SOPHOS

sophos anti-virus

User manual

Sophos Anti-Virus for Windows 2000 and later, version 6

Document date: September 2006

Contents

About this manual **1**

About Sophos Anti−Virus **2**
What is Sophos Anti−Virus? 2
Sophos Anti−Virus window 3
Sophos Anti−Virus system tray icon 4
What is on−access scanning? 5
What is an on−demand scan? 5
What is a right−click scan? 6

Checking the computer is protected **7**
Checking protection is on 7
Turning protection on or off for the computer 7

Scanning items on demand **9**
What is an on−demand scan? 9
Scanning my computer 9
Setting up a scan 10
Scheduling a scan 11
Running a scan 13
Editing a scan 13

Scanning a single item **15**
Scanning a single item 15

Restricting access rights **16**
Types of user 16
Changing membership of Sophos user groups 17

Changing settings for multiple users **18**
Changing settings for all computers 18
Changing settings for all users on the computer 18

Configuring scanning **19**
Changing types of file scanned 19
Excluding items from scanning 21
Authorizing applications for use 25
Changing when on−access scanning occurs 26
Scanning inside archive files 27
Scanning Macintosh files 30
Scanning all files 33
Scanning for potentially unwanted applications 37

Configuring alerts........41
Desktop messaging........41
Email alerting........42
SNMP messaging........45
Event logging........47

Logging........49
Viewing the log for this computer........49
Configuring the log for this computer........50
Viewing the log for an on−demand scan........51

Updating........53
Updating immediately........53
Setting up automatic updating........53
Setting a source for updates........55
Setting an alternative source for updates........57
Scheduling updates........58
Updating via a proxy server........59
Limiting the bandwidth used........60
Logging updates........60

Cleaning up........62
What is cleanup?........62
Getting cleanup information........62
Setting up automatic cleanup........64

Managing quarantine items........71
What is Quarantine manager?........71
Dealing with viruses in quarantine........71
Dealing with applications in quarantine........74
Configuring user rights for Quarantine manager........77
Full computer scan........79

Troubleshooting........80
System tray icon has a white cross........80
System tray icon is grayed out........81
Threat not cleaned........81
Virus fragment reported........82
Threat partially detected........83
Application disappeared from quarantine........84
Computer becomes slow........84
Unable to access disk with infected boot sector........84
Unable to access areas of Sophos Anti−Virus........85
Recovering from threat side−effects........85
Getting further help........87

About this manual

This user manual explains how to use Sophos Anti−Virus for Windows 2000 and later, and how to configure

- scanning for threats
- alerts about threats
- cleanup
- logging
- updating.

The manual also provides help in resolving common problems.

About Sophos Anti−Virus

This section includes the following.

- What is Sophos Anti−Virus?
- Sophos Anti−Virus window
- Sophos Anti−Virus system tray icon
- What is on−access scanning?
- What is an on−demand scan?
- What is a right−click scan?

What is Sophos Anti−Virus?

Sophos Anti−Virus is software that detects and eliminates threats − viruses, worms, Trojans, spyware, and potentially unwanted applications − on your computer or network. In particular, it can

- scan your computer or network for threats
- check each file you access for threats
- alert you when it finds a threat
- clean up infected items
- prevent potentially unwanted applications from running on your computer
- clean potentially unwanted applications from your computer
- keep a log of its activity
- be updated to detect the latest threats.

Sophos Anti−Virus can be installed on computers running Windows 2000 or later.

Sophos Anti−Virus is integrated with Sophos Enterprise Console, which allows network administrators to centrally manage Sophos Anti−Virus on workstations. Sophos Anti−Virus is also integrated with the network security solution Cisco® Network Admission Control (NAC), thus enabling network administrators to include the state of Sophos Anti−Virus when validating host compliance with network admission policy. For more information, refer to the Sophos Enterprise Console help and *Sophos Anti−Virus Cisco NAC integration guide*.

Sophos Anti−Virus can be used in two ways:

- via the Sophos Anti−Virus window
- via the Sophos Anti−Virus system tray icon.

Sophos Anti−Virus can perform three types of scanning:

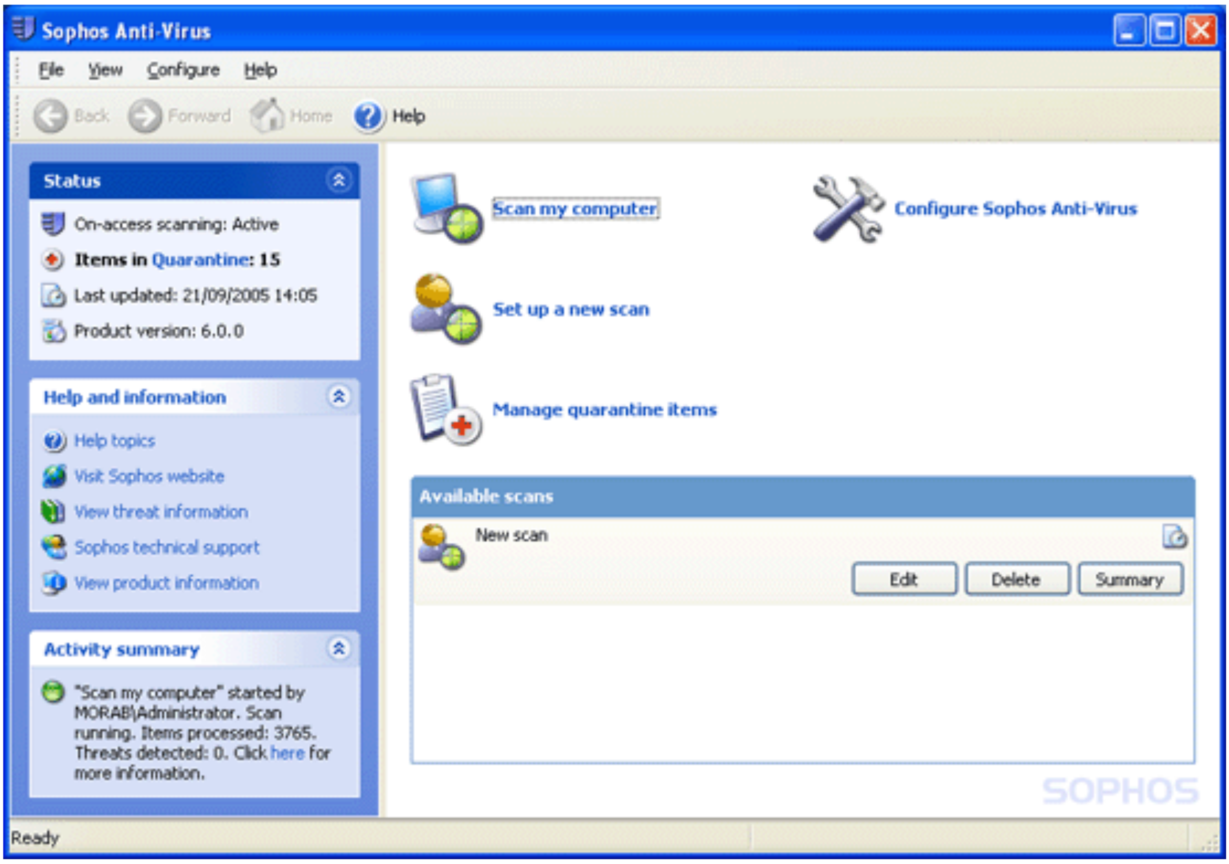
- on−access
- on−demand

- right–click.

Sophos Anti–Virus window

To open the **Sophos Anti–Virus** window, right–click the Sophos Anti–Virus system tray icon to display a menu.

Select **Open Sophos Anti–Virus**. The components of the window are described below.



On-access scanning: Active

Items in Quarantine: 15

Last updated: 21/09/2005 14:05

Product version: 6.0.0

"Scan my computer" started by MORAB\Administrator. Scan running. Items processed: 3765. Threats detected: 0. Click here for more information.

Toolbar

This contains buttons for getting help and navigating between the pages in the right–hand pane of the **Sophos Anti–Virus** window.

Status

This contains the status of on–access scanning, the number of items in Quarantine, the last time Sophos Anti–Virus was updated and the product version number.

Help and information

This enables you to contact Sophos technical support, and access help with Sophos Anti−Virus and information on threats. To see more detailed information about your version of Sophos Anti−Virus and your computer, click **View product information**.

Activity summary

This appears when you run a scan, and contains information about any threats found.

Home page

This is displayed in the right−hand pane when you open the **Sophos Anti−Virus** window. It includes the task list and the **Available scans** list. As you use the **Sophos Anti−Virus** window, the content of the right−hand pane may change. You can return to the home page by clicking the **Home** button.

The task list is displayed at the top of the home page. It enables you to

- scan your computer
- set up scans
- manage quarantine items
- configure Sophos Anti−Virus.

The **Available scans** list lists the scans that have been set up. From here, you can run, edit or delete each scan, and view a summary of what happened the last time the scan was run.

Sophos Anti−Virus system tray icon

The Sophos Anti−Virus system tray icon is always displayed, even if the **Sophos Anti−Virus** window is closed.

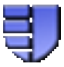
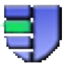
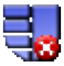
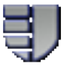
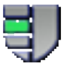
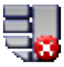
If you move the mouse pointer over the icon, the tool tip displays the last time Sophos Anti−Virus was updated.

If you right−click the icon, a menu is displayed. From here, you can

- update Sophos Anti−Virus
- configure updating
- check the progress of an update
- open the **Sophos Anti−Virus** window.

You need to be a Sophos Administrator to configure updating.

The appearance of the icon changes depending on whether on–access scanning is active, whether Sophos Anti–Virus is updating and whether Sophos Anti–Virus updated successfully last time.

Icon appearance	Explanation
	A blue shield means that on–access scanning is active. Sophos Anti–Virus updated successfully last time.
	If a green stripe appears running over a blue shield, this means that Sophos Anti–Virus is updating. On–access scanning is active.
	If a red circle with a white cross in it appears over a blue shield, this means that updating has failed. On–access scanning is active.
	A gray shield means that on–access scanning is inactive. Sophos Anti–Virus updated successfully last time.
	If a green stripe appears running over a gray shield, this means that Sophos Anti–Virus is updating. On–access scanning is inactive.
	If a red circle with a white cross in it appears over a gray shield, this means that updating has failed. On–access scanning is inactive.

To learn what to do if a red circle with a white cross in it appears over the system tray icon, or if the icon is grayed out, refer to System tray icon has a white cross or System tray icon is grayed out.

What is on–access scanning?

On–access scanning intercepts files as they are accessed, and grants access to only those that do not pose a threat to your computer.

For more information on scanning on access, refer to Checking the computer is protected and Configuring scanning.

What is an on–demand scan?

An **on–demand scan** is a scan of the computer, or parts of the computer, that you can run immediately or schedule to run at another time.

For more information on scanning on demand, refer to Scanning items on demand and Configuring scanning.

What is a right−click scan?

A **right−click scan** is a scan of selected item(s) in Windows Explorer or on the desktop, that you can run by right−clicking the selection to display a menu, and selecting **Scan with Sophos Anti−Virus**.

For more information on right−click scanning, refer to Scanning a single item and Configuring scanning.

Checking the computer is protected

This section includes the following.

- Checking protection is on
- Turning protection on or off for the computer

Checking protection is on

The computer is protected by on−access scanning.

On−access scanning intercepts files as they are accessed, and grants access to only those that do not pose a threat to your computer.

When on−access scanning is active, a blue shield is displayed in the system tray.

When on−access scanning is inactive, the shield is gray.

The status of on−access scanning is also indicated in the **Sophos Anti−Virus** window under **Status**.

If your computer is on a network, on−access scanning has probably already been configured. However, if you want to change the settings, refer to Configuring scanning.

Turning protection on or off for the computer

If you turn protection *off*, Sophos Anti−Virus does *not* scan files that you access for threats.

You need Sophos Administrator rights to turn protection on or off for a computer.

1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

2. Click **On−access scanning**.

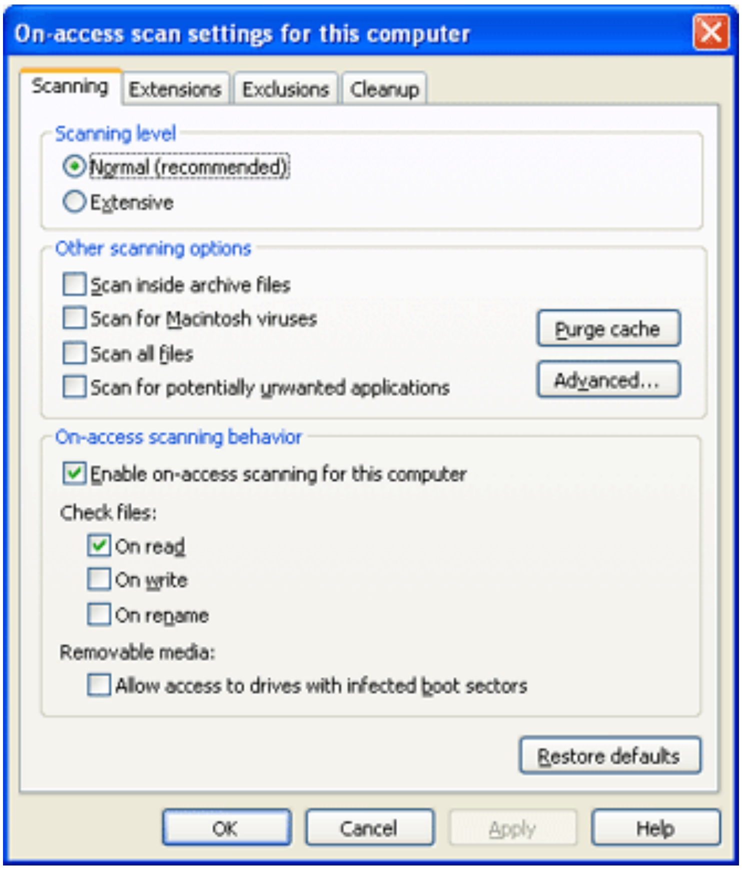
3. In the **On−access scan settings for this computer** dialog box, click the **Scanning** tab.

To turn on–access scanning ***on*** for the computer, select **Enable on–access scanning for this computer**, and click **OK**. The Sophos Anti–Virus system tray icon turns blue.

To turn on–access scanning ***off*** for the computer, deselect **Enable on–access scanning for this computer**, and click **OK**. The Sophos Anti–Virus system tray icon turns gray.

In the **Sophos Anti–Virus** window, the **Status** menu is updated.

Sophos Anti–Virus retains the settings you make here, even after you restart the computer. If you have turned on–access scanning off, it remains ***inactive*** until you turn it on again.



On-access scan settings for this computer

Scanning | Extensions | Exclusions | Cleanup

Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

□ Scan inside archive files

□ Scan for Macintosh viruses

□ Scan all files

□ Scan for potentially unwanted applications

On-access scanning behavior

☑ Enable on-access scanning for this computer

Check files:

☑ On read

□ On write

□ On rename

Removable media:

□ Allow access to drives with infected boot sectors

If you turn on–access protection off, you can still run on–demand scans of your computer.

Scanning items on demand

This section includes the following.

- What is an on–demand scan?
- Scanning my computer
- Setting up a scan
- Scheduling a scan
- Running a scan
- Editing a scan

What is an on–demand scan?

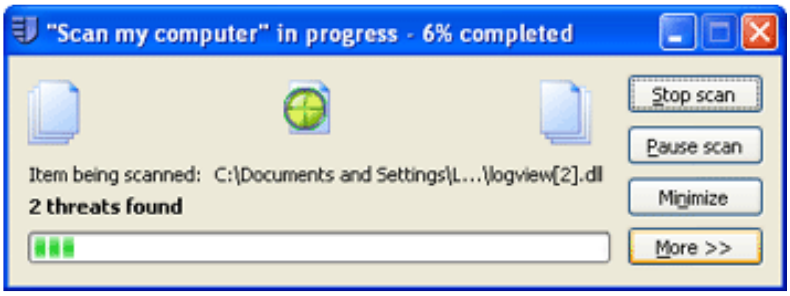
An **on–demand scan** is a scan of the computer, or parts of the computer, that you can run immediately or schedule to run at another time.

Scanning my computer

To run a scan of all fixed disk drives, including boot sectors, on the computer, do as follows.

In the home page of the **Sophos Anti–Virus** window, click **Scan my computer**.

A progress dialog box is displayed and the **Activity summary** appears in the **Sophos Anti–Virus** window.


"Scan my computer" in progress - 6% completed

Item being scanned: C:\Documents and Settings\L...\logview[2].dll

2 threats found

If any threats are found, click **More** and refer to Managing quarantine items.

To stop scanning, click **Stop scan**.

The **Scan my computer** scan does not scan Macintosh files stored on Windows computers. If you want Sophos Anti–Virus to scan executable

Macintosh files, you must set up a custom on−demand scan and enable scanning of Macintosh files for that scan.

For information on setting up, scheduling, running and configuring a scan, refer to the rest of this section and Configuring scanning.

Setting up a scan

1. In the home page of the **Sophos Anti−Virus** window, click **Set up a new scan** to display the scan setup page.

2. In the **Scan name** text box, type a name for the scan.

3. In the **Items to scan** panel, select the drives and folders you want to scan. To do this, click the check box to the left of each drive or folder. To learn about the icons that appear in the check boxes, refer to Representation of items to scan.

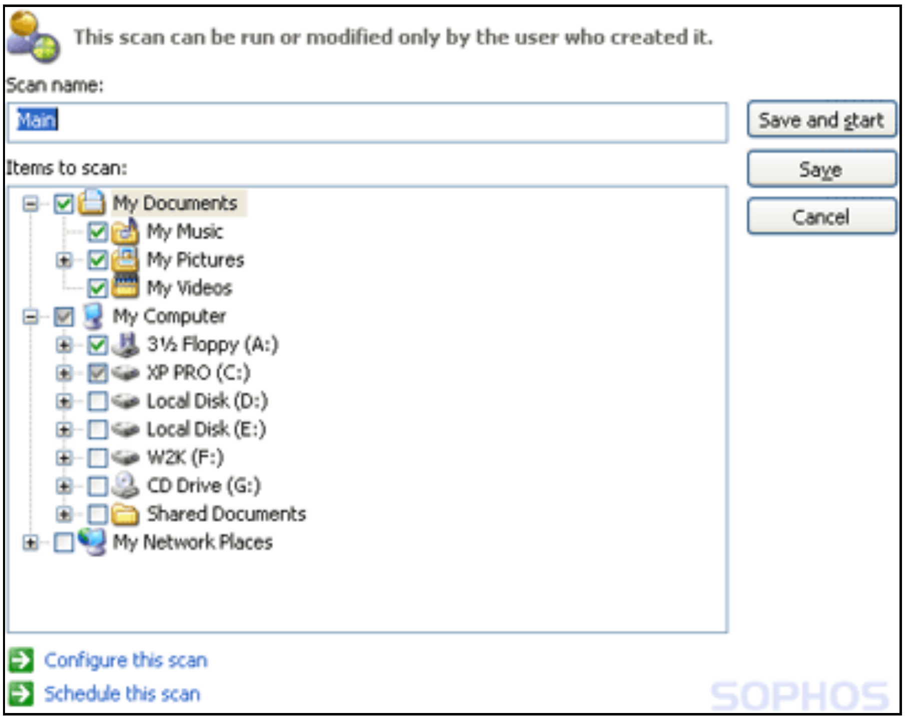
   Drives or folders that are unavailable (because they are offline or have been deleted) are displayed in a strikethrough font. They are removed from the **Items to scan** panel if they are deselected or there is a change in the selection of their parent drive or folder(s).

4. To configure the scan further, click **Configure this scan**. (Refer to Configuring scanning for more information.)

5. To schedule the scan, click **Schedule this scan**. (Refer to Scheduling a scan for more information.)

   You can't manually run a scan that you have scheduled. Scheduled scans are displayed in the **Available scans** list with a clock icon.

6. Click **Save** to save the scan or **Save and start** to save and run the scan.



This scan can be run or modified only by the user who created it.

Scan name: Main

Items to scan:

- ☑ My Documents
  - ☑ My Music
  - ☑ My Pictures
  - ☑ My Videos
- ☑ My Computer
  - ☑ 3½ Floppy (A:)
  - ☑ XP PRO (C:)
  - □ Local Disk (D:)
  - □ Local Disk (E:)
  - □ W2K (F:)
  - □ CD Drive (G:)
  - □ Shared Documents
- □ My Network Places

Representation of items to scan

In the **Items to scan** panel, different icons are displayed in the check box next to each item (drive or folder), depending on which items will be scanned. These icons are shown below with explanations.

Icon	Explanation
□	The item and all sub–items *are not* selected for scanning.
☑	The item and all sub–items *are* selected for scanning.
☑	The item is partially selected: the item is not selected, but some sub–items are selected for scanning.
☒	The item and all sub–items are excluded from this particular scan.
☑	The item is partially excluded: the item is selected, but some sub–items are excluded from this particular scan.
⊘	The item and all sub–items are excluded from all on–demand scans, because of an on–demand exclusion that has been set up.

Scheduling a scan

You need Sophos Administrator rights to schedule a scan, or to view and edit scheduled scans created by other users.

To schedule a scan that you are setting up or editing, do as follows.

You can't manually run a scan that you have scheduled. Scheduled scans are displayed in the **Available scans** list with a clock icon.

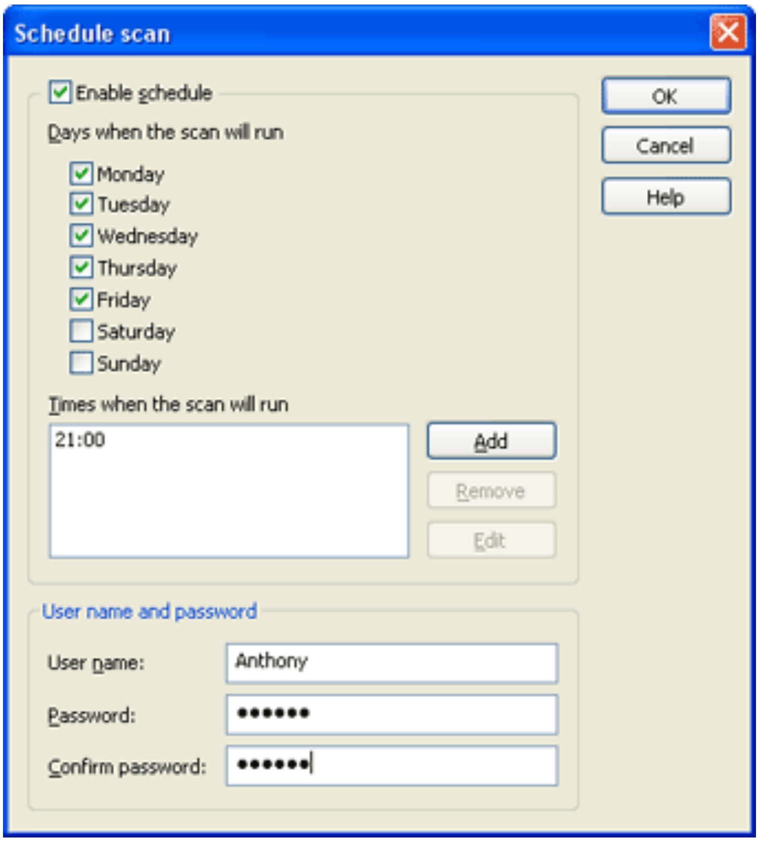
1. In the right–hand pane of the **Sophos Anti–Virus** window, click **Schedule this scan**.
2. In the **Schedule scan** dialog box, select **Enable schedule**.

   Select the day(s) on which the scan should run.

   Add the time(s) by clicking **Add**.

   If necessary, remove or edit a time by selecting it and clicking **Remove** or **Edit**, respectively.
3. Type a **user name** and **password**. Password cannot be blank.

   The scheduled scan runs with the access rights of that user.
4. Click **OK**.



Schedule scan

☑ Enable schedule

Days when the scan will run

☑ Monday
☑ Tuesday
☑ Wednesday
☑ Thursday
☑ Friday
□ Saturday
□ Sunday

Times when the scan will run

21:00

User name and password

User name: Anthony

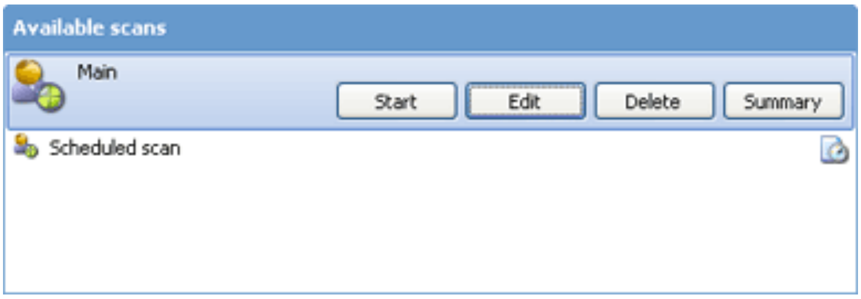
Password: ••••••

Confirm password: ••••••

Running a scan

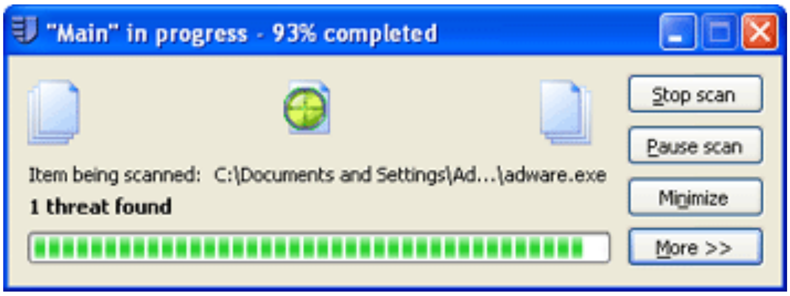
To run a scan that has been set up, do as follows.

In the home page of the **Sophos Anti–Virus** window, in the **Available scans** list, select the scan you want to run. Click **Start**.



You can't manually run a scan that you have scheduled. Scheduled scans are displayed in the **Available scans** list with a clock icon.

A progress dialog box is displayed and the **Activity summary** appears in the **Sophos Anti–Virus** window.


"Main" in progress - 93% completed

Item being scanned: C:\Documents and Settings\Ad...\adware.exe

1 threat found

If any threats are found, click **More** and refer to Managing quarantine items.

To stop scanning, click **Stop scan**.

For information on setting up, scheduling and configuring a scan, refer to the rest of this section and Configuring scanning.

Editing a scan

To edit a scan that has been set up, do as follows.

1. In the home page of the **Sophos Anti–Virus** window, in the **Available scans** list, select the scan you want to edit. Click **Edit** to display the scan setup page.

2. To rename the scan, in the **Scan name** text box, type a name for the scan.

3. To change which items to scan, in the **Items to scan** panel, select or deselect the drives and folders you want to scan. To do this, click the check box to the left of each drive or folder. To learn about the icons that appear in the check boxes, refer to Representation of items to scan.

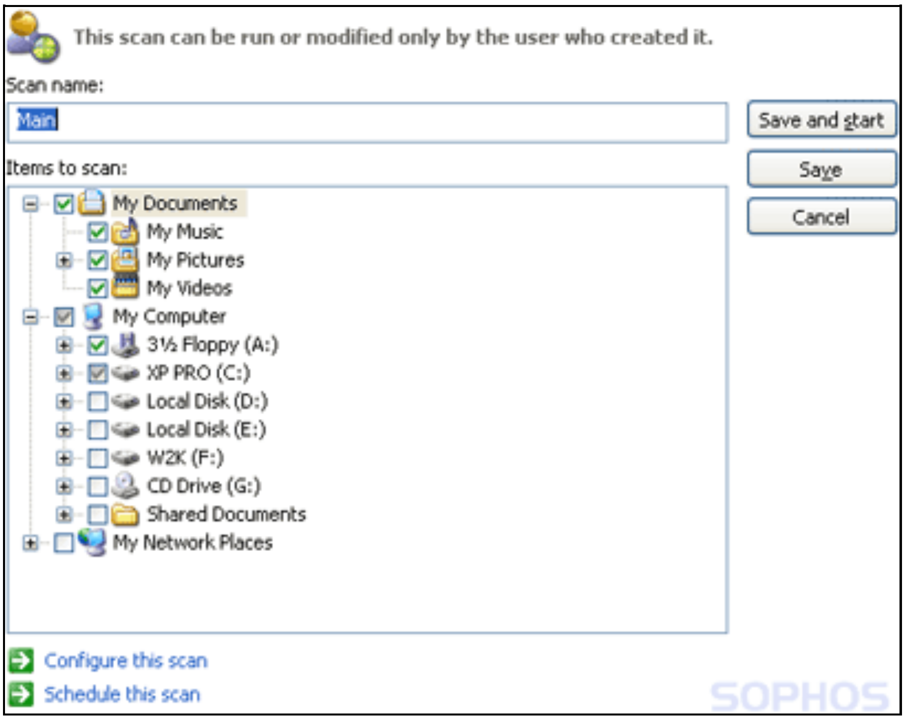
   Drives or folders that are unavailable (because they are offline or have been deleted) are displayed in a strikethrough font. They are removed from the **Items to scan** panel if they are deselected or there is a change in the selection of their parent drive or folder(s).

4. To configure the scan further, click **Configure this scan**. (Refer to Configuring scanning for more information.)

5. To schedule the scan, click **Schedule this scan**. (Refer to Scheduling a scan for more information.)

   You can't manually run a scan that you have scheduled. Scheduled scans are displayed in the **Available scans** list with a clock icon.

6. Click **Save** to save the scan or **Save and start** to save and run the scan.



This scan can be run or modified only by the user who created it.

Scan name: Main

Items to scan:

- ☑ My Documents
  - ☑ My Music
  - ☑ My Pictures
  - ☑ My Videos
- ☑ My Computer
  - ☑ 3½ Floppy (A:)
  - ☑ XP PRO (C:)
  - □ Local Disk (D:)
  - □ Local Disk (E:)
  - □ W2K (F:)
  - □ CD Drive (G:)
  - □ Shared Documents
- □ My Network Places

To delete a scan, in the home page of the **Sophos Anti−Virus** window, in the **Available scans** list, select the scan you want to delete. Click **Delete**, and then click **Yes** to confirm the deletion.

Scanning a single item

This section includes the following.

- Scanning a single item

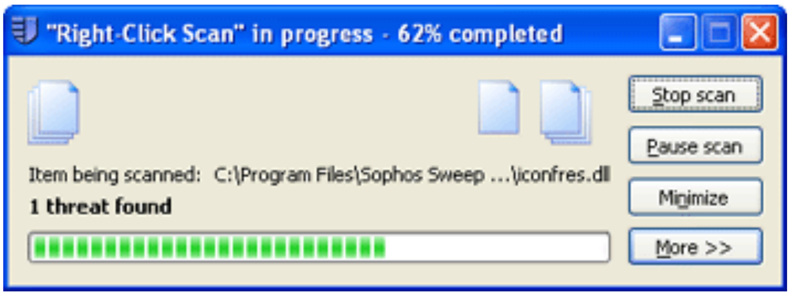
Scanning a single item

You can scan a single item by performing a right–click scan.

A **right–click scan** is a scan of selected item(s) in Windows Explorer or on the desktop, that you can run by right–clicking the selection to display a menu, and selecting **Scan with Sophos Anti–Virus**.

1. Open Windows Explorer. To do this, at the taskbar, click **Start**|**Programs**|**Accessories**|**Windows Explorer**.
2. Select the file(s), folder(s) and/or disk drives you want to scan.
3. Right–click the selection to display a menu, and select **Scan with Sophos Anti–Virus**.

A progress dialog box is displayed.



"Right-Click Scan" in progress - 62% completed

Item being scanned: C:\Program Files\Sophos Sweep ...\iconfres.dll

1 threat found

If any threats are found, click **More** and refer to Managing quarantine items.

To stop scanning, click **Stop scan**.

For information on configuring a scan, refer to Configuring scanning.

Restricting access rights

This section includes the following.

- Types of user
- Changing membership of Sophos user groups

Types of user

Sophos Anti−Virus restricts access to certain parts of the software to certain types of user. This security is based on the user groups that have been set up in Windows on this computer. When Sophos Anti−Virus is installed, each user is assigned to one of the Sophos user groups depending on their Windows user group, as follows.

- Members of the Windows Administrators group are assigned to the SophosAdministrator group.
- Members of the Windows Power Users group are assigned to the SophosPowerUser group.
- Members of the Windows Users group are assigned to the SophosUser group.

Any user who is not assigned to one of the Sophos user groups, including Guest users, can perform only

- on−access scanning
- scans run from a right−click menu.

Members of the SophosUser group can perform the above functions and

- access the Sophos Anti−Virus window
- set up and run on−demand scans
- configure scans run from a right−click menu
- manage, with limited privileges, quarantined items.

Members of the SophosPowerUser group have the same rights as members of the SophosUser group with the addition of greater privileges in Quarantine manager.

Members of the SophosAdministrator group can use or configure any part of Sophos Anti−Virus.

Changing membership of Sophos user groups

To change the Sophos user group for a user, you must do as follows. (Refer to your Windows documentation if necessary.)

1. Use Windows to move the user from one Sophos user group to another.

2. When that user logs on to Windows again, they should find that their access rights have changed accordingly.

Changing settings for multiple users

This section includes the following.

- Changing settings for all computers
- Changing settings for all users on the computer

Changing settings for all computers

To configure Sophos Anti−Virus on workstations from a central location on the network, refer to the Sophos Enterprise Console help.

Changing settings for all users on the computer

To configure Sophos Anti−Virus for all users on the computer, in the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**. From the **Configure** page, you can change the following settings.

- On−access scanning
- On−demand extensions and exclusions
- User rights for Quarantine manager
- List of authorized applications
- Messaging
- Log for this computer
- Updating

You need to be a Sophos Administrator to change these settings.

Configuring scanning

This section includes the following.

- Changing types of file scanned
- Excluding items from scanning
- Authorizing applications for use
- Changing when on−access scanning occurs
- Scanning inside archive files
- Scanning Macintosh files
- Scanning for potentially unwanted applications
- Scanning all files

Changing types of file scanned

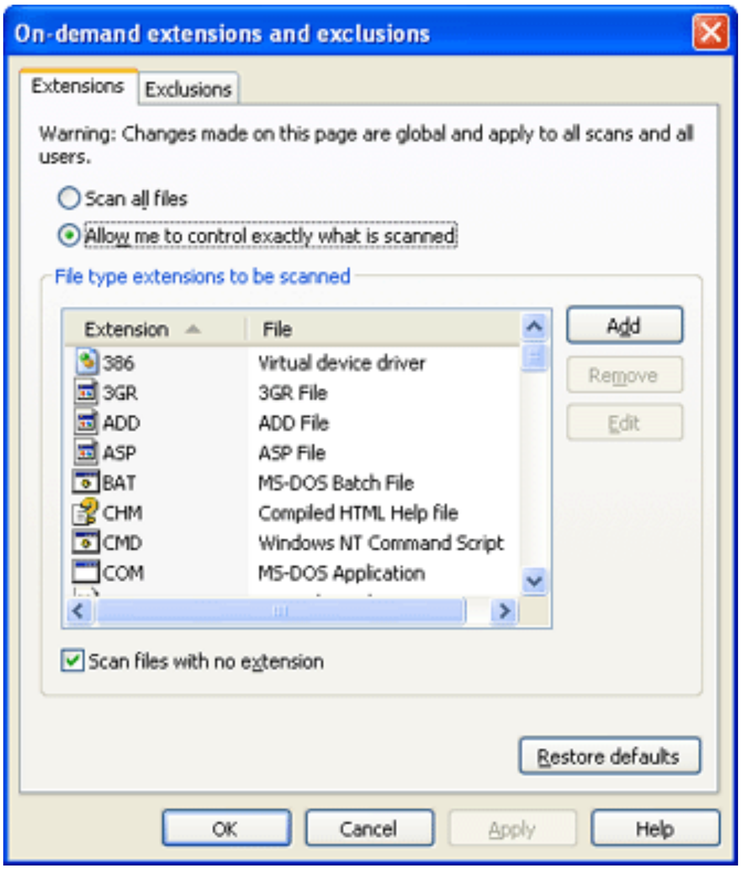
⚠ If the Sophos Enterprise Console is used to administer Sophos Anti−Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

2. To change the settings for ***on−access scanning***, click **On−access scanning**.

   To change the settings for ***on−demand scanning*** and ***right−click scanning***, click **On−demand extensions and exclusions**.

3. Click the **Extensions** tab. Set the options as described below.



Warning: Changes made on this page are global and apply to all scans and all users.

○ Scan all files

● Allow me to control exactly what is scanned

File type extensions to be scanned

Extension	File
386	Virtual device driver
3GR	3GR File
ADD	ADD File
ASP	ASP File
BAT	MS-DOS Batch File
CHM	Compiled HTML Help file
CMD	Windows NT Command Script
COM	MS-DOS Application

☑ Scan files with no extension

Scan all files

Click this to enable scanning of all files, regardless of the filename extension.

Sophos does not recommend selecting this option, except on the advice of Sophos technical support. Selecting the **Scan all files** option makes scanning slower and is generally not required.

Allow me to control exactly what is scanned

Click this to restrict scanning to only files with a particular filename extension, specified in the extension list.

The extension list includes file types that Sophos recommends are scanned. Be careful if you alter the list as explained below.

To add a filename extension to the list, click **Add**. You can use the wildcard ? to match any single character.

To remove a filename extension from the list, select the extension and click **Remove**.

To change a filename extension in the list, select the extension and click **Edit**.

When you select **Allow me to control exactly what is scanned**, **Scan files with no extension** is selected by default. To disable scanning of files with no filename extension, clear the **Scan files with no extension** check box.

Excluding items from scanning

⚠ If the Sophos Enterprise Console is used to administer Sophos Anti−Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

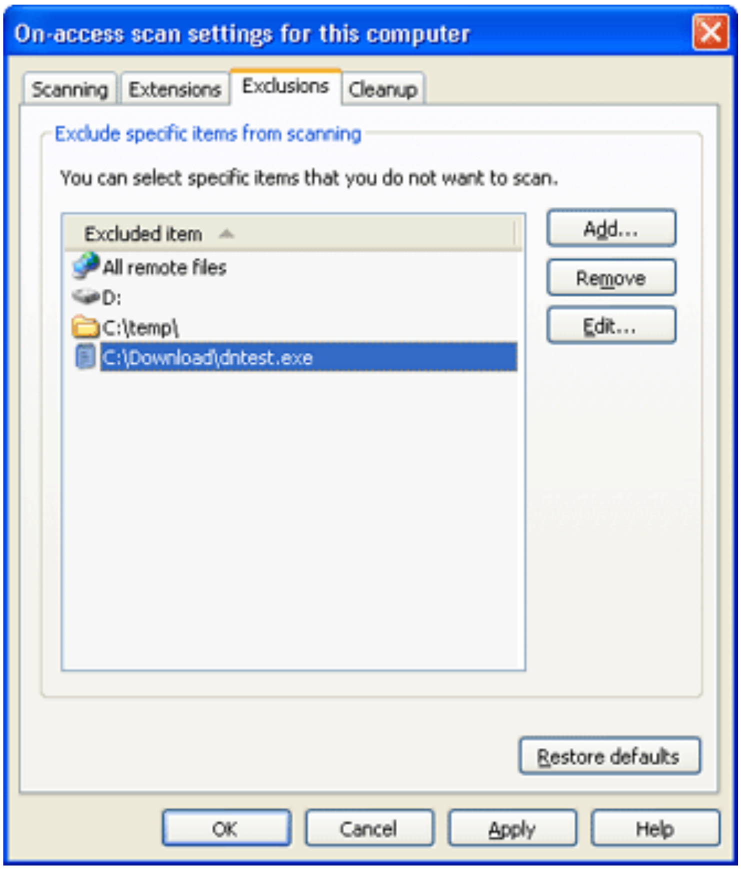
The procedure described below applies to *all* on−demand scans. To exclude items from a *particular* on−demand scan, refer to Editing a scan.

1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

2. To change the settings for ***on−access scanning***, click **On−access scanning**.

   To change the settings for ***on−demand scanning*** and ***right−click scanning***, click **On−demand extensions and exclusions**.

3. Click the **Exclusions** tab. Set the options as described below.



Exclude specific items from scanning

You can select specific items that you do not want to scan.

Excluded item

- All remote files
- D:
- C:\temp\
- C:\Download\dntest.exe

Excluded item

To specify items that should be excluded from scanning, click **Add**. In the **Exclude item** dialog box, specify the type and name of the item to be excluded. Refer to Specifying excluded items.

To remove items from the list of excluded items, click **Remove**.

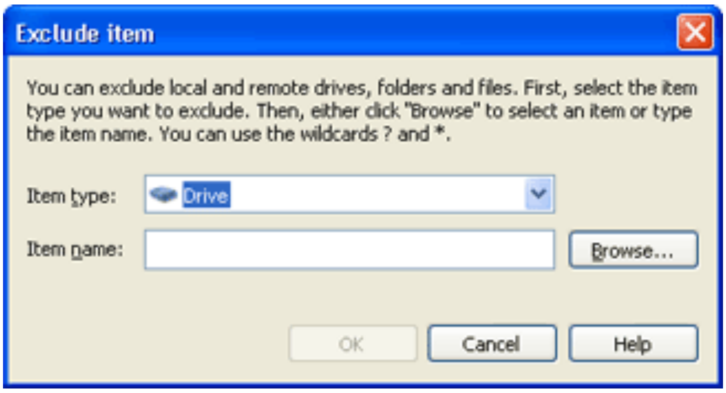
To change items in the list of excluded items, click **Edit**.

Specifying excluded items

In the **Exclude item** dialog box, select the **Item type**. **All remote files** means all files not on this computer. Unless you select **All remote files**, specify the **Item name** by using the **Browse** button or typing in the text box.

If you work on a 64–bit platform, the **Browse** button will not be visible in the **Exclude item** dialog.

Further details on specifying item names are given below.



You can exclude local and remote drives, folders and files. First, select the item type you want to exclude. Then, either click "Browse" to select an item or type the item name. You can use the wildcards ? and *.

Item type: Drive

Item name:

- **Filename**

  You can specify only the name of a file, and Sophos Anti–Virus excludes all files with that name, wherever they are located. For example

  fred.bmp

  causes Sophos Anti–Virus to exclude all files called fred.bmp, wherever they are located.

- **Full path**

  You can specify the exact location and name of a file, and Sophos Anti–Virus excludes only that particular file. The path can include the drive or the share. For example

  C:\Miscellaneous\fred.bmp

  causes Sophos Anti–Virus to exclude fred.bmp in the Miscellaneous folder on the C: drive.

  \\Server1\Users\Fred\Letter.rtf

  causes Sophos Anti–Virus to exclude Letter.rtf in the Fred folder in the Users share on Server1.

  If you don't specify the drive or share, Sophos Anti–Virus matches the path at the root of any drive or share.

- **Partial path**

  You can specify a drive or share, and Sophos Anti–Virus excludes everything from that drive or share and below. For example

A:

causes Sophos Anti−Virus to exclude everything on the A: drive.

You can specify a folder, and Sophos Anti−Virus excludes everything from that folder and below. For example

D:\Tools\

causes Sophos Anti−Virus to exclude everything from the Tools folder on the D: drive and all subfolders.

You can specify a folder and filename, and Sophos Anti−Virus excludes any folder and filename that match. For example

logs\log.txt

causes Sophos Anti−Virus to exclude log.txt in any folder called logs on any drive or share.

Wildcards

The wildcard ? can be used only in a filename or extension. It generally matches any single character. However, when used at the end of a filename or extension, it matches zero or one character. For example file??.txt matches file.txt, file1.txt and file12.txt but not file123.txt.

The wildcard * can be used only in a filename or extension, in the form [filename].* or *.[extension]. For example, file*.txt, file.txt* and file.*txt are invalid.

Multiple filename extensions

Filenames with multiple extensions are treated as if the last extension is the extension and the rest are part of the filename. For example,

[filename].[extension1].[extension2] means the filename is [filename].[extension1] and the extension is [extension2].

Standard naming conventions

The filename or path is validated against standard naming conventions (e.g. a folder name may contain spaces but may not contain only spaces).

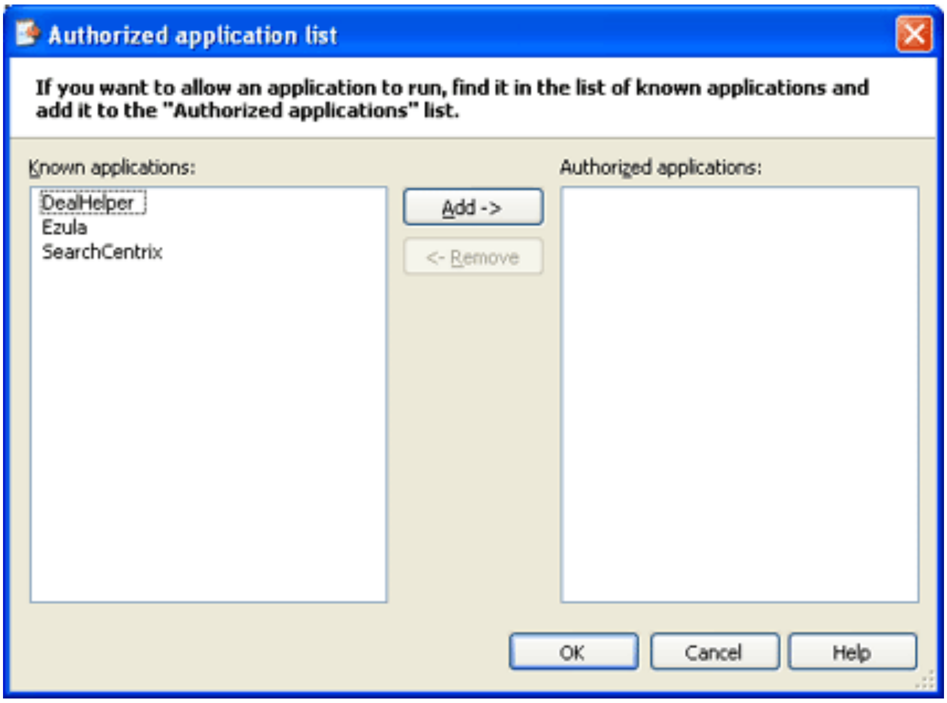
Authorizing applications for use

If the Sophos Enterprise Console is used to administer Sophos Anti–Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

If you want to run on your computer an application that Sophos Anti–Virus has classified as potentially unwanted, you can authorize this application as follows.

1. In the home page of the **Sophos Anti–Virus** window, click **Configure Sophos Anti–Virus**.

2. In the **Configure** page, click **Authorized application list**. The **Authorized application list** dialog box appears.



If you want to allow an application to run, find it in the list of known applications and add it to the "Authorized applications" list.

3. In the left–hand pane, under **Known applications**, select the application you want to authorize and click **Add**. The application now appears in the right–hand pane, under **Authorized applications**.

If you want to prevent a currently authorized application from running on your computer, remove the application from the list of authorized applications by selecting it in the **Authorized applications** list and clicking **Remove**.

You can also authorize applications in Quarantine manager. For information on how to do this, refer to Dealing with applications in quarantine.

Changing when on−access scanning occurs

⚠ If the Sophos Enterprise Console is used to administer Sophos Anti−Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

You can specify whether Sophos Anti−Virus scans files when they're opened, when they're saved or when they're renamed.

1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

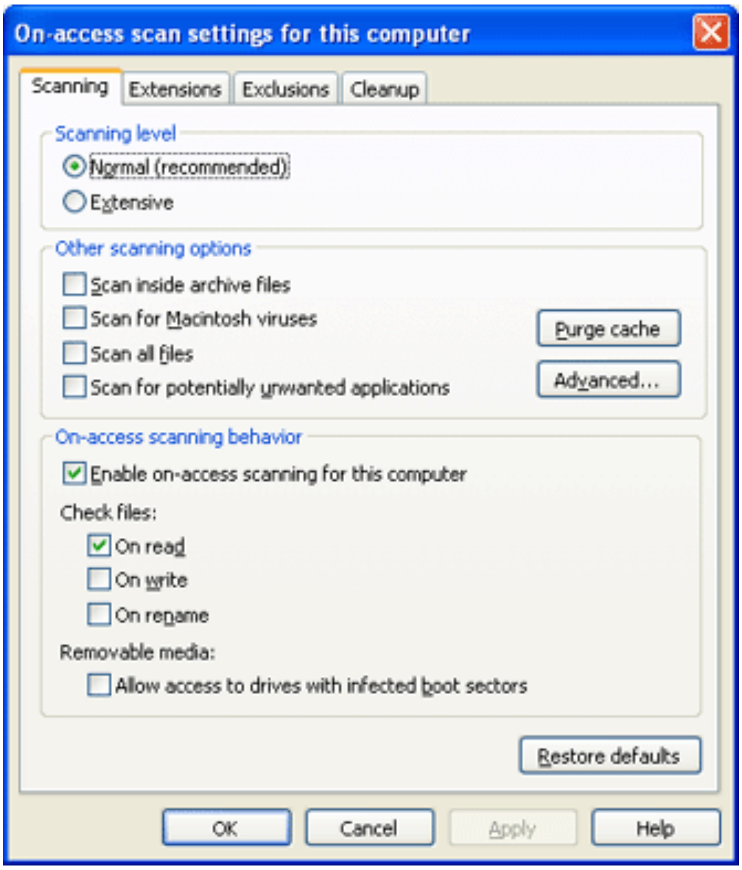
2. In the **Configure** page, click **On−access scanning**.

3. In the **On−access scan settings for this computer** dialog box, click the **Scanning** tab. Set the options as described below.

   To specify that files must be scanned when they're opened, select **On read**. This is the recommended option.

   To specify that files must be scanned when they're saved, select **On write**.

To specify that files must be scanned when they're renamed, select **On rename**.



On-access scan settings for this computer

Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

□ Scan inside archive files

□ Scan for Macintosh viruses

□ Scan all files

□ Scan for potentially unwanted applications

On-access scanning behavior

☑ Enable on-access scanning for this computer

Check files:

☑ On read

□ On write

□ On rename

Removable media:

□ Allow access to drives with infected boot sectors

Scanning inside archive files

Scanning inside archive files makes scanning significantly slower and is generally not required. Even if you don't select the option, when you attempt to access a file extracted from the archive file, the extracted file is scanned. Sophos therefore does not recommend selecting this option.

If you want to enable Sophos Anti–Virus to scan inside archive files, you can do this for

- on–access scanning
- on–demand scanning
- scans run from a right–click menu.

Scanning inside archives on access

On–access scanning automatically checks files in an archive when you access them. Scanning inside archives is therefore optional and is **not recommended for use in on–access scanning**.

Scanning inside archives on demand

⚠ **Scanning inside archive files makes scanning significantly slower and is rarely required. Even if you don't select the option, when you attempt to access a file extracted from the archive file, the extracted file is scanned.**

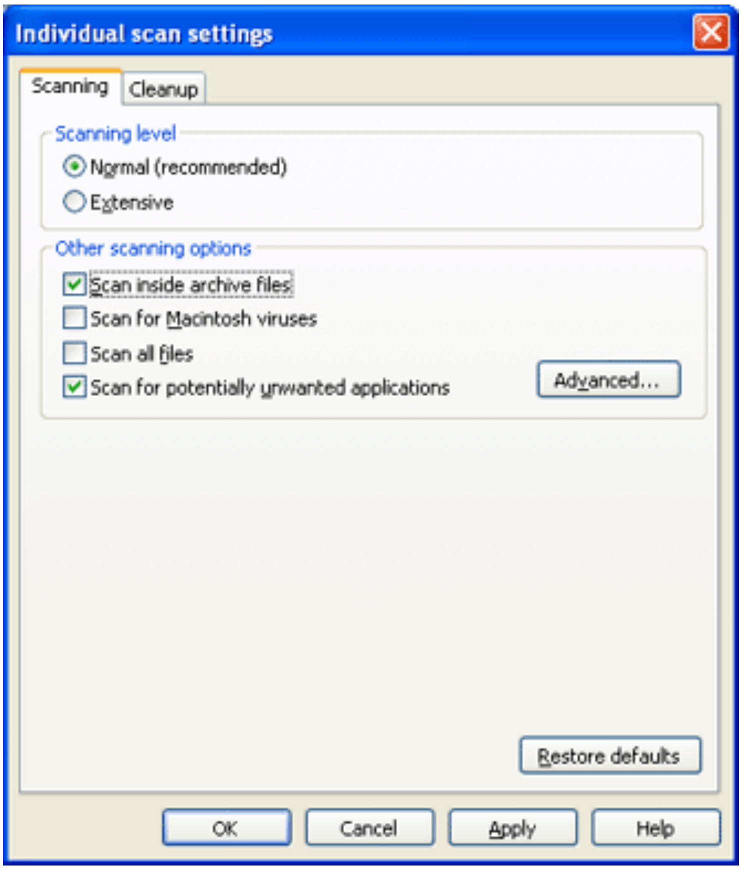
Whether you select this option or not, files compressed with dynamic compression utilities (PKLite, LZEXE and Diet) are scanned.

1. In the home page of the **Sophos Anti–Virus** window, in the **Available scans** list, select the scan you want to edit. Click **Edit**.

2. In the scan setup page, click **Configure this scan**.

3. In the **Individual scan settings** dialog box, click the **Scanning** tab.

4. Select **Scan inside archive files**.



Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

☑ Scan inside archive files

□ Scan for Macintosh viruses

□ Scan all files

☑ Scan for potentially unwanted applications

To enable scanning inside only particular archive file types, click **Advanced**. In the **Advanced scanning settings** dialog box, select the archive file types that you want Sophos Anti–Virus to scan inside.

The advanced settings are very specialized and you should use them only with advice from Sophos technical support.

Scanning inside archive files from a right–click menu

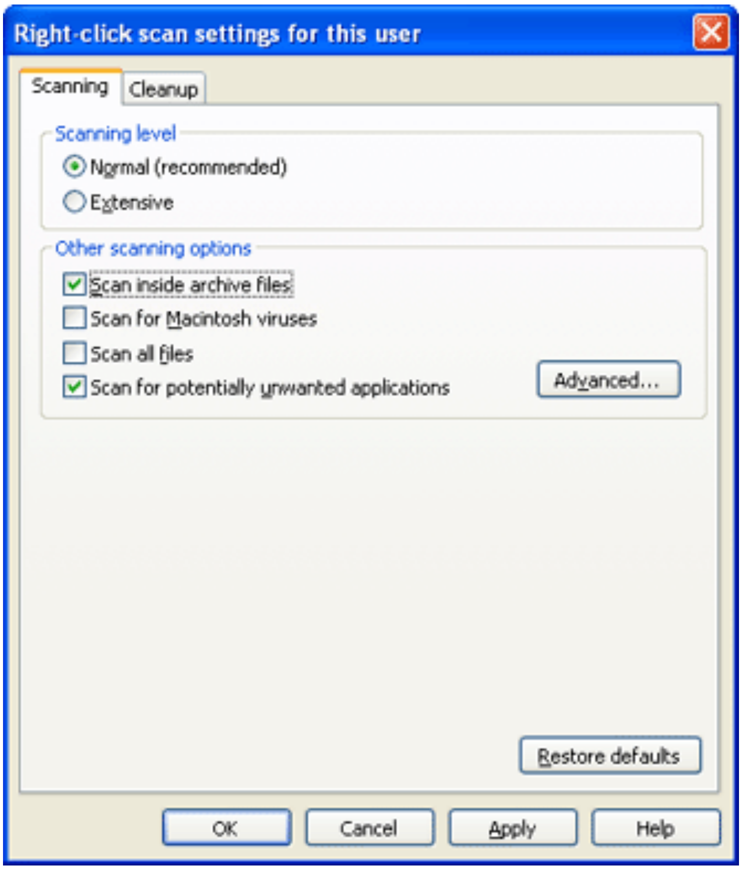
Scanning inside archive files makes scanning significantly slower. Even if you don't select the option, when you attempt to access a file extracted from the archive file, the extracted file is scanned.

Whether you select this option or not, files compressed with dynamic compression utilities (PKLite, LZEXE and Diet) are scanned.

1. On the **Configure** menu, click **Right–click scanning**.

2. In the **Right–click scan settings for this user** dialog box, click the **Scanning** tab.

3. Select **Scan inside archive files**.



Right-click scan settings for this user

Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

☑ Scan inside archive files

☐ Scan for Macintosh viruses

☐ Scan all files

☑ Scan for potentially unwanted applications

To enable scanning inside only particular archive file types, click **Advanced**. In the **Advanced scanning settings** dialog box, select the archive file types that you want Sophos Anti–Virus to scan inside.

⚠ The advanced settings are very specialized and you should use them only with advice from Sophos technical support.

Scanning Macintosh files

You can enable Sophos Anti–Virus to scan Macintosh files stored on Windows computers. You can do this for

- on–access scanning
- on–demand scanning
- scans run from a right–click menu.

Scanning Macintosh files on access

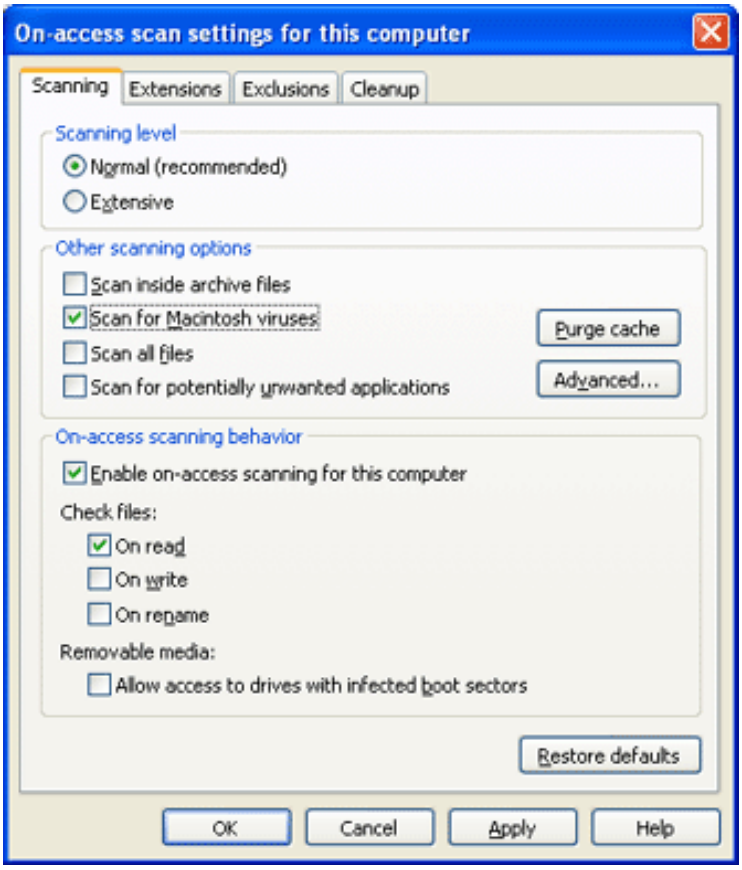
⚠ If the Sophos Enterprise Console is used to administer Sophos Anti–Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

1. In the home page of the **Sophos Anti–Virus** window, click **Configure Sophos Anti–Virus**.

2. In the **Configure** page, click **On–access scanning**.

3. In the **On–access scan settings for this computer** dialog box, click the **Scanning** tab.

4. Select **Scan for Macintosh viruses**. This enables Sophos Anti−Virus to scan executable Macintosh files.



On-access scan settings for this computer

Scanning level

● Normal (recommended)
○ Extensive

Other scanning options

□ Scan inside archive files
☑ Scan for Macintosh viruses
□ Scan all files
□ Scan for potentially unwanted applications

On-access scanning behavior

☑ Enable on-access scanning for this computer

Check files:

☑ On read
□ On write
□ On rename

Removable media:

□ Allow access to drives with infected boot sectors

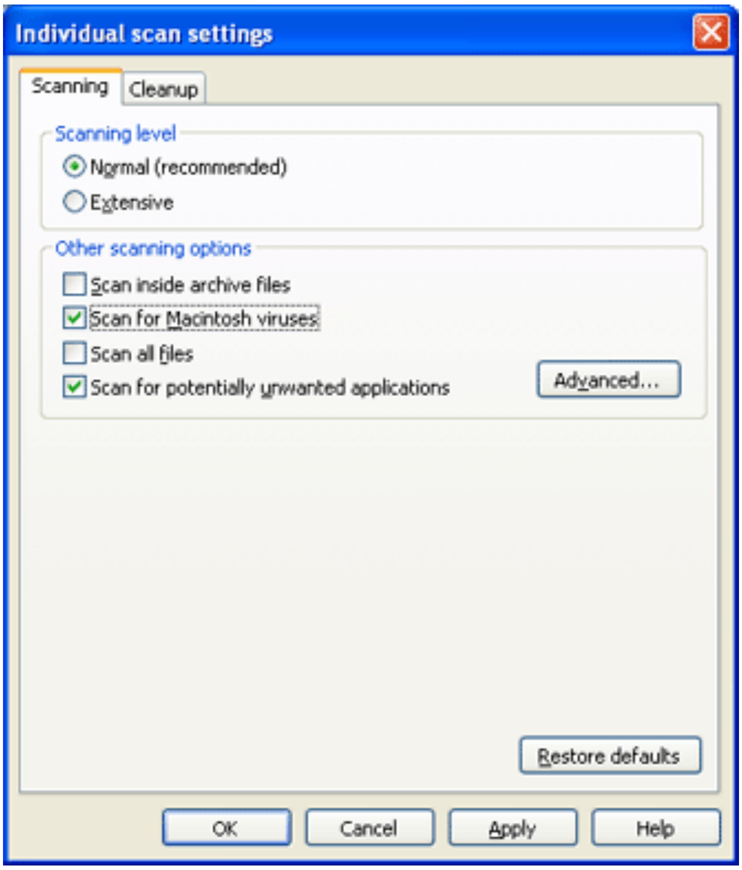
Scanning Macintosh files on demand

1. In the home page of the **Sophos Anti−Virus** window, in the **Available scans** list, select the scan you want to edit. Click **Edit**.

2. In the scan setup page, click **Configure this scan**.

3. In the **Individual scan settings** dialog box, click the **Scanning** tab.

4. Select **Scan for Macintosh viruses**. This enables Sophos Anti−Virus to scan executable Macintosh files.



Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

☐ Scan inside archive files

☑ Scan for Macintosh viruses

☐ Scan all files

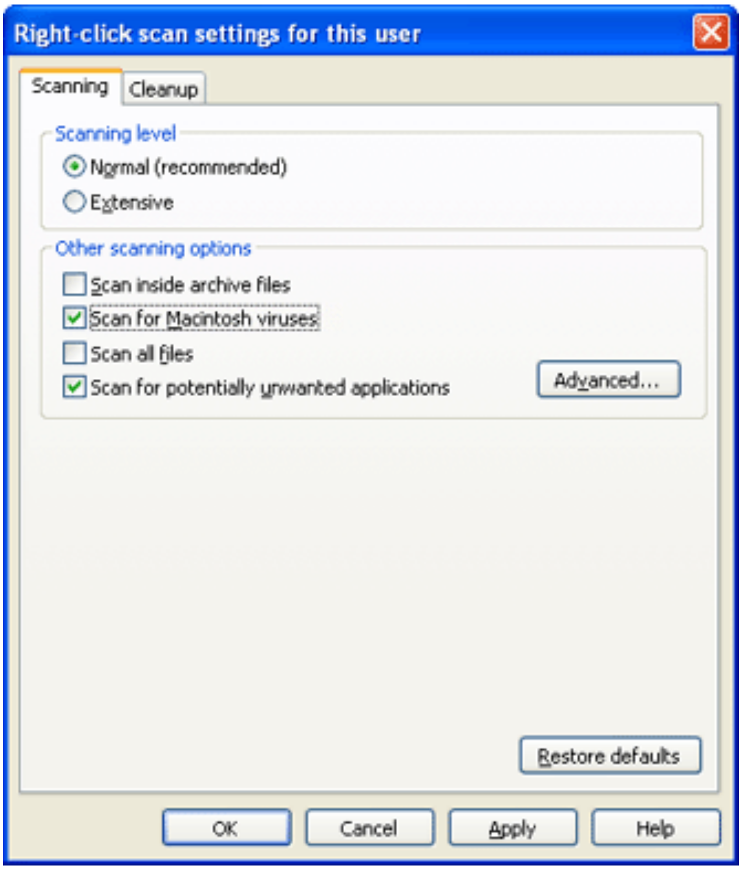
☑ Scan for potentially unwanted applications

Scanning Macintosh files from a right−click menu

1. On the **Configure** menu, click **Right−click scanning**.

2. In the **Right−click scan settings for this user** dialog box, click the **Scanning** tab.

3. Select **Scan for Macintosh viruses**. This enables Sophos Anti−Virus to scan executable Macintosh files.



Right-click scan settings for this user

Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

□ Scan inside archive files

☑ Scan for Macintosh viruses

□ Scan all files

☑ Scan for potentially unwanted applications

Scanning all files

Scanning all files, regardless of the filename extension, makes scanning slower and is generally not required. Sophos does not recommend selecting this option, except on the advice of Sophos technical support.

If you want to enable Sophos Anti−Virus to scan all files, you can do this for

- on−access scanning
- on−demand scanning
- scans run from a right−click menu.

Scanning all files on access

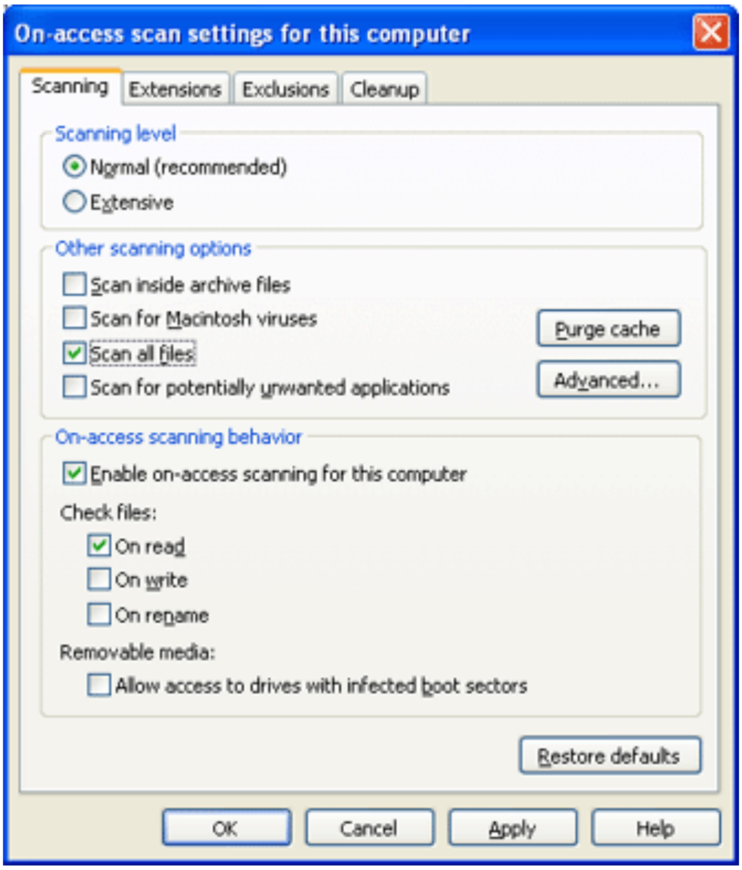
If the Sophos Enterprise Console is used to administer Sophos Anti−Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

2. In the **Configure** page, click **On−access scanning**.

3. In the **On−access scan settings for this computer** dialog box, click the **Scanning** tab.

4. Select **Scan all files**.



On-access scan settings for this computer

Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

□ Scan inside archive files

□ Scan for Macintosh viruses

☑ Scan all files

□ Scan for potentially unwanted applications

On-access scanning behavior

☑ Enable on-access scanning for this computer

Check files:

☑ On read

□ On write

□ On rename

Removable media:

□ Allow access to drives with infected boot sectors

Scanning all files on demand

You can enable

- all on−demand scans
- a particular on−demand scan

to scan all files.

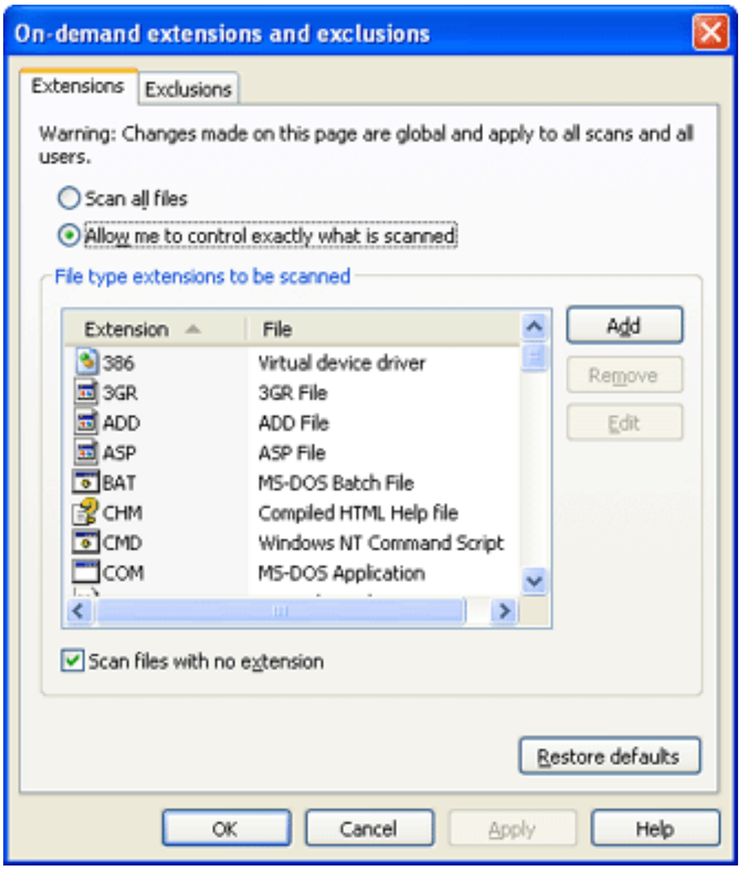
Enabling all on−demand scans to scan all files

1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

2. In the **Configure** page, click **On−demand extensions and exclusions**.

3. In the **On–demand extensions and exclusions** dialog box, click the **Extensions** tab.

4. Click **Scan all files**.



Warning: Changes made on this page are global and apply to all scans and all users.

○ Scan all files
● Allow me to control exactly what is scanned

File type extensions to be scanned

Extension	File
386	Virtual device driver
3GR	3GR File
ADD	ADD File
ASP	ASP File
BAT	MS-DOS Batch File
CHM	Compiled HTML Help file
CMD	Windows NT Command Script
COM	MS-DOS Application

☑ Scan files with no extension

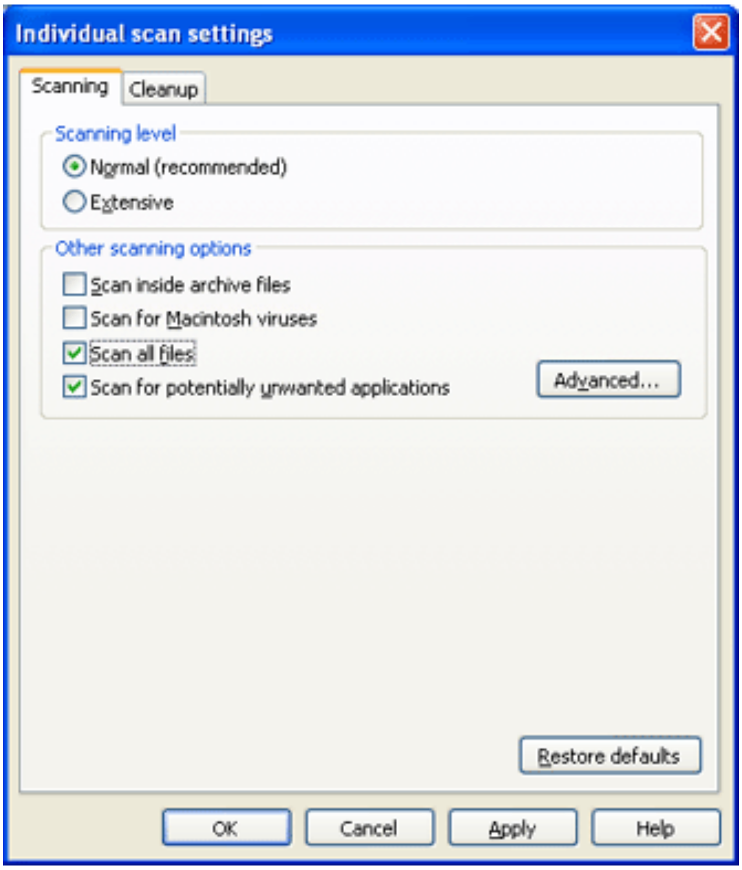
Enabling a particular on–demand scan to scan all files

1. In the home page of the **Sophos Anti–Virus** window, in the **Available scans** list, select the scan you want to edit. Click **Edit**.

2. In the scan setup page, click **Configure this scan**.

3. In the **Individual scan settings** dialog box, click the **Scanning** tab.

4. Select **Scan all files**.



Individual scan settings

Scanning level
● Normal (recommended)
○ Extensive

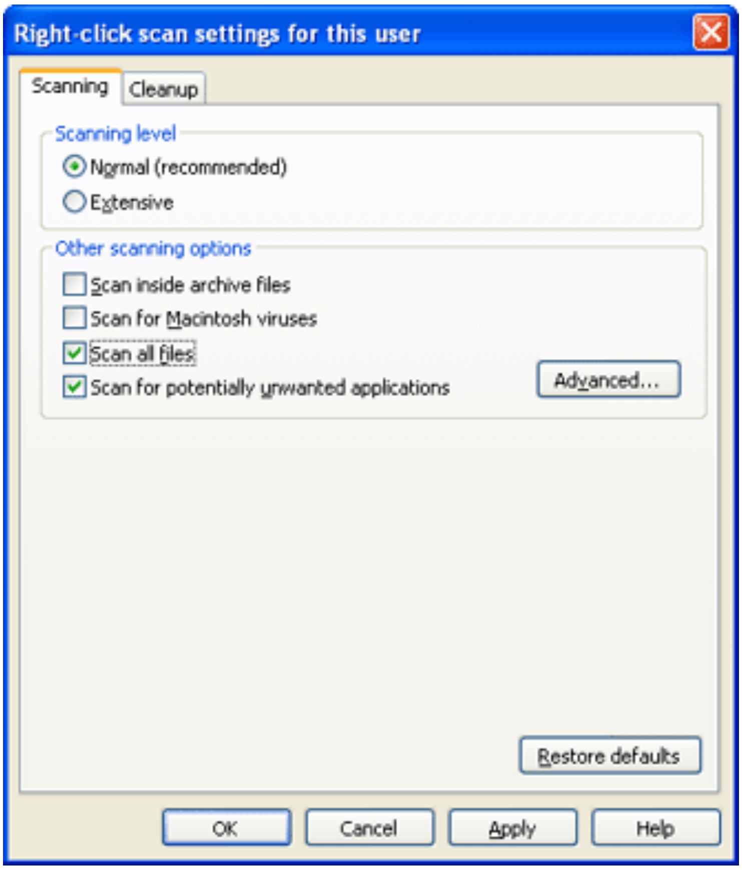
Other scanning options
□ Scan inside archive files
□ Scan for Macintosh viruses
☑ Scan all files
☑ Scan for potentially unwanted applications

Scanning all files from a right−click menu

1. On the **Configure** menu, click **Right−click scanning**.

2. In the **Right−click scan settings for this user** dialog box, click the **Scanning** tab.

3. Select **Scan all files**.



Scanning level

● Normal (recommended)
○ Extensive

Other scanning options

☐ Scan inside archive files
☐ Scan for Macintosh viruses
☑ Scan all files
☑ Scan for potentially unwanted applications

Scanning for potentially unwanted applications

You can enable Sophos Anti–Virus to scan for potentially unwanted applications. You can do this for

- on–access scanning
- on–demand scanning
- scans run from a right–click menu.

Scanning for potentially unwanted applications on access

If the Sophos Enterprise Console is used to administer Sophos Anti–Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

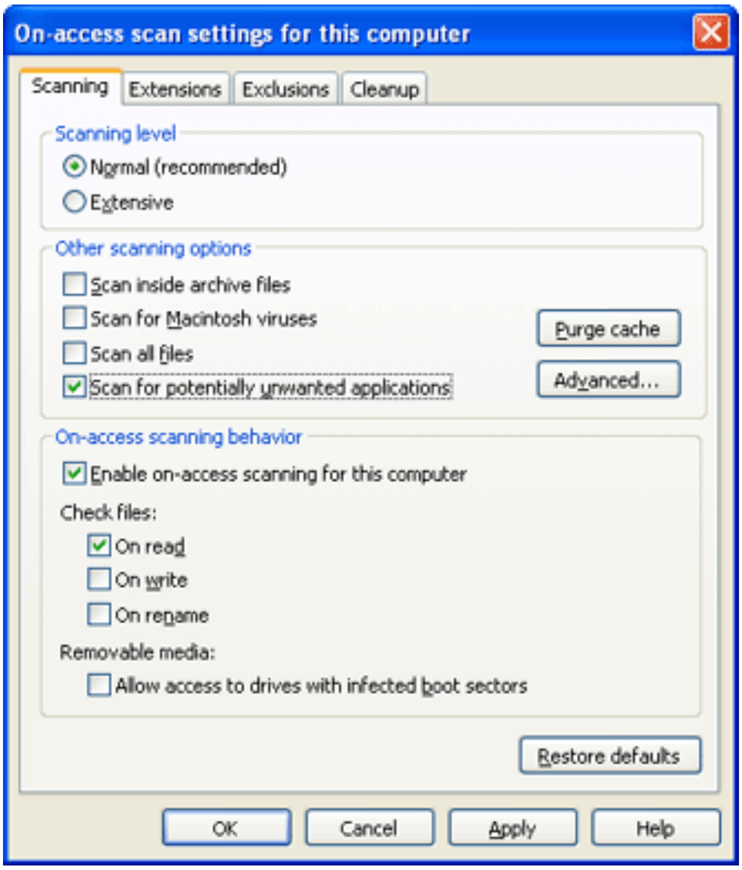
1. In the home page of the **Sophos Anti–Virus** window, click **Configure Sophos Anti–Virus**.

2. In the **Configure** page, click **On–access scanning**.

3. In the **On–access scan settings for this computer** dialog box, click the **Scanning** tab.

4. Select **Scan for potentially unwanted applications**.

⚠ The advanced settings are very specialized and you should use them only with advice from Sophos technical support.



On-access scan settings for this computer

Scanning level

● Normal (recommended)
○ Extensive

Other scanning options

□ Scan inside archive files
□ Scan for Macintosh viruses
□ Scan all files
☑ Scan for potentially unwanted applications

On-access scanning behavior

☑ Enable on-access scanning for this computer

Check files:

☑ On read
□ On write
□ On rename

Removable media:

□ Allow access to drives with infected boot sectors

Scanning for potentially unwanted applications on demand

1. In the home page of the **Sophos Anti–Virus** window, in the **Available scans** list, select the scan you want to edit. Click **Edit**.

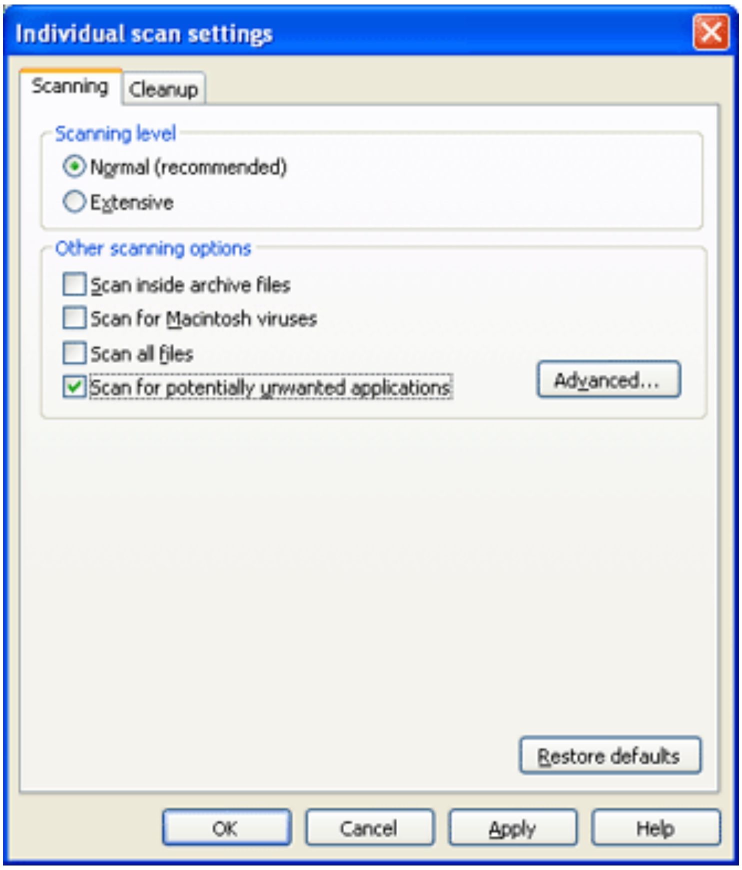
2. In the scan setup page, click **Configure this scan**.

3. In the **Individual scan settings** dialog box, click the **Scanning** tab.

4. Select **Scan for potentially unwanted applications**.

⚠ The advanced settings are very specialized and you should use them only with advice from Sophos technical support.

⚠ If in the **Advanced scanning settings** dialog box you choose to disable scanning of memory and registry while scanning for potentially unwanted applications, Sophos Anti–Virus will ***not*** be able to fully detect and subsequently remove certain applications from your computer.



Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

□ Scan inside archive files

□ Scan for Macintosh viruses

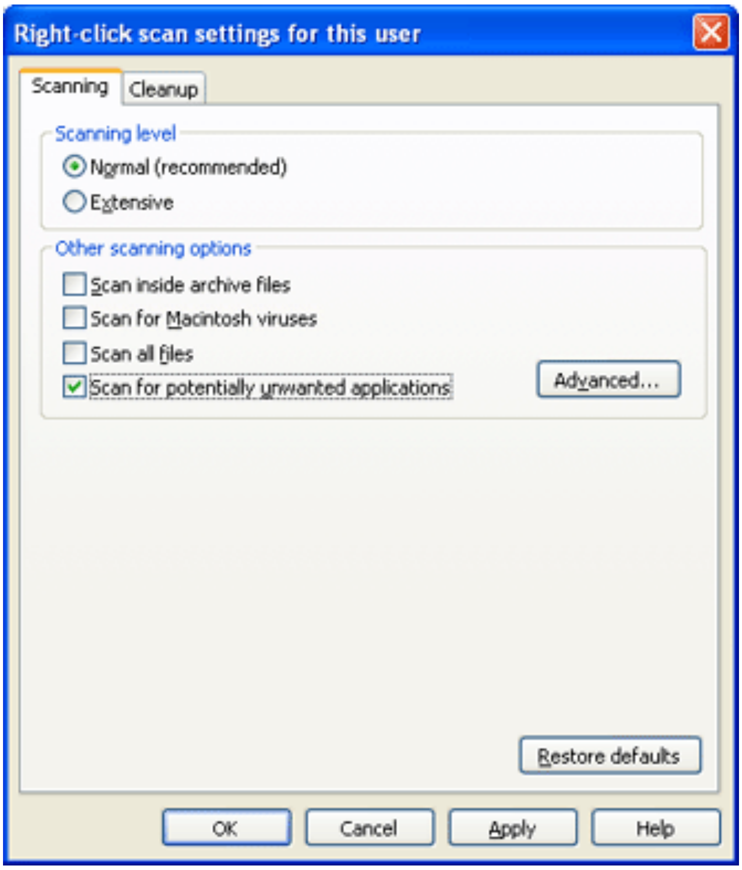
□ Scan all files

☑ Scan for potentially unwanted applications

Scanning for potentially unwanted applications from a right–click menu

1. On the **Configure** menu, click **Right–click scanning**.
2. In the **Right–click scan settings for this user** dialog box, click the **Scanning** tab.
3. Select **Scan for potentially unwanted applications**.

The advanced settings are very specialized and you should use them only with advice from Sophos technical support.



Right-click scan settings for this user

Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

□ Scan inside archive files

□ Scan for Macintosh viruses

□ Scan all files

☑ Scan for potentially unwanted applications

Configuring alerts

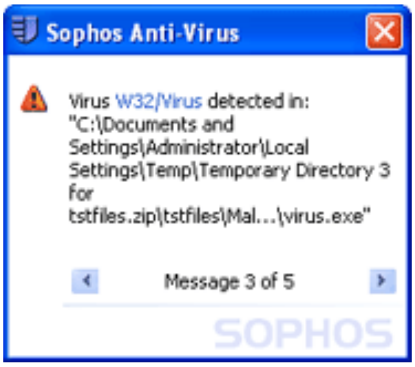
This section includes the following.

- Desktop messaging
- Email alerting
- SNMP messaging
- Event logging

Desktop messaging

If the Sophos Enterprise Console is used to administer Sophos Anti−Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

Sophos Anti−Virus can display desktop messages like the one shown below when a threat is found. This applies only to on−access scanning.



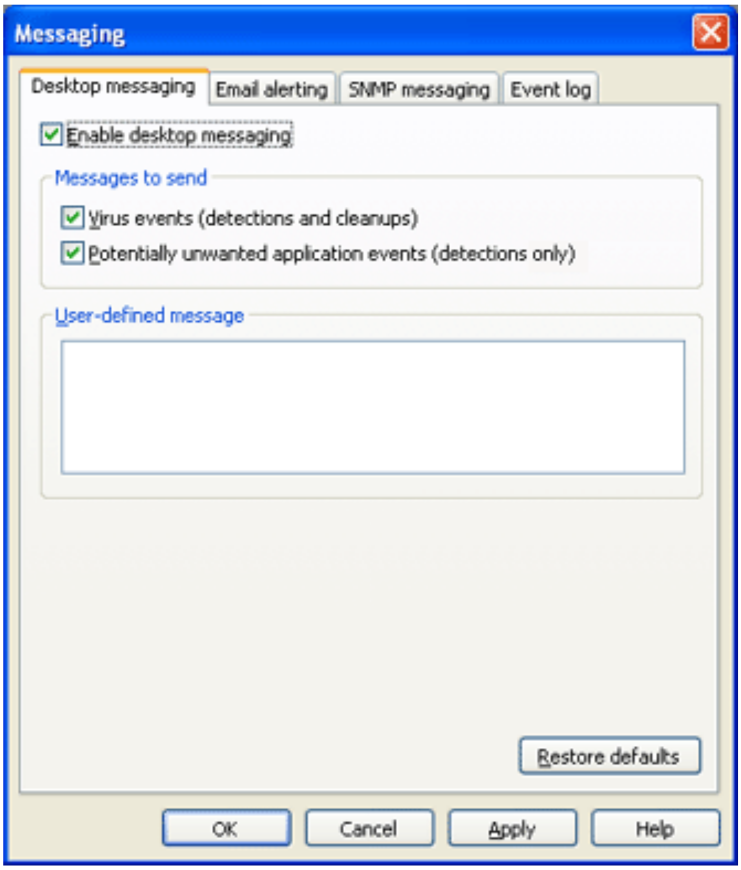
Virus W32/Virus detected in: "C:\Documents and Settings\Administrator\Local Settings\Temp\Temporary Directory 3 for tstfiles.zip\tstfiles\Mal...\virus.exe"

To enable Sophos Anti−Virus to display desktop messages, do as follows.

1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

2. In the **Configure** page, click **Messaging**.

3. In the **Messaging** dialog box, click the **Desktop messaging** tab. Set the options as described below.



☑ Enable desktop messaging

☑ Virus events (detections and cleanups)

☑ Potentially unwanted application events (detections only)

Enable desktop messaging

Select this to enable Sophos Anti–Virus to display desktop messages when a threat is found.

Messages to send

Select the events for which you want Sophos Anti–Virus to display desktop messages.

User–defined message

In this text box, you can type a message that will be added to the end of the standard message.

Email alerting

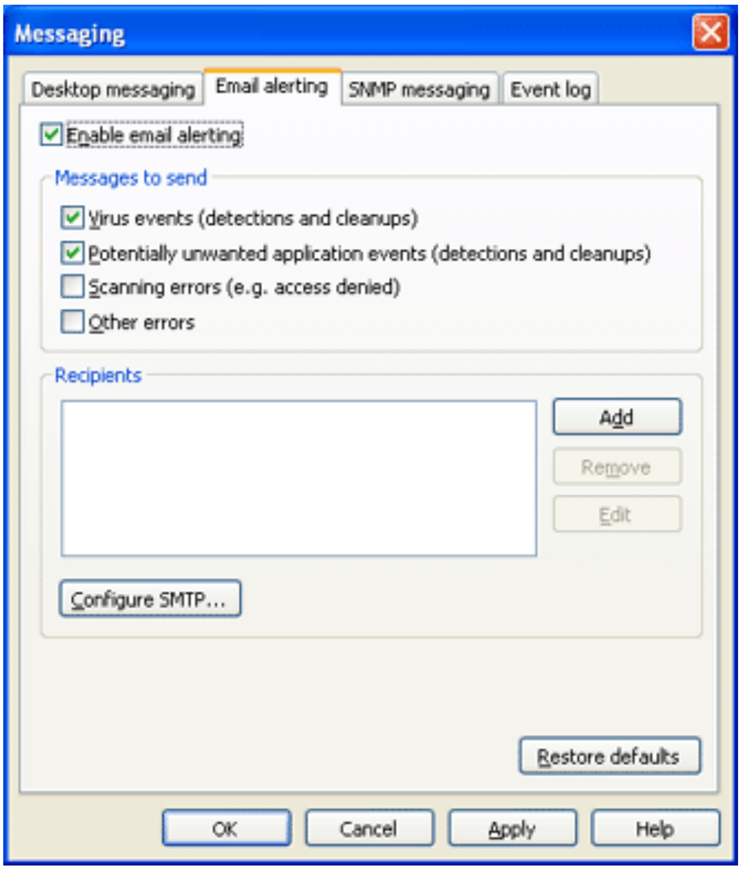
If the Sophos Enterprise Console is used to administer Sophos Anti–Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

To enable Sophos Anti–Virus to send email alerts when a threat is found or an error occurs, do as follows. This applies to on–access, on–demand and right–click scanning.

1. In the home page of the **Sophos Anti–Virus** window, click **Configure Sophos Anti–Virus**.

2. In the **Configure** page, click **Messaging**.

3. In the **Messaging** dialog box, click the **Email alerting** tab. Set the options as described below.



Messaging

☑ Enable email alerting

Messages to send

☑ Virus events (detections and cleanups)
☑ Potentially unwanted application events (detections and cleanups)
☐ Scanning errors (e.g. access denied)
☐ Other errors

Recipients

Enable email alerting

Select this to enable Sophos Anti–Virus to send email alerts.

Messages to send

Select the events for which you want Sophos Anti–Virus to send email alerts. **Scanning errors** include instances when Sophos Anti–Virus is denied access to an item that it attempts to scan.

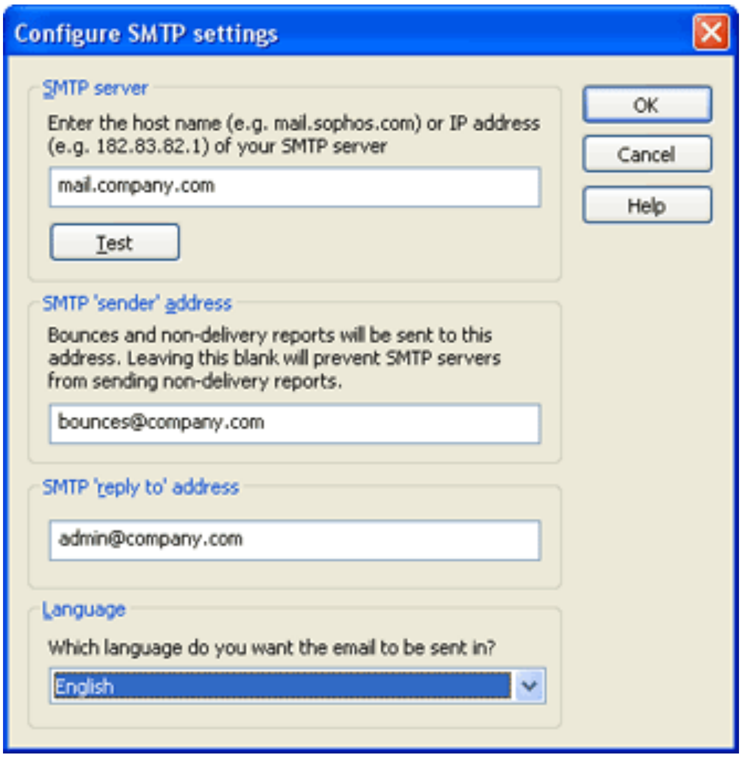
Recipients

Click **Add** or **Remove** to add or remove, respectively, email addresses to which email alerts should be sent. Click **Edit** to change an email address you have added.

Configure SMTP

Click this to change the settings for the SMTP server and the language of the email alerts. (Refer to Configure SMTP settings.)

Configure SMTP settings



SMTP server

Enter the host name (e.g. mail.sophos.com) or IP address (e.g. 182.83.82.1) of your SMTP server

mail.company.com

SMTP 'sender' address

Bounces and non-delivery reports will be sent to this address. Leaving this blank will prevent SMTP servers from sending non-delivery reports.

bounces@company.com

SMTP 'reply to' address

admin@company.com

Language

Which language do you want the email to be sent in?

English

SMTP server

In the text box, type the host name or IP address of the SMTP server. Click **Test** to test that a connection to the SMTP server can be made. (This does *not* send a test email.)

SMTP 'sender' address

In the text box, type an email address to which bounces and non–delivery reports can be sent.

SMTP 'reply to' address

As email alerts are sent from an unattended mailbox, you can type in the text box an email address to which replies to email alerts can be sent.

Language

Click the drop−down arrow, and select the language in which email alerts should be sent.

SNMP messaging

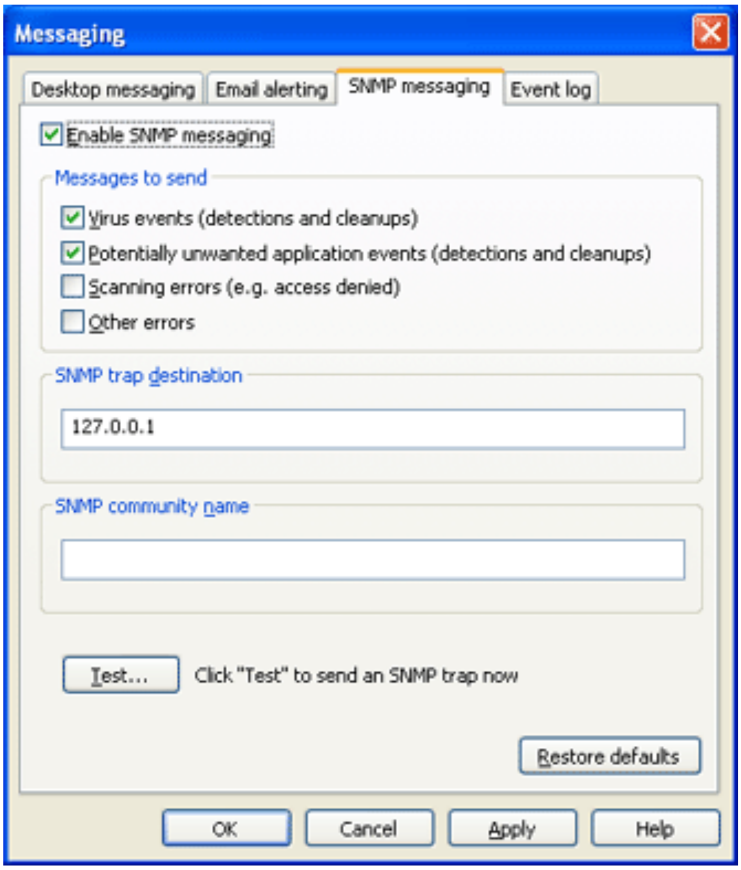
⚠ If the Sophos Enterprise Console is used to administer Sophos Anti−Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

To enable Sophos Anti−Virus to send SNMP messages when a threat is found or an error occurs, do as follows. This applies to on−access, on−demand and right−click scanning.

1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

2. In the **Configure** page, click **Messaging**.

3. In the **Messaging** dialog box, click the **SNMP messaging** tab. Set the options as described below.



☑ Enable SNMP messaging

Messages to send

☑ Virus events (detections and cleanups)

☑ Potentially unwanted application events (detections and cleanups)

□ Scanning errors (e.g. access denied)

□ Other errors

SNMP trap destination: 127.0.0.1

SNMP community name:

Click "Test" to send an SNMP trap now

Enable SNMP messaging

Select this to enable Sophos Anti–Virus to send SNMP messages.

Messages to send

Select the events for which you want Sophos Anti–Virus to send email alerts. **Scanning errors** include instances when Sophos Anti–Virus is denied access to an item that it attempts to scan.

SNMP trap destination

In the text box, type the IP address or name of the computer to which alerts are sent.

SNMP community name

In the text box, type the SNMP community name.

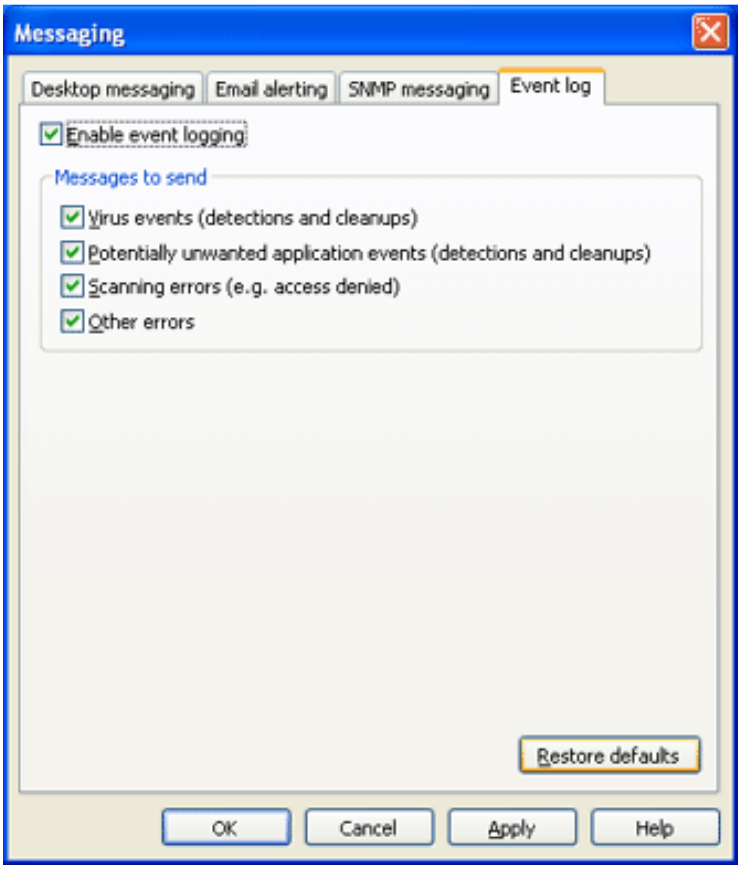
Test

Click this to send a test SNMP message to the SNMP trap destination you have specified.

Event logging

To enable Sophos Anti–Virus to add alerts to the Windows 2000 or later event log when a threat is found or an error occurs, do as follows. This applies to on–access, on–demand and right–click scanning.

1. In the home page of the **Sophos Anti–Virus** window, click **Configure Sophos Anti–Virus**.
2. In the **Configure** page, click **Messaging**.
3. In the **Messaging** dialog box, click the **Event log** tab. Set the options as described below.



☑ Enable event logging

Messages to send

☑ Virus events (detections and cleanups)

☑ Potentially unwanted application events (detections and cleanups)

☑ Scanning errors (e.g. access denied)

☑ Other errors

Enable event logging

Select this to enable Sophos Anti–Virus to send messages to the Windows event log.

Messages to send

Select the events for which you want Sophos Anti−Virus to send messages. **Scanning errors** include instances when Sophos Anti−Virus is denied access to an item that it attempts to scan.

Logging

This section includes the following.

- Viewing the log for this computer
- Configuring the log for this computer
- Viewing the log for an on–demand scan

Viewing the log for this computer

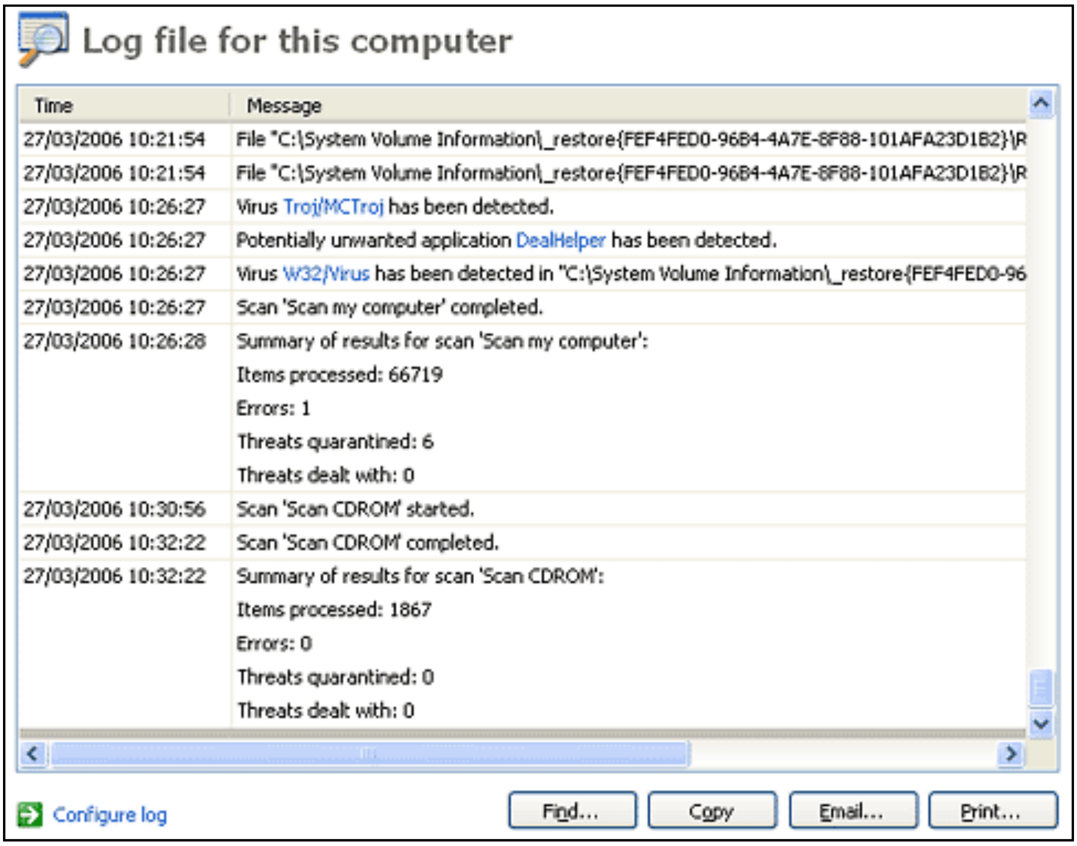
The **log for this computer** is a log of all scanning on the computer.

1. In the home page of the **Sophos Anti–Virus** window, click **Configure Sophos Anti–Virus**.

2. In the **Configure** page, click **View log** to display the log for the computer.

3. From the log page, you can copy the log to the clipboard, or email, or print the log.

   To find specific text in the log, click **Find** and enter the text you want to find.



Log file for this computer

```
Time                 Message
27/03/2006 10:21:54  File "C:\System Volume Information\_restore{FEF4FED0-96B4-4A7E-8F88-101AFA23D1B2}\R
27/03/2006 10:21:54  File "C:\System Volume Information\_restore{FEF4FED0-96B4-4A7E-8F88-101AFA23D1B2}\R
27/03/2006 10:26:27  Virus Troj/MCTroj has been detected.
27/03/2006 10:26:27  Potentially unwanted application DealHelper has been detected.
27/03/2006 10:26:27  Virus W32/Virus has been detected in "C:\System Volume Information\_restore{FEF4FED0-96
27/03/2006 10:26:27  Scan 'Scan my computer' completed.
27/03/2006 10:26:28  Summary of results for scan 'Scan my computer':
                     Items processed: 66719
                     Errors: 1
                     Threats quarantined: 6
                     Threats dealt with: 0
27/03/2006 10:30:56  Scan 'Scan CDROM' started.
27/03/2006 10:32:22  Scan 'Scan CDROM' completed.
27/03/2006 10:32:22  Summary of results for scan 'Scan CDROM':
                     Items processed: 1867
                     Errors: 0
                     Threats quarantined: 0
                     Threats dealt with: 0
```

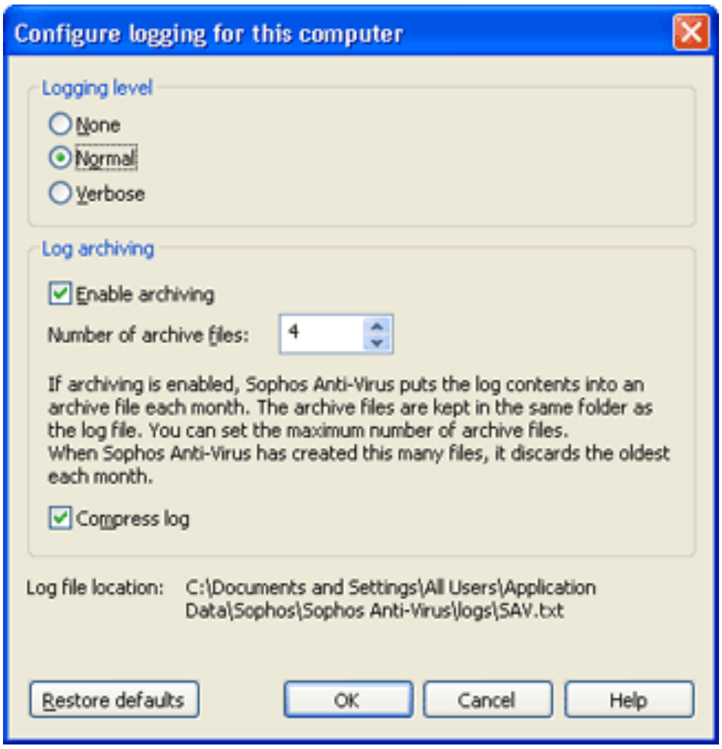
Configuring the log for this computer

The **log for this computer** is a log of all scanning on the computer.

It is stored in the following location:

C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Anti–Virus\logs\SAV.txt

1. In the home page of the **Sophos Anti–Virus** window, click **Configure Sophos Anti–Virus**.
2. In the **Configure** page, click **View log**.
3. In the log page, click **Configure log** to display the **Configure logging for this computer** dialog box. Set the options as described below.



Configure logging for this computer

Logging level

○ None
● Normal
○ Verbose

Log archiving

☑ Enable archiving

Number of archive files: 4

If archiving is enabled, Sophos Anti-Virus puts the log contents into an archive file each month. The archive files are kept in the same folder as the log file. You can set the maximum number of archive files.
When Sophos Anti-Virus has created this many files, it discards the oldest each month.

☑ Compress log

Log file location: C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Anti-Virus\logs\SAV.txt

Logging level

To stop anything being logged, click **None**. To log summary information, error messages and so on, click **Normal**. To log most information, including files scanned, major stages of a scan, and so on, click **Verbose**.

Log archiving

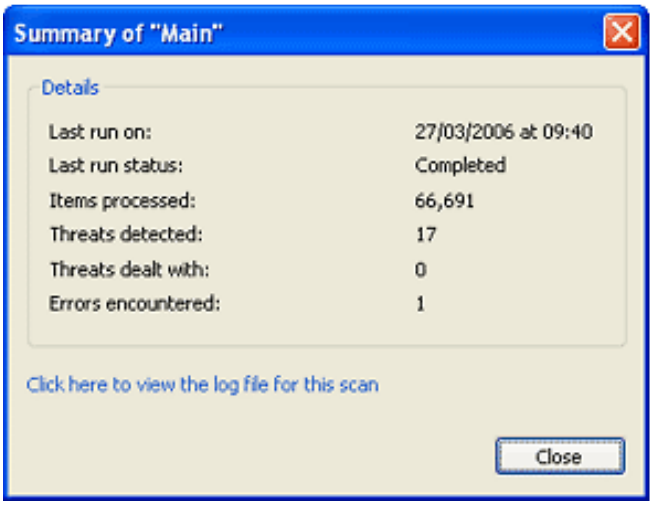
To enable the log file to be archived monthly, select **Enable archiving**. Select the **Number of archive files** to store before the oldest one is deleted. Select **Compress log** to reduce the size of the log file.

Viewing the log for an on–demand scan

The **log for an on–demand scan** is a log of what happened each time that scan was run.

1. In the home page of the **Sophos Anti–Virus** window, in the **Available scans** list, select the scan for which you want to view the log. Click **Summary**.

2. In the summary dialog box, click the link at the bottom.



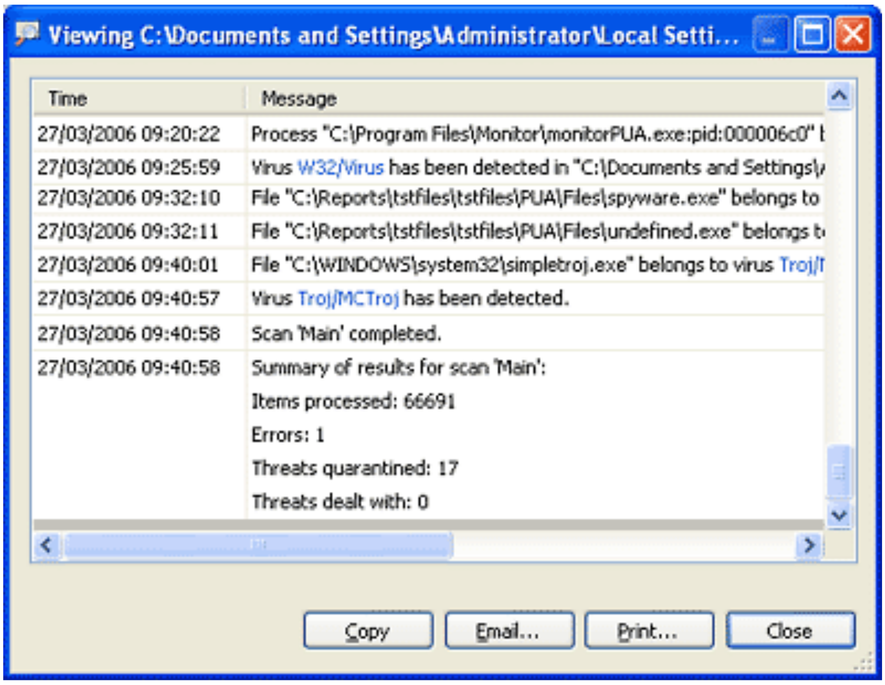
Summary of "Main"

Details

Last run on:	27/03/2006 at 09:40
Last run status:	Completed
Items processed:	66,691
Threats detected:	17
Threats dealt with:	0
Errors encountered:	1

Click here to view the log file for this scan

3. From the log window, you can copy the log to the clipboard, or email or print the log.


Viewing C:\Documents and Settings\Administrator\Local Setti...
Copy
Email...
Print...
Close

Time	Message
27/03/2006 09:20:22	Process "C:\Program Files\Monitor\monitorPUA.exe:pid:000006c0" b
27/03/2006 09:25:59	Virus W32/Virus has been detected in "C:\Documents and Settings\
27/03/2006 09:32:10	File "C:\Reports\tstfiles\tstfiles\PUA\Files\spyware.exe" belongs to
27/03/2006 09:32:11	File "C:\Reports\tstfiles\tstfiles\PUA\Files\undefined.exe" belongs t
27/03/2006 09:40:01	File "C:\WINDOWS\system32\simpletroj.exe" belongs to virus Troj/I
27/03/2006 09:40:57	Virus Troj/MCTroj has been detected.
27/03/2006 09:40:58	Scan 'Main' completed.
27/03/2006 09:40:58	Summary of results for scan 'Main': Items processed: 66691 Errors: 1 Threats quarantined: 17 Threats dealt with: 0

Updating

This section includes the following.

- Updating immediately
- Setting up automatic updating
- Setting a source for updates
- Setting an alternative source for updates
- Scheduling updates
- Updating via a proxy
- Limiting the bandwidth used
- Logging updates

Updating immediately

If you have installed Sophos Anti–Virus as recommended in Sophos documentation, updating occurs automatically.

If you want to update Sophos Anti–Virus immediately, you can do so.

1. Locate the Sophos Anti–Virus icon in the system tray (shown below).

2. Right–click the icon to display a menu, and select **Update now**.

Alternatively, double–click the Sophos Anti–Virus system tray icon.

Provided Sophos Anti–Virus has been correctly configured, it checks the usual source for new software and, if necessary, updates itself.

For information on configuring updating, refer to the other pages in this section.

Setting up automatic updating

If your computer is on a network, or if your administrator installed Sophos Anti–Virus for you, Sophos Anti–Virus should have been set to update itself automatically.

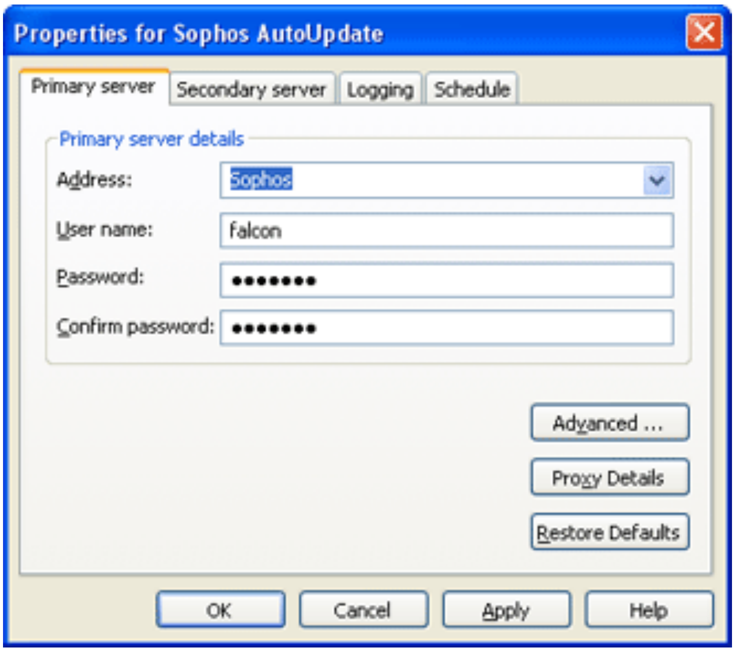
If automatic updating has not been set up, follow the steps below. For full information on the options at each step, refer to the section describing that configuration page.

You need to be a Sophos Administrator to set up automatic updating.

1. Locate the Sophos Anti−Virus icon in the system tray (shown below).

2. Right−click the icon to display a menu, and select **Configure updating**.

3. In the **Properties for Sophos AutoUpdate** dialog box, click the **Primary server** tab and set the source for updates. Your administrator can give you the details you need to enter.


Properties for Sophos AutoUpdate

Primary server details

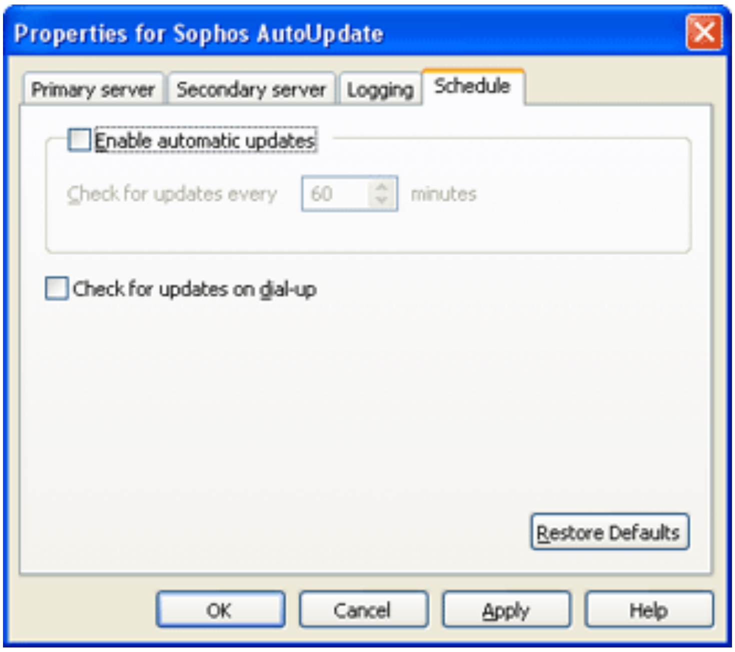
Address: Sophos

User name: falcon

Password: •••••••

Confirm password: •••••••

4. Click the **Schedule** tab and schedule updates.



☐ Enable automatic updates

Check for updates every 60 minutes

☐ Check for updates on dial-up

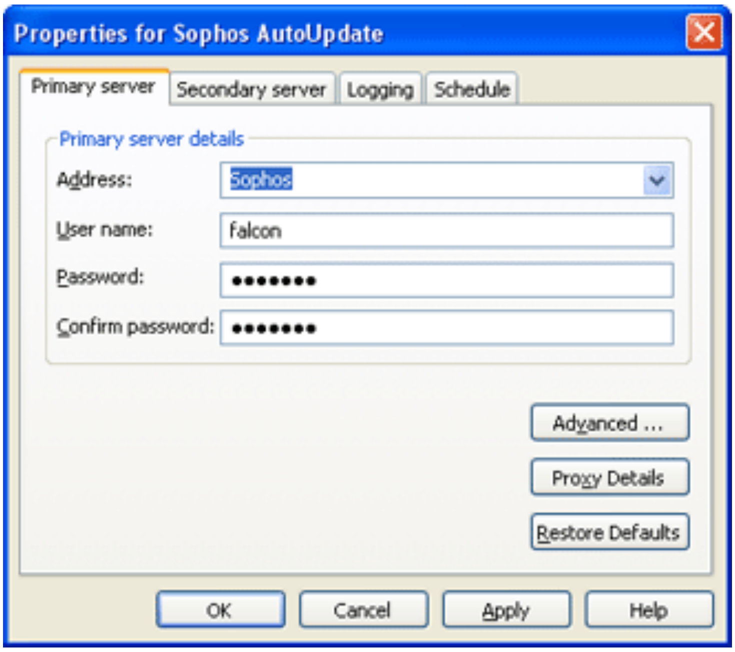
Setting a source for updates

If you want Sophos Anti–Virus to update itself automatically, you must specify where it fetches updates from.

1. Locate the Sophos Anti–Virus icon in the system tray (shown below).

2. Right–click the icon to display a menu, and select **Configure updating**.

3. In the **Properties for Sophos AutoUpdate** dialog box, click the **Primary server** tab and enter the details needed as described below.



Properties for Sophos AutoUpdate

Address: Sophos

User name: falcon

Password: •••••••

Confirm password: •••••••

Address

Enter the address (UNC (network) path or web address) from which Sophos Anti–Virus will usually fetch updates. If you select **Sophos**, Sophos Anti–Virus will download updates directly from Sophos via the internet.

Your administrator can give you the address and account details you need.

User name

If necessary, enter the **User name** for the account that will be used to access the server, and then enter and confirm the **Password**.

If the **User name** needs to be qualified to indicate the domain, use the form domain\username.

If you want to limit the bandwidth used, click **Advanced**.

If you access the internet via a proxy server, click **Apply** and then **Proxy Details**. Note that some internet service providers require web requests to be sent to a proxy server.

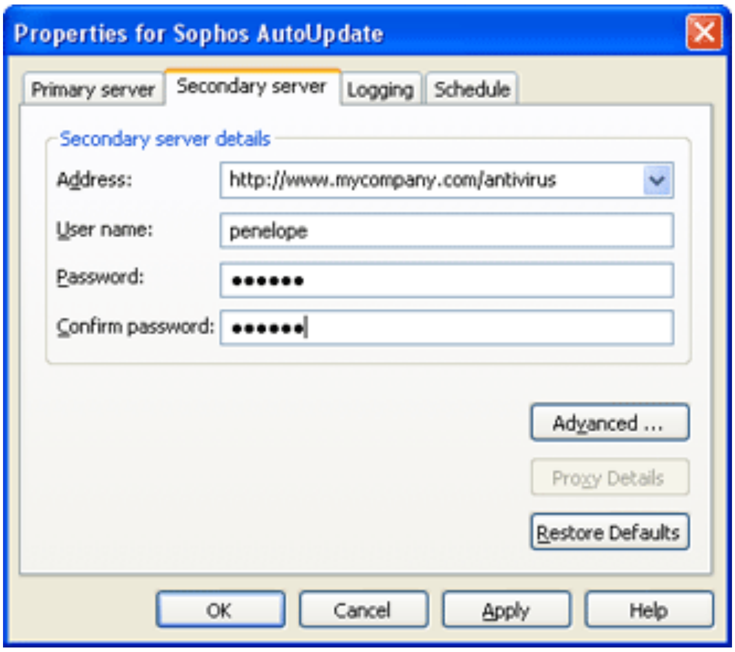
Setting an alternative source for updates

You can set an alternative source for updates. If Sophos Anti–Virus cannot contact its usual source, it will attempt to update from this alternative source.

1. Locate the Sophos Anti–Virus icon in the system tray (shown below).

2. Right–click the icon to display a menu, and select **Configure updating**.

3. In the **Properties for Sophos AutoUpdate** dialog box, click the **Secondary server** tab. Then enter the details as described below.



Address: http://www.mycompany.com/antivirus

User name: penelope

Password: ••••••

Confirm password: ••••••

Address

Enter the **Address** (UNC (network) path or web address) from which Sophos Anti–Virus will fetch updates if it cannot contact the usual source. If you select **Sophos**, Sophos Anti–Virus will download updates directly from Sophos via the internet.

Your administrator can give you the address and account details you need.

User name

If necessary, enter the **User name** for the account that will be used to access the server, and then enter and confirm the **Password**.

If the **User name** needs to be qualified to indicate the domain, use the form domain\username.

If you want to limit the bandwidth used, click **Advanced**.

If you access the address via a proxy server, click **Apply** and then **Proxy Details**. Note that some internet service providers require web requests to be sent to a proxy server.

Scheduling updates

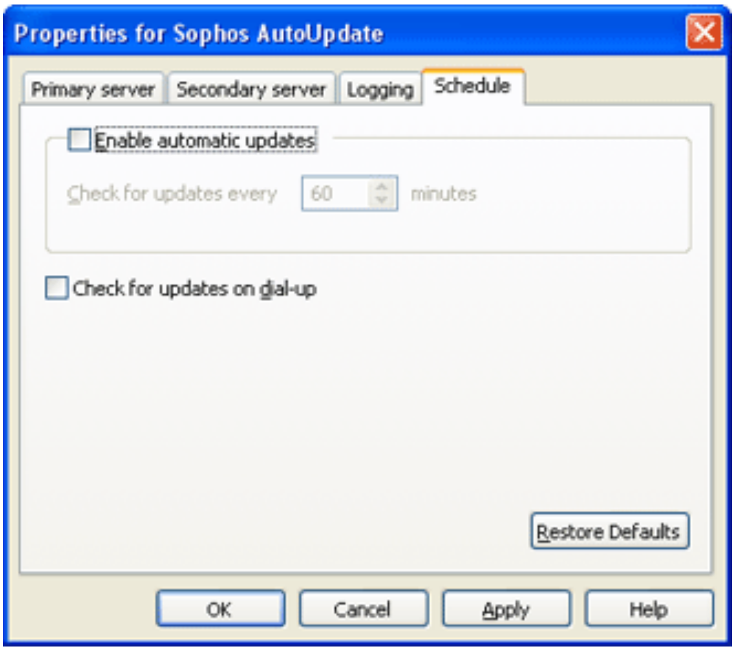
You can specify when or how often Sophos Anti−Virus updates itself.

If the Sophos Enterprise Console is used to administer Sophos Anti−Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

1. Locate the Sophos Anti−Virus icon in the system tray (shown below).

2. Right−click the icon to display a menu, and select **Configure updating**.

3. In the **Properties for Sophos AutoUpdate** dialog box, click the **Schedule** tab. Then enter the details as described below.



Properties for Sophos AutoUpdate

☐ Enable automatic updates

Check for updates every 60 minutes

☐ Check for updates on dial-up

If you want Sophos Anti−Virus to update itself at regular intervals, select **Enable automatic updates**. Then enter the frequency (in minutes) with which Sophos Anti–Virus will check for updated software. The default is 60 minutes.

If the updates are downloaded directly from Sophos, you cannot update more frequently than every 60 minutes.

If you update via a dial–up connection to the internet, select **Check for updates on dial–up**. Sophos Anti–Virus will attempt to update whenever you connect to the internet.

Updating via a proxy server

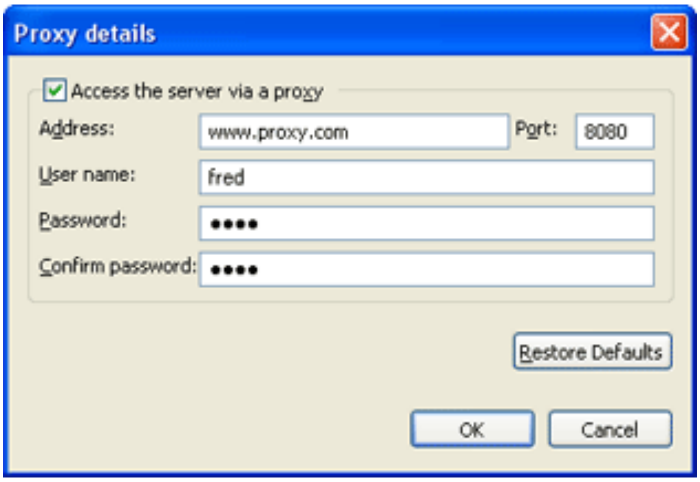
If Sophos Anti–Virus fetches updates via the internet, you must enter details of any proxy server that you use to connect to the internet.

1. Locate the Sophos Anti–Virus icon in the system tray (shown below).

2. Right–click the icon to display a menu, and select **Configure updating**.

3. In the **Properties for Sophos AutoUpdate** dialog box, click the **Primary server** tab or the **Secondary server** tab as required. Ensure that all the details have been correctly entered. Then click **Apply** and then **Proxy Details**.

4. In the **Proxy details** dialog box, select **Access the server via a proxy**. Then enter the proxy server **Address** and **Port** number. Enter a **User name** and **Password** that give access to the proxy server. If the user name needs to be qualified to indicate the domain, use the form domain\username.



Proxy details

☑ Access the server via a proxy

Address: www.proxy.com Port: 8080

User name: fred

Password: ••••

Confirm password: ••••

Limiting the bandwidth used

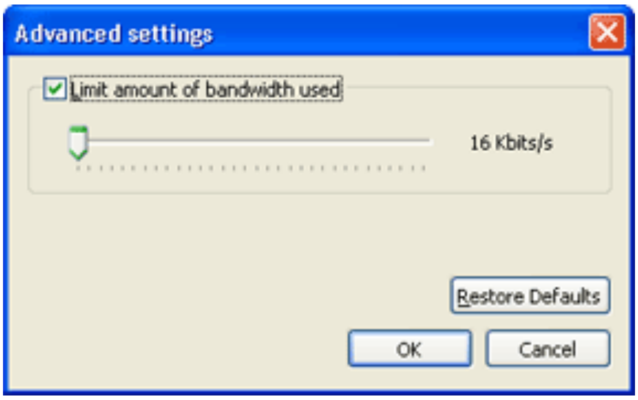
You can limit the bandwidth used for updating. This prevents Sophos Anti−Virus from using all your bandwidth when you need it for other purposes, e.g. downloading your email.

1. Locate the Sophos Anti−Virus icon in the system tray (shown below).

2. Right−click the icon to display a menu, and select **Configure updating**.

3. In the **Properties for Sophos AutoUpdate** dialog box, click the **Primary server** tab or the **Secondary server** tab as required. Then click **Advanced**.

4. In the **Advanced settings** dialog box, select **Limit amount of bandwidth used** and use the slider control to specify the bandwidth in Kbits/second. If you specify more bandwidth than the computer has available, Sophos Anti−Virus uses all that is available.



Advanced settings

☑ Limit amount of bandwidth used

16 Kbits/s

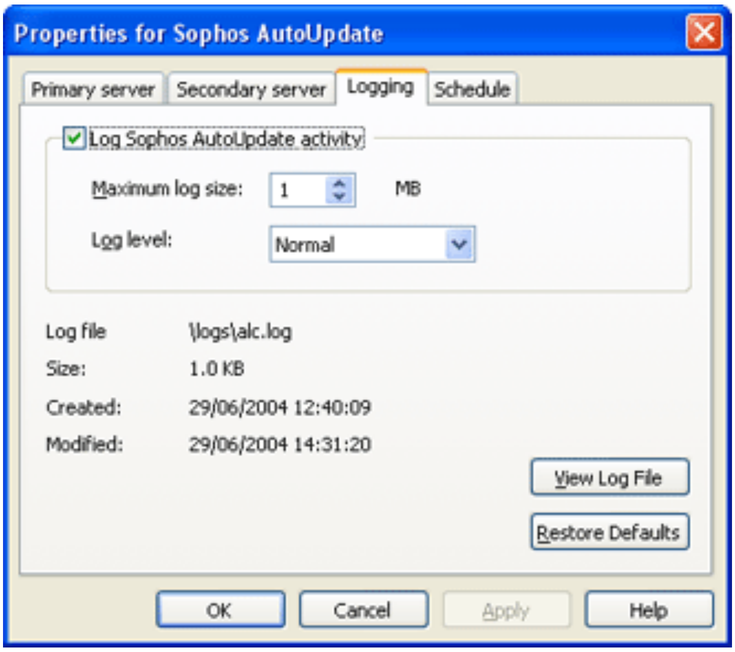
Logging updates

You can configure Sophos Anti−Virus to record updating activity in a log file.

1. Locate the Sophos Anti−Virus icon in the system tray (shown below).

2. Right−click the icon to display a menu, and select **Configure updating**.

3. In the **Properties for Sophos AutoUpdate** dialog box, click the **Logging** tab. Ensure that **Log Sophos AutoUpdate activity** is selected. Then set other options as described below. When you want to open the log, click **View Log File**.



☑ Log Sophos AutoUpdate activity

Maximum log size: 1 MB

Log level: Normal

Log file \logs\alc.log

Size: 1.0 KB

Created: 29/06/2004 12:40:09

Modified: 29/06/2004 14:31:20

Maximum log size

Specify a maximum size for the log in MB.

Log level

You can select **Normal** or **Verbose** logging. Verbose logging provides information on many more activities than usual, so the log will grow faster. Use this setting only when detailed logging is needed for troubleshooting.

Cleaning up

This section includes the following.

- What is cleanup?
- Getting cleanup information
- Setting up automatic cleanup

What is cleanup?

Cleanup eliminates threats on your computer. In particular, it removes a virus from a file or boot sector, or potentially unwanted application from the computer. However, it doesn't undo any actions the virus or application has already taken.

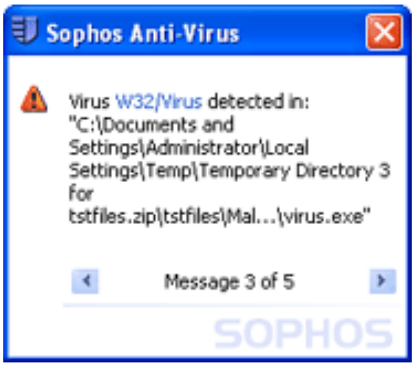
Getting cleanup information

When a threat is found on your computer, it is very important that you check the threat analysis on the Sophos website for information on the threat and cleanup advice. You can do this via

- the desktop alert (on−access scanning)
- the scan progress dialog box (on−demand and right−click scanning)
- Quarantine manager (all scanning types)

Getting information via the desktop alert

If on−access scanning is enabled on your computer, Sophos Anti−Virus displays a desktop alert when a threat is found. In the message box, click the name of the threat you want to find out about.

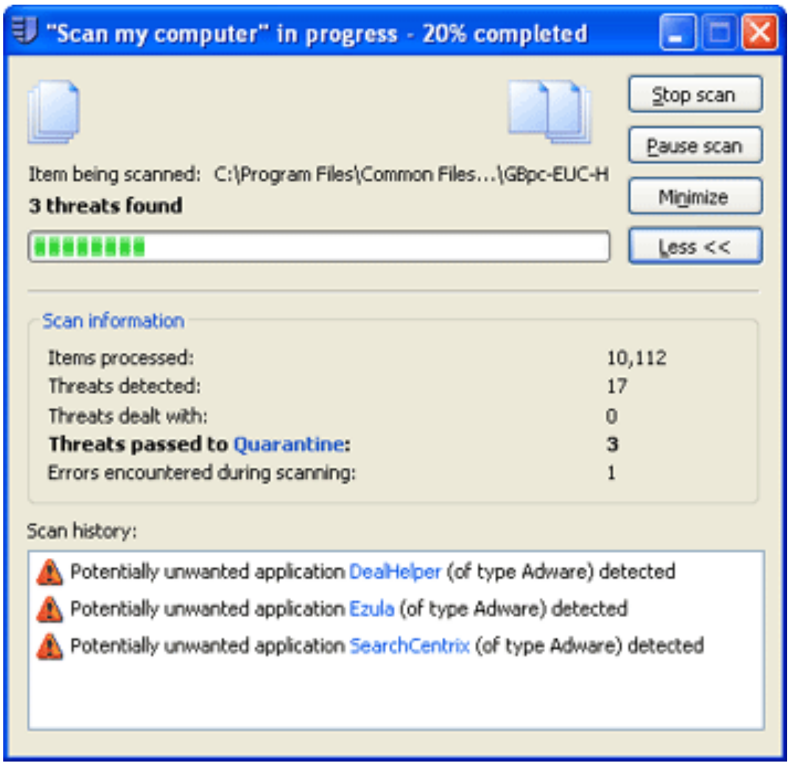


Virus W32/Virus detected in: "C:\Documents and Settings\Administrator\Local Settings\Temp\Temporary Directory 3 for tstfiles.zip\tstfiles\Mal...\virus.exe"

Sophos Anti−Virus connects you to the analysis of the threat on the Sophos website.

Getting information via the scan progress dialog box

For an on–demand scan or a scan run from a right–click menu, in the log that is displayed in the scan progress dialog box (or scan summary dialog box, displayed after the scan has finished), click the name of the threat you want to find out about.



"Scan my computer" in progress - 20% completed

Item being scanned: C:\Program Files\Common Files...\GBpc-EUC-H

3 threats found

Scan information

Items processed:	10,112
Threats detected:	17
Threats dealt with:	0
Threats passed to Quarantine:	**3**
Errors encountered during scanning:	1

Scan history:

⚠ Potentially unwanted application DealHelper (of type Adware) detected

⚠ Potentially unwanted application Ezula (of type Adware) detected

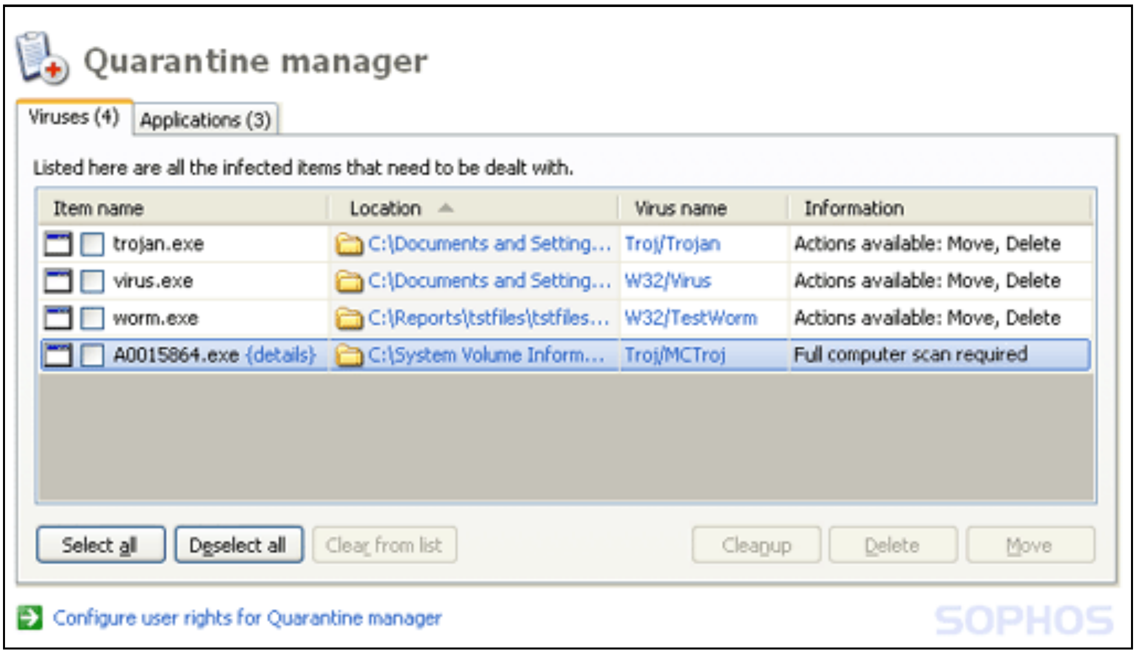
⚠ Potentially unwanted application SearchCentrix (of type Adware) detected

Sophos Anti–Virus connects you to the analysis of the threat on the Sophos website.

Getting information via Quarantine manager

Open Quarantine manager. To do this, in the home page of the **Sophos Anti–Virus** window, click **Manage quarantine items**.

In the **Virus name** column on the **Viruses** tab, or **Application name** column on the **Applications** tab, click the name of the threat you want to find out about.



Listed here are all the infected items that need to be dealt with.

Item name	Location	Virus name	Information
☐ trojan.exe	C:\Documents and Setting...	Troj/Trojan	Actions available: Move, Delete
☐ virus.exe	C:\Documents and Setting...	W32/Virus	Actions available: Move, Delete
☐ worm.exe	C:\Reports\tstfiles\tstfiles...	W32/TestWorm	Actions available: Move, Delete
☐ A0015864.exe {details}	C:\System Volume Inform...	Troj/MCTroj	Full computer scan required

Sophos Anti−Virus connects you to the analysis of the threat on the Sophos website.

Setting up automatic cleanup

When on−access scanning is turned on, or when you run an on−demand or right−click scan, Sophos Anti−Virus can automatically do the following:

- clean up many infected items
- make infected items safe in ways other than cleanup
- clean potentially unwanted applications from your computer (during on−demand and right−click scans only).

Any actions that Sophos Anti−Virus takes against infected items and applications are logged in the log for this computer or log for the on−demand scan.

To fully clean some threats consisting of several components from your computer, you will need to restart the computer. If this is the case, you will be given an option to restart your computer immediately or later. The final cleanup steps will be performed after the computer is restarted.

You can set up automatic cleanup for

- on−access scanning
- on−demand scanning
- scans run from a right−click menu.

Setting up automatic cleanup for on–access scanning

If the Sophos Enterprise Console is used to administer Sophos Anti–Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

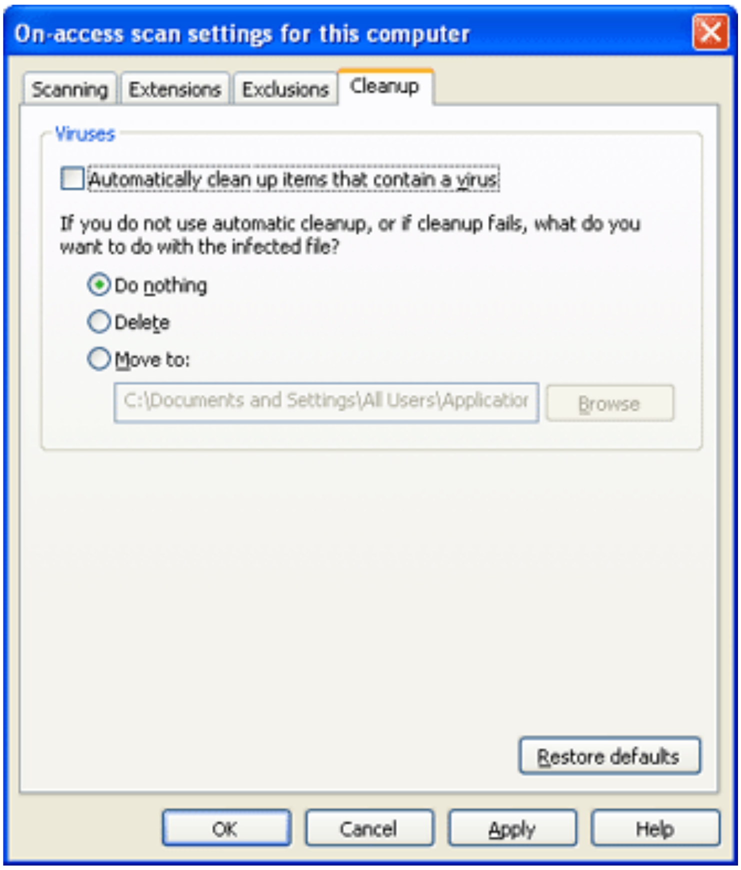
Automatic cleanup of potentially unwanted applications and multi–component infections is not available for on–access scanning. To clean unwanted applications and multi–component infections from your computer, use Quarantine manager.

To set up automatic cleanup for on–access scanning, do as follows.

1. In the home page of the **Sophos Anti–Virus** window, click **Configure Sophos Anti–Virus**.

2. In the **Configure** page, click **On–access scanning**.

3. Click the **Cleanup** tab. Set the options as described below.



□ Automatically clean up items that contain a virus

If you do not use automatic cleanup, or if cleanup fails, what do you want to do with the infected file?

● Do nothing

○ Delete

○ Move to:

C:\Documents and Settings\All Users\Applicatior

Viruses

- Select **Automatically clean up items that contain a virus** to enable Sophos Anti–Virus to disinfect floppy disk boot sectors, documents, programs and anything else that is selected for scanning. Cleanup of documents does not repair any changes the virus has made in the document. (Refer to Getting cleanup information to find out how to view details on the Sophos website of the virus's side−effects.) Cleanup of programs should be used only as a temporary measure. You should subsequently replace programs that have been cleaned, from the original disks or a clean backup.

You can't automatically clean your computer from multi−component infections during on−access scanning.

To learn how to clean your computer from viruses using Quarantine manager, refer to Dealing with viruses in quarantine.

- Sophos Anti−Virus can make an infected file safe in ways other than cleanup. You can select other actions that you want Sophos Anti−Virus to take against infected files if you do not use automatic cleanup, or if cleanup fails. However,

  ⚠ **You should use these options only if advised to by Sophos technical support.** Otherwise, use Quarantine manager to clean your computer from viruses, worms, and Trojans found by Sophos Anti−Virus.

  Click **Delete** to dispose of the file. Click **Move to** to move the file to another folder, which you can select using **Browse**. Moving an executable file reduces the likelihood of it being run.

  You can't automatically delete or move infected mailboxes.

  You can't automatically move components of a multi−component infection.

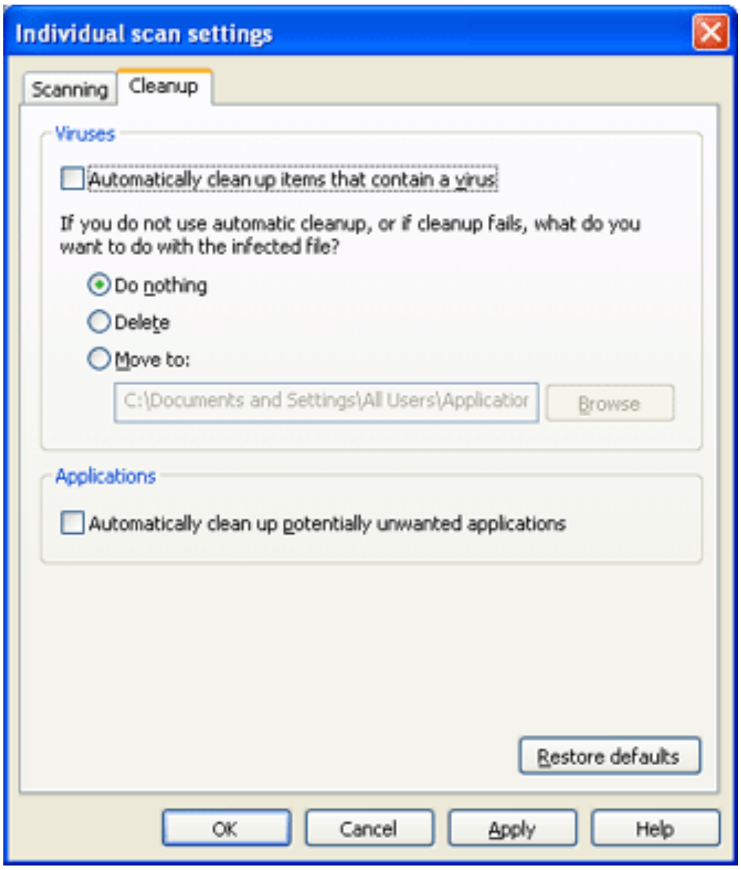
Setting up automatic cleanup for on−demand scanning

To set up automatic cleanup for an on−demand scan, do as follows.

1. In the home page of the **Sophos Anti−Virus** window, in the **Available scans** list, select the scan for which you want to enable cleanup. Click **Edit** to display the scan setup page.

2. Click **Configure this scan**.

3. Click the **Cleanup** tab. Set the options as described below.



□ Automatically clean up items that contain a virus

If you do not use automatic cleanup, or if cleanup fails, what do you want to do with the infected file?

● Do nothing

○ Delete

○ Move to: C:\Documents and Settings\All Users\Applicatior

□ Automatically clean up potentially unwanted applications

Viruses

- Select **Automatically clean up items that contain a virus** to enable Sophos Anti−Virus to disinfect floppy disk boot sectors, documents, programs and anything else that is selected for scanning. Cleanup of documents does not repair any changes the virus has made in the document. (Refer to Getting cleanup information to find out how to view details on the Sophos website of the virus's side−effects.) Cleanup of programs should be used only as a temporary measure. You should subsequently replace programs that have been cleaned, from the original disks or a clean backup.

- Sophos Anti−Virus can make an infected file safe in ways other than cleanup. You can select other actions that you want Sophos Anti−Virus to take against infected files if you do not use automatic cleanup, or if cleanup fails. However,

  ⚠ **You should use these options only if advised to by Sophos technical support.** Otherwise, use Quarantine manager to clean your computer from viruses, worms, and Trojans found by Sophos Anti−Virus.

Click **Delete** to dispose of the file. Click **Move to** to move the file to another folder, which you can select using **Browse**. Moving an executable file reduces the likelihood of it being run.

You can't automatically delete or move infected mailboxes.

You can't automatically move a multi−component infection.

Applications

- Select **Automatically clean up potentially unwanted applications** to enable Sophos Anti−Virus to remove all known components of a potentially unwanted application from the computer for all users. Cleanup does not repair any changes the application has already taken. (Refer to Getting cleanup information to find out how to view details on the Sophos website of the potentially unwanted application's side−effects.)

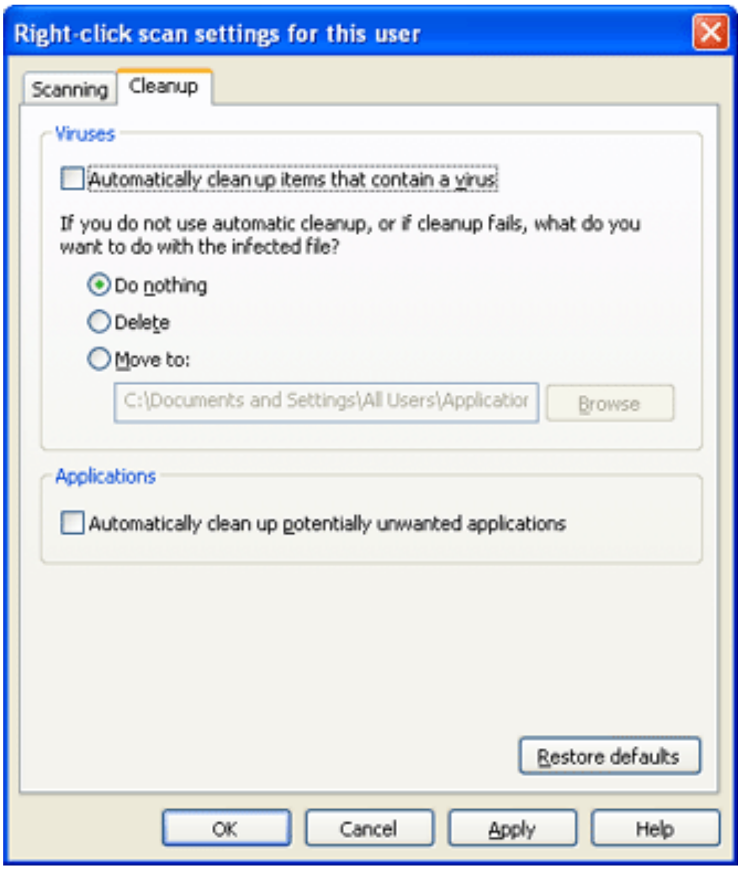
To learn how to clean your computer from threats using Quarantine manager, refer to Dealing with viruses in quarantine or Dealing with applications in quarantine.

Setting up automatic cleanup for a right−click scan

To set up automatic cleanup for a right−click scan, do as follows.

1. In the **Sophos Anti−Virus** window, on the **Configure** menu, click **Right−click scanning**.

2. Click the **Cleanup** tab. Set the options as described below.



Viruses

□ Automatically clean up items that contain a virus

If you do not use automatic cleanup, or if cleanup fails, what do you want to do with the infected file?

● Do nothing

○ Delete

○ Move to:

C:\Documents and Settings\All Users\Applicatior

Applications

□ Automatically clean up potentially unwanted applications

Viruses

- Select **Automatically clean up items that contain a virus** to enable Sophos Anti–Virus to disinfect floppy disk boot sectors, documents, programs and anything else that is selected for scanning. Cleanup of documents does not repair any changes the virus has made in the document. (Refer to Getting cleanup information to find out how to view details on the Sophos website of the virus's side–effects.) Cleanup of programs should be used only as a temporary measure. You should subsequently replace programs that have been cleaned, from the original disks or a clean backup.

- Sophos Anti–Virus can make an infected file safe in ways other than cleanup. You can select other actions that you want Sophos Anti–Virus to take against infected files if you do not use automatic cleanup, or if cleanup fails. However,

  You should use these options only if advised to by Sophos technical support. Otherwise, use Quarantine manager to clean your computer from viruses, worms, and Trojans found by Sophos Anti–Virus.

Click **Delete** to dispose of the file. Click **Move to** to move the file to another folder, which you can select using **Browse**. Moving an executable file reduces the likelihood of it being run.

You can't automatically delete or move infected mailboxes.

You can't automatically move a multi−component infection.

Applications

- Select **Automatically clean up potentially unwanted applications** to enable Sophos Anti−Virus to remove all known components of a potentially unwanted application from the computer for all users. Cleanup does not repair any changes the application has already taken. (Refer to Getting cleanup information to find out how to view details on the Sophos website of the potentially unwanted application's side−effects.)

To learn how to clean your computer from threats using Quarantine manager, refer to Dealing with viruses in quarantine or Dealing with applications in quarantine.

Managing quarantine items

This section includes the following.

- What is Quarantine manager?
- Dealing with viruses in quarantine
- Dealing with applications in quarantine
- Configuring user rights for Quarantine manager

What is Quarantine manager?

Quarantine manager enables you to deal with the threats found by a scan, that were not eliminated automatically when the scan was run. Each item is here for one of the following reasons.

- No cleanup options (clean up, delete, move) were chosen for the scan that found the item.
- A cleanup option was chosen for the scan that found the item but the option failed.
- The item is multiply–infected and still contains additional threats.
- The threat has only been partially detected, and full computer scan is needed to fully detect it.

Potentially unwanted applications and multi–component infections detected during on–access scanning are always listed in Quarantine manager. Automatic cleanup of potentially unwanted applications and multi–component infections is not available for on–access scanning.

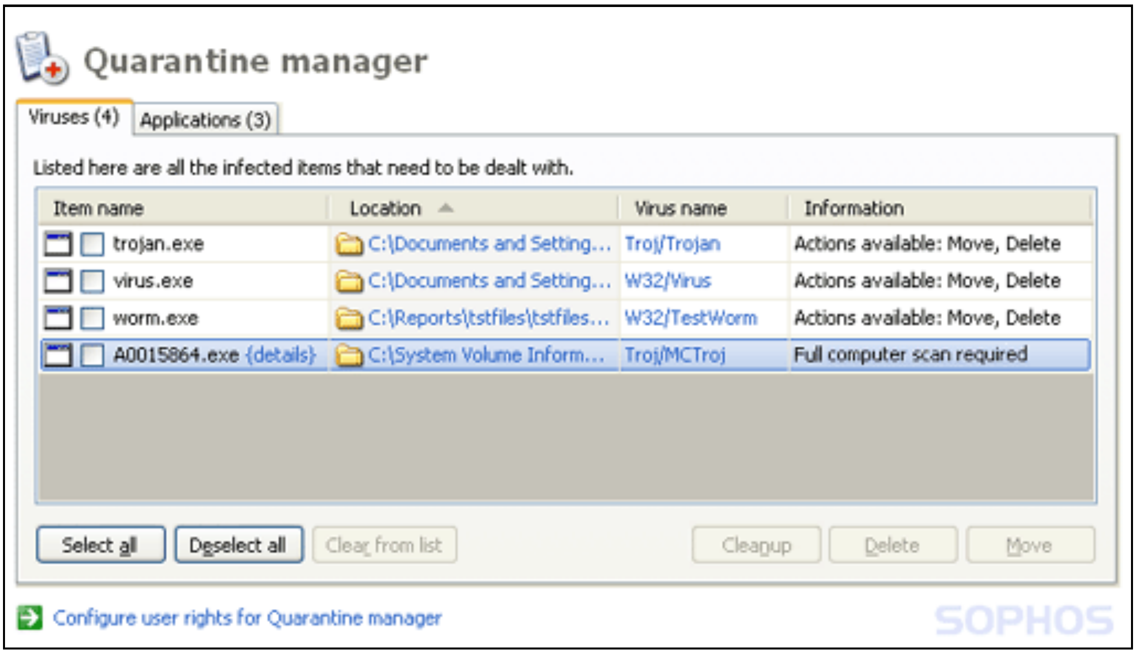
A cleanup option may have failed because of insufficient access rights. If you have greater rights, you can use Quarantine manager to clean up, delete or move an infected item, and to clean an application from or authorize it to run on the computer.

Dealing with viruses in quarantine

Virus here is used to refer to any virus, worm, Trojan, or other malicious software.

1. Open Quarantine manager. To do this, in the home page of the **Sophos Anti–Virus** window, click **Manage quarantine items**.

2. In the **Quarantine manager** page, on the **Viruses** tab, all the infected items are listed.



Listed here are all the infected items that need to be dealt with.

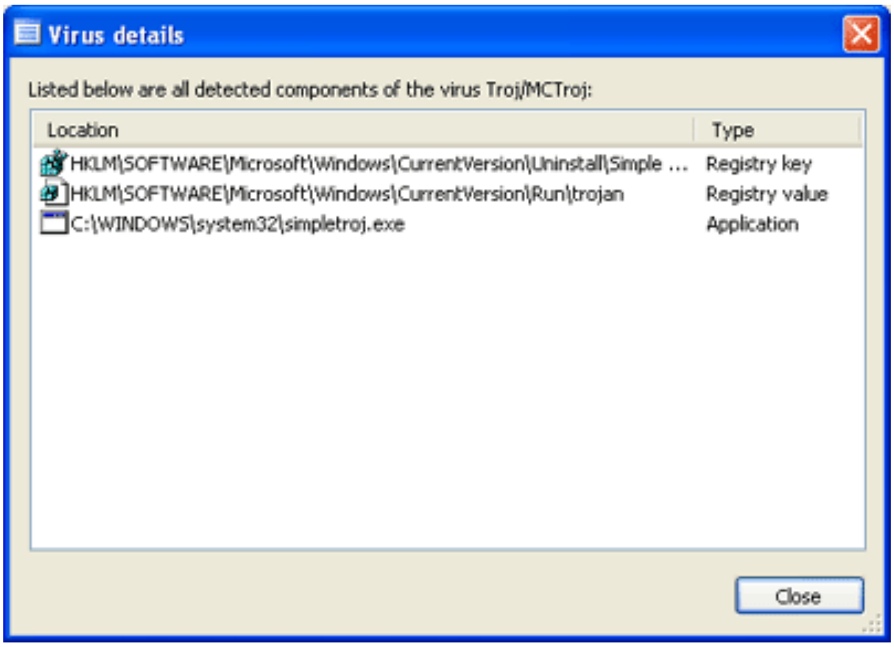
Item name	Location	Virus name	Information
□ trojan.exe	C:\Documents and Setting...	Troj/Trojan	Actions available: Move, Delete
□ virus.exe	C:\Documents and Setting...	W32/Virus	Actions available: Move, Delete
□ worm.exe	C:\Reports\tstfiles\tstfiles...	W32/TestWorm	Actions available: Move, Delete
□ A0015864.exe {details}	C:\System Volume Inform...	Troj/MCTroj	Full computer scan required

Configure user rights for Quarantine manager

Details of infected items

Information about each infected item is shown in the columns.

Item name displays the name of the infected item. If a **{details}** link appears next to the item name, this means that the item is infected with a multi–component infection. Click the link to open the **Virus details** dialog and see the list of other components that are part of the infection.



Listed below are all detected components of the virus Troj/MCTroj:

Location	Type
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Simple ...	Registry key
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\trojan	Registry value
C:\WINDOWS\system32\simpletroj.exe	Application

Location displays whereabouts the item is stored on disk. You can click this to list the items in order of location.

Virus name displays the virus with which the item is infected. To learn more about the virus, click its name, and Sophos Anti−Virus will connect you to the analysis of the virus on the Sophos website.

Information displays one of the following.

- ♦ Actions you can perform on the infected item. There are three options: Clean up, Delete, and Move.
  To configure what you can do, refer to Configuring user rights for Quarantine manager.
- ♦ Actions required before Sophos Anti−Virus can clean the virus from your computer, such as full computer scan or reboot.
- ♦ A message saying that the virus has been partially cleaned and manual removal is required.
- ♦ A message saying that you do not have sufficient rights to perform any action on this infected item.
  If this is the case, contact your administrator.

Actions to take against the infected items

To deal with the viruses, use the buttons described below.

Select all/Deselect all

Click these buttons to select or deselect all the items. This enables you to perform the same action on a group of items. To select or deselect a particular item, click the check box to the left of the item name.

Clear from list

Click this to remove selected items from the list, if you are sure they don't contain a virus. This doesn't delete the items from disk, however.

Cleanup

Click this to clean up the selected items. This disinfects the file or boot sector, that is, removes a virus from the file or boot sector. Cleanup of documents does not repair any changes the virus has made in the document. Cleanup of programs should be used only as a temporary measure. You should subsequently replace cleaned programs from the original disks or a clean backup.

To fully clean some viruses consisting of several components from your computer, you will need to restart the computer. If this is the case, you will be given an option to restart your computer immediately or later. The final cleanup steps will be performed after the computer is restarted.

Delete

Click this to dispose of the selected items. This deletes the infected files from your computer. Use this function with care.

Move

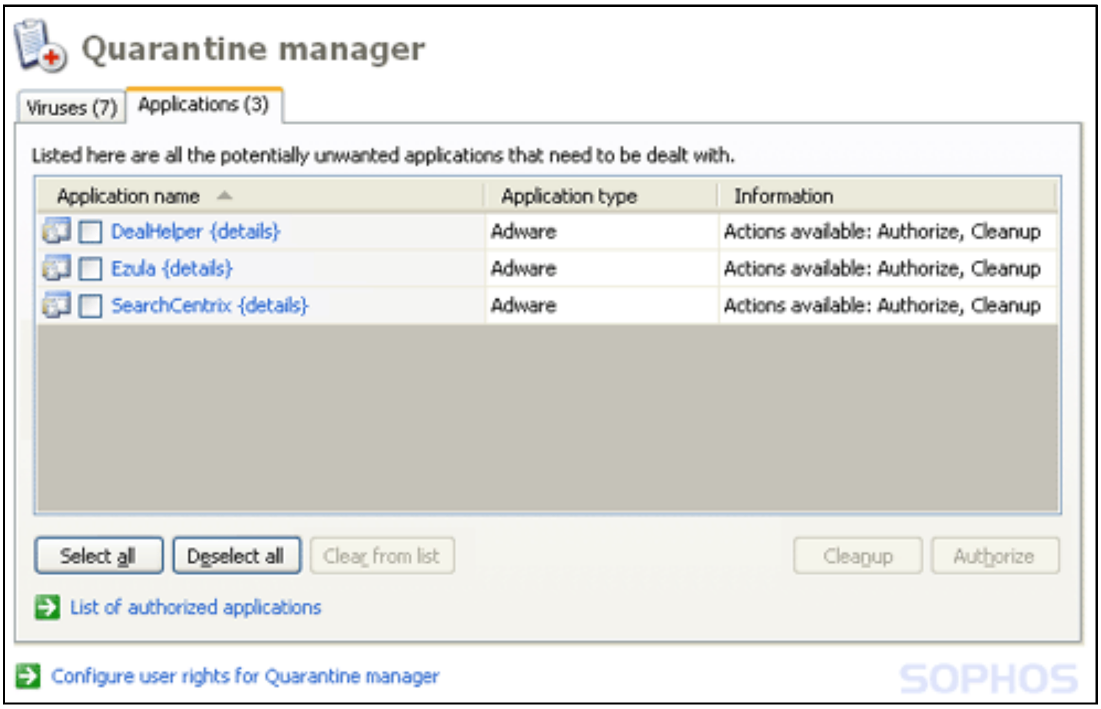
Click this to move the selected items to another folder. The items are moved to the folder that was specified when cleanup was set up. Moving an executable file reduces the likelihood of it being run. Use this function with care.

Sometimes, if you delete or move an infected file, your system may stop working properly. Also, an infected file may only be part of multiple infection, in which case deleting or moving this particular file will not clean your computer from the infection. In this case, contact Sophos technical support to get assistance in dealing with the infected items.

Dealing with applications in quarantine

1. Open Quarantine manager. To do this, in the home page of the **Sophos Anti−Virus** window, click **Manage quarantine items**.

2. In the **Quarantine manager** page, on the **Applications** tab, all the potentially unwanted applications are listed.



Listed here are all the potentially unwanted applications that need to be dealt with.

Application name	Application type	Information
□ DealHelper {details}	Adware	Actions available: Authorize, Cleanup
□ Ezula {details}	Adware	Actions available: Authorize, Cleanup
□ SearchCentrix {details}	Adware	Actions available: Authorize, Cleanup

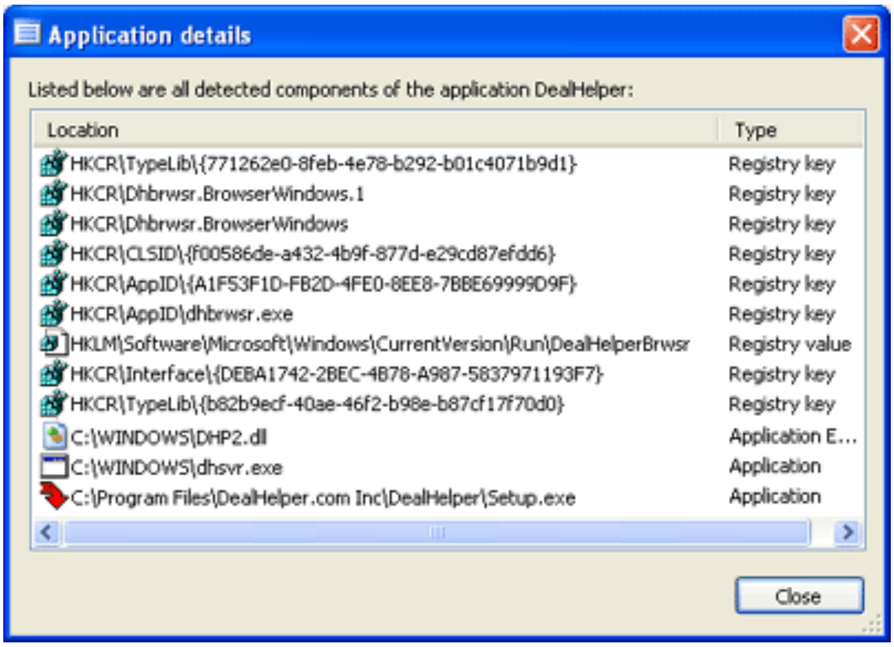
Select all
Deselect all
Clear from list
Cleanup
Authorize
List of authorized applications
Configure user rights for Quarantine manager
SOPHOS

Details of potentially unwanted applications

Information about each potentially unwanted application is shown in the columns.

Application name displays the name of the application. To learn more about the application, click its name, and Sophos Anti−Virus will connect you to the analysis of the application on the Sophos website.

To view the list of the application's components, click the **{details}** link that appears next to the application name.



Listed below are all detected components of the application DealHelper:

Location	Type
HKCR\TypeLib\{771262e0-8feb-4e78-b292-b01c4071b9d1}	Registry key
HKCR\Dhbrwsr.BrowserWindows.1	Registry key
HKCR\Dhbrwsr.BrowserWindows	Registry key
HKCR\CLSID\{f00586de-a432-4b9f-877d-e29cd87efdd6}	Registry key
HKCR\AppID\{A1F53F1D-FB2D-4FE0-8EE8-7BBE69999D9F}	Registry key
HKCR\AppID\dhbrwsr.exe	Registry key
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\DealHelperBrwsr	Registry value
HKCR\Interface\{DEBA1742-2BEC-4B78-A987-5837971193F7}	Registry key
HKCR\TypeLib\{b82b9ecf-40ae-46f2-b98e-b87cf17f70d0}	Registry key
C:\WINDOWS\DHP2.dll	Application E...
C:\WINDOWS\dhsvr.exe	Application
C:\Program Files\DealHelper.com Inc\DealHelper\Setup.exe	Application

Application type displays the type of the application, such as adware, system monitor, dialer, remote administration tool, or hacking tool. For information about different types of potentially unwanted application, visit the Sophos threat information web page.

Information displays one of the following.

- Actions you can perform on the application. There are two options: Authorize and Clean up.
- Actions required before Sophos Anti–Virus can clean the application from your computer, such as full computer scan or reboot.
- A message saying that the application has been partially cleaned and manual removal is required.
- A message saying that you do not have sufficient rights to perform any action on this application.
  If this is the case, contact your administrator.

Actions to take against potentially unwanted applications

To deal with the applications, use the buttons described below.

Select all/Deselect all

Click these buttons to select or deselect all the applications. This enables you to perform the same action on a group of applications. To select or deselect a particular application, click the check box to the left of the application name.

Clear from list

Click this to remove selected applications from the list, if you trust them. This doesn't remove the applications from disk, however.

Cleanup

Click this to remove all known components of selected applications from the computer for all users. To clean an application from the computer, you must be a member of both Windows Administrators and SophosAdministrator groups.

To fully clean some applications consisting of several components from your computer, you will need to restart the computer. If this is the case, you will be given an option to restart your computer immediately or later. The final cleanup steps will be performed after the computer is restarted.

Authorize

Click this to authorize selected applications on the computer, if you trust them. This adds the applications to the list of authorized applications so that Sophos Anti−Virus does not prevent the applications from running on your computer. To configure who can authorize applications, refer to Configuring user rights for Quarantine manager.

List of authorized applications

Click this to see the **Potentially unwanted applications** dialog, containing the lists of known and authorized applications.

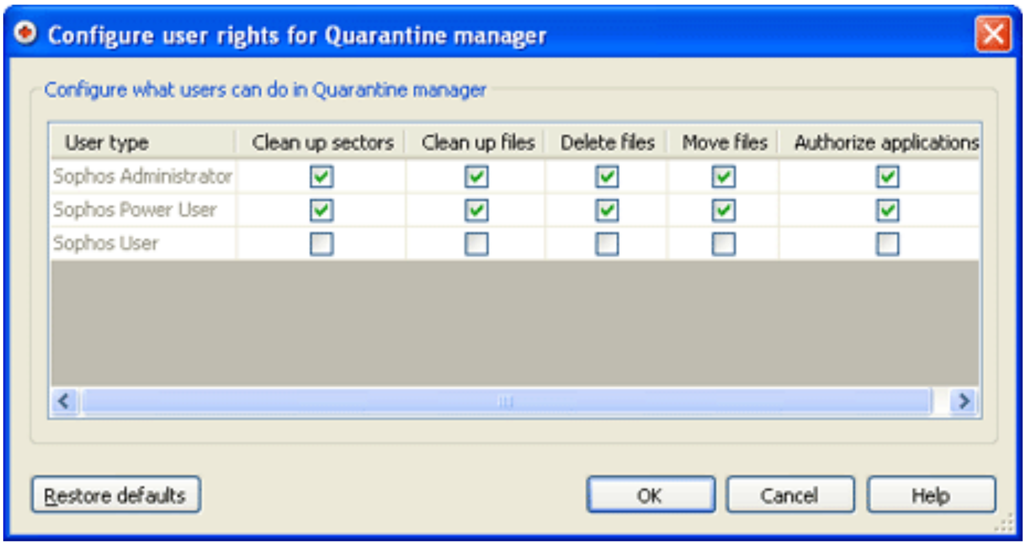
Configuring user rights for Quarantine manager

You need to be a Sophos Administrator to change these settings.

1. In the home page of the **Sophos Anti−Virus** window, click **Manage quarantine items**.

2. In the **Configure** page, click **User rights for Quarantine manager**.

3. In the **Configure user rights for Quarantine manager** dialog box, select the rights that each level of user should have, as explained below.



Configure user rights for Quarantine manager

Configure what users can do in Quarantine manager

User type	Clean up sectors	Clean up files	Delete files	Move files	Authorize applications
Sophos Administrator	☑	☑	☑	☑	☑
Sophos Power User	☑	☑	☑	☑	☑
Sophos User	□	□	□	□	□

User type

You can change the rights for each of the three types of user. For more information on user types, refer to Types of user. Remember that the rights you set here apply only to Quarantine manager.

Clean up sectors

Select this to enable the user to clean up floppy disk boot sectors.

Clean up files

Select this to enable the user to clean up documents and programs. Cleanup of documents does not repair any changes the virus has made in the document. Cleanup of programs should be used only as a temporary measure. You should subsequently replace cleaned programs from the original disks or a clean backup.

Delete files

Select this to enable the user to dispose of infected files.

Move files

Select this to enable the user to move infected files to another folder. Moving an executable file reduces the likelihood of it being run.

Authorize applications

Select this to enable the user to authorize applications that have been classified as potentially unwanted by Sophos Anti−Virus. Authorizing an application allows it to run on the computer.

To clean up an application, you must be a member of both Windows Administrators and SophosAdministrator groups.

Full computer scan

You may need to run full computer scan to determine all components of a multi−component threat or potentially unwanted application, before Sophos Anti−Virus can clean it from your computer.

1. To scan all disk drives, including boot sectors, on the computer, run the Scan my computer scan.

2. If the threat or application has still not been fully detected, it may be because you have insufficient access rights, or some drives or folders on the computer, containing the application's components, are excluded from scanning. Check the list of the items excluded from scanning. If there are some items on the list, remove them from the list and scan your computer again.

If you do not have sufficient rights to scan your entire computer, contact your administrator.

Sophos Anti−Virus may not be able to fully detect or remove potentially unwanted applications with components installed on network drives.

For advice, contact Sophos technical support.

Troubleshooting

This section includes the following.

- System tray icon has a white cross
- System tray icon is grayed out
- Threat not cleaned
- Virus fragment reported
- Threat partially detected
- Application disappeared from quarantine
- Computer becomes slow
- Unable to access disk with infected boot sector
- Unable to access areas of Sophos Anti−Virus
- Recovering from threat side−effects
- Getting further help

System tray icon has a white cross

If a red circle with a white cross in it appears over the Sophos Anti−Virus system tray icon, updating has failed.

To find out more about an update failure, look at the update log. Right−click the Sophos Anti−Virus system tray icon to display a menu. Select **Configure updating**. Then click the **Logging** tab and click **View Log File**.

The sections below explain why updating may fail, and how you can change the settings to correct the problem.

You need Sophos Administrator rights to change the updating settings.

Sophos Anti−Virus contacts the wrong source for updates

1. Right−click the Sophos Anti−Virus system tray icon to display a menu. Select **Configure updating**.

2. Click the **Primary server** tab. Check that the address and account details are those supplied by your administrator.

Sophos Anti−Virus cannot use your proxy server

If your copy of Sophos Anti−Virus updates itself via the internet, you must ensure that it can use your proxy server (if there is one).

1. Right−click the Sophos Anti−Virus system tray icon to display a menu. Select **Configure updating**.

2. Click the **Primary server** tab. Then click **Proxy Details**.

3. In the **Proxy details** dialog box, enter the proxy server address and port number, and the account details.

Automatic updating is not correctly scheduled

1. Right−click the Sophos Anti−Virus system tray icon to display a menu. Select **Configure updating**.

2. Click the **Schedule** tab. If your computer is networked, or if you update via a broadband internet connection, select **Enable automatic updates** and enter the frequency of updating. If you update via a dial−up connection, select **Check for updates on dial−up**.

The source for updates is not being maintained

Your company may have moved the directory (on the network or on a web server) from which you should update. Alternatively, they may not be maintaining the directory. If you think this may be the case, contact your network administrator.

System tray icon is grayed out

If the Sophos Anti−Virus system tray icon is grayed out, the computer is not protected by on−access scanning.

To enable on−access scanning for all users on the computer, refer to Turning protection on or off for the computer.

Threat not cleaned

If Sophos Anti−Virus hasn't cleaned a threat from your computer, it may be because of the following.

Automatic cleanup is disabled

If Sophos Anti−Virus has not attempted to clean a virus, check that automatic cleanup has been enabled. Automatic cleanup of potentially unwanted applications is not available for on−access scanning.

Cleanup failed

If Sophos Anti−Virus could not clean a threat ("Cleanup failed"), it may be that it cannot clean that type of threat, or you have insufficient access rights.

Full computer scan is required

You may need to run full computer scan to determine all components of a multi−component threat, before Sophos Anti−Virus can clean it from your computer.

1. To scan all disk drives, including boot sectors, on the computer, run the Scan my computer scan.
2. If the threat has still not been fully detected, it may be because you have insufficient access rights, or some drives or folders on the computer, containing the threat's components, are excluded from scanning. Check the list of the items excluded from scanning. If there are some items on the list, remove them from the list and scan your computer again.

Removable medium is write−protected

If dealing with a removable medium (e.g. floppy disk, CD), make sure that it is not write−protected.

NTFS volume is write−protected

If dealing with files on an NTFS volume (Windows 2000 or later), make sure that it is not write−protected.

Virus fragment has been reported

Sophos Anti−Virus does not clean a virus fragment because it has not found an exact virus match. Refer to Virus fragment reported.

Virus fragment reported

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

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.

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.

Database containing a virus

When running a full scan, Sophos Anti−Virus may report that there is a virus fragment in a database file. If this is the case, do not delete the database. Contact Sophos technical support for advice.

Threat partially detected

If Sophos Anti−Virus has partially detected a threat (Trojan or potentially unwanted application), full computer scan is required to determine all components of the threat.

1. To scan all disk drives, including boot sectors, on the computer, run the Scan my computer scan.

2. If the threat has still not been fully detected, it may be because you have insufficient access rights, or some drives or folders on the computer, containing the threat's components, are excluded from scanning. Check the list of the items excluded from scanning. If there are some items on the list, remove them from the list and scan your computer again.

Sophos Anti−Virus may not be able to fully detect or remove threats with components installed on network drives.

For advice, contact Sophos technical support.

Application disappeared from quarantine

If a potentially unwanted application detected by Sophos Anti−Virus disappeared from Quarantine manager without your taking actions on it, the application must have been authorized from the Sophos Enterprise Console or by another user. Check the list of authorized applications to see if the application has been authorized.

Computer becomes slow

If your computer has become very slow, it may be that you have a potentially unwanted application of system monitor type running on and monitoring your computer. If you have on−access scanning enabled, you may also see many desktop alerts warning about a potentially unwanted application. To solve the problem, do the following.

1. Turn on−access scanning off.

2. Run the Scan my computer scan to detect all components of the application.

   If after the scan the application is partially detected, refer to Potentially unwanted application partially detected, step 2.

3. Clean the application from your computer.

Unable to access disk with infected boot sector

If the Sophos Enterprise Console is used to administer Sophos Anti−Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

By default, Sophos Anti−Virus prevents access to removable disks whose boot sectors are infected. To allow access (e.g. to copy files from a floppy disk infected with a boot sector virus), do as follows.

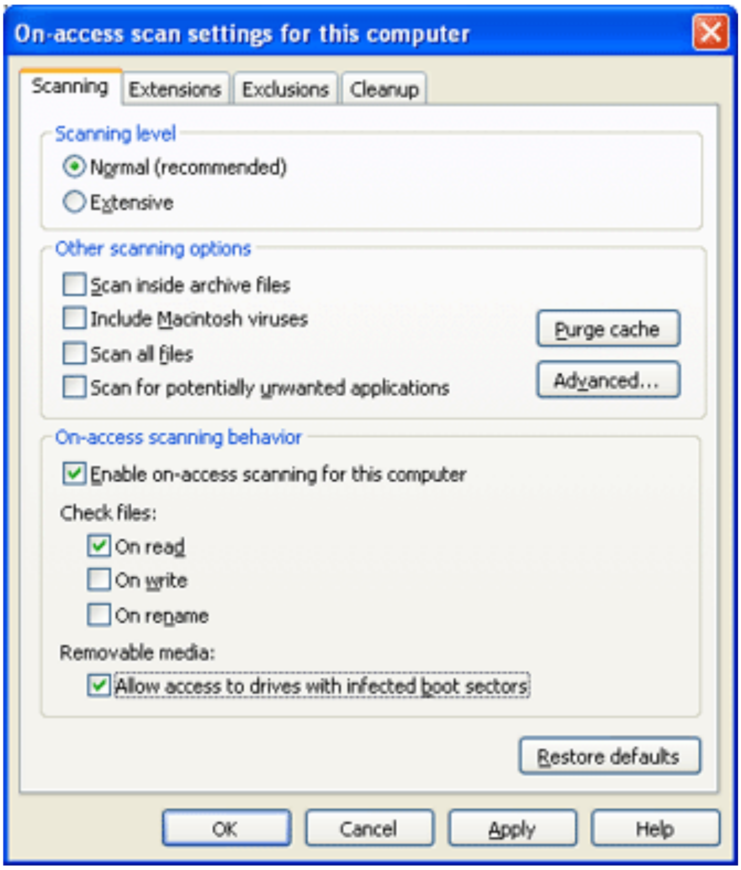
1. In the home page of the **Sophos Anti−Virus** window, click **Configure Sophos Anti−Virus**.

2. In the **Configure** page, click **On−access scanning**.

3. In the **On−access scan settings for this computer** dialog box, click the **Scanning** tab.

4. Select **Allow access to drives with infected boot sectors**.

Deselect the option when you have finished accessing the disk.



Scanning level

● Normal (recommended)

○ Extensive

Other scanning options

□ Scan inside archive files

□ Include Macintosh viruses

□ Scan all files

□ Scan for potentially unwanted applications

On-access scanning behavior

☑ Enable on-access scanning for this computer

Check files:

☑ On read

□ On write

□ On rename

Removable media:

☑ Allow access to drives with infected boot sectors

Unable to access areas of Sophos Anti–Virus

If you are unable to use or configure particular areas of Sophos Anti–Virus, it might be because access to these areas is restricted to particular types of user. Refer to Restricting access rights.

Recovering from threat side–effects

This section includes the following.

- Recovering from virus side–effects
- Recovering from potentially unwanted application side–effects

Recovering from virus side–effects

Recovery from virus infection depends on how the virus infected the computer.

Virus side–effects

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 in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect.

What to do

It is very important that you read the threat analysis on the Sophos website, and check documents carefully after cleanup. Refer to Getting cleanup information to find out how to view details on the Sophos website of the virus's side−effects.

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.

Recovering from potentially unwanted application side−effects

Removing potentially unwanted applications may have some side−effects that cannot be eliminated during cleanup.

Operating system has been modified

Some applications modify the Windows operating system, for example, change your internet connection settings. Sophos Anti−Virus cannot always restore all settings to the values they had before installation of the application. If, for example, an application changed the browser home page, then Sophos Anti−Virus cannot know what the previous home page setting was.

Utilities not cleaned

Some potentially unwanted applications can install utilities, such as .dll or .ocx files, on your computer. If a utility is harmless (that is, it does not possess the qualities of a potentially unwanted application), for example, a language library, and is not integral to the application, Sophos Anti−Virus may not detect it as part of the application. In this case, the file won't be removed from your computer even after the application that installed it has been cleaned from it.

Application is part of a program you need

Sometimes a potentially unwanted application, such as adware, is part of a program that you intentionally installed, and needs to be there for the program to run. If you remove the application, the program may stop running on your computer.

What to do

It is very important that you read the threat analysis on the Sophos website. Refer to Getting cleanup information to find out how to view details on the Sophos website of the potentially unwanted application's side−effects.

To be able to recover your system and its settings to their previous state, you should maintain regular backups of your system. You should also make backup copies of the original executable files of the programs you want to use. For more information or advice on recovering from potentially unwanted application's side−effects, contact Sophos technical support.

Getting further help

For technical support information, visit

www.sophos.com/support

If you contact technical support, provide as much information as possible, including

- Sophos software version number(s)
- operating system(s) and patch level(s)
- the exact text of any error messages you may have received.