

# SOPHOS



**Windows NT/2000/XP single user**  
Installation guide

## About this guide

This guide tells you how to do the following on a single Windows NT/2000/XP computer.

- Install and configure Sophos Anti-Virus.
- Deal with viruses.
- Set up automatic disinfection.
- Keep Sophos Anti-Virus up to date.
- Uninstall Sophos Anti-Virus if you no longer need it.

## More information

This guide describes **recommended** installation and basic configuration options.

- You can find details of all other installation and configuration options in the *Sophos Anti-Virus Windows NT/2000/XP user manual*.
- Most Sophos documentation is published on the Sophos CD each month.

## Technical support

UK (24 hours):	(+44) 1235 559933	<a href="mailto:support@sophos.com">support@sophos.com</a>
USA:	(+1) 888 767 4679	<a href="mailto:supportus@sophos.com">supportus@sophos.com</a>
Australia (24 hours):	(+61) 2 9409 9111	<a href="mailto:support@sophos.com.au">support@sophos.com.au</a>
France:	(+33) 1 41 99 94 20	<a href="mailto:support@sophos.fr">support@sophos.fr</a>
Germany:	(+49) 6136 91193	<a href="mailto:support@sophos.de">support@sophos.de</a>
Japan (24 hours):	(+81) 45 348 8400	<a href="mailto:support@sophos.co.jp">support@sophos.co.jp</a>
Singapore:	(+65) 6776 7467	<a href="mailto:supportasia@sophos.com">supportasia@sophos.com</a>

## **Contents**

1 Installing and configuring Sophos Anti-Virus	3
2 Dealing with viruses	13
3 Setting up automatic disinfection	16
4 Keeping Sophos Anti-Virus up to date	19
5 Uninstalling Sophos Anti-Virus	27

# 1 Installing and configuring Sophos Anti-Virus

There are three steps:

- Install Sophos Anti-Virus (section 1.1).
- Download the latest virus identity files (IDEs) from the Sophos website (section 1.2).
- Optimise on-access scanning (section 1.3).

## 1.1 Install Sophos Anti-Virus

**!** You must uninstall any other anti-virus software before installing Sophos Anti-Virus.

Install Sophos Anti-Virus as follows.

1. Log on as Administrator. If it is a Windows XP computer, ensure all other users are logged off.

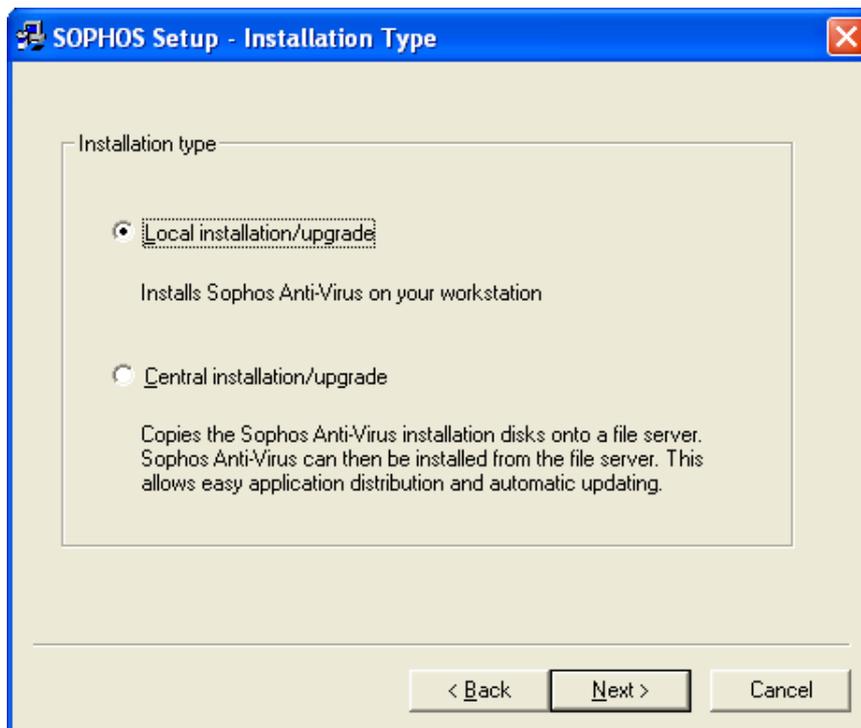
If you have already downloaded and unzipped the Sophos Anti-virus for Windows NT/2000/XP files from the Sophos website, go to [step 4](#).

2. Insert the Sophos CD in the CD drive. The CD should auto-run. If auto-run is disabled, run D:\Launchcd (where D: is the CD drive).
3. In the **Sophos CD** window, click **Sophos Anti-Virus**. At the next screen, click **Windows NT/2000/XP**, and start the setup program.

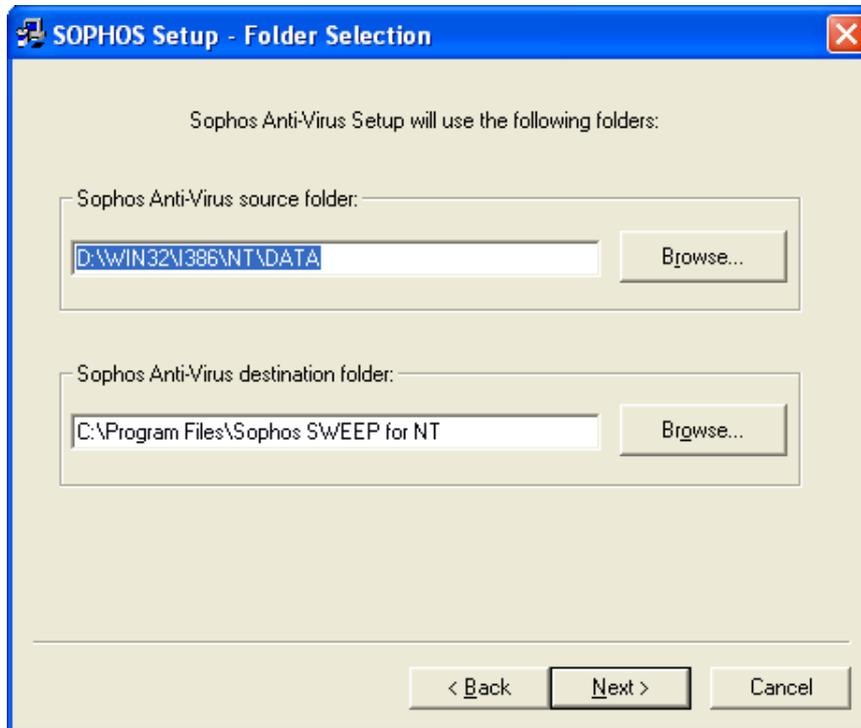
4. In the **SOPHOS Setup** dialog box, click **Next** to continue the installation.



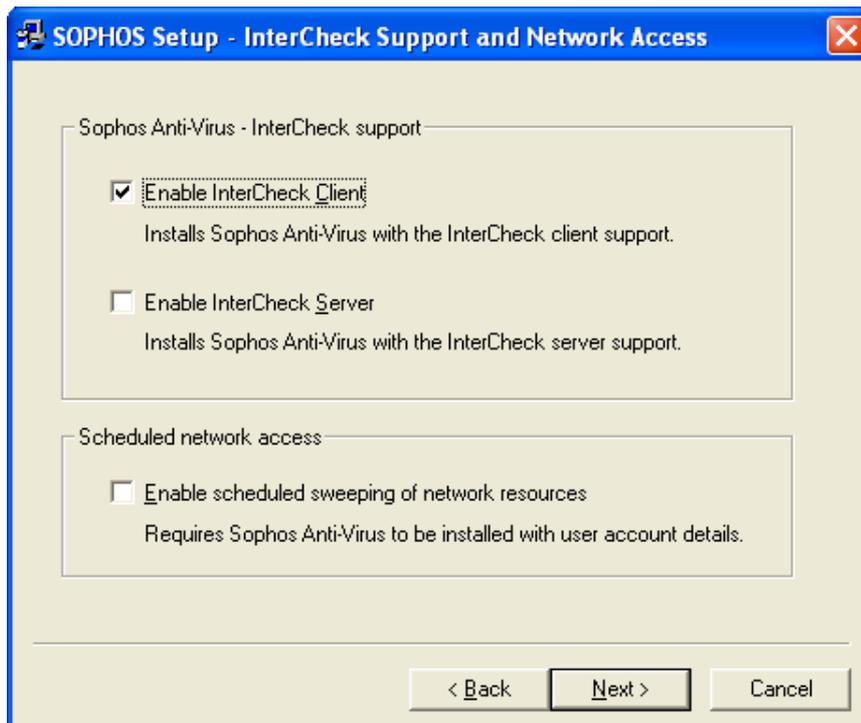
5. In the **SOPHOS Setup - Installation Type** dialog box, click **Local installation/upgrade**. Click **Next**.



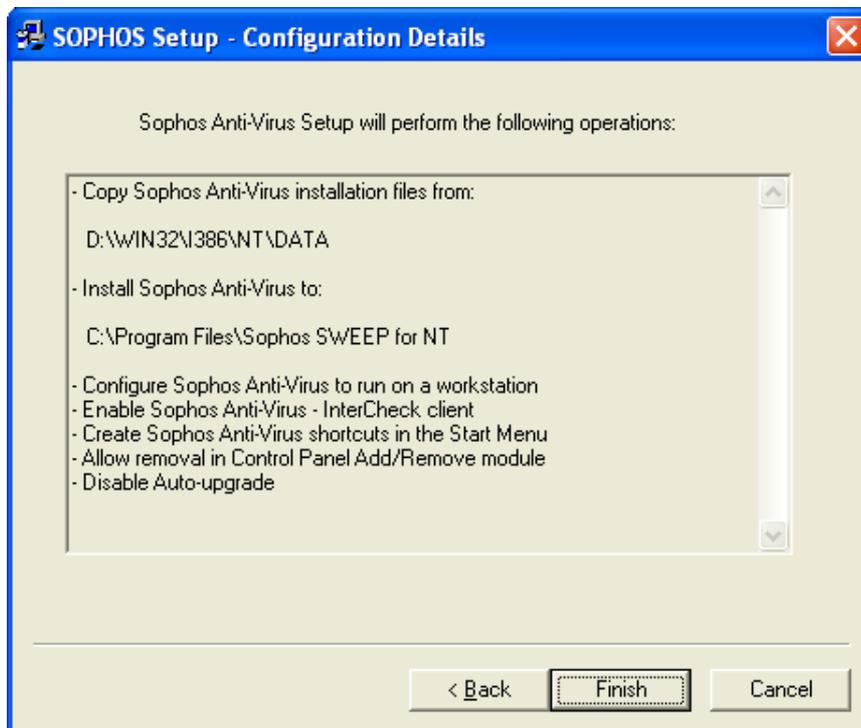
6. In the **SOPHOS Setup - Folder Selection** dialog box, click **Next** to accept the default folders.



7. In the **SOPHOS Setup - InterCheck Support and Network Access** dialog box, select **Enable InterCheck Client** only. Click **Next**.



8. In the **SOPHOS Setup - Configuration Details** dialog box, click **Finish** to complete the installation.

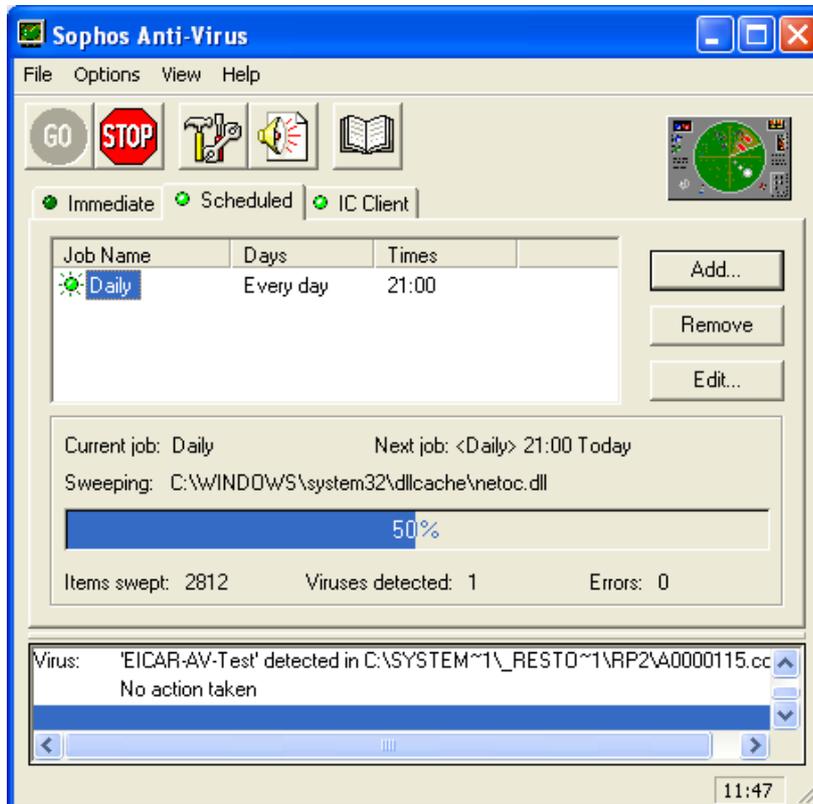


9. In the **SOPHOS Setup** message box, click **Run SWEEP**.



Sophos Anti-Virus starts to perform an initial scan of the computer. This takes place in the background, and may take some time to complete.

10. In the **Sophos Anti-Virus** window, click the **Scheduled** tab to display the scan progress.



11. Wait until the scan has finished.

**If Sophos Anti-Virus has not found a virus**, go straight to section 1.2 to download the latest IDEs.

**If Sophos Anti-Virus has found a virus**, it will display a message similar to the one shown below. Click **OK**. Deal with the virus first (section 2) and then complete the rest of the installation and configuration (sections 1.2 and 1.3).



## 1.2 Add the latest virus identity files (IDEs)

**?** A **virus identity file (IDE)** is a file that enables Sophos Anti-Virus to detect a specific virus. You need IDEs to protect your computer against viruses discovered since your version of Sophos Anti-Virus was compiled.

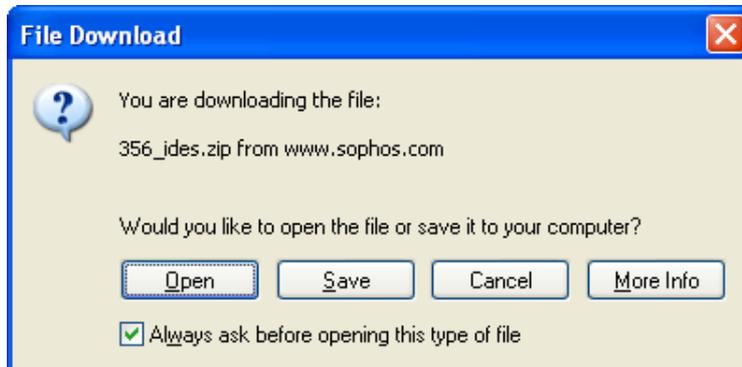
1. Go to the IDE download page of the Sophos website ([www.sophos.com/downloads/ide/](http://www.sophos.com/downloads/ide/)).

If you use Internet Explorer 5.0, click the **Virus identities (IDE) files FAQ** link and read the note on IE 5.0.

2. Click **Download Zip**.



3. **If the computer is running Windows NT or XP**, in the **File Download** dialog box, click **Save** to save it to your computer.



- If the computer is running Windows 2000**, in the **File Download** dialog box, click **OK** to save it to your computer.



4. In the **Save As** dialog box, save this zipped file to any location on the hard disk (e.g. the desktop). At this time it is not important where you save it to, as long as you know where it is.
5. On the hard disk, locate and double-click the zipped file you saved in the previous step (called \*\_ide.zip, where \* is the latest Sophos Anti-Virus version number).

6. **If the computer is running Windows XP**, in the \*\_ide.zip window, click **Extract all files**. In the **Select a destination** dialog box, browse to

C:\Program Files\Sophos SWEEP for NT

and click **OK**.

**If the computer is running Windows NT or Windows 2000**, your unzip utility displays a dialog box that enables you to extract the files from the zipped file (archive). Save the extracted files to

C:\Program Files\Sophos SWEEP for NT

-  If you do not have an unzip program on your computer, scroll down the page and download the IDEs one by one, to the location above.

7. Restart the computer.

You have completed installation of Sophos Anti-Virus.

It is recommended that you now optimise on-access scanning (section 1.3).

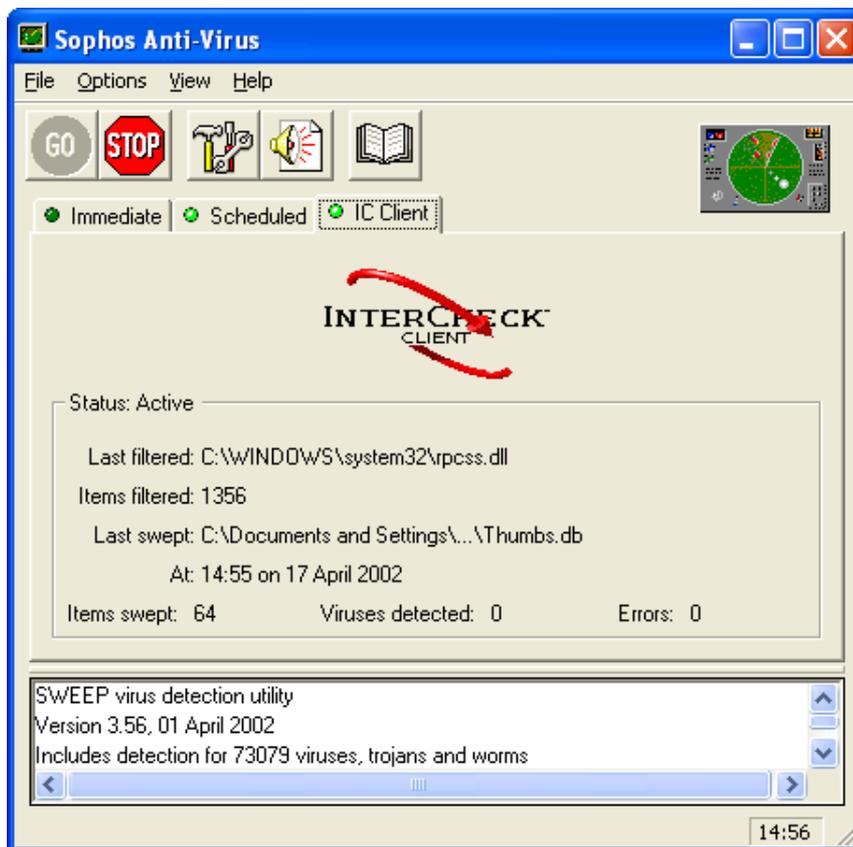
### 1.3 Optimise on-access scanning

Your installation includes an on-access scanner called InterCheck.

- ❓ **InterCheck** checks files for viruses every time they are accessed by the computer. If it finds a virus in a file (e.g. in an email attachment), it prevents your computer from opening it. InterCheck on-access scanning is currently active on your computer.

By default, InterCheck only checks files as they are opened ('on read'). In this section you enable InterCheck to detect viruses that write to or rename files without opening them.

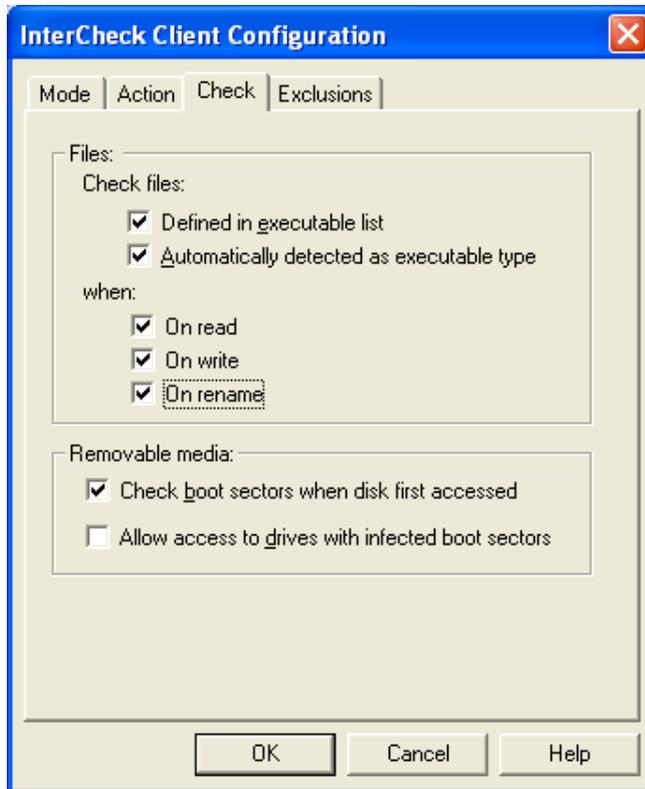
1. At the taskbar, click **Start | Programs | Sophos Anti-Virus | Sophos Anti-Virus**.
2. In the **Sophos Anti-Virus** window, click the **IC Client** tab.



2. Click the **Configuration** button.



3. In the **InterCheck Client Configuration** dialog box, click the **Check** tab. As well as the currently selected items, select **On write** and **On rename**. Click **OK**.



You do not need to configure Sophos Anti-Virus further.

Section 2 contains information about how to deal with a virus. [Section 3](#) describes how to set up automatic disinfection.

- ❗ **Remember to update Sophos Anti-Virus every month. In addition, you must update Sophos Anti-Virus whenever there is a significant new virus threat. Updating is described in [section 4](#).**

## 2 Dealing with viruses

This section explains what you should do if you have a virus on your computer. You should

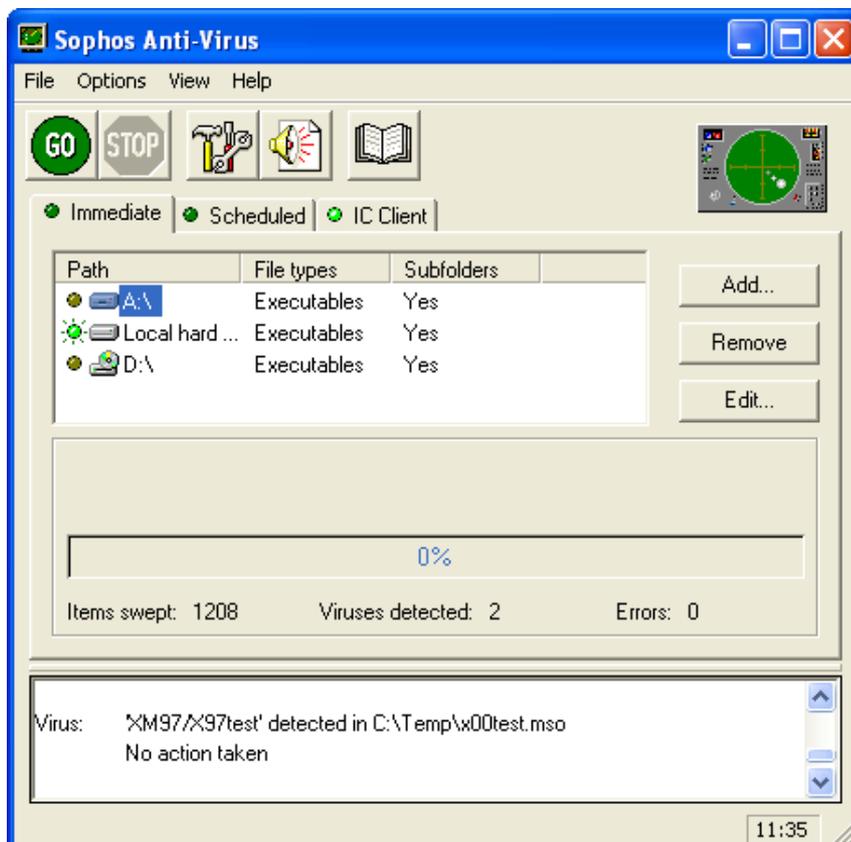
- find out about the virus (section 2.1)
- perform disinfection, if appropriate (section 2.2).

This section assumes you have already installed Sophos Anti-Virus as described in section 1.1.

### 2.1 Find out about the virus

In order to deal with the virus, you must first find out about it as follows.

1. At the taskbar, click **Start | Programs | Sophos Anti-Virus | Sophos Anti-Virus**.
2. The log at the bottom of the **Sophos Anti-Virus** window shows the name of the virus. Double-click the name of the virus to view its analysis on the Sophos website.



3. Read the information on the web page about what type of virus it is, and how to recover from it.

**If, according to the analysis, you have a macro virus**, you can attempt to disinfect documents as explained next (section 2.2). **If you have another type of virus**, follow the recovery instructions on the website.

## 2.2 How to perform disinfection

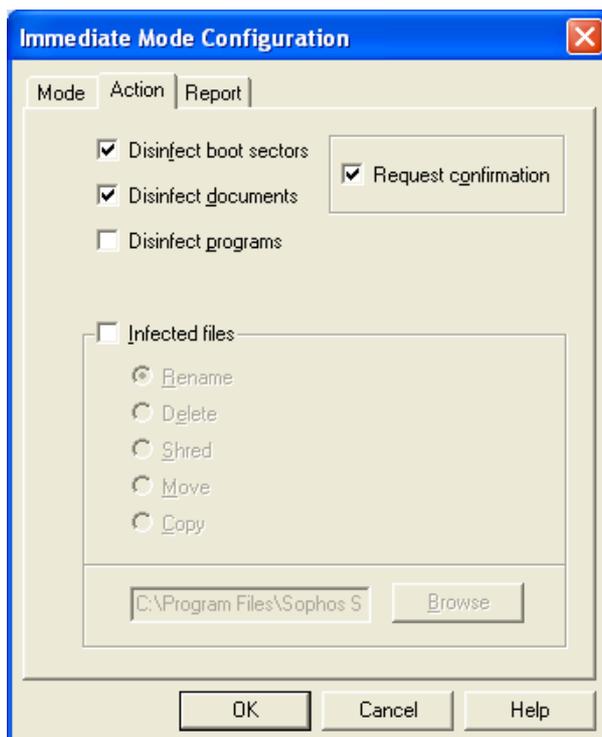
This section explains how to use Sophos Anti-Virus to perform disinfection. To do this, you run an immediate scan with disinfection enabled.

**?** An **immediate scan** is a virus scan of the computer or parts of the computer that you can carry out at any time.

1. In the **Sophos Anti-Virus** window, click the **Immediate** tab.
2. Click the **Configuration** button.



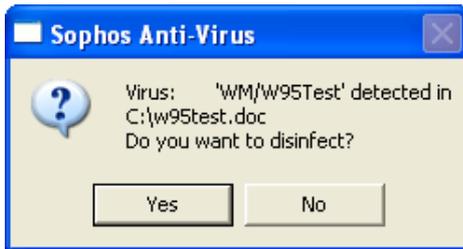
3. In the **Immediate Mode Configuration** dialog box, click the **Action** tab. Select **Disinfect documents**. This ensures that Sophos Anti-Virus will attempt to disinfect any infected documents it finds during an immediate scan. Click **OK**.



- Click **GO** to start the scan.



- If Sophos Anti-Virus discovers an infected document or boot sector, a dialog box similar to the following is displayed. Click **Yes**.



- When the scan has finished, check the contents of the log in the **Sophos Anti-Virus** window.

*If the log says that a file has been disinfected*, repeat the scan. If no viruses are reported, you have completed disinfection. Otherwise, keep repeating the scan until the number of viruses reported does not decrease.

*If the number of viruses reported does not decrease after further scans or if the log says that a file could not be disinfected*, you should attempt to disinfect the file manually, using the disinfection instructions for that virus on the Sophos website. In the log, double-click the name of the virus to view its analysis on the Sophos website.

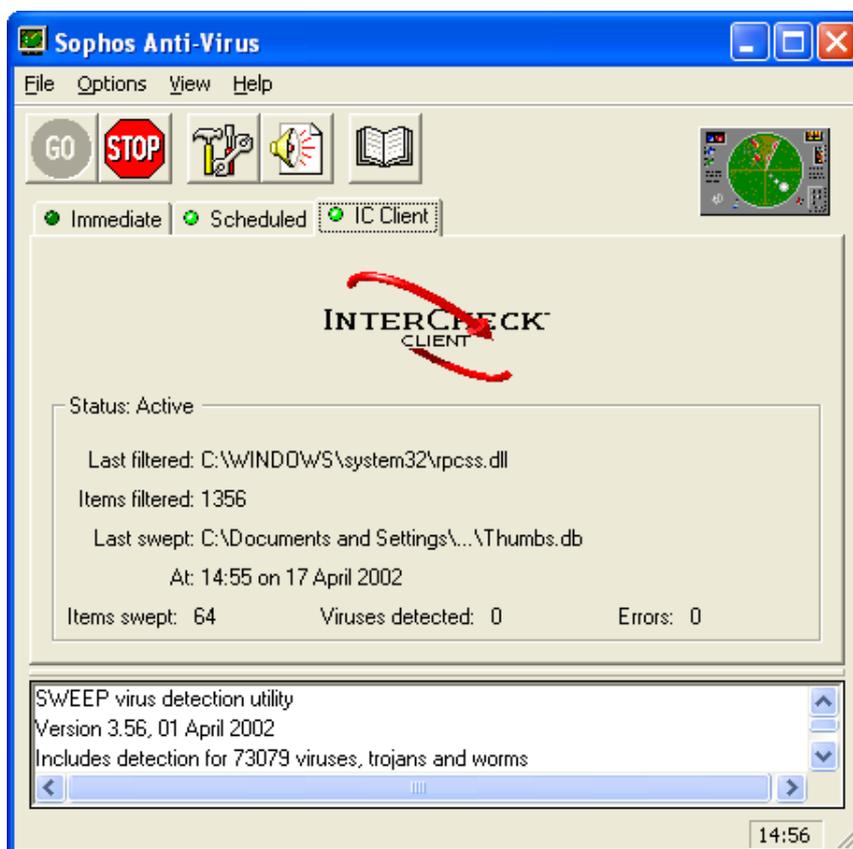
- ⚠ **Always check infected items after they have been disinfected. Disinfection removes the virus, but does not reverse the side-effects. Check the analysis of the virus on the Sophos website for more information.**

### 3 Setting up automatic disinfection

This section explains how to set up automatic disinfection of any document found by InterCheck to be infected with a virus.

**?** **InterCheck** checks files for viruses every time they are accessed by the computer. If it finds a virus in a file (e.g. in an email attachment), it prevents your computer from opening it. InterCheck on-access scanning is currently active on your computer.

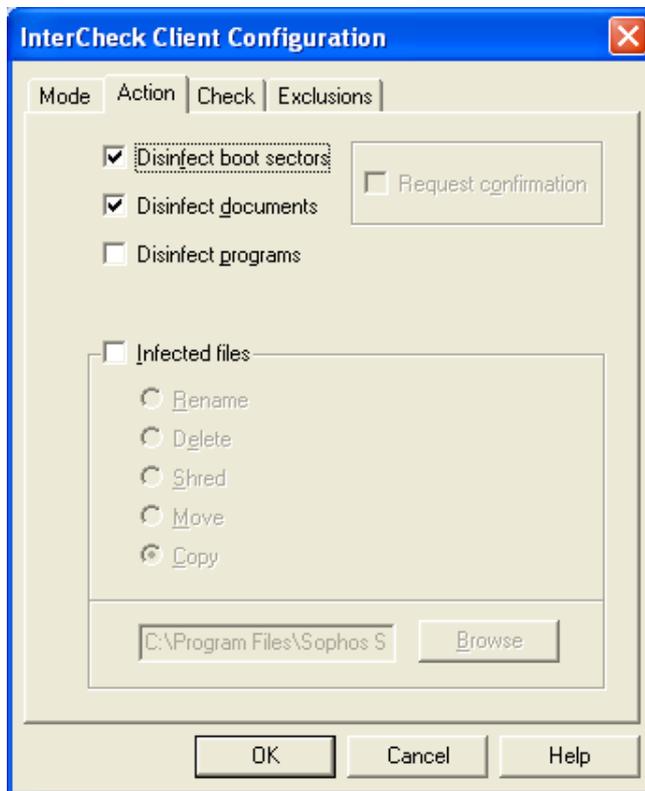
1. Log on to the computer with Administrator rights.
2. At the taskbar, click **Start | Programs | Sophos Anti-Virus | Sophos Anti-Virus**.
3. In the **Sophos Anti-Virus** window, click the **IC Client** tab.



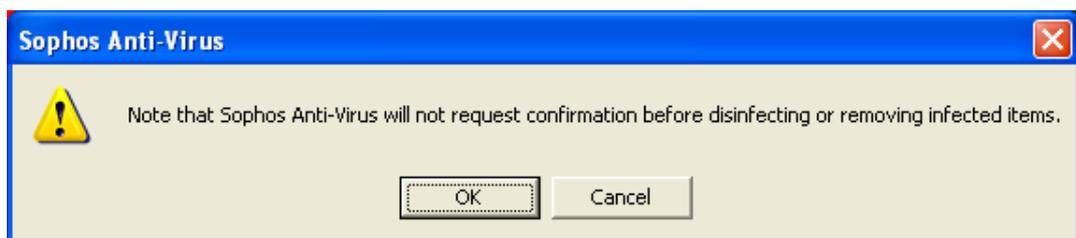
4. Click the **Configuration** button.



5. In the **InterCheck Client Configuration** dialog box, click the **Action** tab. Ensure **Disinfect Boot Sectors** is selected and select **Disinfect documents**.



6. The following message is displayed. It means that if InterCheck finds a virus in a file, it will attempt to disinfect it without first asking for permission. Click **OK**.

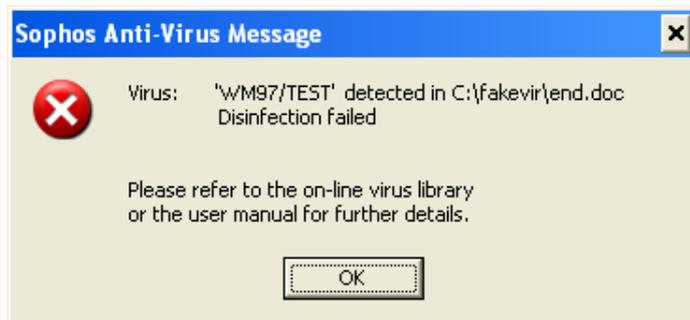


7. In the **InterCheck Client Configuration** dialog box, click **OK**.

From now on Sophos Anti-Virus will try to disinfect any boot sectors or documents it finds to be infected with a virus.

- ❗ **Always check infected items after they have been disinfecting. Disinfection removes the virus, but does not reverse the side-effects. Check the analysis of the virus on the Sophos website for more information.**

If InterCheck discovers a virus that cannot be automatically disinfected, a dialog box similar to the following is displayed.



If this happens, write down the name of the virus, then click **OK**. Open the **Sophos Anti-Virus** window and double-click the name of the virus in the log at the bottom of the window. You are connected directly to an analysis of the virus on the Sophos website, which includes disinfection advice.

## 4 Keeping Sophos Anti-Virus up to date

Sophos Anti-Virus must be updated regularly to enable it to detect all the latest viruses. You must update Sophos Anti-Virus

- each month, when the new version of Sophos Anti-Virus is released (section 4.1)
- whenever a significant new virus threat is discovered (section 4.2).

### 4.1 To update Sophos Anti-Virus each month

There are two steps:

- Update the Sophos Anti-Virus files (section 4.1.1).
- Add new virus identity files (IDEs) (section 4.1.2).

#### 4.1.1 Update the Sophos Anti-Virus files

1. *If you update Sophos Anti-Virus from the Sophos website each month*, go to [www.sophos.com/downloads/products](http://www.sophos.com/downloads/products) and click **I am an existing licensed Sophos customer**.

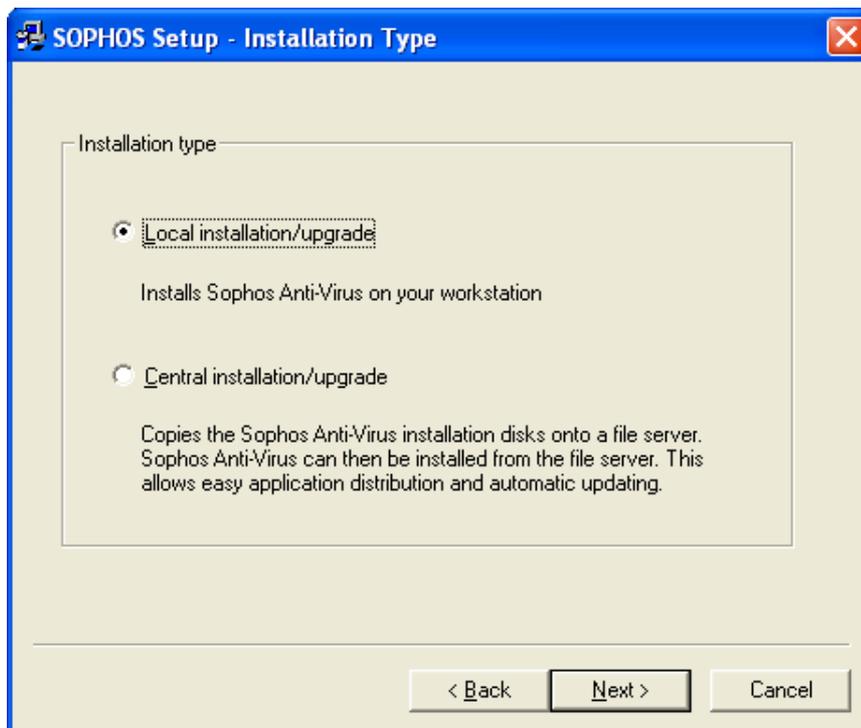
*If you update Sophos Anti-Virus from a new CD each month*, insert the Sophos CD in the CD drive, click **Sophos Anti-Virus**, click **Windows NT/2000/XP**, start the setup program and go straight to [step 9](#), below.

2. Enter your username and password and click **Submit**.
- 🔗 If you do not know your username and password, send an email to [customerservice@sophos.com](mailto:customerservice@sophos.com) stating your full details.
3. In the list of platforms, click **Sophos Anti-Virus for Windows NT/2000/XP**.
4. In the **Products** table, click **Sophos Anti-Virus for Windows NT/2000/XP**.
5. Click the name of the Self-extractable Zip archive. In the **File Download** dialog box, click **Save** (or **OK**) and save it to your hard disk (e.g. the desktop). At this time it is not important where you save it to, as long as you know where it is.
6. Locate and double-click the archive. Click **OK** on the **WinZip Self-Extractor** message box.
7. Click **Unzip** in the **Sophos Anti-Virus for Windows NT/2000/XP** dialog box.
8. Click **OK** in the **WinZip Self-Extractor** message box to begin setup.

9. In the **SOPHOS Setup** dialog box, click **Next**.



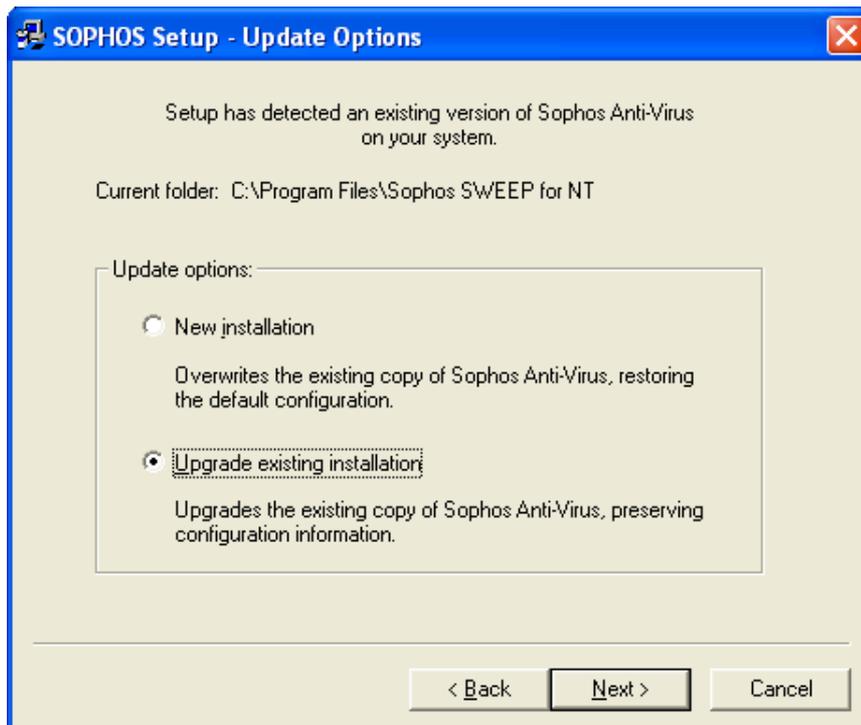
10. In the **SOPHOS Setup - Installation Type** dialog box, click **Local installation/upgrade**. Click **Next**.



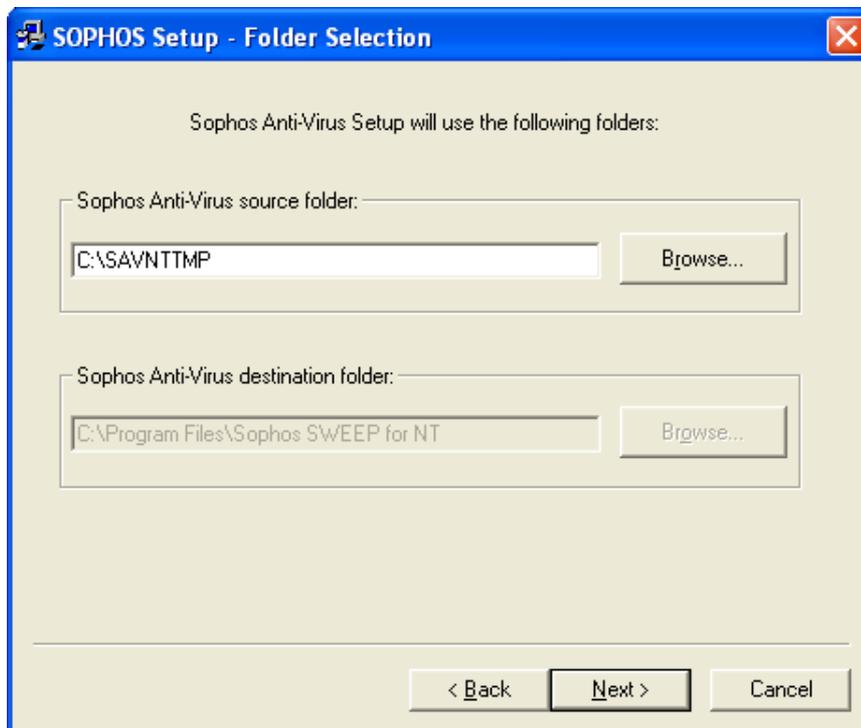
11. In the **SOPHOS Setup - Active applications** dialog box, click **Close** to close down InterCheck Monitor.



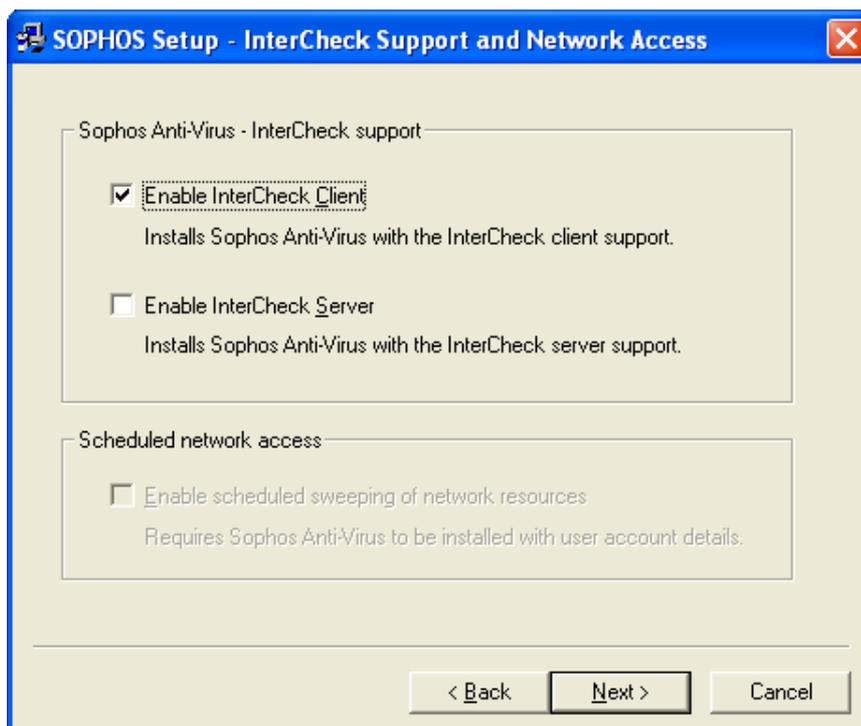
12. In the **SOPHOS Setup - Update Options** dialog box, click **Upgrade existing installation**. Click **Next**.



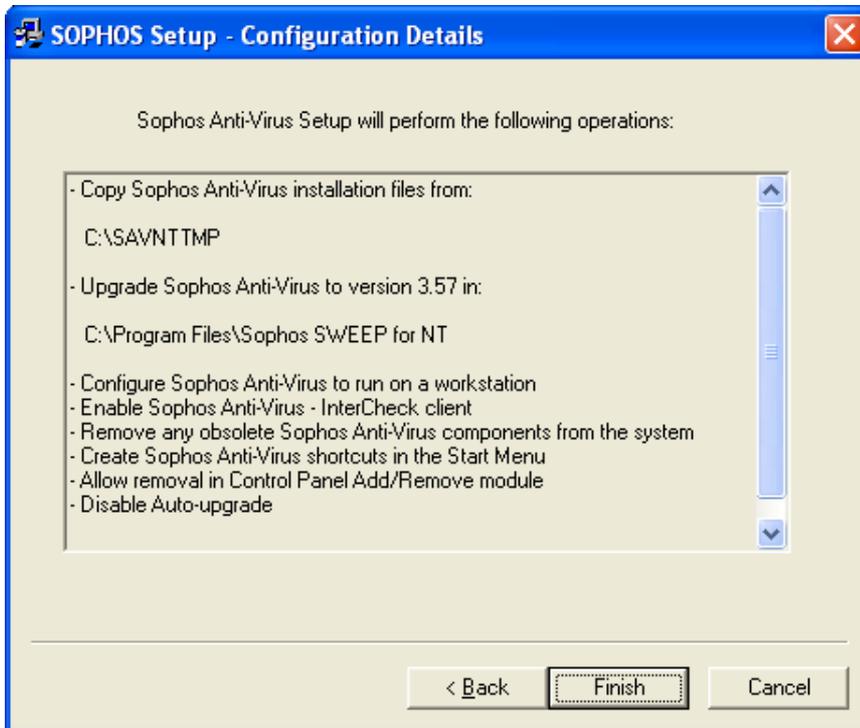
13. In the **SOPHOS Setup - Folder Selection** dialog box, click **Next** to accept the default folders.



14. In the **SOPHOS Setup - InterCheck Support and Network Access** dialog box, select **Enable InterCheck Client** only. Click **Next**.



15. In the **SOPHOS Setup - Configuration Details** dialog box, click **Finish** to complete the installation.



16. In the **SOPHOS Setup** message box, click **Finish** or **Restart Now**.

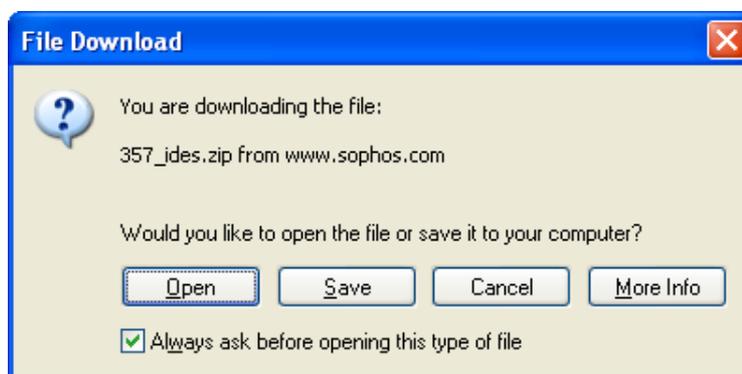


Now replace out-of-date IDEs (section 4.1.2).

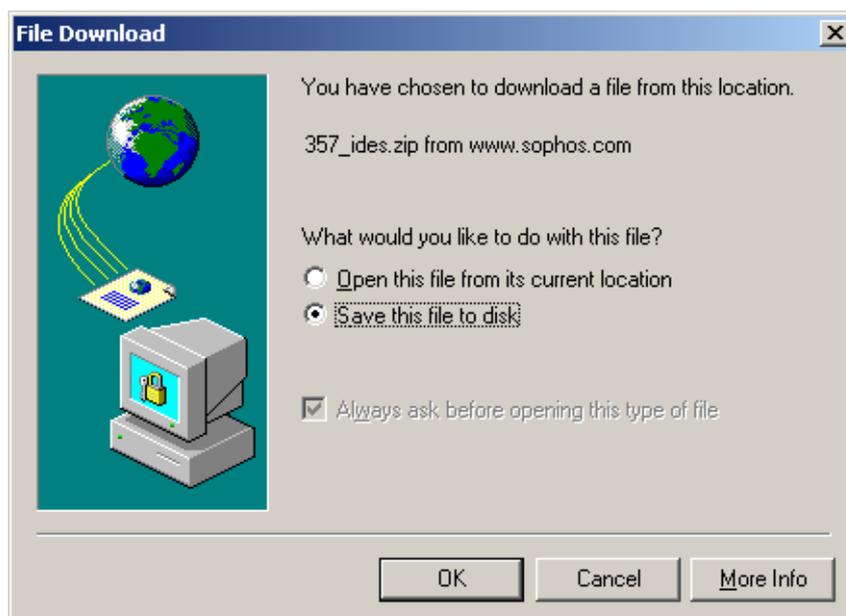
### 4.1.2 Replace the out-of-date IDEs

You must remember to download new IDEs after you have updated the Sophos Anti-Virus files.

1. If necessary, delete any \*\_ide.zip files you downloaded either during installation or the last time you updated Sophos Anti-Virus.
2. Go to the IDE downloads page of the Sophos website ([www.sophos.com/downloads/ide](http://www.sophos.com/downloads/ide)) and click **Download Zip**.
3. **If the computer is running Windows NT or XP**, in the **File Download** dialog box, click **Save** to save it to your computer.



**If the computer is running Windows 2000**, in the **File Download** dialog box, click **OK** to save it to your computer.



4. In the **Save As** dialog box, save the zipped file to any location on the hard disk (e.g. the desktop). At this time it is not important where you save it to, as long as you know where it is.
5. On the hard disk, locate and double-click the zipped file (called \*\_ide.zip, where \* is the latest Sophos Anti-Virus version number).
6. **If the computer is running Windows XP**, in the \*\_ide.zip window, click **Extract all files**. In the **Select a destination** dialog box, browse to

C:\Program Files\Sophos SWEEP for NT

and click **OK** to save the files to this location.

**If the computer is running Windows NT or Windows 2000**, your unzip utility displays a dialog box that enables you to extract the files from the zipped file (archive). Save the extracted files to

C:\Program Files\Sophos SWEEP for NT

-  If you do not have an unzip program on your computer, scroll down the page and download the IDEs one by one, to the location above.

7. Restart the computer.

You have completed the monthly update of Sophos Anti-Virus.

## 4.2 To update Sophos Anti-Virus when a new virus is discovered

This type of update is carried out between monthly updates of Sophos Anti-Virus. Whenever there is a significant new virus threat, such as a fast-spreading email worm, you must download the IDE for it from the Sophos website.

- ❗ To receive email notifications about IDEs and other alerts, register at [www.sophos.com/virusinfo/notifications](http://www.sophos.com/virusinfo/notifications).
  - 1. Log on with Administrator rights and go to [www.sophos.com/downloads/ide](http://www.sophos.com/downloads/ide).
  - 2. Scroll down the web page and click on the name of the IDE you want to download.
  - 3. In the **File Download** dialog box, click **Save** (or **OK**) to save it to your computer.
  - 4. In the **Save As** dialog box, browse to  
C:\Program Files\Sophos SWEEP for NT  
and click **Save**.
  - 5. Restart the computer.
  - 6. At the task bar, click **Start | Programs | Sophos Anti-Virus | Sophos Anti-Virus**.
  - 7. In the **Sophos Anti-Virus** window, on the **Options** menu, click **Purge Checksums**.
- Sophos Anti-Virus will start to use the new IDE.

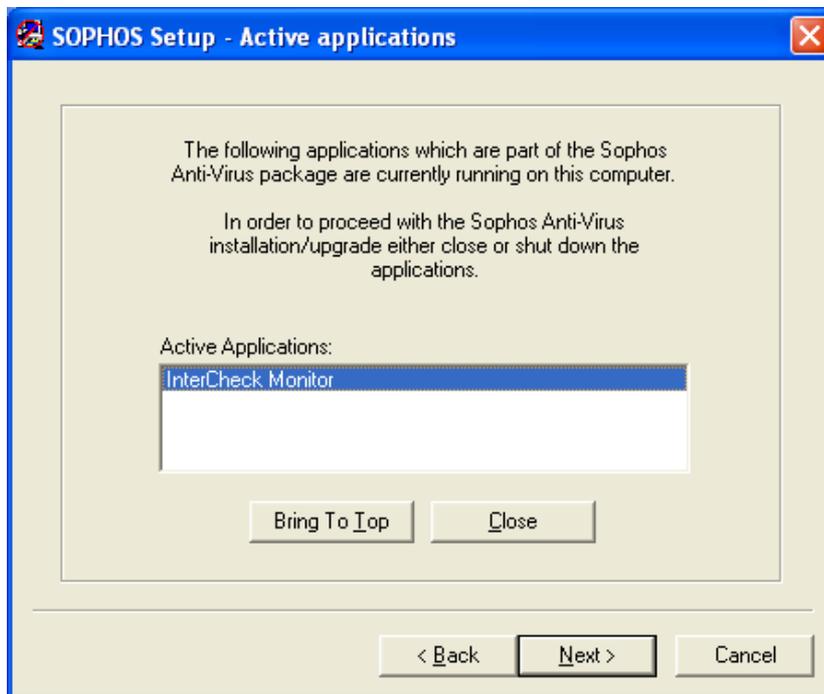
## 5 Uninstalling Sophos Anti-Virus

If you no longer need Sophos Anti-Virus, uninstall it as follows.

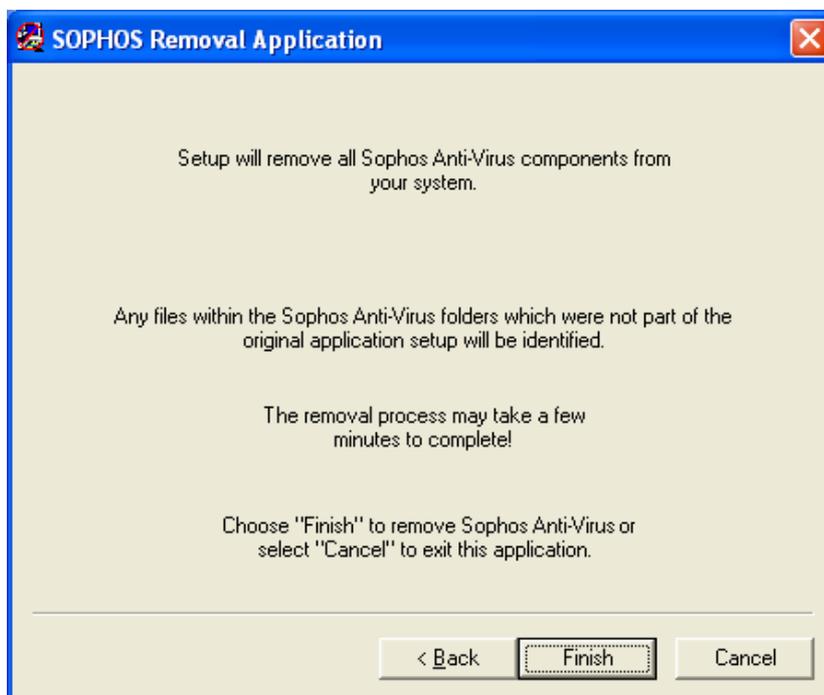
1. Log on to the computer with Administrator rights.
2. At the taskbar, click **Start | Programs | Sophos Anti-Virus | Uninstall Sophos Anti-Virus**.
3. In the **SOPHOS Removal Application** dialog box, click **Next**.



4. In the **SOPHOS Setup - Active applications** dialog box, click **Close**. Then click **Next**.



5. In the **SOPHOS Removal Application** dialog box, click **Finish**.



Sophos Anti-Virus is removed from the computer.