

Sophos Anti-Virus for Staff & Home Users using Windows XP

Author: Rachael Johnson

Draft Version 0.2, February 2007

1. Introduction

Sophos Anti-Virus is installed on all staff and Open Access computers, providing virus checking, automatic reporting and disinfection for College systems. It has been configured to provide maximum protection from malicious software with minimal user intervention and disruption, receiving regular, automated updates as they become available, ensuring the highest possible levels of protection.

2. Scanning Methods

Sophos can be used to scan for viruses in three different ways:

- On-access – intercepts and scans files as they are accessed, providing access only if files are safe. On-access scanning is enabled and preconfigured by default on all PCs.
- On-demand – a scan of all or part of a computer that can be run upon demand, either immediately or via a predefined schedule. Pre-defined, pre-configured scans may be provided by the Administrator, or users can create their own scans to suit their particular requirements.
- By right-clicking – enables scanning of selected items which can be initiated by right-clicking the selected items and choosing **Scan with Sophos Anti-Virus** from the resulting menu.

3. Using Sophos Anti-Virus

You can open Sophos Anti-Virus by right-clicking on the blue shield icon in the System Tray and selecting **Open Sophos Anti-Virus**.

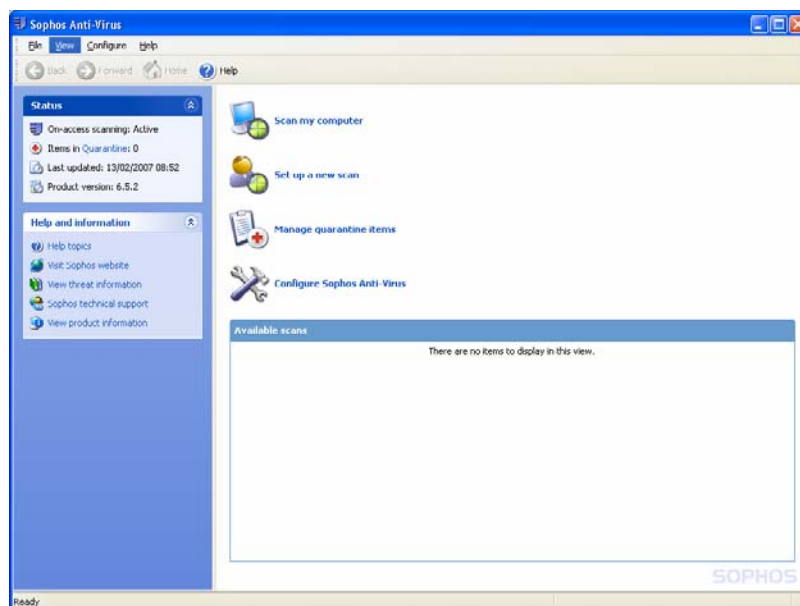


Fig.1 Sophos Anti-Virus home page

3.1 User Access Rights

The access rights assigned to each user will depend on the user's status on their local machine:

- If you are assigned Administrator rights on your personal computer, you will automatically be assigned a member of the SophosAdministrators group. This enables you to use or configure any part of the software.
- If you are assigned PowerUser rights on your personal computer, you will automatically be assigned a member of the SophosPowerUser group, which grants the same rights as SophosUser (below), in addition to greater privileges in Quarantine Manager.
- If you are assigned User rights on your personal computer, you will automatically be assigned membership of the SophosUser group, which allows you to access the software, set up and run on-demand scans and configure right-click scans, as well as manage quarantined items with limited privileges.
- Guest users can perform only on-access scanning and scans run from a right-click menu.

Sophos Anti-Virus is configured and administered centrally by the Sophos Anti-Virus Administrator. Any changes made locally to Sophos Anti-Virus settings may be overridden by changes made centrally. On-access scanning settings should NOT be adjusted by users individually. Any attempt to do so may significantly interfere with the levels of protection afforded by Sophos Anti-Virus and affect the security of your data as well as that of others.

4. Virus Scanning

4.1 On-access scanning – checking that protection is enabled

When on-access scanning is active, a blue shield icon appears in the System tray. If on-access scanning is switched off, the shield icon is grey. The status of on-access scanning can also be checked in the Sophos Anti-Virus window, under **Status**. On-access scanning is enabled by default on all College PC systems and offers the best protection against virus infections.

4.2 Scanning items on-demand

4.2.1 Running an Immediate Scan

An immediate scan of fixed local drives can be implemented by clicking on the **Scan My Computer** icon in the Sophos Anti-Virus home page window (see *Fig.1*). A progress dialog box is displayed during the course of the scan (see *Fig.2 below*). Click **More** if any threats are found, for further details

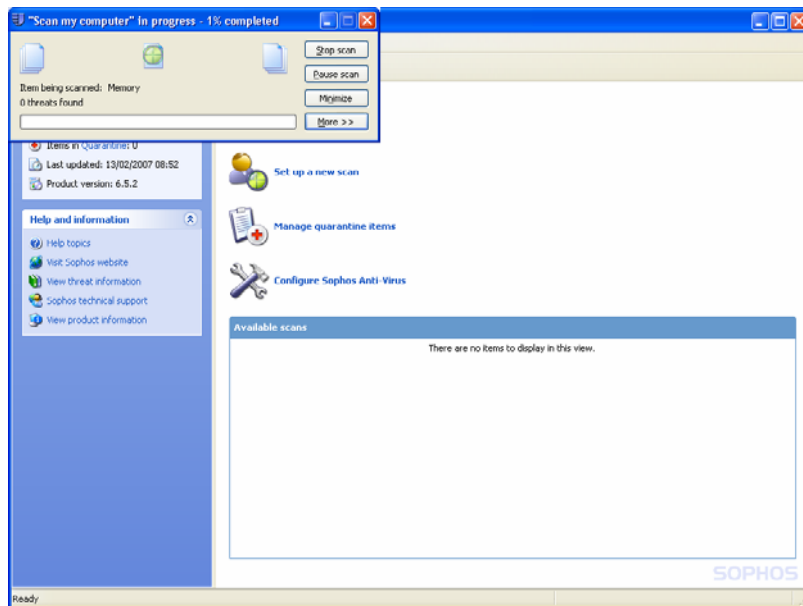


Fig.2 Scan My Computer dialog box

4.2.2 Setting up a new scan

- In the Sophos Anti-Virus home page (see Fig.1) click on the **Set up a new scan** icon to display the scan setup page
- Enter a name for the scan in the **Scan name** box
- Select the drives and folders you want to scan in the **Items to scan** panel by clicking the check box to the left of each folder or drive.
- For scheduling options, click **Schedule this scan** and refer to Section 4.2.3
- For further configuration options, click **Configure this scan** and refer to Section 4.3
- Click **Save** to save the scan or **Save and Start** to save and start the scan

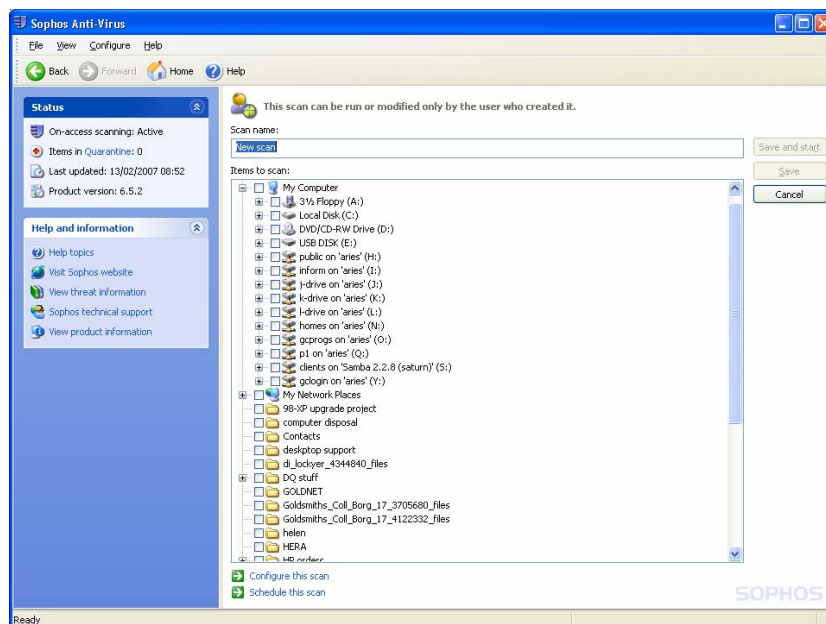


Fig.3 Setting up a new scan

4.2.3 Scheduling a scan

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

- In the **Setting up a new scan** window, click **Schedule this scan**
- In the **Schedule Scan** dialog box, select **Enable schedule**
- Select the day(s) on which you want the scan to run. Add the times by clicking **Add**.
- Type in your College username and password. These fields cannot be blank. The scan will run with the access rights of the user.
- Click ok.

4.2.4 Running a Scan

To run a scan that has been set up, look in the **Available Scans** list in the Sophos Anti-Virus home page window, Select the scan you want to run and click **Start**. A progress dialog box is displayed and the **Activity Summary** appears in the Sophos Anti-Virus window.

You can't manually run a scan that has been scheduled. Scheduled scans are displayed in the Available Scans list with a clock icon.

If any threats are found, click **More** for further information and refer to **Managing Quarantine Items**.

4.3 Configuring Scanning

With the scanning options available you can make a number of changes to the way that Sophos Anti-Virus scans for viruses, from changing the types of files scanned to setting up exclusions or including the scanning of archive files. To access scanning options, open the Sophos Anti-Virus main window and select **Configure Sophos Anti-Virus**.

Sophos Anti-Virus is preconfigured and administered centrally by the Sophos Enterprise Console. Any changes made here may be overridden. On-access scanning settings should NOT be adjusted by users individually.

4.3.1 Configuring On-demand scanning

If you wish to change the scanning settings for an on-demand scan, open Sophos Anti-Virus and select **Configure Sophos Anti-Virus**. In the next window, select **On demand extensions and exclusions** from the list under the **Configure** menu (see *Fig.4*). From this window you can opt to scan all files by checking the **Scan all files** box, or make a selection of a precise group of files that you wish to scan by checking the **Allow me to control exactly what is scanned** option.

It should be noted that changing the on-demand scanning options will have a global effect on all scans arranged by any users of the particular computer.

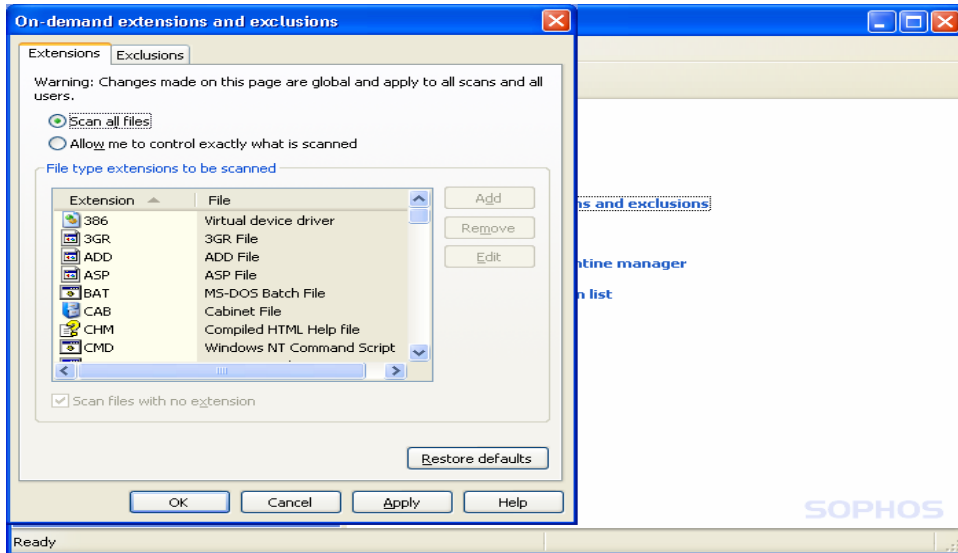


Fig.4 Configuring On-demand scanning

You can also exclude files from scanning if you wish. To do so, click on the **Exclusions** tab in the **On-demand extensions and exclusions** window and click **Add**. You can then browse to the files which you would like to exclude from scanning.

4.3.2 Scanning inside archive files

You can enable Sophos Anti-Virus to scan inside archive files on-access, on-demand and by right-clicking. On-access settings are preconfigured centrally and any on-access scanning changes made on a local computer will be overridden.

Scanning inside archive files will significantly increase the time taken to complete a scan and is rarely required. Preconfigured on-access settings will automatically scan files extracted from archives when you attempt to access them.

To enable scanning inside archive files on-demand, follow the instructions in section 4.2.2, *Setting up a new scan* and select **Configure this scan**. In the resulting **Individual Scan settings** window, check the **Scan inside archive files** box (see Fig.5 below).

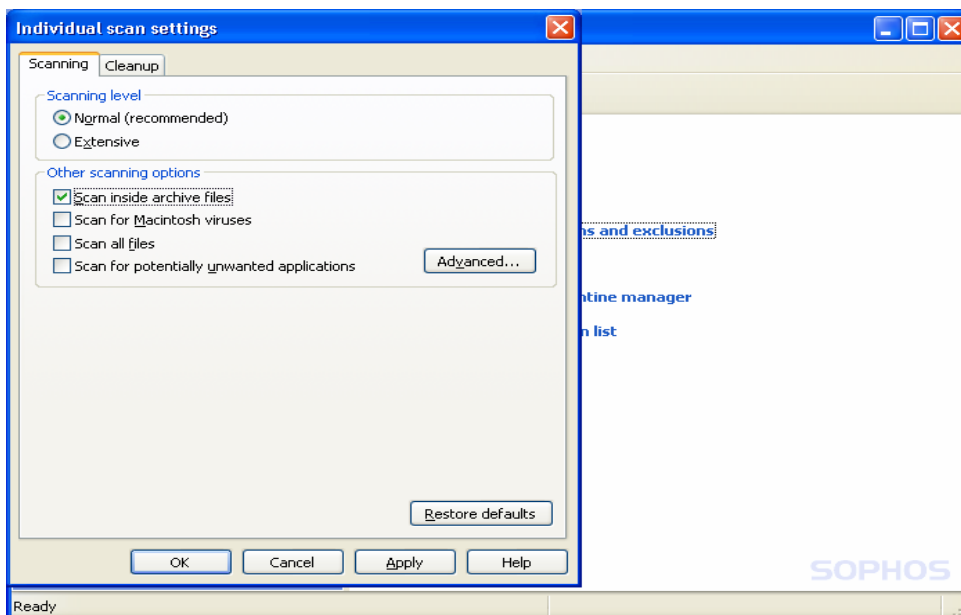


Fig. 5 Individual Scan settings

Archive files can also be scanned from a right-click menu as follows:

- From the **Configure** menu, select **Right-click scanning**
- In the **Right-click scan settings for this user** dialog box, click the **Scanning** tab
- Select **Scan inside archive files**

4.3.3 Scanning Macintosh files

Should you need to, you can configure Sophos Anti-Virus to scan Macintosh files for on-access, on-demand and for right-click scanning. To do so, follow the instructions in section 4.3.2 for scanning inside archive files.

4.3.4 Configuring Right-click scanning

To configure right-click scanning:

- Open the Sophos Anti-Virus main window and select **Configure Sophos Anti-Virus**.
- Select **Right-click scanning**
- Click on the **Scanning** tab. Here you can select normal or extensive scanning, as well as options to scan inside archive files, scan Macintosh files and so on.
- To configure cleanup settings for right-click scanning, click on the **Cleanup** tab. It is recommended that you use the settings shown in *Fig.6*, below.

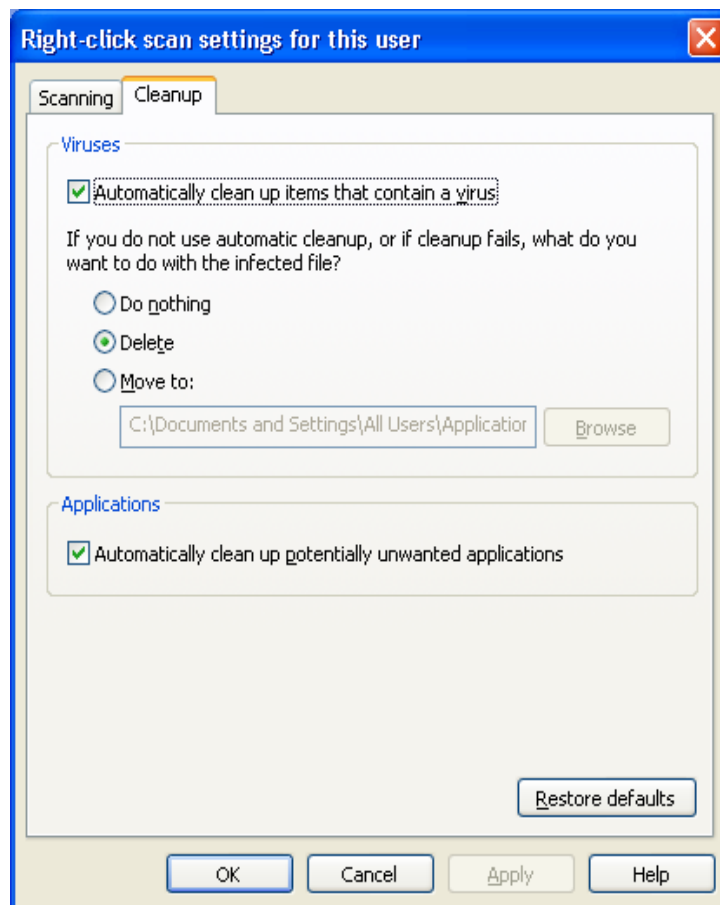


Fig.6 Right-click scan settings for this user

5. Configuring Alerts

Sophos Anti-Virus Alerts are preconfigured by IT Services and any changes made locally are likely to be overridden by Sophos Enterprise Console.

5.1 Desktop Messaging

Sophos Anti-Virus is preconfigured to display desktop messages in the event that a virus threat is found. This applies only to on-access scanning. Sophos is currently set to display desktop messages concerning virus threats but not concerning Potentially Unwanted Applications (PUAs).

5.2 Email Alerting

Sophos Anti-Virus is preconfigured to send email alerts concerning virus threats to IT Services staff, ensuring that any necessary follow up to a virus threat can be made promptly. It is currently set to report on virus events and those relating to PUAs. The virus alert received by IT Services advises upon the status of the virus or PUA threat found and whether any further action is necessary. If further action is necessary you will be contacted by a member of IT Services.

5.3 Event Logging

By default, Sophos Anti-Virus will add alerts to the Windows event log when a virus or PUA event occurs. It can also be configured to log other events such as scanning or other errors. If you wish to enable these additional scanning options, complete the following steps:

- Open Sophos Anti-Virus and click **Configure Sophos Anti-Virus**
- In the **Configure** page, click **Messaging**
- In the **Messaging** dialog box, click the **Event log** tab.
- Set the additional options by checking the **Scanning Errors** and **Other errors** boxes.

6. Updating

Sophos Anti-Virus has been configured to update automatically several times per day from one of two College server locations. You can check when the product was last updated by resting your mouse cursor over the Sophos Anti-Virus blue shield icon. Information will then be displayed concerning the last time that your machine checked for updates.

7. Cleaning Up

Cleanup eliminates virus threats from your computer. On-access scanning is preconfigured to cleanup files containing threats and to delete any which cannot be cleaned up. However, cleaning up will not undo any actions already taken by the virus.

7.1 Getting Information

Sophos Anti-Virus displays a desktop alert when a threat is found during on-access scanning. In the message box, you can click on the name of the threat you want to find out about. Sophos Anti-Virus will then connect you to the threat analysis pages on the Sophos website.

For an on-demand scan or a scan run from a right-click menu, you can find out more about a particular threat by clicking on its name in the scan progress or scan summary dialog box. As before, Sophos Anti-Virus will connect you to the Sophos website for further information.

7.2 Setting up automatic cleanup for on-demand scanning

On-demand scanning is not centrally preconfigured and can be adjusted to suit individual requirements. To set up automatic cleanup for an on-demand scan which you have created, do as follows:

- Open **Sophos Anti-Virus** and select the scan for which you would like to enable cleanup in the **Available Scans** list. Click **Edit** to display the scan setup page.
- Select **Configure this scan**, then click the **Cleanup** tab. If you wish to enable automatic cleanup, check the **Automatically clean up items that contain a virus** box.

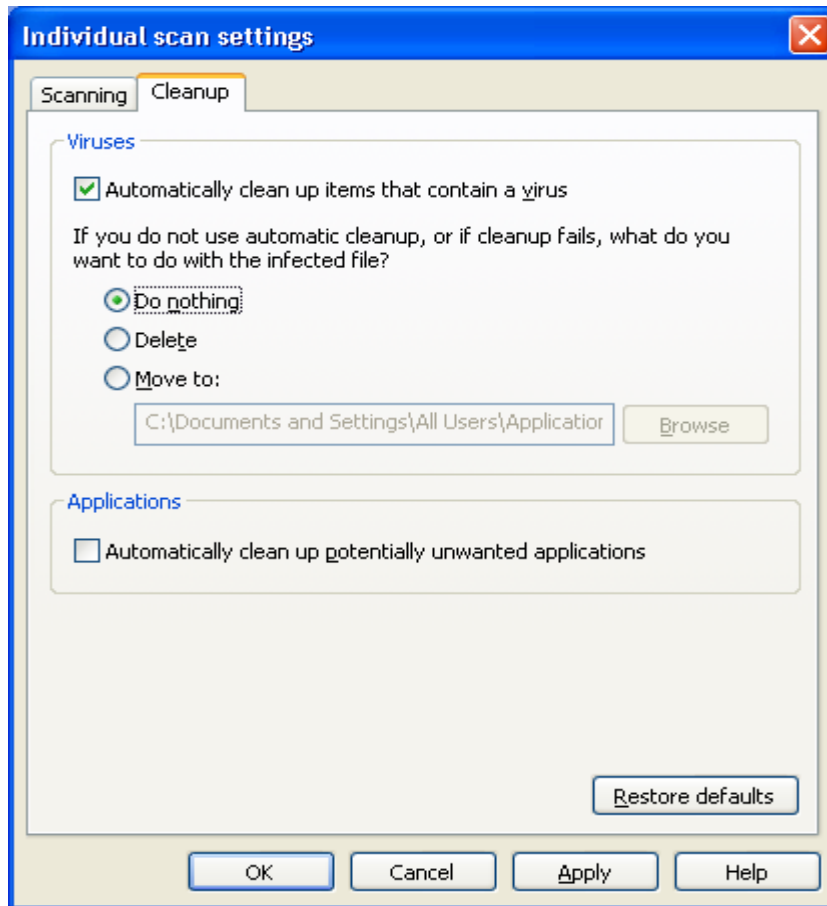


Fig.7 Cleanup settings

- You can choose other options for your scan as shown above in *Fig.7*

7.3 Setting up automatic cleaning for a right-click scan

To set up automatic cleanup for a right-click scan, follow the directions below:

- In the Sophos Anti-Virus window, in the **Configure** menu, click **Right-click scanning**. Click the **Cleanup** tab. Set the options as described in Section 7.2, above.

7.4 Potentially Unwanted Applications

You may wish to enable scanning for and cleanup of Potentially Unwanted Applications (PUAs) in on-demand scans or in right-click scans. To do so, check the **Automatically clean up potentially unwanted applications** box as shown in *Fig.7*, above.

8. Managing Quarantine Items

Quarantine Manager enables you to deal with any threats found by a scan which were not eliminated automatically. Any items listed in Quarantine Manager will be there for one of the following reasons:

- No cleanup options were selected for the scan that found the item
- A cleanup option was selected for the scan that found the item but the option failed
- The item is multiply-infected and still contains threats
- The threat was only partially detected and a full scan is needed to fully detect it

8.1 Dealing with viruses in quarantine

Access the Quarantine Manager by opening Sophos Anti-Virus and clicking on **Manage Quarantine Items**. The Quarantine Manager window appears, as shown in *Fig.8*, below, including a list of all infected items.

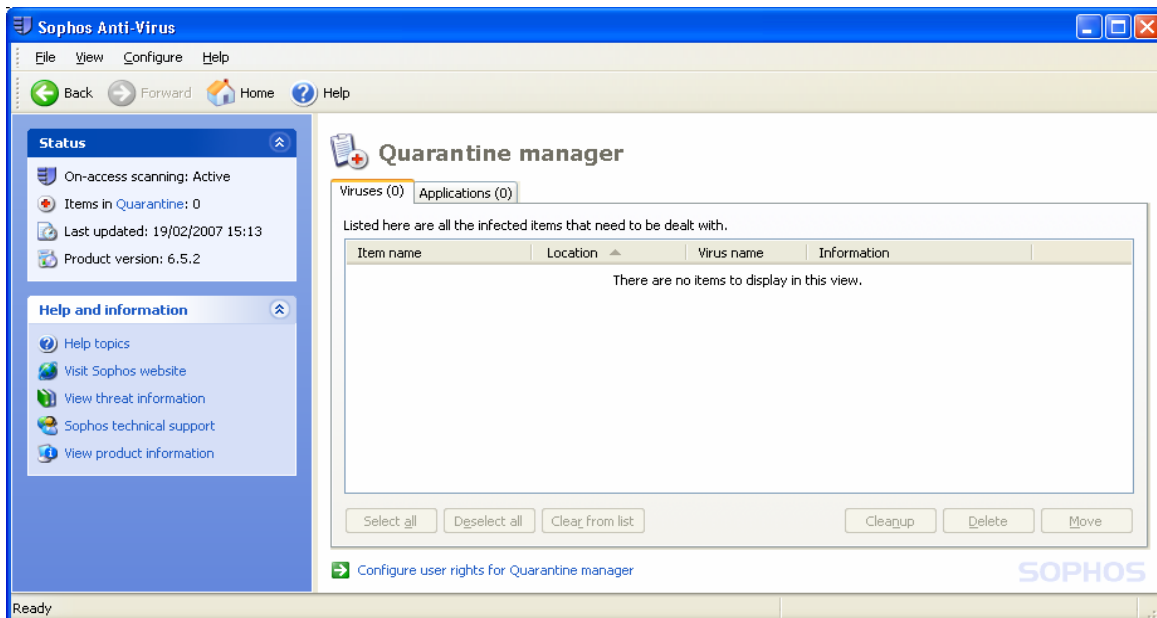


Fig.8 Quarantine Manager

If any items are multiply infected a **Details** link appears next to the item name. Click the link to open the **Virus Details** dialog to see the list of components that are part of the infection.

8.1.1 Actions to take against infected items

A number of actions are available:

Select all/Deselect all - use to select or deselect item. Allows you to perform the same actions on a group of items

Clear from list- use this to remove selected items from the list if you are certain they do not contain a virus

Cleanup - use to cleanup (e.g. disinfect) selected items. Cleanup will remove the virus but not the changes which the virus may have made.

Delete - disposes of the selected items. Use this item with care as it may cause your computer to stop functioning properly.

Move - Move the selected item to another folder. As with the delete function, use with care.

8.2 Dealing with Applications in Quarantine

Potentially Unwanted Applications (PUAs) can be viewed in Quarantine Manager as described in Section 8.1.

8.2.1 Actions to take against potentially unwanted applications

A number of the actions available for dealing with PUAs are the same as those for dealing with infected items: **Select All/Deselect All**, **Clear from list** and **Cleanup** are all available. Options specific to PUAs are listed below:

Authorise - Use this option to authorise selected applications on the computer, if you trust them. This adds the selected items to a list of authorised applications to ensure that Sophos Anti-Virus does not prevent them from running on your computer.

9. Troubleshooting

The appearance of the blue shield icon in the system tray provides a quick visual check of the status of Sophos Anti-Virus. If you experience any problems with Sophos Anti-Virus it is a good idea to make a note of the appearance of the icon before contacting the ITS Helpdesk.

Icon Appearance	Explanation
Blue shield	On-access scanning is active. Sophos Anti-Virus updated successfully last time
Green stripe over blue shield	Sophos Anti-Virus is updating. On-access scanning is active
Red circle with white cross appears over blue shield	Updating has failed. On-access scanning is active.
Grey shield	On-access scanning is inactive. Sophos Anti-Virus updated successfully last time
Green stripe over grey shield	Sophos Anti-Virus is updating. On-access scanning is inactive
Red circle with white cross over grey shield	Updating has failed. On-access scanning is inactive.

For all other troubleshooting matters or any queries or problems relating to Sophos Anti-Virus please contact the ITS Helpdesk in the first instance on x7555 or email helpdesk.