

Sophos Endpoint Security and Control standalone startup guide



Sophos Endpoint Security and Control for Windows, version 10.0
Sophos Anti-Virus for Mac OS X, version 8

Document date: April 2012



Contents

- 1 Before you begin.....3
- 2 Protecting Windows computers.....4
- 3 Protecting Mac OS X computers.....8
- 4 Technical support.....10
- 5 Legal notices.....11

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 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 Endpoint Security and Control

You must log on as an administrator to install Sophos Endpoint Security and Control.

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 supplied by Sophos or by your system administrator, go to the 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 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 Endpoint Security and Control will be installed. Click **Next**.
 6. On the **Update source** page, enter the location from which the computer will get updates. Sophos recommends that you do this now.
 - a) In the **Address** box, select **Sophos** or, if your system administrator has given you an address, enter that address.
 - b) In the **Username** and **Password** boxes, type the username and password that is needed to access the update source provided by Sophos or by your system administrator.
 - c) If you access the network or internet via a proxy, select the **Access the update source via a proxy** checkbox, click **Next** to enter the proxy details.

Note: To enter the update source later, select the **I will enter these details later** check box. After the installation is complete, open Sophos Endpoint Security and Control and select **Configure AutoUpdate**.

By default, Sophos Endpoint Security and Control will update itself every 60 minutes, provided the update source details are provided and the computer is connected to the network.

7. On the **Select additional components to install** page, select the **Install Sophos Client Firewall** check box if you want to install firewall and click **Next**.
8. On the **Remove third-party security software** page, select the **Remove third-party security software** check box if you have a third-party anti-virus or firewall software installed and click **Next**.

9. On the **Ready to install Sophos Endpoint Security and Control** page, click **Next**.

You should see the software being installed on 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.

10. On the last page of the install wizard, choose whether to restart the computer and click **Finish**.

You need to restart the computer:



- To enable the firewall.
- To complete the removal of third-party security software.

Installation of Sophos Endpoint Security and Control is complete when the Sophos Endpoint Security and Control icon is displayed in the Windows System Tray on the right of the taskbar.



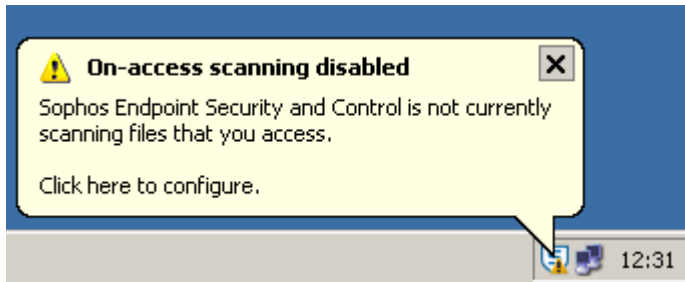
2.1.1 What do the system tray icons mean?

The Sophos Endpoint Security and Control system tray icon changes if there are pending alerts, or a problem with protection against threats. The following table displays the icons that are displayed in the system tray and the reasons it may be displayed.

Icon	Reason
	<ul style="list-style-type: none"> ■ When on-access scanning is not running on your computer. ■ When a firewall message is displayed. ■ When a controlled application message is displayed. ■ When a device control message is displayed. ■ When a data control message is displayed. ■ When a website is blocked.
	<ul style="list-style-type: none"> ■ When Sophos Endpoint Security and Control fails to update itself. ■ When a Sophos service has failed.

A balloon message appears along with one of the above mentioned icons explaining the cause.

For example, if on-access scanning is not enabled on your computer the **On-access scanning disabled** balloon message is displayed at the system tray as follows:



2.2 Configure the firewall

You must configure the firewall to:

- Deal with the firewall messages.
- Allow programs that you use to access the network or internet.
- Block unknown programs.

2.2.1 Deal with firewall messages

By default, 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.

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**.

If you are unable to block traffic for just that occasion, the application generating the traffic might not have been identified. In such a case, choose either allow or block, as appropriate. You can change it again later by editing the firewall configuration. For more information, see the Sophos Endpoint Security and Control Help.

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 network or internet.

2.2.2 Enable your programs to access the network or internet

You must enable the firewall to allow the programs that you want to access the network or internet.

1. Open the program for which you want to allow network or internet access, such as a browser or email program.

2. The firewall displays a message informing you that a new or modified application has requested network access. Click **Add the checksum to existing checksums for this application** and click **OK**.
3. The firewall displays a second message informing you that an application (such as your browser or email program) has requested network access. Click **Create rule for this application using preset**, and ensure you select the appropriate setting for the program (such as **Browser**, **Email Client**) in the box, and click **OK**.

You can also edit the firewall configuration to enable programs access the network or internet in any mode. For information, see the Sophos Endpoint Security and Control Help.

2.2.3 Enable other programs to access the network or internet

You may need to enable other programs to access the network or internet, for example, Windows Update. To do this, use the interactive mode and follow the same procedure as in [Enable your programs to access the network or internet](#) (page 6).

To enable FTP download, see the Sophos Endpoint Security and Control Help.

2.2.4 Block unknown programs

You should now enable the firewall to deal with traffic automatically and block unknown programs.

1. In the system tray, right-click the Sophos Endpoint Security and Control icon to display a menu. Select **Open Sophos Endpoint Security and Control**.
2. In the **Sophos Endpoint Security and Control** window, in the **Firewall** section, click **Configure firewall**.

The **Firewall configuration** dialog box is displayed.

3. In the **General** tab, under **Configuration**, click **Configure**.
4. In the location configuration dialog box, in the **Working mode** section, select **Block by default - all traffic which has no matching rule is blocked**.

From now on, the firewall does not display a message when it encounters unknown traffic. Instead, it logs such traffic in its log. To enable balloon messages when firewall detects unauthorized traffic, you must modify the firewall configuration. For more information, see Sophos Endpoint Security and Control Help.

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 later.

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 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 Mac 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 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 **User Name** 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 **User Name** 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 **User Name** 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. Also, depending on how the updates location has been set up, the folder ESCOSX might be ESOSX instead.

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) In the dialog box that appears, type the address and port number of the proxy in the **Address** fields. In the **User Name** 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 network. 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

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

5 Legal notices

Copyright © 2012 Sophos Limited. 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 license terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos, Sophos Anti-Virus and SafeGuard are registered trademarks of Sophos Limited, Sophos Group and Utimaco Safeware AG, as applicable. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.