

# SOPHOS

## Sophos Endpoint Security and Control standalone startup guide

Sophos Anti-Virus for Windows, version 7  
Sophos Anti-Virus for Mac OS X, version 7

Document date: October 2009



# Contents

1 Before you begin.....	3
2 Protecting Windows computers.....	4
3 Protecting Mac OS X computers.....	11
4 Technical support.....	13
5 Copyright.....	14

# 1 Before you begin

## 1.1 System requirements

For system requirements, see the system requirements page of the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

In addition, you must have internet access to download the software from the Sophos website.

## 1.2 What information you will need

You will need the following information for installation and configuration:

- Web address and download credentials for the Sophos Endpoint Security and Control standalone installer and/or the Sophos Anti-Virus for Mac OS X standalone installer, as required
- Address of the update source, unless you will be updating from Sophos directly
- Credentials that are needed to access the update source
- Details of the proxy server that you may be using to access the update source (the address and port number, the user credentials)

## 2 Protecting Windows computers

### 2.1 Install Sophos Anti-Virus and Sophos Client Firewall

Log on as an administrator first.

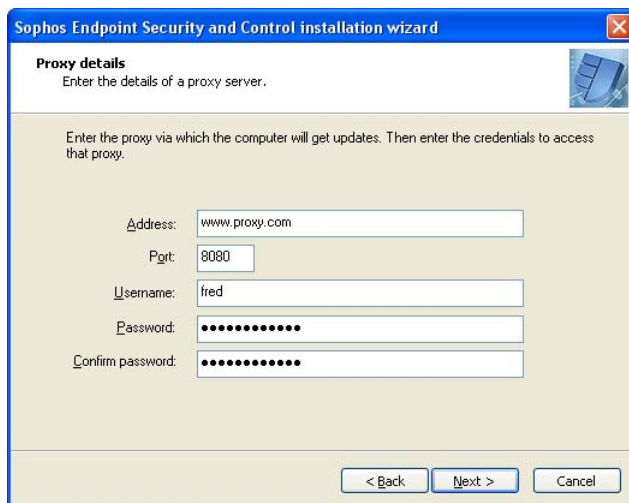
If you have third-party security software installed:

- Ensure that its user interface is closed.
  - Ensure that third-party firewall and HIPS software is turned off or configured to allow the Sophos installer to run.
1. Using the web address and download credentials provided by your system administrator, go to the Sophos website and download the standalone installer for your version of Windows.
  2. Locate the installer in the folder where it was downloaded. Double-click the installer. In the installer window, click **Install** to extract the installer's contents to your computer and start the installation wizard.
  3. On the first page of the **Sophos Endpoint Security and Control installation wizard**, click **Next**.
  4. On the **License Agreement** page, click **I accept the terms in the license agreement** if you agree to the terms and want to continue. Click **Next**.
  5. On the **Destination folder** page, if necessary, change the folder to which Sophos Anti-Virus will be installed. Click **Next**.
  6. On the **Update source** page, you enter the location from which the computer will get updates. Sophos recommends that you do this now.
    - a) In the **Address** box, specify the address of the update source by selecting **Sophos** or, if your system administrator has supplied you with an address, typing that address.
    - b) In the **Username** box, type the username that is needed to access the update source, which the system administrator has supplied.
    - c) In the **Password** and **Confirm password** boxes, type and confirm the password that is needed to access the update source, which the system administrator has supplied.
    - d) If you access the internet via a proxy, select the **Access the update source via a proxy** check box, click **Next** and go to step 7. Otherwise, click **Next** and go to step 8.



**Note:** To enter the update source later, select the **I will enter these details later** check box. Sophos Anti-Virus will not update itself until you enter these details. Go to step 8.

7. On the **Proxy details** page, specify the details of the proxy server.
  - a) In the **Address** box, type the address of the proxy server.
  - b) In the **Port** box, type the port number of the proxy server.
  - c) In the **Username** box, type the username that is needed to access the proxy server . If the username needs to be qualified to indicate the domain, use the form domain\username.
  - d) In the **Password** and **Confirm password** boxes, type and confirm the password that is needed to access the proxy server.
  - e) Click **Next**.



8. If you want to install Sophos Client Firewall, on the **Select additional components to install** page, select the **Install Sophos Client Firewall** check box. Click **Next**.
9. If you have third-party anti-virus or firewall software installed, on the **Remove third-party security software** page, make sure that the **Remove third-party security software** check box is selected. Click **Next**.
10. On the **Ready to install Sophos Endpoint Security and Control** page, click **Next**. You should see the software being installed on your computer.
11. If you need to restart your computer to complete the installation, on the last page, choose whether you want to do this now or later. Click **Finish**.

To enable Sophos Client Firewall, you must restart your computer.

If you chose to remove third-party security software, this is completed after you restart your computer.

**Important:** Third-party security software removal does not, by default, remove the associated update tools, because other third-party security software might still be using them. However, if they are not being used, you can remove them via Control Panel.

Installation of Sophos Anti-Virus is complete when the Sophos Anti-Virus system tray icon is blue.



If the icon is gray, this means that the on-access scanner is not running and your computer has no on-access protection against threats. For help contact your system administrator.

If you specified an update source from which Sophos Anti-Virus can update itself, it will do this automatically from the update source that you specified. By default, it will do this every 60 minutes, provided that the computer is connected to the internet. If a red circle with a white cross in it appears over the Sophos Anti-Virus system tray icon, Sophos Anti-Virus failed to update itself. For help, contact your system administrator.

If you installed Sophos Client Firewall, the Sophos Client Firewall system tray icon is displayed after you restart your computer.



The firewall is in “interactive” mode, which means that it displays a message when it detects an application or process that has not yet been authorized. In each case, you can block or allow the activity. This enables you to set up the firewall to your requirements.

If you did not specify an update source from which Sophos Anti-Virus can update itself, continue to [Configure Sophos Anti-Virus to update itself](#) (page 7).

Otherwise, if you installed Sophos Client Firewall, go straight to [Configure Sophos Client Firewall](#) (page 8).

## 2.2 Configure Sophos Anti-Virus to update itself

You only need to follow the instructions in this section if you did not specify an update source during installation.

Log on as an administrator.

1. In the system tray, right-click the Sophos Anti-Virus icon to display a menu. Select **Configure updating**.
2. In the **Properties for Sophos AutoUpdate** dialog box, click the **Primary server** tab.
  - a) In the **Address** box, specify the address of the update source by selecting **Sophos** or, if your system administrator has supplied you with an address, typing that address.
  - b) In the **User name** box, type the username that is needed to access the update source, which the system administrator has supplied.
  - c) In the **Password** and **Confirm password** boxes, type and confirm the password that is needed to access the update source, which the system administrator has supplied.
  - d) If you access the internet via a proxy, click **Apply**, and then click **Proxy Details** and go to step 3. Otherwise, go to step 4.



3. In the **Proxy details** dialog box, select the **Access the server via a proxy** check box.
  - a) In the **Address** box, type the address of the proxy server.
  - b) In the **Port** box, type the port number of the proxy server.
  - c) In the **User name** box, type the username that is needed to access the proxy server . If the username needs to be qualified to indicate the domain, use the form domain\username.
  - d) In the **Password** and **Confirm password** boxes, type and confirm the password that is needed to access the proxy server.
  - e) Click **OK**.



4. In the **Properties for Sophos AutoUpdate** dialog box, click **OK**.

Sophos Anti-Virus will update itself automatically from the update source that you specified. By default, it will do this every 60 minutes, provided that the computer is connected to the internet. If a red circle with a white cross in it appears over the Sophos Anti-Virus system tray icon, Sophos Anti-Virus failed to update itself. For help, contact your system administrator.

If you installed Sophos Client Firewall, continue to [Configure Sophos Client Firewall](#) (page 8).

## 2.3 Configure Sophos Client Firewall

You must configure the firewall to:

- Block unknown traffic.
- Allow traffic that is related to programs that you use to access the internet.

Then, you should switch the firewall to non-interactive mode to deal with traffic automatically according to this configuration.

### 2.3.1 Deal with firewall messages

The firewall displays a message when it is in interactive mode and it encounters unknown traffic. The message asks you whether to allow the traffic.

To get started, block the unknown traffic for just that occasion. For example, if the firewall displays a message about a hidden process, click **Block this process this time** and click **OK**.

There are some cases in which you should not block the traffic. These include the checksum and application rule messages that relate to your browser, email program, and other programs that you want to be able to access the internet.

### **2.3.2 Enable your browser to access the internet**

1. Open your browser. The firewall displays a message informing you that a new or modified application (in this case your browser) has requested network access. Click **Add the checksum to existing checksums for this application** and click **OK**.
2. The firewall displays a second message informing you that an application (your browser) has requested network access. Click **Create rule for this application using preset**, ensure that you have the default setting of **Browser** showing in the box, and click **OK**.

### **2.3.3 Enable your email program to access the internet**

1. Open your email program. The firewall displays a message informing you that a new or modified application (in this case your email program) has requested network access. Click **Add the checksum to existing checksums for this application** and click **OK**.
2. The firewall displays a second message informing you that an application (your email program) has requested network access. Click **Create rule for this application using preset**, ensure that you have the default setting of **Email Client** showing in the box, and click **OK**.

### **2.3.4 Enable other programs to access the internet**

You may need to enable other programs to access the internet, for example, Windows Update. To do this, the firewall must be in interactive mode. Follow the same procedure as in [Enable your browser to access the internet](#) (page 9).

To enable FTP download, see "Getting started" in the firewall Help or user manual.

### **2.3.5 Switch firewall to non-interactive mode**

When you have configured the firewall to deal with traffic that relates to particular programs as explained earlier, you should enable the firewall to deal with traffic automatically.

1. In the system tray, right-click the Sophos Client Firewall icon to display a menu. Select **Configure**.
2. In the **Sophos Client Firewall Configuration Editor** dialog box, click the **General** tab.
3. Click **Non-interactive** and click **OK**.

From now on, the firewall does not display a message when it encounters unknown traffic. Instead, it logs such traffic in its log. If the firewall detects unauthorized traffic, the firewall system tray icon turns red to indicate that there is an alert.

**Note:** You might sometimes need to switch back to interactive mode, for example, to run Windows Update. After running your chosen program, Sophos recommends that you switch back to non-interactive mode.

## **2.4 Clear Sophos Client Firewall alerts**

If the firewall detects unauthorized traffic, the firewall system tray icon turns red to indicate that there is an alert, and the blocked application's name is shown in the icon's ToolTip. To clear the alert, do as follows:

- ❖ In the system tray, right-click the Sophos Client Firewall icon to display a menu. Select **Clear Alert**.

The firewall icon turns blue to show that there are no alerts.

## 3 Protecting Mac OS X computers

### 3.1 Install Sophos Anti-Virus

You must uninstall any third-party anti-virus software before installing Sophos Anti-Virus.

Log in using an administrator account first.

1. Using the web address and download credentials provided by your administrator, go to the Sophos website and download the Sophos Anti-Virus standalone installer for Mac OS X.
2. Locate the installer disk image in the folder where it was downloaded. Open the disk image. Find Sophos Anti-Virus.mpkg and double-click it to start the Mac installer.
3. Click **Continue**. Follow the steps until installation is finished.

Installation of Sophos Anti-Virus is complete when the Sophos Anti-Virus icon on the right-hand side of the menu bar is black.



If the icon is gray, this means that the on-access scanner is not running and your computer has no on-access protection against threats. For help, contact your administrator.

### 3.2 Configure Sophos Anti-Virus to update

Ensure that you are logged in using an administrator account.

1. Click the Sophos Anti-Virus icon on the right-hand side of the menu bar, and then choose **Open Sophos Anti-Virus Preferences** from the shortcut menu.
2. Click **AutoUpdate**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Change the preferences as follows:
  - To enable Sophos Anti-Virus to update directly from Sophos, choose **Sophos** from the **Update from primary location** pop-up menu. In the **Username** and **Password** fields, type the updating credentials that were given to you by Sophos.
  - To enable Sophos Anti-Virus to update from your company web server, choose **Company web server** from the **Update from primary location** pop-up menu. In the **Address** field, type the web address of the location from which updates will be downloaded. In the **Username** and **Password** fields, type the updating credentials that are needed to access the server.

- To enable Sophos Anti-Virus to update from a network volume, choose **Network volume** from the **Update from primary location** pop-up menu. In the **Address** field, type the network address of the location from which updates will be downloaded. In the **Username** and **Password** fields, type the updating credentials that are needed to access the volume.

The following are examples of the address. Replace the text inside the brackets with the appropriate names:

`http://<server>/<web share>/Sophos Anti-Virus/ESCOSX`

`smb://<server>/<Samba share>/Sophos Anti-Virus/ESCOSX`

`afp://<server>/<AppleShare share>/Sophos Anti-Virus/ESCOSX`

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

5. To enable Sophos Anti-Virus to update via the proxy that has been set up in System Preferences, choose **Use system proxy settings** from the pop-up menu at the bottom of the **primary location** section.
6. To enable Sophos Anti-Virus to update via a proxy whose settings you specify:
  - a) Choose **Use custom proxy settings** from the pop-up menu at the bottom of the **primary location** section.
  - b) Click **Edit Settings**.
  - c) In the dialog box that appears, type the address and port number of the proxy in the **Address** fields. In the **Username** and **Password** fields, type the credentials that are needed to access the proxy.
7. Select **Check for updates on connection to network or internet**.

Sophos Anti-Virus will update automatically from the update source that you specified. By default, it will do this every 60 minutes, provided that the computer is connected to the internet. If a white cross is superimposed on the Sophos Anti-Virus icon on the right-hand side of the menu bar, Sophos Anti-Virus failed to update itself. For help, contact your administrator.

## 4 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

## **5 Copyright**

Copyright © 2008, 2009 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.