



Sophos Anti-Virus for Mac OS X Help

For networked and single computers running Mac OS X version 10.4 or later

Product version: 7

Document date: October 2009



Contents

| | |
|--|----|
| 1 About Sophos Anti-Virus..... | 3 |
| 2 On-access scanning..... | 4 |
| 3 The default scan of this Mac..... | 10 |
| 4 Custom scans..... | 11 |
| 5 Finder item scans..... | 16 |
| 6 Configure email alerts..... | 18 |
| 7 Updating..... | 19 |
| 8 Dealing with threats..... | 24 |
| 9 Restoring default preferences..... | 31 |
| 10 Use Sophos Anti-Virus via Terminal..... | 33 |
| 11 Solving problems..... | 34 |
| 12 Technical support..... | 37 |
| 13 Copyright..... | 38 |

1 About Sophos Anti-Virus

Sophos Anti-Virus for Mac OS X, version 7 is software that detects and deals with threats (viruses, worms, Trojans, and spyware) on your Mac or network.

On-access scanning is your main method of protection against threats. Whenever you access (copy, save, move, or open) a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your Mac.

In addition to on-access scanning, Sophos Anti-Virus supplies several types of **on-demand scan** to provide additional protection. An on-demand scan is a scan that you initiate. You can scan anything from a single file to everything on your Mac that you have permission to read:

- **Default scan of this Mac**

Scan all files on local volumes that you have permission to read. Any removable storage devices that are inserted are included.

- **Custom scans**

Scan specific sets of files, folders, or volumes.

- **Finder item scans**

Scan a file, folder, or volume that you have selected in Finder.

2 On-access scanning

On-access scanning is your main method of protection against threats. Whenever you access (copy, save, move, or open) a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your Mac.

2.1 Enable or disable on-access scanning

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

By default, on-access scanning is enabled automatically when you start your Mac.

To enable or disable on-access scanning:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Change the setting as follows:
 - To *enable* on-access scanning, click **Start Scanning**. The status changes to **On** and the Sophos Anti-Virus icon in the menu bar turns black.



- To *disable* on-access scanning, click **Stop Scanning**. The status changes to **Off** and the Sophos Anti-Virus icon in the menu bar turns gray.



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

2.2 Configuring on-access scanning

2.2.1 Add an on-access exclusion

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

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

To add an on-access exclusion:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Excluded Items**.
5. 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.

2.2.2 Edit an on-access exclusion

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

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

To edit an on-access exclusion:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Excluded Items**.
5. 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 5).

2.2.3 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 |
| 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 |

2.2.4 Delete an on-access exclusion

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

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

To delete an on-access exclusion:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Excluded Items**.
5. In the list of excluded items, select the exclusion that you want to delete and click **Delete (-)**.

2.2.5 Enable on-access scanning inside archives and compressed files

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

Note: Sophos recommends that you do not enable this option, for the following reasons:

- Scanning inside archives and compressed files makes scanning significantly slower.
- Whether you enable this option or not, when you open a file extracted from an archive, the extracted file is scanned.
- Whether you enable this option or not, files compressed with dynamic compression utilities (PKLite, LZEXE and Diet) are 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 your Mac.

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

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Options**.
5. Select “**Inside archives and compressed files**”.

2.2.6 Enable on-access scanning of files on network volumes

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

By default, scanning of files that you access on network volumes is disabled because it can slow down access.

To enable on-access scanning of files on network volumes:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Options**.
5. Select “**Files on network volumes**”.

2.2.7 Configure desktop alerts

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

Sophos Anti-Virus displays a desktop alert if a serious error occurs during on-access scanning. By default, it also displays a desktop alert if it detects a threat during on-access scanning. You can configure the desktop alerts that are displayed when a threat is detected.

To configure desktop alerts:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **Messaging**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Change the preferences as follows:
 - To specify an additional message to be displayed in desktop alerts about threats, type the message in the “**Add custom message**” field.
 - To disable desktop alerts about threats, deselect “**Display a desktop alert when a threat is detected on access**”.

2.2.8 Change logging preferences

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

All on-access scanning activity, including threats detected, and all updating activity is logged in the on-access scanning and updating log. Sophos Anti-Virus can also log such activity in the system log.

To change the logging preferences for on-access scanning and updating:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **Logging**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.

4. Change the preferences as follows:

- To change the log filename or location, click **Choose File** and enter the new filename or location in the dialog.
- To delete all entries from the log, click **Clear Log**.
- To log all on-access scanning and updating activity in the system log, select “**Log events to system log**”.

2.3 View on-access scanning and updating log

To view the log of all on-access scanning activity, including threats detected, and all updating activity:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **Logging** pane, click **View Log**.

The log is displayed in Console. At the start of each log entry, there is a tag to show whether the entry was logged by the on-access scanner (com.sophos.intercheck) or AutoUpdate (com.sophos.autoupdate).

3 The default scan of this Mac

The default scan of this Mac is a scan of all files on local volumes that you have permission to read. Any removable storage devices that are inserted are included.

3.1 Scan this Mac

- ❖ To scan all files on local volumes that you have permission to read, choose **Scan > Scan This Mac**.

Sophos Anti-Virus displays the progress of the scan in the main Sophos Anti-Virus window.

Note: You can also run the scan in one of the following ways:

- In the main Sophos Anti-Virus window, click **Scan This Mac**.
- Click the Sophos Anti-Virus icon on the right-hand side of the menu bar, and then choose **Scan This Mac** from the shortcut menu.
- Control-click the Sophos Anti-Virus application icon in the Dock, and then choose **Scan This Mac** from the shortcut menu.

3.2 Disable scanning inside archives and compressed files for the default scan of this Mac

By default, scanning inside archives and compressed files is enabled for the default scan of this Mac.

To disable scanning inside archives and compressed files for the default scan of this Mac:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **On-demand Scanning** pane, deselect “**Scan inside archives and compressed files**”.

Note: The setting of this option applies to both the default scan of this Mac and Finder item scans.

3.3 View log of the default scan of this Mac

1. If the main Sophos Anti-Virus window is not open, choose **Window > Sophos Anti-Virus** to open it.
2. In the main Sophos Anti-Virus window, click **View Scan Log**.

The log is displayed in Console.

4 Custom scans

A custom scan is a scan of specific sets of files, folders, or volumes.

4.1 Run a custom scan

1. If the main Sophos Anti-Virus window is not open, choose **Window > Sophos Anti-Virus** to open it.
2. If the **Custom Scans** list is not displayed, click the disclosure triangle next to **Custom Scans**.
3. In the **Custom Scans** list, select the scan that you want to run.
4. Click **Start Scan**.

Sophos Anti-Virus displays the progress of the scan in the main Sophos Anti-Virus window.

Note: You can also run a scan when you are editing it by clicking **Start Scan** in the scan editor.

4.2 Add a custom scan

1. Choose **File > New**.
2. In the scan editor that is displayed, edit the scan as follows:
 - To rename the scan, in the **Scan Name** field, type the new name.
 - To specify what to scan, see [Specify what to scan](#) (page 12).
 - To specify what not to scan, see [Add a custom scan exclusion](#) (page 13), [Edit a custom scan exclusion](#) (page 13), or [Delete a custom scan exclusion](#) (page 14) as appropriate.
 - To disable scanning inside archives and compressed files, see [Disable scanning inside archives and compressed files for a custom scan](#) (page 15).

The scan is added to the **Custom Scans** list in the main Sophos Anti-Virus window.

Note: You can also add a scan by clicking **Add (+)** at the bottom of the main Sophos Anti-Virus window.

4.3 Copy a custom scan

1. If the main Sophos Anti-Virus window is not open, choose **Window > Sophos Anti-Virus** to open it.
2. If the **Custom Scans** list is not displayed, click the disclosure triangle next to **Custom Scans**.
3. In the **Custom Scans** list, select the scan that you want to copy.
4. Choose **File > Duplicate**.

5. In the scan editor that is displayed, edit the scan as follows:

- To rename the scan, in the **Scan Name** field, type the new name.
- To specify what to scan, see [Specify what to scan](#) (page 12).
- To specify what not to scan, see [Add a custom scan exclusion](#) (page 13), [Edit a custom scan exclusion](#) (page 13), or [Delete a custom scan exclusion](#) (page 14) as appropriate.
- To disable scanning inside archives and compressed files, see [Disable scanning inside archives and compressed files for a custom scan](#) (page 15).

The scan is added to the **Custom Scans** list in the main Sophos Anti-Virus window.

Note: You can also copy a selected scan in the main Sophos Anti-Virus window in one of the following ways:

- Press Command-D.
- At the bottom of the window, choose **Duplicate** from the Action pop-up menu.

4.4 Editing a custom scan

4.4.1 Open the custom scan editor

1. If the main Sophos Anti-Virus window is not open, choose **Window > Sophos Anti-Virus** to open it.
2. If the **Custom Scans** list is not displayed, click the disclosure triangle next to **Custom Scans**.
3. In the **Custom Scans** list, double-click the scan that you want to edit.

Note: You can also open the editor by selecting the scan that you want to edit, and choosing **Edit Scan** from the Action pop-up menu at the bottom of the window.

4.4.2 Rename a custom scan

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the scan editor, in the **Scan Name** field, type the new name.

4.4.3 Specify what to scan

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the **Scan Items** pane, do one of the following:
 - Drag the item(s) to be scanned to the list of items to scan.
 - Click **Add (+)** and choose the item(s) to be scanned from the dialog.

Note: If you do not have sufficient privileges to see the contents of a folder that you add, Sophos Anti-Virus displays the folder with a No Access symbol and does not scan it.

4.4.4 Add a custom scan exclusion

You can exclude files, folders, and volumes from a custom scan.

To add a custom scan exclusion:

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the **Excluded Items** pane, 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.

4.4.5 Edit a custom scan exclusion

You can exclude files, folders, and volumes from a custom scan.

To edit a custom scan exclusion:

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the **Excluded Items** pane, double-click an item and edit the item.
For information about specifying which items are excluded, see [Exclusion rules](#) (page 13).

4.4.6 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 |

| Item(s) to exclude | Syntax to use |
|---|--|
| 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 |
| 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 |

4.4.7 Delete a custom scan exclusion

You can exclude files, folders, and volumes from a custom scan.

To delete a custom scan exclusion:

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the **Excluded Items** pane, select the item that you want to delete and click **Delete (-)**.

4.4.8 Disable scanning inside archives and compressed files for a custom scan

By default, scanning inside archives and compressed files is enabled.

To disable scanning inside archives and compressed files for a custom scan:

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the **Options** pane, deselect “**Inside archives and compressed files**”.

4.5 Delete a custom scan

1. If the main Sophos Anti-Virus window is not open, choose **Window > Sophos Anti-Virus** to open it.
2. If the **Custom Scans** list is not displayed, click the disclosure triangle next to **Custom Scans**.
3. In the **Custom Scans** list, select the scan that you want to delete.
4. Click **Delete (-)**.

4.6 View a custom scan log

1. If the main Sophos Anti-Virus window is not open, choose **Window > Sophos Anti-Virus** to open it.
2. If the **Custom Scans** list is not displayed, click the disclosure triangle next to **Custom Scans**.
3. In the **Custom Scans** list, select the scan for which you want to view the log.
4. At the bottom of the window, choose **View Scan Log** from the Action pop-up menu.

The log is displayed in Console.

Note: You can also view a custom scan log when you are editing a custom scan by clicking **View Scan Log** in the scan editor.

5 Finder item scans

A Finder item scan is a scan of a file, folder, or volume that you have selected in Finder.

5.1 Run a Finder item scan from a shortcut menu

1. In Finder, select the file, folder, or volume that you want to scan.
You can select more than one item.
2. Control-click the selection, and then do one of the following:
 - On Mac OS X version 10.5, choose **More** > “**Scan with Sophos Anti-Virus**” from the shortcut menu.
 - On other Mac OS X versions, choose “**Scan with Sophos Anti-Virus**” from the shortcut menu.

Sophos Anti-Virus displays the progress of the scan in a dialog.

5.2 Run a Finder item scan by dragging an item to the Dock icon

1. In Finder, select the file, folder, or volume that you want to scan.
You can select more than one item.
2. Drag the selection to the Sophos Anti-Virus application icon in the Dock.
Sophos Anti-Virus displays the progress of the scan in a dialog.

5.3 Run a Finder item scan from the Services submenu

1. On Mac OS X version 10.6, in Finder, select the file, folder, or volume that you want to scan.
You can select more than one item.
2. Choose **Finder** > **Services** > “**Scan with Sophos Anti-Virus**”.
Sophos Anti-Virus displays the progress of the scan in a dialog.

5.4 Disable scanning inside archives and compressed files for a Finder item scan

By default, scanning inside archives and compressed files is enabled for a Finder item scan.

To disable scanning inside archives and compressed files for a Finder item scan:

1. Choose **Sophos Anti-Virus** > **Preferences**.

2. In the **On-demand Scanning** pane, deselect “**Scan inside archives and compressed files**”.

Note: The setting of this option applies to both the default scan of this Mac and Finder item scans.

5.5 View a Finder item scan log

- ❖ In the progress dialog that is displayed when you run a Finder item scan, click **View Scan Log**.

The log is displayed in Console.

6 Configure email alerts

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

Sophos Anti-Virus can send an email if it detects a threat or a serious error occurs. This applies to on-access scanning, the default scan of this Mac, custom scans, and Finder item scans. By default, email alerts are disabled.

To configure email alerts:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **Messaging**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Select “**Send an email alert when a threat is detected or an error occurs**”.
5. Change the preferences as follows:
 - To enable Sophos Anti-Virus to send an email alert only if it detects a threat, select **Threats**.
 - To enable Sophos Anti-Virus to send an email alert if it detects a threat or a serious error occurs, select “**Threats and errors**”.
 - To specify the email address *to* which email alerts should be sent, type the address in the **Recipient** field.
 - To specify the address of the email server from which email alerts should be sent, type the address in the **Outgoing Email Server** field.
 - To specify the email address *from* which email alerts should be sent, type the address in the **Sender** field.

7 Updating

7.1 Update Sophos Anti-Virus immediately

By default, Sophos Anti-Virus updates every hour. However, you can update it immediately.

To update Sophos Anti-Virus immediately, do one of the following:

- ❖ Choose **Sophos Anti-Virus > Update Now**.
- ❖ Click the Sophos Anti-Virus icon on the right-hand side of the menu bar, and then choose **Update Now** from the shortcut menu.
- ❖ Control-click the Sophos Anti-Virus application icon in the Dock, and then choose **Update Now** from the shortcut menu.

7.2 Configuring updating

7.2.1 Set a source for updates

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

To specify where Sophos Anti-Virus downloads updates from:

1. Choose **Sophos Anti-Virus > Preferences**.
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.

If Sophos Anti-Virus must access the update source via the proxy that has been set up in System Preferences, see [Enable updating via the system proxy](#) (page 21). If Sophos Anti-Virus must access the update source via another proxy, see [Enable updating via a custom proxy](#) (page 21).

7.2.2 Set an alternative source for updates

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

To specify where Sophos Anti-Virus downloads updates from if it cannot contact its usual source:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **AutoUpdate**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Select “**Use a secondary location**”. Then, change the preferences as follows:
 - To enable Sophos Anti-Virus to update directly from Sophos, choose **Sophos** from the “**Update from secondary 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 secondary 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 secondary 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.

If Sophos Anti-Virus must access the update source via the proxy that has been set up in System Preferences, see [Enable updating via the system proxy](#) (page 21). If Sophos Anti-Virus must access the update source via another proxy, see [Enable updating via a custom proxy](#) (page 21).

7.2.3 Enable updating via the system proxy

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

You can specify that you want Sophos Anti-Virus to update via the proxy that has been set up in System Preferences.

To enable updating via the system proxy:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **AutoUpdate**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Choose “**Use system proxy settings**” from the pop-up menu at the bottom of the “**primary location**” section or the “**secondary location**” section, as required.

7.2.4 Enable updating via a custom proxy

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

You can specify the settings of a proxy via which you want Sophos Anti-Virus to update.

To enable updating via a custom proxy:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **AutoUpdate**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Choose “**Use custom proxy settings**” from the pop-up menu at the bottom of the “**primary location**” section or the “**secondary location**” section, as required.
5. Click **Edit Settings**.
6. In the dialog 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.

7.2.5 Schedule updates

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

By default, Sophos Anti-Virus updates every hour. However, you can change when or how often it updates.

To schedule updates:

1. Choose **Sophos Anti-Virus > Preferences**.
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 at regular intervals, select “**Check for updates every**” and enter the time period.
 - To enable Sophos Anti-Virus to update every time that a network connection is established, select “**Check for updates on connection to network or internet**”.

7.2.6 Change logging preferences

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

All on-access scanning activity, including threats detected, and all updating activity is logged in the on-access scanning and updating log. Sophos Anti-Virus can also log such activity in the system log.

To change the logging preferences for on-access scanning and updating:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **Logging**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Change the preferences as follows:
 - To change the log filename or location, click **Choose File** and enter the new filename or location in the dialog.
 - To delete all entries from the log, click **Clear Log**.
 - To log all on-access scanning and updating activity in the system log, select “**Log events to system log**”.

7.3 Check the progress of an update

- ❖ To check the progress of an update that was started by you or scheduled, click the Sophos Anti-Virus icon on the right-hand side of the menu bar, and then choose **Show AutoUpdate Window** from the shortcut menu.

Note: To view a log of all updating activity, see [View on-access scanning and updating log](#) (page 23).

7.4 View on-access scanning and updating log

To view the log of all on-access scanning activity, including threats detected, and all updating activity:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **Logging** pane, click **View Log**.

The log is displayed in Console. At the start of each log entry, there is a tag to show whether the entry was logged by the on-access scanner (`com.sophos.intercheck`) or AutoUpdate (`com.sophos.autoupdate`).

8 Dealing with threats

8.1 About dealing with threats

When a threat is found on your Mac, get information about the threat from the Sophos website (see [Get threat information](#) (page 24)).

The information might tell you to deal with the threat by running a default scan of this Mac with one of the following options enabled:

- [Clean up infected files \(the default scan of this Mac\)](#) (page 24)
- [Move infected files \(the default scan of this Mac\)](#) (page 25)
- [Delete infected files \(the default scan of this Mac\)](#) (page 25)

Important: Dealing with the threat does not undo any actions the threat has already taken.

8.2 Get threat information

When a threat is found on your Mac, it is very important that you check the threat analysis on the Sophos website for information about the threat and advice about dealing with it.

- ❖ To get threat information, 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.

8.3 Dealing with threats detected by the default scan of this Mac

8.3.1 Clean up infected files (the default scan of this Mac)

You can configure Sophos Anti-Virus to remove viruses from infected files, if the default scan of this Mac detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To clean up infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **On-demand Scanning** pane, choose “**Clean up infected files**” from the “**When a threat is found**” pop-up menu.
3. From the “**If cleanup fails**” pop-up menu, choose what action Sophos Anti-Virus should take if cleanup fails:
 - To take no action, choose “**Alert only**”. However, if you have enabled email alerts, Sophos Anti-Virus sends an email alert.

- To delete infected files, choose “**Delete infected files**”.
- To move infected files to another folder to prevent them being run, choose “**Move infected files**”.

By default, the files are moved to /Users/Shared/Infected/. To choose a different folder, click **Choose Folder**, and enter the folder in the dialog.

Any actions that Sophos Anti-Virus takes against infected files are logged in the log of the Finder item scan.

Important: Cleaning up infected documents does not repair any changes the virus has made to the document. Cleaning up infected programs should be used only as a temporary measure. You should subsequently replace cleaned programs from the original disks or a clean backup.

Note: The setting of this option applies to both the default scan of this Mac and Finder item scans.

8.3.2 Move infected files (the default scan of this Mac)

You can configure Sophos Anti-Virus to move infected files to another folder to prevent them being run, if the default scan of this Mac detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To move infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **On-demand Scanning** pane, choose “**Move infected files**” from the “**When a threat is found**” pop-up menu.

By default, the files are moved to /Users/Shared/Infected/. To choose a different folder, click **Choose Folder**, and enter the folder in the dialog.

Any actions that Sophos Anti-Virus takes against infected files are logged in the log of the default scan of this Mac.

Note: The setting of this option applies to both the default scan of this Mac and Finder item scans.

8.3.3 Delete infected files (the default scan of this Mac)

You can configure Sophos Anti-Virus to delete infected files, if the default scan of this Mac detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To delete infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **On-demand Scanning** pane, choose “**Delete infected files**” from the “**When a threat is found**” pop-up menu.

Any actions that Sophos Anti-Virus takes against infected files are logged in the log of the default scan of this Mac.

Note: The setting of this option applies to both the default scan of this Mac and Finder item scans.

8.4 Dealing with threats detected by on-access scanning

8.4.1 Clean up infected files (on-access scanning)

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

You can configure Sophos Anti-Virus to remove viruses from infected files, if on-access scanning detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To clean up infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Choose “**Clean up infected files**” from the “**When a threat is found**” pop-up menu.
5. From the “**If cleanup fails**” pop-up menu, choose what action Sophos Anti-Virus should take if cleanup fails:
 - To deny access to infected files, choose “**Deny access to infected files**”.
 - To delete infected files, choose “**Delete infected files**”.
 - To move infected files to another folder to prevent them being run, choose “**Deny access and move infected files**”.

By default, the files are moved to /Users/Shared/Infected/. To choose a different folder, click **Choose Folder**, and enter the folder in the dialog.

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

Important: Cleaning up infected documents does not repair any changes the virus has made to the document. Cleaning up infected programs should be used only as a temporary measure. You should subsequently replace cleaned programs from the original disks or a clean backup.

8.4.2 Move infected files (on-access scanning)

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

You can configure Sophos Anti-Virus to move infected files to another folder to prevent them being run, if on-access scanning detects a threat. Note that Sophos Anti-Virus always denies access to infected files.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To move infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Choose “**Deny access and move infected files**” from the “**When a threat is found**” pop-up menu.

By default, the files are moved to /Users/Shared/Infected/. To choose a different folder, click **Choose Folder**, and enter the folder in the dialog.

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

8.4.3 Delete infected files (on-access scanning)

Important: If your organization has specified default preferences, these defaults might override changes that you make here.

You can configure Sophos Anti-Virus to delete infected files, if on-access scanning detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To delete infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Choose “**Delete infected files**” from the “**When a threat is found**” pop-up menu.

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

8.5 Dealing with threats detected by custom scans

8.5.1 Clean up infected files (custom scans)

You can configure Sophos Anti-Virus to remove viruses from infected files, if a custom scan detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To clean up infected files:

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the **Options** pane, choose “**Clean up infected files**” from the “**When a threat is found**” pop-up menu.
3. From the “**If cleanup fails**” pop-up menu, choose what action Sophos Anti-Virus should take if cleanup fails:
 - To take no action, choose “**Alert only**”. However, if you have enabled email alerts, Sophos Anti-Virus sends an email alert.
 - To delete infected files, choose “**Delete infected files**”.
 - To move infected files to another folder to prevent them being run, choose “**Move infected files**”.

By default, the files are moved to /Users/Shared/Infected/. To choose a different folder, click **Choose Folder**, and enter the folder in the dialog.

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

Important: Cleaning up infected documents does not repair any changes the virus has made to the document. Cleaning up infected programs should be used only as a temporary measure. You should subsequently replace cleaned programs from the original disks or a clean backup.

8.5.2 Move infected files (custom scans)

You can configure Sophos Anti-Virus to move infected files to another folder to prevent them being run, if a custom scan detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To move infected files:

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the **Options** pane, choose “**Move infected files**” from the “**When a threat is found**” pop-up menu.

By default, the files are moved to /Users/Shared/Infected/. To choose a different folder, click **Choose Folder**, and enter the folder in the dialog.

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

8.5.3 Delete infected files (custom scans)

You can configure Sophos Anti-Virus to delete infected files, if a custom scan detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To delete infected files:

1. If the scan editor is not open, open it. To find out how to do this, see [Open the custom scan editor](#) (page 12).
2. In the **Options** pane, choose “**Delete infected files**” from the “**When a threat is found**” pop-up menu.

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

8.6 Dealing with threats detected by Finder item scans

8.6.1 Clean up infected files (Finder item scans)

You can configure Sophos Anti-Virus to remove viruses from infected files, if a Finder item scan detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To clean up infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **On-demand Scanning** pane, choose “**Clean up infected files**” from the “**When a threat is found**” pop-up menu.
3. From the “**If cleanup fails**” pop-up menu, choose what action Sophos Anti-Virus should take if cleanup fails:
 - To take no action, choose “**Alert only**”. However, if you have enabled email alerts, Sophos Anti-Virus sends an email alert.
 - To delete infected files, choose “**Delete infected files**”.
 - To move infected files to another folder to prevent them being run, choose “**Move infected files**”.

By default, the files are moved to /Users/Shared/Infected/. To choose a different folder, click **Choose Folder**, and enter the folder in the dialog.

Any actions that Sophos Anti-Virus takes against infected files are logged in the log of the Finder item scan.

Important: Cleaning up infected documents does not repair any changes the virus has made to the document. Cleaning up infected programs should be used only as a temporary measure. You should subsequently replace cleaned programs from the original disks or a clean backup.

Note: The setting of this option applies to both the default scan of this Mac and Finder item scans.

8.6.2 Move infected files (Finder item scans)

You can configure Sophos Anti-Virus to move infected files to another folder to prevent them being run, if a Finder item scan detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To move infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **On-demand Scanning** pane, choose “**Move infected files**” from the “**When a threat is found**” pop-up menu.

By default, the files are moved to /Users/Shared/Infected/. To choose a different folder, click **Choose Folder**, and enter the folder in the dialog.

Any actions that Sophos Anti-Virus takes against infected files are logged in the log of the Finder item scan.

Note: The setting of this option applies to both the default scan of this Mac and Finder item scans.

8.6.3 Delete infected files (Finder item scans)

You can configure Sophos Anti-Virus to delete infected files, if a Finder item scan detects a threat.

Important: Sophos Anti-Virus does not ask for confirmation before dealing with an infected file.

To delete infected files:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **On-demand Scanning** pane, choose “**Delete infected files**” from the “**When a threat is found**” pop-up menu.

Any actions that Sophos Anti-Virus takes against infected files are logged in the log of the Finder item scan.

Note: The setting of this option applies to both the default scan of this Mac and Finder item scans.

9 Restoring default preferences

9.1 Restore default on-demand scanning preferences

To set the on-demand scanning preferences to defaults recommended by Sophos:

1. Choose **Sophos Anti-Virus > Preferences**.
2. In the **On-demand Scanning** pane, click **Restore Defaults**.

9.2 Restore default on-access scanning preferences

You can set the on-access scanning preferences to defaults. If your organization has specified default on-access scanning preferences, the on-access scanning preferences will be set to these defaults. Otherwise, they will be set to defaults recommended by Sophos.

To restore default on-access scanning preferences:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **On-access Scanning**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Restore Defaults**.

9.3 Restore default updating preferences

You can restore the updating preferences to defaults. If your organization has specified default updating preferences, the updating preferences will be set to these defaults. Otherwise, they will be set to defaults recommended by Sophos.

To restore default updating preferences:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **AutoUpdate**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Restore Defaults**.

9.4 Restore default logging preferences

You can restore the logging preferences for on-access scanning and updating to defaults. If your organization has specified default logging preferences, the logging preferences will be set to these defaults. Otherwise, they will be set to defaults recommended by Sophos.

To restore default logging preferences:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **Logging**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Restore Defaults**.

9.5 Restore default messaging preferences

You can restore the messaging preferences to defaults. If your organization has specified default messaging preferences, the messaging preferences will be set to these defaults. Otherwise, they will be set to defaults recommended by Sophos.

To restore default messaging preferences:

1. Choose **Sophos Anti-Virus > Preferences**.
2. Click **Messaging**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Click **Restore Defaults**.

10 Use Sophos Anti-Virus via Terminal

You can run a scan via Terminal, Mac OS X's command-line interface. To display the command-line Help for this feature:

1. Open Terminal.
To do this, find the folder Applications/Utilities and double-click Terminal.
2. At the command prompt, type:
`sweep -h`

11 Solving problems

11.1 Sophos Anti-Virus does not update

Symptoms

Sophos Anti-Virus is unable to update or does not attempt to do so. If it is unable to update, a white cross is superimposed on the Sophos Anti-Virus icon on the right-hand side of the menu bar.



Causes

To find out why this is happening, view the updating log. For information, see [View on-access scanning and updating log](#) (page 23).

Resolve the problem

- If Sophos Anti-Virus is contacting the wrong source for updates, see [Set a source for updates](#) (page 19). Check that the settings are correct.
- If Sophos Anti-Virus cannot use your proxy server, see [Enable updating via the system proxy](#) (page 21) or [Enable updating via a custom proxy](#) (page 21), depending on which type of proxy you are using. Check that the settings are correct.
- If Sophos Anti-Virus is not attempting to update when you expect it to, see [Schedule updates](#) (page 21). Check that the settings are correct.

11.2 Update Now menu command is dimmed

Symptoms

The **Update Now** menu command is dimmed in the **Sophos Anti-Virus** menu, the menu bar icon shortcut menu, or the Dock icon shortcut menu.

Causes

Updating is not configured.

Resolve the problem

See [Configuring updating](#) (page 19).

11.3 Sophos Anti-Virus icon is gray

Symptoms

The Sophos Anti-Virus icon on the right-hand side of the menu bar is gray.



Causes

Your Mac is not protected by on-access scanning.

Resolve the problem

Enable on-access scanning. For information about how to do this, see [Enable or disable on-access scanning](#) (page 4).

11.4 Scan with Sophos Anti-Virus menu command is not present

Symptoms

If you try to run a Finder item scan from a shortcut menu, the menu doesn't contain the command "Scan with Sophos Anti-Virus".

Causes

The command isn't contained in the menu immediately after you install Sophos Anti-Virus.

Resolve the problem

Log in to your Mac again.

11.5 File not disinfected

Symptoms

Sophos Anti-Virus reports that an infected file has not been disinfected.

Causes

This could be for one of the following reasons:

- Automatic cleanup has not been enabled for the type of scanning that detected the file.
- The infected item is on a write-protected volume.

- Sophos Anti-Virus has detected a virus/spyware fragment rather than an active virus or item of spyware.

Resolve the problem

Depending on the reason for the file not being disinfected, do one of the following:

- Enable automatic cleanup. For information, see [Dealing with threats detected by on-access scanning](#) (page 26), [Dealing with threats detected by the default scan of this Mac](#) (page 24), [Dealing with threats detected by custom scans](#) (page 27), or [Dealing with threats detected by Finder item scans](#) (page 29).
- Enable write access to the volume if possible.
- Contact Sophos technical support for advice about dealing with a virus/spyware fragment. For information about contacting technical support, see [Technical support](#) (page 37).

11.6 Virus/spyware fragment detected

Symptoms

Sophos Anti-Virus reports that it has detected a virus/spyware fragment.

Causes

This indicates that part of a file matches part of a virus or item of spyware. There are two possible causes:

- Many new viruses or items of spyware are based on existing ones. Therefore, code fragments that are typical of a known virus or item of spyware might appear in files that are infected with a new one.
- Many viruses or items of spyware contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive part of the virus/spyware (possibly a substantial part) may appear in the host file, and this is detected by Sophos Anti-Virus.

Resolve the problem

Contact Sophos technical support for advice. For information about contacting technical support, see [Technical support](#) (page 37).

12 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

13 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.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source¹⁰, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹¹ know so we can promote your project in the DOC software success stories¹².

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹³ around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹⁴, TAO¹⁵, CIAO¹⁶, and CoSMIC¹⁷ web sites are maintained by the DOC Group¹⁸ at the Institute for Software Integrated Systems (ISIS)¹⁹ and the Center for Distributed Object Computing of Washington University, St. Louis²⁰ for the development of open-source software as part of the

open-source software community²¹. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²² know.

Douglas C. Schmidt²³

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. mailto:doc_group@cs.wustl.edu
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>
17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>

22. <mailto:d.schmidt@vanderbilt.edu>

23. <http://www.dre.vanderbilt.edu/~schmidt/>

Boost

Version 1.0, 17 August 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the “Software”) to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

dlcompat

Copyright © 2002 Jorge Acereda (jacereda@users.sourceforge.net) & Peter O’Gorman (ogorman@users.sourceforge.net)

Portions may be copyright others, see the Authors section below.

Maintained by Peter O’Gorman (ogorman@users.sourceforge.net)

Bug Reports and other queries should go to ogorman@users.sourceforge.net

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT,

TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Authors

Original code by Jorge Acereda (jacereda@users.sourceforge.net). This was heavily modified by Peter O’Gorman (ogorman@users.sourceforge.net).

With input from (in alphabetical order):

- Stéphane Conversy (conversy@lri.fr)
- Francis James Franklin (fjf@alinameridon.com)
- Ben Hines (bhines@alumni.ucsd.edu)
- Max Horn (max@quendi.de)
- Karin Kosina (kyrah@sim.no)
- Darin Ohashi (DOhashi@maplesoft.com)
- Benjamin Reed (ranger@befunk.com)

Forgive me if I missed you, and e-mail me (ogorman@users.sourceforge.net) to get added to this list.

libxml2

Except where otherwise noted in the source code (e.g. the files hash.c, list.c and the trio files, which are covered by a similar licence but with different Copyright notices) all the files are:

Copyright © 1998–2003 Daniel Veillard. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE DANIEL VEILLARD BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of Daniel Veillard shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from him.

Authors

- Daniel Veillard (daniel@veillard.com)
- Bjorn Reese (breese@users.sourceforge.net)
- William Brack (wbrack@mmm.com.hk)
- Igor Zlatkovic (igor@zlatkovic.com) for the Windows port
- Aleksey Sanin (aleksey@aleksey.com)

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

pycrypto

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided “as is” without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

– amk (www.amk.ca)