

SOPHOS

Sophos Anti-Virus for Mac OS X, version 4.9 startup guide

For networked Macs running Mac OS X

Document date: June 2007



About this guide

- 💡 If you have a Windows server, you are recommended to use Sophos Enterprise Console to install and update Sophos Anti-Virus on your Mac OS X computers. See the *Sophos Endpoint Security and Control network startup guide* instead of this guide.
- 💡 If you have a single Mac OS X computer, see the *Sophos Anti-Virus standalone startup guide* instead of this guide.
- 💡 If you have a UNIX or Linux server, see Sophos support knowledgebase article 12987 (www.sophos.com/support/knowledgebase/article/12987.html) instead of this guide.
- 💡 If you have a NetWare server, see Sophos support knowledgebase article 12988 (www.sophos.com/support/knowledgebase/article/12988.html) instead of this guide.

This guide tells you how to

- install Sophos Anti-Virus on networked Mac OS X computers
- set up automatic updating and email virus alerts
- run a scan
- eliminate viruses manually
- remove Sophos Anti-Virus.

You can find details of all other configuration options in the *Sophos Anti-Virus for Mac OS X user manual*.

Sophos documentation is published at www.sophos.com/support/docs/ and on the Sophos CDs.

Contents

1 System requirements	3
2 Installing Sophos Anti-Virus	4
3 Scanning a computer for viruses	8
4 Eliminating viruses	10
5 Uninstalling Sophos Anti-Virus	13
Technical support	14

1 System requirements

1.1 Sophos Update Manager

Sophos Update Manager enables you to download and deploy anti-virus software.

Operating system requirement:

- Mac OS X 10.3 or later

Sophos recommends that you install it on a server, because workstations continually check this Mac for anti-virus updates.

Disk space and memory requirements:

- 40 MB of free hard disk space
- 128 MB of RAM

Other requirements:

- Internet connection
- Access to and from the other Macs on the network

1.2 Sophos Anti-Virus

Operating system requirement:

- Mac OS X 10.2 or later

Disk space and memory requirements:

- 70 MB of free hard disk space
- 128 MB of RAM

2 Installing Sophos Anti-Virus

- ❗ You must uninstall any other vendor's anti-virus software before installing Sophos Anti-Virus.

Installation on networked Macs involves two main stages:

- Create a central installation on the server.
- Install Sophos Anti-Virus on the server and workstations from the central installation.

2.1 Create the central installation

You must create the central installation on a Mac that meets the system requirements in [sections 1.1 and 1.2](#).

1. Go to the Mac server, or a Mac workstation that has access to the server.

Download the **Sophos Anti-Virus for Mac network installer** from the Sophos website and run it.

Alternatively, insert the **Sophos Network Install CD**. On the desktop, double-click the CD icon. In the window that is displayed, open the **Sophos Anti-Virus OS X** folder. Double-click **Sophos Anti-Virus Network.pkg**.

2. A Mac installer is run. Click **Continue**. Follow the steps until the installation is finished.



A central installation is placed in the **Sophos Anti-Virus/ESOSX** folder on the volume you specified.

You now use a program called Sophos Update Manager to configure

- the central installation to update from Sophos (section 2.2)
- workstations to update from the central installation (section 2.3)
- workstations to send virus alerts to the server (section 2.4).

After configuration, Update Manager automatically downloads updates from Sophos to the central installation, from which workstations automatically update.

2.2 Configure the central installation to update from Sophos

2.2.1 Configure general settings

1. Browse to the **Applications** folder on the volume on which you created the central installation. Double-click **Sophos Update Manager**.
2. In the **Sophos Update Manager** window, click the **Software Update** toolbar icon.
3. On the **General** tabbed page, in the **Username** and **Password** text boxes, enter the username and password that were supplied to you by Sophos for connecting to the Sophos website.
4. Make sure that the **Location of downloaded software updates** text box contains the location that you specified during installation. If not, you must specify the location.

2.2.2 Configure the proxy

By default, Update Manager connects to Sophos using your system proxy settings. If you want to change this, do as follows. Otherwise, continue to section 2.3.

1. Click the **Proxy** tab.
2. If you don't want Update Manager to connect via a proxy, click **Do not use proxy**.
3. If you want to specify other proxy settings for Update Manager to use, click **Use custom proxy settings** and enter the settings in the **Address**, **Port**, **Username**, and **Password** text boxes.

2.3 Configure workstations to update from the central installation

2.3.1 Configure the source for updates

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **AutoUpdate** tabbed page, on the pop-up menu, ensure that **Network Settings** is chosen.

On the **Primary Server** tabbed page, click **Network volume** or **Company web server**, depending on where you created the central installation. In the **URL** text box, enter the path to the share where the **Sophos Anti-Virus/ESOSX** folder is located. Include the share type, the server name, the share name and the **Sophos Anti-Virus/ESOSX** folder itself.

For example, enter:

```
afp://<server name>/<afp share name>/Sophos Anti-Virus/ESOSX  
(for an AppleShare share)
```

```
http://<server name>/<web share name>/Sophos Anti-Virus/ESOSX  
(for a web share)
```

```
smb://<server name>/<Samba share name>/Sophos Anti-Virus/ESOSX  
(for a Samba share)
```

You can use an IP address or NetBIOS name instead to refer to the server. Using an IP address can be better if you have any DNS problems.

If necessary, enter the **Username** and **Password** needed to access the central installation. If the share type is afp, the password must be no longer than eight characters.

2.3.2 Configure the proxy

By default, workstations connect to the central installation using your system proxy settings. If you want to change this, do as follows. Otherwise, continue to section 2.4.

1. Click the **Primary Proxy** tab.
2. If you don't want workstations to connect via a proxy, click **Do not use proxy**.
3. If you want to specify other proxy settings for workstations to use, click **Use custom proxy settings** and enter the settings in the **Address**, **Port**, **Username**, and **Password** text boxes.

2.4 Configure workstations to send virus alerts to the server

1. Click the **Notification** tab.
2. Select the **Enable on-access scanner email notification** check box (and the option for the immediate scanner as well if users will do on-demand scanning). Enter the email address of the **Recipient** to whom you want alerts sent. Enter a **Sender** address to which undelivered alerts can be returned. Then enter the address of the **Outgoing mail server** and the Mac **Port** that is used to send virus reports.
3. Click **Set** and close Update Manager.

2.5 Install Sophos Anti-Virus on networked Macs

Before installation on each Mac, you must ensure that

- System Preferences is closed
- the server where you created the central installation is mounted on the desktop, unless you're installing on this server.

To perform the installation, do as follows.

1. At the Mac where you want to install Sophos Anti-Virus, browse to the **Sophos Anti-Virus/ESOSX** folder on the server where you created the central installation.
2. If you're installing on a workstation, copy **Sophos Anti-Virus.mpkg** to the Desktop.
3. Double-click Sophos Anti-Virus.mpkg.



Sophos Anti-Virus.mpkg

4. A Mac installer is run. Click **Continue**. Follow the steps until installation is finished. In the Installation Type dialog box, you are recommended to accept **Easy Install**.

When installation is complete, your computer is protected by on-access scanning.

3 Scanning a computer for viruses

On workstations, Sophos Anti-Virus automatically checks each file as you access it and grants access only if it is virus-free.

If you want to scan the server, or run an on-demand scan on a workstation, do as follows.

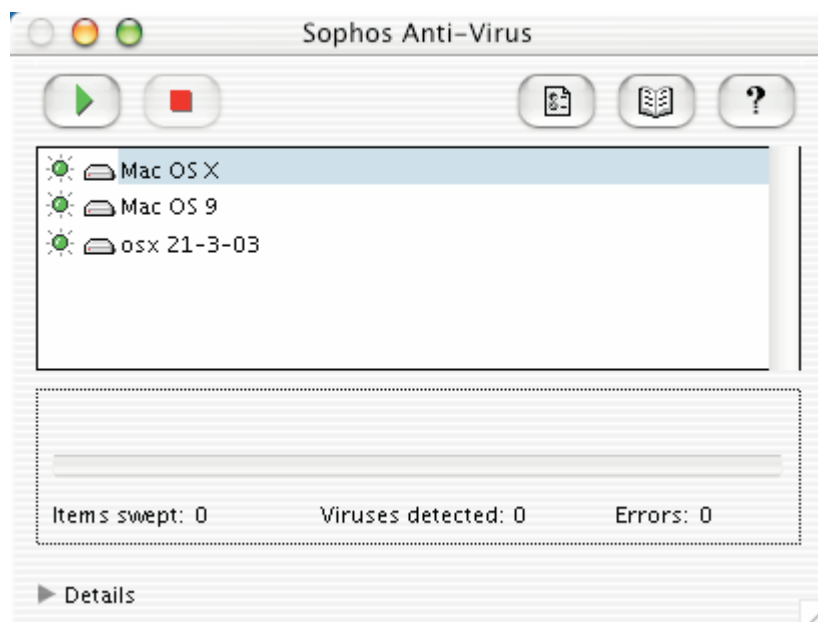
? An **on-demand scan** is a virus scan of the computer or parts of the computer that you can carry out at any time.

1. Click the Sophos Anti-Virus icon (a shield) in the system status bar. In the menu that is displayed, choose **Open Sophos Anti-Virus**.



! Alternatively, in Finder, click **Applications**. Then double-click **Sophos Anti-Virus**.

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

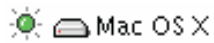


Items with an illuminated green light beside them are selected for scanning. Click the light to select or deselect items.

To scan all selected items, click the **Start** button in the toolbar.



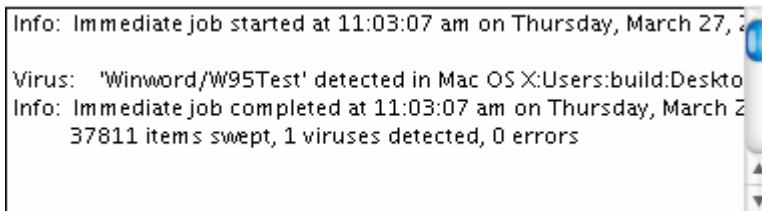
To scan any item listed, double-click its icon in the list, for example



To scan any item on your computer, simply drag and drop the file from the **Finder** window onto the **Start** button.

To scan several files, folders or disks, drag and drop them from the **Finder** window onto the list. Then click the **Start** button.

- ❗ To remove items from the list, drag them to the Trash icon in the Dock.
- 3. Click **Details** at the bottom left of the **Sophos Anti-Virus** window to see the results of the scan.



- ❗ If Sophos has found a virus, double-click on its name in the **Details** pane to be connected to its virus analysis on the Sophos website.

For information on eliminating viruses, see section 4.

4 Eliminating viruses

Sophos Anti-Virus can disinfect certain infected files automatically. For details, see the *Sophos Anti-Virus for Mac OS X user manual*.

To deal with viruses found during an on-demand scan, you should

- find out about the virus (section 4.1)
- perform disinfection, if appropriate (section 4.2).

4.1 Find out about the virus

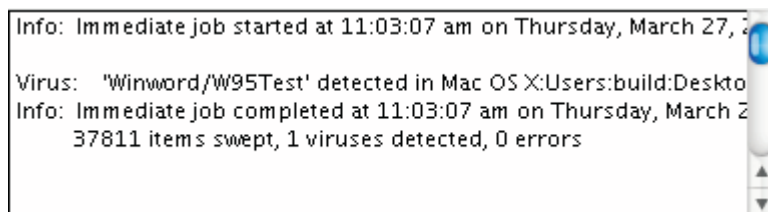
In order to deal with the virus, you must first find out what kind of virus it is and what types of files it infects.

1. If the **Sophos Anti-Virus** window is not already open, open it as follows.

Click the Sophos Anti-Virus icon in the system status bar. In the menu that is displayed, choose **Open Sophos Anti-Virus**.



1. Alternatively, in Finder, click **Applications**. Then double-click **Sophos Anti-Virus**.
2. At the bottom of the **Sophos Anti-Virus** window, click **Details** to open the log. The log shows the names of the virus(es). 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 or program virus, you can attempt to disinfect documents as explained next (section 4.2). ***If you have another type of virus***, follow the recovery instructions on the website.

4.2 How to perform disinfection

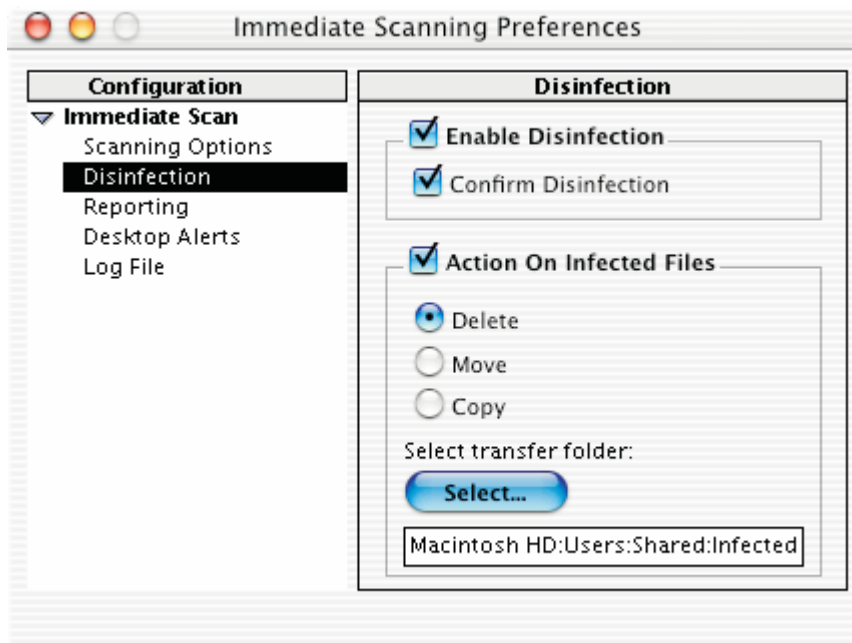
This section explains how to use Sophos Anti-Virus to perform disinfection. To do this, you run an on-demand scan with disinfection enabled.

? An **on-demand 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 **Preferences** button.



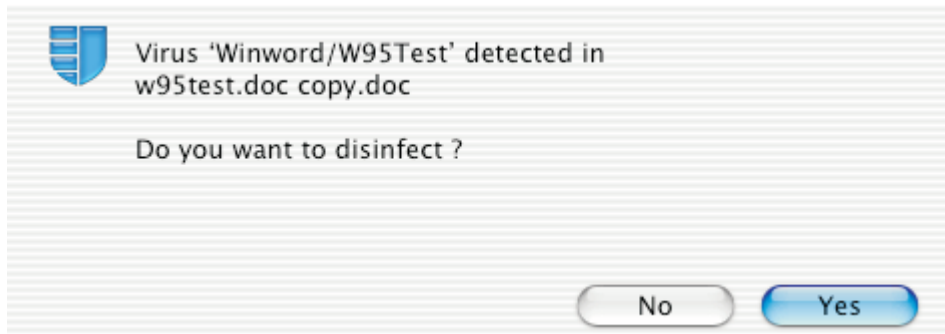
2. In the **Immediate Scanning Preferences** dialog box, on the **Immediate Scan** menu, click **Disinfection**. Select **Enable Disinfection**. Leave **Confirm Disinfection** selected. Close the dialog box.



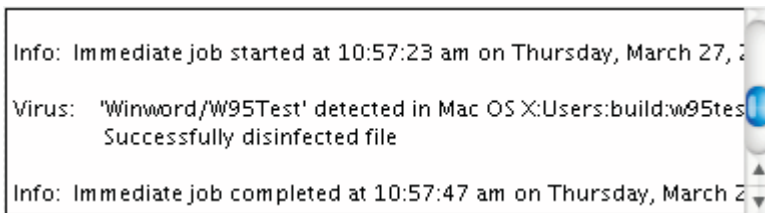
3. In the **Sophos Anti-Virus** window, click the **Start** button to start the scan.



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



5. When the scan has finished, click **Details** at the bottom of the **Sophos Anti-Virus** window to view the on-screen log.



If the log says that a file could not be disinfected, you should attempt to disinfect the file, 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.**

5 Uninstalling Sophos Anti-Virus

To remove Sophos Anti-Virus, you need to

- uninstall Sophos Anti-Virus on each workstation (section 5.1)
- remove the central installation manually (section 5.2)
- uninstall Update Manager on the server (section 5.3).

5.1 Uninstall Sophos Anti-Virus on workstations

1. Go to each Mac where you want to uninstall Sophos Anti-Virus. Browse to `/Library/Application Support/Sophos Anti-Virus` and double-click **Remove Sophos Anti-Virus.pkg**.
2. The uninstaller is run. Follow the instructions.

5.2 Remove the central installation

1. Go to the Mac server, or to the workstation from which you made the central installation. Locate the **Sophos Anti-Virus/ESOSX** folder on the volume where you made the central installation.
2. Drag and drop the folder into Trash (or select the folder and press `⌘-backspace`).

5.3 Uninstall Update Manager

1. Go to the Mac server, or to the workstation from which you made the central installation. Browse to `/Library/Application Support/Sophos Update Manager` and double-click **Remove Sophos Update Manager.pkg**.
2. The uninstaller is run. Follow the instructions.

Technical support

For technical support, visit

www.sophos.com/support

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

Copyright 2004–2007 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.