1 About Sophos Endpoint Security and Control help

This Help file provides information about Sophos Endpoint Security and Control and explains procedures step by step.
2 About Sophos Endpoint Security and Control

Sophos Endpoint Security and Control is an integrated suite of security software.

**Sophos Anti-Virus** detects and cleans up viruses, Trojans, worms, and spyware, as well as adware and other potentially unwanted applications. Our HIPS (Host Intrusion Prevention System) technology can also protect your computer from suspicious files and rootkits. In addition, Malicious Traffic Detector can detect communications between your computer and command and control servers involved in a botnet or other malware attack.

**Sophos Behavior Monitoring** uses our HIPS technology to protect Windows computers from unidentified or "zero-day" threats and suspicious behavior.

**Sophos Live Protection** improves detection of new malware without the risk of unwanted detections. This is achieved by doing an instant lookup against the very latest known malware. When new malware is identified, Sophos can send out updates within seconds.

**Sophos Web Protection** provides enhanced protection against web threats by preventing access to locations that are known to host malware. It blocks endpoints' access to such sites by performing a real-time lookup against Sophos's online database of malicious websites. It also scans downloaded data and files and checks file reputation.

**Sophos Application Control** blocks unauthorized applications such as Voice over IP, instant messaging, file sharing, and game software.

**Sophos Device Control** blocks unauthorized external storage devices and wireless connection technologies.

**Sophos Data Control** prevents the accidental leakage of personally-identifiable information from managed computers.

**Sophos Web Control** provides protection, control, and reporting for computers that are located, or roam, outside the corporate network.

**Sophos Client Firewall** prevents worms, Trojans, and spyware from stealing and distributing sensitive information, and also prevents intrusion from hackers.

**Sophos AutoUpdate** offers fail-safe updating and can throttle bandwidth when updating over low-speed network connections.

**Sophos Tamper Protection** prevents unauthorized users (users with limited technical knowledge) and known malware from uninstalling Sophos security software or disabling it through the Sophos Endpoint Security and Control interface.
3 About the Home page

The Home page is displayed in the right-hand pane when you open the Sophos Endpoint Security and Control window. It enables you to configure and use the software.

As you use Sophos Endpoint Security and Control, the content of the right-hand pane will change. To return to the Home page, click the Home button on the toolbar.
4 Sophos groups

4.1 About Sophos groups

Sophos Endpoint Security and Control restricts access to certain parts of the software to members of certain Sophos groups.

When Sophos Endpoint Security and Control is installed, each user on this computer is initially assigned to a Sophos group depending on their Windows group.

<table>
<thead>
<tr>
<th>Windows group</th>
<th>Sophos group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>SophosAdministrator</td>
</tr>
<tr>
<td>Power Users</td>
<td>SophosPowerUser</td>
</tr>
<tr>
<td>Users</td>
<td>SophosUser</td>
</tr>
</tbody>
</table>

Users who are not assigned to a Sophos group, including Guest users, can only perform the following tasks:

- On-access scanning
- Right-click scanning

**SophosUsers**

SophosUsers can perform the tasks above and also perform the following tasks:

- Open the Sophos Endpoint Security and Control window
- Set up and run on-demand scans
- Configure right-click scanning
- Manage (with limited privileges) quarantined items
- Create and configure firewall rules

**SophosPowerUsers**

SophosPowerUsers have the same rights as SophosUsers, with the addition of the following rights:

- Greater privileges in Quarantine manager
- Access to Authorization manager

**SophosAdministrators**

SophosAdministrators can use and configure any part of Sophos Endpoint Security and Control.
Note
If tamper protection is enabled, a SophosAdministrator must know the tamper protection password to perform the following tasks:
• Configure on-access scanning.
• Configure suspicious behavior detection.
• Disable tamper protection.
For more information, see About tamper protection on this computer (page 81).

4.2 Add a user to a Sophos group

If you are a domain administrator or a member of the Windows Administrators group on this computer, you can change the Sophos group in which a user has membership. You would typically do this in order to change their access rights to Sophos Endpoint Security and Control.

To add a user to a Sophos group:
2. In the console tree, click Users.
3. Right-click the user’s account, and then click Properties.
4. On the Member Of tab, click Add.
5. In Enter the object names to select, type one of the Sophos group names:
   • SophosAdministrator
   • SophosPowerUser
   • SophosUser
6. If you want to validate the Sophos group name, click Check Names.

When the user next logs on to the computer, they will find that their access rights to Sophos Endpoint Security and Control have changed.

Notes
• To open Computer Management, click Start, and then click Control Panel. Double-click Administrative Tools, and then double-click Computer Management.
• To remove the user from a Sophos user group, on the Member Of tab, select the group in Member of, and then click Remove.

4.3 Configure user rights for Quarantine manager

If you are a member of the SophosAdministrator group, you can configure the user rights for Quarantine manager.
1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > User rights for Quarantine manager.
2. Select the user type that may perform each type of action.
**Note**  
With the exception of the **Authorize** option, the rights you set here apply only to **Quarantine manager**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clean up sectors</strong></td>
<td>Users can clean up floppy disk boot sectors.</td>
</tr>
<tr>
<td><strong>Clean up files</strong></td>
<td>Users can clean up documents and programs.</td>
</tr>
<tr>
<td><strong>Delete files</strong></td>
<td>Users can delete infected files.</td>
</tr>
<tr>
<td><strong>Move files</strong></td>
<td>Users can move infected files to another folder.</td>
</tr>
<tr>
<td><strong>Authorize</strong></td>
<td>Users can authorize suspicious items, adware, and PUAs in order to allow them to run on the computer. This option applies to both <strong>Authorization manager</strong> and <strong>Quarantine manager</strong>.</td>
</tr>
</tbody>
</table>
5 Sophos Anti-Virus

5.1 About on-access and on-demand scanning

On-access scanning

On-access scanning is your main method of protection against viruses and other threats. Whenever you open, save, copy or rename a file, Sophos Anti-Virus scans the file and grants access to it only if it does not pose a threat to your computer or has been authorized for use. For more information, see Configure on-access scanning (page 7).

On-demand scanning

On-demand scans provide additional protection. As the name suggests, you initiate an on-demand scan. You can scan anything from a single file to your entire computer. For more information, see Types of on-demand scan (page 12).

5.2 On-access scanning

5.2.1 About on-access scanning best practice

This section contains recommendations to help you get the best from on-access scanning. We recommend that you use the default on-access scan settings, as they represent the best balance between protecting your computer against threats and overall system performance. For information about the recommended on-access scan settings, see Sophos support knowledgebase article 114345 (http://www.sophos.com/en-us/support/knowledgebase/114345.aspx).

5.2.2 Configure on-access scanning

CAUTION

On-access scanning may not detect viruses if certain encryption software is installed. Change the startup processes to ensure that files are decrypted when on-access scanning begins. For more information on how to use anti-virus and HIPS policy with encryption software, see Sophos support knowledgebase article 12790 http://www.sophos.com/en-us/support/knowledgebase/12790.aspx.
**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

By default, Sophos Anti-Virus detects and cleans up the following threats during an on-access scan:

- viruses
- Trojans
- worms
- spyware

To configure on-access scanning:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning**.
2. To change when on-access scanning occurs, under **Check files on**, set the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>Scan files when they are copied, moved, or opened.</td>
</tr>
<tr>
<td>Rename</td>
<td>Scan files when they are renamed.</td>
</tr>
<tr>
<td>Write</td>
<td>Scan files when they are saved or created.</td>
</tr>
</tbody>
</table>

3. Under **Scan for**, set the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware and PUAs</td>
<td>Adware displays advertising (for example, pop-up messages) that may affect user productivity and system efficiency. PUAs (Potentially Unwanted Applications) are not malicious, but are generally considered unsuitable for business networks.</td>
</tr>
<tr>
<td>Suspicious files</td>
<td>Suspicious files exhibit a combination of characteristics that are commonly, but not exclusively, found in viruses.</td>
</tr>
</tbody>
</table>

4. Under **Other scanning options**, set the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow access to drives with infected boot sectors</td>
<td>Turn on this option to allow access to an infected bootable removable medium or device such as a bootable CD, floppy disk, or USB flash drive. Use this option only if advised to by Sophos technical support. See also the Troubleshooting topic Allow access to drives with infected boot sectors (page 89).</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Scan all files</td>
<td>We recommend that you leave this option turned off, as it will affect computer performance adversely. You should scan all files only during a weekly scan.</td>
</tr>
<tr>
<td>Scan inside archive files</td>
<td>Turn on this option to scan the contents of archives or compressed files. You need to do this only if you download and distribute such files without extracting the contents.</td>
</tr>
<tr>
<td></td>
<td>We recommend that you leave this option turned off, as it makes scanning significantly slower.</td>
</tr>
<tr>
<td></td>
<td>You will still be protected against any threats in archives or compressed files, as any components of an archive or compressed file that may be malware will be blocked by on-access scanning:</td>
</tr>
<tr>
<td></td>
<td>• When you open a file extracted from the archive file, the extracted file is scanned.</td>
</tr>
<tr>
<td></td>
<td>• Files compressed with dynamic compression utilities such as PKLite, LZEXE, and Diet are scanned.</td>
</tr>
<tr>
<td>Scan system memory</td>
<td>Turn on this option to automatically run an hourly background scan that detects malware hiding in the computer’s system memory (the memory that is used by the operating system).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This option is available only on 32-bit operating systems.</td>
</tr>
</tbody>
</table>

### 5.2.3 Temporarily disable on-access scanning

If you are a member of the SophosAdministrator group, you may need to temporarily disable on-access scanning for maintenance or troubleshooting, and then re-enable it. You can disable on-access protection and still run on-demand scans on your computer.

Sophos Endpoint Security and Control retains the settings you make here, even after you restart your computer. If you disable on-access scanning, your computer is unprotected until you re-enable it.

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning.
2. Clear the Enable on-access scanning for this computer check box.
5.2.4 Configure on-access cleanup

Important
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

To configure on-access cleanup:
1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning.
2. Click the Cleanup tab.
3. To automatically clean up infected items, under Viruses/spyware, select the Automatically clean up items that contain virus/spyware check box.

Note
If you turn on this option, cleaning up some viruses/spyware will trigger a full system scan, which tries to clean up all the viruses on your computer. This might take a long time.

4. Under Viruses/spyware, select an action for Sophos Anti-Virus to take against infected items if you have disabled automatic cleanup, or if automatic cleanup fails:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access only</td>
<td>Sophos Anti-Virus asks you what to do before continuing.</td>
</tr>
<tr>
<td></td>
<td>This is the default setting.</td>
</tr>
<tr>
<td>Delete</td>
<td>Use these settings only if advised to by Sophos technical support.</td>
</tr>
<tr>
<td>Deny access and move to</td>
<td>Otherwise, use Quarantine Manager to clean your computer of viruses/spyware found by Sophos Anti-Virus. See .</td>
</tr>
</tbody>
</table>

5. Under Suspicious files, select an action for Sophos Anti-Virus to take when it finds files containing code that is commonly used in malware:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny access</td>
<td>Sophos Anti-Virus asks you what to do before continuing.</td>
</tr>
<tr>
<td></td>
<td>This is the default setting.</td>
</tr>
<tr>
<td>Delete</td>
<td>Use these settings only if advised to by Sophos technical support.</td>
</tr>
<tr>
<td>Deny access and move to</td>
<td>Instead, use Quarantine Manager to clean your computer of suspicious files found by Sophos Anti-Virus. See Deal with viruses/spyware in quarantine (page 35).</td>
</tr>
</tbody>
</table>
5.2.5 Reset scanned file checksums

The list of scanned file checksums is reset when a Sophos Anti-Virus update occurs, or when you restart your computer. The list is then rebuilt with new data as files are scanned by Sophos Anti-Virus.

You can reset the list of scanned file checksums from within Sophos Endpoint Security and Control if you do not want to restart your computer.

To reset scanned file checksums:
1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning.
2. On the Scanning tab, click Purge cache.

5.2.6 Specify on-access scanning file extensions

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

You can specify which file extensions are scanned during on-access scanning.

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning.
2. Click the Extensions tab, set the options as described below.

**Scan all files**
Click this to enable scanning of all files, regardless of the filename extension.

**Allow me to control exactly what is scanned**
Click this to restrict scanning to only files with a particular filename extension, specified in the extension list.

**CAUTION**
The extension list includes file types that we recommend are scanned. Be careful if you alter the list as explained below.

To add a filename extension to the list, click Add. You can use the wildcard ? to match any single character.

To remove a filename extension from the list, select the extension and click Remove.

To change a filename extension in the list, select the extension and click Edit.

When you select Allow me to control exactly what is scanned, Scan files with no extension is selected by default. To disable scanning of files with no filename extension, deselect Scan files with no extension.
5.3 On-demand scanning

5.3.1 Types of on-demand scan

Right-click scan
Scan a file, folder, or drive in Windows Explorer at any time.
• Run a right-click scan (page 15)

Custom scan
Scan specific sets of files or folders. You can either manually run a custom scan or schedule it to run unattended.
• Run a custom scan (page 19)
• Schedule a custom scan (page 19)

Full computer scan
Scan your entire computer, including the boot sector and system memory, at any time.
• Run a full computer scan (page 20)

5.3.2 Specify on-demand scanning file extensions

Important
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

You can specify which file extensions are scanned during on-demand scanning.
1. On the Configure menu, click On-demand extensions and exclusions.
2. Click the Extensions tab, set the options as described below.

   Scan all files
   Click this to enable scanning of all files, regardless of the filename extension.

   Allow me to control exactly what is scanned
   Click this to restrict scanning to only files with a particular filename extension, specified in the extension list.

CAUTION
The extension list includes file types that we recommend are scanned. Be careful if you alter the list as explained below.
To add a filename extension to the list, click **Add.** You can use the wildcard `?` to match any single character.

To remove a filename extension from the list, select the extension and click **Remove.**

To change a filename extension in the list, select the extension and click **Edit.**

When you select **Allow me to control exactly what is scanned,** **Scan files with no extension** is selected by default. To disable scanning of files with no filename extension, deselect **Scan files with no extension.**

### 5.3.3 Right-click scanning

#### Configure right-click scanning

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it will **not** override any changes you make here.

By default, Sophos Anti-Virus detects and cleans up the following threats during a right-click scan:

- viruses
- Trojans
- worms
- spyware
- adware and other Potentially Unwanted Applications (PUAs)

To configure right-click scanning:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Right-click scanning.**
2. Under **Scan for,** set the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware and PUAs</td>
<td>Adware displays advertising (for example, pop-up messages) that may affect user productivity and system efficiency. PUAs (Potentially Unwanted Applications) are not malicious, but are generally considered unsuitable for business networks.</td>
</tr>
<tr>
<td>Suspicious files</td>
<td>Suspicious files exhibit a combination of characteristics that are commonly, but not exclusively, found in viruses.</td>
</tr>
</tbody>
</table>

3. Under **Other scanning options,** set the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan all files</td>
<td>We recommend that you leave this option turned off, as it will affect computer performance adversely. You should scan all files only during a weekly scan.</td>
</tr>
</tbody>
</table>
### Option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Scan inside archive files             | Turn on this option to scan the contents of archives or compressed files. You need to do this only if you download and distribute such files without extracting the contents. We recommend that you leave this option turned off, as it makes scanning significantly slower. You will still be protected against any threats in archives or compressed files, as any components of an archive or compressed file that may be malware will be blocked by on-access scanning:  
• When you open a file extracted from the archive file, the extracted file is scanned.  
• Files compressed with dynamic compression utilities such as PKLite, LZEXE, and Diet are scanned. |

---

**Configure right-click cleanup**

Sophos Endpoint Security and Control

To configure right-click cleanup:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Right-click scanning**.
2. Click the **Cleanup** tab.
3. To automatically clean up infected items, under **Viruses/spyware**, select the **Automatically clean up items that contain virus/spyware** check box.
4. Select an action for Sophos Anti-Virus to take against infected items if you have not enabled automatic cleanup, or if automatic cleanup fails:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log only</td>
<td>Sophos Anti-Virus takes no action other than recording the infected items in the scanning log. See <a href="#">View the scanning log</a> (page 44). This is the default setting.</td>
</tr>
<tr>
<td>Delete</td>
<td>Use these settings only if advised to by Sophos technical support. Otherwise, use Quarantine Manager to clean your computer of viruses/spyware found by Sophos Anti-Virus. See <a href="#">Deal with viruses/spyware in quarantine</a> (page 35).</td>
</tr>
</tbody>
</table>

5. Under **Suspicious files**, select an action for Sophos Anti-Virus to take when it finds files containing code that is commonly used in malware:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log only</td>
<td>Sophos Anti-Virus takes no action other than recording the infected items in the scanning log.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>This is the default setting.</td>
</tr>
<tr>
<td>Delete</td>
<td>Use these settings only if advised to by Sophos technical support. Otherwise, use Quarantine Manager to clean your computer of viruses/spyware found by Sophos Anti-Virus. See Deal with viruses/spyware in quarantine (page 35).</td>
</tr>
<tr>
<td>Move to</td>
<td></td>
</tr>
</tbody>
</table>

6. To remove all known components of adware and Potentially Unwanted Applications (PUAs) from the computer for all users, under Adware and PUAs, select the Automatically clean up adware and PUAs check box. Cleanup does not repair any changes the adware or PUA has already made.
   - For information about viewing details on the Sophos website of the adware or PUA’s side-effects, see Get cleanup information (page 40).
   - For information about cleaning your computer from adware and PUAs using Quarantine Manager, see Deal with adware and PUAs in quarantine (page 36).

**Run a right-click scan**

You can scan files, folders and drives from Windows Explorer or the desktop by running a right-click scan.

1. Using Windows Explorer, or on the desktop, select the file, folder or disk drive you want to scan. You can select multiple files and folders.
2. Right-click the selection, and then click Scan with Sophos Anti-Virus.

If any threats or controlled applications are found, click More, and then refer to the Managing quarantine items section of this Help file.

**5.3.4 Custom scans**

**Create a custom scan**

1. On the Home page, under Anti-virus and HIPS, click Scans. For information about the Home page, see About the Home page (page 3).
2. Click Set up a new scan.
3. In the Scan name box, type a name for the scan.
4. In the Items to scan panel, select the drives and folders you want to scan. To do this, select the check box to the left of each drive or folder. To learn about the icons that appear in the check boxes, refer to Representation of items to scan (page 16).

**Note**

Drives or folders that are unavailable (because they are offline or have been deleted) are displayed in a strikethrough font. They are removed from the Items to scan panel if they are deselected or if there is a change in the selection of their parent drive or folder(s).

5. To configure the scan further, click Configure this scan. (Refer to for more information.)
6. To schedule the scan, click **Schedule this scan**. (Refer to **Configure a custom scan** [page 16] for more information.)

7. Click **Save** to save the scan or **Save and start** to save and run the scan.

**Representation of items to scan**

In the **Items to scan** panel, different icons are displayed in the check box next to each item (drive or folder), depending on which items will be scanned. These icons are shown below with explanations.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>The item and all sub-items <em>are not</em> selected for scanning.</td>
</tr>
<tr>
<td>✓</td>
<td>The item and all sub-items <em>are</em> selected for scanning.</td>
</tr>
<tr>
<td>✔</td>
<td>The item is partially selected: the item is not selected, but some sub-items are selected for scanning.</td>
</tr>
<tr>
<td>✗</td>
<td>The item and all sub-items are excluded from this particular scan.</td>
</tr>
<tr>
<td>✔</td>
<td>The item is partially excluded: the item is selected, but some sub-items are excluded from this particular scan.</td>
</tr>
<tr>
<td>✗</td>
<td>The item and all sub-items are excluded from all on-demand scans, because of an on-demand exclusion that has been set up. For information, see <strong>Exclude items from on-access scanning</strong> [page 21].</td>
</tr>
</tbody>
</table>

**Configure a custom scan**

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

By default, Sophos Anti-Virus detects and cleans up the following threats during a custom scan:

- viruses
- Trojans
- worms
- spyware
- adware and other Potentially Unwanted Applications (PUAs)
- rootkits

To configure a custom scan:

1. On the **Home** page, under **Anti-virus and HIPS**, click **Scans**. For information about the **Home** page, see **About the Home page** [page 3].
2. In the **Available scans** list, select the scan you want to edit, and then click **Edit**.
3. Click **Configure this scan**.
4. Under **Scan for**, set the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adware and PUAs</td>
<td>Adware displays advertising (for example, pop-up messages) that may affect user productivity and system efficiency.</td>
</tr>
</tbody>
</table>
## Option Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PUAs (Potentially Unwanted Applications) are not malicious, but are generally considered unsuitable for business networks.</td>
<td></td>
</tr>
<tr>
<td>Suspicious files</td>
<td>Suspicious files exhibit a combination of characteristics that are commonly, but not exclusively, found in viruses.</td>
</tr>
<tr>
<td>Rootkits</td>
<td>If you are a member of the SophosAdministrator group, scanning for rootkits is always carried out when you run a full computer scan. You can also scan for rootkits as part of a custom scan.</td>
</tr>
</tbody>
</table>

### 5. Under **Other scanning options**, set the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan all files</td>
<td>We recommend that you scan all files only during a weekly scan, as scanning all files will affect computer performance adversely.</td>
</tr>
</tbody>
</table>
| Scan inside archive files   | Turn on this option to scan the contents of archives or compressed files. You need to do this only if you download and distribute such files without extracting the contents. We recommend that you leave this option turned off, as it makes scanning significantly slower. You will still be protected against any threats in archives or compressed files, as any components of an archive or compressed file that may be malware will be blocked by on-access scanning:  
  • When you open a file extracted from the archive file, the extracted file is scanned.  
  • Files compressed with dynamic compression utilities such as PKLite, LZEXE, and Diet are scanned. |
| Scan system memory          | Turn on this option to automatically run an hourly background scan that detects malware hiding in the computer's system memory (the memory that is used by the operating system).  
  **Note**  
  This option is available only on 32-bit operating systems. |
| Run scan at lower priority  | On Windows Vista and above, run the custom scan with lower priority so that it has minimal impact on user applications. |
Configure cleanup for a custom scan

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

To configure cleanup for a custom scan:

1. In the **Available scans** list, select the scan you want to edit, and then click **Edit**.
2. Click **Configure this scan**.
3. Click the **Cleanup** tab.
4. To automatically clean up infected files, under **Viruses/spyware**, select the **Automatically clean up files that contain virus/spyware** check box.
5. Select an action for Sophos Anti-Virus to take against infected items if you have not enabled automatic cleanup, or if automatic cleanup fails:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log only</td>
<td>Sophos Anti-Virus takes no action other than recording the infected items in the log for the custom scan. See <a href="#">View the scanning log</a> (page 44).</td>
</tr>
<tr>
<td></td>
<td>This is the default setting.</td>
</tr>
<tr>
<td>Delete</td>
<td>Use these settings only if advised to by Sophos technical support. Once advised, use Quarantine Manager to clean your computer of viruses/spyware.</td>
</tr>
<tr>
<td>Move to</td>
<td>Otherwise, use Quarantine Manager to clean your computer of viruses/spyware found by Sophos Anti-Virus. See <a href="#">Deal with adware and PUAs in quarantine</a> (page 36).</td>
</tr>
</tbody>
</table>

6. Under **Suspicious files**, select an action for Sophos Anti-Virus to take when it finds files containing code that is commonly used in malware:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log only</td>
<td>Sophos Anti-Virus takes no action other than recording the infected items in the scanning log.</td>
</tr>
<tr>
<td></td>
<td>This is the default setting.</td>
</tr>
<tr>
<td>Delete</td>
<td>Use these settings only if advised to by Sophos technical support. Once advised, use Quarantine Manager to clean your computer of viruses/spyware.</td>
</tr>
<tr>
<td>Move to</td>
<td>Otherwise, use Quarantine Manager to clean your computer of viruses/spyware found by Sophos Anti-Virus. See <a href="#">Get cleanup information</a> (page 40).</td>
</tr>
</tbody>
</table>

7. To remove all known components of adware and Potentially Unwanted Applications (PUAs) from the computer for all users, under **Adware and PUAs**, select the **Automatically clean up adware and PUAs** check box.

Cleanup does not repair any changes the adware or PUA has already made.
Sophos Endpoint Security and Control Help

- For information about viewing details on the Sophos website of the adware or PUA’s side-effects, see Get cleanup information (page 40).
- For information about cleaning your computer from adware and PUAs using Quarantine Manager, see Deal with adware and PUAs in quarantine (page 36).

Schedule a custom scan

If you are a member of the SophosAdministrator group, you can schedule a custom scan, or view and edit scheduled scans created by other users.

1. On the Home page, under Anti-virus and HIPS, click Scans.
   For information about the Home page, see About the Home page (page 3).
2. In the Available scans list, select the scan you want to edit, and then click Edit.
3. Click Schedule this scan.
4. In the Schedule scan dialog box, select Enable schedule.
   Select the day(s) on which the scan should run.
   Add the time(s) by clicking Add.
   If necessary, remove or edit a time by selecting it and clicking Remove or Edit, respectively.
5. Type the user name and password. Make sure that the password is not blank.
   The scheduled scan runs with the access rights of that user.

Note
If the scan detects components of a threat in memory, and you have chosen not to automatically clean up viruses/spyware for the scan, the scan stops. This is because further scanning could enable the threat to spread. You must clean up the threat before running the scan again.

Run a custom scan

Note
You cannot manually run scheduled custom scans. Scheduled scans are displayed in the Available scans list with a clock icon.

1. On the Home page, under Anti-virus and HIPS, click Scans.
   For information about the Home page, see About the Home page (page 3).
2. In the Available scans list, select the scan you want to run, and then click Start.
   A progress dialog box is displayed and the Activity summary panel appears in the Sophos Endpoint Security and Control window.

Note
If the scan detects components of a threat in memory, and you have chosen not to automatically clean up viruses/spyware for the scan, the scan stops. This is because further scanning could enable the threat to spread. You must clean up the threat before running the scan again.

If any threats or controlled applications are found, click More and refer to Managing quarantine items.
**Rename a custom scan**

1. On the Home page, under Anti-virus and HIPS, click Scans.
   - For information about the Home page, see About the Home page (page 3).
2. In the Available scans list, select the scan you want to edit, and then click Edit.
3. In the Scan name box, type the new name for the scan.

**View the log for a custom scan**

1. On the Home page, under Anti-virus and HIPS, click Scans.
   - For information about the Home page, see About the Home page (page 3).
2. In the Available scans list, click Summary for the custom scan.
3. In the Summary dialog box, click the link at the bottom.
   - From the log page, you can copy the log to the clipboard, or email, or print the log.
   - To find specific text in the log, click Find and enter the text you want to find.

**View the summary of a custom scan**

1. On the Home page, under Anti-virus and HIPS, click Scans.
   - For information about the Home page, see About the Home page (page 3).
2. In the Available scans list, click Summary for the custom scan.

**Delete a custom scan**

1. On the Home page, under Anti-virus and HIPS, click Scans.
   - For information about the Home page, see About the Home page (page 3).
2. In the Available scans list, select the scan you want to delete, and then click Delete.

**5.3.5 Run a full computer scan**

To scan your entire computer system, including the boot sector and system memory:

- On the Home page, under Anti-virus and HIPS, click Scan my computer.
  - For information about the Home page, see About the Home page (page 3).

A progress dialog box is displayed and the Activity summary appears in the Sophos Endpoint Security and Control window.

**Note**

If the scan detects components of a threat in memory, the scan stops. This is because further scanning could enable the threat to spread. You must clean up the threat before running the scan again.

If any threats or controlled applications are found, click More and refer to the Managing quarantine items section.
5.4 Excluding items from scanning

5.4.1 Exclude items from on-access scanning

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

To edit the list of files, folders, and drives that are excluded from on-access scanning:

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning.
2. Click the Exclusions tab, and then choose one of the following options.
   - To specify a file, folder, or drive that should be excluded from on-access scanning, click Add.
   - To delete an exclusion, click Remove.
   - To change an exclusion, click Edit.
3. To add or edit an excluded item, in the Exclude item dialog box, select the Item type. The All remote files item type is for excluding files that are not stored on local drives. You might select this if you want to increase speed of access to such files and you trust the available remote file locations.
4. Specify the Item name by using the Browse button or typing in the text box.

**Note**
If you work on a 64-bit platform, the Browse button will not be visible in the Exclude item dialog.

For more information on specifying item names, see Exclude items from on-access scanning (page 21).

5.4.2 Exclude items from on-demand scanning

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

The procedure described below applies to all on-demand scans. For information on excluding specific items from a custom scan, see Create a custom scan (page 15).

To edit the list of files, folders, and drives that are excluded from on-demand scanning:

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-demand extensions and exclusions.
2. Click the Exclusions tab, and then choose one of the following options.
   - To specify a file, folder, or drive that should be excluded from on-demand scanning, click Add.
   - To delete an exclusion, click Remove.
   - To change an exclusion, click Edit.
3. To add or edit an excluded item, in the **Exclude item** dialog box, select the **Item type**.

4. Specify the **Item name** by using the **Browse** button or typing in the text box.

**Note**

If you work on a 64-bit platform, the **Browse** button will not be visible in the **Exclude item** dialog.

For more information on specifying item names, see **Exclude items from on-access scanning** (page 21).

### 5.4.3 Specify scanning exclusions

#### Standard naming conventions

Sophos Anti-Virus validates the paths and file names of scanning exclusion items against standard Windows naming conventions. For example, a folder name may contain spaces but may not contain *only* spaces.

#### Multiple file extensions

File names with multiple extensions are treated as if the last extension is the extension and the rest are part of the file name:

```
MySample.txt.doc = file name MySample.txt + extension .doc.
```

#### Excluding specific files, folders, processes, or drives

<table>
<thead>
<tr>
<th>Exclusion type</th>
<th>Description</th>
<th>Examples</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specific file</td>
<td>Specify both the path and file name to exclude a specific file. The path can include a drive letter or network share name.</td>
<td>C:\Documents\CV.doc \Server\Users \Documents \CV.doc</td>
<td>To make sure that exclusions are always applied correctly, add both the long and 8.3-compliant file and folder names: C:\Program Files \Sophos\Sophos Anti-Virus C:\Progra-1\Sophos \Sophos-1 For more information, see knowledgebase article 13045.</td>
</tr>
<tr>
<td>Specific process</td>
<td>Specify both the path and the file name to exclude a specific executable file (process).</td>
<td>C:\Windows \notepad.exe</td>
<td>You must specify the full path.</td>
</tr>
<tr>
<td>All files with the same name</td>
<td>Specify a file name without a path to exclude all files with that name wherever they are located in the file system.</td>
<td>spacer.gif</td>
<td></td>
</tr>
</tbody>
</table>
## Exclusions

<table>
<thead>
<tr>
<th>Exclusion type</th>
<th>Description</th>
<th>Examples</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everything on a drive or network share</td>
<td>Specify a drive letter or network share name to exclude everything on that drive or network share.</td>
<td>C:\Server &lt;sharename&gt;\</td>
<td>When you specify a network share, include a trailing slash after the share name.</td>
</tr>
<tr>
<td>Specific folder</td>
<td>Specify a folder path including a drive letter or network share name to exclude everything in that folder and below.</td>
<td>D:\Tools\logs\</td>
<td>Include a trailing slash after the folder name.</td>
</tr>
<tr>
<td>All folders with the same name</td>
<td>Specify a folder path without a drive letter or network share name to exclude everything from that folder and below on any drive or network share.</td>
<td>\Tools\logs\ [excludes the following folders: C:\Tools\logs, \Server\Tools\logs]</td>
<td>You must specify the entire path up to the drive letter or network share name. In this example, specifying \logs\ would not exclude any files.</td>
</tr>
</tbody>
</table>

### Wildcards

You can use the wildcards shown in this table.

**Note**

Only * and ? can be used on Windows Server 2003.

<table>
<thead>
<tr>
<th>Token</th>
<th>Matches</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>* [Star]</td>
<td>Zero or more of any character except \ or /.</td>
<td>For example: c:***.txt excludes all files named *.txt in the top level folders on C:.</td>
</tr>
</tbody>
</table>
| ** [Star Star] | Zero or more of any characters including \ and /, when bracketed by \ or / characters or used at the start or end of an exclusion. Any other use of ** is treated a single * and matches zero or more of any character except \ or /.. | For example:  
  - c:\foo\**\bar matches: c:\foo \bar, c:\foo\more\bar, c:\foo\even\more\bar  
  - **\bar matches: c:\foo\bar  
  - c:\foo\** matches: c:\foo\more \bar  
  - c:\foo**\bar matches: c:\foo\more\bar but NOT c:\foo\more\bar |
| \ (Backslash) | Either \ or /.                                                            |                                                                                                      |
| / (Forward slash) | Either / or \.                                                           |                                                                                                      |
| ? (Question mark) | One single character, unless at the end of a string where it can match zero characters. |                                                                                                      |
Examples

Here are some examples of the use of wildcards.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Interpreted as</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>foo</td>
<td>**\foo</td>
<td>Exclude any file named foo (in any location).</td>
</tr>
<tr>
<td>foo\bar</td>
<td>**\foo\bar</td>
<td>Exclude any file named bar in a folder named foo (in any location).</td>
</tr>
<tr>
<td>*.txt</td>
<td>***.txt</td>
<td>Exclude all files named *txt (in any location).</td>
</tr>
<tr>
<td>C:</td>
<td>C:</td>
<td>Exclude drive C: from scanning (including the drive's master boot record).</td>
</tr>
<tr>
<td>C:\</td>
<td>C:\</td>
<td>Exclude all files on drive C: from scanning (but scan the drive's master boot record).</td>
</tr>
<tr>
<td>C:\foo\</td>
<td>C:\foo\</td>
<td>All files and folders underneath C: \foo, including C:\foo itself.</td>
</tr>
<tr>
<td>C:\foo*.txt</td>
<td>C:\foo*.txt</td>
<td>All files contained in C:\foo named *.txt.</td>
</tr>
</tbody>
</table>

Variables for exclusions

You can use variables when you set up scanning exclusions.

The table below shows the variables and examples of the locations they correspond to on each operating system.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Windows 7 or later, Windows Server 2008 or later</th>
<th>Windows Server 2003, Windows XP, Windows Vista</th>
</tr>
</thead>
<tbody>
<tr>
<td>%allusersprofile%\</td>
<td>C:\ProgramData\</td>
<td>C:\Documents and Settings\All Users\</td>
</tr>
<tr>
<td>%appdata%\</td>
<td>C:\Users*\AppData\Roaming\</td>
<td>C:\Documents and Settings* Application Data\</td>
</tr>
<tr>
<td>%commonprogramfiles%\</td>
<td>C:\Program Files\Common Files\</td>
<td>C:\Program Files\Common Files\</td>
</tr>
<tr>
<td>%commonprogramfiles(x86)%\</td>
<td>C:\Program Files (x86)\Common Files\</td>
<td>C:\Program Files (x86)\Common Files\</td>
</tr>
<tr>
<td>%localappdata%\</td>
<td>C:\Users*\AppData\Local\</td>
<td>C:\Documents and Settings* Local Settings\Application Data\</td>
</tr>
<tr>
<td>%programdata%\</td>
<td>C:\ProgramData\</td>
<td>C:\Documents and Settings\All Users\Application Data\</td>
</tr>
</tbody>
</table>
5.5 Sophos Behavior Monitoring

5.5.1 About behavior monitoring

As part of on-access scanning, Sophos Behavior Monitoring protects Windows computers from unidentified or “zero-day” threats and suspicious behavior.

Runtime detection can intercept threats that cannot be detected before execution. Behavior monitoring uses the following runtime detection methods to intercept threats:

• Malicious and suspicious behavior detection
• Buffer overflow detection

Malicious and suspicious behavior detection

Suspicious behavior detection uses Sophos’s Host Intrusion Prevention System (HIPS) to dynamically analyze the behavior of all programs running on the computer to detect and block activity that appears to be malicious. Suspicious behavior may include changes to the registry that could allow a virus to run automatically when the computer is restarted.

Suspicious behavior detection watches all system processes for signs of active malware, such as suspicious writes to the registry or file copy actions. It can be set to warn the administrator and/or block the process.

Malicious behavior detection dynamically analyses all programs running on the computer to detect and block activity that is known to be malicious.

Buffer overflow detection

Buffer overflow detection is important for dealing with zero-day exploits.

It dynamically analyzes the behavior of programs running on the system in order to detect when an attempt is made to exploit a running process using buffer overflow techniques. It will catch attacks targeting security vulnerabilities in both operating system software and applications.
5.5.2 Enable behavior monitoring

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you are a member of the SophosAdministrator group, you can enable behavior monitoring.

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Behavior monitoring**.
2. In the **Configure Behavior Monitoring** dialog box, select the **Enable behavior monitoring** check box.

5.5.3 Block malicious behavior

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

Malicious behavior detection is the dynamic analysis of all programs running on the computer to detect and block activity that is known to be malicious.

If you are a member of the SophosAdministrator group, you can change the settings for detecting and reporting malicious behavior:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Behavior monitoring**.
2. In the **Configure Behavior Monitoring** dialog box, select the **Enable behavior monitoring** check box.
3. To alert the administrator and block malicious behavior, select the **Detect malicious behavior** check box.

5.5.4 Prevent suspicious behavior

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

Suspicious behavior detection watches all system processes for signs of active malware, such as suspicious writes to the registry or file copy actions. It can be set to warn the administrator and/or block the process.

If you are a member of the SophosAdministrator group, you can change the settings for detecting and reporting suspicious behavior:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Behavior monitoring**.
2. In the **Configure Behavior Monitoring** dialog box, select the **Enable behavior monitoring** check box.
3. Select the Detect malicious behavior check box.

4. To alert the administrator and block suspicious processes, select the Detect suspicious behavior check box.

5. To alert the administrator, but not block suspicious processes, select the Alert only, do not block suspicious behavior check box.

For the strongest protection, we advise you to scan for suspicious files. For more information, see the following topics:

- Configure on-access scanning (page 7)
- Configure right-click scanning (page 13)
- Configure a custom scan (page 16)

### 5.5.5 Prevent buffer overflows

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

Buffer overflow detection dynamically analyzes the behavior of programs running on the system in order to detect when an attempt is made to exploit a running process using buffer overflow techniques.

If you are a member of the SophosAdministrator group, you can change the settings for detecting and reporting buffer overflows:

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Behavior monitoring.

2. In the Configure Behavior Monitoring dialog box, select the Enable behavior monitoring check box.

3. To alert the administrator and block buffer overflows, select the Detect buffer overflows check box.

4. To alert the administrator, but not block buffer overflows, select the Alert only, do not block check box.

### 5.6 Sophos Live Protection

#### 5.6.1 About Sophos Live Protection

Sophos Live Protection decides whether a suspicious file is a threat and, if it is a threat, takes immediate action as specified in the Sophos Anti-Virus cleanup configuration.

Sophos Live Protection improves detection of new malware without the risk of unwanted detections. This is achieved by doing an instant lookup against the very latest known malware. When new malware is identified, Sophos can send out updates within seconds.

Sophos Live Protection uses the following options:

- **Enable Live Protection**

  If the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on
the computer, certain file data (such as its checksum and other attributes) is sent to Sophos to assist with further analysis.

The in-the-cloud checking performs an instant lookup of a suspicious file in the SophosLabs database. If the file is identified as clean or malicious, the decision is sent back to the computer and the status of the file is automatically updated.

- **Automatically send sample files to Sophos**

  If a file is considered suspicious, but cannot be positively identified as malicious based on the file data alone, you can allow Sophos to request a sample of the file. If this option is enabled, and Sophos does not already hold a sample of the file, the file will be submitted automatically.

  Submitting sample files helps Sophos to continuously enhance detection of malware without the risk of false positives.

### 5.6.2 Turn Sophos Live Protection options on or off

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you are a member of the SophosAdministrator group, you can turn the Sophos Live Protection options on or off:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Sophos Live Protection**.
2. In the **Sophos Live Protection** dialog box:
   - To turn the sending of file data to Sophos on or off, select or clear the **Enable Live Protection** check box.
   - To turn the sending of file samples to Sophos on or off, select or clear the **Automatically send sample files to Sophos** check box.

   This option is available only if you have already selected **Enable Live Protection**.

**Note**

When a file sample is sent to Sophos for online scanning, the file data is always sent with the sample.

### 5.6.3 View the log for Sophos Live Protection

The file data sent to Sophos for online scanning and file status updates after the scanning is complete are recorded in the scanning log for this computer.

If Sophos Live Protection is enabled, the log shows:

- The path of each file for which data was sent to Sophos.
- The time when the data was sent.
- The reason for failure (if known) if sending the data failed.
- The current status of the file (for example, "virus/spyware" if the file has been identified as malicious).

To view the scanning log:
On the Home page, under Anti-virus and HIPS, click View anti-virus and HIPS log. For information about the Home page, see About the Home page (page 3). From the log page, you can copy the log to the clipboard, or email, or print the log. To find specific text in the log, click Find and enter the text you want to find.

5.7 Sophos Web Protection

5.7.1 About Sophos Web Protection

Sophos Web Protection provides enhanced protection against web threats. It includes the following features:

- Live URL filtering
- Scanning of downloaded content
- Checking of the reputation of downloaded files

Live URL filtering

Live URL filtering blocks access to websites that are known to host malware. This feature works by performing a real-time lookup against Sophos’s online database of infected websites.

When access to a malicious website is blocked, the event is recorded in the scanning log. For information about viewing the scanning log, see View the scanning log (page 44).

Content scanning

Content scanning scans data and files downloaded from the internet (or intranet) and proactively detects malicious content. This feature scans content hosted at any location, including locations not listed in the database of infected websites.

Download reputation

Download reputation is calculated based on the file’s age, source, prevalence, deep content analysis and other characteristics.

Note

Download reputation is supported only on Windows 7 and later.

By default, an alert will be displayed when a file with low or unknown reputation is downloaded. We recommend that you do not download such files. If you trust the file’s source and publisher, you can choose to download the file. Your action and the file’s URL will be recorded in the scanning log.
**Note**

Download reputation is calculated based on the data in the SophosLabs’ in-the-cloud database and requires Sophos Live Protection to be enabled in order to perform lookups and obtain the data. (By default, Sophos Live Protection is enabled.)

For more information about download reputation, see knowledgebase article 121319.

### Web protection configuration settings

By default, web protection is enabled: access to malicious websites is blocked, downloaded content is scanned and the reputation of downloaded files is checked.

For more information about the web protection settings and how to change them, see Configure Sophos Web Protection (page 30).

### Supported web browsers

Web protection is supported on the following web browsers:

- Internet Explorer
- Edge
- Google Chrome
- Firefox (except for download reputation)
- Safari (except for download reputation)
- Opera

Web content accessed via an unsupported browser is not filtered and will not be blocked.

## 5.7.2 Configure Sophos Web Protection

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

To change Sophos Web Protection settings:

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Web protection.
2. To block or unblock access to malicious websites, next to Block access to malicious websites, select On or Off. This option is enabled by default. For information on how to authorize a website that is classified as malicious, see Authorize a website for use (page 32).
3. To enable or disable scanning of downloaded data and files, next to Content scanning, select As on-access scanning, On, or Off. By default, As on-access scanning is selected, that is, content scanning is disabled or enabled simultaneously with on-access scanning.
4. To change what happens when a file with low or unknown reputation is downloaded, under Download reputation, next to Action, select either Prompt user (default) or Log only.
If you select **Prompt user**, every time a low reputation file is downloaded, an alert will be displayed, informing about this and asking whether to block or allow the download. We recommend that you do not download such files. If you trust the file’s source and publisher, you can choose to download the file. The choice to block or allow the download and the file’s URL will be recorded in the scanning log.

If you select **Log only**, no alert will be displayed; the download will be allowed and recorded in the scanning log.

5. To choose how rigorous you want reputation scanning to be, next to **Threshold**, select **Recommended** (default) or **Strict**.

   - If you select **Recommended**, an alert will be displayed and/or a log record created every time a file with low or unknown reputation is downloaded.
   - If you select **Strict**, an alert will be displayed and/or a log record created every time a file with low, unknown, or medium reputation is downloaded.

For more information about download reputation, see knowledgebase article 121319.
For information about viewing the scanning log, see View the scanning log (page 44).

### 5.8 Authorizing items for use

#### 5.8.1 Authorize adware and PUAs

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you want to run adware or an application that Sophos Anti-Virus has classified as potentially unwanted, you can authorize it.

To authorize adware and PUAs:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Authorization**.
2. On the **Adware or PUAs** tab, in the **Known adware or PUAs** list, select the adware or PUA.
3. Click **Add**.

The adware or PUA appears in the **Authorized adware or PUAs** list.

**Note**

You can also authorize adware and PUAs in Quarantine manager. For information on how to do this, see Deal with adware and PUAs in quarantine (page 36).

#### 5.8.2 Block authorized adware and PUAs

To prevent currently-authorized adware and PUAs from running on your computer:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Authorization**.
2. On the **Adware or PUAs** tab, in the **Authorized adware or PUAs** list, select the adware or PUA you want to block.
3. Click Remove.

5.8.3 Authorize suspicious items

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you want to allow an item that Sophos Anti-Virus has classified as suspicious, you can authorize it as follows.

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Authorization.
2. Click the tab for the type of item that has been detected (for example, Buffer overflow).
3. In the Known list, select the suspicious item.
4. Click Add.

The suspicious item appears in the Authorized list.

**Note**
You can also authorize suspicious items in Quarantine manager. For information on how to do this, see the following topics:
- Deal with adware and PUAs in quarantine (page 36)
- Deal with suspicious behavior in quarantine (page 38)

5.8.4 Pre-authorize suspicious items

If you want to allow an item that Sophos Endpoint Security and Control has not yet classified as suspicious, you can pre-authorize it.

To pre-authorize a suspicious item:

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Authorization.
2. Click the tab for the type of item that has been detected (for example, Buffer overflow).
3. Click New entry.
4. Locate the suspicious item, and then double-click it.

The suspicious item appears in the Authorized list.

5.8.5 Authorize a website for use

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you want to unblock a website that Sophos has classified as malicious, you can add it to the list of authorized sites. Authorizing a website will prevent URLs from that website being verified with Sophos online web filtering service.
**CAUTION**

Authorizing a website that has been classified as malicious could expose you to threats, so make sure that it is safe to access the website before you authorize it.

To authorize a website for use:

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > Authorization**.
2. Click the **Websites** tab.
3. Click **Add**.
4. Type the domain name or IP address.

The website appears in the **Authorized websites** list.

---

### 5.9 Managing quarantine items

#### 5.9.1 About Quarantine manager

Quarantine manager enables you to deal with the items found by scanning that were not eliminated automatically during scanning. Each item is here for one of the following reasons.

- No cleanup options (clean up, delete, move) were chosen for the type of scan that found the item.
- A cleanup option was chosen for the type of scan that found the item but the option failed.
- The item is multiply-infected and still contains additional threats.
- The threat has only been partially detected, and a full computer scan is needed to fully detect it. To find out how to do this, refer to **Run a full computer scan** (page 20).
- The item exhibits suspicious behavior.
- The item is a controlled application.

**Note**

Adware, PUAs, and multi-component infections detected during on-access scanning are always listed in Quarantine manager. Automatic cleanup of adware, PUAs, and multi-component infections is not available for on-access scanning.

A cleanup option may have failed because of insufficient access rights. If you have greater rights, you can use Quarantine manager to deal with the item(s).

Threats that are detected during web page scanning are not listed in Quarantine manager because the threats are not downloaded to your computer. Therefore, there is no need to take any action.

#### 5.9.2 Quarantine Manager layout

Quarantine Manager lists all the items that have been detected by scanning and enables you to deal with them. The elements of the **Quarantine Manager** window are shown below.
Click the **Show** list to filter the type of items that are displayed.

The identity of the item, including a link to its analysis on the Sophos website.

The file name and location of the item.

If the item is associated with a rootkit, it is displayed as **Hidden**.

If a **more** link is displayed next to the filename, this means that the item is infected with a multi-component infection. Click the link to see the list of other components that are part of the infection. If some components are associated with a rootkit, the dialog box indicates that they are hidden.

The action that you can take to deal with the item.

Unless the item is hidden, there are three actions: **Clean up**, **Delete**, and **Move**.

If you click one of the actions, the action is performed on the item immediately, following confirmation. Hidden files can only be cleaned up.

The list of items that have been detected.

To sort the items, click one of the column headings.

Click **Select all** to perform the same action on all the items.

To deselect an item, clear its check box in the **Type** column.

If you have selected all the items and then want to clear the selection, click **Deselect all**.

To select an item, click its check box in the **Type** column.

Click **Clear from List** to remove selected items from the list without dealing with them.

This action does not delete the items from disk.

Click **Perform action** to display a list of actions that you can perform on the selected items.
5.9.3 Deal with viruses/spyware in quarantine

**Note**

*Virus* here is used to refer to any virus, worm, Trojan, or other malicious software.

1. **On the Home page, under Anti-virus and HIPS, click Manage quarantine items.**
   
   For information about the Home page, see About the Home page (page 3).

2. **In the Show list, click Viruses/spyware.**
   
   Information about each item is shown in the columns.

   - **Name** displays the identity that Sophos Anti-Virus has detected. To learn more about the virus/spyware, click the identity, and Sophos Anti-Virus connects you to the analysis of the virus/spyware on the Sophos website.
   
   - **Details** displays the name and location of the item. If the item is associated with a rootkit, it is displayed as "Hidden". If a more link is displayed next to the filename, this means that the item is infected with a multi-component infection. Click the link to see the list of other components that are part of the infection. If any of the components are associated with a rootkit, the dialog box indicates that some components are hidden.
   
   - **Available actions** displays actions that you can perform on the item. Unless the item is hidden, there are three actions: Clean up, Delete, and Move, described below. If you click one of the actions, the action is performed on the item, following confirmation. Hidden files can only be cleaned up.

**Dealing with the infected items**

To deal with the viruses/spyware, use the buttons described below.

**Select all/Deselect all**

Click these buttons to select or deselect all the items. This enables you to perform the same action on a group of items. To select or deselect a particular item, select the check box to the left of the item type.

**Clear from list**

Click this to remove selected items from the list, if you are sure that they do not contain a virus or spyware. This does not delete the items from disk, however.

**Perform action**

Click this to display a list of actions that you can perform on the selected items.

- Click **Clean up** to remove a virus or item of spyware from the selected items. Cleanup of documents does not repair any side-effects of the virus in the document.

**Note**

To fully clean some viruses/spyware consisting of several components from your computer, or to clean up hidden files, you will need to restart the computer. If this is the case, you will be given an option to restart your computer immediately or later. The final cleanup steps will be performed after the computer is restarted.
Note
Cleanup of some viruses causes a full system scan to be run, which tries to clean up all the viruses. This might take a long time. The available action changes to Cleaning up until the scan has finished.

- Click Delete to delete the selected items from your computer. Use this function with care.
- Click Move to move the selected items to another folder. The items are moved to the folder that was specified when cleanup was set up. Moving an executable file reduces the likelihood of it being run. Use this function with care.

CAUTION
Sometimes, if you delete or move an infected file, your computer may stop working properly because it cannot find the file. Also, an infected file may only be part of a multiple infection, in which case deleting or moving this particular file will not clean the infection from your computer. In this case, contact Sophos technical support to get assistance in dealing with the items.

For information about contacting technical support, see Technical support (page 100).
To configure what action you can perform, refer to Configure user rights for Quarantine manager (page 5).

5.9.4 Deal with adware and PUAs in quarantine

1. On the Home page, under Anti-virus and HIPS, click Manage quarantine items.
   For information about the Home page, see About the Home page (page 3).
2. In the Show list, click Adware or PUAs.

Information about each item is shown in the columns.

Name displays the identity that Sophos Anti-Virus has detected. To learn more about the adware or PUA, click the identity, and Sophos Anti-Virus connects you to the analysis of the adware or PUA on the Sophos website.

Details displays the subtype of the adware or PUA. If the item is associated with a rootkit, it is displayed as “Hidden”. If a more link is displayed next to the subtype, this means that the item is a multi-component item of adware or PUA. Click the link to see the list of other components that are part of the adware or PUA. If any of the components are associated with a rootkit, the dialog box indicates that some components are hidden.

Available actions displays actions that you can perform on the item. There are two actions: Authorize and Clean up, described below. If you click one of the actions, the action is performed on the item, following confirmation.

Dealing with the adware and PUAs

To deal with the adware and PUAs, use the buttons described below.

Select all/Deselect all
Click these buttons to select or deselect all the items. This enables you to perform the same action on a group of items. To select or deselect a particular item, select the check box to the left of the item type.

Clear from list
Click this to remove selected items from the list, if you trust them. This does not delete the items from disk, however.

**Perform action**

Click this to display a list of actions that you can perform on the selected items.

- Click **Authorize** to authorize the selected items on the computer, if you trust them. This adds the items to the list of authorized adware and PUAs so that Sophos Anti-Virus does not prevent them from running on your computer.
- Click **Clean up** to remove all known components of selected items from the computer for all users. To clean adware and PUAs from the computer, you must be a member of both Windows Administrators and SophosAdministrator groups.

**Note**

To fully clean some adware and PUAs consisting of several components from your computer, or to clean up hidden files, you will need to restart the computer. If this is the case, you will be given an option to restart your computer immediately or later. The final cleanup steps will be performed after the computer is restarted.

To configure what actions you can perform, refer to Configure user rights for Quarantine manager (page 5).

To see the list of known and authorized adware and PUAs, click **Configure authorization**.

### 5.9.5 Deal with suspicious files in quarantine

A **suspicious file** is a file that exhibits a combination of characteristics that are commonly, but not exclusively, found in viruses.

1. On the Home page, under **Anti-virus and HIPS**, click **Manage quarantine items**.
   
   For information about the Home page, see **About the Home page** (page 3).

2. In the **Show** list, click **Suspicious files**.

Information about each item is shown in the columns.

**Name** displays the identity that Sophos Anti-Virus has detected. To learn more about the suspicious file, click the identity, and Sophos Anti-Virus connects you to the analysis of the suspicious file on the Sophos website.

**Details** displays the name and location of the item. If the item is associated with a rootkit, it is displayed as “Hidden”.

**Available actions** displays actions that you can perform on the item. Unless the item is hidden, there are three actions: Authorize, Delete and Move, described below. If you click one of the actions, the action is performed on the item, following confirmation. Hidden files can only be authorized.

### Dealing with the suspicious files

To deal with the suspicious files, use the buttons described below.

**Select all/Deselect all**

Click these buttons to select or deselect all the items. This enables you to perform the same action on a group of items. To select or deselect a particular item, select the check box to the left of the item type.
Clear from list
Click this to remove selected items from the list, if you trust them. This does not delete the items from disk, however.

Perform action
Click this to display a list of actions that you can perform on the selected items.

- Click **Authorize** to authorize the selected items on the computer, if you trust them. This adds the items to the list of authorized suspicious items so that Sophos Anti-Virus does not prevent them from being accessed.
- Click **Delete** to delete the selected items from your computer. Use this function with care.
- Click **Move** to move the selected items to another folder. The items are moved to the folder that was specified when cleanup was set up. Moving an executable file reduces the likelihood of it being run. Use this function with care.

**CAUTION**
Sometimes, if you delete or move an infected file, your computer may stop working properly because it cannot find the file.

To configure what actions you can perform, refer to Configure user rights for Quarantine manager (page 5).
To see the list of authorized suspicious files, click **Configure authorization**.

### 5.9.6 Deal with suspicious behavior in quarantine

**Suspicious behavior** is activity that appears to be malicious.

1. On the **Home** page, under **Anti-virus and HIPS**, click **Manage quarantine items**.
   For information about the **Home** page, see About the **Home** page (page 3).
2. In the **Show** list, click **Suspicious behavior**.

Information about each item is shown in the columns.

- **Name** displays the identity that Sophos Anti-Virus has detected. To learn more about the behavior, click the identity, and Sophos Anti-Virus connects you to the analysis of the behavior on the Sophos website.
- **Details** displays the name and location of the item.
- **Available actions** displays actions that you can perform on the item. If you have enabled blocking of suspicious behavior, there is one action: Authorize, described below. If you click the action, the action is performed on the item, following confirmation.

Dealing with the suspicious behavior

To deal with the suspicious behavior, use the buttons described below.

**Select all/Deselect all**
Click these buttons to select or deselect all the items. This enables you to perform the same action on a group of items. To select or deselect a particular item, select the check box to the left of the item type.

**Clear from list**
Click this to remove selected items from the list, if you trust them. This does not delete the items from disk, however.

**Perform action**

Click this to display a list of actions that you can perform on the selected items.

- Click **Authorize** to authorize the selected items on the computer, if you trust them. This adds the items to the list of authorized suspicious items so that Sophos Anti-Virus does not prevent the behavior.

To configure what actions you can perform, refer to [Configure user rights for Quarantine manager](page 5).

To see the list of authorized suspicious behavior, click **Configure authorization**.

### 5.9.7 Deal with controlled applications in quarantine

A *controlled application* is an application that is prevented from running on your computer by your organisation's security policy.

1. On the **Home** page, under Anti-virus and HIPS, click **Manage quarantine items**.
   - For information about the **Home** page, see [About the Home page](page 3).
2. In the **Show** list, click **Controlled applications**.

Information about each item is shown in the columns.

- **Name** displays the identity that Sophos Anti-Virus has detected. To learn more about the controlled application, click the identity, and Sophos Anti-Virus connects you to the analysis of the controlled application on the Sophos website.

- **Details** displays the subtype of the controlled application. If a **more** link is displayed next to the subtype, click it to see the list of other components that are part of the controlled application.

- **Available actions** displays actions that you can perform on the item. However, there are no actions available for controlled applications apart from clearing the item from the list, described below.

#### Dealing with the controlled applications

To deal with the controlled applications, use the buttons described below.

- **Select all/Deselect all**

  Click these buttons to select or deselect all the items. This enables you to perform the same action on a group of items. To select or deselect a particular item, select the check box to the left of the item type.

- **Clear from list**

  Click this to remove selected items from the list. This does not delete the items from disk, however. Controlled applications must be authorized by the central console before you can use them.
5.10 Cleaning up

5.10.1 About cleanup

Cleanup eliminates threats on your computer by doing one of the following:

- Removing the virus/spyware from floppy disk boot sectors, documents, programs, and anything else that is selected for scanning
- Moving or deleting the suspicious file
- Deleting the item of adware or PUA

When Sophos Anti-Virus automatically cleans up items that contain virus/spyware, it will delete any items that are purely malware and will try to disinfect any items that have been infected. These disinfected files should be considered permanently damaged, as the virus scanner cannot know what the file contained before it was damaged.

Cleaning up documents

Cleaning up documents does not repair any side-effects of the virus/spyware in the document. See Get cleanup information (page 40) to find out how to view details on the Sophos website of the virus/spyware's side-effects.

Cleaning up programs

Cleaning up programs should be used only as a temporary measure. You should subsequently replace cleaned programs from the original disks or a clean backup.

Cleaning up web page threats

Cleanup is not required for threats that are detected by web page scanning, because the threats are not downloaded to your computer.

Note

Cleaning up a threat might not be able to undo all the actions the threat has taken on this computer. 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 computer’s configuration. Cleaning up an infected document does not repair any changes the threat has made to the document.

5.10.2 Get cleanup information

When a threat is found on your computer, it is very important that you check the threat analysis on the Sophos website for information on the threat and cleanup advice. You can do this from the following places:

- The desktop alert (on-access scanning)
- The scan progress dialog box (custom and right-click scanning)
- Quarantine manager (all scanning types)

**Get information via the desktop alert**

If on-access scanning is enabled on your computer, Sophos Anti-Virus displays a desktop alert when a threat is found.

In the message box, click the name of the threat that you want to find out about. Sophos Anti-Virus connects you to the analysis of the threat on the Sophos website.

**Get information via the scan progress dialog box**

For custom and right-click scans, in the log that is displayed in the scan progress dialog box (or scan summary dialog box, displayed after the scan has finished), click the name of the threat that you want to find out about.

Sophos Anti-Virus connects you to the analysis of the threat on the Sophos website.

**Get information via Quarantine manager**

1. On the Home page, under Anti-virus and HIPS, click Manage quarantine items. For information about the Home page, see About the Home page (page 3).
2. In the Name column, click the name of the threat that you want to find out about.

Sophos Anti-Virus connects you to the analysis of the threat on the Sophos website.

### 5.11 Configuring alerts

#### 5.11.1 Configure anti-virus desktop messaging

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

To enable Sophos Anti-Virus to display desktop messages when a threat is found, do as follows. This applies only to on-access scanning.

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Alerting > Messaging.
2. In the Messaging dialog box, click the Desktop messaging tab. Set the options as described below.

**Enable desktop messaging**

Select this to enable Sophos Anti-Virus to display desktop messages when a threat is found.

**Messages to send**

Select the events for which you want Sophos Anti-Virus to display desktop messages.

**User-defined message**

In this text box, you can type a message that will be added to the end of the standard message.
Note
User-defined messages will not be displayed on Windows 8 and later.

5.11.2 Configure anti-virus email alerting

Important
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

To enable Sophos Anti-Virus to send email alerts when a threat is found or an error occurs, do as follows. This applies to on-access, on-demand and right-click scanning.

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Alerting > Messaging.
2. In the Messaging dialog box, click the Email alerting tab. Set the options as described below.

Enable email alerting
Select this to enable Sophos Anti-Virus to send email alerts.

Messages to send
Select the events for which you want Sophos Anti-Virus to send email alerts. Scanning errors include instances when Sophos Anti-Virus is denied access to an item that it attempts to scan.

Sophos Anti-Virus does not send email alerts for threats that are detected by web page scanning because the threats are not downloaded to your computer. Therefore, there is no need to take any action.

Recipients
Click Add or Remove to add or remove, respectively, email addresses to which email alerts should be sent. Click Edit to change an email address you have added.

Configure SMTP
Click this to change the settings for the SMTP server and the language of the email alerts. (Refer to the table below.)

<table>
<thead>
<tr>
<th>Configure SMTP settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP server</td>
<td>In the text box, type the host name or IP address of the SMTP server. Click Test to test that a connection to the SMTP server can be made. (This does not send a test email.)</td>
</tr>
<tr>
<td>SMTP ‘sender’ address</td>
<td>In the text box, type an email address to which bounces and non-delivery reports can be sent.</td>
</tr>
<tr>
<td>SMTP ‘reply to’ address</td>
<td>As email alerts are sent from an unattended mailbox, you can type in the text box an email address to which replies to email alerts can be sent.</td>
</tr>
<tr>
<td>Language</td>
<td>Click the drop-down arrow, and select the language in which email alerts should be sent.</td>
</tr>
</tbody>
</table>
5.11.3 Configure anti-virus SNMP messaging

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

To enable Sophos Anti-Virus to send SNMP messages when a threat is found or an error occurs, do as follows. This applies to on-access, on-demand and right-click scanning.

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Alerting > Messaging.**
2. In the **Messaging** dialog box, click the **SNMP messaging** tab. Set the options as described below.

   **Enable SNMP messaging**
   Select this to enable Sophos Anti-Virus to send SNMP messages.

   **Messages to send**
   Select the events for which you want Sophos Anti-Virus to send SNMP messages. **Scanning errors** include instances when Sophos Anti-Virus is denied access to an item that it attempts to scan.

   Sophos Anti-Virus does not send SNMP messages for threats that are detected by web page scanning because the threats are not downloaded to your computer. Therefore, there is no need to take any action.

   **SNMP trap destination**
   In the text box, type the IP address or name of the computer to which alerts are sent.

   **SNMP community name**
   In the text box, type the SNMP community name.

   **Test**
   Click this to send a test SNMP message to the SNMP trap destination you have specified.

5.11.4 Configure anti-virus event logging

To enable Sophos Anti-Virus to add alerts to the Windows event log when a threat is found or an error occurs, do as follows. This applies to on-access, on-demand and right-click scanning.

1. Click **Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Alerting > Messaging.**
2. In the **Messaging** dialog box, click the **Event log** tab. Set the options as described below.

   **Enable event logging**
   Select this to enable Sophos Anti-Virus to send messages to the Windows event log.

   **Messages to send**
   Select the events for which you want Sophos Anti-Virus to send messages. **Scanning errors** include instances when Sophos Anti-Virus is denied access to an item that it attempts to scan.

   Sophos Anti-Virus does not send messages for threats that are detected by web page scanning because the threats are not downloaded to your computer. Therefore, there is no need to take any action.
5.12 Scanning log

5.12.1 Configure the scanning log

The scanning log for this computer is stored in the following locations.

| Other Windows platforms | C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Anti-Virus\logs\SAV.txt |

1. Click Home > Anti-virus and HIPS > View anti-virus and HIPS log > Configure log.
2. In the Configure logging for this computer dialog box, set the options as described below.

   **Logging level**

   To stop anything being logged, click None. To log summary information, error messages and so on, click Normal. To log most information, including files scanned, major stages of a scan, and so on, clickVerbose.

   **Log archiving**

   To enable the log file to be archived monthly, select Enable archiving. The archive files are stored in the same folder as the log file. Select the Number of archive files to store before the oldest one is deleted. Select Compress log to reduce the size of the log file.

5.12.2 View the scanning log

- On the Home page, under Anti-virus and HIPS, click View anti-virus and HIPS log.
  For information about the Home page, see About the Home page (page 3).

From the log page, you can copy the log to the clipboard, or email, or print the log.
To find specific text in the log, click Find and enter the text you want to find.
6 Sophos Application Control

6.1 About scanning for controlled applications

A controlled application is an application that is prevented from running on your computer by your organisation's security policy.

Scanning for controlled applications is enabled or disabled by a management console as part of an application control policy, and is included as part of on-access scanning.

For information about on-access scanning, see About on-access and on-demand scanning (page 7).

6.2 Disable scanning for controlled applications

Important
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If scanning for controlled applications is enabled, it might prevent you from uninstalling some applications. If you are a member of the SophosAdministrator group, you can temporarily disable scanning for controlled applications on this computer.

To disable scanning for controlled applications:
1. On the Configure menu, click Application control.
2. Clear the Enable on-access scanning check box.
7 Sophos Device Control

7.1 About device control on this computer

If a management console is not used to administer Sophos Endpoint Security and Control on this computer, the device control functionality is not included.

Device control is enabled or disabled by a management console. If device control is enabled, it might prevent you from connecting a device to this computer for maintenance or troubleshooting. If this is the case, you can temporarily disable device control on this computer. For information, see Disable scanning for controlled applications (page 45).

7.2 What types of device are controlled?

Device control enables you to block the following types of device: storage, network, short range, and media.

Storage

• Removable storage devices (for example, USB flash drives, PC Card readers, and external hard disk drives)
• Optical media drives (CD-ROM/DVD/Blu-ray drives)
• Floppy disk drives
• Secure removable storage devices (for example, hardware-encrypted USB flash drives)

For a list of supported secure removable storage devices, see Sophos knowledgebase article 63102.

Tip
Using the secure removable storage category, you can easily allow the use of supported secure removable storage devices while blocking other removable storage devices.

Network

• Modems
• Wireless (Wi-Fi interfaces, 802.11 standard)

For network interfaces, you can also select the Block bridged mode that helps to significantly reduce the risk of network bridging between a corporate network and a non-corporate network. The mode works by disabling either wireless or modem network adapters when an endpoint is connected to a physical network (typically through an Ethernet connection). Once the endpoint is disconnected from the physical network, the wireless or modem network adapters are seamlessly re-enabled.
Short Range

- Bluetooth interfaces
- Infrared (IrDA infrared interfaces)

Device control blocks both internal and external devices and interfaces. For example, a policy which blocks Bluetooth interfaces will block both of the following:

- The built-in Bluetooth interface in a computer
- Any USB-based Bluetooth adapters plugged into the computer

Media

- MTP/PTP

This includes mobile phones, tablets, digital cameras, media players and other devices that connect to a computer using Media Transfer Protocol (MTP) or Picture Transfer Protocol (PTP).

7.3 Temporarily disable device control

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you are a member of the SophosAdministrator group and you want to connect a device to this computer for maintenance or troubleshooting (for example, to install software from a CD), you can temporarily disable device control.

To disable device control on this computer:
1. On the Configure menu, click Device control.
2. Clear the Enable Sophos Device Control check box.

7.4 Configure the device control log

1. On the Configure menu, click Device control.
2. Under Logging level, select one of the options:
   - Click None to stop anything being logged.
   - Click Normal to log summary information, error messages, and so on.
   - Click Verbose to provide information on many more activities than usual. Use this setting only when you need detailed logging for troubleshooting, since the log will grow in size rapidly.
3. Under Log archiving, follow the instructions on the screen.
7.5 View the device control log

- On the Home page, under Device control, click View device control log. For information about the Home page, see About the Home page (page 3).

From the log page, you can copy the log to the clipboard, or email, or print the log. To find specific text in the log, click Find and enter the text you want to find.
8 Sophos Data Control

8.1 About data control on this computer

If a management console is not used to administer Sophos Endpoint Security and Control on this computer, the data control functionality is not included.

Data control is enabled or disabled by a policy issued by a management console. However, if you are a member of the SophosAdministrator group, you can temporarily disable data control on this computer for maintenance or troubleshooting. For information, see Disable scanning for controlled applications (page 45).

8.2 Temporarily disable data control

**Important**

If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you are a member of the SophosAdministrator group, you can temporarily disable data control on this computer for maintenance or troubleshooting:

1. On the **Configure** menu, click **Data control**.
2. Clear the **Enable Sophos Data Control** check box.

8.3 How do I add a file to a storage device?

If data control is enabled on this computer, the data control policy may block any attempt to add a file to a monitored storage device using the following methods:

- Saving data from within a program
- Using the DOS copy command
- Creating a new file on the device using Windows Explorer

If you see a desktop alert that warns you about this, you should save the file to your hard disk or to a network drive, and then use Windows Explorer to copy it to the storage device.

8.4 Configure the data control log

1. On the **Configure** menu, click **Data control**.
2. Under **Logging level**, select one of the options:
   - Click **None** to stop anything being logged.
   - Click **Normal** to log summary information, error messages, and so on.
   - Click **Verbose** to provide information on many more activities than usual. Use this setting only when you need to test new data control rules, since the log will grow in size rapidly.
3. Under Log archiving, follow the instructions on the screen.

8.5 View the data control log

- On the Home page, under Data control, click View data control log.
  For information about the Home page, see About the Home page (page 3).

From the log page, you can copy the log to the clipboard, or email, or print the log.
To find specific text in the log, click Find and enter the text you want to find.
9 Sophos Web Control

9.1 About web control on this computer

Sophos Web Control provides protection, control, and reporting for computers that are located, or roam, outside the corporate network.

Note
This feature is not included with all licenses. If you want to use it, you might need to change your license.

If a management console is not used to administer Sophos Endpoint Security and Control on this computer, the web control functionality is not included.

Web control is enabled or disabled by a policy issued by a management console. However, if you are a member of the SophosAdministrator group, you can temporarily disable web control on this computer. For information on how to do this, see Disable scanning for controlled applications (page 45).

9.2 Temporarily disable web control

Important
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you are a member of the SophosAdministrator group, you may need to temporarily disable web control for maintenance or troubleshooting, and then re-enable it.

To disable web control on this computer:
1. On the Configure menu, click Web control.
2. Clear the Enable web control check box.
10 Sophos Client Firewall

10.1 Getting started with the firewall

When the firewall is first installed, you may need to configure it. Whether you need to do this depends on how it has been installed. There are two types of installation:

- Installed on a network computer and managed from a management console
- Installed on a standalone computer and managed from the computer

Firewall managed from a management console

If the firewall is installed and managed from a management console, it allows or blocks applications and traffic according to rules set by policy.

Unless the policy has put the firewall into interactive mode (see below), you will not be prompted with any messages and do not need to configure the firewall in any way.

Firewall managed from this computer

If the firewall is managed on this computer, we recommend that you start by creating rules to allow network access for common applications and services such as Web browsers and email clients.

For information on creating rules, see About configuring the firewall (page 52).

The firewall will also initially be in interactive mode (see below). Leave the firewall in interactive mode for a period of time so that you can allow or block other applications and services you use.

Once you have configured the firewall, and it recognizes the applications you commonly use, we recommend that you change to one of the non-interactive modes.

For information, see Change to a non-interactive mode (page 60).

What's interactive mode?

In interactive mode, the firewall prompts you to allow or block any applications and traffic for which it does not have a rule.

For information about how to deal with messages from the firewall, see About interactive mode (page 60).

On Windows 8 and later, interactive mode is not available. You must add specific policy rules to allow or block applications. Alternatively, you can use the event viewer in the management console to manage application rules interactively.

10.2 Configuring the firewall

10.2.1 About configuring the firewall

You can configure the firewall in many different ways and then enable it. However, if a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make.

A few common functions are listed below:
• Enable interactive mode (page 60)
• Filter ICMP messages (page 58)
• Allow all traffic on a LAN (page 54)
• Allow FTP downloads (page 54)
• Create a global rule (page 64)
• Allow an application (page 56)
• Allow applications to launch hidden processes (page 69)
• Allow applications to use rawsockets (page 69)
• Use checksums to authenticate applications (page 70)

10.2.2 Temporarily disable the firewall

If you are a member of the SophosAdministrator group, you may need to temporarily disable the firewall for maintenance or troubleshooting, and then re-enable it.

Sophos Endpoint Security and Control retains the settings you make here, even after you restart your computer. If you disable the firewall, your computer is unprotected until you re-enable it.

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, select the Allow all traffic check box next to the primary or secondary location.

10.2.3 Allow email

Important
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Applications tab.
4. Click Add, locate the email application, and then double-click it.

The email application is allowed as a trusted application.

Trusted applications are allowed full and unconditional network access, including access to the internet. For greater security, you can apply the preset rules supplied by Sophos:

1. In the list of allowed applications, click the email application.
2. Click the arrow next to Custom > Add rules from preset > Email client.

10.2.4 Allow the use of a web browser

Note
If you allow the use of a web browser, you also allow FTP access.

1. On the Home page, under Firewall, click Configure firewall.
For information about the Home page, see About the Home page (page 3).

2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Applications tab.
4. Click Add, locate the web browser application, and then double-click it.

The web browser application is allowed as a trusted application.

Trusted applications are allowed full and unconditional network access, including access to the internet. For greater security, you can apply the preset rules supplied by Sophos:

1. In the list of allowed applications, click the web browser application.
2. Click Custom > Add rules from preset > Browser.

**10.2.5 Allow FTP downloads**

**Note**
If you have allowed the use of a web browser which can access FTP servers, you do not need to allow FTP downloads as well.

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Applications tab.
4. Click Add, locate the FTP application, and then double-click it.

The FTP application is allowed as a trusted application.

Trusted applications are allowed full and unconditional network access, including access to the internet. For greater security, you can apply the preset rules supplied by Sophos:

1. In the list of allowed applications, click the FTP application.
2. Click Custom > Add rules from preset > FTP Client.

**10.2.6 Allow all traffic on a LAN**

To allow all traffic between computers on a LAN (Local Area Network):

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. On the LAN tab, do one of the following:
   • Click Detect LAN to detect the LAN that your computer is on and add it to the list of network addresses.
   • Click Add. In the Select address dialog box, select the Address format, type the domain name or IP address, and then click Add.

**Note**
If you select Local network (detected automatically), you do not need to type anything. This option is not available on Windows 8 and later. For information about local network detection, see About local network detection (page 64).

3. Click OK to close the Select Address dialog box.
4. In the **LAN settings** list, select the **Trusted** check box for a network.

**Note**

- If you allow all traffic between the computers on a LAN, you also allow file and printer sharing on it.

10.2.7 Allow all file and printer sharing on a LAN

**Note**

If you have already allowed all traffic between computers on a LAN (Local Area Network), you do not need to allow file and printer sharing as well.

To allow all file and printer sharing on a LAN:
1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   
   For information about the **Home** page, see **About the Home page** (page 3).
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. On the **LAN** tab, do one of the following:
   
   - Click **Detect LAN** to detect the LAN that your computer is on and add it to the list of network addresses.
   - Click **Add**. In the **Select address** dialog box, select the **Address format**, type the domain name or IP address, and then click **Add**.

**Note**

If you select **Local network (detected automatically)**, you do not need to type anything. This option is not available on Windows 8 and later. For information about local network detection, see **About local network detection** (page 64).

4. Click **OK** to close the **Select Address** dialog box.
5. In the **LAN settings** list, select the **NetBIOS** check box for a LAN to allow file and printer sharing on it.

For information on how to block or allow file and printer sharing on other LANs than those in the **LAN settings** list, see the following topics:

- **Block unwanted file and printer sharing** (page 56)
- **Allow flexible control of file and printer sharing** (page 55)

For information on how to allow all traffic on a LAN, see **Allow all traffic on a LAN** (page 54).

10.2.8 Allow flexible control of file and printer sharing

If you want more flexible control of file and printer sharing on your networks (for example, unidirectional NetBIOS traffic), you can do the following:

1. Allow file and printer sharing on other LANs (Local Area Networks) than those in the **LAN settings** list. This allows NetBIOS traffic on those LANs to be processed by the firewall rules.
2. Create high-priority global rules which allow communication to/from hosts with the appropriate NetBIOS ports and protocols. We recommend that you create global rules to explicitly block all unwanted file and printer sharing traffic rather than let it be handled by the default rule.

To allow file and printer sharing on other LANs than those in the LAN settings list:

1. On the Home page, under Firewall, click Configure firewall. For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. On the LAN tab, clear the Block file and printer sharing for other networks check box.

### 10.2.9 Block unwanted file and printer sharing

To block file and printer sharing on LANs other than those specified in the LAN settings list on the LAN tab:

1. On the Home page, under Firewall, click Configure firewall. For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. On the LAN tab, select the Block file and printer sharing for other networks check box.

### 10.2.10 Allow an application

1. On the Home page, under Firewall, click Configure firewall. For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Applications tab.
4. Click Add, locate the application, and then double-click it.

The application is allowed as trusted.

Trusted applications are allowed full and unconditional network access, including access to the internet. For greater security, you can apply one or more application rules to specify the conditions under which the application can run.

- Create an application rule (page 67)
- Apply preset application rules (page 66)

### 10.2.11 Block an application

1. On the Home page, under Firewall, click Configure firewall. For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Applications tab.
4. If the application is not in the list, click Add, locate the application, and then double-click it.
5. Select the application in the list, and then click Block.
10.2.12 Block IPv6

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Based on the operating system:
   • In Windows 7 and earlier operating systems, on the General tab, under Blocking, select Block IPv6 packets.
   • On Windows 8 or later, on the Global Rules tab, select Block all IPv6 traffic.

10.2.13 Turn the use of checksums on or off

If you enable the use checksums to authenticate applications, when you trust or block applications they are identified based on their checksums automatically (you can also manually add checksums). If the application does not match a checksum it is blocked.

If you disable this option, applications are identified by their filename.

To turn the use of checksums to authenticate applications on or off:
1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Based on the operating system:
   • In Windows 7 and earlier operating systems, under Blocking, clear the Use checksums to authenticate applications check box.
   • On Windows 8 or later, click the Applications tab and clear the Use checksums to authenticate applications check box.

   To turn the use of checksums to authenticate applications on, select the check box.

10.2.14 Turn blocking of modified processes on or off

**Note**
This option is not available on Windows 8 and later as it is handled automatically by the Sophos Anti-Virus HIPS technology.

Malware may attempt to evade the firewall by modifying a process in memory that has been initiated by a trusted program, and then using the modified process to access the network on its behalf.

You can configure the firewall to detect and block processes that have been modified in memory.

To turn blocking of modified processes on or off:
1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. On the General tab, under Blocking, clear the Block processes if memory is modified by another application (32-bit operating systems only) check box to turn blocking of modified processes off.

   To turn blocking of modified processes on, select the check box.

If the firewall detects that a process has been modified in memory, it adds rules to prevent the modified process from accessing the network.

**Notes**

- We do not recommend that you turn blocking of modified processes off permanently. You should turn it off only when you need to.
- Blocking of modified processes is not supported on 64-bit versions of Windows.
- Only the modified process is blocked. The modifying program is not blocked from accessing the network.

### 10.2.15 Filter ICMP messages

Internet Control Message Protocol (ICMP) messages allow the computers on a network to share error and status information. You can allow or block specific types of incoming or outgoing ICMP message.

You should only filter ICMP messages if you are familiar with networking protocols. For explanations of the ICMP message types, see *Explanation of ICMP message types* (page 58).

To filter ICMP messages:

1. On the **Home** page, under **Firewall**, click **Configure firewall**.

   For information about the **Home** page, see *About the Home page* (page 3).

2. Under **Configurations**, click **Configure** next to the location that you want to configure.

3. Click the **ICMP** tab. The interface differs based on the operating system:

   - In Windows 7 and earlier operating systems, select the **In** or **Out** check box to allow incoming or outgoing messages of the specified type.
   - On Windows 8 or later, ICMP messages types are categorized into sections. You can select common settings from the drop-down list, or click **Details** to view or edit the settings.

### 10.2.16 Explanation of ICMP message types

**Network error reporting**

| **Destination Unreachable, Echo Reply** | Sent by a router when it cannot deliver an IP datagram. A datagram is the unit of data, or packet, transmitted in a TCP/IP network. |
| **Source Quench** | Sent by a host or router if it is receiving data too quickly for it to handle. The message is a request that the source reduce its rate of datagram transmission. |
Time Exceeded
Sent by a router if the datagram has reached the maximum limit of routers through which it can travel.

Parameter Problem
Sent by a router if a problem occurs during the transmission of a datagram such that it cannot complete processing. One potential source of such a problem is invalid datagram header.

Network troubleshooting

Echo Request, Echo Reply
Used to test destination accessibility and status. A host sends an Echo Request and listens for a corresponding Echo Reply. This is most commonly done using the ping command.

IPv4 network address and routing configuration

Redirect
Sent by a router if it receives a datagram that should have been sent to a different router. The message contains the address to which the source should direct future datagrams. This is used to optimize the routing of network traffic.

Router Advertisement, Router Solicitation
Allow hosts to discover the existence of routers. Routers periodically broadcast their IP addresses via Router Advertisement messages. Hosts may also request a router address by broadcasting a Router Solicitation message to which a router will reply with a Router Advertisement.

Timestamp Request, Timestamp Reply
Used to synchronize the clocks between hosts and to estimate transit time.

Information Request, Information Reply
Obsolete. These messages were used earlier by hosts to determine their inter-network addresses, but are now considered outdated and should not be used.

Address Mask Request, Address Mask Reply
Used to find the mask of the subnet (i.e. what address bits define the network). A host sends an Address Mask Request to a router and receives an Address Mask Reply in return.

10.2.17 Restore the firewall default settings

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Managing configuration, click Restore Defaults.
10.3 Working in interactive mode

10.3.1 About interactive mode

Note
Interactive mode is not available on Windows 8 and later. You must add specific policy rules to allow or block applications. Alternatively, you can use the event viewer in the management console to manage application rules interactively.

In interactive mode, the firewall displays a learning dialog each time an unknown application or service requests network access. The learning dialog asks you whether to allow the traffic once, block it once, or whether to create a rule for that type of traffic.

In interactive mode, you will see the following types of learning dialog:

- Hidden process learning dialogs (page 61)
- Protocol learning dialogs (page 61)
- Application learning dialogs (page 61)
- Rawsocket learning dialogs (page 61)
- Checksum learning dialogs (page 62)

10.3.2 Enable interactive mode

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. On the General tab, under Working mode, click Interactive.

10.3.3 Change to a non-interactive mode

There are two non-interactive modes:

- Allow by default
- Block by default

In the non-interactive modes, the firewall deals with network traffic automatically using your rules. Network traffic which has no matching rule is either all allowed (if it is outbound) or all blocked.

To change to a non-interactive mode:

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. On the General tab, under Working mode, click Allow by default or Block by default.
10.3.4 Hidden process learning dialogs

A hidden process is when one application launches another one to perform some network access for it. Malicious applications sometimes use this technique to evade firewalls: they launch a trusted application to access the network rather than doing it themselves.

The hidden process learning dialog displays information about the hidden process and the application that launched it.

- Enable hidden process learning dialogs (page 61)

10.3.5 Enable hidden process learning dialogs

If you are using interactive mode, the firewall can display a learning dialog when it detects a new launcher.

If you are using interactive mode and this option is not selected, new launchers are blocked from launching hidden processes.

To enable hidden process learning dialogs:
1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Processes tab.
4. Select the Warn about new launchers check box.

10.3.6 Protocol learning dialogs

If the firewall detects network activity by the system that it cannot relate to a specific application, it prompts for the creation of a protocol rule.

The protocol learning dialog displays information about the unrecognized network activity, i.e. the protocol and remote address.

10.3.7 Application learning dialogs

If the firewall detects an application attempting to access the network in a way that is not covered by any existing rule, it prompts for the creation of an application rule.

The application learning dialog displays information about the unrecognized network activity, i.e. the remote service and the remote address.

10.3.8 Rawsocket learning dialogs

Rawsockets allow processes to control all aspects of the data they send over the network and can be used for malicious purposes.

If the firewall detects a rawsocket attempting to access the network in a way that is not covered by any existing rule, it prompts for the creation of a rawsocket rule.

The rawsocket learning dialog displays information about the rawsocket.
• Enable rawsocket learning dialogs (page 62)

10.3.9 Enable rawsocket learning dialogs

If you are using interactive mode, the firewall can display a learning dialog when it detects a rawsocket attempting to access the network in a way that is not covered by any existing rule.

If you are using interactive mode and this option is not selected, rawsockets are blocked from accessing the network.

To enable rawsocket learning dialogs:
1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Processes tab.
4. Select the Warn about the use of rawsockets check box.

10.3.10 Checksum learning dialogs

If the firewall detects a new or modified application, it displays a checksum learning dialog.

Checksum learning dialog is displayed only if you use checksums to authenticate applications. For information, see Turn the use of checksums on or off (page 57).

If you want to allow the application to access the network, you must add its checksum (a unique identifier) to the list of recognized checksums.

Select one of the following options:
• Add the checksum to existing checksums for this application allows multiple versions of this application.
• Replace any existing checksum for this application replaces all existing checksums for the application with the one requesting access, and thereby allows only the latest version of this application.
• Block this application until it is restarted blocks the application on this occasion.

10.4 Firewall configuration files

10.4.1 About firewall configuration files

Sophos Client Firewall enables you to export the firewall general settings and rules as a configuration file. You can use this feature to do the following:
• Back up and restore your entire firewall configuration.
• Save a general settings configuration and install it on multiple computers.
• Create rules for applications on one computer and export them for use on other computers running the same set of applications.
• Use the management console to merge configurations created on several different computers to create a policy that is valid for all computers on the network.
10.4.2 Export a firewall configuration file

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Click Export.
3. Give your configuration file a name and location, and then click Save.

10.4.3 Import a firewall configuration file

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Click Import.
3. Select a configuration file and click Open.
4. Follow the instructions on the screen.

10.5 Firewall rules

10.5.1 About firewall rules

Global rules
Global rules apply to all network communications and to applications even if they have application rules.

Application rules
You can have one or more rules for an application. You can either use preset rules created by Sophos or create custom rules to give you fine control over the access allowed for an application.


10.5.2 About the order in which rules are applied

For connections that use rawsockets, only the global rules are checked.

For connections that do not use rawsockets, various rules are checked, depending on whether the connection is to a network address that is listed on the LAN tab or not.

If the network address is listed on the LAN tab, the following rules are checked:

- If the address has been marked as Trusted, all traffic on the connection is allowed with no further checks.
- If the address has been marked as NetBIOS, file and printer sharing on any connection that meets the following criteria is allowed:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Port</th>
<th>Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Remote</td>
<td>137-139 or 445</td>
</tr>
</tbody>
</table>
If the network address is not listed on the LAN tab, other firewall rules are checked in the following order:

1. Any NetBIOS traffic that has not been allowed using the LAN tab is dealt with according to the setting of the Block file and printer sharing for other networks check box:
   - If the check box is selected, the traffic is blocked.
   - If the check box is cleared, the traffic is processed by the remaining rules.
2. The high-priority global rules are checked, in the order in which they are listed.
3. If the connection has not already had rules applied to it, the application rules are checked.
4. If the connection has still not been handled, the normal-priority global rules are checked, in the order in which they are listed.
5. If no rules have been found to handle the connection:
   - In Allow by default mode, the traffic is allowed (if it is outbound).
   - In Block by default mode, the traffic is blocked.
   - In Interactive mode, the user is asked to decide. This mode is not available in Windows 8 and later.

   **Note**
   If you have not changed the working mode, the firewall will be in Block by default mode.

### 10.5.3 About local network detection

**Note**
This option is not available on Windows 8 and later.

You can assign the local network for this computer to firewall rules.

The firewall determines this computer’s local network when it starts, and then monitors for any changes whilst it is running. If any change is detected, the firewall updates any local network rules with the new local network address range.

**CAUTION**
We strongly advise caution when using local network rules as part of configurations that may be used in “out of office” locations. For more information, see Create a secondary configuration (page 72).

### 10.5.4 Global rules

**Create a global rule**
Important
We recommend that you create global rules only if you are familiar with networking protocols.

Global rules apply to all network communications and to applications which do not already have a rule.

To create a global rule:
1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Global Rules tab.
4. Click Add.
5. Under Rule name, type a name for the rule.
   The rule name must be unique within the list of rules. Two global rules cannot have the same name.
6. On Windows 8 or later, under Protocol, select the protocol you want to use.
7. To apply the rule before any application rules or normal priority global rules, select the Higher priority than Application rules check box.
   For information on the order in which rules are applied, see About the order in which rules are applied (page 63).
8. Under Select the events the rule will handle, select the conditions that the connection must match for the rule to apply.
9. Under Select the action with which the rule will respond, select either Allow it or Block it.
10. Do one of the following:
    • To allow other connections to and from the same remote address while the initial connection exists, select Concurrent connections. This option is only available for TCP rules.
    • To intelligently allow replies from the remote computer based on the initial connection, select Stateful inspection. This option is only available for UDP rules.

Note
On Windows 8 and later, these options are not displayed as Stateful inspection is always used and Concurrent connections are not supported.

11. Under Rule description, click an underlined value.

Edit a global rule

Important
We recommend that you change global rules only if you are familiar with networking protocols.

To edit a global rule:
1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Global Rules tab.
4. In the Rule list, select the rule that you want to edit.
5. Click **Edit**.
   For information on the global rule settings, see *Create a global rule* (page 64).

### Copy a global rule

To copy a global rule and append it to the list of rules:

1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   For information about the **Home** page, see *About the Home page* (page 3).
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. Click the **Global Rules** tab.
4. In the **Rule** list, select the rule that you want to copy.
5. Click **Copy**.

### Delete a global rule

1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   For information about the **Home** page, see *About the Home page* (page 3).
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. Click the **Global Rules** tab.
4. In the **Rule** list, select the rule that you want to delete.
5. Click **Remove**.

### Change the order in which global rules are applied

Global rules are applied in the order in which they appear from top to bottom in the list of rules.

To change the order in which the global rules are applied:

1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   For information about the **Home** page, see *About the Home page* (page 3).
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. Click the **Global Rules** tab.
4. In the **Rule** list, click the rule that you want to move up or down in the list.
5. Click **Move Up** or **Move Down**.

### 10.5.5 Application rules

#### Apply preset application rules

A preset is a set of application rules created by Sophos. To append preset rules to the list of rules for an application:

1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   For information about the **Home** page, see *About the Home page* (page 3).
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. Click the **Global Rules** tab.
4. Select the application in the list, and then click the arrow next to **Custom**.
5. Point to **Add rules from preset**, and then click a preset.
Create an application rule

To create a custom rule which allows fine control over the access allowed for an application:

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Global Rules tab.
4. Select the application in the list, and then click Custom.
   You can also double-click the application in the list.
5. In the Application Rules dialog box, click Add.
6. Under Rule name, type a name for the rule.
   The rule name must be unique within the list of rules. Two application rules cannot have the
   same name, but two applications can each have a rule with the same name.
7. On Windows 8 or later, under Protocol, select the protocol you want to use.
8. Under Select the events the rule will handle, select the conditions that the connection must
   match for the rule to apply.
9. Under Select the action with which the rule will respond, select either Allow it or Block it.
10. Do one of the following:
   • To allow other connections to and from the same remote address while the initial connection
       exists, select Concurrent connections. This option is only available for TCP rules.
   • To intelligently allow replies from the remote computer based on the initial connection, select
       Stateful inspection. This option is only available for UDP rules.

   Note
   On Windows 8 and later, these options are not displayed as Stateful inspection is always
   used and Concurrent connections are not supported.

11. Under Rule description, click an underlined value.

Edit an application rule

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Global Rules tab.
4. Select the application in the list, and then click Custom.
   You can also double-click the application in the list.
5. In the Application Rules dialog box, click Edit.
6. Under Rule name, type a name for the rule.
   The rule name must be unique within the list of rules. Two application rules cannot have the
   same name, but two applications can each have a rule with the same name.
7. On Windows 8 or later, under Protocol, select the protocol you want to use.
8. Under Select the events the rule will handle, select the conditions that the connection must
   match for the rule to apply.
9. Under Select the action with which the rule will respond, select either Allow it or Block it.
10. Do one of the following:
• To allow other connections to and from the same remote address while the initial connection exists, select Concurrent connections. This option is only available for TCP rules.
• To intelligently allow replies from the remote computer based on the initial connection, select Stateful inspection. This option is only available for UDP rules.

**Note**
On Windows 8 and later, these options are not displayed as Stateful inspection is always used and Concurrent connections are not supported.

11. Under Rule description, click an underlined value.

### Copy an application rule

To copy an application rule and append it to the list of rules:

1. On the Home page, under Firewall, click Configure firewall.
   - For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Global Rules tab.
4. Select the application in the list, and then click Custom.
   - You can also double-click the application in the list.
5. In the Application Rules dialog box, select the rule you want to copy and click Copy.

### Delete an application rule

1. On the Home page, under Firewall, click Configure firewall.
   - For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Global Rules tab.
4. Select the application in the list, and then click Custom.
5. In the Application Rules dialog box, select the rule you want to remove and click Remove.

### Change the order in which application rules are applied

Application rules are applied in the order in which they appear from top to bottom in the list of rules.

To change the order in which the application rules are applied:

1. On the Home page, under Firewall, click Configure firewall.
   - For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Global Rules tab.
4. Select the application in the list, and then click Custom.
   - You can also double-click the application in the list.
5. In the Rule list, click the rule that you want to move up or down in the list.
6. Click Move Up or Move Down.
Allow applications to launch hidden processes

Note
This option is not available on Windows 8 and later as it is handled automatically by the Sophos Anti-Virus HIPS technology.

An application sometimes launches another hidden process to perform some network access for it.

Malicious applications can use this technique to evade firewalls: they launch a trusted application to access the network rather than doing so themselves.

The firewall sends an alert to the management console, if one is being used, the first time a hidden process is detected.

To allow applications to launch hidden processes:
1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Processes tab.
4. In the upper area, click the Add button.
5. Locate the application, and then double-click it.

If you are using interactive mode, the firewall can display a learning dialog when it detects a new launcher.
   • Enable interactive mode (page 60)
   • Enable hidden process learning dialogs (page 61)

Allow applications to use rawsockets

Note
This option is not available on Windows 8 and later. The firewall will treat rawsockets in the same way as ordinary sockets.

Some applications can access a network through rawsockets, which gives them control over all aspects of the data they send over the network.

Malicious applications can exploit rawsockets by faking their IP address or send deliberately corrupt messages.

The firewall sends an alert to the management console, if one is being used, the first time a rawsocket is detected.

To allow applications to access the network through rawsockets:
1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. Click the Processes tab.
4. In the lower area, click the Add button.
5. Locate the application, and then double-click it.
If you are using interactive mode, the firewall can display a learning dialog when a rawsocket is detected.

- Enable interactive mode (page 60)
- Enable rawsocket learning dialogs (page 62)

### Use checksums to authenticate applications

Each version of an application has a unique checksum. The firewall can use this checksum to decide whether an application is allowed or not.

By default, the firewall checks the checksum of each application that runs. If the checksum is unknown or has changed, the firewall blocks it or (in interactive mode) asks the user what to do.

The firewall also sends an alert to the management console, if one is being used, the first time a new or modified application is detected.

To add a checksum to the list of allowed checksums:

1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   
   For information about the **Home** page, see [About the Home page](#). (page 3).
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. Click the **Checksums** tab.
4. Click **Add**.
5. Locate the application, and then double-click it.

If you are using interactive mode, the firewall can display a learning dialog when it detects a new or modified application.

- Enable interactive mode (page 60)
- Enable hidden process learning dialogs (page 61)

### 10.6 Location awareness

#### 10.6.1 About location awareness

Location awareness is a feature of Sophos Client Firewall that assigns a firewall configuration to each network adapter on your computer, depending on the current location of the network adapter.

The most common scenario in which this feature is used is where you have a company laptop and you work from home. You are using two network connections simultaneously:

- For work use, you connect to your office network through a VPN client and a **virtual network adapter**.
- For personal use, you connect to your ISP through a network cable and a **physical network adapter**.

In this scenario, you need the office configuration to be applied to the virtual office connection and the non-office, generally more restrictive, configuration to be applied to the non-office ISP connection.
Note
The non-office configuration will require sufficient rules to allow the "virtual" office connection to be established.

10.6.2 Set up location awareness

1. Define the list of gateway MAC addresses or domain names of your primary locations. Typically, these are your office networks.
2. Create the firewall configuration that will be used for your primary locations. Typically, this configuration is less restrictive.
3. Create a secondary firewall configuration. Typically, this configuration is more restrictive.
4. Choose a configuration to apply.

Depending on the detection method you are using, the firewall obtains the DNS or gateway address for each of your computer’s network adapters, and then matches it against your list of addresses.

- If any of the addresses in your list matches the address of a network adapter, the adapter is assigned the configuration for the **primary location**.
- If none of the addresses in your list matches the address of a network adapter, the adapter is assigned the policy for the **secondary location**.

The active location is displayed in the **Status** panel in the Sophos Endpoint Security and Control window. If both configurations have been applied, **Active = Both**.

**Important**
The secondary configuration switches from **Interactive mode** to **Block by default mode** when both the following conditions are met:

- Both locations are active.
- The primary configuration is not interactive.

10.6.3 Define your primary locations

1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   For information about the **Home** page, see **About the Home page** (page 3).
2. Click the **Location detection** tab.
3. Under **Detection method**, click **Configure** next to the method that you want to use to define your primary locations:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify location by DNS</td>
<td>You create a list of domain names and expected IP addresses that correspond to your primary locations.</td>
</tr>
<tr>
<td>Identify location by gateway MAC address</td>
<td>You create a list of gateway MAC addresses that correspond to your primary locations.</td>
</tr>
</tbody>
</table>

4. Follow the instructions on the screen.
10.6.4 Create a secondary configuration

The firewall uses your secondary configuration when it detects that you are not connected to your primary location.

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Select the Add configuration for a second location check box.

Now set up the configuration for your secondary location. For information on how to do this, see About configuring the firewall (page 52) and the other topics in the Configuring the firewall section.

CAUTION
If this computer is a laptop, and it is used out of the office, it may connect to an unknown local network. If this happens, firewall rules in the secondary configuration that use the local network as an address may inadvertently allow unknown traffic. For that reason, we strongly advise caution when using local network rules as part of secondary configurations.

10.6.5 Choose a configuration to apply

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. On the General tab, under Applied location, click one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply the configuration for the detected location</td>
<td>The firewall applies either the primary or secondary configuration to each network connection according to the detection settings for location awareness (as described in Set up location awareness (page 71)).</td>
</tr>
<tr>
<td>Apply the configuration for the primary location</td>
<td>The firewall applies the primary configuration to all network connections.</td>
</tr>
<tr>
<td>Apply the configuration for the secondary location</td>
<td>The firewall applies the secondary configuration to all network connections.</td>
</tr>
</tbody>
</table>

10.7 Firewall reporting

10.7.1 About firewall reporting

By default, the firewall reports state changes, events, and errors to the management console.

Firewall state changes
The firewall regards the following as state changes:

• Changes to the working mode
• Changes to the software version
• Changes to whether the firewall is configured to allow all traffic
• Changes to whether the firewall complies with policy

When you are working in interactive mode, your firewall configuration may deliberately differ from the policy applied by the management console. In that case, you can choose not to send “differs from policy” alerts to the management console when you make changes to certain parts of your firewall configuration.

For more information, see Turn reporting of local changes on or off (page 73).

**Firewall events**

An *event* is when an unknown application on your computer, or your computer’s operating system, tries to communicate with another computer over a network connection.

You can prevent the firewall from reporting events to the management console.

For more information, see Turn off reporting of unknown network traffic (page 73)

---

### 10.7.2 Turn reporting of local changes on or off

**Note**

This option is not available on Windows 8 and later.

If your firewall configuration differs from policy, you can turn reporting of local changes off.

Turning reporting of local changes off stops the firewall sending “differs from policy” alerts to the management console about changes made to the global rules, applications, processes, or checksums. You may want to do this, for example, when you are working in interactive mode, since these are settings that can be changed by using the learning dialogs.

If the firewall configuration on this computer is intended to conform to policy, you should turn reporting of local changes on.

To turn reporting of local changes off:

1. On the Home page, under Firewall, click Configure firewall.
   
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. On the General tab, under Reporting, clear the Display an alert in the management console if local changes are made to the global rules, applications, processes or checksums check box to turn reporting of local changes off.
   
   To turn reporting of local changes on, select the check box.

### 10.7.3 Turn off reporting of unknown network traffic

You can prevent the firewall from reporting unknown network traffic to the management console. The firewall regards traffic as unknown if there is no rule for it.

To prevent the firewall from reporting unknown network traffic to the management console:

1. On the Home page, under Firewall, click Configure firewall.
   
   For information about the Home page, see About the Home page (page 3).
2. Under Configurations, click Configure next to the location that you want to configure.
3. On the **General** tab, under **Blocking**, select the **Use checksums to authenticate applications** check box.

4. Under **Reporting**, clear the **Report unknown applications and traffic to the management console** check box.

### 10.7.4 Turn off reporting of firewall errors

**Important**
We do not recommend that you turn off reporting of firewall errors permanently. You should turn off reporting only when you need to.

To prevent the firewall from reporting errors to the management console:

1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   For information about the **Home** page, see [About the Home page](#) (page 3).
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. On the **General** tab, under **Reporting**, clear the **Report errors to the management console** check box.

### 10.7.5 Configure desktop messaging

You can control what messages the firewall displays on the desktop.

Unknown applications and traffic notifications are not shown in interactive mode since the same information is displayed in the learning dialogs.

1. On the **Home** page, under **Firewall**, click **Configure firewall**.
   For information about the **Home** page, see [About the Home page](#) (page 3).
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. On the **General** tab, under **Desktop messaging**, do one of the following:
   - To display notifications for firewall warnings and errors, select the **Show warnings and errors** check box.
   - To display notifications for unknown applications and traffic, select the **Show unknown applications and traffic** check box.

### 10.8 Firewall logging

#### 10.8.1 About the firewall log viewer

The Sophos Client Firewall log viewer enables you to view, filter, and save details of the following:

- All connections
- Connections that have been allowed or blocked
- Firewall events
- The system log
10.8.2 Open the firewall log viewer

- On the Home page, under Firewall, click View Firewall log.
  For information about the Home page, see About the Home page (page 3).

10.8.3 Configure firewall logging

To manage the size and contents of the firewall’s event log database:

1. On the Home page, under Firewall, click Configure firewall.
   For information about the Home page, see About the Home page (page 3).
2. Click the Log tab.
3. To manage the size of the firewall’s event log database, select one of the following options:
   - To allow the database to grow without limit, click Keep all records.
   - To clear out old records, click Delete old records, and then configure the Log cleanup settings.
4. Under Log cleanup settings, select one or more of the following options:
   - Click the Delete records after check box, and then enter or select a figure in the Days box.
   - Click the Keep no more than check box, and then enter or select a figure in the Records box.
   - Click the Keep size under check box, and then enter or select a figure in the MB box.

10.8.4 Change how the firewall log viewer looks

1. On the Home page, under Firewall, click View firewall log.
   For information about the Home page, see About the Home page (page 3).
2. On the View menu, click Layout.
3. In the Customize View dialog box, select items to hide or display:
   - The Console tree is displayed in the left pane.
   - The Toolbar is displayed at the top of the firewall log viewer.
   - The Description bar is displayed above the data in the right pane.
   - The Status bar is displayed at the bottom of the firewall log viewer.

10.8.5 Customize the data format

You can change the format used to display the following items of data in the firewall logs:

- Display ports as a number or a name, for example HTTP or 80.
- Display applications as icons, file paths, or both.
- Specify the size of unit that is used to display the data transfer speed, for example KBytes or MBytes.
- Hide or display the gridlines.

To customize the data format:

1. On the Home page, under Firewall, click View firewall log.
For information about the Home page, see About the Home page (page 3).
2. On the View menu, click Customize.
3. Select the options you want.

10.8.6 Hide or display columns in the firewall log viewer

1. On the Home page, under Firewall, click View firewall log.
   For information about the Home page, see About the Home page (page 3).
2. Click an item in the console tree that displays columns in the details pane.
3. On the View menu, select Add/Remove Columns.
   You can also right-click any of the column headings.
4. In the Columns dialog box, do one of the following:
   • To hide a column, clear its check box.
   • To display a column, select its check box.

10.8.7 Reorder columns in the firewall log viewer

1. On the Home page, under Firewall, click View firewall log.
   For information about the Home page, see About the Home page (page 3).
2. Click an item in the console tree that displays columns in the details pane.
3. On the View menu, select Add/Remove Columns.
   You can also right-click any of the column headings.
4. In the Columns dialog box, click a column name, and then click Move Up or Move Down to change the position of the column.

Notes

• You can also reorder columns in the details pane by using a mouse to drag a column heading to the left or right of its original position. As you drag a column, highlighting between the column headings indicates the new position of the column.
• You can resize columns by using the mouse to drag column headings.

10.8.8 Filter records in a firewall log

You can sort the firewall log records by creating a filter.

To filter the firewall log records:
1. On the Home page, under Firewall, click View firewall log.
   For information about the Home page, see About the Home page (page 3).
2. In the console tree, select a log.
3. On the Action menu, click Add filter.
4. Follow the instructions in the Filter wizard.

The filter appears in the console tree immediately below the node for the log you want to filter.
10.8.9 Export all records from a firewall log

To export all the records from the firewall log to a text or CSV file:

1. On the Home page, under Firewall, click View firewall log.
   For information about the Home page, see About the Home page (page 3).
2. In the console tree, select a log.
3. Right-click the record list, and then click Export All Records.
4. In the File name box, type a name for the file.
5. In the Save as type list, click the file type that you want.

10.8.10 Export selected records from a firewall log

To export selected records from a firewall log to a text or CSV file:

1. On the Home page, under Firewall, click View firewall log.
   For information about the Home page, see About the Home page (page 3).
2. In the console tree, select a log.
3. Select the records you want to export.
   If the records update rapidly, on the View menu, clear the Auto refresh check box.
5. In the File name box, type a name for the file.
6. In the Save as type list, click the file type that you want.
11 Sophos AutoUpdate

11.1 Update immediately

By default, Sophos AutoUpdate is scheduled to update every 10 minutes if you are permanently connected to your company network, or every 60 minutes if you are permanently connected to the internet.

If you are on a dial-up connection, Sophos AutoUpdate is scheduled to update when you connect to the internet or your network, and every 60 minutes after that.

To update immediately:

• Right-click the Sophos Endpoint Security and Control system tray icon, and then click Update now.

11.2 Schedule updates

Important
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

You can specify when or how often Sophos AutoUpdate updates.

1. On the Configure menu, click Updating.
2. Click the Schedule tab.
3. Select Enable automatic updates, and then enter the frequency (in minutes) with which Sophos AutoUpdate will update.
   - If the updated files are downloaded from your company network, updates are every 10 minutes by default.
   - If the updated files are downloaded over the internet from the Sophos server, Sophos AutoUpdate cannot update more frequently than every 60 minutes.

11.3 Set a source for updates

If you want Sophos AutoUpdate to update automatically, you must specify where it downloads updates from.

1. On the Configure menu, click Updating.
2. Click the Primary location tab.
3. In the Address list, enter the UNC path or web address of the update server.
   To download updates directly from Sophos via the internet, select Sophos in the Address list.
4. In the User name box, type the user name for the account that will be used to access the update server.
   - If the user name needs to be qualified to indicate the domain, use the form domain\username.
5. In the **Password** box, type the password for the account that will be used to access the update server.

### 11.4 Set an alternative source for updates

You can set an alternative source for updates. If Sophos AutoUpdate cannot update from its usual source, it will attempt to update from the alternative source.

1. On the **Configure** menu, click **Updating**.
2. Click the **Secondary location** tab.
3. In the **Address** list, enter the UNC path or web address of the update server.
   - To download updates directly from Sophos via the internet, select **Sophos** in the **Address** list.
4. In the **User name** box, type the user name for the account that will be used to access the update server.
   - If the user name needs to be qualified to indicate the domain, use the form `domain\username`.
5. In the **Password** box, type the password for the account that will be used to access the update server.

### 11.5 Update via a proxy server

If Sophos AutoUpdate updates via the internet, you must enter details of any proxy server that it must use to connect to the internet.

1. On the **Configure** menu, click **Updating**.
2. Click the **Primary location** or **Secondary location** tab.
3. Click **Proxy Details**.
4. Select the **Access the location via a proxy** check box.
5. Enter the proxy server **Address** and **Port** number.
6. Enter a **User name** and **Password** that grant access to the proxy server.
   - If the user name needs to be qualified to indicate the domain, use the form `domain\username`.

### 11.6 Update via a dial-up connection

To update via a dial-up connection to the internet:

1. On the **Configure** menu, click **Updating**.
2. Click the **Schedule** tab.
3. Select **Check for updates on dial-up**.
   - Sophos AutoUpdate will update whenever you connect to the internet.

### 11.7 Limit the bandwidth used for updating

To prevent Sophos AutoUpdate from using all your bandwidth when you need it for other purposes (such as downloading your email), you can limit the amount of bandwidth it uses.
1. On the Configure menu, click Updating.
2. Click the Primary location or Secondary location tab.
3. Click Advanced.
4. Select the Limit amount of bandwidth used check, and move the slider to specify the amount of bandwidth Sophos AutoUpdate uses.

**Note**
If you specify more bandwidth than is available, Sophos AutoUpdate uses all the bandwidth.

### 11.8 Log updating activity

You can configure Sophos AutoUpdate to record updating activity in a log file.

1. On the Configure menu, click Updating.
2. Click the Logging tab.
3. Select the Log Sophos AutoUpdate activity check box.
4. In the Maximum log size box, type or select the maximum size in MB for the log.
5. In the Log level list, select Normal or Verbose logging.
   
   **Verbose logging** provides information on many more activities than usual, so the log will grow faster. Use this option only when you need a detailed log for troubleshooting.

### 11.9 View the updating log file

1. On the Configure menu, click Updating.
2. Click the Logging tab.
3. Click View Log File.
12 Sophos Tamper Protection

12.1 About tamper protection on this computer

Tamper protection enables you to prevent unauthorized users (users with limited technical knowledge) and known malware from uninstalling Sophos security software or disabling it through the Sophos Endpoint Security and Control interface.

**Note**

Tamper protection is not designed to protect against users with extensive technical knowledge. It will not protect against malware which has been specifically designed to subvert the operation of the operating system to avoid detection. This type of malware will only be detected by scanning for threats and suspicious behavior. For more information, see the section Sophos Anti-Virus (chapter 4).

What does tamper protection mean for users of this computer?

**SophosUsers and SophosPowerUsers**

Tamper protection does not affect members of the SophosUser and SophosPowerUser groups. When tamper protection is enabled, they will be able to perform all tasks that they are usually authorized to perform, without the need to enter the tamper protection password.

SophosUsers or SophosPowerUsers cannot enable or disable tamper protection.

For more information about the tasks that each Sophos group is authorized to perform, see About Sophos groups (page 4).

**SophosAdministrators**

Members of the SophosAdministrator group can enable or disable tamper protection.

If a management console is used to administer Sophos Endpoint Security and Control on this computer, the tamper protection policy set up in the console determines the tamper protection configuration and password. If tamper protection is enabled from the console, ask your console administrator for a password if you need to perform any of the tasks mentioned below.

If you are a member of the SophosAdministrator group and if tamper protection is enabled, you must know the tamper protection password to perform the following tasks:

- Re-configure on-access scanning or suspicious behavior detection settings. For more information, see Enter the tamper protection password to configure the software (page 83).
- Disable tamper protection. For more information, see Disable tamper protection (page 82).
- Uninstall Sophos Endpoint Security and Control components (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, Sophos Remote Management System) using Control Panel.
- Uninstall Sophos SafeGuard Disk Encryption using Control Panel.

A SophosAdministrator who does not know the password will be able to perform all other tasks except for the ones mentioned above.

If tamper protection is disabled, but the tamper protection password has been set previously, you must use the **Authenticate user** option to authenticate yourself before you can re-enable tamper protection. All other configuration options available to the SophosAdministrators group...
are enabled when tamper protection is disabled. For more information about re-enabling tamper protection, see Re-enable tamper protection (page 83).

12.2 Enable tamper protection

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

When Sophos Endpoint Security and Control is first installed, tamper protection is disabled. If you are a SophosAdministrator, you can enable tamper protection.

To enable tamper protection:

1. On the **Home** page, under **Tamper protection**, click **Configure tamper protection**.
   For information about the **Home** page, see About the Home page (page 3).
2. In the **Tamper Protection Configuration** dialog box, select the **Enable tamper protection** check box.
3. Click **Set** under the **Password** box. In the **Tamper Protection Password** dialog box, enter and confirm the password.

   **Tip**
   The password must be at least eight characters long, and must contain numbers and upper and lower-case letters.

12.3 Disable tamper protection

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you are a member of the SophosAdministrator group, you can disable tamper protection.

To disable tamper protection:

1. If you haven’t already authenticated yourself, and the **Configure tamper protection** option on the **Home** page is unavailable, follow the instructions in Enter the tamper protection password to configure the software (page 83) before proceeding to step 2.
2. On the **Home** page, under **Tamper protection**, click **Configure tamper protection**.
   For information about the **Home** page, see About the Home page (page 3).
3. In the **Tamper Protection Configuration** dialog box, clear the **Enable tamper protection** check box and click **OK**.
12.4 Re-enable tamper protection

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

If you are a member of the SophosAdministrator group, you can re-enable tamper protection.

To re-enable tamper protection:

1. On the **Home** page, under **Tamper protection**, click **Authenticate user**.
   For information about the **Home** page, see **About the Home page** (page 3).
2. In the **Tamper Protection Authentication** dialog box, enter the tamper protection password and click **OK**.
3. On the **Home** page, under **Tamper protection**, click **Configure tamper protection**.
4. In the **Tamper Protection Configuration** dialog box, select the **Enable tamper protection** check box.

12.5 About the tamper protection password

When tamper protection is enabled, you must enter the tamper protection password if you want to configure on-access scanning, configure suspicious behavior detection, or disable tamper protection. You must be a member of the SophosAdministrator group to do this.

You need to enter the tamper protection password only once after you open Sophos Endpoint Security and Control. If you close Sophos Endpoint Security and Control and then open it again, you will need to enter the password again.

If you want to uninstall any of the Sophos Endpoint Security and Control components, you must enter the tamper protection password before you can disable tamper protection and then uninstall the software.

If tamper protection is disabled but the tamper protection password has been set previously, you must enter the password before you can re-enable tamper protection.

You will need to enter the tamper protection password to enable tamper protection if:

- You have previously enabled tamper protection, created a tamper protection password, and then disabled tamper protection.
- A tamper protection password has been created in the management console, but tamper protection is not enabled.

12.6 Enter the tamper protection password to configure the software

If you are a member of the SophosAdministrator group, you can authenticate yourself by entering the tamper protection password.

To authenticate yourself:

1. On the **Home** page, under **Tamper protection**, click **Authenticate user**.
12.7 Change the tamper protection password

**Important**
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.

You must be a member of the SophosAdministrator group to change the tamper protection password.

To change the tamper protection password:

1. If you haven’t already authenticated yourself, and the **Configure tamper protection** option on the Home page is unavailable, follow the instructions in **Enter the tamper protection password to configure the software** (page 83) before proceeding to step 2.
2. On the Home page, under **Tamper protection**, click **Configure tamper protection**.
   For information about the Home page, see **About the Home page** (page 3).
3. In the **Tamper Protection Configuration** dialog box, click **Change** under the **Password** box.
4. In the **Tamper Protection Password** dialog box, enter and confirm a new password.

**Tip**
The password should be at least eight characters long and contain numbers and mixed-case letters.

12.8 Uninstall Sophos security software

If you are a member of the SophosAdministrator group, you can uninstall the Sophos security software using Control Panel:

- Sophos Endpoint Security and Control components (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, Sophos Remote Management System)
- Sophos SafeGuard Disk Encryption

To uninstall Sophos security software when tamper protection is enabled:

1. On the Home page, under **Tamper protection**, click **Authenticate user**.
   For information about the Home page, see **About the Home page** (page 3).
2. In the **Tamper Protection Authentication** dialog box, enter the tamper protection password and click **OK**.
3. On the Home page, under **Tamper protection**, click **Configure tamper protection**.
4. In the **Tamper Protection Configuration** dialog box, clear the **Enable tamper protection** check box and click **OK**.
   Tamper protection is disabled.
5. In **Control Panel**, open **Add or Remove Programs**, locate the software you want to remove and click **Change/Remove** or **Remove**. Follow the instructions on screen for uninstalling the software.
12.9 View the tamper protection log

The tamper protection log shows two types of event:

- Successful tamper protection authentication events, showing the name of the authenticated user and the time of authentication.
- Failed attempts to tamper, showing the name of the targeted Sophos product or component, the time of the attempt, and the details of the user responsible for the attempt.

You must be a member of the SophosAdministrator group to view the tamper protection log.

To view the tamper protection log:

- On the Home page, under Tamper protection, click View tamper protection log.
  For information about the Home page, see About the Home page (page 3).

From the log page, you can copy the log to the clipboard, or email, or print the log.
To find specific text in the log, click Find and enter the text you want to find.
13 Troubleshooting

13.1 Updating has failed

13.1.1 About update failures

To find out more about an update failure, look at the update log: for information on how to do this, see View the updating log file (page 80).

The sections below explain why updating may fail, and how you can change the settings to correct the problem.

- Sophos Endpoint Security and Control contacts the wrong source for updates (page 86)
- Sophos Endpoint Security and Control cannot use your proxy server (page 86)
- Automatic updating is not correctly scheduled (page 86)
- The source for updates is not being maintained (page 87)

13.1.2 Sophos Endpoint Security and Control contacts the wrong source for updates

1. On the Configure menu, click Updating.
2. On the Primary location tab, check that the address and account details are those supplied by your administrator.
   For information on configuring the Primary location tab, see Set a source for updates (page 78).

13.1.3 Sophos Endpoint Security and Control cannot use your proxy server

If Sophos Endpoint Security and Control updates itself via the internet, you must make sure that it can use your proxy server (if there is one).

1. On the Configure menu, click Updating.
2. On the Primary location tab, click Proxy Details.
3. Ensure that the proxy server address, the port number, and the account details are correct.
   For information on entering proxy details, see Update via a proxy server (page 79).

13.1.4 Automatic updating is not correctly scheduled

1. On the Configure menu, click Updating.
2. Click the Schedule tab. (For information on the Schedule tab, see Schedule updates (page 78).)
3. If your computer is networked, or if you update via a broadband internet connection, select Enable automatic updates and enter the updating frequency. If you update via a dial-up connection, select Check for updates on dial-up.
13.1.5 The source for updates is not being maintained

Your company may have moved the directory (on the network or on a web server) from which you should update. Alternatively, they may not be maintaining the directory.

If you think this may be the case, contact your network administrator.

13.2 Threat not cleaned

If Sophos Anti-Virus has not cleaned a threat from your computer, it may be because of the following.

Automatic cleanup is disabled

If Sophos Anti-Virus has not attempted cleanup, check that automatic cleanup has been enabled. For information on enabling automatic cleanup, see the following topics:

• Configure on-access cleanup (page 10)
• Configure right-click cleanup (page 14)
• Configure cleanup for a custom scan (page 18)

Automatic cleanup of adware and PUAs is not available for on-access scanning.

Cleanup failed

If Sophos Anti-Virus could not clean a threat ("Cleanup failed"), it may be that it cannot clean that type of threat, or you have insufficient access rights.

Full computer scan is required

You may need to run a full computer scan to determine all components of a multi-component threat, or to detect a threat in files that were previously hidden, before Sophos Anti-Virus can clean it from your computer.

1. To scan all disk drives, including boot sectors, on the computer, run the Scan my computer scan. For information, see Run a full computer scan (page 20).

2. If the threat has still not been fully detected, it may be because you have insufficient access rights, or some drives or folders on the computer, containing the threat’s components, are excluded from scanning. For information, see Exclude items from on-access scanning (page 21). Check the list of the items excluded from scanning. If there are some items on the list, remove them from the list and scan your computer again.

Removable medium is write-protected

If dealing with a removable medium (e.g. floppy disk, CD), make sure that it is not write-protected.
NTFS volume is write-protected

If dealing with files on an NTFS volume (Windows XP or later), make sure that it is not write-protected.

Virus/spyware fragment has been reported

Sophos Anti-Virus does not clean a virus/spyware fragment because it has not found an exact virus/spyware match. Refer to Virus/spyware fragment reported (page 88).

13.3 Virus/spyware fragment reported

If a virus/spyware fragment is reported, do the following:

1. Update your protection immediately, so that Sophos Anti-Virus has the latest virus identity files.
2. Run a full computer scan.
   - Update immediately (page 78)
   - Run a full computer scan (page 20)

If virus/spyware fragments are still reported, contact Sophos technical support for advice.
   - Technical support (page 100)

The report of a virus/spyware fragment indicates that part of a file matches part of a virus or item of spyware. There are three possible causes:

Variant of a known virus or item of spyware

Many new viruses or items of spyware are based on existing ones, so that code fragments typical of a known virus or item of spyware may appear as part of a new one. If a virus/spyware fragment is reported, it is possible that Sophos Anti-Virus has detected a new virus or item of spyware, which could become active.

Corrupted virus

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by Sophos Anti-Virus. A corrupted virus cannot spread.

Database containing a virus or item of spyware

When running a full computer scan, Sophos Anti-Virus may report that there is a virus/spyware fragment in a database file. If this is the case, do not delete the database. Contact Sophos technical support for advice.

For information about contacting technical support, see Technical support (page 100).
13.4 Threat partially detected

To scan all disk drives, including boot sectors, on the computer, run a full computer scan.

- Run a full computer scan (page 20)

If the threat has still not been fully detected, it may be because some drives or folders on the computer, containing the threat’s components, are excluded from scanning. If there are some of these items on the exclusion list, remove them, and then scan your computer again.

- Exclude items from on-demand scanning (page 21)

If the threat has still not been fully detected, it may be because you have insufficient access rights. Sophos Anti-Virus may not be able to fully detect or remove threats with components installed on network drives.

13.5 Adware or PUA disappeared from quarantine

If an item of adware or PUA detected by Sophos Anti-Virus has disappeared from Quarantine manager without you taking any action, the adware or PUA might have been authorized or cleaned up from the management console or by another user. Check the list of authorized adware and PUAs to see if it has been authorized. To find out how to do this, refer to Authorize adware and PUAs (page 31).

13.6 Computer becomes slow

If your computer has become very slow, it may be that you have a PUA running on and monitoring your computer. If you have on-access scanning enabled, you may also see many desktop alerts warning about a PUA. To solve the problem, do the following.

1. Run the Scan my computer scan to detect all components of the PUA. For information, see Run a full computer scan (page 20).

   Note
   If after the scan the PUA is partially detected, refer to Threat partially detected (page 89), step 2.

2. Clean the adware or PUA from your computer. To find out how to do this, refer to Deal with adware and PUAs in quarantine (page 36).

13.7 Allow access to drives with infected boot sectors

Important
If a management console is used to administer Sophos Endpoint Security and Control on this computer, it may override any changes you make here.
By default, Sophos Anti-Virus prevents access to removable disks whose boot sectors are infected.

To allow access (for example, to copy files from a floppy disk infected with a boot sector virus):

1. Click Home > Anti-virus and HIPS > Configure anti-virus and HIPS > Configure > On-access scanning.
2. On the Scanning tab, select Allow access to drives with infected boot sectors check box.

**Important**

As soon as you have finished accessing the disk, clear the check box, and then remove the disk from the computer so that it cannot try to re-infect the computer on restart.

### 13.8 Unable to access areas of Sophos Endpoint Security and Control

If you are unable to use or configure particular areas of Sophos Endpoint Security and Control it might be because access to these areas is restricted to members of particular Sophos user groups.

For more information about Sophos user groups, see About Sophos groups (page 4).

### 13.9 Recovering from virus side-effects

Recovery from virus infection depends on how the virus infected the computer.

**Virus side-effects**

Some viruses leave you with no side-effects to deal with, others may have such extreme side-effects that you have to restore a hard disk in order to recover.

Some viruses gradually make minor changes to data. This type of corruption can be hard to detect.

**What to do**

It is very important that you read the threat analysis on the Sophos website, and check documents carefully after cleanup. Refer to Get cleanup information (page 40) to find out how to view details on the Sophos website of the virus’s side-effects.

Sound backups are crucial. If you did not have them before you were infected, start keeping them in case of future infections.

Sometimes you can recover data from disks damaged by a virus. Sophos can supply utilities for repairing the damage caused by some viruses.

Contact Sophos technical support for advice.

For information about contacting technical support, see Technical support (page 100).
13.10 Recovering from adware and PUA side-effects

Removing adware and PUAs may have some side-effects that cannot be eliminated during cleanup.

Operating system has been modified

Some items of adware and PUAs modify the Windows operating system, for example, change your internet connection settings. Sophos Anti-Virus cannot always restore all settings to the values they had before installation of the adware or PUA. If, for example, an item of adware or PUA changed the browser home page, then Sophos Anti-Virus cannot know what the previous home page setting was.

Utilities not cleaned

Some items of adware and PUAs can install utilities, such as .dll or .ocx files, on your computer. If a utility is harmless (that is, it does not possess the qualities of adware and PUAs), for example, a language library, and is not integral to the adware or PUA, Sophos Anti-Virus may not detect it as part of the adware or PUA. In this case, the file is not removed from your computer even after the adware or PUA that installed the file has been cleaned from the computer.

Adware or PUA is part of a program you need

Sometimes an item of adware or PUA is part of a program that you intentionally installed, and needs to be there for the program to run. If you remove the adware or PUA, the program may stop running on your computer.

What to do

It is very important that you read the threat analysis on the Sophos website. Refer to Get cleanup information (page 40) to find out how to view details on the Sophos website of the adware or PUA’s side-effects.

To be able to recover your system and its settings to their previous state, you should maintain regular backups of your system. You should also make backup copies of the original executable files of the programs you want to use.

For more information or advice on recovering from adware and PUA side-effects, contact Sophos technical support.

For information about contacting technical support, see Technical support (page 100).

13.11 Password error reported

If you are trying to schedule a custom scan, and an error message is displayed about the password, make sure of the following:
• The password is correct for the user account
• The password is not blank

To make sure that the password is correct, check the properties of the user account in User Accounts in Control Panel.

13.12 "Service failure" error message

Symptoms

You see one of the following error messages in the notification area:
• Anti-virus and HIPS: service failure
• Firewall: service failure

Causes

One of the Sophos Endpoint Security and Control services on your computer has failed, and needs to be restarted.

Resolve the problem

2. Do one of the following:
   • If you see an Anti-virus and HIPS: service failure error message, right-click Sophos Anti-Virus, and then click Restart.
   • If you see a Firewall: service failure error message, right-click Sophos Client Firewall Manager, and then click Restart.

Notes

• To open Services, click Start, click Control Panel, double-click Administrative Tools, and then double-click Services.

13.13 Firewall log database is corrupted

Symptom

Whilst using the firewall log viewer, you see the error message “The current Sophos Client Firewall log database is corrupted.”

Cause

The firewall’s event log database has become corrupted and needs to be recreated.
Resolve the problem

You need to be a member of the Windows Administrators group on this computer to do this.

2. Right-click Sophos Client Firewall Manager, and then click Stop.
3. Using Windows Explorer, navigate to C:\Documents and Settings\All Users \Application Data\Sophos\Sophos Client Firewall\logs.
   To view this hidden folder, you may need to display hidden files and folders in Windows Explorer.
4. Delete op_data.mdb.
5. In Services, right-click Sophos Client Firewall Manager, and then click Start.

Notes

- To open Services, click Start, click Control Panel, double-click Administrative Tools, and then double-click Services.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>adware and PUAs</td>
<td>Adware displays advertising, for example, pop-up messages, which affects user productivity and system efficiency. A potentially unwanted application (PUA) is an application that is not inherently malicious but is generally considered unsuitable for the majority of business networks.</td>
</tr>
<tr>
<td>application rule</td>
<td>A rule that applies only to packets of data transferred over the network to or from a particular application.</td>
</tr>
<tr>
<td>Authorization manager</td>
<td>The module that enables you to authorize adware and PUAs, suspicious files, and applications that exhibit suspicious behavior and buffer overflows.</td>
</tr>
<tr>
<td>automatic cleanup</td>
<td>Cleanup that is performed without any intervention or acceptance by you.</td>
</tr>
<tr>
<td>blocked</td>
<td>A status showing that applications (including hidden processes), connections, protocols, ICMP messages, and so on have been refused network access.</td>
</tr>
<tr>
<td>buffer overflow detection</td>
<td>Detects buffer overflow attacks.</td>
</tr>
<tr>
<td>checksum</td>
<td>Each version of an application has a unique checksum. The firewall can use this checksum to decide whether an application is allowed or not.</td>
</tr>
<tr>
<td>cleanup</td>
<td>Cleanup eliminates threats on your computer by removing a virus from a file or boot sector, moving or deleting a suspicious file, or deleting an item of adware or PUA. It is not available for threats that are detected by web page scanning because the threats are not downloaded to your computer. Therefore, there is no need to take any action.</td>
</tr>
<tr>
<td>Content Control List (CCL)</td>
<td>A set of conditions that specify file content, for example, credit or debit card numbers, or bank account details near to other forms of personally identifiable information. There are two types of Content Control List: SophosLabs Content Control List and custom Content Control List.</td>
</tr>
<tr>
<td>content rule</td>
<td>A rule that contains one or more Content Control Lists and specifies the action that is taken if the user attempts to transfer data that matches all the Content Control Lists in the rule to the specified destination.</td>
</tr>
<tr>
<td>controlled application data</td>
<td>Detection data that defines which applications are controlled.</td>
</tr>
</tbody>
</table>
custom rule
A rule created by the user to specify the circumstances under which an application is allowed to run.

data control
A feature to reduce accidental data loss from workstations. It works by taking action when a workstation user tries to transfer a file that meets criteria defined in the data control policy and rules. For example, when a user attempts to copy a spreadsheet containing a list of customer data to a removable storage device or upload a document marked as confidential into a webmail account, data control will block the transfer, if configured to do so.

data view
The view that displays different data depending on the item selected in the tree view.

description bar
A bar in the log viewer which appears above the data view and contains the name of the currently selected item in the tree view.

device control
A feature to reduce accidental data loss from workstations and restrict introduction of software from outside of the network. It works by taking action when a workstation user tries to use an unauthorized storage device or networking device on their workstation.

download reputation
Reputation of a file downloaded from the internet. The reputation is calculated based on the file’s age, source, prevalence, deep content analysis and other characteristics. It helps to establish whether the file is safe or is a potential risk and may harm a user’s computer if downloaded.

extensive scanning
Scans every part of every file.

firewall event
A situation that occurs when an unknown application, or the operating system, on one computer tries to communicate with another computer over a network connection in a way that was not specifically requested by the applications running on the other computer.

firewall policy
The settings issued by the management console which the firewall uses to monitor the computer’s connection to the internet and other networks.

global rules
Rules that are applied to all network connections and applications which do not already have a rule. They take lower priority than the rules set on the LAN page. They also take lower priority than application rules (unless the user specifies otherwise).

hidden process
An application sometimes launches a hidden process to perform some network access for it. Malicious applications may use this technique to
evade firewalls: they launch a trusted application to access the network rather than doing so themselves.

**high-priority global rule**
A rule that is applied before any other global or application rule.

**Host Intrusion Prevention System (HIPS)**
Overall term for pre-execution behavior analysis and runtime behavior analysis.

**ICMP**
Abbreviation for "Internet Control Message Protocol." A network-layer internet protocol that provides error correction and other information relevant to IP packet processing.

**ICMP settings**
The settings that specify which types of network management communication are allowed.

**instant messaging**
A category of controlled applications that includes instant messaging client applications (e.g. MSN).

**interactive mode**
The mode in which the firewall displays one or more learning dialogs when it detects network traffic for which it has no rule. This feature applies only to Sophos Client Firewall for Windows 7 and earlier.

**learning dialog**
A dialog box that asks the user to choose whether to allow or block network activity when an unknown application requests network access. This feature applies only to Sophos Client Firewall for Windows 7 and earlier.

**log cleanup settings**
The settings that control when records are deleted.

**log viewer**
A form where users can view details from the event database, such as connections that have been allowed or blocked, the system log and any alerts that have been raised.

**Malicious Traffic Detection**
A feature that detects communications between compromised computers and attackers' command and control servers.

**manual cleanup**
Cleanup that is performed by using special disinfectors or utilities, or by deleting files manually.

**match**
Equal the content that is defined in a Content Control List.

**NetBIOS**
Abbreviation for "Network Basic Input/Output System." Software that provides an interface between the operating system, the I/O bus, and the network. Nearly all Windows-based LANs are based on NetBIOS.

**network protocol**
A set of rules or standards designed to enable computers to connect with one another over a
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-interactive mode</td>
<td>The mode in which the firewall either blocks or allows all network traffic for which it has no rule.</td>
</tr>
<tr>
<td>normal scanning</td>
<td>Scans only those parts of each file that are likely to be infected with a virus.</td>
</tr>
<tr>
<td>on-access scan</td>
<td>Your main method of protection against threats. Whenever you copy, move, or open a file, or start a program, Sophos Anti-Virus scans the file or program and grants access to it only if it does not pose a threat to your computer or has been authorized for use.</td>
</tr>
<tr>
<td>on-demand scan</td>
<td>A scan that you initiate. You can use an on-demand scan to scan anything from a single file to everything on your computer that you have permission to read.</td>
</tr>
<tr>
<td>primary configuration</td>
<td>The firewall configuration used for the corporate network that the user connects to for their day-to-day business.</td>
</tr>
<tr>
<td>process settings</td>
<td>The settings that specify whether modified or hidden processes should be allowed network access.</td>
</tr>
<tr>
<td>Quarantine manager</td>
<td>The module that enables you to view and deal with items that have been quarantined.</td>
</tr>
<tr>
<td>rawsocket</td>
<td>Rawsockets allow processes to control all aspects of the data they send over the network and can be used for malicious purposes.</td>
</tr>
<tr>
<td>right-click scan</td>
<td>A scan of file(s) in Windows Explorer or on the desktop that you run using the shortcut menu.</td>
</tr>
<tr>
<td>rootkit</td>
<td>A Trojan or technology that is used to hide the presence of a malicious object (process, file, registry key, or network port) from the computer user or administrator.</td>
</tr>
<tr>
<td>runtime behavior analysis</td>
<td>Dynamic analysis performed by suspicious behavior detection and buffer overflow detection.</td>
</tr>
<tr>
<td>scanning error</td>
<td>An error in scanning a file, e.g. access denied.</td>
</tr>
<tr>
<td>scheduled scan</td>
<td>A scan of your computer, or parts of your computer, that runs at set times.</td>
</tr>
<tr>
<td>secondary configuration</td>
<td>The firewall configuration used when users are not connected to the main corporate network, but to another network such as a hotel or airport wireless network or another corporate network.</td>
</tr>
<tr>
<td>spyware</td>
<td>A program that installs itself onto a user’s computer by stealth, subterfuge, or social engineering, and sends information from that computer to a third party without the user's permission or knowledge.</td>
</tr>
</tbody>
</table>
Sophos Live Protection
A feature that uses in-the-cloud technology to instantly decide whether a suspicious file is a threat and take action specified in the Sophos anti-virus cleanup configuration.

stateful inspection
Firewall technology that keeps a table of active TCP and UDP network connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.

storage device
Removable storage devices (for example, USB flash drives, PC Card readers, and external hard disk drives), CD/DVD drives, floppy disk drives, and secure removable storage devices (for example, SanDisk Cruzer Enterprise, Kingston Data Traveller, IronKey Enterprise, and IronKey Basic USB flash drives with hardware encryption).

suspicious behavior detection
Dynamic analysis of the behavior of all programs running on the system in order to detect and block activity which appears to be malicious.

suspicious file
A file that exhibits a combination of characteristics that are commonly, but not exclusively, found in viruses.

system memory
The memory that acts as a bridge between applications and the actual data processing done at the hardware level. It is used by the operating system.

system rule
A rule that will be applied to all applications and will allow or block low-level system network activity.

tamper protection
A feature that prevents unauthorized users (local administrators and users with limited technical knowledge) and known malware from uninstalling Sophos security software or disabling it through the Sophos Endpoint Security and Control interface.

threat event
Detection or disinfection of a threat.

tree view
The view that controls what data the log viewer displays in its data view.

true file type
The file type that is ascertained by analyzing the structure of a file as opposed to the filename extension. This is a more reliable method.

trusted application
An application that is allowed full and unconditional access to the network.

unidentified virus
A virus for which there is no specific identity.

unknown traffic
A form of network access by an application or service for which the firewall has no rule.

virus identity file (IDE)
A file that enables Sophos Anti-Virus to detect and disinfect a particular virus, Trojan, or worm.
Voice over IP

A category of controlled applications that includes Voice over IP client applications.

working mode

The setting that determines whether the firewall applies actions with input from the user (interactive mode) or automatically (the non-interactive modes). The interactive mode was removed in Sophos Client Firewall for Windows 8 and later.
15 Technical support

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

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.
16 Legal notices

Copyright © 2018 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.

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 Software License

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 https://www.sophos.com/en-us/support/contact-support.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.

crt

# $FreeBSD$
# @(#)COPYRIGHT 8.2 (Berkeley) 3/21/94

The compilation of software known as FreeBSD is distributed under the following terms:

Copyright (c) 1992-2013 The FreeBSD 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.

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.

The 4.4BSD and 4.4BSD-Lite software is distributed under the following terms:

All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by The Regents of the University of California.


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 acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.

4. 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.

The Institute of Electrical and Electronics Engineers and the American National Standards Committee X3, on Information Processing Systems have given us permission to reprint portions of their documentation.

In the following statement, the phrase "this text" refers to portions of the system documentation.

Portions of this text are reprinted and reproduced in electronic form in the second BSD Networking Software Release, from IEEE Std 1003.1-1988, IEEE Standard Portable Operating System Interface for Computer Environments (POSIX), copyright C 1988 by the Institute of Electrical and Electronics Engineers, Inc. In the event of any discrepancy between these versions and the original IEEE Standard, the original IEEE Standard is the referee document.

In the following statement, the phrase "This material" refers to portions of the system documentation. This material is reproduced with permission from American National Standards Committee X3, on Information Processing Systems. Computer and Business Equipment Manufacturers Association (CBEMA), 311 First St., NW, Suite 500, Washington, DC 20001-2178. The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at ftp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License. Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

"3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors."
Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

dtoa.c

The author of this software is David M. Gay.


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.

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.
IEEE Software Taggant Library

This software was developed by The Institute of Electrical and Electronics Engineers, Incorporated (IEEE), through the Industry Connections Security Group (ICSG) of its Standards Association. Portions of it include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/), and those portions are governed by the OpenSSL Toolkit License.

IEEE License

Copyright (c) 2012 IEEE. 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 IEEE Industry Connections Security Group (ICSG)."

4. The name "IEEE" must not be used to endorse or promote products derived from this software without prior written permission from the IEEE Standards Association (stds.ipr@ieee.org).

5. Products derived from this software may not contain "IEEE" in their names without prior written permission from the IEEE Standards Association (stds.ipr@ieee.org).

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the IEEE Industry Connections Security Group (ICSG)."

THIS SOFTWARE IS PROVIDED "AS IS" AND "WITH ALL FAULTS." IEEE AND ITS CONTRIBUTORS EXPRESSLY DISCLAIM ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION: (A) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; (B) ANY WARRANTY OF NON-INFRINGEMENT; AND (C) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, EFFECTIVENESS, CURRENCY OR COMPLETENESS OF THE SOFTWARE.

IN NO EVENT SHALL IEEE 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 AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

THIS SOFTWARE USES STRONG CRYPTOGRAPHY, WHICH MAY BE SUBJECT TO LAWS AND REGULATIONS GOVERNING ITS USE, EXPORTATION OR IMPORTATION. YOU ARE SOLELY RESPONSIBLE FOR COMPLYING WITH ALL APPLICABLE LAWS AND REGULATIONS, INCLUDING, BUT NOT LIMITED TO, ANY THAT GOVERN YOUR USE, EXPORTATION OR IMPORTATION OF THIS SOFTWARE. IEEE AND ITS CONTRIBUTORS DISCLAIM ALL LIABILITY ARISING FROM YOUR USE OF THE SOFTWARE IN VIOLATION OF ANY APPLICABLE LAWS OR REGULATIONS.
Info-ZIP

Copyright © 1990–2007 Info-ZIP. All rights reserved.

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


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 and libraries) 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, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP—must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from 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 the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.


Jansson

Copyright (c) 2009-2013 Petri Lehtinen <petri@digip.org>

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.

Lua

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Lua License. A copy of the license agreement for any such included software can be found at http://www.lua.org/copyright.html

Microsoft software

This Sophos product may include certain Microsoft software, licensed to Sophos for inclusion and use herein.

Mersenne Twister (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.

OpenSSL Cryptography and SSL/TLS 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
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.]

Protocol Buffers (libprotobuf)

Copyright 2008, Google Inc.

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 Google Inc. 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.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when
generating it. This code is not standalone and requires a support library to be linked with it. This
support library is itself covered by the above license.

**pstdint**

Copyright (c) 2005-2007 Paul Hsieh
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 name of the author may not be used to endorse or promote products derived from this
   software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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.

**Simple ECMAScript Engine (SEE)**


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.

SQLCipher

Copyright © 2008-2012 Zetetic LLC
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 the ZETETIC LLC 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 ZETETIC LLC "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 ZETETIC LLC 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.
Udis86

Copyright (c) 2002-2009 Vivek Thampi
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.

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.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the FreeBSD Project.

Unicode

UNICODE, INC. LICENSE AGREEMENT – DATA FILES AND SOFTWARE


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

Windows Template Library (WTL)

This product may contain Windows Template Library (WTL) and/or WixToolset code, which are licensed under the Common Public License 1.0. The source code for the components is available from Sophos, upon request, by emailing TPCRequest@sophos.com

wow64ext library

This is used in Sophos Virus Removal Tool as a shared library [wow64ext.dll], which may be removed or substituted without affecting other functionality. Its use is covered by the following license:
GNU LESSER GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc.

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, "this License" refers to version 3 of the GNU Lesser General Public License, and the "GNU GPL" refers to version 3 of the GNU General Public License.

"The Library" refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An "Application" is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.


The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.
4. **Combined Works.**

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at runtime a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. **Combined Libraries.**

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. **Revised Versions of the GNU Lesser General Public License.**

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.
If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.
Index

A
access rights 4, 90
accessing disks 7, 89
adding users to Sophos groups 5
adware
  authorizing 31
  automatic cleanup 14, 18
  scanning for 7, 13, 16
adware in quarantine, dealing with 36
all files, scanning 7, 13, 16
allowing
  applications 56
  email 53
  file and printer sharing 55, 55
  FTP downloads 54
  hidden processes 69
  LAN traffic 54
  rawsockets 69
  web browsers 53
analyses of threats 40
anti-virus
  configuring desktop messaging 41
  configuring email alerting 42
  configuring event logging 43
  configuring SNMP messaging 43
applications
  allowing 56
  blocking 56
  using checksums to authenticate 70
archive files, scanning 7, 13, 16
authenticate applications, using checksums to 70
authorized adware, blocking 31
authorized PUAs, blocking 31
authorizing
  adware 31
  buffer overflows 32, 38
  controlled applications 39
  PUAs 31
  suspicious behavior 32, 38
  suspicious files 32
  websites 32
automatic cleanup
  adware 14, 18
  PUAs 14, 18
  spyware 10, 14, 18
  suspicious files 10, 14, 18
  viruses 10, 14, 18

B
bandwidth used for updating, limiting 79
behavior monitoring
  enabling 26
  blocking
    applications 56
    authorized adware 31
    authorized PUAs 31
    file and printer sharing 56
    IPv6 57
    malicious websites 30
buffer overflows
  authorizing 32, 38
  detecting 27

central reporting, configuring 72
checksum learning dialogs
  enabling 57
  interactive mode 62
checksums, using to authenticate applications 70
cleanup
  about 40
  troubleshooting 87
configuring
  anti-virus desktop messaging 41
  anti-virus email alerting 42
  anti-virus event logging 43
  anti-virus SNMP messaging 43
  central reporting 72
  custom scans 16
  firewall logging 75
  on-access scanning 7
  right-click scanning 13
  scanning log 44
  user rights for Quarantine manager 5
count scanning 29, 30
controlled applications
  authorizing 39
  dealing with 39
  scanning for 45
creating custom scans 15
custom scan log
  viewing 20
custom scans
  configuring 16
  creating 15
  deleting 20
  renaming 20
  running 19
  scheduling 19

data control, temporarily disabling 49
dealing with adware in quarantine 36
dealing with controlled applications 39
dealing with PUAs in quarantine 36
dealing with spyware in quarantine 35
dealing with suspicious behavior in quarantine 38
dealing with suspicious files in quarantine 37
dealing with viruses in quarantine 35
deleting custom scans 20
detecting buffer overflows 27
detecting malicious behavior 26
detecting suspicious behavior 26
device control 47
disabling on-access scanning 9
disabling scanning 47
disabling scanning for controlled applications 45
disabling the firewall 53
disabling web control 51
disinfection 87
download reputation 29, 30

email, allowing 53
enabling checksum learning dialogs 57
enabling on-access scanning 9
encryption software
  on-access scanning 7, 7, 9, 11, 21
excluding items from on-access scanning 21
excluding items from on-demand scanning 21
exporting firewall configuration files 63
exporting records from firewall log viewer 77, 77

file and printer sharing, allowing 55, 55
file and printer sharing, blocking 56
file sharing, allowing 55, 55
file sharing, blocking 56
filtering ICMP messages 58
filtering log records 76
firewall
  disabling 53
firewall configuration files
  exporting 63
  importing 63
firewall log viewer
  exporting records 77, 77
firewall logging
  configuring 75
fragment 87
fragment reported, troubleshooting 88
FTP downloads, allowing 54
full computer scans, running 20

getting cleanup information 40
getting started
  what to do first 52
global rules
  setting 64, 66, 68

hidden processes, allowing 69
HIPS 25
Home page 3
Host Intrusion Prevention System 25

ICMP messages
  filtering 58
  information about 58
icons
  items to scan 16
immediate updating 78
importing firewall configuration files 63
in-the-cloud technology 27
infected boot sector 7, 89
information on cleanup 40
interactive mode
  application messages 61
  checksum learning dialogs 62
  hidden process messages 61
  protocol messages 61
  rawsocket messages 61
  interactive mode, about 60
  interactive mode, enabling 60
IPv6
  blocking 57

LAN traffic, allowing 54
limiting bandwidth used for updating 79
location awareness
  about 70
  creating secondary configurations 72
  defining primary locations 71
  using two network adapters 70
log records
  filtering 76
log viewer
  about 74
logging updates 80
Mac viruses, scanning for 7
malicious behavior
  detecting 26
malicious websites
  protection 30
non-interactive mode, changing to a 60

on-access and on-demand scanning, difference 7
on-access scanning
  configuring 7
  disabling 9
  enabling 9
  excluding items from 21
  specifying file extensions 11
on-demand scanning
  excluding items from 21
specifying file extensions 12
on-demand scans, types of 12

P
partial detection 89
password error 91
pre-authorizing suspicious items 32
primary locations
defining 71
primary server 78
printer sharing, allowing 55, 55
printer sharing, blocking 56
priority, scanning 16
proxy server 79
PUAs
authorizing 31
automatic cleanup 14, 18
scanning for 7, 13, 16
PUAs in quarantine, dealing with 36

Q
Quarantine manager 33

R
rawsockets, allowing 69
recovering from side-effects 91
renaming custom scans 20
resetting scanned file checksums 11
right-click scanning 15
right-click scanning, configuring 13
right-click scans, running 15
rootkits, scanning for 16
rule
set 65, 66, 66
rule priority 63
run scan at lower priority 16
running custom scans 19
running full computer scans 20
running right-click scans 15
runtime behavior analysis 26

S
scanned file checksums, resetting 11
scanning all files 7, 13, 16
scanning archive files 7, 13, 16
scanning for adware and PUAs 7, 13, 16
scanning for controlled applications 45
scanning for controlled applications, disabling 45
scanning for Mac viruses 7
scanning for rootkits 16
scanning for suspicious files 7, 13, 16
scanning log
configuring 44
viewing 44
scanning single items 15
scanning system memory 7, 16
scheduling a scan 91
scheduling custom scans 19
scheduling updates 78
secondary configurations
creating 72
secondary server 79
security information 40
setting a rule 65, 66, 66
setting global rules 64, 66, 68
side-effects 91
single item scanning 15
slow computer, troubleshooting 89
Sophos groups
adding users to 5
Sophos Live Protection
disabling 28
enabling 28
in-the-cloud technology 27
log 28
overview 27
turning off 28
turning on 28
specifying on-access scanning file extensions 11
spyware
automatic cleanup 10, 14, 18
spyware in quarantine, dealing with 35
suspending scanning 47
suspicious behavior
authorizing 32, 38
detecting 26
suspicious behavior in quarantine, dealing with 38
suspicious files
authorizing 32
automatic cleanup 10, 14, 18
scanning for 7, 13, 16
suspicious files in quarantine, dealing with 37
suspicious items, pre-authorizing 32
system memory scanning 7, 16
system tray icon 86

T
tamper protection
authenticating user 83
changing password 84
configuring the software 83
disabling 82
enabling 82
entering password 83
log 85
overview 81
re-enabling 83
turning off 82
turning on 82
uninstalling Sophos Endpoint Security and Control 84
uninstalling Sophos security software 84
threat partially detected 89
two network adapters
using 70
types of on-demand scan 12
uninstalling Sophos security software 84
updating 78, 80, 86
updating via dial-up connection 78
URL filtering 29, 30
user groups 4, 90
user rights 4, 90
user rights for Quarantine manager, configuring 5

viewing
  custom scan log 20
  scanning log 44
viruses
  automatic cleanup 10, 14, 18
  recovering from side-effects 90
viruses in quarantine, dealing with 35

web browsers, allowing 53
web control
  disabling 51
  overview 51
web protection
  blocking access to malicious websites 29, 30
  configuring 30
  content scanning 29, 30
  download reputation 29, 30
  overview 29
  URL filtering 29, 30
websites
  authorizing 32
working mode, changing to interactive 60