

# SOPHOS

## Sophos Update Manager for Mac OS X Help

Product version: 2.5

Document date: May 2009



# Contents

|   |    |
|---|----|
| 1 About Sophos Update Manager.....                                | 3  |
| 2 Update the central installation from Sophos immediately.....    | 4  |
| 3 Configuring the central installation to update from Sophos..... | 5  |
| 4 View the central installation updating log.....                 | 7  |
| 5 Configuring Macs centrally.....                                 | 8  |
| 6 Solving problems.....   | 17 |
| 7 Technical support.....  | 18 |
| 8 Copyright.....  | 19 |

# 1 About Sophos Update Manager

Sophos Update Manager is software that enables you to:

- Update the Sophos Anti-Virus central installation on your Mac server with updates from Sophos
- Configure all the Macs on your network to update from the central installation and also, if necessary, directly from Sophos
- Configure Sophos Anti-Virus centrally for all your Macs

## **2 Update the central installation from Sophos immediately**

By default, Update Manager updates the central installation from Sophos every 10 minutes.

To update the central installation from Sophos immediately:

1. In the **Sophos Update Manager** window, click the **Software Update** toolbar icon.
2. In the **General** pane, click **Update Now**.

Update Manager checks Sophos for new software and, if necessary, updates the central installation.

## 3 Configuring the central installation to update from Sophos

### 3.1 Specify credentials to update from Sophos

To enable the central installation to update from Sophos, you must specify credentials to connect to Sophos.

To specify credentials to update from Sophos:

1. In the **Sophos Update Manager** window, click the **Software Update** toolbar icon.
2. In the **General** pane, in the **User Name** and **Password** fields, type the credentials that were given to you by Sophos for connecting to the Sophos website.
3. Click **Apply**.

### 3.2 Change the central installation location

1. In the **Sophos Update Manager** window, click the **Software Update** toolbar icon.
2. In the **General** pane, the field labeled “**Download updates to**” should contain the location that you specified during installation. Click **Choose** and enter the new location in the dialog box.
3. Click **Apply**.

### 3.3 Enable or disable central installation updating via a proxy

1. In the **Sophos Update Manager** window, click the **Software Update** toolbar icon.
2. In the **Proxy** pane, specify the preferences as follows:
  - To enable Update Manager to use the proxy settings that have been set up in System Preferences, choose **Use System Proxy Settings** from the pop-up menu.
  - To enable Update Manager to use the proxy settings that you enter in this pane, choose **Use Custom Proxy Settings** from the pop-up menu. In the **Address** field, type the address of the proxy. In the **User Name** and **Password** fields, type the credentials that are needed to access the proxy.
  - To disable updating via a proxy, choose **Do Not Use Proxy** from the pop-up menu.
3. Click **Apply**.

### 3.4 Schedule central installation updating

By default, Update Manager updates the central installation every 10 minutes.

To change the frequency of updates or to turn off scheduled updates:

1. In the **Sophos Update Manager** window, click the **Software Update** toolbar icon.

2. In the **General** pane, specify the preferences as follows:
  - To change the frequency of updates, change the value in the field that is labeled “**Check for updates from Sophos every**”, or choose a different unit of time from the pop-up menu.
  - To turn off scheduled updates, deselect the checkbox that is labeled “**Check for updates from Sophos every**”.
3. Click **Apply**.

### **3.5 Configure how central installation updating is logged**

By default, all activity related to updating of the central installation is logged in the Update Manager log.

To configure how central installation updating is logged:

1. In the **Sophos Update Manager** window, click the **Software Update** toolbar icon.
2. In the **Logging** pane, specify the preferences as follows:
  - To log all updating activity in the system log, select the checkbox labeled “**Log to system log**”.
  - To change the Update Manager log filename or location, click **Choose** and enter the new filename or location in the dialog box.
  - To disable logging in the Update Manager log, deselect the checkbox labeled “**Log to file**”.
3. Click **Apply**.

## **4 View the central installation updating log**

1. In the **Sophos Update Manager** window, click the **Software Update** toolbar icon.
2. In the **Logging** pane, click **View Log**.

The log is displayed in TextEdit.

## 5 Configuring Macs centrally

### 5.1 Configuring updating

#### 5.1.1 Specify the primary update source for Macs

The primary update source is the usual source from which the Macs on your network fetch Sophos Anti-Virus updates.

To specify the primary update source for Macs:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **AutoUpdate** pane, choose **Network Settings** from the pop-up menu.
3. In the **Network Settings** pane, click **Primary Server**.
4. In the **Primary Server** pane, change the preferences as follows:
  - To enable Sophos Anti-Virus to update directly from Sophos, choose **Sophos** from the **Update From** 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** pop-up menu. In the **Address** field, type the web address of the central installation. 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** pop-up menu. In the **Address** field, type the network address of the central installation. 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 to refer to the server. Using an IP address can be better if you have any DNS problems.

5. Click **Apply**.

If Sophos Anti-Virus must access the update source via a proxy, see [Enable or disable updating of Macs via a proxy](#) (page 9).

## 5.1.2 Specify the secondary update source for Macs

If the Macs on your network cannot contact the primary update source for Sophos Anti-Virus updates, they can try to contact a secondary source.

To specify the secondary update source for Macs:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **AutoUpdate** pane, from the pop-up menu choose **Network Settings**.
3. In the **Network Settings** pane, click **Secondary Server**.
4. In the **Secondary Server** pane, make sure that the checkbox labeled “**Use secondary server**” is selected. Then, change the preferences as follows:
  - To enable Sophos Anti-Virus to update directly from Sophos, choose **Sophos** from the **Update From** 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** pop-up menu. In the **Address** field, type the web address of the central installation. 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** pop-up menu. In the **Address** field, type the network address of the central installation. 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 to refer to the server. Using an IP address can be better if you have any DNS problems.

5. Click **Apply**.

If Sophos Anti-Virus must access the update source via a proxy, see [Enable or disable updating of Macs via a proxy](#) (page 9).

## 5.1.3 Enable or disable updating of Macs via a proxy

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **AutoUpdate** pane, choose **Network Settings** from the pop-up menu.
3. In the **Network Settings** pane, click **Primary Proxy** or **Secondary Proxy** as required.

4. In the **Primary Proxy** pane or **Secondary Proxy** pane, change the preferences as follows:
  - To enable Sophos Anti-Virus to use the proxy settings that have been set up in System Preferences, choose **Use System Proxy Settings** from the pop-up menu.
  - To enable Sophos Anti-Virus to use the proxy settings that you enter in this pane, choose **Use Custom Proxy Settings** from the pop-up menu. In the **Address** field, type the address of the proxy. In the **User Name** and **Password** fields, type the credentials that are needed to access the proxy.
  - To disable updating via a proxy, choose **Do Not Use Proxy** from the pop-up menu.
5. Click **Apply**.

#### 5.1.4 Schedule updating of Macs

By default, the installations of Sophos Anti-Virus on your Macs update themselves every hour.

To change when or how often Sophos Anti-Virus updates itself:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **AutoUpdate** pane, choose **Schedule and Logging** from the pop-up menu.
3. In the group box labeled “**Check for updates**”, change the preferences as follows:
  - To enable Sophos Anti-Virus to update itself at regular intervals, select the **Every** checkbox and enter the time period.
  - To enable Sophos Anti-Virus to update itself every time that a network connection is established, select the checkbox labeled “**When connection is made to network or internet**”.
4. Click **Apply**.

#### 5.1.5 Configure how updating of Macs is logged

By default, all activity related to updating of a particular Mac is logged in the AutoUpdate log on that Mac.

To configure how updating of Macs is logged:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **AutoUpdate** pane, choose **Schedule and Logging** from the pop-up menu.
3. In the **Logging** group box, change the preferences as follows:
  - To log all updating activity in the system log, select the checkbox labeled “**Log to system log**”.
  - To change the AutoUpdate log filename or location, click **Choose** and enter the new filename or location in the dialog box.
  - To disable logging in the AutoUpdate log, deselect the checkbox labeled “**Log to file**”.
4. Click **Apply**.

## 5.2 Enable or disable on-access scanning

By default, on-access scanning is enabled automatically when your Macs are started.

To enable or disable on-access scanning:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **General** from the pop-up menu.
3. In the **General** pane, change the setting as follows:
  - To *enable* on-access scanning, select the checkbox labeled “**Enable on-access scanning**” and click **Apply**.
  - To *disable* on-access scanning, deselect the checkbox labeled “**Enable on-access scanning**” and click **Apply**.

**Important:** If you disable on-access scanning, Sophos Anti-Virus does not scan for threats any files that you access. This puts your Macs at risk.

## 5.3 Configuring on-access scanning

### 5.3.1 Add an on-access exclusion

You can exclude files, folders, and volumes from on-access scanning.

To add an on-access exclusion:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **Exclusions** from the pop-up menu.
3. Do one of the following:
  - Drag the item(s) to be excluded to the list of excluded items.
  - Click **Add (+)** and choose the item(s) to be excluded from the dialog box.
4. Click **Apply**.

### 5.3.2 Edit an on-access exclusion

You can exclude files, folders, and volumes from on-access scanning.

To edit an on-access exclusion:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **Exclusions** from the pop-up menu.

3. In the list of excluded items, double-click an item and edit the item.  
For information about specifying which items are excluded, see [Exclusion rules](#) (page 12).
4. Click **Apply**.

### 5.3.3 Exclusion rules

When you add or edit an exclusion, you can type any POSIX path, whether it is a volume, folder, or file. To specify which items are excluded, use the following rules:

| Item(s) to exclude                                  | Syntax to use   |
|---|---|
| A folder and sub-folders recursively                | Suffix the exclusion with a slash                               |
| A folder but not sub-folders                        | Suffix the exclusion with a double slash                        |
| A file  | Do <i>not</i> suffix the exclusion with a slash or double slash |
| A folder or file in a specific location             | Prefix the exclusion with a slash                               |
| A folder or file anywhere locally or on the network | Do <i>not</i> prefix the exclusion with a slash                 |
| A file whose name has a specific filename extension | Substitute an asterisk (*) for the filename stem                |

#### Examples

| Exclusion path          | Item(s) that are excluded   |
|-------------------------|---|
| /MyFolder/MyApplication | The file MyApplication in a specific location   |
| /MyFolder/              | All files in the folder MyFolder in a specific location and sub-folders recursively                     |
| /MyFolder//             | All files in the folder MyFolder in a specific location but not sub-folders                             |
| MyFolder/MyApplication  | The file MyApplication in any folder that is called MyFolder, locally or on the network                 |
| MyFolder/               | All files in any folder that is called MyFolder, locally or on the network, and sub-folders recursively |
| MyFolder//              | All files in any folder that is called MyFolder, locally or on the network, but not sub-folders         |

| Exclusion path  | Item(s) that are excluded   |
|-----------------|---|
| MyApplication   | The file MyApplication anywhere locally or on the network                     |
| *.mov           | All files whose filename extension is .mov anywhere locally or on the network |
| /MyFolder/*.mov | All files whose filename extension is .mov in a specific location             |

### 5.3.4 Delete an on-access exclusion

You can exclude files, folders, and volumes from on-access scanning.

To delete an on-access exclusion:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **Exclusions** from the pop-up menu.
3. In the list of excluded items, select the exclusion that you want to delete and click **Delete (-)**.
4. Click **Apply**.

### 5.3.5 Enable on-access scanning inside archives and compressed files

By default, scanning inside archives and compressed files is disabled because it makes scanning significantly slower and is generally not required. Even if you do not enable the option, files that are compressed with dynamic compression utilities (PKLite, LZEXE, and Diet) are scanned, and when you attempt to access a file extracted from an archive, the extracted file is scanned.

However, you might want to enable the option so that the contents of an archive or compressed file are scanned before it is downloaded or emailed from one of your Macs.

To enable on-access scanning inside archives and compressed files:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **General** from the pop-up menu.
3. In the **General** pane, select the checkbox labeled “**Scan inside archives and compressed files**”.
4. Click **Apply**.

### 5.3.6 Disable on-access scanning of network volumes

By default, scanning of files that you access on network volumes is enabled.

To disable on-access scanning of network volumes:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **General** from the pop-up menu.
3. In the **General** pane, deselect the checkbox labeled “**Scan network volumes**”.
4. Click **Apply**.

### 5.3.7 Disable desktop alerts

By default, Sophos Anti-Virus displays a desktop alert if it detects a threat during on-access scanning.

To disable desktop alerts:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **Desktop Alerts** from the pop-up menu.
3. In the **Desktop Alerts** pane, deselect the checkbox labeled “**Enable desktop alerts**”.
4. Click **Apply**.

### 5.3.8 Configure how on-access scanning is logged

By default, all on-access scanning activity, including viruses/spyware found, is logged in the Sophos Anti-Virus log.

To configure how on-access scanning is logged:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **Logging** from the pop-up menu.
3. In the **Logging** pane, change the preferences as follows:
  - To log all on-access scanning activity in the system log, select the checkbox labeled “**Log to system log**”.
  - To change the Sophos Anti-Virus log filename or location, click **Choose** and enter the new filename or location in the dialog box.
  - To disable logging in the Sophos Anti-Virus log, deselect the checkbox labeled “**Log to file**”.
4. Click **Apply**.

## 5.4 Cleaning up

### 5.4.1 About cleanup

Cleanup eliminates threats on your Macs by removing a virus from a file, or moving or deleting the infected file. However, it does not undo any actions the threat has already taken.

## 5.4.2 Get cleanup information

When a threat is found on one of your Macs, it is very important that you check the threat analysis on the Sophos website for information on the threat and cleanup advice.

- ❖ To view the threat analysis, go to <http://www.sophos.com/security/analyses/viruses-and-spyware/> and search for the threat name that is shown in the Sophos Anti-Virus log, desktop alert, or email notification.

## 5.4.3 Configure cleanup for on-access scanning

When on-access scanning is enabled, Sophos Anti-Virus can automatically disinfect many infected items or make infected items safe in ways other than disinfection.

To configure cleanup for on-access scanning:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. At the top of the **Scanning** pane, choose **Cleanup** from the pop-up menu.
3. In the **Cleanup** pane, change the preferences as follows:
  - To enable automatic disinfection of infected files, select the checkbox labeled “**Automatically clean up items that contain viruses or spyware**”.
  - To move infected files to another location to prevent them being run, select the checkbox labeled “**and move to folder**”. By default, the files are moved to /Users/Shared/Infected/. To choose a different location, click **Choose**, and enter the location in the dialog box.
  - To delete infected files, select the button labeled “**delete infected files**”.
4. Click **Apply**.

Any actions that Sophos Anti-Virus takes against infected items are logged in the Sophos Anti-Virus log.

## 5.5 Configure email notification

Sophos Anti-Virus can send an email if it detects a threat or an error occurs. By default, email notification is disabled.

To configure email notification:

1. In the **Sophos Update Manager** window, click the **SAV Preferences** toolbar icon.
2. In the **Notification** pane, make sure that the checkbox labeled “**Enable email notification**” is selected.
3. Change the preferences as follows:
  - To enable Sophos Anti-Virus to send an email notification only if it finds a threat, select **Report threats**.

- To enable Sophos Anti-Virus to send an email notification if it finds a threat or there is an error, select **Report threats and errors**.
- To specify the email address *to* which email notifications should be sent, type the address in the **Recipient** field.
- To specify the email address *from* which email notifications should be sent, type the address in the **Sender** field.
- To specify the address of the email server from which email notifications should be sent, type the address in the **Outgoing Mail Server** field.

4. Click **Apply**.

## 5.6 Restore default preferences

- ❖ To restore the default preferences for on-access scanning, cleanup, and email notification, in the **Sophos Update Manager** window, click **Restore Defaults**.

**Note:** The button is displayed only when the **Scanning** pane or the **Notification** pane is selected.

## 6 Solving problems

### 6.1 The central installation does not get updated

#### Symptoms

Update Manager does not attempt to update the central installation or is unable to do so.

#### Causes

To find out why this is happening, view the updating log. For information, see [View the central installation updating log](#) (page 7).

#### Resolve the problem

- If Update Manager is providing the wrong credentials to update from Sophos, see [Specify credentials to update from Sophos](#) (page 5). Check that the credentials are correct.
- If Update Manager is updating a different central installation to what you expect, see [Change the central installation location](#) (page 5). Check that the location is correct.
- If Update Manager cannot use your proxy server, see [Enable or disable central installation updating via a proxy](#) (page 5). Check that the settings are correct.
- If Update Manager is not attempting to update the central installation when you expect it to, see [Schedule central installation updating](#) (page 5). Check that the settings are correct.

### 6.2 Update Now button is dimmed

#### Symptoms

The Update Now button is dimmed in the **General** pane.

#### Causes

The central installation is not configured to update from Sophos.

#### Resolve the problem

See [Configuring the central installation to update from Sophos](#) (page 5).

## **7 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

## **8 Copyright**

Copyright © 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.