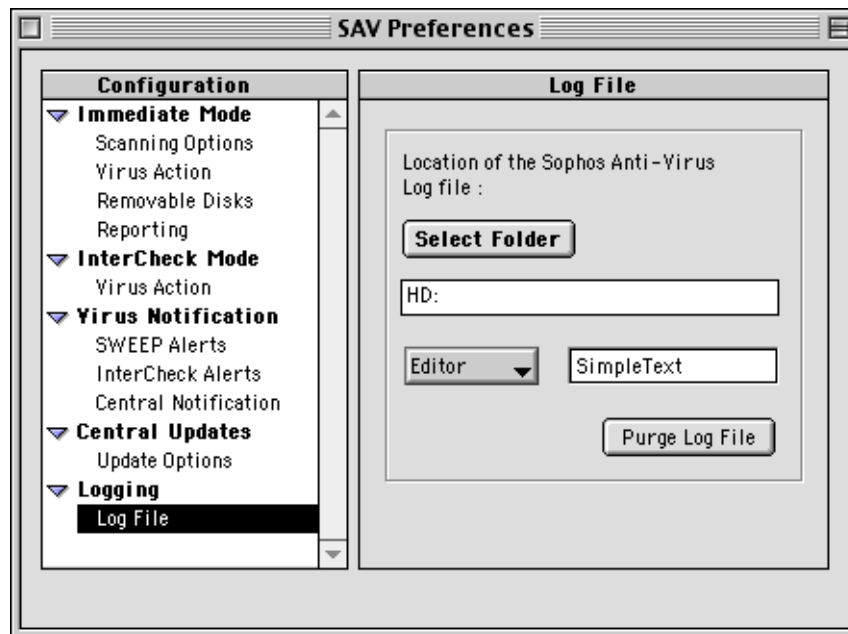
Click **Select Folder** to specify the location of the CID.

Sophos Anti-Virus will now check the specified folder on startup and when the **Sophos Anti-Virus** window is opened, and automatically download a more recent version of Sophos Anti-Virus if it finds it.

For information about updating the CID, see the *Sophos Anti-Virus Mac OS 8 or 9 on a network installation guide*.

3.10 Logging – Log File

Enables you to configure Sophos Anti-Virus's continuous log of all scanning activity and viruses found, which is written to a log file on disk.

The log file cannot be disabled.

Location of the Sophos Anti-Virus Log file

Click **Select Folder** to specify a folder for the log file. By default, it is located in the desktop folder of the startup disk.

Click **Editor** to choose the text editor with which the report file should be opened. The default is SimpleText.

Purge Log File

Purges the contents of the log file.

4 Other menu options

This section describes the options for purging the checksum file and restoring default preferences settings.

4.1 Purge Checksums

This applies only to InterCheck on-access scanning.

From the menu bar, on the **Special** pull down menu, choose **Purge Checksums**.

```
Special  Help
Virus Info          ⌘L
Purge Checksums  ⌘M
Restore Defaults  ⌘D
```
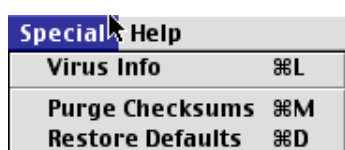
This will purge the checksum file (i.e. the list of items that have already been found to be virus-free and that can be accessed without further checking).

You may want to do this if you have recently deleted a large number of files from the computer, and therefore no longer need to keep a record of their checksums.

4.2 Restore defaults

From the menu bar, on the **Special** pull down menu, choose **Restore Defaults**.

```
Special  Help
Virus Info          ⌘L
Purge Checksums  ⌘M
Restore Defaults  ⌘D
```
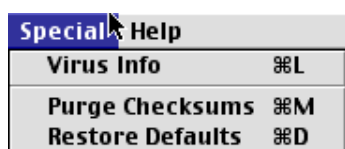
This restores the preferences in the **SAV Preferences** dialog box to their original defaults.

💡 This does not reset the Central Updates preferences (see section 3.9).

Troubleshooting

5 Troubleshooting

This section provides answers to some common problems that you may encounter when using Sophos Anti-Virus for Mac OS 8 or 9.

If your problem is not described in this section, refer to the Sophos website www.sophos.com which includes frequently asked questions (FAQs), virus analyses, the latest IDEs, product downloads and technical articles.

If your problem is not described on the website, contact Sophos technical support.

5.1 Drag and Drop functions do not work

Drag and Drop scanning (or Drag and Drop editing of the area list) is available only on Macintosh computers running later versions of the Macintosh operating system.

5.2 Auto-updating fails to happen

In the **SAV Preferences** dialog box, ensure that auto-updating is enabled and that the Macintosh is configured to check the central installation directory (CID) you are updating. See section 3.9.

5.3 Document not disinfected

Sophos Anti-Virus may report that an infected document has not been disinfected. This could be because

■ the infected item is on a write-protected disk or removable medium

■ Sophos Anti-Virus has discovered a virus fragment rather than an active virus.

Automatic disinfection is available only if it has been enabled in the **SAV Preferences** dialog box (see section 3).

5.4 Virus fragment reported

The report of a virus fragment indicates that part of a file matches part of a virus. There are three possible causes:

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus, which could become active. If you suspect that this is the case, please send Sophos a sample and a description.

Corrupted virus

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by Sophos Anti-Virus. A corrupted virus cannot spread. If a virus fragment is reported, contact Sophos technical support for advice.

Database containing a virus

When running a full scan, Sophos Anti-Virus may report that there is a virus fragment in a database file. Contact Sophos technical support for advice.

5.5 Sophos Anti-Virus reports errors

After a scan, Sophos Anti-Virus may report that some errors were found. There are two main reasons for errors:

File is corrupt

It can therefore not be scanned by Sophos Anti-Virus.

File is encrypted

Sophos Anti-Virus cannot scan encrypted files. However, if an encrypted file contains macros (for example it is a .doc or .xls file), the macros will not have been encrypted. You may be warned that the file is encrypted, but the parts of the file that can contain macro viruses will still be scanned.

Glossary and index

Glossary

Boot sector	The first part of the operating system to be read into memory when a computer is switched on (booted). The program stored in the boot sector is then executed, which loads the rest of the operating system from the system files on disk.
Checksum	A value calculated from item(s) of data. InterCheck creates a list of checksums of the files on the computer. If the checksum of a file is found to have changed, it is sent for scanning because it may have become infected with a virus.
CID	Central installation directory; a central copy of Sophos Anti-Virus files from which Sophos Anti-Virus is installed and updated automatically on the server and workstations. You must create a different CID for each platform on the network, and remember to keep every CID up to date.
IDE	Virus identity file; enables Sophos Anti-Virus to detect a specific virus. You need IDEs to protect your network against viruses discovered since your version of Sophos Anti-Virus was compiled.
Immediate scan	A virus scan that is triggered by the user from the Sophos Anti-Virus window. It is possible to configure what is scanned, how it is scanned and what action should be taken if a virus is found.
InterCheck	A component of Sophos Anti-Virus that intercepts files as they are accessed, and uses checksumming to determine whether or not they should be sent for virus scanning. It can be installed on servers, then switched off if found to affect performance.
InterCheck Server	A component of Sophos Anti-Virus that enables workstations to send virus alerts to a central location. InterCheck Server is not available in Sophos Anti-Virus for Macintosh, but Macintosh computers can be configured to send virus reports to an InterCheck Server on another platform (section 3.8).

Macro virus

A type of virus that uses macros in a data file to become active in memory and attach itself to other data files. Unlike other types of virus, macro viruses can attain a degree of platform independence.

On-demand scan

An immediate or scheduled scan.

SWEEP

The component of Sophos Anti-Virus that provides immediate virus scanning and disinfection.

Virus

A computer program that can spread across computers and networks by attaching itself to a program (such as a macro or boot sector) and making copies of itself.

Index