SOPHOS
simple **+** secure

Sophos Anti-Virus for Mac OS X: Home Edition
Help

For standalone Macs running Mac OS X

Product version: 9C
Document date: June 2013

Contents

About Sophos Anti-Virus

Sophos Anti-Virus for Mac: Home Edition is software that detects and deals with threats (viruses, worms, and Trojans) on your Mac. As well as being able to detect Mac OS X threats, it can also detect Windows threats that might be stored on your Mac and transferred to Windows computers.

Sophos Anti-Virus is preconfigured with the recommended settings for protection. We recommend that you don't make changes to the settings unless there is a specific need or problem that you are aiming to address.

About the Scans window

The elements of the **Scans** window are shown below:
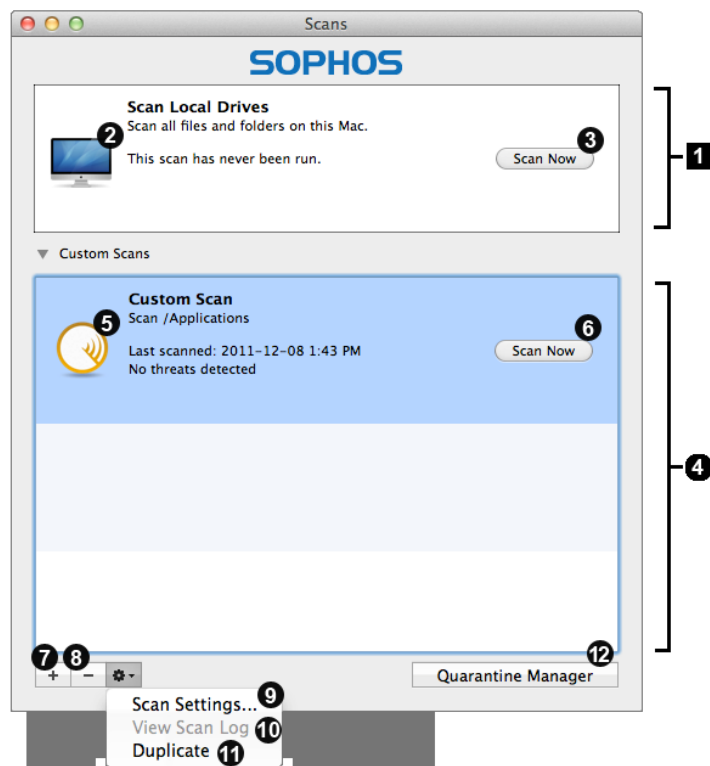
1. The main scan of local drives that Sophos provides as standard. For more information, see *Scanning your Mac* (page 12).

2. Double-click this to open preferences. For more information, see *Configuring scans* (page 13).

3. Click this to scan your Mac. For more information, see *Scan This Mac* (page 12).

4. The list of scans that you have added. For more information, see *Custom scans* (page 14). The first time that you open the window, you must click the disclosure triangle next to **Custom Scans** to reveal the list.

5. Double-click this to configure the custom scan. For more information, see *Configuring a custom scan* (page 16).

6. Click this to run the custom scan.

7 Click this to add a custom scan. For more information, see *Add a custom scan* (page 14).

8 Click this to delete a custom scan.

9 Choose **Scan Settings** to configure the selected custom scan. For more information, see *Configuring a custom scan* (page 16).

10 Choose **View Scan Log** to view the log of the selected custom scan in Console.

11 Choose **Duplicate** to use the selected custom scan as the basis for a new scan. For more information, see *Copy a custom scan* (page 15).

12 Click **Quarantine Manager** to open the **Quarantine Manager** window. For more information, see *About Quarantine Manager* (page 23).

Scanning for threats

About scanning for threats

On-access scanning is your main method of protection against threats. Whenever you access (copy, 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. By default, on-access scanning is turned on and preconfigured with the recommended settings for protection. We recommend that you don't make changes to the settings unless there is a specific need or problem that you are aiming to address.

On-demand scans 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 to which you have access:

- **Scan This Mac**

  Scan all files to which you have access on local volumes. If you authenticate as an administrator, files to which you do not have access are scanned as well. Any removable storage devices that are inserted are included.

  You might want to run this scan because you want to deal with a threat that Sophos Anti-Virus has detected or you want to discover that files are infected *before* you need to use them.

- **Custom scans**

  Scan specific sets of files, folders, or volumes.

  You might want to run a custom scan because you want to scan only suspicious parts of a disk or you want to discover that files are infected *before* you need to use them.

- **Finder item scans**

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

  You might want to run a Finder item scan for one of the following reasons: you want to scan the contents of an archive or compressed file *before* you need to open it, you want to scan something before you email it, or you want to scan a CD or DVD.

You can set up **email alerts** so that any scan type can warn of threats or serious errors.

You can also use **Terminal** to run scans from the command line.

On-access scanning

On-access scanning is your main method of protection against threats. Whenever you access (copy, 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. By default, on-access scanning is turned on and preconfigured with the recommended settings for protection. We recommend that you don't make changes to the settings unless there is a specific need or problem that you are aiming to address.

Turn on-access scanning on or off

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

To turn on-access scanning on or off:

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 turn on-access scanning *on*, click **Start Scanning**. The status changes to **on** and the Sophos Anti-Virus icon in the menu bar turns black.

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

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

Configuring on-access scanning

Add an on-access exclusion

You can exclude files, folders, or volumes from on-access scanning. For example, you might want to exclude:

- Files that are large and therefore take a long time to scan
- Files that cause a scanning error
- Files that cause a false-positive
- Backup volumes because the files that are stored on them are scanned when they're backed up anyway

Important: Excluding files, folders, or volumes from scanning reduces your protection against threats.

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.

   For information about specifying which items are excluded, see *Exclusion rules* (page 8).

Edit an on-access exclusion

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 8).

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 *not* 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 *not* 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

Exclusion path	Item(s) that are excluded
`*.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

Delete an on-access exclusion

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** (-).

Enable on-access scanning inside archives and compressed files

By default, on-access scanning inside archives and compressed files is disabled. However, you might want to enable the option if you are dealing with several such files at a time and the cost of not detecting a threat is high. For example, you might be emailing some archives or compressed files to an important contact.

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.

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**".

Enable on-access scanning of files on network volumes

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**".

Note: Files on network volumes that you access through an alias are not scanned.

Configure on-access scanning to automatically clean up threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure on-access scanning to automatically clean up threats that it detects.

📝 **Important:** Sophos Anti-Virus does not ask for confirmation before cleaning up a threat.

To configure on-access scanning to automatically clean up threats:

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 threat**" 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 the threat, choose "**Deny access**".
   - To delete the threat, choose "**Delete threat**".
   - To move the threat to another folder to prevent it being run, choose "**Deny access and move threat**".

     By default, the threats 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 threats are logged in the Sophos Anti-Virus log.

📝 **Important:** Cleaning up a threat might not be able to undo all the actions the threat has taken on this Mac. For example, if the threat changed the value of a setting, the cleanup process might not know the original setting. You might have to verify the Mac's configuration. Cleaning up an infected document does not repair any changes the threat has made to the document.

Configure on-access scanning to automatically move threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure on-access scanning to automatically move threats that it detects to another folder. Moving an infected program reduces the likelihood of it being run. Note that Sophos Anti-Virus always denies access to infected files that it has moved, as long as on-access scanning is turned on.

📝 **Important:** You should use this option only if advised to at the support forum. Sophos Anti-Virus does not ask for confirmation before moving a threat.

To configure on-access scanning to automatically move threats:

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 threat**" from the "**When a threat is found**" pop-up menu.
   By default, the threats 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 threats are logged in the Sophos Anti-Virus log.

Configure on-access scanning to automatically delete threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure on-access scanning to automatically delete threats that it detects.

📝 **Important:** You should use this option only if advised to at the support forum. Sophos Anti-Virus does not ask for confirmation before deleting a threat.

To configure on-access scanning to automatically delete threats:

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 threat**" from the "**When a threat is found**" pop-up menu.

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

📝 **Important:** Deleting a threat does not undo any actions the threat has taken on this Mac.

Restore default on-access scanning preferences

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

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**.

Configure desktop alerts

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 add your own message to the 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**".

Restore default alerting preferences

To set the alerting preferences to defaults recommended by Sophos:

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**.

Change logging preferences

All on-access scanning activity (including threats detected) and all updating activity is logged in the Sophos on-access scanning and updating log. Sophos Anti-Virus can also log such activity in the Mac OS X 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 Log 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**".

Restore default logging preferences

To set the logging preferences to defaults recommended by Sophos:

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**.

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).

Scanning your Mac

You can initiate a scan of your Mac at any time. This will scan all files to which you have access on local volumes. If you authenticate as an administrator, files to which you do not have access are scanned as well. Any removable storage devices that are inserted are included.

You might want to run a scan because you want to deal with a threat that Sophos Anti-Virus has detected or you want to discover files that are infected *before* you need to use them.

Scan This Mac

You can run a scan of all files on this Mac to which you have access. If you are an admin user, this scan also includes all files to which you do *not* usually have access.

- 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 **Scans** window.

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

   - In the **Scans** window, in the **Scan Now** box, click the Play button.
   - Click the Sophos Anti-Virus icon on the right-hand side of the menu bar, and then choose **Scan Now** 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.

Configuring scans

Disable scanning inside archives and compressed files

By default, scanning inside archives and compressed files is enabled when you scan your Mac.

To disable scanning inside archives and compressed files for scans:

1. In the **Scans** window, double-click the **Scan This Mac** box.
2. Select **Options**.
3. Deselect "**Scan inside archives and compressed files**".

Configure scans to automatically clean up threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure the local drives scan to automatically clean up threats that it detects.

📝 **Important:** Sophos Anti-Virus does not ask for confirmation before cleaning up a threat.

To configure the local drives scan to automatically clean up threats:

1. In the **Scans** window, double-click the **Scan This Mac** box.
2. Select **Options**.
3. Choose "**Clean up threat**" from the "**When a threat is found**" pop-up menu.
4. From the "**If cleanup fails**" pop-up menu, choose what action Sophos Anti-Virus should take if cleanup fails:

   - To take no action, choose "**Log only**". However, if you have enabled email alerts, Sophos Anti-Virus also sends an email alert.
   - To delete the threat, choose "**Delete threat**".
   - To move the threat to another folder to prevent it being run, choose "**Move threat**".

     By default, the threats 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 threats are logged in the log of the local drives scan.

📝 **Important:** Cleaning up a threat might not be able to undo all the actions the threat has taken on this Mac. For example, if the threat changed the value of a setting, the cleanup process might not know the original setting. You might have to verify the Mac's configuration. Cleaning up an infected document does not repair any changes the threat has made to the document.

Configure scans to automatically move threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure scans to automatically move threats that it detects to another folder. Moving an infected program reduces the likelihood of it being run.

📝 **Important:** You should use this option only if advised to at the support forum. Sophos Anti-Virus does not ask for confirmation before moving a threat.

To configure the local drives scan to automatically move threats:

1. In the **Scans** window, double-click the **Scan This Mac** box.
2. Select **Options**.
3. Choose "**Move threat**" from the "**When a threat is found**" pop-up menu.

By default, the threats 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 threats are logged in the scan log.

Configure scans to automatically delete threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure scans to automatically delete detected threats.

📝 **Important:** You should use this option only if advised to at the support forum. Sophos Anti-Virus does not ask for confirmation before deleting a threat.

To configure scans to automatically delete threats:

1. In the **Scans** window, double-click the **Scan This Mac** box.
2. Select **Options**.
3. In the **Scan This Mac** pane, choose "**Delete threat**" from the "**When a threat is found**" pop-up menu.

Any actions that Sophos Anti-Virus takes against threats are logged in the scan log.

📝 **Important:** Deleting a threat does not undo any actions the threat has taken on this Mac.

View the log of a scan

- Choose **Scan ➤ View Scan Log**.

The log is displayed in Console.

Custom scans

A custom scan is a scan that you initiate. It is a scan of specific sets of files, folders, or volumes.

You might want to run a custom scan because you want to scan only suspicious parts of a disk or you want to discover files that are infected *before* you need to use them.

Run a custom scan

1. If the **Scans** window is not open, choose **Window ➤ Scans** 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 the **Scan Now** button.
   The progress of the scan is displayed in the **Sophos Anti-Virus** window.

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 16).

- To specify what not to scan, see *Add a custom scan exclusion* (page 17), *Edit a custom scan exclusion* (page 17), or *Delete a custom scan exclusion* (page 18) as appropriate.
- To disable scanning inside archives and compressed files, see *Disable scanning inside archives and compressed files for a custom scan* (page 18).

The scan is added to the **Custom Scans** list in the **Scans** window.

📝 **Note:**

You can also add a scan in one of the following ways:

- Click **Add** (+) at the bottom of the **Scans** window.
- From Finder, drag items to be scanned to a blank space in the **Custom Scans** list.

Add a custom scan of a threat

If a threat is listed in Quarantine Manager, you can add a custom scan of that threat.

1. If the **Scans** window is not open, choose **Window ➤ Scans** to open it.
2. If the **Custom Scans** list is not displayed, click the disclosure triangle next to **Custom Scans**.
3. If the **Quarantine Manager** window is not open, choose **Window ➤ Quarantine Manager** to open it.
4. In Quarantine Manager, do one of the following:

   - In the list of threats, select the threats that you want to add to a new custom scan.

     Drag the selected threats to a blank space in the **Custom Scans** list.

   - In the **Threat Details** box, select the files that you want to add to a new custom scan.

     Drag the selected files to a blank space in the **Custom Scans** list.

   - In the **Threat Details** box, click **Path and Filename**, and then choose "**Create a Custom Scan of These Files**" from the pop-up menu.

5. In the scan editor that is displayed, to rename the scan, in the **Scan Name** field, type the new name.
6. In the **Options** pane, choose "**Delete threat**" from the "**When a threat is found**" pop-up menu.

The scan is added to the **Custom Scans** list.

Copy a custom scan

1. If the **Scans** window is not open, choose **Window ➤ Scans** 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. Double-click the new scan, then 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 16).
   - To specify what not to scan, see *Add a custom scan exclusion* (page 17), *Edit a custom scan exclusion* (page 17), or *Delete a custom scan exclusion* (page 18) as appropriate.
   - To disable scanning inside archives and compressed files, see *Disable scanning inside archives and compressed files for a custom scan* (page 18).

The scan is added to the **Custom Scans** list in the **Scans** window.

📝 **Note:** You can also copy a selected scan in the **Scans** window in one of the following ways:

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

Configuring a custom scan

Open the custom scan editor

1. If the **Scans** window is not open, choose **Window ➤ Scans** 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 in one of the following ways:

- Select the scan that you want to edit and click the Edit button.
- Select the scan that you want to edit and choose **Edit Scan** from the Action pop-up menu at the bottom of the window.

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 16).
2. In the scan editor, in the **Scan Name** field, type the new name.

Specify what to scan

- Do one of the following:

  - From Finder, drag items to be scanned to the custom scan in the **Scans** window.
  - In the scan editor, click **Add** (+) and choose the items to be scanned from the dialog.

    To find out how to open the scan editor, see *Open the custom scan editor* (page 16).

📝 **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.

Add a threat to a custom scan

If a threat is listed in Quarantine Manager, you can add it to an existing custom scan.

1. If the **Scans** window is not open, choose **Window ➤ Scans** to open it.
2. If the **Custom Scans** list is not displayed, click the disclosure triangle next to **Custom Scans**.
3. If the **Quarantine Manager** window is not open, choose **Window ➤ Quarantine Manager** to open it.
4. In Quarantine Manager, do one of the following:

   - In the list of threats, select the threats that you want to add to an existing custom scan.

     Drag the selected threats to your chosen scan in the **Custom Scans** list.

   - In the **Threat Details** box, select the files that you want to add to an existing custom scan.

     Drag the selected files to your chosen scan in the **Custom Scans** list.

   📝 **Note:** If the editor for your chosen scan is already open, you can drag the selected threats or files to that.

Add a custom scan exclusion

You can exclude files, folders, or volumes from a custom scan. For example, you might want to exclude:

- Files that are large and therefore take a long time to scan
- Files that cause a scanning error
- Files that cause a false-positive
- Backup volumes because the files that are stored on them are scanned when they're backed up anyway

📝 **Important:** Excluding files, folders, or volumes from scanning reduces your protection against threats.

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 16).
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.

   For information about specifying which items are excluded, see *Exclusion rules* (page 17).

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 16).
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 17).

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 *not* 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 *not* 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

Exclusion path	Item(s) that are excluded
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

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 16).
2. In the **Excluded Items** pane, select the item that you want to delete and click **Delete** (-).

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 16).
2. In the **Options** pane, deselect "**Inside archives and compressed files**".

Schedule a custom scan to run at specific times

Users who are administrators can configure a custom scan to run automatically at scheduled times. Scans can be scheduled to run on every day of the week at a specific time or times.

1. If the scan editor is not open, open it. To find out how to do this, see *Open the custom scan editor* (page 16).
2. In the **Schedule** pane, select the "**Enable Schedule**" checkbox.
3. Select the days on which you want the custom scan to run.
4. Click **Add** (+) to add a new time.
5. Set the new entry to the time you want the scan.

📝 **Note:** You can add additional times by clicking **Add** (+), and remove times by clicking **Delete** (-).

Configure a custom scan to automatically clean up threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure a custom scan to automatically clean up threats that it detects.

📝 **Important:** Sophos Anti-Virus does not ask for confirmation before cleaning up a threat.

To configure a custom scan to automatically clean up threats:

1. If the scan editor is not open, open it. To find out how to do this, see *Open the custom scan editor* (page 16).
2. In the **Options** pane, choose "**Clean up threat**" 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 "**Log only**". However, if you have enabled email alerts, Sophos Anti-Virus also sends an email alert.

- To delete the threat, choose "**Delete threat**".
- To move the threat to another folder to prevent it being run, choose "**Move threat**".

  By default, the threats 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 threats are logged in the log of the custom scan.

📝 **Important:** Cleaning up a threat might not be able to undo all the actions the threat has taken on this Mac. For example, if the threat changed the value of a setting, the cleanup process might not know the original setting. You might have to verify the Mac's configuration. Cleaning up an infected document does not repair any changes the threat has made to the document.

Configure a custom scan to automatically move threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure a custom scan to automatically move threats that it detects to another folder. Moving an infected program reduces the likelihood of it being run.

📝 **Important:** You should use this option only if advised to at the support forum. Sophos Anti-Virus does not ask for confirmation before moving a threat.

To configure a custom scan to automatically move threats:

1. If the scan editor is not open, open it. To find out how to do this, see *Open the custom scan editor* (page 16).
2. In the **Options** pane, choose "**Move threat**" from the "**When a threat is found**" pop-up menu.

   By default, the threats 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 threats are logged in the log of the custom scan.

Configure a custom scan to automatically delete threats

To deal with threats, we recommend that you use Quarantine Manager (see *Dealing with threats* (page 22)). However, you can configure a custom scan to automatically delete threats that it detects.

📝 **Important:** You should use this option only if advised to at the support forum. Sophos Anti-Virus does not ask for confirmation before deleting a threat.

To configure a custom scan to automatically delete threats:

1. If the scan editor is not open, open it. To find out how to do this, see *Open the custom scan editor* (page 16).
2. In the **Options** pane, choose "**Delete threat**" from the "**When a threat is found**" pop-up menu.

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

📝 **Important:** Deleting a threat does not undo any actions the threat has taken on this Mac.

Delete a custom scan

1. If the **Scans** window is not open, choose **Window ➤ Scans** 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** (-).

View a custom scan log

1. If the **Scans** window is not open, choose **Window ➤ Scans** 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.

Configure email alerts

Sophos Anti-Virus can send an email if it detects a threat or a serious error occurs. This applies to on-access scanning, user-initiated scans, 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.

   Note: You can use more than one email address, by separating addresses with commas.

Restore default alerting preferences

To set the alerting preferences to defaults recommended by Sophos:

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**.

Live Protection

Live Protection enables real-time online lookups of potential threats. With Live Protection enabled, Sophos Anti-Virus will check suspicious files against the extensive SophosLabs cloud database to determine whether the file should be blocked or allowed. To configure Live Protection:

1. Choose **Sophos Anti-Virus ➤ Preferences** .
2. Click **Live Protection**.
3. If some settings are dimmed, click the lock icon and type an administrator name and password.
4. Move the toggle switch to "**On**" to enable Live Protection.

Restore default Live Protection setting

To restore the Live Protection setting to the default recommended by Sophos:

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

Web Protection

Sophos Web Protection provides enhanced protection against web threats. It works by looking up website URLs in the Sophos online database of infected websites, and then blocking access to any websites that are known to host malware.

Supported Browsers

The following browsers support web protection:

- Firefox
- Google Chrome
- Safari
- Opera

General Settings

Web Protection can be configured to block access to malicious websites, scan downloads to help protect against malicious content, or both. To configure Web Protection:

1. Choose **Sophos Anti-Virus ➤ Preferences** .
2. Select **Web Protection**.
3. Click **General** on the **Web Protection** panel.
4. If some settings are dimmed, click the lock icon and type an administrator name and password.
5. Move the upper toggle switch to **On** to protect your Mac from sites that Sophos has identified to be hosting malicious content.

6. Move the lower toggle switch to **On** to block malicious downloads before they reach your browser. This will perform an additional check by passing downloads through the content scanning engine.

Allowed Websites

You may want to exclude certain websites from Web Protection. You can add a domain name to bypass Web Protection filtering for an entire domain. You can also add an IPv4 address to bypass Web Protection filtering for that address. To add an allowed website:

1. Choose **Sophos Anti-Virus ➤ Preferences** .
2. Select **Web Protection**.
3. Click **Allowed Websites** on the **Web Protection** panel.
4. If some settings are dimmed, click the lock icon and type an administrator name and password.
5. Click the **+** button to add a site that will be excluded from Web Protection. Enter the domain name, IP address, or IP address range in CIDR notation that you want to exclude from Web Protection. You cannot enter a specific path.

    Examples of valid allowed websites:

    - `example.com` will allow all of the `example.com` domain.
    - `address.example.com` will allow `address.example.com` or `this.address.example.com`, but not `different.example.com`.
    - `192.0.2.0` will allow only `192.0.2.0`.
    - `192.0.2.0/24` will allow all addresses from `192.0.2.0` to `192.0.2.255`.

    Note: Local addresses are automatically included in the list of allowed websites.

Use Sophos Anti-Virus from Terminal

You can run a scan from 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
```

Dealing with threats

If a threat is detected on your Mac, it is listed in a component of Sophos Anti-Virus called Quarantine Manager. You should open Quarantine Manager and deal with the threat there.

Open Quarantine Manager

To open Quarantine Manager, do one of the following:

- Choose **Window ➤ Quarantine Manager** .

- Click the Sophos Anti-Virus icon on the right-hand side of the menu bar, and then choose **Open Quarantine Manager** from the shortcut menu.
- In the **Scans** window, click **Quarantine Manager**.

About Quarantine Manager

Quarantine Manager lists all the threats that have been detected by scanning and enables you to deal with them. The elements of the **Quarantine Manager** window are shown below:
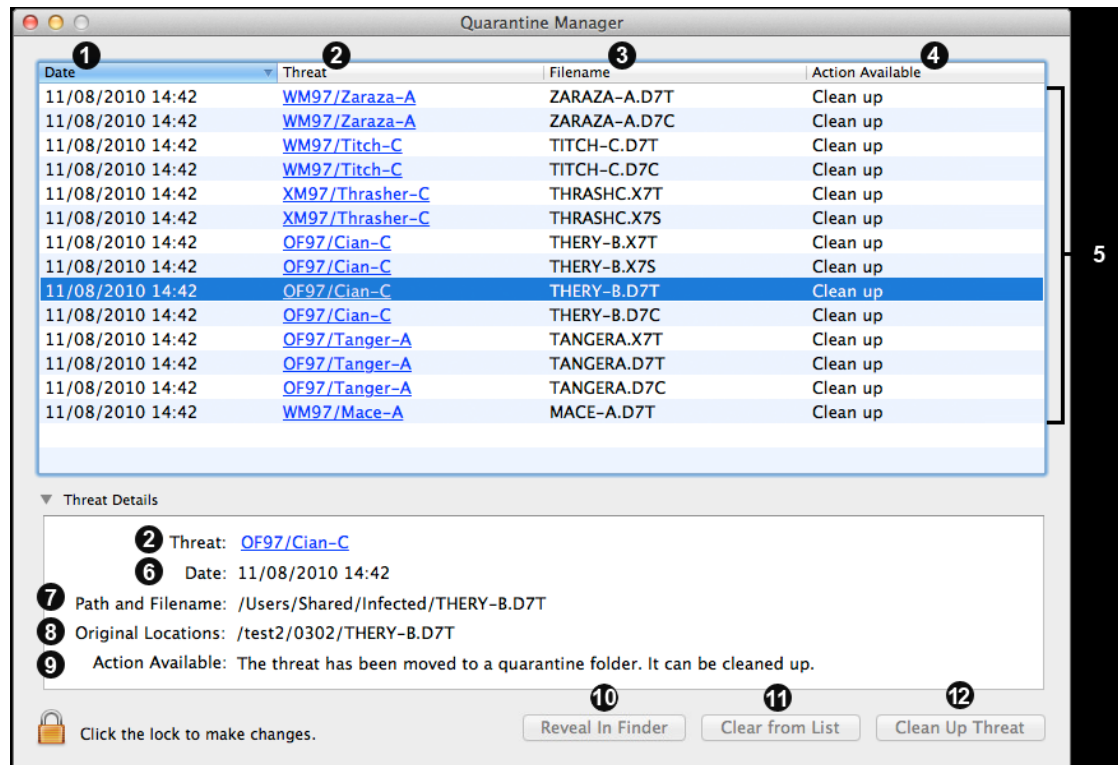
1   The date and time of detection. If the threat has been detected multiple times, only the first detection is included here.

2   The name of the threat, including a link to the analysis on the Sophos website.

3   The main file associated with the threat.

4   The action that you can take to deal with the threat.

5   The list of threats that have been detected. You can sort the threats by clicking any of the column headings. You can select one or more threats to deal with at a time. The maximum number of threats listed is 200. If this limit is reached, the newest threats replace the oldest.

6   The date and time of detection. If the threat has been detected multiple times, only the first and last detections are included here.

7   The locations and names of all the files that comprise the threat.

8   If the threat has been moved during scanning or partially removed, this element is displayed. All the original files that comprise the threat are listed.

9   The action that you can take to deal with the threat and a summary of what action has been taken so far, if applicable.

⑩ Click **Reveal In Finder** to open the finder at the location of the file associated with the selected threat. For more information, see *Deal with threats in Quarantine Manager* (page 24).

⑪ Click "**Clear from List**" to clear a selected threat from Quarantine Manager without dealing with the threat itself. For more information, see *Clear a threat from Quarantine Manager* (page 25).

⑫ Click **Clean Up Threat** to clean up a selected threat. For more information, see *Deal with threats in Quarantine Manager* (page 24).

View threat details in Quarantine Manager

In Quarantine Manager, you can view more details on how a threat has affected your Mac, for example all the files that comprise the threat.

Some details are hidden unless you authenticate by clicking the lock icon at the bottom of the **Quarantine Manager** window.

To view details of a threat in Quarantine Manager:

1. In Quarantine Manager, select the threat for which you want to view the details.

   You can select more than one threat but the details that are displayed are less specific.

2. Click the disclosure triangle next to **Threat Details**.

   The threat details are displayed in the **Threat Details** box. For a description of each field, see *About Quarantine Manager* (page 23).

If the paths of the files that comprise the threat are shortened because they're too long to display, you can copy the paths to the Clipboard so that you can paste them into a text editor. To copy the paths, in the **Threat Details** box, click "**Path and Filename**", and then choose "**Copy the Paths of These Files**" from the pop-up menu.

Deal with threats in Quarantine Manager

1. In Quarantine Manager, click the **Action Available** column heading to sort the list of threats according to the action available.

2. Select all the threats for which the action available is "**Clean up**".

3. Click **Clean Up Threat**.

   You must authenticate by clicking the lock icon at the bottom of the **Quarantine Manager** window.

   Any threats that are cleaned up are cleared from the list.

4. Click the **Action Available** column heading to sort the list of threats.

5. If there are any threats for which the action available is **Restart**, restart your Mac to complete the cleanup.

6. Click the **Action Available** column heading to sort the list of threats.

7. If there are any threats for which the action available is "**Scan this Mac**", run a scan of local drives (see *Scan This Mac* (page 12)).

8. Click the **Action Available** column heading to sort the list of threats.

9. If there are any threats for which the action available is "**Clean up**", go back to step 3.

10. If there are any threats for which the action available is "**Clean up manually**":

    a) Add a new custom scan of the threats, as explained in *Add a custom scan of a threat* (page 15).

    b) Run the scan, as explained in *Run a custom scan* (page 14).

📝 **Important:** Cleaning up a threat might not be able to undo all the actions the threat has taken on this Mac. For example, if the threat changed the value of a setting, the cleanup process might not know the original setting. You might have to verify the Mac's configuration. Cleaning up an infected document does not repair any changes the threat has made to the document.

Disable cleanup warning

By default, Sophos Anti-Virus warns you before it cleans up threats in Quarantine Manager.

To disable the cleanup warning:

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. Deselect "**Warn before cleaning up threats in Quarantine Manager**".

📝 **Note:** You can also disable the cleanup warning by selecting "**Do not show this message again**" in the warning dialog.

Clear a threat from Quarantine Manager

To clear a threat, you must authenticate by clicking the lock icon at the bottom of the **Quarantine Manager** window.

You might want to clear a threat because:

- It's been confirmed as a false-positive
- You are confident that you have successfully cleaned it up manually
- You have removed infected removable media
- You want to clear the list of threats before running a scan of local drives

To clear a threat from Quarantine Manager:

1. In Quarantine Manager, select the threat that you want to clear.
   You can select more than one threat at a time.
2. Click "**Clear from List**".

Clearing a threat does not delete any files.

Updating

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.

The Sophos Anti-Virus icon on the right-hand side of the menu bar will display a moving arrow to indicate that an update is being performed.

Configuring updating

Because Sophos Anti-Virus for Mac: Home Edition is preconfigured to update from Sophos, only a limited range of configuration options is available.

Schedule updates

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**".

Restore default updating preferences

To set the updating preferences to defaults recommended by Sophos:

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**.

Change logging preferences

All on-access scanning activity (including threats detected) and all updating activity is logged in the Sophos on-access scanning and updating log. Sophos Anti-Virus can also log such activity in the Mac OS X 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 Log 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**".

Restore default logging preferences

To set the logging preferences to defaults recommended by Sophos:

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**.

Check the progress of an update

- When an update is being performed, the Sophos Anti-Virus icon on the right-hand side of the menu bar will indicate this by displaying a moving arrow. Or, to check the progress of an update, 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 27).

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).

Remove Sophos Anti-Virus

1. Find the folder /Applications and double-click Sophos Remove.
2. In the confirmation dialog, click **Remove Sophos Anti-Virus**.
3. In the user account dialog, type an administrator name and password. Click **OK**.

Sophos Anti-Virus is removed from your Mac.

Solving problems

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 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 27).

Resolve the problem

- If Sophos Anti-Virus is not attempting to update when you expect it to, see *Schedule updates* (page 26). Check that the settings are correct.

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

Turn on on-access scanning. For information about how to do this, see *Turn on-access scanning on or off* (page 7).

"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.

Manual cleanup required

Symptoms

A threat is displayed in Quarantine Manager with the available action "**Clean up manually**".

Causes

This could be for one of the following reasons:

- Sophos Anti-Virus does not have threat data to clean up the threat.
- The threat is on a write-protected volume.

Resolve the problem

Depending on the reason for the threat not being cleaned up, do one of the following:

- If Sophos Anti-Virus does not have threat data to clean up the threat, you must clean up the threat manually:

    1. Add a new custom scan of the threats, as explained in *Add a custom scan of a threat* (page 15).
    2. Run the scan, as explained in *Run a custom scan* (page 14).

    📝 **Important:** Cleaning up a threat might not be able to undo all the actions the threat has taken on this Mac. For example, if the threat changed the value of a setting, the cleanup process might not know the original setting. You might have to verify the Mac's configuration.

- If you can turn on write access to the volume:

    1. Clear the threat from Quarantine Manager (see *Clear a threat from Quarantine Manager* (page 25)).
    2. Scan for the threat again.
    3. Turn on write access to the volume.
    4. Clean up the threat in Quarantine Manager (see *Deal with threats in Quarantine Manager* (page 24)).

Technical support

If you have any questions, ask other users of the software for help by visiting the FreeTalk forum at *http://openforum.sophos.com/MacAV*. Sophos does not provide technical support by telephone or email for Sophos Anti-Virus for Mac: Home Edition.

Legal notices

Copyright © 2013 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

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

ACE™, TAO™, CIAO™, and CoSMIC™

ACE[1], TAO[2], CIAO[3], and CoSMIC[4] (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt[5] and his research group[6] at Washington University[7], University of California[8], Irvine, and Vanderbilt University[9], Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, 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 us[10] know so we can promote your project in the DOC software success stories[11].

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 companies[12] 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 ACE[13], TAO[14], CIAO[15], and CoSMIC[16] web sites are maintained by the DOC Group[17] at the Institute for Software Integrated Systems (ISIS)[18] and the Center for Distributed Object Computing of Washington University, St. Louis[19] for the development of open-source software as part of the open-source software community[20]. 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 acknowledgethat 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, WashingtonUniversity, 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 me[21] know.

Douglas C. Schmidt[22]

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. mailto:doc_group@cs.wustl.edu

11. http://www.cs.wustl.edu/~schmidt/ACE-users.html

12. http://www.cs.wustl.edu/~schmidt/commercial-support.html

13. http://www.cs.wustl.edu/~schmidt/ACE.html

14. http://www.cs.wustl.edu/~schmidt/TAO.html

15. http://www.dre.vanderbilt.edu/CIAO/

16. http://www.dre.vanderbilt.edu/cosmic/

17. http://www.dre.vanderbilt.edu/

18. http://www.isis.vanderbilt.edu/

19. http://www.cs.wustl.edu/~schmidt/doc-center.html

20. http://www.opensource.org/

21. mailto:d.schmidt@vanderbilt.edu

22. http://www.dre.vanderbilt.edu/~schmidt/

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at *http://www.apache.org/licenses/LICENSE-2.0*.

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.

Common Public License

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

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

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

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

curl

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

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 OF THIRD PARTY RIGHTS. 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.

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

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 NONINFRINGEMENT. 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.

dtoa.c

The author of this software is David M. Gay.

Copyright © 1991, 2000 by Lucent Technologies.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR LUCENT MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

GNU General Public License

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to *savlinuxgpl@sophos.com*. A copy of the GPL terms can be found at *www.gnu.org/copyleft/gpl.html*

ICU

ICU version 1.8.1 or later

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1995–2008 International Business Machines Corporation and others

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, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

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

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

Info-ZIP

Copyright © 1990–2005 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions—including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, and dynamic, shared, or static library versions—must be plainly marked as such and must not be misrepresented as being the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases—including, but not limited to, labeling of the altered versions with the names "Info- ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or of the Info-ZIP URL(s).

4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

libmagic – file type detection

Copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994–2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

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 immediately at the beginning of the file, without modification, 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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "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.

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 license 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)

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

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 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.

Medusa web server

Medusa was once distributed under a 'free for non-commercial use' license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

mt19937ar.c

Copyright (c) 1997–2002 Makoto Matsumoto and Takuji Nishimura. 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. The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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.

netaddr

Copyright © 2008-2011, David P. D. Moss. All rights reserved.

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

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- Neither the name of David P. D. Moss nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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.

License for incorporated software:

intset.py - Immutable integer set type

Copyright © 2006, Heiko Wundram.

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 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.

Open Source Initiative

The Sophos software that is described in this document may include some software that is licensed (or sublicensed) to the user under the Open Source Initiative (OSI), which, among other rights, permits the user to copy, modify, and redistribute certain programs or portions thereof, and have access to the source code. OSI licenses require for any software licensed under their terms which is distributed in object code form, that the source code for such software also be made available to the users of the object code. For any such software, the source code is available by submitting a request to Sophos; via email to *support@sophos.com* or via the web at *http://www.sophos.com/en-us/support/contact-support/contact-information.aspx*. The license agreement for any such included software can be found at *http://opensource.org/licenses/eclipse-1.0.php*

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 © 1998–2011 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 license 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 license [including the GNU Public License.]

OPSWAT, Inc.

This software contains technology licensed from and copyrighted © by OPSWAT, Inc. OPSWAT is a trademark of OPSWAT, Inc.

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)

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.

2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.

4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR

ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.

5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.

6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.

7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.

8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

Regex++, Index

Part of PureMessage uses Regex++, Index (version 3.04, 18 April 2000).

Copyright © 1998-2000, Dr John Maddock

Permission to use, copy, modify, distribute and sell the Regex ++, index library and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation.

Shavlik Technologies

This software contains HFNetChk technology licensed from Shavlik Technologies, LLC. © Shavlik Technologies, LLC.

Simple ECMAScript Engine

Copyright © 2003, 2004, 2005, 2006, 2007 David Leonard. 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. Neither the name of David Leonard nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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.

strcasestr.c

Copyright © 1990, 1993 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

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. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "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 REGENTS 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.

strnstr.c

Copyright © 2001 Mike Barcroft (mike@FreeBSD.org). Copyright © 1990, 1993 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Chris Torek.

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. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "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 REGENTS 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.

TinyXML XML parser

www.sourceforge.net/projects/tinyxml

Original code by Lee Thomason (www.grinninglizard.com)

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Unicode

UNICODE, INC. LICENSE AGREEMENT – DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/. Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991–2007 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE 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 OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

UnRAR

The source code of UnRAR utility is freeware. This means:

1. All copyrights to RAR and the utility UnRAR are exclusively owned by the author - Alexander Roshal.
2. The UnRAR sources may be used in any software to handle RAR archives without limitations free of charge, but cannot be used to re-create the RAR compression algorithm, which is proprietary. Distribution of modified UnRAR sources in separate form or as a part of other software is permitted, provided that it is clearly stated in the documentation and source comments that the code may not be used to develop a RAR (WinRAR) compatible archiver.
3. The UnRAR utility may be freely distributed. It is allowed to distribute UnRAR inside of other software packages.
4. THE RAR ARCHIVER AND THE UnRAR UTILITY ARE DISTRIBUTED "AS IS". NO WARRANTY OF ANY KIND IS EXPRESSED OR IMPLIED. YOU USE AT YOUR OWN RISK. THE AUTHOR WILL NOT BE LIABLE FOR DATA LOSS, DAMAGES, LOSS OF PROFITS OR ANY OTHER KIND OF LOSS WHILE USING OR MISUSING THIS SOFTWARE.
5. Installing and using the UnRAR utility signifies acceptance of these terms and conditions of the license.
6. If you don't agree with terms of the license you must remove UnRAR files from your storage devices and cease to use the utility.

Thank you for your interest in RAR and UnRAR.

Alexander L. Roshal

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

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

• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
• 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.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT HOLDER 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.

XPExplorerBar

Copyright © 2004-2005, Mathew Hall

All rights reserved.

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

• Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
• 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.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT OWNER 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.

zlib compression tools

© 1995–2002 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate *not* receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.