SOPHOS

Sophos Anti-Virus for Windows, version 7
user manual

For Windows 2000 and later

Document date: August 2008

Contents

1 About Sophos Anti-Virus

Sophos Anti-Virus is software that detects and deals with

- threats (see *http://www.sophos.com/security/*): viruses, worms, Trojans, spyware, suspicious files, suspicious behavior, adware, PUAs (potentially unwanted applications), and rootkits
- applications that are controlled as part of your company policy
- devices that are blocked as part of your company policy

on your computer or network. In particular, it can

- scan your computer or network for threats, and controlled applications
- check if each file you access is a threat or controlled application
- check if each web page you view contains a threat (applies only to Internet Explorer version 6 or later)
- alert you when it finds a threat, controlled application, or blocked device
- clean up infected items
- stop suspicious behavior
- prevent adware and PUAs from running on your computer
- clean adware and PUAs 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 a management console, which enables 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 management 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. For information, see *Sophos Anti-Virus window* on page 5
- via the Sophos Anti-Virus system tray icon. For information, see *Sophos Anti-Virus system tray icon* on page 6.

Sophos Anti-Virus can perform

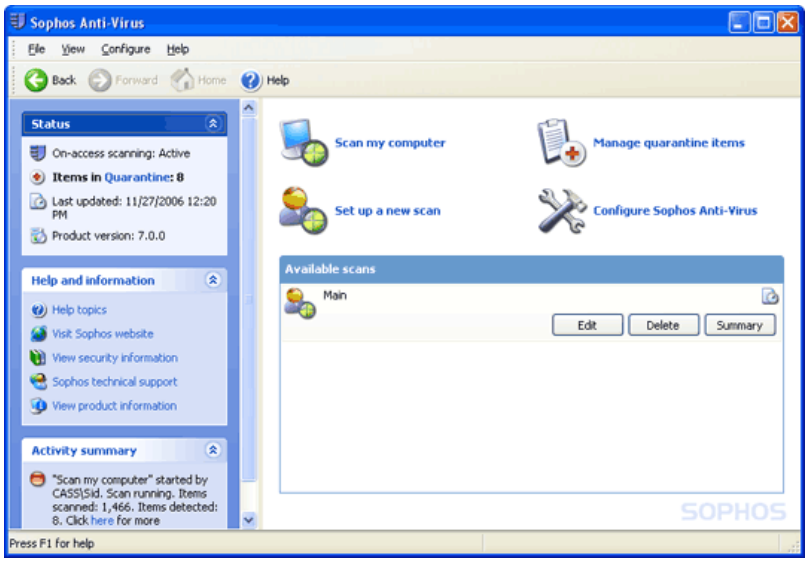
- On-access scanning. For information, see *What is on-access scanning?* on page 7.
- On-demand scanning. For information, see *What is an on-demand scan?* on page 7.
- Right-click scanning. For information, see *What is a right-click scan?* on page 8.
- Runtime behavior analysis. For information, see *What is runtime behavior analysis?* on page 8.

2 Introduction to Sophos Anti-Virus

2.1 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.



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 and controlled applications. 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 items 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. For information, see *Scanning my computer* on page 10.
- set up scans. For information, see *Setting up a scan* on page 11.
- manage quarantine items. For information, see *What is quarantine manager?* on page 39
- 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.

2.2 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. For information, see *Updating immediately* on page 30.
- configure updating. For information, see *Setting up automatic updating* on page 30.
- check the progress of an update
- open the **Sophos Anti-Virus** window.

Note: You need to be a member of the SophosAdministrator group 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.

Icon appearance	Explanation
	
	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* on page 48 or *System tray icon is grayed out* on page 49.

2.3 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 or are authorized for use.

For more information on scanning on access, refer to *Checking protection is on* on page 9 and *Configuring scanning*.

2.4 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*.

2.5 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* on page 14 and *Configuring scanning*.

2.6 What is runtime behavior analysis?

Runtime behavior analysis comprises suspicious behavior detection and buffer overflow detection. Suspicious behavior detection is the dynamic analysis of all programs running on the computer to detect and block activity that appears to be malicious.

For more information on runtime behavior analysis, refer to *Detecting suspicious behavior and buffer overflows* on page 24.

3 Checking the computer is protected

3.1 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 or are authorized for use.

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.

Note: 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*.

3.2 Turning protection on or off for the computer

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

Note: You need to be a member of the SophosAdministrator group to turn protection on or off for a computer.

1. On the **Configure** menu, click **On-access scanning**.
2. 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.

   Note: 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.

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

4 Scanning items on demand

4.1 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.

4.2 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**. For information about the home page, see *Sophos Anti-Virus window* on page 5.

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

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

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

Note: 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 more information on custom on-demand scans, see *Setting up a scan* on page 11. For more information on scanning Macintosh files, see *Scanning Macintosh files* on page 23.

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

4.3 Setting up a scan

1. On the **File** menu, click **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, select 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* on page 13.

   Note: 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 if 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* on page 11 for more information.)

   Note: You cannot 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.

4.4 Scheduling a scan

Note: You need to be a member of the SophosAdministrator group 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. For information on setting up a scan, see *Setting up a scan* on page 11. For information on editing a scan, see *Editing a scan* on page 12.

Note: You cannot 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.

4.5 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**. For information about the home page, see *Sophos Anti-Virus window* on page 5.

Note: You cannot 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.

If any threats or controlled applications 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*.

4.6 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. For information about the home page, see *Sophos Anti-Virus window* on page 5.
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, select 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* on page 13.

   Note: 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* on page 11 for more information.)

   Note: You cannot 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.

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. For information about the home page, see *Sophos Anti-Virus window* on page 5.

4.7 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. For information, see*Excluding items from scanning* on page 18.

5 Scanning a single item

5.1 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.

If any threats or controlled applications 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*.

6 Restricting access rights

6.1 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 and access to Authorization manager.

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

6.2 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.

7 Changing settings for multiple users

7.1 Changing settings for all computers

To configure Sophos Anti-Virus on workstations from a central location on the network, refer to the management console help.

7.2 Changing settings for all users on the computer

To configure Sophos Anti-Virus for all users on the computer, use the **Configure** menu. From here, you can configure the following.

- On-access scanning
- On-demand extensions and exclusions
- Runtime behavior analysis
- Application control
- User rights for Quarantine manager
- List of authorized adware and PUAs and suspicious items
- Messaging
- Logging
- Updating

You need to be a member of the SophosAdministrator group to change these settings.

8 Configuring scanning

8.1 Opening the scan settings dialog box

The scan settings for the three types of scanning are in three different dialog boxes.

To open the **on-access scan** settings dialog box, on the **Configure** menu, click **On-access scanning**.

To open the **on-demand scan** settings dialog box, in the home page of the **Sophos Anti-Virus** window, in the **Available scans** list, select the scan you want to edit. Click **Edit**. In the scan setup page, click **Configure this scan**. For information about the home page, see *Sophos Anti-Virus window* on page 5.

To open the **right-click scan** settings dialog box, on the **Configure** menu, click **Right-click scanning**.

8.2 Changing types of file scanned

Caution: If a management 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. To change the settings for **on-access scanning**, on the **Configure** menu, click **On-access scanning**.

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

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

   Scan all files

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

   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.

   Caution: 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, deselect **Scan files with no extension**.

8.3 Excluding items from scanning

Caution: If a management console is used to administer Sophos Anti-Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

Note: The procedure described below applies to *all* on-demand scans. To exclude items from a *particular* on-demand scan, refer to *Editing a scan* on page 12.

1. To change the settings for **on-access scanning**, on the **Configure** menu, click **On-access scanning**.

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

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

   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* below.

   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.

Note: 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.

- **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 do not 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 any single character or no characters. 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).

8.4 Changing when on-access scanning occurs

Caution: If a management 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 are opened, when they are saved, or when they are renamed.

1. On the **Configure** menu, click **On-access scanning**.
2. 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 are opened, select **On read**. This is the recommended option.

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

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

8.5 Scanning for suspicious files

Caution: If a management console is used to administer Sophos Anti-Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

A *suspicious file* is a file that exhibits a combination of characteristics that are commonly, but not exclusively, found in viruses.

1. Open the scan settings dialog box for the type of scanning that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Options** tab.
3. Select or deselect **Scan for suspicious files**, as required.

   Note: If you disable scanning for suspicious files, scanning for rootkits is disabled at the same time.

8.6 Scanning for adware and PUAs

Caution: If a management 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. Open the scan settings dialog box for the type of scanning that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Options** tab.
3. Select **Scan for adware/PUAs**.

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

8.7 Scanning for controlled applications

A *controlled application* is a legitimate consumer application that can undermine productivity and network performance.

Scanning for controlled applications is enabled or disabled by a management console as part of an application control policy, and is included as part of on-demand scanning. For information, see *What is an on-demand scan?* on page 10.

If scanning for controlled applications is enabled, it might prevent you from uninstalling some applications. If this is the case, you can temporarily disable scanning for controlled applications on this computer. For information, see *Disabling scanning for controlled applications* on page 21.

8.8 Disabling scanning for controlled applications

1. Log on to the computer as a member of the SophosAdministrator group.
2. On the **Configure** menu, click **Application control**.
3. Clear the **Enable on-access scanning** check box.

Note:

- The next policy update deployed by the management console may override changes made here.
- If you disable on-access scanning for controlled applications, scanning for blocked devices will be disabled at the same time. For more information, see *Scanning for blocked devices* on page 21.

8.9 Scanning for blocked devices

A *blocked device* is a type of device which has not been authorised for use on your computer. There are two types of device you can choose to block: *storage devices* and *wireless connections*.

Storage devices

- Floppy disk drives
- CD / DVD drives
- Removable storage (USB flash drives, PC Card readers, USB hard disk drives)

Wireless connections

- Bluetooth interfaces
- IrDA interfaces
- Wi-Fi (802.11 standard) interfaces

Scanning for blocked devices is enabled or disabled by a management console as part of an application control policy.

Caution: Scanning for blocked devices is **not** included as part of on-demand scanning.

If you are a Sophos Administrator and you want to connect a device to this computer for maintenance or troubleshooting (for example, to install software from a CD), you can temporarily disable on-access scanning for blocked devices. For information, see *Disabling on-access scanning for blocked devices* on page 22.

8.10 Disabling on-access scanning for blocked devices

1. Log on to the computer as a member of the SophosAdministrator group.
2. On the **Configure** menu, click **Application control**.
3. Clear the **Enable on-access scanning** check box.

All devices that were blocked by policy on the computer are now enabled.

Note:

- The next policy update deployed by the management console may override changes made here.
- If you disable on-access scanning for blocked devices, scanning for controlled applications will be disabled at the same time. For more information, see *Scanning for controlled applications* on page 21.

8.11 Scanning for rootkits

Caution: If a management console is used to administer Sophos Anti-Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

Scanning for rootkits is always performed when you run the **Scan my computer** scan (if you are a member of the SophosAdministrator group). However, if you want to change the setting for another on-demand scan that has been set up, do as follows.

1. Open the scan settings dialog box for the on-demand scan that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Options** tab.
3. Select or deselect **Scan for suspicious files and rootkits**, as required.

   Note: If you disable scanning for rootkits, scanning for suspicious files is disabled at the same time.

8.12 Scanning inside archive files

Caution: Scanning inside archive files makes scanning significantly slower and is generally not required. Even if you do not 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.

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

1. Open the scan settings dialog box for the type of scanning that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Options** tab.
3. Select **Scan inside archive files**.

   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.

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

8.13 Scanning Macintosh files

Caution: If a management 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 enable Sophos Anti-Virus to scan Macintosh files stored on Windows computers.

1. Open the scan settings dialog box for the type of scanning that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Options** tab.
3. Select **Scan for Macintosh viruses**. This enables Sophos Anti-Virus to scan executable Macintosh files.

8.14 Scanning complete contents of files

Caution: If a management 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 detect some viruses, you must enable scanning of the complete contents of each file.

Caution: Sophos does not recommend selecting this option, except on the advice of Sophos technical support.

1. Open the scan settings dialog box for the type of scanning that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Options** tab.
3. In the **Scanning level** panel, click **Extensive**.
4. When you have cleaned up the virus(es), click **Normal**.

9 Configuring runtime behavior analysis

9.1 Detecting suspicious behavior and buffer overflows

Caution: If a management console is used to administer Sophos Anti-Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

Suspicious behavior is activity that appears to be malicious.

If you want to change the settings for detection of suspicious behavior and buffer overflows, do as follows.

Note: You need to be a member of the SophosAdministrator group to change these settings.

1. On the **Configure** menu, click **HIPS runtime behavior analysis** to display the **HIPS runtime behavior analysis** dialog box.
2. To enable or disable detection of suspicious behavior, select or deselect **Detect suspicious behavior**, respectively.

   To enable or disable detection of buffer overflows, select or deselect **Detect buffer overflows**, respectively.

   Note: The buffer overflow detection feature is not available for Windows Vista and 64-bit versions of Windows. These operating systems are protected against buffer overflows by Microsoft's Data Execution Prevention (DEP) feature.

3. If this is a new installation of Sophos Anti-Virus on this computer, by default, suspicious behavior and buffer overflows are *detected* but not *blocked*. If this is an upgrade, by default, suspicious behavior and buffer overflows are not detected.

Caution: Sophos recommends that you run Sophos Anti-Virus in detect-only mode for a time and authorize the programs you need before enabling automatic blocking of suspicious behavior and buffer overflows. This approach avoids blocking programs that your users may need.

To enable *blocking* of suspicious behavior and buffer overflows as well as *detection*, clear the **Alert only** check box.

10 Configuring alerts

10.1 Desktop messaging

Caution: If a management 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 display desktop messages when a threat is found, do as follows. This applies only to on-access scanning.

1. On the **Configure** menu, click **Messaging**.
2. In the **Messaging** dialog box, click the **Desktop messaging** tab. Set the options as described below.

   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.

10.2 Email alerting

Caution: If a management 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. On the **Configure** menu, click **Messaging**.
2. In the **Messaging** dialog box, click the **Email alerting** tab. Set the options as described below.

   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.

   Sophos Anti-Virus does not send email alerts for threats that are detected by web page scanning because the threats are not downloaded to your computer. Therefore, there is no need to take any action.

   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 the table below.)

Configure SMTP settings	
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.

10.3 SNMP messaging

Caution: If a management 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. On the **Configure** menu, click **Messaging**.
2. In the **Messaging** dialog box, click the **SNMP messaging** tab. Set the options as described below.

   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 SNMP messages. **Scanning errors** include instances when Sophos Anti-Virus is denied access to an item that it attempts to scan.

   Sophos Anti-Virus does not send SNMP messages for threats that are detected by web page scanning because the threats are not downloaded to your computer. Therefore, there is no need to take any action.

   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.

10.4 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. On the **Configure** menu, click **Messaging**.
2. In the **Messaging** dialog box, click the **Event log** tab. Set the options as described below.

   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.

   Sophos Anti-Virus does not send messages for threats that are detected by web page scanning because the threats are not downloaded to your computer. Therefore, there is no need to take any action.

11 Logging

11.1 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** . For information about the home page, see *Sophos Anti-Virus window* on page 5.
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.

11.2 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. On the **Configure** menu, click **Logging**.
2. In the **Configure logging for this computer** dialog box, set the options as described below.

   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**. The archive files are stored in the same folder as the log file. 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.

11.3 Viewing the log for an on-demand scan

The *log for an on-demand scan* is a log of what happened the last time that the 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**. For information about the home page, see *Sophos Anti-Virus window* on page 5.
2. In the summary dialog box, click the link at the bottom.
3. From the log window, you can copy the log to the clipboard, or email or print the log.

12 Updating

12.1 Updating immediately

Note: 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**.

Note: 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.

12.2 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.

Note: You need to be a member of the SophosAdministrator group 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. For information, see *Setting a source for updates* on page 31. Your administrator can give you the details you need to enter.
4. Click the **Schedule** tab and schedule updates. For information, see *Scheduling updates* on page 32.

12.3 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.

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.

Note: 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**.

Note: 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**. For information on the Advanced button, see*Limiting the bandwidth used* on page 34.

If you access the internet via a proxy server, click **Apply** and then **Proxy Details**. For information on proxy details, see *Updating via a proxy server* on page 33. Note that some internet service providers require web requests to be sent to a proxy server.

12.4 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 needed as described below.

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.

Note: 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**.

Note: 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**. For information on the Advanced button, see*Limiting the bandwidth used* on page 34.

If you access the internet via a proxy server, click **Apply** and then **Proxy Details**. For information on proxy details, see *Updating via a proxy server* on page 33. Note that some internet service providers require web requests to be sent to a proxy server.

12.5 Scheduling updates

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

Caution: If a management 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.

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.

Note: 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.

12.6 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 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.

12.7 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.

12.8 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**.

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.

13 Cleaning up

13.1 What is cleanup?

Cleanup eliminates threats on your computer. In particular, it removes a virus from a file or boot sector, moves or deletes a suspicious file, or deletes an item of adware or PUA. However, it does not undo any actions the threat has already taken. It is not available for threats that are detected by web page scanning because the threats are not downloaded to your computer. Therefore, there is no need to take any action.

13.2 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 that you want to find out about.

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 that you want to find out about.

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**. For information about the home page, see *Sophos Anti-Virus window* on page 5.

In the **Name** column, click the name of the threat that you want to find out about.

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

13.3 Setting up automatic cleanup of viruses/spyware

Caution: If a management console is used to administer Sophos Anti-Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

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.

Note: Automatic cleanup of multi-component infections is not available for on-access scanning. To clean multi-component infections from your computer, use Quarantine manager. For information about Quarantine manager, see *Dealing with adware/PUAs in quarantine* on page 43.

Any actions that Sophos Anti-Virus takes against infected items are logged in the log for this computer or log for the on-demand scan. For information, see *Viewing the log for this computer* on page 29 or *Viewing the log for the on-demand scan* on page 29.

To fully clean some multi-component infections 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.

1. Open the scan settings dialog box for the type of scanning that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Cleanup** tab. Set the options as described below.

   - Select **Automatically clean up items that contain virus/spyware** 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 side-effects of the virus in the document. (Refer to *Getting cleanup information* on page 35 to find out how to view details on the Sophos website of the virus's side-effects.)
   - 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,

   Caution: You should use these options only if advised to by Sophos technical support. Otherwise, use Quarantine manager to clean your computer from viruses/spyware found by Sophos Anti-Virus. For information about Quarantine manager, see *Dealing with adware/PUAs in quarantine* on page 43.

   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 cannot automatically move a multi-component infection.

Note: To learn how to clean your computer from viruses/spyware using Quarantine manager, refer to *Dealing with viruses/spyware in quarantine* on page 39.

13.4 Setting up automatic cleanup of suspicious files

Caution: If a management console is used to administer Sophos Anti-Virus on workstations, it may override changes made here. To avoid this, refer to the console help.

When on-access scanning is turned on, or when you run an on-demand or right-click scan, Sophos Anti-Virus can automatically delete or move suspicious files.

A *suspicious file* is a file that exhibits a combination of characteristics that are commonly, but not exclusively, found in viruses.

1. Open the scan settings dialog box for the type of scanning that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Cleanup** tab. In the **Suspicious files** panel, set the options as described below.

Caution: You should use these options only if advised to by Sophos technical support. Otherwise, use Quarantine manager to clean your computer from viruses/spyware found by Sophos Anti-Virus. For information about Quarantine manager, see *Dealing with suspicious files in quarantine* on page 42.

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.

Note: To learn how to clean your computer from suspicious files using Quarantine manager, refer to *Dealing with suspicious files in quarantine* on page 42.

13.5 Setting up automatic cleanup of adware and PUAs

When you run an on-demand or right-click scan, Sophos Anti-Virus can automatically clean adware and PUAs from your computer.

Note: Automatic cleanup of adware and PUAs is not available for on-access scanning. To clean unwanted adware and PUAs from your computer, use Quarantine manager. For information about Quarantine manager, see *Dealing with adware and PUAs in quarantine* on page 43.

Any actions that Sophos Anti-Virus takes against adware and PUAs are logged in the log for this computer or log for the on-demand scan. For information, see *Viewing the log for this computer* on page 29 or *Viewing the log for the on-demand scan* on page 29.

To fully clean some adware and PUAs 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.

1. Open the scan settings dialog box for the type of scanning that you want to configure. (Refer to *Opening the scan settings dialog box* on page 17.)
2. In the scan settings dialog box, click the **Cleanup** tab.
3. Select **Automatically clean up adware/PUAs** to enable Sophos Anti-Virus to remove all known components of adware and PUAs from the computer for all users. Cleanup does not repair any changes the adware or PUA has already made. (Refer to *Getting cleanup information* on page 35 to find out how to view details on the Sophos website of the adware or PUA's side-effects.)

Note: To learn how to clean your computer from adware and PUAs using Quarantine manager, refer to *Dealing with adware and PUAs in quarantine* on page 43.

13.6 Running a full computer scan

You may need to run a full computer scan to determine all components of a multi-component threat, or to detect a threat in files that were previously hidden, 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. To find out how to do this, refer to *Scanning my computer* on page 10.
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. To find out how to do this, refer to *Excluding items from scanning* on page 18. 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 threats with components installed on network drives.

For advice, contact Sophos technical support. For information about contacting technical support, see*Technical support* on page 54.

14 Managing quarantine items

14.1 What is Quarantine manager?

Quarantine manager enables you to deal with the items found by scanning that were not eliminated automatically during scanning. Each item is here for one of the following reasons.

- No cleanup options (clean up, delete, move) were chosen for the type of scan that found the item.
- A cleanup option was chosen for the type of 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 a full computer scan is needed to fully detect it. To find out how to do this, refer to *Running a full computer scan* on page 38.
- The item exhibits suspicious behavior.
- The item is a controlled application.

Note: Adware, PUAs, and multi-component infections detected during on-access scanning are always listed in Quarantine manager. Automatic cleanup of adware, PUAs, 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 deal with the item(s).

Threats that are detected during web page scanning are not listed in Quarantine manager because the threats are not downloaded to your computer. Therefore, there is no need to take any action.

14.2 Dealing with viruses/spyware in quarantine

Note: *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**. For information about the home page, see *Sophos Anti-Virus window* on page 5.
2. In the **Quarantine manager** page, click the drop-down arrow on the **Show** box, and select **Virus/spyware**.

Information about each item is shown in the columns.

Name displays the identity that Sophos Anti-Virus has detected. To learn more about the virus/spyware, click the identity, and Sophos Anti-Virus connects you to the analysis of the virus/spyware on the Sophos website.

Details displays the name and location of the item. If the item is associated with a rootkit, it is displayed as "Hidden". If a **more** link is displayed next to the filename, this means that the item is infected with a multi-component infection. Click the link to see the list of other components

that are part of the infection. If any of the components are associated with a rootkit, the dialog box indicates that some components are hidden.

Available actions displays actions that you can perform on the item. Unless the item is hidden, there are three actions: Clean up, Delete, and Move, described below. If you click one of the actions, the action is performed on the item, following confirmation. Hidden files can only be cleaned up.

Dealing with the infected items

To deal with the viruses/spyware, 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, select the check box to the left of the item type.

Clear from list

Click this to remove selected items from the list, if you are sure that they do not contain a virus or spyware. This does not delete the items from disk, however.

Perform action

Click this to display a list of actions that you can perform on the selected items.

- Click **Clean up** to remove a virus or item of spyware from the selected items. Cleanup of documents does not repair any side-effects of the virus in the document.

  Note: To fully clean some viruses/spyware consisting of several components from your computer, or to clean up hidden files, 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.

- Click **Delete** to delete the selected items from your computer. Use this function with care.
- Click **Move** 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.

Caution: Sometimes, if you delete or move an infected file, your computer may stop working properly because it cannot find the file. Also, an infected file may only be part of a 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 items. For information about contacting technical support, see*Technical support* on page 54.

To configure what action you can perform, refer to *Configuring user rights for Quarantine manager* on page 46.

14.3 Dealing with suspicious behavior in quarantine

Suspicious behavior is activity that appears to be malicious.

1. Open Quarantine manager. To do this, in the home page of the **Sophos Anti-Virus** window, click **Manage quarantine items**. For information about the home page, see *Sophos Anti-Virus window* on page 5.
2. In the **Quarantine manager** page, click the drop-down arrow on the **Show** box, and select **Suspicious behavior**.

Information about each item is shown in the columns.

Name displays the identity that Sophos Anti-Virus has detected. To learn more about the behavior, click the identity, and Sophos Anti-Virus connects you to the analysis of the behavior on the Sophos website.

Details displays the name and location of the item.

Available actions displays actions that you can perform on the item. If you have enabled blocking of suspicious behavior, there is one action: Authorize, described below. If you click the action, the action is performed on the item, following confirmation.

Dealing with the suspicious behavior

To deal with the suspicious behavior, 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, select the check box to the left of the item type.

Clear from list

Click this to remove selected items from the list, if you trust them. This does not delete the items from disk, however.

Perform action

Click this to display a list of actions that you can perform on the selected items.

- Click **Authorize** to authorize the selected items on the computer, if you trust them. This adds the items to the list of authorized suspicious items so that Sophos Anti-Virus does not prevent the behavior.

To configure what actions you can perform, refer to *Configuring user rights for Quarantine manager* on page 46.

To see the list of authorized suspicious behavior, click **Configure authorization**.

14.4 Dealing with suspicious files in quarantine

A *suspicious file* is a file that exhibits a combination of characteristics that are commonly, but not exclusively, found in viruses.

1. Open Quarantine manager. To do this, in the home page of the **Sophos Anti-Virus** window, click **Manage quarantine items**. For information about the home page, see *Sophos Anti-Virus window* on page 5.
2. In the **Quarantine manager** page, click the drop-down arrow on the **Show** box, and select **Suspicious files**.

Information about each item is shown in the columns.

Name displays the identity that Sophos Anti-Virus has detected. To learn more about the suspicious file, click the identity, and Sophos Anti-Virus connects you to the analysis of the suspicious file on the Sophos website.

Details displays the name and location of the item. If the item is associated with a rootkit, it is displayed as "Hidden".

Available actions displays actions that you can perform on the item. Unless the item is hidden, there are three actions: Authorize, Delete and Move, described below. If you click one of the actions, the action is performed on the item, following confirmation. Hidden files can only be authorized.

Dealing with the suspicious files

To deal with the suspicious files, 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, select the check box to the left of the item type.

Clear from list

Click this to remove selected items from the list, if you trust them. This does not delete the items from disk, however.

Perform action

Click this to display a list of actions that you can perform on the selected items.

- Click **Authorize** to authorize the selected items on the computer, if you trust them. This adds the items to the list of authorized suspicious items so that Sophos Anti-Virus does not prevent them from being accessed.
- Click **Delete** to delete the selected items from your computer. Use this function with care.

- Click **Move** 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.

Caution: Sometimes, if you delete or move an infected file, your computer may stop working properly because it cannot find the file.

To configure what actions you can perform, refer to *Configuring user rights for Quarantine manager* on page 46.

To see the list of authorized suspicious files, click **Configure authorization**.

14.5 Dealing with adware and PUAs in quarantine

1. Open Quarantine manager. To do this, in the home page of the **Sophos Anti-Virus** window, click **Manage quarantine items**. For information about the home page, see *Sophos Anti-Virus window* on page 5.
2. In the **Quarantine manager** page, click the drop-down arrow on the **Show** box, and select **Adware/PUA**.

Information about each item is shown in the columns.

Name displays the identity that Sophos Anti-Virus has detected. To learn more about the adware or PUA, click the identity, and Sophos Anti-Virus connects you to the analysis of the adware or PUA on the Sophos website.

Details displays the subtype of the adware or PUA. If the item is associated with a rootkit, it is displayed as "Hidden". If a **more** link is displayed next to the subtype, this means that the item is a multi-component item of adware or PUA. Click the link to see the list of other components that are part of the adware or PUA. If any of the components are associated with a rootkit, the dialog box indicates that some components are hidden.

Available actions displays actions that you can perform on the item. There are two actions: Authorize and Clean up, described below. If you click one of the actions, the action is performed on the item, following confirmation.

Dealing with the adware and PUAs

To deal with the adware and PUAs, 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, select the check box to the left of the item type.

Clear from list

Click this to remove selected items from the list, if you trust them. This does not delete the items from disk, however.

Perform action

Click this to display a list of actions that you can perform on the selected items.

- Click **Authorize** to authorize the selected items on the computer, if you trust them. This adds the items to the list of authorized adware and PUAs so that Sophos Anti-Virus does not prevent them from running on your computer.
- Click **Clean up** to remove all known components of selected items from the computer for all users. To clean adware and PUAs from the computer, you must be a member of both Windows Administrators and SophosAdministrator groups.

Note: To fully clean some adware and PUAs consisting of several components from your computer, or to clean up hidden files, 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.

To configure what actions you can perform, refer to *Configuring user rights for Quarantine manager* on page 46.

To see the list of known and authorized adware and PUAs, click **Configure authorization**.

14.6 Dealing with controlled applications in quarantine

A *controlled application* is a legitimate consumer application that can undermine productivity and network performance.

1. Open Quarantine manager. To do this, in the home page of the **Sophos Anti-Virus** window, click **Manage quarantine items**. For information about the home page, see *Sophos Anti-Virus window* on page 5.
2. In the **Quarantine manager** page, click the drop-down arrow on the **Show** box, and select **Controlled applications**.

Information about each item is shown in the columns.

Name displays the identity that Sophos Anti-Virus has detected. To learn more about the controlled application, click the identity, and Sophos Anti-Virus connects you to the analysis of the controlled application on the Sophos website.

Details displays the subtype of the controlled application. If a **more** link is displayed next to the subtype, click it to see the list of other components that are part of the controlled application.

Available actions displays actions that you can perform on the item. However, there are no actions available for controlled applications apart from clearing the item from the list, described below.

Dealing with the controlled applications

To deal with the controlled applications, 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, select the check box to the left of the item type.

Clear from list

Click this to remove selected items from the list. This does not delete the items from disk, however. Controlled applications must be authorized by the central console before you can use them.

14.7 Dealing with blocked devices in quarantine

1. Open Quarantine manager. To do this, in the home page of the **Sophos Anti-Virus** window, click **Manage quarantine items**. For information about the home page, see *Sophos Anti-Virus window* on page 5.
2. In the **Quarantine manager** page, click the drop-down arrow on the **Show** box, and select **Controlled applications**.

Information about each item is shown in the columns.

Name displays the device that Sophos Anti-Virus has detected. To learn more about the device type, click it and Sophos Anti-Virus connects you to an analysis of the device type on the Sophos website.

Details displays the subtype of the device. If a **more** link is displayed next to the subtype, click it to see the list of other components that are part of the device.

Available actions displays actions that you can perform on the item. However, there are no actions available for blocked devices apart from clearing the item from the list, described below.

Dealing with the blocked devices

To deal with the blocked devices, 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, select the check box to the left of the item type.

Clear from list

Click this to remove selected items from the list. Blocked devices must be authorized by the central console before you can use them.

14.8 Configuring user rights for Quarantine manager

Note: You need to be a member of the SophosAdministrator group to change these settings.

1. On the **Configure** menu, click **User rights for Quarantine manager**.
2. In the **Configure user rights for Quarantine manager** dialog box, select the levels of user that may perform each type of action. For more information on user types, refer to *Types of user* on page 15. Remember that the rights you set here apply only to Quarantine manager. The types of action are explained below.

Clean up sectors

This refers to cleaning up floppy disk boot sectors.

Clean up files

This refers to cleaning 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

This refers to disposal of infected files.

Move files

This refers to moving infected files to another folder. Moving an executable file reduces the likelihood of it being run.

Authorize

This refers to authorizing suspicious items, adware, and PUAs, in order to allow them to run on the computer. It applies to Authorization manager and Quarantine manager.

Note: To clean up adware and PUAs, you must be a member of both Windows Administrators and SophosAdministrator groups.

15 Authorizing items for use

15.1 Authorizing adware and PUAs for use

Caution: If a management 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 adware or an application that Sophos Anti-Virus has classified as potentially unwanted, you can authorize it as follows.

1. On the **Configure** menu, click **Authorization**.
2. In the **Authorization manager** dialog box, click the **Adware/PUAs** tab.
3. In the **Known adware/PUAs** list box, select the adware or PUA you want to authorize and click **Add**. The adware or PUA now appears in the **Authorized adware/PUAs** list box.

If you want to prevent currently authorized adware and PUAs from running on your computer, select them in the **Authorized adware/PUAs** list and click **Remove**.

Note: You can also authorize adware and PUAs in Quarantine manager. For information on how to do this, refer to *Dealing with adware and PUAs in quarantine* on page 43.

15.2 Authorizing suspicious items for use

Caution: If a management 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 allow an item that Sophos Anti-Virus has classified as suspicious, you can authorize it as follows.

1. On the **Configure** menu, click **Authorization**.
2. In the **Authorization manager** dialog box, click the tab for the type of item that has been detected (e.g. **Buffer overflow**).
3. To authorize the item, select it in the **Known** list and move it to the **Authorized** list.

Note: You can also authorize suspicious items in Quarantine manager. For information on how to do this, refer to *Dealing with suspicious files in quarantine* on page 42 and *Dealing with suspicious behavior in quarantine* on page 41.

If you want to allow an item that Sophos Anti-Virus has *not* yet classified as suspicious, you can pre-authorize it as follows.

1. Click **New entry**.
2. Browse to the item and select it to add it to the **Authorized** list.

16 Troubleshooting

16.1 System tray icon has a white cross

16.1.1 Cause

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.

Note: You need to be a member of the SophosAdministrator group to change the updating settings.

16.1.2 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. (For information on the **Primary server** tab, see *Setting a source for updates* on page 31.) Check that the address and account details are those supplied by your administrator.

16.1.3 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. For information on proxy details, see *Updating via a proxy server* on page 33.

16.1.4 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. (For information on the **Schedule** tab, see *Scheduling updates* on page 32.) 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**.

16.1.5 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.

16.2 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* on page 9.

16.3 Threat not cleaned

If Sophos Anti-Virus has not cleaned a threat from your computer, it may be because of the following.

Automatic cleanup is disabled

If Sophos Anti-Virus has not attempted cleanup, check that automatic cleanup has been enabled. To enable automatic cleanup, refer to *Cleaning up*. Automatic cleanup of adware and PUAs 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 a full computer scan to determine all components of a multi-component threat, or to detect a threat in files that were previously hidden, 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. For information, see *Scanning my computer* on page 10.
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. For information, see *Excluding items from scanning* on page 18. 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/spyware fragment has been reported

Sophos Anti-Virus does not clean a virus/spyware fragment because it has not found an exact virus/spyware match. Refer to *Virus/spyware fragment reported* on page 50.

16.4 Virus/spyware fragment reported

If a virus/spyware fragment is reported, update Sophos Anti-Virus on the affected computer, so that it has the latest virus identity files. Then run a scan of the computer. If virus/spyware fragments are still reported, contact Sophos technical support for advice. For information about contacting technical support, see*Technical support* on page 54.

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

Variant of a known virus or item of spyware

Many new viruses or items of spyware are based on existing ones, so that code fragments typical of a known virus or item of spyware may appear as part of a new one. If a virus/spyware fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus or item of spyware, 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 or item of spyware

When running a full scan, Sophos Anti-Virus may report that there is a virus/spyware fragment in a database file. If this is the case, do not delete the database. Contact Sophos technical support for advice. For information about contacting technical support, see*Technical support* on page 54.

16.5 Threat partially detected

If Sophos Anti-Virus has partially detected a threat (Trojan, adware, or PUA), a 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. For information, see *Scanning my computer* on page 10.
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. For information, see *Excluding items from scanning* on page 18. 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. For information about contacting technical support, see*Technical support* on page 54.

16.6 Adware or PUA disappeared from quarantine

If an item of adware or PUA detected by Sophos Anti-Virus disappeared from Quarantine manager without your taking action on it, the adware or PUA might have been authorized or cleaned up from the management console or by another user. Check the list of authorized adware and PUAs to see if it has been authorized. To find out how to do this, refer to *Authorizing adware and PUAs for use* on page 47.

16.7 Computer becomes slow

If your computer has become very slow, it may be that you have a PUA running on and monitoring your computer. If you have on-access scanning enabled, you may also see many desktop alerts warning about a PUA. To solve the problem, do the following.

1. Run the **Scan my computer** scan to detect all components of the PUA. For information, see *Scanning my computer* on page 10.

   Note: If after the scan the PUA is partially detected, refer to *Threat partially detected* on page 51, step 2.

2. Clean the adware or PUA from your computer. To find out how to do this, refer to *Dealing with adware and PUAs in quarantine* on page 43.

16.8 Unable to access disk with infected boot sector

Caution: If a management 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. On the **Configure** menu, click **On-access scanning**.
2. In the **On-access scan settings for this computer** dialog box, click the **Scanning** tab.
3. Select **Allow access to drives with infected boot sectors**.

Caution: When you have finished accessing the disk, deselect the option. Remove the disk from the computer so that it cannot try to re-infect the computer on restart.

16.9 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*.

16.10 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* on page 35 to find out how to view details on the Sophos website of the virus's side-effects.

Sound backups are crucial. If you did not have them before you were infected, start keeping 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. For information about contacting technical support, see*Technical support* on page 54.

16.11 Recovering from adware and PUA side-effects

Removing adware and PUAs may have some side-effects that cannot be eliminated during cleanup.

Operating system has been modified

Some items of adware and PUAs 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 adware or PUA. If, for example, an item of adware or PUA changed the browser home page, then Sophos Anti-Virus cannot know what the previous home page setting was.

Utilities not cleaned

Some items of adware and PUAs 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 adware and PUAs), for example, a language library, and is not integral to the adware or PUA, Sophos Anti-Virus may not detect it as part of the adware or PUA. In this case, the file is not removed from your computer even after the adware or PUA that installed the file has been cleaned from the computer.

Adware or PUA is part of a program you need

Sometimes an item of adware or PUA is part of a program that you intentionally installed, and needs to be there for the program to run. If you remove the adware or PUA, 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* on page 35 to find out how to view details on the Sophos website of the adware or PUA'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 adware and PUA side-effects, contact Sophos technical support. For information about contacting technical support, see*Technical support* on page 54.

16.12 Password error reported

If you are trying to schedule an on-demand scan, and an error message is displayed concerning the password, make sure that

- the password is correct for the account
- the password is not blank.

To check that the password is correct, check the properties of the account via Control Panel. (Refer to your Windows documentation if necessary.)

17 Technical support

For technical support, visit *http://www.sophos.com/support*.

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

- Sophos software version number(s)
- Operating system(s) and patch level(s)
- The exact text of any error messages

18 Copyright

Index

P

R

S

T

U

V