SOPHOS
Cybersecurity made simple.

Sophos Enterprise Console Help
product version: 5.5
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About Sophos Enterprise Console</td>
<td>1</td>
</tr>
<tr>
<td>Accessibility</td>
<td>2</td>
</tr>
<tr>
<td>Recommended accessibility settings</td>
<td>2</td>
</tr>
<tr>
<td>Guide to the Sophos Enterprise Console Interface</td>
<td>4</td>
</tr>
<tr>
<td>User interface layout</td>
<td>4</td>
</tr>
<tr>
<td>Toolbar buttons</td>
<td>4</td>
</tr>
<tr>
<td>Dashboard panels</td>
<td>6</td>
</tr>
<tr>
<td>Security status icons</td>
<td>7</td>
</tr>
<tr>
<td>Navigating the Endpoints view</td>
<td>8</td>
</tr>
<tr>
<td>Computer list icons</td>
<td>9</td>
</tr>
<tr>
<td>Filter computers by the name of a detected item</td>
<td>10</td>
</tr>
<tr>
<td>Find a computer in Sophos Enterprise Console</td>
<td>11</td>
</tr>
<tr>
<td>Navigating the Update managers view</td>
<td>12</td>
</tr>
<tr>
<td>Getting started with Sophos Enterprise Console</td>
<td>13</td>
</tr>
<tr>
<td>Setting up Sophos Enterprise Console</td>
<td>15</td>
</tr>
<tr>
<td>Managing roles and sub-estates</td>
<td>15</td>
</tr>
<tr>
<td>Creating and using groups</td>
<td>24</td>
</tr>
<tr>
<td>Creating and using policies</td>
<td>27</td>
</tr>
<tr>
<td>Discovering computers on the network</td>
<td>34</td>
</tr>
<tr>
<td>Synchronizing with Active Directory</td>
<td>38</td>
</tr>
<tr>
<td>Configure the Sophos Mobile URL</td>
<td>45</td>
</tr>
<tr>
<td>Multi-factor authentication</td>
<td>46</td>
</tr>
<tr>
<td>Protecting computers</td>
<td>49</td>
</tr>
<tr>
<td>Prepare for installation of security software</td>
<td>49</td>
</tr>
<tr>
<td>Remove third-party security software</td>
<td>49</td>
</tr>
<tr>
<td>Protect computers automatically</td>
<td>50</td>
</tr>
<tr>
<td>Locate installers for protecting computers manually</td>
<td>52</td>
</tr>
<tr>
<td>Checking whether your network is protected</td>
<td>52</td>
</tr>
<tr>
<td>Configure the Dashboard</td>
<td>53</td>
</tr>
<tr>
<td>Check that computers are protected</td>
<td>53</td>
</tr>
<tr>
<td>Check that computers are up to date</td>
<td>54</td>
</tr>
<tr>
<td>Find computers with problems</td>
<td>54</td>
</tr>
<tr>
<td>Dealing with alerts and errors</td>
<td>55</td>
</tr>
<tr>
<td>Scanning and cleaning up computers now</td>
<td>58</td>
</tr>
<tr>
<td>Updating computers</td>
<td>61</td>
</tr>
<tr>
<td>Configuring the update manager</td>
<td>61</td>
</tr>
<tr>
<td>Configuring software subscriptions</td>
<td>69</td>
</tr>
<tr>
<td>Configuring the updating policy</td>
<td>73</td>
</tr>
<tr>
<td>Change primary server credentials</td>
<td>78</td>
</tr>
<tr>
<td>Schedule updates</td>
<td>80</td>
</tr>
<tr>
<td>Monitoring the update manager</td>
<td>82</td>
</tr>
<tr>
<td>Update out-of-date computers</td>
<td>83</td>
</tr>
<tr>
<td>Configuring policies</td>
<td>85</td>
</tr>
<tr>
<td>Anti-virus and HIPS policy</td>
<td>85</td>
</tr>
<tr>
<td>On-access scanning</td>
<td>87</td>
</tr>
<tr>
<td>On-demand and scheduled scanning</td>
<td>93</td>
</tr>
<tr>
<td>Behavior monitoring</td>
<td>100</td>
</tr>
<tr>
<td>Sophos Live Protection</td>
<td>104</td>
</tr>
<tr>
<td>Web protection</td>
<td>106</td>
</tr>
<tr>
<td>Scanned file types and exclusions</td>
<td>109</td>
</tr>
<tr>
<td>Authorizing items for use</td>
<td>113</td>
</tr>
<tr>
<td>Firewall policy</td>
<td>117</td>
</tr>
</tbody>
</table>

(2020/02/14)
Copy computer details for a computer...................................................................................... 220
Print computer details for a computer.......................................................................................221
Troubleshooting................................................................................................................................. 222
Computers are not running on-access scanning........................................................................ 222
The firewall is disabled.................................................................................................................... 222
The firewall is not installed............................................................................................................ 222
Computers have outstanding alerts.............................................................................................. 223
Computers are not managed by the console..................................................................................223
Can't protect computers in the Unassigned group.................................................................... 224
Sophos Endpoint Security and Control installation failed............................................................ 224
Computers are not updated............................................................................................................ 225
Anti-virus settings do not take effect on Macs.............................................................................. 225
Anti-virus settings do not take effect on Linux or UNIX............................................................... 225
Linux or UNIX computer does not comply with policy............................................................... 225
New scan appears unexpectedly on a Windows computer........................................................... 226
Connectivity and timeout problems.............................................................................................. 226
Adware and PUAs are not detected............................................................................................... 226
Partially detected item.................................................................................................................... 226
Frequent alerts about potentially unwanted applications.............................................................. 227
Cleanup failed.................................................................................................................................. 227
Recover from virus side-effects....................................................................................................... 228
Recover from application side-effects............................................................................................ 228
Data control does not detect files uploaded via embedded browsers .......................................... 228
Data control does not scan uploaded or attached files................................................................ 229
Uninstalled update manager is displayed in the console............................................................... 229
Support........................................................................................................................................ 230
Glossary........................................................................................................................................... 231
Legal notices.................................................................................................................................... 237
1 About Sophos Enterprise Console

Sophos Enterprise Console is a single, automated console that manages and updates Sophos security software on computers running Windows, Mac OS X, Linux and UNIX operating systems, and in virtual environments with VMware vShield.

Sophos Enterprise Console enables you to do the following:

- Protect your network against malware, risky file types and websites, and malicious network traffic, as well as adware and other potentially unwanted applications.
- Control which websites users can browse to, further protecting the network against malware, and preventing users from browsing to inappropriate websites.
- Control which applications can run on the network.
- Manage client firewall protection on endpoint computers.
- Assess computers for missing patches.
- Reduce accidental data loss, such as unintentional transfer of sensitive data, from endpoint computers.
- Prevent users from using unauthorized external storage devices and wireless connection technologies on endpoint computers.
- Prevent users from re-configuring, disabling, or uninstalling Sophos security software.

Note
Some of the features above are not included with all licenses. If you want to use them, you might need to change your license.

Related information
2 Accessibility

Our software is compliant with the Web Content Accessibility Guidelines (WCAG) 2.1 level AA. You can find more information on these guidelines in related information.

To provide access we use the Microsoft Active Accessibility (MSAA) protocol and use the standard Windows conventions for control interaction.

Our software is accessible using JAWS (Job Access With Speech) and NVDA (NonVisual Desktop Access). We recommend that you use JAWS 2019 or later and NVDA 2019.1 or later. If you don't have JAWS or NVDA you can download them. You can find links for downloading JAWS and NVDA in related information. If you need further help with JAWS and NVDA you can contact their technical support.

If you want to use assistive technology products with our software we recommend that you are familiar with how your chosen product works and the available keyboard commands.

You can find specific recommendations for Sophos Enterprise Console in Recommended accessibility settings.

To use the Report Manager we recommend that you use Microsoft Narrator.

JAWS and NVDA can’t navigate in the report displayed in Report Viewer. They read out text only if you move the mouse pointer over objects. You can navigate in the report in Microsoft Narrator using the keyboard.

Related concepts
Recommended accessibility settings (page 2)

Use the following settings to get the best experience with Sophos Enterprise Console.

Related information
Web Content Accessibility Guidelines
JAWS
NVDA

2.1 Recommended accessibility settings

Use the following settings to get the best experience with Sophos Enterprise Console.

You need to set your punctuation and symbol settings so that:

- Backslash symbols are read out.
- Asterisk symbols are read out (as "star").
- Question mark symbols aren’t read.

Alternatively, you can add symbols like backslash or asterisk ( * ) to Symbol Pronunciation.

Note
For dialogs that use question mark as a wildcard symbol we recommend changing the symbol pronunciation level to all while you are using the dialog. Such dialogs will tell you that you need to do this.
To make Sophos Enterprise Console easier to see you can use the Microsoft Magnifier. Find out more about Microsoft Magnifier.

Or you can change the scaling in Windows. To do this:
1. Go to Settings > Display.
2. Change the value of Scale and layout or enter a Custom scaling value.

**JAWS (Job Access With Speech)**

Set the punctuation and symbol settings to Most. You can do this for default profile only.

- In Utilities, click Settings Center > Punctuation > Punctuation level and click Most.

There is no hotkey assigned by default. We recommend assigning hotkey "JAWS + P".

Add symbols to Symbol Pronunciation. To do this:
1. In Utilities, click Settings Center > Punctuation > Punctuation and click Customize Punctuation.

You need to adjust some settings in JAWS to make sure it reads all headers and labels.

- To force JAWS to read the header, use CTRL+[JAWS BUTTON]+[Column Number].
- Turn on control descriptions, click Utilities > Settings Center > Configure Verbosity > Control Description.

If you are using the Advanced profile you need to turn on group label reading, click Utilities > Settings Center > Configure Verbosity > Control Group Name.

**NVDA (NonVisual Desktop Access)**

Set the punctuation and symbol settings to Most. To do this:

- Click [ NVDA BUTTON ] + P to change the punctuation level.
- In Preferences > Settings... > Speech, select Most in Punctuation.

Add symbols to Symbol Pronunciation. You can do this by:
1. In Preferences, click Punctuation/symbol pronunciation....
2. Find the list entry for the symbol and click Level and Send actual symbol to synthesizer.

**Related information**

Microsoft Magnifier
3 Guide to the Sophos Enterprise Console interface

3.1 User interface layout

The Sophos Enterprise Console user interface consists of the following areas:

Toolbar

The toolbar contains shortcuts to the most common commands for using and configuring your Sophos security software.

Dashboard

The Dashboard provides an at-a-glance view of your network's security status.

Computer list

The computer list is displayed at the bottom right. It has two views:

- **Endpoints** view displays the computers in the group that is selected in the Groups pane at the bottom left.
- **Update managers** view displays the computers where Sophos Update Manager is installed.

Related concepts

Toolbar buttons (page 4)
Navigating the Endpoints view (page 8)
Navigating the Update managers view (page 12)

Related reference

Dashboard panels (page 6)

3.2 Toolbar buttons

The following table describes the toolbar buttons. Some toolbar buttons are available only in specific circumstances. For example, the Protect button to install anti-virus and firewall software is only available if a group of computers is selected in the Groups pane in the Endpoints view.

<table>
<thead>
<tr>
<th>Toolbar Button</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Discover computers icon]</td>
<td>Discover computers</td>
<td>Searches for computers on the network and adds them to the console.</td>
</tr>
<tr>
<td>Toolbar Button</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>-------</td>
</tr>
<tr>
<td>Create group</td>
<td>Creates a new group for computers.</td>
<td></td>
</tr>
<tr>
<td>View/Edit policy</td>
<td>Opens the policy selected in the Policies pane for editing.</td>
<td></td>
</tr>
<tr>
<td>Protect</td>
<td>Installs anti-virus and firewall software on the computers selected in the computer list.</td>
<td></td>
</tr>
<tr>
<td>Endpoints</td>
<td>Switches to the Endpoints view in the computer list. The Endpoints view displays the computers in the group that is selected in the Groups pane.</td>
<td></td>
</tr>
<tr>
<td>Update managers</td>
<td>Switches to the Update managers view in the computer list. The Update managers view displays computers where Sophos Update Manager is installed.</td>
<td></td>
</tr>
<tr>
<td>Dashboard</td>
<td>Shows or hides the Dashboard. The Dashboard provides an at-a-glance view of your network's security status.</td>
<td></td>
</tr>
<tr>
<td>Reports</td>
<td>Starts Report Manager so that you can generate reports about alerts and events on your network.</td>
<td></td>
</tr>
<tr>
<td>Sophos Central</td>
<td>Takes you to Sophos Central. For information about Sophos Central, see knowledgebase article 119598. For information about migrating to Sophos Central, see knowledgebase article 122264.</td>
<td></td>
</tr>
<tr>
<td>Configure Sophos Mobile URL</td>
<td>When the Sophos Mobile URL is configured, this opens the Sophos Mobile web console. This is a device management solution for mobile devices (such as smartphones and tablets) that helps you to manage apps and security settings.</td>
<td></td>
</tr>
</tbody>
</table>

**Related concepts**
- Discovering computers on the network (page 34)
- Navigating the Endpoints view (page 8)
- Navigating the Update managers view (page 12)
- Generating reports (page 208)

**Related tasks**
- Create a group (page 25)
- Edit a policy (page 33)
- Protect computers automatically (page 50)
- Configure the Sophos Mobile URL (page 45)

**Related reference**
- Dashboard panels (page 6)
3.3 Dashboard panels

The **Dashboard** contains the following panels:

<table>
<thead>
<tr>
<th>Dashboard Panel</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computers</td>
<td>Displays the total number of computers on the network and the number of connected, managed, and unmanaged computers. To view a list of managed, unmanaged, connected, or all computers, click a link in the <strong>Computers</strong> area.</td>
</tr>
<tr>
<td>Updates</td>
<td>Displays the status of update managers.</td>
</tr>
<tr>
<td>Computers with alerts</td>
<td>Displays the number and percentage of managed computers with alerts about: • Known and unknown viruses and spyware • Suspicious behavior and files • Adware and other potentially unwanted applications To view a list of managed computers with outstanding alerts, click the panel title <strong>Computers with alerts</strong>.</td>
</tr>
<tr>
<td>Computers over event threshold</td>
<td>Displays the number of computers with events over the threshold within the last seven days. To view a list of computers with device control, data control, controlled application, or firewall events, click a link in the <strong>Computers over event threshold</strong> panel. Depending on your license, some of the event types may not be displayed.</td>
</tr>
<tr>
<td>Policies</td>
<td>Displays the number and percentage of managed computers with group policy violations or policy comparison errors. It also includes computers that haven't yet responded to the changed policy sent to them from the console. To view a list of managed computers that differ from policy, click the panel title <strong>Policies</strong>.</td>
</tr>
<tr>
<td>Protection</td>
<td>Displays the number and percentage of managed and connected computers on which Sophos Endpoint Security and Control or Sophos Anti-Virus is out of date or uses unknown detection data. To view a list of managed connected out-of-date computers, click the panel title <strong>Protection</strong>.</td>
</tr>
</tbody>
</table>
### 3.4 Security status icons

The following table describes the security status icons displayed in the Dashboard and the Sophos Enterprise Console status bar.

<table>
<thead>
<tr>
<th>Security status icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="checkmark" alt="Normal" /></td>
<td>Normal&lt;br&gt;The number of affected computers is below the warning level.</td>
</tr>
<tr>
<td><img src="warning" alt="Warning" /></td>
<td>Warning&lt;br&gt;The warning level has been exceeded.</td>
</tr>
<tr>
<td><img src="exclamation" alt="Critical" /></td>
<td>Critical&lt;br&gt;The critical level has been exceeded.</td>
</tr>
</tbody>
</table>

### Dashboard panel health icons

A Dashboard panel health icon is displayed in the upper-right corner of a Dashboard panel. It shows the status of the specific security area represented by the panel.

A Dashboard panel health icon shows the status of a panel icon with the most severe status, that is:

- A panel health icon changes from Normal to Warning when a warning level is exceeded for at least one icon in the panel.
- A panel health icon changes from Warning to Critical when a critical level is exceeded for at least one icon in the panel.

### The network health icon

The network health icon is displayed on the right side of the Sophos Enterprise Console status bar. It shows the overall security status of your network.

The network health icon shows the status of the Dashboard panel with the most severe status, that is:

- The network's overall health icon changes from Normal to Warning when a warning level is exceeded for at least one icon in the Dashboard.
- The network's overall health icon changes from Warning to Critical when a critical level is exceeded for at least one icon in the Dashboard.
Sophos Enterprise Console

When you first install or upgrade Sophos Enterprise Console, the Dashboard uses the default warning and critical levels. You can configure your own warning and critical levels.

You can also set up email alerts to be sent to your chosen recipients when a warning or critical level has been exceeded for a Dashboard panel.

**Related tasks**

Set up network status email alerts (page 194)
You can set up email alerts to be sent to your chosen recipients when a warning or critical level has been exceeded for a dashboard section.

**Related reference**

Dashboard panels (page 6)

### 3.5 Navigating the Endpoints view

**Computer list**

In the **Endpoints** view, the computer list displays the endpoint computers in the group that is selected in the **Groups** pane.

This view contains a number of tabs. The **Status** tab shows whether the computers are protected by on-access scanning, whether they are compliant with their group policies, which features are enabled, and whether the software is up to date. This tab also shows if there are any alerts. The other tabs give more detailed information on each of these subjects.

You can filter the computer list using the **View** filter. In the **View** drop-down list, select which computers you want to see. For example, select **Computers with potential problems** to display computers with problems.

You can also filter the computer list by the name of a detected item such as malware, potentially unwanted application, or suspicious file.

You can search for computers by computer name, computer description or IP address.

You can copy or print data displayed in the computer list.

**Groups pane**

In the **Groups** pane, you create groups and put networked computers in them. You can create groups yourself or you can import Active Directory containers, with or without computers, and use them as Enterprise Console computer groups.

The **Unassigned** group is for computers that are not yet in a group that you created.

**Policies pane**

In the **Policies** pane, you create and configure the policies applied to groups of computers.
Related concepts
Creating and using groups (page 24)
Creating and using policies (page 27)
Related tasks
Filter computers by the name of a detected item (page 10)
Find a computer in Sophos Enterprise Console (page 11)
Copy data from the computer list (page 220)
Print data from the computer list (page 220)
Related reference
Computer list icons (page 9)

3.6 Computer list icons

Alerts

<table>
<thead>
<tr>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>A red warning sign displayed in the <strong>Alerts and errors</strong> column on the <strong>Status</strong> tab means that a virus, worm, Trojan, spyware, or suspicious behavior has been detected.</td>
</tr>
</tbody>
</table>
| !     | A yellow warning sign displayed in the **Alerts and errors** column on the **Status** tab indicates one of the following problems:  
  - A suspicious file has been detected.  
  - An adware or other potentially unwanted application has been detected.  
  - An error has occurred.  
A yellow warning sign displayed in the **Policy compliance** column indicates that the computer is not using the same policy or policies as other computers in its group. |

If there are multiple alerts or errors on a computer, the icon of an alert that has the highest priority will be displayed in the **Alerts and errors** column. Alert types are listed below in descending order of priority.

1. Virus and spyware alerts  
2. Suspicious behavior alerts  
3. Suspicious file alerts  
4. Adware and PUA alerts  
5. Software application errors (for example, installation errors)

If several alerts with the same priority are received from the same computer, the most recent alert will be displayed in the computer list.

Protection disabled or out of date

A gray feature icon in the feature status column on the **Status** tab means that the feature is disabled. For example, a gray shield...
5
in the **On-access** column means that on-access scanning is inactive.

A clock icon

1
in the **Up to date** column means that the security software is out of date.

## Computer status

<table>
<thead>
<tr>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="green" /></td>
<td>A computer sign with a green connector means that the computer is managed by Sophos Enterprise Console.</td>
</tr>
<tr>
<td><img src="image" alt="yellow hourglass" /></td>
<td>A computer sign with a yellow hourglass means that installation of security software is pending.</td>
</tr>
<tr>
<td><img src="image" alt="yellow down arrow" /></td>
<td>A computer sign with a yellow down arrow means that installation of security software is in progress.</td>
</tr>
<tr>
<td><img src="image" alt="gray" /></td>
<td>A gray computer sign means that the computer is not managed by Sophos Enterprise Console.</td>
</tr>
<tr>
<td><img src="image" alt="red cross" /></td>
<td>A computer sign with a red cross means that the computer that is usually managed by Sophos Enterprise Console is disconnected from the network. (Unmanaged disconnected computers are not shown.)</td>
</tr>
</tbody>
</table>

### 3.7 Filter computers by the name of a detected item

You can filter the computer list by the name of a detected item such as malware, potentially unwanted application, or suspicious file. You can do so by configuring the filter "Managed computers affected by...". The filter is displayed in the **View** drop-down list along with the other computer list filters.

To configure the filter:

1. On the **Tools** menu, click **Configure Filters**.
2. In the **Configure Computer List Filter** dialog box, enter the name of a detected item you want to filter by. You can find the names of items detected on your network in:
   - Computer list view, **Alert and Error Details** tab, **Item detected** column.
     Please note that if a computer has multiple detected items, the **Item detected** column will display only the latest highest priority item, which may not be the one you filter by.
   - **Resolve alerts and errors** dialog box. To open the dialog box, select a computer or computers in the computer list or a group of computers in the **Groups** pane, right-click and click **Resolve Alerts and Errors**.
   - **Computer details** dialog box. To open the dialog box, double-click the affected computer. Then scroll down to the **Outstanding alerts and errors** section.
   - **Reports** (for example, **Alert summary** or **Alerts and events by item name**). To open the Report Manager, on the **Tools** menu, click **Manage Reports**.
You can use wildcards. Use ? for any single character and * for any string of characters. For example, if you enter "Mal*" and then apply the filter, the computer list view will show computers infected with malware whose name begins with "Mal", such as "Mal/Conficker-A" and "Mal/ Packer".

### 3.8 Find a computer in Sophos Enterprise Console

You can search for a computer or computers in Sophos Enterprise Console by:

- Computer name
- Computer description
- IP address

1. To find a computer, do either of the following:
   - Press CTRL+F.
   - On the **Edit** menu, click **Find a Computer**.
   - Click anywhere in the computer list, right-click, and then click **Find a Computer**.

2. In the **Find** dialog box, enter your search criteria.

   The **Find what** field is not case sensitive. Trailing wildcards are implicit.

You can use the wildcards * and ?

For example:

<table>
<thead>
<tr>
<th>Search criteria</th>
<th>Search results</th>
</tr>
</thead>
<tbody>
<tr>
<td>UKlapt</td>
<td>Finds any string beginning with “uklapt”, for example, UKlaptop-011, UKlaptop-155, uklaptop132.</td>
</tr>
<tr>
<td>Ukla*</td>
<td>Finds any string beginning with “ukla”. The wildcard is not needed as it is there implicitly; search returns the same results as in the previous example, UKlaptop-011, UKlaptop-155, uklaptop132.</td>
</tr>
<tr>
<td>*ukla</td>
<td>Finds any string containing “ukla”, for example, UKlaptop-011, 055uklax, 056-Dukla-sales.</td>
</tr>
<tr>
<td>Ukl*t</td>
<td>Finds any string beginning with “ukl”, containing a “t”, and ending with any character, for example, UKlaptop-011, ukLite55.</td>
</tr>
<tr>
<td>?klap</td>
<td>Finds any string beginning with any single character followed by “klap” and ending with any character, for example, UKlaptop-011, uklapland33.</td>
</tr>
<tr>
<td>UKl??t</td>
<td>Finds any string beginning with “ukl”, followed by two characters, followed by “t”, and ending with any character, for example, UKlaptop-011, uklist101.</td>
</tr>
</tbody>
</table>
3.9 Navigating the Update managers view

Computer list

In the **Update managers** view, you set up automatic updating of Sophos security software from the Sophos website and view the status and details of your update managers.

The computer list displays the computers where Sophos Update Manager is installed.

Software subscriptions

You use the **Software Subscriptions** pane to create or edit software subscriptions that specify which versions of endpoint software are downloaded from Sophos for each platform.
4 Getting started with Sophos Enterprise Console

This is an overview of the tasks you need to perform to protect your network after you have installed Sophos Enterprise Console and completed the Download Security Software Wizard. For more information about using Sophos Enterprise Console, refer to the other materials and sections mentioned.

We recommend that you refer to the Sophos Enterprise Console policy setup guide for advice on best practices for using and managing Sophos security software.

If you haven't completed the Download Security Software Wizard do this first.

To protect your network, follow these steps:

1. Create groups.
   - You can create groups yourself, one by one, or you can import Active Directory containers, with or without computers, and use them as Sophos Enterprise Console computer groups.
   - If you want to import Active Directory containers, we recommend that you first import containers from Active Directory without computers. You can then assign group policies to the groups, and then add computers to the groups, for example, by synchronizing the groups with Active Directory.

2. Set up policies.
   - Sophos Enterprise Console has a set of default policies that are essential to keep your network protected. You can use default Updating and Anti-virus and HIPS policies out of the box.
     a) To configure the firewall policy, run the Firewall policy wizard.

3. Discover computers on the network and add them to the console.
   - If you have imported containers and computers from Active Directory in step 1, you do not need to do anything.

4. Protect computers.
   - You can choose between two approaches to protecting your networked computers, depending on which suits you best.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using the Protect Computers Wizard</td>
<td>When you drag a computer from the Unassigned group and drop it onto another group, a wizard is launched to help you protect the computers.</td>
</tr>
<tr>
<td>Protecting computers automatically during</td>
<td>If you chose to synchronize with Active Directory, you can also choose to protect your Windows computers automatically. You can do so in the Synchronize with Active Directory Wizard or Synchronization properties dialog box.</td>
</tr>
<tr>
<td>synchronization with Active Directory</td>
<td></td>
</tr>
</tbody>
</table>

5. Check that computers are protected.
a) When installation is complete, look at the list of computers in the new group again. In the On-access column, you should see the word Active: this shows that the computer is protected by on-access scanning, and that it is now managed by Sophos Enterprise Console.

6. Clean up computers.
   a) If a virus, unwanted application, or other issue has been detected on your network, clean up affected computers.

Additional protection options
By default, Sophos Endpoint Security and Control detects malware (viruses, Trojans, worms, spyware), adware and other potentially unwanted applications, suspicious behavior, and malicious network traffic. It also blocks access to websites that are known to host malware and scans content downloaded from the internet. You can enable further security and productivity features.

Administrative options
You can set up different roles in Sophos Enterprise Console, add rights to the roles, and then assign Windows users and groups to the roles. The System Administrator role that includes the Sophos Full Administrators Windows group has full rights and does not require setting up.

You can split your IT estate into sub-estates and assign Sophos Enterprise Console groups of computers to the sub-estates. You can then control access to the sub-estates by assigning Windows users and groups to them. The Default sub-estate contains all Sophos Enterprise Console groups, including the Unassigned group.

Tip
Check out videos that show how to set up and use Sophos Enterprise Console on the SophosGlobalSupport YouTube channel, the Sophos Enduser Protection section.

Related concepts
Creating and using groups (page 24)
Discovering computers on the network (page 34)
Checking whether your network is protected (page 52)
Managing roles and sub-estates (page 15)

Related tasks
Run the Download Security Software Wizard (page 73)
Import containers and computers from Active Directory (page 35)
Set up a basic firewall policy (page 117)
Protect computers automatically (page 50)
Use synchronization to protect computers automatically (page 43)
Clean up computers now (page 59)

Related information
Sophos documentation
5 Setting up Sophos Enterprise Console

5.1 Managing roles and sub-estates

**Note**
If you already use role-based administration, you must have the **Role-based administration** right to set up roles and sub-estates. The System Administrator role that includes the Sophos Full Administrators Windows group has full rights and does not require setting up.

You can set up role-based access to the console by setting up roles, adding rights to the roles, and then assigning Windows users and groups to the roles. For example, a Help Desk engineer can update or clean up computers, but can't configure policies, which is the responsibility of an Administrator.

To open Sophos Enterprise Console, a user must be a member of the Sophos Console Administrators group and be assigned to at least one Sophos Enterprise Console role and one sub-estate. Members of the Sophos Full Administrators group have full access to Sophos Enterprise Console.

You can create your own roles or use preconfigured roles.

You can assign a user as many roles as you like, by adding to the roles either the individual user or a Windows group the user belongs to.

If a user does not have rights to perform a certain task within the console, they can still view configuration settings pertaining to that task. A user who is not assigned any role cannot open Sophos Enterprise Console.

You can also restrict the computers and groups that users can perform operations on. You can split your IT estate into sub-estates and assign Sophos Enterprise Console groups of computers to the sub-estates. You can then control access to the sub-estates by assigning Windows users and groups to them. The **Default** sub-estate contains all Sophos Enterprise Console groups, including the **Unassigned** group.

A user can only see the sub-estate that they are assigned to. If a user has been assigned to more than one sub-estate, they can choose which sub-estate to view, one sub-estate at a time. The sub-estate that is open in Sophos Enterprise Console is the active sub-estate. A user cannot edit a policy that is applied outside their active sub-estate.
5.1.1 What are the preconfigured roles?

There are four preconfigured roles in Sophos Enterprise Console:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
</table>
| System
Administrator | A preconfigured role that has full rights to manage Sophos security software on the network and roles in Sophos Enterprise Console. The System Administrator role cannot be edited or deleted. |
| Administrator  | A preconfigured role that has rights to manage Sophos security software on the network, but cannot manage roles in Sophos Enterprise Console. The Administrator role can be renamed, edited, or deleted. |
| Helpdesk      | A preconfigured role that has remediation rights only, for example, to clean up or update computers. The Helpdesk role can be renamed, edited, or deleted. |
| Guest         | A preconfigured role that has read-only access to Sophos Enterprise Console. The Guest role can be renamed, edited, or deleted. |

You can edit the Administrator, Helpdesk and Guest roles, or create your own roles.

**Related tasks**  
Create a role (page 17)
5.1.2 Create a role

If you already use role-based administration, you must have the Role-based administration right to perform this task.

1. On the Tools menu, click Manage Roles and Sub-Estates.
2. In the Manage roles and sub-estates dialog box, on the Manage roles tab, click Create.
   The Create role dialog box appears.
3. In the Role name field, enter a name for the role.
4. In the Rights pane, select the right or rights you want to assign to the role and click Add.
5. In the Users and groups pane, click Add.
6. In the Select User or Group dialog box, enter the name of a Windows user or group you want to assign to the role. Click OK.
   If necessary, assign more users or groups to the role, as described in steps 5 and 6.

Related concepts
Managing roles and sub-estates (page 15)

5.1.3 Delete a role

If you already use role-based administration, you must have the Role-based administration right to perform this task.

1. On the Tools menu, click Manage Roles and Sub-Estates.
2. In the Manage roles and sub-estates dialog box, on the Manage roles tab, select the role you want to delete and click Delete.

Note
The preconfigured System Administrator role can't be deleted.

Related concepts
Managing roles and sub-estates (page 15)

5.1.4 Edit a role

If you already use role-based administration, you must have the Role-based administration right to perform this task.

1. On the Tools menu, click Manage Roles and Sub-Estates.
2. In the Manage roles and sub-estates dialog box, on the Manage roles tab, select the role you want to edit and click Edit.
   The Edit role dialog box appears.
3. In the Rights pane, assign rights to the role or remove existing rights as appropriate.
4. In the Users and groups pane, add Windows users or groups to the role or remove existing users or groups as appropriate.
5.1.5 Grant rights to a role

If you already use role-based administration, you must have the Role-based administration right to perform this task.

1. On the Tools menu, click Manage Roles and Sub-Estates.
2. In the Manage roles and sub-estates dialog box, on the Manage roles tab, select the role you want to add a right to and click Edit.
   The Edit role dialog box appears.
3. In the Rights pane, in the Available rights list, select a right and click Add.

5.1.6 Create a sub-estate

If you already use role-based administration, you must have the Role-based administration right to perform this task.

1. On the Tools menu, click Manage Roles and Sub-Estates.
2. In the Manage roles and sub-estates dialog box, on the Manage sub-estates tab, click Create.
   The Create sub-estate dialog box appears.
3. In the Sub-estate name field, enter a name for the sub-estate.
4. In the Enterprise Console groups pane, select the groups you want to add to the sub-estate.
5. In the Users and groups pane, click Add to add Windows users or groups to the sub-estate.

5.1.7 Change active sub-estate

If you have been assigned to more than one sub-estate, you can choose which sub-estate you want to view when opening Sophos Enterprise Console, or you can switch among the sub-estates in Sophos Enterprise Console.

You can only view one sub-estate at a time. When you change your active sub-estate, Sophos Enterprise Console is reloaded with a new sub-estate.

To change active sub-estate:

1. On the Tools menu, click Select Active Sub-Estate.
2. In the Select Active Sub-Estate dialog box, select the sub-estate you want to open and click OK.

5.1.8 Edit a sub-estate

If you already use role-based administration, you must have the Role-based administration right to perform this task.
1. On the Tools menu, click Manage Roles and Sub-Estates.
2. In the Manage roles and sub-estates dialog box, on the Manage sub-estates tab, select the sub-estate you want to edit and click Edit.
3. In the Edit sub-estate dialog box, change the name of the sub-estate, change which Sophos Enterprise Console groups are included in the sub-estate, or change which Windows users and groups have access to the sub-estate, as appropriate. Click OK.

Related concepts
Managing roles and sub-estates (page 15)

5.1.9 Copy a sub-estate

If you already use role-based administration, you must have the Role-based administration right to perform this task.
1. On the Tools menu, click Manage Roles and Sub-Estates.
2. In the Manage roles and sub-estates dialog box, on the Manage sub-estates tab, select the sub-estate you want to copy and click Copy.
A copy of the sub-estate appears in the list of sub-estates.
3. Select the newly created sub-estate and click Edit.
4. Rename the sub-estate.
5. Change the groups that are included in the sub-estate or Windows users and groups that have access to it, if you want to.

Related concepts
Managing roles and sub-estates (page 15)

5.1.10 Delete a sub-estate

If you already use role-based administration, you must have the Role-based administration right to perform this task.
1. On the Tools menu, click Manage Roles and Sub-Estates.
2. In the Manage roles and sub-estates dialog box, on the Manage sub-estates tab, select the sub-estate you want to delete and click Delete.
You can't delete the Default sub-estate.

Related concepts
Managing roles and sub-estates (page 15)

5.1.11 View user or group roles and sub-estates

To view the roles and sub-estates a Windows user or group has been assigned to:
1. On the Tools menu, click Manage roles and sub-estates.
2. In the Manage roles and sub-estates dialog box, go to the User and Group View tab and click the Select user or group button.
3. In the Select User or Group dialog box, select a user or group whose roles and sub-estates you want to view and click OK.
5.1.12 What tasks do the rights authorize?

Note
Depending on your license, some of the rights may not be applicable.

<table>
<thead>
<tr>
<th>Right</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditing</td>
<td>Enable auditing, disable auditing</td>
</tr>
<tr>
<td>Computer search, protection and groups</td>
<td>Start search, stop search and find domains for Network search, IP range search and Active Directory search</td>
</tr>
<tr>
<td></td>
<td>Import computers and groups from Active Directory; import groups from Active Directory</td>
</tr>
<tr>
<td></td>
<td>Import computers from a file</td>
</tr>
<tr>
<td></td>
<td>Delete a computer</td>
</tr>
<tr>
<td></td>
<td>Protect a computer</td>
</tr>
<tr>
<td></td>
<td>Synchronize a group with Active Directory</td>
</tr>
<tr>
<td></td>
<td>Change group synchronization properties</td>
</tr>
<tr>
<td></td>
<td>Remove group synchronization</td>
</tr>
<tr>
<td></td>
<td>Move a computer</td>
</tr>
<tr>
<td></td>
<td>Create a group</td>
</tr>
<tr>
<td></td>
<td>Rename a group</td>
</tr>
<tr>
<td></td>
<td>Move a group</td>
</tr>
<tr>
<td></td>
<td>Delete a group</td>
</tr>
<tr>
<td></td>
<td>Assign a policy to a group</td>
</tr>
<tr>
<td>Data control customization</td>
<td>Create a data control rule</td>
</tr>
<tr>
<td></td>
<td>Edit a data control rule</td>
</tr>
<tr>
<td></td>
<td>Copy a data control rule</td>
</tr>
<tr>
<td></td>
<td>Delete a data control rule</td>
</tr>
<tr>
<td></td>
<td>Exclude files from data control scanning</td>
</tr>
<tr>
<td></td>
<td>Create a Content Control List</td>
</tr>
<tr>
<td></td>
<td>Edit a Content Control List</td>
</tr>
<tr>
<td></td>
<td>Copy a Content Control List</td>
</tr>
<tr>
<td></td>
<td>Delete a Content Control List</td>
</tr>
<tr>
<td>Data control events</td>
<td>Display the data control event viewer</td>
</tr>
<tr>
<td></td>
<td>Display data control events in computer details</td>
</tr>
<tr>
<td>Right</td>
<td>Tasks</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>Policy setting - anti-virus and HIPS</td>
<td>Create an anti-virus and HIPS policy  &lt;br&gt; Duplicate an anti-virus and HIPS policy  &lt;br&gt; Rename an anti-virus and HIPS policy  &lt;br&gt; Edit an anti-virus and HIPS policy  &lt;br&gt; Restore default anti-virus and HIPS settings  &lt;br&gt; Delete an anti-virus and HIPS policy  &lt;br&gt; Add or remove entry from threat master list</td>
</tr>
<tr>
<td>Policy setting - application control</td>
<td>Create an application control policy  &lt;br&gt; Duplicate an application control policy  &lt;br&gt; Rename an application control policy  &lt;br&gt; Edit an application control policy  &lt;br&gt; Restore default application control settings  &lt;br&gt; Delete an application control policy</td>
</tr>
<tr>
<td>Policy setting - data control</td>
<td>Create a data control policy  &lt;br&gt; Duplicate a data control policy  &lt;br&gt; Rename a data control policy  &lt;br&gt; Edit a data control policy  &lt;br&gt; Restore default data control settings  &lt;br&gt; Delete a data control policy</td>
</tr>
<tr>
<td>Policy setting - device control</td>
<td>Create a device control policy  &lt;br&gt; Duplicate a device control policy  &lt;br&gt; Rename a device control policy  &lt;br&gt; Edit a device control policy  &lt;br&gt; Restore default device control settings  &lt;br&gt; Delete a device control policy</td>
</tr>
<tr>
<td>Policy setting - firewall</td>
<td>Create a firewall policy  &lt;br&gt; Duplicate a firewall policy  &lt;br&gt; Rename a firewall policy  &lt;br&gt; Edit a firewall policy  &lt;br&gt; Restore default firewall settings  &lt;br&gt; Delete a firewall policy</td>
</tr>
<tr>
<td>Right</td>
<td>Tasks</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policy setting - patch</td>
<td>Create a patch policy</td>
</tr>
<tr>
<td></td>
<td>Duplicate a patch policy</td>
</tr>
<tr>
<td></td>
<td>Rename a patch policy</td>
</tr>
<tr>
<td></td>
<td>Edit a patch policy</td>
</tr>
<tr>
<td></td>
<td>Restore default patch settings</td>
</tr>
<tr>
<td></td>
<td>Delete a patch policy</td>
</tr>
<tr>
<td></td>
<td>Create a tamper protection policy</td>
</tr>
<tr>
<td></td>
<td>Duplicate a tamper protection policy</td>
</tr>
<tr>
<td></td>
<td>Rename a tamper protection policy</td>
</tr>
<tr>
<td></td>
<td>Edit a tamper protection policy</td>
</tr>
<tr>
<td></td>
<td>Restore default tamper protection settings</td>
</tr>
<tr>
<td></td>
<td>Delete a tamper protection policy</td>
</tr>
<tr>
<td>Policy setting - updating</td>
<td>Create an updating policy</td>
</tr>
<tr>
<td></td>
<td>Duplicate an updating policy</td>
</tr>
<tr>
<td></td>
<td>Rename an updating policy</td>
</tr>
<tr>
<td></td>
<td>Edit an updating policy</td>
</tr>
<tr>
<td></td>
<td>Restore default updating settings</td>
</tr>
<tr>
<td></td>
<td>Delete an updating policy</td>
</tr>
<tr>
<td></td>
<td>Create a subscription</td>
</tr>
<tr>
<td></td>
<td>Edit a subscription</td>
</tr>
<tr>
<td></td>
<td>Rename a subscription</td>
</tr>
<tr>
<td></td>
<td>Duplicate a subscription</td>
</tr>
<tr>
<td></td>
<td>Delete a subscription</td>
</tr>
<tr>
<td></td>
<td>Configure update managers</td>
</tr>
<tr>
<td></td>
<td>Create a web control policy</td>
</tr>
<tr>
<td></td>
<td>Duplicate a web control policy</td>
</tr>
<tr>
<td></td>
<td>Rename a web control policy</td>
</tr>
<tr>
<td></td>
<td>Edit a web control policy</td>
</tr>
<tr>
<td></td>
<td>Reset a default web control policy</td>
</tr>
<tr>
<td></td>
<td>Delete a web control policy</td>
</tr>
<tr>
<td>Right</td>
<td>Tasks</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Policy setting - exploit prevention</td>
<td>Create an exploit prevention policy</td>
</tr>
<tr>
<td></td>
<td>Duplicate an exploit prevention policy</td>
</tr>
<tr>
<td></td>
<td>Rename an exploit prevention policy</td>
</tr>
<tr>
<td></td>
<td>Edit an exploit prevention policy</td>
</tr>
<tr>
<td></td>
<td>Add an exploit mitigation exclusion</td>
</tr>
<tr>
<td></td>
<td>Delete an exploit mitigation exclusion</td>
</tr>
<tr>
<td></td>
<td>Reset an exploit prevention policy</td>
</tr>
<tr>
<td></td>
<td>Delete an exploit prevention policy</td>
</tr>
<tr>
<td>Remediation - cleanup</td>
<td>Clean up detected items</td>
</tr>
<tr>
<td></td>
<td>Acknowledge alerts</td>
</tr>
<tr>
<td></td>
<td>Acknowledge errors</td>
</tr>
<tr>
<td>Remediation - updating and scanning</td>
<td>Update computers now</td>
</tr>
<tr>
<td></td>
<td>Run a full system scan of a computer</td>
</tr>
<tr>
<td></td>
<td>Make computers comply with the group policy</td>
</tr>
<tr>
<td></td>
<td>Make update manager comply with configuration</td>
</tr>
<tr>
<td></td>
<td>Instruct update manager to update now</td>
</tr>
<tr>
<td>Report configuration</td>
<td>Create, edit, or delete a report</td>
</tr>
<tr>
<td>Role-based administration</td>
<td>Create a role</td>
</tr>
<tr>
<td></td>
<td>Rename a role</td>
</tr>
<tr>
<td></td>
<td>Delete a role</td>
</tr>
<tr>
<td></td>
<td>Modify the rights of a role</td>
</tr>
<tr>
<td></td>
<td>Add a user or group to a role</td>
</tr>
<tr>
<td></td>
<td>Remove a user or group from a role</td>
</tr>
<tr>
<td></td>
<td>Sub-estate management: create a sub-estate; rename a sub-estate;</td>
</tr>
<tr>
<td></td>
<td>delete a sub-estate; add a sub-estate root group; remove a sub-</td>
</tr>
<tr>
<td></td>
<td>estate root group; add a user or group to a sub-estate; remove a</td>
</tr>
<tr>
<td></td>
<td>user or group from a sub-estate</td>
</tr>
<tr>
<td>System configuration</td>
<td>Modify SMTP server settings; test SMTP server settings; modify</td>
</tr>
<tr>
<td></td>
<td>email alert recipients</td>
</tr>
<tr>
<td></td>
<td>Configure dashboard warning and critical levels</td>
</tr>
<tr>
<td></td>
<td>Configure reporting: configure database alert purging; set the</td>
</tr>
<tr>
<td></td>
<td>company name displayed in reports</td>
</tr>
<tr>
<td></td>
<td>Configure reporting to Sophos: enable or disable reporting to</td>
</tr>
<tr>
<td></td>
<td>Sophos; modify the username; modify the contact email address</td>
</tr>
<tr>
<td></td>
<td>Configure the use of fixed version software packages</td>
</tr>
</tbody>
</table>
5.1.13 How can another user use Sophos Enterprise Console?

Members of the Sophos Full Administrators group have full access to Sophos Enterprise Console.

You can allow other users to use Sophos Enterprise Console. To open Sophos Enterprise Console, a user must be:

- A member of the Sophos Console Administrators group.
- Assigned to at least one Sophos Enterprise Console role.
- Assigned to at least one Sophos Enterprise Console sub-estate.

If you want to assign a user to the Sophos Console Administrators group, use Windows tools to add that user to the group.

To assign a user to an Sophos Enterprise Console role or sub-estate, on the **Tools** menu, click **Manage Roles and Sub-Estates**.

To use a remote or additional Sophos Enterprise Console, a user must be:

- A member of the Sophos Console Administrators group on the server where the Sophos Enterprise Console management server is installed.
- A member of the Distributed COM Users group on the server where the Sophos Enterprise Console management server is installed. (The Distributed COM Users group is located in the Builtin container of the Active Directory Users and Computers tool.)
- Assigned to at least one Sophos Enterprise Console role.
- Assigned to at least one Sophos Enterprise Console sub-estate.

**Related concepts**

Managing roles and sub-estates (page 15)

5.2 Creating and using groups

You must create groups and place computers in them before you can protect and manage those computers.

5.2.1 What are groups for?

Groups are useful because you can:

- Have computers in different groups updated from different sources or on different schedules.
- Use different anti-virus and HIPS, application control, firewall, and other policies for different groups.
- Manage computers more easily.
Tip
You can create groups within groups and apply a specific set of policies to each group and subgroup.

5.2.2 What is a group?

A group

is a folder that holds a number of computers.

You can create groups yourself or you can import Active Directory containers, with or without computers, and use them as computer groups in Sophos Enterprise Console. You can also set up synchronization with Active Directory so that new computers and containers as well as other changes in Active Directory are copied into Sophos Enterprise Console automatically.

Each group has settings for updating, anti-virus and HIPS protection, firewall protection, and so on. All the computers in a group should usually use these settings, which are called a “policy.”

A group can contain subgroups.

5.2.3 What is the Unassigned group?

The Unassigned group is a group where Sophos Enterprise Console holds computers before you put them into groups.

You can't:

• Apply policies to the Unassigned group.
• Create subgroups in the Unassigned group.
• Move or delete the Unassigned group.

5.2.4 Create a group

If you use role-based administration, you must have the Computer search, protection and groups right to perform this task.

To create a new group for computers:

1. In the Endpoints view, in the Groups pane (on the left-hand side of the console), select where you want to create the group.
   • Click the computer name at the top if you want to create a new top-level group.
   • Click an existing group if you want to create a subgroup.
2. On the toolbar, click the Create group icon.
   A “New Group” is added to the list, with its name highlighted.
3. Type a name for the group.

Updating, anti-virus and HIPS, application control, firewall, patch, data control, device control, tamper protection, and web control policies are applied to the new group automatically. You can edit these policies, or apply different policies.
Note
If the new group is a subgroup, it initially uses the same settings as the group it is within.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Assign a policy to a group (page 32)
Edit a policy (page 33)

5.2.5 Add computers to a group

If you use role-based administration, you must have the Computer search, protection and groups right to perform this task.

1. Select the computers that you want to add to a group. For example, click the Unassigned group and select computers there.
2. Drag and drop the computers onto the new group.
   - If you move unprotected computers from the Unassigned group to a group that has automatic updating set up, a wizard is launched to help you protect them.
   - If you move computers from one group to another, they will use the same policies as the computers already in the group they are moved to.

Related concepts
Managing roles and sub-estates (page 15)

5.2.6 Delete computers from a group

If you use role-based administration, you must have the Computer search, protection and groups right to perform this task.

You can delete computers from a group, for example, if you want to remove entries for computers that are no longer on the network.

Note
If you delete computers that are still on the network, they will no longer be listed or managed by the console.

If you’ve upgraded from an earlier version of Sophos Enterprise Console and have computers that are encrypted with legacy Sophos Enterprise Console–managed full disk encryption, do not delete these computers from the console. Encryption recovery may not be possible in this case.

To delete computers:
1. Select the computers that you want to delete.
2. Right-click and select Delete.

If you want to see the computers again, click the Discover computers icon on the toolbar. These computers will not be shown as managed until they are restarted.
5.2.7 Cut and paste a group

If you use role-based administration, you must have the Computer search, protection and groups right to perform this task.

1. Select the group you want to cut and paste. On the Edit menu, click Cut.
2. Select the group where you want to place the group. On the Edit menu, click Paste.

5.2.8 Delete a group

If you use role-based administration, you must have the Computer search, protection and groups right to perform this task.

Any computers that were in the deleted group will be placed in the Unassigned group.

1. Select the group you want to delete.
2. Right-click and select Delete. When prompted, confirm that you want to delete the group and, if the group has any subgroups, its subgroups.

5.2.9 Rename a group

If you use role-based administration, you must have the Computer search, protection and groups right to perform this task.

1. Select the group you want to rename.
2. Right-click and select Rename.

5.2.10 Check which policies a group uses

To see which policies have been assigned to a group:

In the Groups pane, right-click the group. Select View/Edit Group Policy Details.

In the group details dialog box, you can see the policies currently used.

5.3 Creating and using policies

A policy is a collection of settings applied to all the computers in a group.

When you install Sophos Enterprise Console, default policies that offer a basic level of security are created for you. These policies are applied to any groups you create. You can edit the default policies or create new policies.
Note
Some features will be unavailable if your license does not include them.

You can create more than one policy of each type.
You can apply the same policy to more than one group.

5.3.1 What policies are available?

Note
Some features will be unavailable if your license does not include them.

• The **Updating** policy specifies how computers are updated with new security software.
• The **Anti-virus and HIPS** policy specifies how the security software scans computers for viruses, Trojans, worms, spyware, adware, potentially unwanted applications, suspicious behavior and suspicious files, and how it cleans them up.
• The **Application control** policy specifies which applications are blocked and which are allowed on your computers.
• The **Firewall** policy specifies how the firewall protects computers.
• The **Data control** policy specifies rules for monitoring or restricting the transfer of files, based on file content, filename, or file type.
• The **Device control** policy specifies which storage and networking devices are not authorized for use on workstations.
• The **Patch** policy specifies whether patch assessment is enabled and how often computers are assessed for missing patches.
• The **Tamper protection** policy specifies the password that allows authorized endpoint users to reconfigure, disable or uninstall Sophos security software.
• The **Web control** policy specifies which websites can be browsed to by users. A notification is displayed to users for sites that are configured as "block" or "warn."
• The **Exploit prevention** policy specifies which applications, functions and processes are protected against exploitation, such as protecting document files from ransomware (CryptoGuard) or protecting critical functions in web browsers (Safe Browsing).

5.3.2 What are the default policies?

When you install Sophos Enterprise Console, default policies are created for you.

Note
Some features will be unavailable if your license does not include them.

**Updating policy**

The default updating policy in a fresh installation of Sophos Enterprise Console provides:
• Automatic updating of computers every 10 minutes from the default location. The default location is a UNC share `\ComputerName\SophosUpdate`, where ComputerName is the name of the computer where the update manager is installed.

Anti-virus and HIPS policy

The default anti-virus and HIPS policy in a fresh installation of Sophos Enterprise Console provides:
• On-access scanning for viruses, Trojans, worms, spyware, and adware and other potentially unwanted applications (but not suspicious files).
• Detection of buffer overflows, malicious and suspicious behavior of programs running on the system, and malicious network traffic.
• Blocking of access to websites that are known to host malware.
• Scanning of content downloaded from the internet.
• Security alerts displayed on the desktop of the affected computer and added to the event log.

For a full list of the default settings for the Anti-virus and HIPS policy in a fresh installation of Sophos Enterprise Console, see knowledge base article 27267.

Application control policy

By default, all applications and application types are allowed. On-access scanning for applications you may want to control on your network is disabled.

Firewall policy

By default, the Sophos Client Firewall is enabled and blocks all non-essential traffic. Before you use it throughout your network, you should configure it to allow the applications you want to use.

For a full list of the default firewall settings, see knowledge base article 57757.

Data control policy

By default, data control is turned off and no rules are specified to monitor or restrict the transfer of files to the internet or storage devices.

Device control policy

By default, device control is turned off and all devices are allowed.

Patch policy

By default, patch assessment is turned off. For new patch policies, assessment is turned on. Once patch assessment is turned on, computers are assessed daily for missing patches (if you haven't changed the patch assessment interval).
Tamper protection policy

By default, tamper protection is turned off and no password is specified to allow authorized endpoint users to re-configure, disable or uninstall Sophos security software.

Web control policy

By default, web control is turned off, and users can visit any site that is not restricted as part of the Sophos Enterprise Console web protection.

Exploit prevention policy

By default, exploit prevention is turned on.

**Related concepts**
- Web protection (page 106)
- Exploit prevention policy (page 184)

**Related tasks**
- Set up a basic firewall policy (page 117)

**Related information**
- knowledge base article 27267
- knowledge base article 57757

5.3.3 Do I need to create my own policies?

When you install Sophos Enterprise Console, “default” policies are created for you. These policies are applied to any groups you create.

The default policies offer a basic level of security, but to use features like network access control or application control you need to create new policies or change the default policies.

**Note**

When you change the default policy, the change applies to all new policies you create.

**Note**

If you use role-based administration, you must have a respective **Policy setting** right to create or edit a policy. For example, you must have the **Policy setting - anti-virus and HIPS** right to create or edit an anti-virus and HIPS policy.

Updating policy

The default updating policy sets endpoints to check for updates to the recommended subscription every 10 minutes from the default software distribution UNC share. To change subscriptions, update locations and other settings, you can configure update policies.
Anti-virus and HIPS

The default anti-virus and HIPS policy protects computers against viruses and other malware. However, to enable detection of other unwanted or suspicious applications or behavior, you may want to create new policies, or change the default policy.

Application control

To define and block unauthorized applications, you can configure application control policies.

Firewall policy

To allow bona-fide applications access to a network, you can configure firewall policies.

Data control

By default, data control is turned off. To restrict data leakage, you can configure data control policies.

Device control

By default, device control is turned off. To restrict allowed hardware devices, you can configure device control policies.

Patch

By default, patch assessment is turned off. For new patch policies, assessment is turned on. Once patch assessment is turned on, computers are assessed daily for missing patches (if you haven’t changed the patch assessment interval). To turn patch assessment on or off or to change the assessment interval, you can configure patch policies.

Tamper protection

By default, tamper protection is turned off. To enable tamper protection, you can configure tamper policies.

Web control

By default, web control is turned off. You can turn on web control, and configure web control policies.

Exploit prevention

By default, exploit prevention is turned on. You can configure exploit prevention policies.
5.3.4 Create a policy

If you use role-based administration, you must have a respective **Policy setting** right to perform this task.

To create a policy:

1. In the **Endpoints** view, in the **Policies** pane, right-click the type of policy you want to create, for example, “Updating,” and select **Create policy**.
   
   A “New Policy” is added to the list, with its name highlighted.

2. Type a new name for the policy.

3. Double-click the new policy. Enter the settings you want.

   For the instructions on how to choose the settings, see the section on configuring the relevant policy.

You have created a policy that can now be applied to groups.

Related concepts
Managing roles and sub-estates (page 15)

5.3.5 Assign a policy to a group

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task.

1. In the **Policies** pane, highlight the policy.

2. Click the policy and drag it onto the group to which you want to apply the policy. When prompted, confirm that you want to continue.

   **Note**

   Alternatively, you can right-click a group and select **View/Edit Group Policy Details**. You can then select policies for that group from drop-down menus.
5.3.6 Edit a policy

If you use role-based administration:

• You must have a respective Policy setting right to perform this task.
• You cannot edit a policy if it is applied outside your active sub-estate.

To edit a policy for a group or groups of computers:
1. In the Policies pane, double-click the policy you want to edit.
2. Edit the settings.

For instructions on how to configure different policies, see the respective sections.

Related concepts
Managing roles and sub-estates (page 15)

5.3.7 Rename a policy

If you use role-based administration:

• You must have a respective Policy setting right to perform this task.
• You cannot rename a policy if it is applied outside your active sub-estate.

Warning
You cannot rename a “Default” policy.

To rename a policy:
1. In the Policies pane, select the policy you want to rename.
2. Right-click and select Rename policy.

Related concepts
Managing roles and sub-estates (page 15)

5.3.8 Delete a policy

If you use role-based administration:

• You must have a respective Policy setting right to perform this task.
• You cannot delete a policy if it is applied outside your active sub-estate.

Warning
You cannot delete a “Default” policy.

To delete a policy:
In the Policies pane, right-click the policy you want to delete and select Delete Policy.

Any groups that use the deleted policy will revert to using the default policy.
5.3.9 See which groups use a policy

To see which groups a particular policy has been applied to:
In the Policies pane, right-click the policy and select View Groups Using Policy.
A list of the groups that use the policy is displayed.

5.3.10 Check whether computers use the group policy

You can check whether all the computers in a group comply with the policies for that group.
1. Select the group which you want to check.
2. In the computer list, Endpoints view, on the Status tab, look in the Policy compliance column.
   • If you see the words “Same as policy”, the computer complies with the policies for its group.
   • If you see a yellow warning sign and the words “Differs from policy”, the computer is not using
     the same policy or policies as other computers in its group.

For more detailed information about the status of the security features on the computer and
policies applied to the computer, see the respective tab in the Endpoints view, for example, the
Anti-Virus Details tab.

5.3.11 Make computers use the group policy

If you use role-based administration, you must have the Remediation - updating and scanning
right to perform this task.
If you find computers that do not comply with the policies for their group, you can apply the group
policies to that computer.
1. Select the computers that do not comply with the group policy.
2. Right-click and select Comply with. Then select the appropriate policy type, for example, Group
   anti-virus and HIPS policy.

5.4 Discovering computers on the network

To manage computers in Sophos Enterprise Console, you first have to add them to Sophos
Enterprise Console You can use the “Discover computers” function and choose among several
options that allow you to search for networked computers and add them to Sophos Enterprise
Console. There are the following options:
• Import containers and computers from Active Directory.
• Discover computers with Active Directory.
• Discover computers by browsing the network.
• Discover computers by IP range.
• Import computers from a file.

If you use role-based administration, you must have the Computer search, protection and groups right to add computers to the console.

Related concepts
- Managing roles and sub-estates (page 15)

Related tasks
- Import containers and computers from Active Directory (page 35)
- Discover computers with Active Directory (page 36)
- Discover computers by browsing the network (page 36)
- Discover computers by IP range (page 37)
- Import computers from a file (page 38)

5.4.1 Import containers and computers from Active Directory

If you use role-based administration, you must have the Computer search, protection and groups right to perform this task.

Importing groups from Active Directory retrieves the Active Directory container structure and copies it into Sophos Enterprise Console as a computer group structure. You can import the group structure only or groups and computers. If you choose the latter, computers found in Active Directory are placed in their respective group, and not in the Unassigned group.

You can have both “normal” groups that you create and manage yourself and groups imported from Active Directory. You can also synchronize the imported groups with Active Directory.

To import groups from Active Directory:

1. On the toolbar, click the Discover computers icon.
2. In the Discover Computers dialog box, in the Import from Active Directory pane, select Import and click OK.
   Alternatively, select a group you want to import your Active Directory containers into, right-click and select Import from Active Directory.

   The Import from Active Directory Wizard starts.
3. Follow the instructions in the wizard. When asked to choose what to import, select Computers and containers or Containers only, depending on what you want to import.

After you have imported containers from Active Directory, apply policies to the groups.

After you have applied group policies to the groups, you can synchronize the groups with Active Directory, if you want to.

Related concepts
- Managing roles and sub-estates (page 15)
- What policies are available? (page 28)
- Synchronizing with Active Directory (page 38)
5.4.2 Discover computers with Active Directory

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task.

You can use Active Directory to discover networked computers and add them to the **Unassigned** group.

1. On the toolbar, click the **Discover computers** icon.
2. In the **Discover Computers** dialog box, select **Discover with Active Directory** and click **OK**.
3. You are prompted to enter a username and password. You need to do this if you have computers (for example, Windows XP Service Pack 2) that cannot be accessed without account details.
   - The account must have full administrative rights over the target computers.
   - If you are using a domain account, you must enter the username in the form domain\user.
4. In the **Discover Computers** dialog box, select the domains you want to search. Click **OK**.
5. Click the **Unassigned** group to see the computers that have been found.

   To begin managing computers, select them and drag them to a group.

**Related concepts**

Managing roles and sub-estates (page 15)

5.4.3 Discover computers by browsing the network

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task.

**Warning**

We don't recommend you use this method. Using SMB1 and the Computer Browser service imposes huge security risks on the whole network. Microsoft has removed this service and protocol in newer operating systems.

**Note**

If the Computer Browser service and SMB1 are not enabled on the server running Sophos Enterprise Console, this option is not available.

To add a list of computers found in Windows domains and workgroups to the **Unassigned** group:

1. On the toolbar, click the **Discover computers** icon.
2. In the **Discover Computers** dialog box, select **Discover on the network** and click **OK**.
3. In the **Credentials** dialog box, enter a username and password of an account that has sufficient rights to retrieve computer information.
   - The account must have full administrative rights over the target computers. If you are using a domain account, you must enter the username in the form domain\user.
Note
We recommend you use a specific account created for this purpose that has no other privileges.

You can skip this step if your target computers can be accessed without account details.

4. In the **Discover Computers** dialog box, select the domains or workgroups you want to search. Click **OK**.

5. Click the **Unassigned** group to see the computers that have been found.

To begin managing computers, select them and drag them to a group.

**Related concepts**
*Managing roles and sub-estates* (page 15)

### 5.4.4 Discover computers by IP range

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task.

You can use a range of IP addresses to discover networked computers and add them to the **Unassigned** group.

**Warning**
You cannot use IPv6 addresses.

1. On the toolbar, click the **Discover computers** icon.
2. In the **Discover Computers** dialog box, select **Discover by IP range** and click **OK**.
3. In the **Credentials** dialog box, you are prompted to enter a username and password. You need to do this if you have computers (for example, Windows XP Service Pack 2) that cannot be accessed without account details.

   The account must have full administrative rights over the target computers.

   **Note**
   We recommend you use a specific account created for this purpose that has no other privileges.

   If you are using a domain account, you must enter the username in the form domain\user.

   In the **SNMP** pane, you can enter the SNMP community name.
4. In the **Discover Computers** dialog box, enter the **Start of IP Range** and **End of IP Range**. Click **OK**.
5. Click the **Unassigned** group to see the computers that have been found.

To begin managing computers, select them and drag them to a group.

**Related concepts**
*Managing roles and sub-estates* (page 15)
5.4.5 Import computers from a file

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task.

To enable Sophos Enterprise Console to list your computers, you can import the computer names from a file. You can create the file using entries like this:

```
[GroupName1]
Domain1|Windows7|ComputerName1
Domain1|Windows2008ServerR2|ComputerName2
```

**Note**
You do not have to specify which group the computers will be put in. If you enter `[ ]` (with no space between the brackets) for the group name, computers will be put in the **Unassigned** group.


The domain name and the operating system are both optional. So an entry can look like this:

```
[GroupName1]
ComputerName1
```

You import computer names as follows:

1. On the **File** menu, click **Import Computers from File**.
2. In the browser window, select the file.
3. Click the **Unassigned** group to see the computers that have been found.
4. To begin managing computers, select them and drag them to a group.

**Related concepts**
Managing roles and sub-estates (page 15)

5.5 Synchronizing with Active Directory

This section gives an overview of Active Directory synchronization.

**What does Active Directory synchronization do for me?**

With Active Directory synchronization, you can synchronize Sophos Enterprise Console groups with Active Directory containers. New computers and containers discovered in Active Directory are copied into Sophos Enterprise Console automatically. You can also choose to protect discovered Windows workstations automatically. This allows you to minimize the time in which computers can become infected and reduce the amount of work you need to do to organize and protect computers.
Note
Computers running Windows server operating systems, Mac OS, Linux, or UNIX are not protected automatically. You must protect such computers manually.

After you have set up synchronization, you can set up email alerts to be sent to your chosen recipients about new computers and containers discovered during future synchronizations. If you choose to protect computers in synchronized Sophos Enterprise Console groups automatically, you can also set up alerts about automatic protection failures.

How does Active Directory synchronization work?

In Sophos Enterprise Console, you can have both “normal,” unsynchronized groups that you manage yourself and groups synchronized with Active Directory.

When setting up synchronization, you select or create a synchronization point: a Sophos Enterprise Console group to be synchronized with an Active Directory container. All computers and subgroups contained in the Active Directory are copied into Sophos Enterprise Console and kept synchronized with Active Directory.

After you set up synchronization with Active Directory, the synchronized part of Sophos Enterprise Console group structure matches exactly the Active Directory container it is synchronized with. This means the following:

• If a new computer is added to the Active Directory container, then it also appears in Enterprise Console.

• If a computer is removed from Active Directory or is moved into an unsynchronized container, then the computer is moved to the Unassigned group in Sophos Enterprise Console.

Warning
When a computer is moved to the Unassigned group, it stops receiving new policies.

• If a computer is moved from one synchronized container to another, then the computer is moved from one Sophos Enterprise Console group to the other.

• If a computer already exists in a group when it is first synchronized, then it is moved from that group to the synchronized group that matches its location in Active Directory.

• When a computer is moved into a new group with different policies, then new policies are sent to the computer.

By default, synchronization occurs every 60 minutes. You may change the synchronization interval if required.

How do I approach synchronization?

It is your decision what groups to synchronize with Active Directory and how many synchronization points to set up. Consider whether the size of groups that will be created will be manageable. You should be able to deploy software, scan and clean up computers easily. This is especially important for the initial deployment.
Note
If you have a complex Active Directory structure and want to synchronize domain local groups or nested Active Directory groups, see knowledge base article 122529 for information about enabling this functionality.

The recommended approach is as follows:
1. Import the group structure (without computers), using the Import from Active Directory function.
2. Review the imported group structure and choose your synchronization points.
3. Set up group policies and apply them to the groups and subgroups.
4. Synchronize your chosen synchronization points, one at a time, with Active Directory.

Related concepts
What is a synchronization point? (page 40)
What is a synchronized group? (page 40)

Related tasks
Import containers and computers from Active Directory (page 35)
Create a policy (page 32)
Assign a policy to a group (page 32)
Synchronize with Active Directory (page 41)

Related information
knowledge base article 122529

5.5.1 What is a synchronization point?
A synchronization point is a Sophos Enterprise Console group that points to a container (or subtree) in Active Directory. A synchronization point can contain synchronized groups imported from Active Directory.

In the Groups pane, a synchronization point appears as follows:

You can move, rename, or delete a synchronization point. You can also change policies and synchronization settings, including automatic protection settings, for a synchronization point.

You cannot create or delete subgroups in a synchronization point, or move other groups into it. You cannot move computers into or from the synchronization point.

5.5.2 What is a synchronized group?
A synchronized group is a subgroup of a synchronization point, imported from Active Directory.

In the Groups pane, a synchronized group appears as follows:

You can change policies assigned to a synchronized group.

You cannot change any synchronized group settings other than group policies. You cannot rename, move, or delete a synchronized group. You cannot move computers or groups into or from the group.
You cannot create or delete subgroups in the group. You cannot change synchronization settings for the group.

5.5.3 Synchronize with Active Directory

Before you perform this task:

- If you use role-based administration, you must have the Computer search, protection and groups right.
- If you want to protect computers in synchronized groups automatically, make sure you have prepared the computers.
- If you have a complex Active Directory structure and want to synchronize domain local groups or nested Active Directory groups, enable this functionality as described in knowledge base article 122529.

To synchronize with Active Directory:

1. Select a group that will become your synchronization point, right-click and select Synchronize with Active Directory. The Synchronize with Active Directory wizard starts.
2. On the Overview page of the wizard, click Next.
3. On the Choose an Enterprise Console group page, select or create a Sophos Enterprise Console group that you want to keep synchronized with Active Directory (synchronization point). Click Next.
4. On the Choose an Active Directory container page, select an Active Directory container which you want to synchronize the group with. Enter the name of the container (for example, LDAP:// CN=Computers,DC=domain_name,DC=local) or click Browse to browse to the container in Active Directory. Click Next.

Note
If a computer exists in more than one synchronized Active Directory container, it causes a problem, with messages being exchanged continually between the computer and Sophos Enterprise Console. Each computer should be listed only once in Sophos Enterprise Console.

5. If you want to protect Windows workstations automatically, on the page Protect Computers Automatically, select the check box Install Sophos security software automatically, and then select the software you want to install.

Note
For a list of system requirements for the software, see the system requirements page on the Sophos website.

- Before installing Firewall on computers, make sure you have configured the firewall to allow the traffic, applications, and processes you want to use. By default, the firewall is enabled and blocks all non-essential traffic.
- Leave Third-Party Security Software Detection selected if you want to have another vendor’s software removed automatically. If you need to remove another vendor’s updating tool, see Remove third-party security software.

All Windows workstations discovered during this and future synchronizations will be protected automatically, in compliance with their respective group policies.
Note
Computers running Windows server operating systems, Mac OS, Linux, or UNIX will not be protected automatically. You must protect such computers manually, as described in the Sophos Enterprise Console advanced startup guide.

Note
You can enable or disable automatic protection later, in the Synchronization properties dialog box.

Click Next.

6. If you chose to protect computers automatically, on the Enter Active Directory Credentials page, enter the details of an administrator account that will be used to install software on the computers. Click Next.

7. On the Choose the Synchronization Interval page, choose how often you want to synchronize the Sophos Enterprise Console group with the Active Directory container. The default is 60 minutes.

Note
You can change the synchronization interval later, in the Synchronization properties dialog box.

8. On the Confirm Your Choices page, check the details, and then click Next to proceed.

9. On the last page of wizard, you can view the details of the groups and computers that have been synchronized.

You can also set up email alerts to be sent to your chosen recipients about new computers and groups discovered during future synchronizations. If you chose to protect computers in synchronized groups automatically, you can also set up alerts about automatic protection failures. To open the Configure Email Alerts dialog box after you click Finish, select the check box on the last page of the wizard.

a) To close the wizard, click Finish.

Related concepts
Managing roles and sub-estates (page 15)
Firewall policy (page 117)

Related tasks
Prepare for installation of security software (page 49)
Remove third-party security software (page 49)
View and edit synchronization properties (page 43)
Set up Active Directory synchronization email alerts (page 195)
You can set up email alerts to be sent to your chosen recipients about new computers and groups discovered during synchronizations with Active Directory.

Related information
knowledge base article 122529
Sophos system requirements
5.5.4 Use synchronization to protect computers automatically

Before you perform this task:

- If you use role-based administration, you must have the Computer search, protection and groups right.
- Make sure you have prepared computers for automatic installation of the security software.

Windows workstations can be protected automatically when discovered during synchronization with Active Directory.

**Warning**
Computers running Windows server operating systems, Mac OS, Linux, or UNIX will not be protected automatically. You must protect such computers manually as described in the Sophos Enterprise Console advanced startup guide.

You can protect computers in synchronized groups automatically either when setting up synchronization, or by editing the synchronization properties later.

The instructions below tell you how to protect computers by editing the synchronization properties.

1. In the Groups pane, select the group (synchronization point) for which you want to enable automatic protection. Right-click the group and select Synchronization Properties.
2. In the Synchronization Properties dialog box, select the Install Sophos security software automatically check box, and then select the software you want to install.
   - Before installing Firewall on computers, make sure you have configured the firewall to allow the traffic, applications, and processes you want to use. By default, the firewall is enabled and blocks all non-essential traffic.
   - Leave Third-Party Security Software Detection selected if you want to have another vendor's software removed automatically. If you need to remove another vendor's updating tool, see Remove third-party security software.
3. Enter the username and password of an administrator account that will be used to install software on the computers. Click OK.

Should you want to disable automatic protection later, in the Synchronization Properties dialog box, clear the Install Sophos security software automatically check box.

**Related concepts**
Managing roles and sub-estates (page 15)
Firewall policy (page 117)

**Related tasks**
Prepare for installation of security software (page 49)
Synchronize with Active Directory (page 41)
Remove third-party security software (page 49)

5.5.5 View and edit synchronization properties

Before you perform this task:

- If you use role-based administration, you must have the Computer search, protection and groups right.
If you want to protect computers in synchronized groups automatically, make sure you have prepared the computers.

If you have a complex Active Directory structure and want to synchronize domain local groups or nested Active Directory groups, enable this functionality as described in knowledge base article 122529.

To view and edit synchronization properties:

1. In the Groups pane, select the group (synchronization point) for which you want to edit synchronization properties. Right-click the group and select Synchronization Properties. The Synchronization Properties dialog box appears.
2. In the Active Directory container field, you can see the container which the group is synchronized with. If you want to synchronize the group with a different container, remove synchronization and run the Synchronize with Active Directory wizard again.
3. In the Synchronization interval field, set the frequency of synchronization. The default is 60 minutes. The minimum is 5 minutes.
4. Select the Install Sophos security software automatically check box if you want to protect all newly discovered Windows workstations automatically, in compliance with their respective group policies.
   a) Under Features, the anti-virus protection is selected by default. If you want to have other Sophos security software installed, select the relevant check boxes.
   b) Enter the username and password of an administrator account that will be used to install software on the computers.

Note
Only Windows workstations can be protected automatically. Computers running Windows server operating systems, Mac OS, Linux, or UNIX cannot be protected automatically. You must protect such computers manually, as described in the Sophos Enterprise Console advanced startup guide.

Related concepts
Managing roles and sub-estates (page 15)
Related tasks
Prepare for installation of security software (page 49)
Turn synchronization on or off (page 45)
Synchronize with Active Directory (page 41)
Related information
knowledge base article 122529

5.5.6 Synchronize with Active Directory now

Before you perform this task:

- If you use role-based administration, you must have the Computer search, protection and groups right.
- If you want to protect computers in synchronized groups automatically, make sure you have prepared the computers.
- If you have a complex Active Directory structure and want to synchronize domain local groups or nested Active Directory groups, enable this functionality as described in knowledge base article 122529.
You can synchronize Sophos Enterprise Console groups (synchronization points) with Active Directory containers immediately, without waiting for the next scheduled synchronization.

To synchronize with Active Directory immediately:

1. In the **Groups** pane, select the group (synchronization point) which you want to synchronize with Active Directory. Right-click the group and select **Synchronization Properties**.
2. In the **Synchronization Properties** dialog box, make changes as appropriate and click **OK**.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Prepare for installation of security software (page 49)

**Related information**
- knowledge base article 122529

### 5.5.7 Turn synchronization on or off

Before you perform this task:

- If you use role-based administration, you must have the **Computer search, protection and groups** right.
- If you want to protect computers in synchronized groups automatically, make sure you have prepared the computers.
- If you have a complex Active Directory structure and want to synchronize domain local groups or nested Active Directory groups, enable this functionality as described in knowledge base article 122529.

To turn synchronization with Active Directory on or off:

1. To turn the synchronization on, run the **Synchronize with Active Directory** wizard.
2. To turn the synchronization off, select the group (synchronization point) which you do not want to synchronize with Active Directory anymore, right-click and select **Remove Synchronization**. Click **Yes** to confirm.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Prepare for installation of security software (page 49)
- Synchronize with Active Directory (page 41)

**Related information**
- knowledge base article 122529

### 5.6 Configure the Sophos Mobile URL

Sophos Mobile is a device management solution for mobile devices such as smartphones and tablets. Sophos Mobile helps to keep corporate data safe by managing apps and security settings.

You can open the Sophos Mobile web console from Sophos Enterprise Console by clicking the **Sophos Mobile** toolbar button. To do this, you first need to configure the Sophos Mobile URL.

1. On the **Tools** menu, click **Configure Sophos Mobile URL**.

Copyright © Sophos Limited
2. In the **Configure Sophos Mobile URL** dialog box, enter the URL of the Sophos Mobile web console and click **OK**.

### 5.7 Multi-factor authentication

You can use multi-factor authentication in Sophos Enterprise Console.

For each Sophos Enterprise Console administrator we recommend that you use multi-factor authentication and set it up as follows to get the best security.

**Note**

We recommend that you create a recovery account during installation and assign the **Multi-factor authentication** role to this account. You should only use this account for recovery.

For each administrator:

- Create a non-administrative account. The administrator must use this account to access Sophos Enterprise Console.
- Add this account to the **Sophos Console Administrators** and **DCOM Users** groups.
- Add this account to a role and a sub-estate in **Manage Roles and Sub-Estates**. You can also add this account to the **Sophos Full Administrators** Windows local group.
- Enroll this account in multi-factor authentication in Sophos Enterprise Console.

Additionally, remove all administrators (members of Administrators and or Domain Administrators groups) from the **Sophos Console Administrators** group.

**Note**

Make sure there is at least one administrator who has the **Role-based administration** and the **Multi-factor authentication** rights.

### Multi-factor authentication administration dialog

If you have the **Multi-factor authentication** role you can see which administrators have been enrolled in **Multi-factor authentication**. Administrators that appear in the list have been enrolled at least once.

You can turn on, turn off or reset multi-factor authentication for an administrator using the buttons below the list. Click on an administrator to do this.

You can also right-click on an administrator to bring up a context menu with the same options.

**Related concepts**

- Managing roles and sub-estates (page 15)

**Related tasks**

- Setting up multi-factor authentication (page 47)
  
  Follow these instructions to turn on multi-factor authentication.

- Enroll in multi-factor authentication (page 47)
  
  Follow these instructions to enroll.

- Remove multi-factor authentication (page 48)
Follow these instructions to remove multi-factor authentication.

### 5.7.1 Setting up multi-factor authentication

Follow these instructions to turn on multi-factor authentication.

If you use role-based administration, you must have the Multi-factor authentication right to perform this task.

To turn on multi-factor authentication:
1. Click **Tools > Manage Multi-factor authentication**.
2. In **Multi-factor authentication administration**, select **Enable multi-factor authentication** and click **OK**.

**Related concepts**
- [Multi-factor authentication](#) (page 46)
  You can use multi-factor authentication in Sophos Enterprise Console.
- [Managing roles and sub-estates](#) (page 15)

**Related tasks**
- [Enroll in multi-factor authentication](#) (page 47)
  Follow these instructions to enroll.
- [Remove multi-factor authentication](#) (page 48)
  Follow these instructions to remove multi-factor authentication.

### 5.7.2 Enroll in multi-factor authentication

Follow these instructions to enroll.

To enroll in multi-factor authentication:
1. Click **Tools > Manage multi-factor authentication**.
2. Click **Enroll my device**.
   - This displays an enrollment QR code.
3. Scan the QR code with Sophos Mobile.
   - If scanning the QR code with your device does not work or is not an option, you can register your device manually.
   - a) To get the required parameters, click the **Show algorithm details** button below the QR code and enter those parameters in Sophos Mobile.
4. Enter the authentication code displayed on the mobile device then click **OK**.
   - A pop-up dialog tells you the result of your registration.

Once you have enrolled, when you open Sophos Enterprise Console an **Authentication required** dialog opens. You must enter the code generated by your device to use Sophos Enterprise Console.

An authenticated session lasts for ten hours. Five minutes before your session is expired a warning is displayed. A countdown timer is also displayed. You can then extend your session by an additional ten hours or close Sophos Enterprise Console. If the timer runs out, Sophos Enterprise Console restarts and you must authenticate.

**Related concepts**
- [Multi-factor authentication](#) (page 46)
You can use multi-factor authentication in Sophos Enterprise Console.

**Managing roles and sub-estates** *(page 15)*

**Related tasks**

**Setting up multi-factor authentication** *(page 47)*
Follow these instructions to turn on multi-factor authentication.

**Remove multi-factor authentication** *(page 48)*
Follow these instructions to remove multi-factor authentication.

### 5.7.3 Remove multi-factor authentication

Follow these instructions to remove multi-factor authentication.

To unenroll from multi-factor authentication:

1. Click **Tools > Manage Multi-factor authentication**.
2. Authenticate using the code generated by your device.
3. Click **Unenroll my device**.
   You are no longer enrolled in multi-factor authentication.

**Related concepts**

**Multi-factor authentication** *(page 46)*
You can use multi-factor authentication in Sophos Enterprise Console.

**Managing roles and sub-estates** *(page 15)*

**Related tasks**

**Setting up multi-factor authentication** *(page 47)*
Follow these instructions to turn on multi-factor authentication.

**Enroll in multi-factor authentication** *(page 47)*
Follow these instructions to enroll.
6 Protecting computers

You can install Sophos protection software in the following ways:

• To protect computers automatically, use the protect computer wizard provided in Sophos Enterprise Console.
• Alternatively, you can protect computers automatically using Active Directory synchronization.
• To protect computers manually, Sophos Enterprise Console helps to locate the required software. Then go to the computer and install the security software manually.

Related concepts
Synchronizing with Active Directory (page 38)

Related tasks
Protect computers automatically (page 50)
Locate installers for protecting computers manually (page 52)

6.1 Prepare for installation of security software

As well as ensuring that computers meet the general system requirements, you must perform further steps before you can install software on them automatically.

Note
Automatic installation is not possible on Mac, Linux and UNIX computers.

If you use Active Directory, you can prepare your computers using a Group Policy Object (GPO). If you use workgroups, you must configure computers locally.

To watch deployment videos, go to knowledge base article 111180.

Related information
knowledge base article 111180

6.2 Remove third-party security software

If you want to remove any previously installed security software, do the following BEFORE selecting the Third-Party Security Software Detection in the Protect Computers Wizard and installing it:

• If computers are running another vendor’s anti-virus software, ensure that its user interface is closed.
• If computers are running another vendor’s firewall or HIPS product, ensure that it is turned off or configured to allow the Sophos installer to run.
• If you want to remove not just the other vendor’s software but also the other vendor’s update tool (to prevent it from reinstalling the software automatically), follow the steps below. If computers have no update tool installed, you can disregard the steps below.
Note
You have to locally restart any computers from which you remove third-party anti-virus software.

Note
HitmanPro.Alert may already be installed either as a standalone product or from Sophos Central. You should remove HitmanPro.Alert before applying on-premise management from Sophos Enterprise Console.

If computers have another vendor’s update tool installed and you wish to remove the update tool, you will need to modify the configuration file before selecting the Third-Party Security Software Detection option in the Protect Computers Wizard.

Note
If computers are running another vendor’s firewall or HIPS product, you may need to leave that vendor’s update tool intact. See that vendor’s documentation for clarification.

To modify the configuration file:
1. From the Central Installation Directory, find the data.zip file.
2. Extract the crt.cfg configuration file from data.zip.
3. Edit the crt.cfg file to change the line reading "RemoveUpdateTools=0" to "RemoveUpdateTools=1".
4. Save your changes and save crt.cfg to the same directory that contains data.zip. Do not put crt.cfg back into data.zip or it will be overwritten the next time the data.zip file is updated.

When you run the Protect Computers Wizard and select Third-Party Security Software Detection, the modified configuration file will now remove any third-party security update tools as well as third-party security software.

6.3 Protect computers automatically

Before you protect computers from the console:

• You must apply an updating policy to the group before you can protect computers in that group.
• Make sure you have prepared computers for automatic installation of the security software.
• If you use role-based administration, you must have the Computer search, protection and groups right to protect computers.

Automatic installation is not possible on Mac, Linux and UNIX computers. Use manual installation instead. For the instructions, see the Sophos Enterprise Console advanced startup guide.

If you chose to synchronize with Active Directory and protect the computers automatically, you do not need to follow the steps below.

To protect computers automatically:
1. Depending on whether or not the computers you want to protect are already in a group, do one of the following:
   • If the computers you want to protect are in the Unassigned group, drag the computers onto a group.
• If the computers you want to protect are already in a group, select the computers, right-click and click Protect Computers.

The Protect Computers Wizard is launched. Follow the instructions in the wizard.

2. On the Select features page, select the features you want.

Note
For a list of system requirements for the features, see the system requirements page on the Sophos website.

Some features, including anti-virus protection, are always selected and must be installed. You can also select to install the features listed below. Some of the features are available only if your license includes them.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>Before installing the firewall on computers, make sure you have configured the firewall to allow the traffic, applications, and processes you want to use. By default, the firewall is enabled and blocks all non-essential traffic.</td>
</tr>
<tr>
<td>Patch</td>
<td></td>
</tr>
<tr>
<td>Exploit Prevention, Sophos Clean</td>
<td>This protects against ransomware and exploits. It is selected by default if your license includes this feature.</td>
</tr>
<tr>
<td></td>
<td>If you upgrade your license to include Exploit Prevention (with Sophos Clean), it is not automatically installed on computers you already manage. You need to reprotect the computers to install it.</td>
</tr>
<tr>
<td>Third-Party Security Software Detection</td>
<td>Leave Third-Party Security Software Detection selected if you want to have another vendor's software removed automatically. The Third-Party Security Software Detection uninstalls only products with the same functionality as those you install. If you need to remove another vendor's updating tool, see Remove third-party security software.</td>
</tr>
</tbody>
</table>

3. On the Protection summary page, any problems with installation are shown in the Protection issues column. Troubleshoot the installation, or carry out manual installation on these computers (see the Sophos Enterprise Console advanced startup guide). Click Next.

4. On the Credentials page, enter details of an account which can be used to install software.

The account must have the following:
• Local administrator rights on computers you want to protect.
• Be able to log on to the computer where you installed the management server.
• Read access to the Primary server location specified in the Updating policy.
If you are using a domain account, you must enter the username in the form \domain\user. If the computers are on different domains covered by the same Active Directory schema, use the Sophos Enterprise Console account in Active Directory instead.

We recommend you use a specific account created for this purpose that has no other privileges.

**Related concepts**
- Managing roles and sub-estates (page 15)
- Synchronizing with Active Directory (page 38)
- Firewall policy (page 117)
- Sophos Endpoint Security and Control installation failed (page 224)
- Configure update servers (page 75)

**Related tasks**
- Prepare for installation of security software (page 49)
- Remove third-party security software (page 49)

**Related information**
- Sophos system requirements

### 6.4 Locate installers for protecting computers manually

If Sophos Enterprise Console is unable to install anti-virus, firewall, or patch features on certain computers automatically, you can perform the installation manually.

To locate the installers:

1. On the **View** menu, click **Bootstrap Locations**.
2. In the **Bootstrap Locations** dialog box, for each software subscription, you will see the locations that contain the software installers, as well as platforms that the software is supported on and the software versions. Make a note of the location for the installer that you need.

For information about how to install security software manually on different operating systems, see the Sophos Enterprise Console advanced startup guide.

### 6.5 Checking whether your network is protected

For an overview of the network’s security status, use the Dashboard.

You can identify computers with a problem by using the computer list and computer list filters. For example, you can see which computers do not have the firewall or patch features installed, or have alerts that need attention.

You can also check whether all the computers in a group comply with the policies for that group.
Related tasks
Configure the Dashboard (page 53)
Check that computers are protected (page 53)
Check that computers are up to date (page 54)
Find computers with problems (page 54)
Check whether computers use the group policy (page 34)

Related reference
Dashboard panels (page 6)

6.6 Configure the Dashboard

If you use role-based administration, you must have the System configuration right to configure the Dashboard.

The Dashboard displays warning or critical status indicators based on the percentage of managed computers that have outstanding alerts or errors, or on the time since the last update from Sophos.

You can set up the warning and critical levels you want to use.

1. On the Tools menu, click Configure Dashboard.
2. In the Configure Dashboard dialog box, change the threshold values in the Warning level and Critical level text boxes as described below.
   a) Under Computers with outstanding alerts, Computers with Sophos product errors, and Policy and protection, enter a percentage of managed computers affected by a specific problem, that will trigger the change of the respective indicator to “warning” or “critical.”
   b) Under Computers with events, enter the number of events occurred within a seven-day period that will trigger an alert displayed on the Dashboard.
   c) Under Latest protection from Sophos, enter the time since last successful update from Sophos in hours, that will trigger the change of the “Updates” indicator to “warning” or “critical.”
      Click OK.

      If you set a level to zero, warnings are triggered as soon as the first alert is received.

You can also set up email alerts to be sent to your chosen recipients when a warning or critical threshold has been exceeded.

Related concepts
Managing roles and sub-estates (page 15)
Setting up alerts and messages (page 188)

6.7 Check that computers are protected

Computers are protected if they are running on-access scanning and the firewall (if you have installed it). For full protection, the software must also be up to date.

Note
You may have chosen not to use on-access scanning on certain types of computer, for example, file servers. In this case, ensure that the computers use scheduled scans and that they are up to date.

To check that computers are protected:
1. Select the group of computers you want to check.
2. If you want to check computers in subgroups of the group, select **At this level and below** in the drop-down list.
3. In the list of computers, on the **Status** tab, look in the **On-access** column. If you see “Active,” the computer is running on-access scanning. If you see a gray shield, it is not.
4. If you installed the firewall, look in the **Firewall enabled** column. If you see “Yes,” the firewall is enabled. If you see a gray firewall sign and the word “No,” the firewall is disabled.
5. If you use other features, such as application control, data control, or patch, check the status in the respective column.

**Related tasks**
- Check that computers are up to date (page 54)
- Find computers with problems (page 54)

**6.8 Check that computers are up to date**

If you set up Sophos Enterprise Console as recommended, computers should receive updates automatically.

To check that computers are up to date:

1. Select the group of computers you want to check.
2. If you want to check computers in any subgroups, select **At this level and below** in the drop-down list.
3. On the **Status** tab, look in the **Up to date** column, or go to the **Update details** tab.
   - If you see “Yes” in the **Up to date** column, the computer is up to date.
   - If you see a clock icon, the computer is out of date. The text indicates how long the computer has been out of date.

**Related tasks**
- Update out-of-date computers (page 83)

**6.9 Find computers with problems**

To display a list of computers that are not properly protected or have other protection-related problems:

1. Select the group of computers you want to check.
2. In the **View** drop-down list, select which computers you want to find, for example, **Computers with potential problems**.
   - You can also select a subentry of an entry, to display computers affected by a specific problem (for example, computers that differ from group policy, computers with outstanding alerts, or computers where an installation error has occurred).
3. If the group contains subgroups, select also whether you want to find computers **At this level only** or **At this level and below**. Any computers that have protection problems will be listed.

You can also filter the computer list by the name of a detected item such as malware, potentially unwanted application, or suspicious file.
Related concepts

Troubleshooting (page 222)
When you run the Protect computers wizard, installation of security software can fail for a number of reasons.

Related tasks

Filter computers by the name of a detected item (page 10)
Computers are not running on-access scanning (page 222)

6.10 Dealing with alerts and errors

If a virus or spyware, a suspicious item, an adware or other potentially unwanted application is detected, alert icons are displayed on the Status tab in the Endpoints view.

Note

Warnings are also displayed in the console if software is disabled or out of date.

For more details about an alert, for example, the name of the detected item, click the Alert and Error Details tab.

Related concepts

Checking whether your network is protected (page 52)
Monitoring the update manager (page 82)

Related reference

What do the alert icons mean? (page 55)

6.10.1 What do the alert icons mean?

<table>
<thead>
<tr>
<th>Icon</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>A red warning sign displayed in the Alerts and errors column means that a virus, worm, Trojan, spyware, or suspicious behavior has been detected.</td>
</tr>
</tbody>
</table>
| !     | A yellow warning sign displayed in the Alerts and errors column indicates one of the following problems:  
  • A suspicious file has been detected.  
  • An adware or other potentially unwanted application has been detected.  
  • An error has occurred.  
  A yellow warning sign displayed in the Policy compliance column indicates that the computer is not using the same policy or policies as other computers in its group. |

If there are multiple alerts or errors on a computer, the icon of an alert that has the highest priority will be displayed in the Alerts and errors column. Alert types are listed below in descending order of priority.

1. Virus and spyware alerts
2. Suspicious behavior alerts
3. Suspicious file alerts
4. Adware and PUA alerts
5. Software application errors (for example, installation errors)

6.10.2 Deal with alerts about detected items

If you use role-based administration, you must have the Remediation - cleanup right to clean up detected items or clear alerts from the console.

To take action against alerts displayed in the console:

1. In the Endpoints view, select the computers for which you want to see alerts. Right-click and select Resolve Alerts and Errors. The Resolve alerts and errors dialog box is displayed.

2. The action you can take against an alert depends on the cleanup status of the alert. Look in the Cleanup status column and decide what action you want to take.

**Tip**
You can sort alerts by clicking on a column heading. For example, to sort alerts by cleanup status, click the Cleanup status column heading.

<table>
<thead>
<tr>
<th>Cleanup status</th>
<th>Description and actions to take</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cleanable</td>
<td>You can remove the item. To do this, select the alert or alerts and click Cleanup.</td>
</tr>
<tr>
<td>Threat type not cleanable</td>
<td>This type of detected item, for example, suspicious file, suspicious behavior or malicious network traffic, cannot be cleaned up from the console. You have to decide whether you want to allow or block the item. If you do not trust the item, you can send it to Sophos for analysis.</td>
</tr>
<tr>
<td>Not cleanable</td>
<td>This item cannot be cleaned up from the console.</td>
</tr>
<tr>
<td>Full scan required</td>
<td>This item may be cleanable, but a full scan of the endpoint is required before the cleanup can be carried out.</td>
</tr>
<tr>
<td>Restart required</td>
<td>The item has been partially removed, but the endpoint needs to be restarted to complete the cleanup. Endpoints must be restarted locally, not from Sophos Enterprise Console.</td>
</tr>
<tr>
<td>Cleanup failed</td>
<td>The item could not be removed. Manual cleanup may be required.</td>
</tr>
<tr>
<td>Cleanup in progress (started &lt;time&gt;)</td>
<td>Cleanup is in progress.</td>
</tr>
<tr>
<td>Cleanup timed out (started &lt;time&gt;)</td>
<td>Cleanup has timed out. The item may not have been cleaned up. This may happen, for example, when the endpoint is disconnected from the network or the network is busy. You may try to clean up the item again later.</td>
</tr>
</tbody>
</table>
6.10.3 Find information about detected items

If you want to learn more about a threat or other item detected on an endpoint and reported in the console, or need advice on what action to take against the item, follow these steps:

1. In the **Endpoints** view, in the computer list, double-click the affected computer.
2. In the **Computer details** dialog box, scroll down to the **Outstanding alerts and errors** section. In the list of detected items, click the name of the item you are interested in.
   This connects you to the Sophos website, where you can read a description of the item and advice on what actions to take against it.

   **Note**
   Alternatively, you can go to the **Security analyses** page on the Sophos website, select the type of item you want to find, and type the name of the item in the search box.

6.10.4 Deal with alerts about ransomware

If you use role-based administration, you must have the **Remediation - cleanup** right to clean up detected items or clear alerts from the console.

CryptoGuard blocks the process on the endpoint that has generated the ransomware alert. The block is only removed when you acknowledge the alert.

   **Note**
   If the endpoint is restarted the block is removed. A new ransomware alert is generated if the infected process restarts.

   **Note**
   You must manually run Sophos Clean on the computer triggering the detection. If you do not, the computer will trigger the alert and the process will be re-blocked every time it runs.

To take action against ransomware alerts displayed in the console:

1. In the **Endpoints** view, select the computer(s) for which you want to see alerts. Right-click and select **Resolve Alerts and Errors**.
   The **Resolve alerts and errors** dialog box is displayed.
2. Select the ransomware alerts you want to clear and click **Acknowledge**.
Acknowledged (cleared) alerts are no longer displayed in the console. This removes the block on the process.

**Related concepts**
Managing roles and sub-estates (page 15)

### 6.10.5 Clear endpoint alerts or errors from the console

If you use role-based administration, you must have the **Remediation - cleanup** right to clear alerts or errors from the console.

If you are taking action to deal with an alert, or are sure that a computer is safe, you can clear the alert sign displayed in the console.

**Note**
You cannot clear alerts about installation errors. These are cleared only when Sophos Endpoint Security and Control is installed successfully on the computer.

1. In the **Endpoints** view, select the computers for which you want to clear alerts. Right-click and select **Resolve Alerts and Errors**.
   The **Resolve alerts and errors** dialog box is displayed.
2. To clear alerts or Sophos product errors from the console, go to the **Alerts** or **Errors** tab, respectively, select the alerts or errors you want to clear and click **Acknowledge**.
   Acknowledged (cleared) alerts are no longer displayed in the console.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Clear update manager alerts from the console (page 83)

### 6.11 Scanning and cleaning up computers now

#### 6.11.1 Scan computers now

You can scan a computer or computers immediately, without waiting for the next scheduled scan.

If you use role-based administration, you must have the **Remediation - updating and scanning** right to scan computers.

**Warning**
Only Windows, Linux and UNIX computers can perform immediate full system scans originated from the console.

To scan computers immediately:

1. Select the computers in the computer list or a group in the **Groups** pane. Right-click and select **Full system scan**.
   a) Alternatively, on the **Actions** menu, select **Full system scan**.
2. In the **Full system scan** dialog box, review the details of the computers to be scanned and click **OK** to start the scan.

**Note**
If the scan detects components of a threat in memory, the scan stops and an alert is sent to Sophos Enterprise Console. This is because further scanning could enable the threat to spread. You must clean up the threat before running the scan again.

**Related concepts**
Managing roles and sub-estates (page 15)

### 6.11.2 Clean up computers now

You can immediately clean up Windows or Mac computers that are infected with a virus or have unwanted applications on them.

If you use role-based administration, you must have the **Remediation - cleanup** right to clean up computers.

**Note**
To clean up Linux or UNIX computers, you can either set up automatic cleanup from the console or clean up the computers individually.

If an item (for example, a Trojan or potentially unwanted application) has been “partially detected”, before cleaning up the affected computer you will need to carry out a full system scan of the computer to find all the components of the partially detected item. In the computer list, **Endpoints** view, right-click the affected computer and click **Full System Scan**.

To clean up computers immediately:

1. In the computer list, **Endpoints** view, right-click the computers that you want to clean up and then click **Resolve Alerts and Errors**.
2. In the **Resolve Alerts and Errors** dialog box, on the **Alerts** tab, select the check box for each item you want to clean up, or click **Select all**. Click **Cleanup**.

If the cleanup is successful, the alerts shown in the list of computers will no longer be displayed.

If any alerts remain, you should clean up computers manually.

**Note**
Cleanup of some viruses causes a full system scan to be run on the affected computers, which tries to clean up all the viruses. This might take a long time. The alerts are updated at the end of the scan.

**Related concepts**
Managing roles and sub-estates (page 15)
Partially detected item (page 226)

**Related tasks**
Set up automatic cleanup for on-access scanning (page 89)
Deal with detected items if cleanup fails (page 60)
6.11.3 Deal with detected items if cleanup fails

If you cannot clean up computers from the console, you can perform the cleanup manually.

1. In the computer list, double-click the infected computer.
2. In the Computer details dialog box, scroll down to the Outstanding alerts and errors section. In the list of detected items, click the name of the item you want to remove from the computer. This connects you to the Sophos website, where you can read advice on how to clean up the computer.
3. Go to the computer and carry out the cleanup manually.

Note
The Sophos website provides special downloadable disinfectors for certain viruses and worms.
7 Updating computers

7.1 Configuring the update manager

An update manager enables you to set up automatic updating of Sophos security software from a Sophos website. An update manager is installed with and managed from Sophos Enterprise Console.

You can install additional update managers. For example, if you have a complex network with several locations, you may want to install an additional update manager at a remote location.

Related tasks
Add an additional update manager (page 67)

7.1.1 How does an update manager work?

Once you have configured an update manager, it:

• Connects at a scheduled frequency to a data distribution warehouse at Sophos or on your network.
• Downloads updates to the threat detection data and updates for the security software to which the administrator has subscribed.
• Places the updated software in one or more network shares in a form suitable for installation on endpoint computers.

The computers update automatically from the shares, provided the Sophos software installed on them has been configured to do so, for example, by applying an updating policy.

7.1.2 View or edit update manager configuration

If you use role-based administration, you must have the Policy setting - updating right to configure an update manager.

1. If you are in the Endpoints view, click the Update managers button on the toolbar to display the Update managers view.
2. In the list of update managers, select the update manager whose configuration you want to view or edit. Right-click and click View/Edit configuration.

Note
Alternatively, select the update manager, go to the Actions menu, point to Update manager, and then click View/Edit configuration.

The Configure update manager dialog box appears.

3. Edit the configuration.
   • Select and update source for an update manager.
   • Select which software to download.
   • Specify where the software is placed.
Sophos Enterprise Console

- Create or edit and update schedule.
- Configure the update manager log.
- Configure the self-updating of an update manager.

After you configure the update manager, you can configure your updating policies and apply them to the endpoint computers.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Select an update source for an update manager (page 62)
Select which software to download (page 63)
Specify where the software is placed (page 64)
Create or edit an update schedule (page 65)
Configure the update manager log (page 66)
Configure the self-updating of an update manager (page 66)
Clear update manager alerts from the console (page 83)

### 7.1.3 Select an update source for an update manager

If you use role-based administration, you must have the **Policy setting - updating** right to configure an update manager.

You need to select a source from which an update manager will download security software and updates for distribution across the network.

You can select several sources. The first source in the list is the primary source. Additional sources in the list are optional alternate locations that the update manager uses if it cannot collect an update from the primary source.

1. If you are in the **Endpoints** view, click the **Update managers** button on the toolbar to display the **Update managers** view.
2. In the list of update managers, select the update manager for which you want to select an update source. Right-click and click **View/Edit configuration**.
3. In the **Configure update manager** dialog box, on the **Sources** tab, click **Add**.
4. In the **Source details** dialog box, in the **Address** field, enter the address of the source. The address can be a UNC or HTTP path.
   - If you want to download software and updates directly from Sophos, select **Sophos**.
   - If the update source is the default update share created by an update manager located higher in the updating hierarchy, the **Username** and **Password** fields will be pre-populated.
   - The default update share is a UNC share `\\<ComputerName>\SophosUpdate`, where `<ComputerName>` is the name of the computer where the update manager is installed.
   - If the update source is a non-default update share on your network, enter credentials for the account that has read rights to the share. If the **Username** needs to be qualified to indicate the domain, use the form domain\username.
5. If necessary, in the **Username** and **Password** fields, enter the username and password for the account that will be used to access the update source.
   - If the update source is Sophos, enter the download credentials supplied by Sophos.
   - If the update source is the default update share created by an update manager located higher in the updating hierarchy, the **Username** and **Password** fields will be pre-populated.
6. If you access the update source via a proxy server, select **Use a proxy server to connect**. Then enter the proxy server **Address** and **Port** number. Enter a **Username** and **Password** that give
access to the proxy server. If the username needs to be qualified to indicate the domain, use the form `domain\username`. Click **OK**.

The new source appears in the list in the **Configure update manager** dialog box.

If you have already installed an update manager on a different computer, the share where that update manager downloads software and updates will appear on the list of addresses. You can select it as a source for the update manager you are configuring. Then you can move the address that you want to be the primary one to the top of the list, using the **Move up** and **Move down** buttons to the right of the list.

Related concepts
Managing roles and sub-estates (page 15)

### 7.1.4 Select which software to download

If you use role-based administration, you must have the **Policy setting - updating** right to configure an update manager.

You need to select the subscriptions that the update manager will keep up to date.

1. If you are in the **Endpoints** view, click the **Update managers** button on the toolbar to display the **Update managers** view.
2. In the list of update managers, select the update manager for which you want to select the software to download. Right-click and click **View/Edit configuration**.
3. In the **Configure update manager** dialog box, on the **Subscriptions** tab, select a software subscription in the list of available subscriptions.
   a) To view the details of the subscription, for example, what software is included in the subscription, click **View details**.
4. To move the selected subscription to the “Subscribed to” list, click the “Add” button.

   >

5. To move all subscriptions to the “Subscribed to” list, click the “Add all” button.

   >>

Copyright © Sophos Limited
7.1.5 Specify where the software is placed

If you use role-based administration, you must have the **Policy setting - updating** right to configure an update manager.

After you have selected which software to download, you can specify where it should be placed on the network. By default, the software is placed in a UNC share `\<ComputerName>\SophosUpdate`, where `ComputerName` is the name of the computer where the update manager is installed.

You can distribute downloaded software to additional shares on your network. To do this, add an existing network share to the list of available shares and then move it to the list of update shares as described below. Ensure that the Update Manager user account (`SophosUpdateMgr`) has read rights to the shares.

**Note**
You created the Update Manager user account before you installed Sophos Enterprise Console. For more information about the account, see Sophos Enterprise Console startup documentation.

To specify where the software is placed:
1. If you are in the Endpoints view, click the Update managers button on the toolbar to display the Update managers view.

2. In the list of update managers, select the update manager for which you want to select network shares for distributing the software. Right-click and click View/Edit configuration.

3. In the Configure update manager dialog box, on the Distribution tab, select a software subscription from the list.

4. Select a share from the “Available” shares list and move it to the “Update to” list by clicking the “Add” button (>).

   The default share \<ComputerName>\SophosUpdate is always present in the Update to list. You cannot remove this share from the list.

   The “Available” shares list includes all the shares that Sophos Enterprise Console knows about and that are not already being used by another update manager.

   - You can add an existing share to or remove a share from the “Available” shares list, using the “Add” button (>) or “Remove” button (<).

5. If you want to enter a description for a share or credentials needed to write to the share, select the share and click Configure. In the Share Manager dialog box, enter the description and credentials.

   If you want to enter the same credentials for multiple shares, select the shares in the “Update to” list and click Configure. In the Configure multiple shares dialog box, enter credentials that will be used to write to the shares.

Related concepts
Managing roles and sub-estates (page 15)

7.1.6 Create or edit an update schedule

If you use role-based administration, you must have the Policy setting - updating right to configure an update manager.

By default, an update manager checks the Sophos databank for threat detection data updates every 10 minutes.

You can change this update interval. The minimum is 5 minutes and the maximum 1440 minutes (24 hours). We recommend an update interval of 10 minutes for threat detection data, so that you receive protection from new threats promptly after the detection data is published by Sophos.

By default, an update manager checks the Sophos databank for software updates every 60 minutes.

You can change this update interval. The minimum is 10 minutes and the maximum 1440 minutes (24 hours).

For software updates, you can either specify an update interval that is used every hour of every day, or you can create more sophisticated schedules, in which each day can be specified independently and each day can be divided into periods with different update intervals.

You can create a different schedule for each day of the week. Only a single schedule can be associated with a day of the week.

1. If you are in the Endpoints view, click the Update managers button on the toolbar to display the Update managers view.

2. In the list of update managers, select the update manager for which you want to create an update schedule. Right-click and click View/Edit configuration.

3. In the Configure update manager dialog box, on the Schedule tab, enter the interval between threat detection data updates.

4. Enter the interval between software updates.
• If you want to specify an update interval that is used every hour of every day, select the **Check for updates every n minutes** option and enter the interval in minutes.

• If you want to create a more sophisticated schedule, or different schedules for different days of the week, select the **Set up and manage scheduled updates** option and click **Add**.

  In the **Update schedule** dialog box, enter a name for the schedule, select the days of the week, and update intervals.

**Related concepts**
**Managing roles and sub-estates** (page 15)

### 7.1.7 Configure the update manager log

If you use role-based administration, you must have the **Policy setting - updating** right to configure an update manager.

1. If you are in the **Endpoints** view, click the **Update managers** button on the toolbar to display the **Update managers** view.
2. In the list of update managers, select the update manager for which you want to configure the log. Right-click and click **View/Edit configuration**.
3. In the **Configure update manager** dialog box, on the **Logging** tab, select the number of days you want to keep the log for and the log’s maximum size.

**Related concepts**
**Managing roles and sub-estates** (page 15)

### 7.1.8 Configure the self-updating of an update manager

If you use role-based administration, you must have the **Policy setting - updating** right to configure an update manager.

1. If you are in the **Endpoints** view, click the **Update managers** button on the toolbar to display the **Update managers** view.
2. In the list of update managers, select the update manager for which you want to configure self-updating. Right-click and click **View/Edit configuration**.
3. In the **Configure update manager** dialog box, on the **Advanced** tab, select an update manager version you want to keep up to date with. For example, if you select “recommended”, the update manager will always be upgraded to the version that is labeled as such at Sophos. The actual update manager version will change.

**Related concepts**
**Managing roles and sub-estates** (page 15)

### 7.1.9 Make an update manager check for updates immediately

If you use role-based administration, you must have the **Remediation - updating and scanning** right to perform this task.

After you have configured an update manager, it checks for updates and downloads them from its update source to the update shares it maintains automatically, according to the specified schedule.
If you want an update manager to check for and download threat detection data updates, software updates for endpoint computers and software updates for the update manager itself immediately, follow these steps:

1. If you are in the **Endpoints** view, click the **Update managers** button on the toolbar to display the **Update managers** view.
2. In the list of update managers, select the update manager which you want to update. Right-click and click **Update Now**.

**Related concepts**

*Managing roles and sub-estates* (page 15)

### 7.1.10 Make an update manager comply with the configuration settings

If you use role-based administration, you must have the **Policy setting - updating** right to configure an update manager.

1. If you are in the **Endpoints** view, click the **Update managers** button on the toolbar to display the **Update managers** view.
2. In the list of update managers, select the update manager which you want to comply with the configuration settings. Right-click and click **Comply with Configuration**.

**Related concepts**

*Managing roles and sub-estates* (page 15)

### 7.1.11 Add an additional update manager

Sophos Update Manager (SUM) is always installed on the computer where you install Sophos Enterprise Console. If you selected **Custom Setup** during the installation, this is the computer where the management server is installed.

You can add one or more additional update managers to your network. You may want to do this to reduce the load on the update manager that is already installed and distribute updates more efficiently. You can install an additional update manager on a computer that does not yet have an update manager installed.

**Warning**

Do not remove the update manager installed on the same computer as the Sophos Enterprise Console management server. Sophos Enterprise Console cannot protect the network fully until this update manager is configured with an update source. This will enable Sophos Enterprise Console to receive necessary updates (for example, information about the versions of security software that endpoint computers should be running, new and updated Content Control Lists for data control, or the list of new controlled devices and applications).

To enable an additional update manager to download security software from Sophos or another update manager via HTTP, open TCP port 80 (outbound) on the computer on which you want to install the additional update manager. To enable the update manager to download security software from another update manager via a UNC path, open the following outbound ports on the computer: UDP port 137, UDP port 138, TCP port 139, and TCP port 445.
If the computer is running a version of Windows that includes the Network Discovery feature, and the feature is turned off, turn it on and restart the computer.

Log on with an account that has full administrative rights on the computer.

The update manager installer is located on the computer where Sophos Enterprise Console management server is installed, in the shared folder `\Servername\SUMInstallSet`. To view the location of the installer, go to the View menu and click Sophos Update Manager Installer Location.

You can install Sophos Update Manager using Windows Remote Desktop.

To install an additional update manager:

1. Run the Sophos Update Manager installer `Setup.exe`.
   An installation wizard is launched.
2. On the Welcome page of the wizard, click Next.
3. On the License Agreement page, read the license agreement and click I accept the terms in the license agreement if you agree to the terms. Click Next.
4. On the Destination folder page, accept the default or click Change and enter a new destination folder. Click Next.
5. On the Sophos Update Manager Account page, select an account that endpoint computers will use to access the default update share created by the update manager. (The default update share is `\ComputerName\SophosUpdate`, where `ComputerName` is the name of the computer where the update manager is installed.) This account must have read rights to the share and does not need to have administrative rights.
   You can select the default user, select an existing user, or create a new user.
   By default, the installer will create the SophosUpdateMgr account with read rights to the default update share and no interactive logon rights.
   If you want to add more update shares later, select an existing account or create a new account that has read rights to those shares. Otherwise, ensure that the SophosUpdateMgr account has read rights to the shares.
6. On the Sophos Update Manager Account Details page, depending on the option you selected on the previous page, enter a password for the default user, details for the new user, or select an existing account.
   The password for the account must comply with your password policy.
7. On the Ready to Install the Program page, click Install.
8. When installation is complete, click Finish.

The computer where you installed Sophos Update Manager should now appear in Sophos Enterprise Console, Update managers view. (On the View menu, click Update Managers.)

To configure the update manager, select it, right-click, and then click View/Edit Configuration.

**7.1.12 Publish security software on a web server**

You might want to publish Sophos security software on a web server for computers to access via HTTP.

To publish security software on a web server:

1. To find out the path of the shared folder to which the security software has been downloaded, known as the bootstrap location:
   a) In Sophos Enterprise Console, on the View menu, click Bootstrap Locations.
In the **Bootstrap Locations** dialog box, the **Location** column displays the bootstrap location for each platform.

b) Make a note of the path up to but not including the **CIDs** folder. For example: \server name\SophosUpdate

2. Make the bootstrap location, including subfolders, available on the web server. For instructions, see knowledge base article 38238.

**Related information**
knowledge base article 38238

### 7.2 Configuring software subscriptions

A software subscription specifies which versions of endpoint software are downloaded from Sophos for each platform.

The **Download Security Software Wizard** sets up a default subscription called “Recommended.” This subscription includes the recommended versions of any selected software.

If you want to add software to your subscription or subscribe to a version other than the recommended one, configure the subscription.

If you haven't completed the wizard after you installed Sophos Enterprise Console, do this now.

**Related tasks**
Subscribe to security software (page 72)
Run the Download Security Software Wizard (page 73)

### 7.2.1 What types of updating are available?

For each platform (for example, Windows), there are several software packages representing different types of updating and containing different versions of endpoint software. You can choose which software package to download from Sophos for further deployment to endpoint computers by selecting one of the following updating types in the subscription.

<table>
<thead>
<tr>
<th>Updating type</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Recommended** | This is the default package. If you use this package, Sophos updates your software regularly (usually every month) with:  
  • Fixes for issues discovered by customers.  
  • New features that are ready for general availability.  
  If you install Sophos Enterprise Console for the first time and accept the default settings, this is the version that you will be on. |

Copyright © Sophos Limited
### Updating type | Description
--- | ---
**Preview** | This package is aimed at IT and security administrators. If you use this version, you receive new features before they are released in the Recommended version. This means that you can test and evaluate them, perhaps on a test network, before they become generally available. Sometimes the Preview package gives you the same software as Recommended. This happens when no new features are ready to be tested in customer environments.

**Extended** | The Extended version is aimed at customers who have a strict or conservative process for installing updated software on their network. If you use this version, you receive the same updates as the Recommended channel but with a delay of several months. This means that any issues in the product have been identified and fixed long before it is installed on your network.

**Previous ** | The previous version of the currently recommended package. This version can be useful for you if you want a little longer to test new software before you roll it out to your network.

**Previous Extended** | The previous version of the current extended package. This version can be useful for you if you want a little longer to test new software before you roll it out to your network.

### Fixed versions

**Note**
We may change the packages over time. For more information about currently available software packages, see knowledge base article 119216.

The **Download Security Software Wizard** sets up a subscription that specifies the recommended versions of any selected software.

The actual versions downloaded will usually change each month. To check what actual software versions are downloaded, in the **Software Subscription** dialog box, select the package you want to check and click **Details**.

**Related concepts**
**Fixed version software packages** (page 71)
A fixed version is a version that is updated with new threat detection data, but not with the latest software version each month.

**Related information**
knowledge base article 119216
7.2.2 Fixed version software packages

A fixed version is a version that is updated with new threat detection data, but not with the latest software version each month.

An example of a fixed version of Sophos Endpoint Security and Control for Windows is "10.3.15 VE3.60.0". It consists of a three-part version identifier: major release identifier (10), minor release identifier (3), and maintenance release identifier (15) and threat detection engine version (VE3.60.0).

Using fixed packages

By default, the use of fixed version software packages is disabled (under Tools > Configure Use of Fixed Packages). They are not displayed in the Software Subscription dialog box and you cannot subscribe to them.

Tip
If you are subscribed to a fixed software version, we recommend that, to ensure best protection, you change your subscription to a "recommended" package.

If you haven’t used fixed version software packages before but want to do so, you can enable the use of fixed packages under Tools > Configure Use of Fixed Packages. When the use of fixed packages is enabled, they are displayed in the Software Subscription dialog box and you can subscribe to them.

Note
If you use role-based administration, you must have the System configuration right to configure the use of fixed packages.

If you disable the use of fixed packages while you are still subscribed to a fixed package, you will still be subscribed to that package and it will continue to be downloaded until you unsubscribe from it. However, you won’t be able to view or re-subscribe to another fixed package.

If you have remote consoles, changing this configuration option in one of them will take effect in all consoles.

Lifecycle of fixed packages

Fixed versions are downloaded for as long as they are available from Sophos. If a fixed version is due to retire, you will see an alert in the Update managers view next to any update managers that are subscribed to that version. If email alerting is active, the administrator will also receive an email alert.

When a subscribed fixed version is retired, if you do not change your subscription before support ends you are automatically subscribed to a newer Fixed Extended package. For more information see knowledge base article 121139.

For more information about Sophos Endpoint Lifecycle Policy, see knowledge base article 112580.

Related reference
What types of updating are available? (page 69)
7.2.3 Subscribe to security software

If you use role-based administration:

- You must have the **Policy setting - updating** right to edit a software subscription.
- You cannot edit a subscription if it is applied to an updating policy that is applied outside your active sub-estate.

To subscribe to security software:

1. On the **View** menu, click **Update Managers**.
2. In the **Software Subscriptions** pane, double-click the subscription you want to change, or click the **Add** button at the top of the pane to create a new subscription.

   The **Software Subscription** dialog box appears.

   Alternatively, if you want to create a copy of an existing subscription, select the subscription, right-click and click **Duplicate Subscription**. Type a new name for the subscription and then double-click it to open the **Software Subscription** dialog box.

3. In the **Software Subscription** dialog box, edit the name of the subscription, if you wish.
4. Select the platforms for which you want to download the software.
5. By default, you are subscribed to a "Recommended" package. You can also select a non-default package (for example, if you want to preview new features). To do so, click in the **Version** field next to the platform you want to change the package for and then click again. In the drop-down list of available versions, select the version you want to download (for example, "Preview").

After you have subscribed to the security software, you can set up subscription email alerts.

If you created a new software subscription, configure the update manager to maintain it.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Set up software subscription alerts (page 188)
Sophos Enterprise Console displays alerts raised by the update manager in the Alerts column in the Update managers view.

View or edit update manager configuration (page 61)

Related reference
What types of updating are available? (page 69)

7.2.4 Run the Download Security Software Wizard

If you use role-based administration, you must have the Policy setting - updating right to run the Download Security Software Wizard.

If you haven't completed the Download Security Software Wizard after you installed Sophos Enterprise Console, do the following:

On the Actions menu, click Run the Download Security Software Wizard.

The Download Security Software Wizard guides you through selecting and downloading software.

Note
After you have successfully completed the wizard, the Run the Download Security Software Wizard option will disappear from the Actions menu.

Related concepts
Managing roles and sub-estates (page 15)

7.2.5 See which updating policies use the software subscription

To see which updating polices use a particular software subscription:

Select the subscription, right-click and then click View Subscription Usage.

In the Software Subscription Usage dialog box, you see a list of updating polices that use the subscription.

7.3 Configuring the updating policy

Updating policies enable you to keep your computers up to date with your chosen security software. Sophos Enterprise Console checks for updates and updates computers, if necessary, at a specified interval.

The default updating policy enables you to install and update the software specified in the “Recommended” subscription.

If you want to change the default updating policy or create a new updating policy:

• Select a subscription.
• Configure update servers.
• Schedule updates.
• Select a different source for initial installation.
• Log updates.
If you use role-based administration:

- You must have the **Policy setting - updating** right to configure an updating policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

**Related concepts**
- Configure update servers (page 75)
- Managing roles and sub-estates (page 15)

**Related tasks**
- Select a subscription (page 74)
- Schedule updates (page 80)
- Select a different source for initial installation (page 81)
- Log updates (page 81)

### 7.3.1 Select a subscription

If you use role-based administration:

- You must have the **Policy setting - updating** right to configure an updating policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

A subscription specifies which versions of endpoint software are downloaded from Sophos for each platform. The default subscription includes the latest software for Windows.

To select a subscription:

1. Check which updating policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Updating**. Then double-click the policy you want to change.
3. In the **Updating policy** dialog box, click the **Subscription** tab and select the subscription for the software you want to keep up to date.
7.3.2 Configure update servers

By default, computers update from a single primary source UNC share, \ComputerName\SophosUpdate, where ComputerName is the name of the Update Manager’s computer. You can also specify an alternative secondary source for updates, enable location roaming, and enable bandwidth throttling.

If endpoint computers cannot contact their primary source, they attempt to update from their secondary source (if one has been specified). We recommend that you always specify a secondary source.

Both primary and secondary update server locations may be either UNC shares or HTTPS URLs from any accessible Update Manager on your network. The secondary update server location may alternatively be set to get updates directly from Sophos over the internet via HTTPS.
7.3.3 Primary server

The primary server is set up automatically with the default primary server location. By default, computers update from a single primary source UNC share, `\\<ComputerName>\SophosUpdate`, where `<ComputerName>` is the name of the computer where Sophos Update Manager is installed.

To access the share, the computers use the Sophos Update Manager credentials that you entered during the installation of Sophos Enterprise Console. If you followed recommendations in the Sophos Enterprise Console startup guide, the account is named “SophosUpdateMgr”.

If you access the update source via a proxy server, click Proxy details and enter the proxy server details.

You can also enable bandwidth throttling to limit the amount of bandwidth the computers can use when updating. On the Primary Server tab in the updating policy, click the Advanced button. In the Advanced Settings dialog box, select the Limit amount of bandwidth used check box, and then use the slider control to specify the maximum bandwidth in Kbits/second.

Related concepts
Location roaming for laptops (page 76)

Related tasks
Change primary server credentials (page 78)

7.3.4 Location roaming for laptops

Some laptop users may roam extensively or internationally within an organization. When location roaming is enabled (on an updating policy for roaming laptops), roaming laptops attempt to locate and update from the nearest update server location by querying other (fixed) endpoints on the local network they are connected to, minimizing update delays and bandwidth costs.

A roaming laptop gets update server locations and credentials by querying fixed computers on the same local network. If multiple locations are returned, the laptop determines which is nearest and uses that. If none work, the laptop uses the primary (then secondary) locations defined in its updating policy.

Note
When fixed computers send update locations and credentials to the laptop, passwords are obscured both in transmission and storage. However, accounts set up for endpoints to read update server locations should always be as restrictive as possible, allowing only read-only access.

Location roaming is only usable where:

• There is a single common Sophos Enterprise Console for both roaming and fixed endpoints.
• The fixed endpoints use the same software subscription as the roaming laptops.
• There is a primary update location specified in the updating policy used by the roaming laptops.
• Any third-party firewalls are configured to allow update location queries and responses. The port used is normally UDP port 51235 but is configurable; for details see knowledge base article 110371.

You enable location roaming as part of specifying sources for updates. Location roaming should only be enabled on groups of machines that frequently move from office to office.

For frequently asked questions about location roaming, see knowledge base article 112830.

**Related concepts**

*How does location roaming work?* (page 77)

**Related tasks**

*Specify where the software is placed* (page 64)

*Change primary server credentials* (page 78)

**Related information**

knowledge base article 110371

knowledge base article 112830

### 7.3.5 How does location roaming work?

Location roaming is a method of intelligent updating for roaming laptops where updates are performed from a "best" update location and updating does not rely solely on the primary and secondary update locations specified in the laptops’ updating policy.

When location roaming is enabled, the following happens:

1. When a laptop changes its location, the Sophos AutoUpdate component of Sophos Endpoint Security and Control installed on the laptop determines that the MAC address of the default gateway on the connected network has changed since the last update. It then sends an ICMP broadcast over the local subnet to neighboring AutoUpdate installations, using UDP port 51235 by default.

2. The neighboring AutoUpdate installations reply with their updating policy, using the same port. Only the primary update location is sent in the response.

   All Sophos Endpoint Security and Control installations listen for broadcasts regardless of whether location roaming is enabled or not.

   Sensitive information in replies is obfuscated and fields are hashed for integrity.

   Reply messages have a randomized reply time, to avoid message storms. The replies are also ICMP broadcasts, so any other machine that would have replied with the same details will also receive the broadcast and know not to respond.

3. AutoUpdate chooses the "best" location from the locations received and checks whether the sender is managed by the same Sophos Enterprise Console and the subscription ID matches the one used by AutoUpdate on the laptop.

   The "best" update location is determined based on the amount of hops required to access the update location.

4. An update is then attempted and, if successful, the location is cached.

   A maximum of four accessible update locations with the same subscription ID and the lowest hop count are stored on the laptop (in the file `iustatus.xml` in the following location: C:\Program Files\Sophos\AutoUpdate\data\status\iustatus.xml).

   These update locations are checked every time AutoUpdate performs an update.
7.3.6 Enable location roaming

If you use role-based administration:

- You must have the **Policy setting - updating** right to configure an updating policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

You should only enable location roaming on groups of machines that frequently move from office to office.

To enable location roaming:

1. In the **Policies** pane, double-click **Updating**. Then double-click the updating policy you want to change.
2. In the **Updating Policy** dialog box, on the **Primary Server** tab, select the **Allow location roaming** check box.
3. In the **Groups** pane, select a group that uses the updating policy you just changed. Right-click and select **Comply with, Group updating policy**.
   - Repeat this step for each group that uses this updating policy.

**Note**

If you later need to revert back to using the primary and secondary update locations specified in the updating policy, disable location roaming.

**Related concepts**

Managing roles and sub-estates (page 15)

7.4 Change primary server credentials

If you use role-based administration:

- You must have the **Policy setting - updating** right to configure an updating policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To change the primary server credentials:

1. In the **Policies** pane, double-click **Updating**. Then double-click the updating policy you want to change.
2. In the **Updating Policy** dialog box, on the **Primary Server** tab, enter new credentials that will be used to access the server. Change other details, if appropriate.
Note
If your primary update source is a folder on your website and you are using Internet Information Services (IIS) with anonymous authentication, you will still need to enter credentials on the Primary Server tab. Use the credentials for the "initial install source" UNC share, even if you don’t need them to access the webserver. If you leave the Username and Password fields on the Primary Server tab blank, you will not be able to protect endpoint computers from the console.

3. In the Groups pane, select a group that uses the updating policy you just changed. Right-click and select Comply with > Group updating policy.
   a) Repeat this step for each group that uses this updating policy.

Related concepts
Managing roles and sub-estates (page 15)

7.4.1 Set the secondary update server

If you use role-based administration:

- You must have the Policy setting - updating right to configure an updating policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To set the secondary update server location:
1. Check which updating policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Updating, then double-click the policy you want to change.
3. In the Updating Policy dialog box, click the Secondary Server tab, and then select the Specify secondary server details check box.
4. In the Address (HTTP or UNC) box, do one of the following:
   - Enter the HTTP URL or UNC network path of the update server share.
   - Select Sophos.

Note
If you choose an HTTPS URL or a share that is not maintained by a managed Update Manager, Sophos Enterprise Console cannot check that the specified software subscription is available. You must manually ensure that the share contains the specified software subscription, otherwise computers will not be updated.

5. If the policy includes Mac endpoints and you specified a UNC path in the Address field, under Select a file-sharing protocol for Mac OS X, select a protocol for Macs to access the update share.
6. If necessary, in the Username field, enter the username for the account that will be used to access the server, and then enter and confirm the password. For Sophos HTTPS, this is your subscription credentials.
   This account should have only read-only (browsing) access rights to the share you entered in the address field above.
7. To throttle bandwidth, click Advanced. In the Advanced settings dialog box, select the Limit amount of bandwidth used check box, and then use the slider control to specify the maximum bandwidth in Kbits/second.

8. If you access the update source via a proxy server, click Proxy details. In the Proxy details dialog box, select the Access the server via a proxy check box, and then enter the proxy server Address and Port number. Enter a Username and Password that give access to the proxy server. If the username needs to be qualified to indicate the domain, use the form domain \username.

Note
Some internet service providers require HTTPS requests to be sent to a proxy server.

9. Click OK to close the Updating Policy dialog box.

10. In the Groups pane, right-click a group that uses the updating policy you just changed, and then click Comply with > Group Updating Policy.

Repeat this step for each group that uses this updating policy.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

7.5 Schedule updates

If you use role-based administration:

- You must have the Policy setting - updating right to configure an updating policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

By default, endpoint computers check for updates in the network share every 5 minutes.

Warning
If the computers download updates directly from Sophos, this update interval does not apply. Computers running PureMessage can check for updates every 15 minutes. Computers that are not running PureMessage will update every 60 minutes.

To specify the update interval:

1. Check which updating policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Updating. Then double-click the policy you want to change.
3. In the Updating policy dialog box, on the Schedule tab, leave Enable networked computers to use Sophos updates automatically selected. Enter the interval between software updates (in minutes).
4. If the computers update via a dial-up connection to the internet, select Check for updates on dial-up.
Computers will then attempt to update whenever they connect to the internet.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

7.5.1 Select a different source for initial installation

If you use role-based administration:

- You must have the Policy setting - updating right to configure an updating policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

By default, security software is installed on computers and then kept updated from the source specified on the Primary server tab. You can specify a different source for initial installation.

Warning
This setting applies only to Windows.

If your primary server is an HTTPS (web) address, and you want to perform installation on the computers from the console, you must specify a first-time install source.

To make the initial installation from a different source:

1. Check which updating policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Updating. Then double-click the policy you want to change.
3. In the Updating policy dialog box, on the Initial install source tab, clear the Use primary server address check box. Then enter the address of the source you want to use.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

7.5.2 Log updates

If you use role-based administration:

- You must have the Policy setting - updating right to configure an updating policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

By default, computers log their updating activity. The default maximum log size is 1 MB. The default log level is normal.

To change the logging settings:

1. Check which updating policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Updating. Then double-click the policy you want to change.
3. In the Updating policy dialog box, on the Logging tab, leave Log Sophos AutoUpdate activity selected. In the Maximum log size field, specify a maximum size for the log in MB.
4. In the Log level field, select Normal or Verbose logging.
Verbose logging provides information on many more activities than usual, so the log will grow faster. Use this setting only when detailed logging is needed for troubleshooting.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

## 7.6 Monitoring the update manager

### Check the update manager status on the Dashboard

The status of the update managers is displayed in the **Updates** panel on the **Dashboard**. This will tell you when the last update was downloaded from Sophos and display a warning if the time since the last update exceeds the warning or critical threshold.

**Note**
The **Updates** section of the dashboard does not report an alert or error if an update manager is temporarily unable to update. Alerts and errors are only generated if the time since the last update of the update manager exceeds the warning or critical threshold.

### Check the update manager alerts and errors

Update manager alerts and errors are displayed in the **Update managers** view, **Alerts** and **Errors** columns, respectively.

If you subscribed to a fixed version of software, an alert will be displayed when that version is nearing retirement or is retired. An alert will also be displayed if your product license has changed.

To view update manager alerts and errors:

1. If you are in the **Endpoints** view, click the **Update managers** button on the toolbar to display the **Update managers** view.
2. In the list of update managers, look in the **Alerts** and **Errors** columns for any possible problems.
3. If there is an alert or error displayed next to an update manager, right-click that update manager and click **View Update Manager Details**.

   In the **Update manager details** dialog box, you can see the time of the last threat detection data and software updates, status of the subscription or subscriptions that the update manager keeps up to date, and update manager status.

4. To learn more about a specific update manager status and for information on how to resolve it, follow the link in the **Description** column.

   If you need to check or change your subscription, for example, if the product you are subscribed to is nearing retirement, or your product license has changed and the new license does not include that product, see **Subscribe to security software**.

   If new features become available as a result of a license change, you may need to configure new policies before you can use the features.
Subscribe to email alerts

You can set up email alerts to be sent to your chosen recipients when the product version you are subscribed to is nearing retirement or is retired, or when your Sophos product features change as a result of a license change, see Set up software subscription alerts.

Related tasks
Configure the Dashboard (page 53)
Subscribe to security software (page 72)
Set up software subscription alerts (page 188)

Sophos Enterprise Console displays alerts raised by the update manager in the Alerts column in the Update managers view.

7.6.1 Clear update manager alerts from the console

If you use role-based administration, you must have the Remediation - cleanup right to clear alerts from the console.

To clear update manager alerts from the console:

1. In the Update managers view, select the update managers for which you want to clear alerts. Right-click and select Acknowledge Alerts.
   The Update manager alerts dialog box is displayed.
2. To clear alerts from the console, select the alerts you want to clear and click Acknowledge.
   Acknowledged (cleared) alerts are no longer displayed in the console.

Related concepts
Managing roles and sub-estates (page 15)

7.7 Update out-of-date computers

If you use role-based administration, you must have the Remediation - updating and scanning right to update computers.

After you have set up the updating policies and applied them to your networked computers, the computers are kept up to date automatically. You do not need to update computers manually unless there is a problem with updating.

If in the Endpoints view, in the computer list, you see a clock icon next to a computer in the Up to date column on the Status tab, the computer has out-of-date security software. The text indicates how long the computer has been out of date.

A computer can be out of date for one of two reasons:

- That computer has failed to fetch an update from the server.
- The server itself does not have the latest Sophos software.

To diagnose the problem and update the computers:

1. In the Endpoints view, select the group that contains out-of-date computers.
2. On the Status tab, click the Up to date column heading to sort computers by how up to date they are.
3. Click the **Update details** tab and look in the **Primary server** column. This shows you the directory that each computer updates from.

4. Now look at the computers that update from one specific directory.
   - If some are out of date, but others are not, the problem is with individual computers. Select them, right-click and click **Update Computers Now**.
   - If all are out of date, the problem could be with the directory. On the **View** menu, click **Update Managers**. Select the update manager that maintains the directory that you suspect to be out of date, right-click and click **Update Now**. Then on the **View** menu, click **Endpoints**. Select the out-of-date computers, right-click and click **Update Computers Now**.

If you have several update managers and are not sure which one maintains the out-of-date directory, use the Updating Hierarchy report to see which shares are maintained by each update manager. To view the Updating Hierarchy report, on the **Tools** menu, click **Manage Reports**. In the **Report Manager** dialog box, select **Updating hierarchy** and click **Run**. Look in the “Shares managed by update managers” section of the report.

**Related concepts**

- Managing roles and sub-estates (page 15)
8 Configuring policies

8.1 Anti-virus and HIPS policy

An anti-virus and HIPS policy enables you to do the following:

- Detect known and unknown viruses, Trojans, worms, and spyware automatically as soon as users attempt to copy, move, or open files that contain them.
- Scan for adware and other potentially unwanted applications.
- Scan computers for suspicious files and rootkits.
- Detect malicious network traffic, that is, communications between endpoint computers and command and control servers involved in botnet or other malware attacks.
- Automatically clean up computers as soon as a virus or other threat is found.
- Analyze the behavior of the programs running on the system.
- Scan computers at set times.

You can use different scanning settings for each group of computers.

Note
Sophos Labs can independently control which files are scanned. They may add or remove scanning of certain file types in order to provide the best protection.

For information about scanning and cleanup options that do not take effect on Mac, Linux or UNIX, see Settings not applicable on Mac, Linux or UNIX.

Related concepts
Behavior monitoring (page 100)
Settings not applicable on Mac, Linux or UNIX (page 85)

Related tasks
Set up automatic cleanup for on-access scanning (page 89)
Create a scheduled scan (page 93)
Configure on-access scanning (page 87)
Configure scanning settings for a scheduled scan (page 94)

8.1.1 Settings not applicable on Mac, Linux or UNIX

While all types of scan and cleanup on Windows computers can be fully managed from Sophos Enterprise Console, there are a number of settings that do not take effect on Mac, Linux or UNIX computers.

Mac OS X

For information about anti-virus and HIPS policy settings that apply to Macs, see knowledge base article 118859.
Linux

The following automatic cleanup options do not apply to Linux computers and will be ignored by them.

Automatic cleanup options for on-access scanning:
- Deny access and move to default location
- Deny access and move to

Automatic cleanup options for scheduled scanning:
- Move to default location
- Move to

For more information about anti-virus and HIPS policy settings that apply to Linux computers, see knowledge base article 117344.

UNIX

Sophos Enterprise Console cannot perform on-access scans on UNIX computers.

You can configure scheduled scans, alerting, logging, and updating centrally from Sophos Enterprise Console.

Note
These features also include some parameters that cannot be set using Sophos Enterprise Console. You can set these parameters from the Sophos Anti-Virus command-line interface on each UNIX computer locally. Sophos Enterprise Console ignores them.

You can also configure on-demand scans from the Sophos Anti-Virus command-line interface on each UNIX computer locally.

For more information about setting additional parameters or configuring Sophos Anti-Virus for UNIX locally, see the Sophos Anti-Virus for UNIX configuration guide.

The following automatic cleanup options for scheduled scanning do not apply to UNIX computers and will be ignored by them.
- Move to default location
- Move to

For more information about anti-virus and HIPS policy settings that apply to UNIX computers, see knowledge base article 117344.
8.2 On-access scanning

8.2.1 About on-access scanning best protection

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 knowledge base article 114345.

We recommend that you refer to the Sophos Enterprise Console policy setup guide for advice on best practices for using and managing Sophos security software.

Related information
knowledge base article 114345
Sophos documentation

8.2.2 Configure on-access scanning

If you use role-based administration:

- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

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 knowledge base article 12790.

To configure on-access scanning:

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. In the On-access scanning panel, beside Enable on-access scanning, click Configure.
5. 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>
</table>
| Read       | • Scan files when they are copied, moved, or opened.  
            | • Scan programs when they are started.              |
| Rename     | Scan files when they are renamed.                 |
### Option | Description
--- | ---
**Write** | Scan files when they are saved or created.

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Adware and PUAs**     | • 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.                                      |
| **Suspicious files**    | Suspicious files display certain characteristics (for example, dynamic decompression code) that are commonly, but not exclusively, found in malware. However, these characteristics are not sufficiently strong for the file to be identified as a new piece of malware. \  
                           This option applies only to Sophos Endpoint Security and Control for Windows.                                                                 |

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Allow access to drives with infected boot sectors** | 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.                                                                                     |
| **Scan inside archive files**                    | Scan the contents of archives or compressed files before they are downloaded or emailed from managed computers.  
                                                   We recommend that you leave this option turned off, as it makes scanning significantly slower.                                                   
                                                   Users 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 users 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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan system memory</strong></td>
<td>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>
</tbody>
</table>

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

**Related information**
- knowledge base article 12790

### 8.2.3 Turn on-access scanning on or off

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

By default, Sophos Endpoint Security and Control scans files as the user attempts to access them, and denies access unless the file is clean.

You may decide to turn off on-access scanning on Exchange servers or other servers where performance might be affected. In this case, put the servers in a special group and change the anti-virus and HIPS policy used for that group as shown below.

**To turn on-access scanning on or off:**

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**. Then double-click the policy you want to change.
   - The **Anti-Virus and HIPS policy** dialog box is displayed.
3. In the **On-access scanning** panel, select or clear the **Enable on-access scanning** check box.

If you turn off on-access scanning on a server, we recommend that you set up scheduled scans on the relevant computers.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)
- Create a scheduled scan (page 93)

### 8.2.4 Set up automatic cleanup for on-access scanning

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.
By default, Sophos Endpoint Security and Control automatically cleans up computers as soon as a virus or other threat is found. You can change the settings for automatic cleanup as described below.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. In the On-access scanning panel, beside Enable on-access scanning, click Configure.
5. In the On-access scan settings dialog box, click the Cleanup tab.
6. Set automatic scanning options.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

**Related reference**
- Automatic cleanup settings for on-access scanning (page 90)

### 8.2.5 Automatic cleanup settings for on-access scanning

**Viruses/spyware**

Select or clear the *Automatically clean up items that contain a virus/spyware* check box.

You can also specify what should be done with the items if cleanup fails:

- *Deny access only*
- *Delete*
- *Deny access and move to default location*
- *Deny access and move to (enter a full UNC path)*

**Note**

The *Deny access and move to default location* and *Deny access and move to* settings do not apply to Linux or UNIX computers and will be ignored by them.

**Suspicious files**

**Warning**

These settings apply only to Windows computers.

You can specify what should be done with suspicious files when they are detected:

- *Deny access only*
- *Delete*
- *Deny access and move to default location*
- *Deny access and move to (enter a full UNC path)*
8.2.6 Specify on-access scanning file extensions

If you use role-based administration:

- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

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

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. In the On-access scanning panel, beside Enable on-access scanning, click Configure.
5. Click the Extensions tab, and then configure the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan all files</td>
<td>Scan all files regardless of the filename extension. If you turn on this option, the other options on the Extensions tab are turned off. Scanning all files will affect computer performance, so we recommend that you only turn on this option as part of a weekly scheduled scan.</td>
</tr>
<tr>
<td>Scan only executable and other vulnerable files</td>
<td>• Check all files with executable file extensions (for example, .exe, .bat, .pif) or files that have the possibility of being infected (for example, .doc, .chm, .pdf). • Quickly check the structure of all files, and then scan them if their format is that of an executable file.</td>
</tr>
<tr>
<td>Additional file type extensions to be scanned</td>
<td>To scan additional file types, click Add, and then type a file extension such as PDF in the Extension box. You can use the wildcard ? to match any single character. To stop scanning a file type, select its extension in the list, and then click Remove. To change a file type, select its extension in the list, and then click Edit.</td>
</tr>
<tr>
<td>Scan files with no extension</td>
<td>Files with no extension could be malware, so we recommend that you leave this option turned on.</td>
</tr>
<tr>
<td>Exclude</td>
<td>To exclude specific file types from on-access scanning, click Add, and then type a file extension such as PDF in the Extension box.</td>
</tr>
</tbody>
</table>
### 8.2.7 Exclude items from on-access scanning

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can exclude items from on-access scanning.

**Warning**

These options apply only to Windows, Mac OS X, and Linux.

Sophos Enterprise Console cannot perform on-access scans on UNIX computers.

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**. Then double-click the policy you want to change.

   The **Anti-virus and HIPS Policy** dialog box is displayed.
3. In the **On-access scanning** panel, click the **Configure** button.
4. Click the tab for **Windows Exclusions**, **Mac Exclusions**, or **Linux/UNIX Exclusions**. To add items to the list, click **Add** and enter the full path in the **Exclude Item** dialog box.

   The items you can exclude from scanning differ on each type of computer.

   - To exclude files that are not stored on local drives, select the **Exclude remote files** check box. You might select this if you want to increase speed of access to such files and you trust the available remote file locations.

   If you select **Exclude remote files** on the **Windows Exclusions** tab, data control will not scan files uploaded or attached from a network location using a monitored application, for example, an email client, a web browser, or an instant messaging (IM) client. This is because data control uses the same set of exclusions as the Sophos Anti-Virus on-access scanner (InterCheck™). If remote file scanning is disabled, it will not send any remote files for a data control check. This restriction does not apply to storage device monitoring.

   You can export the list of Windows exclusions to a file and then import it into another policy.

**Related concepts**

Managing roles and sub-estates (page 15)
8.2.8 Import or export on-access scanning exclusions

If you use role-based administration:

• You must have the Policy setting - anti-virus and HIPS right to perform this task.
• You cannot edit a policy if it is applied outside your active sub-estate.

You can export the list of Windows exclusions for on-access scanning to a file, and then import it into another policy.

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. In the On-access scanning panel, beside Enable on-access scanning, click Configure.
5. On the Windows Exclusions tab, click either Export or Import.

8.3 On-demand and scheduled scanning

In the On-demand scanning panel of the Anti-virus and HIPS policy, you can:

• Set up scheduled scans.
• Configure scanning options such as extensions and exclusions for all types of on-demand scan-scheduled scans, the full system scan, and default on-demand scans on individual computers.

8.3.1 Create a scheduled scan

If you use role-based administration:

• You must have the Policy setting - anti-virus and HIPS right to perform this task.
• You cannot edit a policy if it is applied outside your active sub-estate.

To have computers scanned by Sophos Endpoint Security and Control at set times, you can create a scheduled scan.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. In the On-demand scanning panel, under Set up and manage scheduled scans, click Add. The Scheduled scan settings dialog box is displayed.

5. In the Scan name box, type a name for the scan.

6. Under What to scan, select the check boxes for items to scan. By default, all local hard disks and UNIX mounted filesystems are scanned.

7. Under When scan occurs, select the check boxes for the day(s) on which the scan should run.

8. To specify the time(s) when the scan will run, click Add.
   • To change a time, select it in the Times when the scan will run list, and then click Edit.
   • To delete a time, select it in the Times when the scan will run list, and then click Remove.

Note
If the scan detects components of a threat in memory, and you have not set up automatic cleanup for the scan, the scan stops and an alert is sent to Sophos Enterprise Console. This is because further scanning could enable the threat to spread. You must clean up the threat before running the scan again.

Related concepts
Managing roles and sub-estates (page 15)
Related tasks
Check which policies a group uses (page 27)
Configure scanning settings for a scheduled scan (page 94)
Set up automatic cleanup for on-access scanning (page 89)

8.3.2 Configure scanning settings for a scheduled scan

If you use role-based administration:
• You must have the Policy setting - anti-virus and HIPS right to perform this task.
• You cannot edit a policy if it is applied outside your active sub-estate.

To configure the scanning settings for a scheduled scan:
1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. In the Set up and manage scheduled scans list, select the scan, and then click Edit.
5. In the Scheduled scan settings dialog box, click Configure.
6. Under Scan files for, configure the settings 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>
<tr>
<td></td>
<td>• PUAs (Potentially Unwanted Applications) are not malicious, but are generally considered unsuitable for business networks.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Suspicous files</td>
<td>Suspicious files display certain characteristics (for example, dynamic decompression code) that are commonly, but not exclusively, found in malware. However, these characteristics are not sufficiently strong for the file to be identified as a new piece of malware.</td>
</tr>
</tbody>
</table>
|                     | **Warning**  
|                     | This setting applies only to Sophos Endpoint Security and Control for Windows.                                                               |
| Rootkits            | A rootkit is 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. |

7. 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 inside archive files</td>
<td>Scan the contents of archives and other compressed files.</td>
</tr>
<tr>
<td></td>
<td>We don't recommend that you scan inside archive files during a scheduled scan, as it will add a significant amount of time to the scan. We recommend instead that you use on-access scanning (on-read and on-write) to protect your network. Any malware components of an unpacked archive will be blocked by the on-read and on-write scanners when they are accessed.</td>
</tr>
<tr>
<td></td>
<td>If you would like to scan all archives on a few computers using a scheduled scan, we recommend that you do the following:</td>
</tr>
<tr>
<td></td>
<td>• Create an extra scheduled scan.</td>
</tr>
<tr>
<td></td>
<td>• In the <strong>Configure &gt; On-demand scan settings</strong> dialog box, on the <strong>Extensions</strong> tab, add only the archive extensions to the list of extensions to be scanned.</td>
</tr>
<tr>
<td></td>
<td>• Make sure that <strong>Scan all files</strong> is disabled.</td>
</tr>
<tr>
<td></td>
<td>This will allow you to scan the archive files whilst making the scan as short as possible.</td>
</tr>
<tr>
<td>Scan system memory</td>
<td>Detect malware hiding in the computer's system memory (the memory that is used by the operating system).</td>
</tr>
</tbody>
</table>

Copyright © Sophos Limited
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run scan at lower priority</td>
<td>On Windows Vista and above, run the scheduled scan with lower priority so that it has minimal impact on user applications.</td>
</tr>
</tbody>
</table>

For detailed advice about adjusting the default scanning settings for a scheduled scan, see knowledge base article 63985.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

**Related information**
- knowledge base article 63985

### 8.3.3 Set up automatic cleanup for scheduled scanning

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

By default, Sophos Endpoint Security and Control automatically cleans up computers as soon as a virus or other threat is found. You can change the settings for automatic cleanup as described below.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**.
3. Double-click the policy you want to change.
   - The **Anti-Virus and HIPS Policy** dialog box is displayed.
4. In the **Set up and manage scheduled scans** list, select the scan, and then click **Edit**.
5. Beside **Change scanning and cleanup settings**, click **Configure**.
   - The **Scanning and cleanup settings** dialog box is displayed.
6. Click the **Cleanup** tab.
7. Set the automatic cleanup settings.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

**Related reference**
- Automatic cleanup settings for on-access scanning (page 90)

### 8.3.4 Automatic cleanup settings for scheduled scanning

**Viruses/spyware**

Select or clear the **Automatically clean up items that contain a virus/spyware** check box.
You can also specify what should be done with the items if cleanup fails:

- Log only
- Delete
- Move to default location
- Move to (enter a full UNC path)

Notes
- Moving an executable file reduces the likelihood of it being run.
- You cannot automatically move a multi-component infection.

Adware and PUA

Select Automatically clean up adware and PUA.

Note
This setting applies only to Windows computers.

Suspicious files

You can specify what should be done with suspicious files when they are detected:

- Log only
- Delete
- Move to default location
- Move to (enter a full UNC path)

Notes
- These settings apply only to Windows computers.
- Moving an executable file reduces the likelihood of it being run.
- You cannot automatically move a multi-component infection.

8.3.5 Specify file extensions for on-demand and scheduled scanning

If you use role-based administration:

- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can specify which file extensions are scanned during on-demand and scheduled scanning.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change. The Anti-Virus and HIPS Policy dialog box is displayed.
4. In the On-demand scanning panel, click Configure.
The **On-demand scan settings** dialog box is displayed.

5. On the **Extensions** tab, configure the options as described below.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan all files</strong></td>
<td>Scan all files regardless of the filename extension. If you turn on this option, the other options on the <strong>Extensions</strong> tab are turned off. Scanning all files will affect computer performance, so we recommend that you only turn on this option as part of a weekly scheduled scan.</td>
</tr>
</tbody>
</table>
| **Scan only executable and other vulnerable files** | • Check all files with executable file extensions (for example, .exe, .bat, .pif) or files that have the possibility of being infected (for example, .doc, .chm, .pdf).  
• Quickly check the structure of all files, and then scan them if their format is that of an executable file. |
| **Additional file type extensions to be scanned** | To scan additional file types, click **Add**, and then type a file extension such as **PDF** in the **Extension** box. You can use the wildcard ? to match any single character.  
To stop scanning a file type, select its extension in the list, and then click **Remove**.  
To change a file type, select its extension in the list, and then click **Edit**. |
| **Scan files with no extension**     | Files with no extension could be malware, so we recommend that you leave this option turned on.                                                                                                             |
| **Exclude**                         | To exclude specific file types from scheduled scanning, click **Add**, and then type a file extension such as **PDF** in the **Extension** box.  
To start scanning a file type, select its extension in the list, and then click **Remove**.  
To change a file type, select its extension in the list, and then click **Rename**. |

For detailed advice about configuring the extension settings for scheduled scanning, see knowledge base article 63985.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

**Related information**
- knowledge base article 63985
8.3.6 Exclude items from on-demand and scheduled scanning

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can exclude items from on-demand and scheduled scanning.

**Warning**
The “excluded items” settings for scheduled scans also apply to full system scans run from the console and "scan my computer" scans run on networked computers.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**. Then double-click the policy you want to change.
3. The **Anti-virus and HIPS policy** dialog box is displayed. In the **On-demand scanning** panel, click **Configure**.
4. Click the **Windows Exclusions**, **Linux/UNIX Exclusions**, or **Mac Exclusions** tab. To add items to the list, click **Add** and enter the full path in the **Exclude item** dialog box.

The items you can exclude from scanning differ on each type of computer.

You can export the list of Windows exclusions to a file and then import it into another policy.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Scan computers now (page 58)
Check which policies a group uses (page 27)
Import or export on-access scanning exclusions (page 93)

**Related reference**
Items that can be excluded from scanning (page 109)

8.3.7 Import or export Windows exclusions for on-demand and scheduled scanning

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can export the list of Windows exclusions for on-demand and scheduled scanning to a file, and then import it into another policy.

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**.
3. Double-click the policy you want to change.
   - The **Anti-Virus and HIPS Policy** dialog box is displayed.
4. In the **On-demand scanning** panel, click **Configure**.
5. On the **Windows Exclusions** tab, click either **Export** or **Import**.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

## 8.4 Behavior monitoring

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

Run-time detection can intercept threats that cannot be detected before execution. Behavior monitoring uses the following run-time detection methods to intercept threats:

- Malicious and suspicious behavior detection
- Malicious traffic 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 analyzes all programs running on the computer to detect and block activity that is known to be malicious.

### Malicious traffic detection

Malicious traffic detection detects communications between endpoint computers and command and control servers involved in botnet or other malware attacks.

**Note**

Malicious traffic detection requires Sophos Live Protection to be enabled in order to perform lookups and obtain the data. (By default, Sophos Live Protection is enabled.)

### 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.
8.4.1 Turn behavior monitoring on or off

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

By default, behavior monitoring is enabled.

To turn behavior monitoring on or off:

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**.
3. Double-click the policy you want to change.
   - The **Anti-Virus and HIPS policy** dialog box is displayed.
4. In the **On-access scanning** panel, select or clear the **Enable behavior monitoring** check box.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Check which policies a group uses (page 27)

8.4.2 Detect malicious behavior

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

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.

By default, malicious behavior detection is enabled.

To change the settings for detecting and reporting malicious behavior:

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**.
3. Double-click the policy you want to change.
   - The **Anti-Virus and HIPS policy** dialog box is displayed.
4. In the **On-access scanning** panel, make sure the **Enable behavior monitoring** check box is selected.
5. Beside **Enable behavior monitoring**, click **Configure**.
6. In the **Configure Behavior Monitoring** dialog box:
   - To alert the administrator and block malicious behavior, select the **Detect malicious behavior** check box.
   - To disable malicious behavior detection, clear the **Detect malicious behavior** check box.
Note
If you disable malicious behavior detection, suspicious behavior detection will also be disabled. Please note that malicious traffic detection will not be disabled.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

8.4.3 Detect malicious traffic

If you use role-based administration:

• You must have the Policy setting - anti-virus and HIPS right to perform this task.
• You cannot edit a policy if it is applied outside your active sub-estate.
• Malicious traffic detection requires Sophos Live Protection to be enabled. (By default, Sophos Live Protection is enabled.)

Malicious traffic detection detects communications between endpoint computers and command and control servers involved in botnet or other malware attacks.

Note
Malicious traffic detection uses the same set of exclusions as the Sophos Anti-Virus on-access scanner (InterCheck ™).

By default, malicious traffic detection is enabled for new installations of Sophos Enterprise Console 5.3 or later. If you upgraded from an earlier version of Sophos Enterprise Console, you need to enable malicious traffic detection to benefit from the feature.

To change the settings for detecting malicious traffic:

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change. The Anti-Virus and HIPS policy dialog box is displayed.
4. In the On-access scanning panel, make sure the Enable behavior monitoring check box is selected.
5. Beside Enable behavior monitoring, click Configure.
6. In the Configure Behavior Monitoring dialog box, make sure the Detect malicious behavior check box is selected.
7. To turn malicious traffic detection on or off, select or clear the Detect malicious traffic check box.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Exclude items from on-access scanning (page 92)
Check which policies a group uses (page 27)
8.4.4 Detect suspicious behavior

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

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.

By default, suspicious behavior is detected and reported, but not blocked.

To change the settings for detecting and reporting suspicious behavior:

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**.
3. Double-click the policy you want to change. The **Anti-Virus and HIPS policy** dialog box is displayed.
4. In the **On-access scanning** panel, make sure the **Enable behavior monitoring** check box is selected.
5. Beside **Enable behavior monitoring**, click **Configure**.
6. In the **Configure Behavior Monitoring** dialog box, make sure the **Detect malicious behavior** check box is selected.
   - To alert the administrator and block suspicious processes, select the **Detect suspicious behavior** check box and clear the **Alert only, do not block suspicious behavior** check box.
   - To alert the administrator, but not block suspicious processes, select both the **Detect suspicious behavior** check box and the **Alert only, do not block suspicious behavior** check box.

For the strongest protection, we advise you to enable suspicious file detection.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)
- Configure on-access scanning (page 87)

8.4.5 Detect buffer overflows

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

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.

By default, buffer overflows are detected and blocked.

To change the settings for detecting and reporting buffer overflow attacks:
1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change. The Anti-Virus and HIPS policy dialog box is displayed.
4. In the On-access scanning panel, make sure the Enable behavior monitoring check box is selected.
5. Beside Enable behavior monitoring, click Configure. In the Configure Behavior Monitoring dialog box:
   • To alert the administrator and block buffer overflows, select the Detect buffer overflows check box and clear the Alert only, do not block check box.
   • To alert the administrator, but not block buffer overflows, select both the Detect buffer overflows check box and the Alert only, do not block check box.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

8.5 Sophos Live Protection

Sophos Live Protection uses in-the-cloud technology to instantly decide whether a suspicious file is a threat and take action specified in the anti-virus and HIPS policy.

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 malicious files. When new malware is identified, Sophos can send out updates within seconds.

To take full advantage of Live Protection, you must ensure that the following options are enabled.

Enable Live Protection: If on-access scanning 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 characteristics such as checksum are 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.

Note
The Malicious Traffic Detection and Download Reputation features require Live Protection to be enabled in order to perform instant lookups in the SophosLabs online database and obtain the latest threat or reputation data.

Enable Live Protection for on-demand scanning: If you want on-demand scans to use the same in-the-cloud checking as on-access scanning, select this option.

Automatically send file samples to Sophos: If a file is deemed potentially malicious but cannot be positively identified as malicious based on its characteristics alone, Live Protection allows Sophos to request a sample of the file. When Live Protection is enabled, if this option is enabled and Sophos does not already hold a sample of the file, the file is submitted automatically. Submission of such sample files helps Sophos to continuously enhance detection of malware without the risk of false positives.
Note
The maximum sample size is 10 MB. The timeout for sample upload is 30 seconds. It is not recommended to automatically send samples over a slow connection (less than 56 Kbps).

Note
You must ensure that Sophos domain to which the file data is sent is trusted in your web filtering solution. For details, see knowledge base article 62637.

If you use a Sophos web filtering solution, for example the WS1000 Web Appliance, you do not need to do anything - Sophos domains are already trusted.

Related information
knowledge base article 62637

8.5.1 Turn Sophos Live Protection on or off

If you use role-based administration:

- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

Sophos Live Protection checks suspicious files against the latest information in the SophosLabs database.

By default, Live Protection sends file data such as checksums to Sophos for checking, but does not send sample files for analysis. To take full advantage of Live Protection, you should select the option to send sample files.

To turn Live Protection options on or off:

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS. Then double-click the policy you want to change.
3. In the Anti-virus and HIPS Policy dialog box, click the Sophos Live Protection button.
4. In the Sophos Live Protection dialog box:
   - Select or clear the Enable Live Protection check box. This turns Live Protection on or off for on-access scanning.

   Note
   The Malicious Traffic Detection and Download Reputation features require Live Protection to be enabled in order to perform instant lookups in the SophosLabs online database and obtain the latest threat or reputation data.

   - Select or clear the Enable Live Protection for on-demand scanning check box. This turns Live Protection on or off for on-demand scans.
   - Select or clear the Automatically send file samples to Sophos check box.
     The samples can be sent only when Live Protection is enabled.
Note
When a file sample is sent to Sophos for online scanning, the file data (the checksum etc.) is always sent with the sample.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

8.6 Web protection

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.

Note
If you want to have more control over which websites users are allowed to access, for example, if you wish to protect users from visiting websites for which your organization could be legally liable, use the Web Control feature.

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 you attempt to download a file with low or unknown reputation. 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 knowledge base 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.

### 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.

### Web protection events

When access to a malicious website is blocked, an event is logged that can be viewed in the Web Event Viewer and in the Computer details of the endpoint computer where the event occurred. If you use the Web Control feature, both web protection and web control events are displayed in the Web Event Viewer and Computer details.

**Related concepts**
Web control policy (page 176)

**Related tasks**
Configure web protection options (page 107)
View web events (page 204)
View latest web events on a computer (page 205)

**Related information**
knowledge base article 121319

### 8.6.1 Configure web protection options

If you use role-based administration:
You must have the **Policy setting - anti-virus and HIPS** right to perform this task.

You cannot edit a policy if it is applied outside your active sub-estate.

To turn web protection on or off:
1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
2. In the **Policies** pane, double-click **Anti-virus and HIPS**.
3. Double-click the policy you want to change.
4. In the **Anti-virus and HIPS** policy dialog box, click the **Web Protection** button.
5. In the **Web Protection** dialog box, under **Malware protection**, next to **Block access to malicious websites**, select **On** or **Off** to block or unblock access to malicious websites. This option is enabled by default.
6. 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.
7. To change what happens when a user attempts to download a file with low or unknown reputation, under **Download reputation**, next to **Action**, select either **Prompt user** (default) or **Log only**.

**Note**
Download reputation requires Sophos Live Protection to be enabled. (By default, Sophos Live Protection is enabled.)

- If you select **Prompt user**, every time a user attempts to download a low reputation file, an alert will be displayed, informing about this and asking whether to block or allow the download. We recommend that users do not download such files. If they trust the file's source and publisher, they 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 and logged as a web event in Sophos Enterprise Console.
- If you select **Log only**, no alert will be displayed; the download will be allowed and recorded in the scanning log and logged as a web event in Sophos Enterprise Console.
8. 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 or a log record and event created every time a user attempts to download a file with low or unknown reputation.
    - If you select **Strict**, an alert will be displayed or a log record and event created every time a user attempts to download a file with low, unknown, or medium reputation.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Check which policies a group uses (page 27)
Authorize websites (page 116)
8.7 Scanned file types and exclusions

By default, Sophos Endpoint Security and Control scans file types that are vulnerable to viruses. The file types that are scanned by default not only differ between operating systems, but also change as the product is updated.

To see a list of the file types that are scanned by default, go to a computer with the relevant operating system, open Sophos Endpoint Security and Control or Sophos Anti-Virus, and then look for the extensions configuration page.

You can also choose to scan additional file types or exempt some file types from scanning.

Windows

To see a list of the file types scanned by default on a Windows computer:

1. Open Sophos Endpoint Security and Control.
2. Under Anti-virus and HIPS, click Configure anti-virus and HIPS, and then click On-demand extensions and exclusions.

macOS

Sophos Anti-Virus for macOS scans all file extensions during on-access scanning.

Linux or UNIX

To make changes on a Linux computer, use the savconfig and savscan commands as described in the Sophos Anti-Virus for Linux configuration guide.

To make changes on a UNIX computer, use the savscan command as described in the Sophos Anti-Virus for UNIX configuration guide.

Related tasks
Specify on-access scanning file extensions (page 91)
Specify file extensions for on-demand and scheduled scanning (page 97)

8.7.1 Items that can be excluded from scanning

On each type of computer, there are different limitations on the items that you can exclude from scanning.

Windows

On Windows, you can exclude drives, folders, files, and processes.
You can use the * and ? wildcards.
The wildcard ? generally matches any single character. However, when used at the end of a file name or extension, it matches any single character or no characters. For example, file???.txt matches file.txt, file1.txt and file12.txt but not file123.txt.

You can use also the wildcards to exclude folders and processes.

**macOS**

On macOS, you can exclude files, folders, and volumes.
You can specify which items are excluded by prefixing or suffixing the exclusion with a slash or suffixing the exclusion with a double slash.

For more information, see the Sophos Anti-Virus for macOS help.

**Linux or UNIX**

On Linux and UNIX, you can exclude directories and files.
You can specify any POSIX path, whether it is a file or a directory, for example, /folder/file.
You can use the ? and * wildcards.

**Note**

Sophos Enterprise Console only supports path-based Linux and UNIX exclusions. You can also set up other types of exclusion directly on the managed computers. Then you can use regular expressions, exclude file types and filesystems. For information on how to do this, see the Sophos Anti-Virus for Linux configuration guide or the Sophos Anti-Virus for UNIX configuration guide.

If you set up another path-based exclusion on a managed Linux or UNIX computer, this computer is reported to the console as differing from the group policy.

**Related tasks**

Exclude items from on-access scanning (page 92)
Exclude items from on-demand and scheduled scanning (page 99)

**8.7.2 Specifying scanning exclusions for Windows**

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, 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:\Program\Sophos\Sophos~1 For more information, see knowledge base article 13045.</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>
<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>D:\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>Exclusion type</td>
<td>Description</td>
<td>Examples</td>
<td>Comments</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 but excluding 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 ? and * wildcards.

Use the ? wildcard in a file name or extension to match any single character.

At the end of a file name or extension, the ? wildcard matches any single character or no characters. For example, file???.txt matches file.txt, file1.txt, and file12.txt, but not file123.txt.

Use the * wildcard in a file name or extension, in the form [file name].* or *.[extension]:

<table>
<thead>
<tr>
<th>Correct</th>
<th>Incorrect</th>
</tr>
</thead>
<tbody>
<tr>
<td>file.*</td>
<td>file.txt*</td>
</tr>
<tr>
<td>*.txt</td>
<td>file.*txt</td>
</tr>
</tbody>
</table>

You can exclude files with a specific beginning and extension:

file*.txt

The above example excludes the following files from scanning:

file.txt
file1.txt
file12.txt
file.1.txt
file.12.txt
file12.12.txt

The following files are not excluded by applying the exclusion defined above:

file.1txt
file.12txt
file.txt1
file.txt12
1file.txt
8.8 Authorizing items for use

8.8.1 Authorize adware and PUAs

If you use role-based administration:

- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

If you have enabled Sophos Endpoint Security and Control to detect adware and other potentially unwanted applications (PUAs), it may prevent the use of an application that you require.

To authorize an adware or PUA application:

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. Click Authorization.
   The Authorization Manager dialog box is displayed.
5. On the Adware and PUAs tab, in the Known adware and PUAs list, select the application you want to authorize.
   If you cannot see the application that you want to authorize, you can add it to the list of known adware and PUAs yourself.
6. Click Add.
   The adware or PUA appears in the Authorized adware and PUAs list.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)
Pre-authorize adware and PUAs (page 113)

8.8.2 Pre-authorize adware and PUAs

If you use role-based administration:

- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

If you want to allow an application to be used that Sophos Endpoint Security and Control has not yet classified as an adware or PUA, you can pre-authorize it by adding it to the list of authorized adware and PUAs yourself.

1. Go to the Sophos Adware and PUAs web page.
2. Find, and then copy, the name of the application that you want to pre-authorize.
3. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
4. In the Policies pane, double-click Anti-virus and HIPS.
5. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
6. Click Authorization.
   The Authorization Manager dialog box is displayed.
7. On the Adware and PUAs tab, click New entry.
8. In the Add New Adware or PUA dialog box, paste the application name that you copied in step 2.
   The adware or PUA appears in the Authorized adware and PUAs list.

If you have made a mistake or simply want to remove an application from the Authorization Manager, delete it from the list of known adware and PUAs:
1. In the Authorized adware and PUAs list, select the application.
2. Click Remove.
3. In the Known adware or PUAs list, select the application.
4. Click Delete entry.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

Related information
Adware and PUAs.

8.8.3 Block authorized adware and PUAs

If you use role-based administration:

- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

To prevent currently-authorized adware and PUAs from running on computers:
1. Check which anti-virus and HIPS policy is used by the group of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS. Then double-click the policy you want to change.
3. In the Anti-Virus and HIPS Policy dialog box, click the Authorization button.
4. On the Adware or PUAs tab, in the Authorized adware and PUAs list, select the application you want to block.
5. Click Remove.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)
8.8.4 Authorize suspicious items

If you use role-based administration:

- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

If you have enabled one or more HIPS options (for example, suspicious behavior detection, buffer overflow detection, or suspicious file detection), but you want to use some of the items detected, you can authorize them as follows:

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. Click Authorization.
   The Authorization Manager dialog box is displayed.
5. Click the tab for the type of behavior that has been detected.
   In this example, we’ll use Buffer Overflow.
6. In the Known applications list, select the application you want to authorize.
   If you cannot see the application you want to authorize, you can add it to the list of authorized applications yourself.
7. Click Add.
   The suspicious application appears in the Authorized applications list.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)
Pre-authorize adware and PUAs (page 113)

8.8.5 Pre-authorize potentially suspicious items

If you want to allow the use of an application or file that Sophos Endpoint Security and Control has not yet classified as suspicious, you can pre-authorize it by adding it to the list of authorized items yourself.

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Anti-virus and HIPS.
3. Double-click the policy you want to change.
   The Anti-Virus and HIPS Policy dialog box is displayed.
4. Click Authorization.
   The Authorization Manager dialog box is displayed.
5. Click the tab for the type of behavior that has been detected.
   In this example, we’ll use Buffer Overflow.
6. Click New entry.
   The Open dialog box is displayed.
7. Browse to the application, and then double-click it.
The suspicious application appears in the **Authorized applications** list.

If you have made a mistake or simply want to remove an application from the **Authorization Manager**, delete it from the list of known files:

1. In the **Authorization Manager** dialog box, click the tab for the type of behavior that has been detected.
   
   In this example, we’ll use **Suspicious Files**.

2. In the **Authorized files** list, select the file.

3. Click **Remove**.

4. In the **Known files** list, select the file.

5. Click **Delete entry**.

**Related tasks**

Check which policies a group uses (page 27)

8.8.6 Authorize websites

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

If you want to authorize 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's online web filtering service.

**CAUTION**

Authorizing a website that Sophos has classified as malicious could expose your users to threats. Make sure that it is safe to visit the website before you authorize it.

To authorize a website:

1. Check which anti-virus and HIPS policy is used by the groups of computers you want to configure.

2. In the **Policies** pane, double-click **Anti-virus and HIPS**.

3. Double-click the policy you want to change.
   
   The **Anti-Virus and HIPS Policy** dialog box is displayed.

4. Click **Authorization**.
   
   The **Authorization Manager** dialog box is displayed.

5. On the **Websites** tab, click **Add**.
   
   - To edit a website entry, select it in the **Authorized websites** list, and then click **Edit**.
   
   - To delete a website entry, select it in the **Authorized websites** list, and then click **Remove**.

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

   - If you have download scanning enabled and your users visit a website that contains a threat, access to the site will be blocked even if it is listed as an authorized website.

   - If you use the web control feature, when you authorize a website that is blocked by your **Web control** policy, the website will still be blocked. To allow access to the website, you will need to exempt it from web control filtering as well as authorize it in the anti-virus and HIPS policy.
8.9 Firewall policy

The Firewall policy specifies how the firewall protects computers.

By default, the Sophos Client Firewall is enabled and blocks all non-essential traffic. Before you use it throughout your network, you should configure it to allow the applications you want to use.

For a full list of the default firewall settings, see knowledge base article 57757.

A number of features have been removed from Sophos Client Firewall 3.0 for Windows 8 and later and are available only to computers running Windows 7 or earlier. These features are:

- Interactive mode
- Hidden process detection
- Modified memory detection
- Rawsocket applications (rawsockets are treated the same as other connections)
- Non-stateful rules
- The option Concurrent connections for TCP rules
- The option Where the local port is equal to the remote port

8.9.1 Basic firewall configuration

Set up a basic firewall policy

By default, the firewall is enabled and blocks all non-essential traffic. Therefore, you should configure it to allow the applications you want to use, and test it before installing it on all computers. See the Sophos Enterprise Console policy setup guide for detailed advice.

For more information about the default firewall settings, see knowledge base article 57757.

For information about preventing network bridging, see Device control policy.

Note
When you apply a new or updated policy to computers, applications that were allowed before may be blocked briefly until the new policy is fully applied. You should notify your users about this before you apply new policies.
Note
If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To set up a basic firewall policy:

1. In the **Policies** pane, double-click **Firewall**.
2. Double-click the **Default** policy to edit it.
   The **Firewall Policy** wizard appears. Follow the instructions on the screen. There is additional information on some of the options below.
3. On the **Configure firewall** page, select the type of location:
   - Select **Single location** for computers that are always on the network, for example, desktops.
   - Select **Dual location** if you want the firewall to use different settings according to the location where computers are used, for example, in the office (on the network) and out of office (off the network). You may want to set up dual location for laptops.
4. On the **Operational mode** page, select how the firewall will handle inbound and outbound traffic:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block inbound and outbound traffic</td>
<td>• Default level. Offers the highest security.</td>
</tr>
<tr>
<td></td>
<td>• Only allows essential traffic through the firewall and authenticates the identity of applications using checksums.</td>
</tr>
<tr>
<td></td>
<td>• To allow applications commonly used in your organization to communicate through the firewall, click <strong>Trust</strong>.</td>
</tr>
<tr>
<td>Block inbound and allow outbound traffic</td>
<td>• Offers a lower security level than <strong>Block inbound and outbound traffic</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Allows your computers to access the network and internet without you having to create special rules.</td>
</tr>
<tr>
<td></td>
<td>• All applications are allowed to communicate through the firewall.</td>
</tr>
<tr>
<td>Monitor</td>
<td>• Applies to network traffic the rules that you have set up. If traffic has no matching rule, it is reported to the console, and only allowed if it is outbound.</td>
</tr>
<tr>
<td></td>
<td>• Enables you to collect information about your network, and to then create suitable rules before deploying the firewall to your computers.</td>
</tr>
</tbody>
</table>

5. On the **File and printer sharing** page, select **Allow file and printer sharing** if you want to allow computers to share local printers and folders on the network.

After you have set up the firewall, you can view firewall events (for example, applications blocked by the firewall) in the **Firewall - Event Viewer**.
The number of computers with events over a specified threshold within the last seven days is also displayed on the Dashboard.

**Related concepts**
- Device control policy (page 164)
- Managing roles and sub-estates (page 15)
- About trusting applications (page 125)
- About using monitor mode (page 119)

**Related tasks**
- Check which policies a group uses (page 27)
- View firewall events (page 200)

**Related information**
- knowledge base article 57757

---

**About using monitor mode**

You can enable monitor mode on test computers and use the Firewall Event Viewer to view which traffic, applications, and processes are being used. You can then use the Event Viewer to create rules that allow or block reported traffic, applications, and processes.

**Note**

When you create a rule using the Firewall Event Viewer and add it to the firewall policy, the firewall mode changes from **Monitor** to **Custom**.

If you do not want to allow unknown traffic by default, you can use interactive mode. In interactive mode, the firewall prompts the user to allow or block any applications and traffic for which it does not have a rule.

**Related concepts**
- Interactive mode (page 123)

**Related tasks**
- Create a firewall event rule (page 122)

---

**Add and trust an application**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

Trusted applications are allowed full and unconditional network access, including access to the internet.

To add an application to the firewall policy and trust it:

1. On the **Operational mode** page of the **Firewall Policy** wizard, click **Trust**. The **Firewall Policy** dialog box appears.
2. Click **Add**. The **Firewall policy - Add trusted application** dialog box appears.
3. In the **Search period** field, click the drop-down arrow and select the period for which you want to display application events.
You can either select a fixed period, for example, **Within 24 hours**, or select **Custom** and specify your own time period by selecting the starting and ending dates and times.

4. If you want to view application events of a certain type, in the **Event type** field, click the drop-down arrow and select the event type.

5. If you want to view application events for a certain file, in the **File name** field, enter the file name.
   - If you leave this field empty, application events for all files will be displayed.
   - You can use wildcards in this field. Use ? for any single character and * for any string of characters.

6. Click **Search** to display a list of application events.

7. Select an application event, and then click **OK**.

The application is added to the firewall policy and marked as **Trusted**.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

### Allow all traffic on a LAN

If you use role-based administration:
- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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

1. Check which firewall policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Firewall**, and then double-click the policy you want to change.
3. On the **File and printer sharing** page of the **Firewall Policy** wizard, select **Use custom settings**, and then click **Custom**.
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.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

### Allow file and printer sharing

If you use role-based administration:
- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To allow computers to share local printers and folders on the network:

1. Check which firewall policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Firewall**, and then double-click the policy you want to change.
3. On the **File and printer sharing** page of the **Firewall Policy** wizard, select **Allow file and printer sharing**.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

**Allow flexible control of file and printer sharing**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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

- 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.
- 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. Check which firewall policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Firewall**, and then double-click the policy you want to change.
3. On the **File and printer sharing** page of the **Firewall Policy** wizard, select **Use custom settings**, and then click **Custom**.
4. Clear the **Block file and printer sharing for other networks** check box.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

**Block unwanted file and printer sharing**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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

1. Check which firewall policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Firewall**, and then double-click the policy you want to change.
3. On the **File and printer sharing** page of the **Firewall Policy** wizard, select **Use custom settings**, and then click **Custom**.
4. Select the **Block file and printer sharing for other networks** check box.
Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

Create a firewall event rule

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can create rules for all firewall events except the “modified memory” events.

To create a firewall event rule:

1. On the **Events** menu, click **Firewall Events**.
2. In the **Firewall - Event Viewer** dialog box, select an event for the application you want to create a rule for and click **Create Rule**.
3. In the dialog box that appears, select an option that you want to apply to the application.
4. Select which location you want to apply the rule to (primary, secondary, or both). If you select to apply the rule to the secondary location or both locations, the rule will be added only to policies which have a secondary location configured. Click **OK**.

**Note**

The “new application” and “modified application” events are location independent (they add checksums which are shared between both locations). You cannot select a location for these events.

5. From the list of firewall policies, select a policy or policies which you want to apply the rule to. Click **OK**.

**Note**

You cannot add a rule to a policy that is applied outside your active sub-estate.

**Note**

If you want to create an application rule directly from a firewall policy, use the advanced firewall policy configuration pages.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)
Create an application rule from a firewall policy (page 138)

Temporarily disable the firewall

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
To turn the firewall off for a group of computers:

1. Check which firewall policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Firewall. Then double-click the policy you want to change. The Firewall Policy wizard appears.
3. On the welcome page of the wizard, do one of the following:
   - If you want to turn the firewall off for all locations you have set up (primary location and secondary location, if you configured one), click Next. On the Configure firewall page, select Allow all traffic (the firewall is turned off). Complete the wizard.
   - If you want to turn the firewall off for one of the locations (primary or secondary), click the Advanced firewall policy button. In the Firewall Policy dialog box that appears, select Allow all traffic next to Primary location or Secondary location. Click OK. Complete the Firewall Policy wizard.

If you disable the firewall, your computers are unprotected until you re-enable it. To enable the firewall, clear the Allow all traffic check box.

Related concepts
Managing roles and sub-estates (page 15)
Related tasks
Check which policies a group uses (page 27)

8.9.2 Advanced firewall configuration

Open the advanced configuration pages

If you use role-based administration:

- You must have the Policy setting - firewall right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

If you want to have greater control over the firewall settings and the ability to fine-tune them, you can use the advanced firewall policy configuration pages to configure the firewall.

To open the advanced firewall configuration pages:

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.

Related concepts
Managing roles and sub-estates (page 15)

Interactive mode

On computers running Windows 7 or earlier, you can enable interactive mode. The firewall then displays a learning dialog on the endpoint computer each time an unknown application or service
requests network access. The learning dialog asks the user whether to allow or block the traffic, or whether to create a rule for that type of traffic.

**Note**
On Windows 8 and later, interactive mode is not available. You must add specific policy rules to allow or block applications. You can use the **Firewall - Event Viewer** to manage application rules interactively.

**Related tasks**
Create a firewall event rule (page 122)

Enable interactive mode
If you use role-based administration:
- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

The firewall can work in interactive mode, asking the user how to deal with detected traffic.

To put the firewall in interactive mode on a group of computers:
1. Check which firewall policy is used by the groups of computers you want to configure.
2. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
3. Under **Configurations**, click **Configure** next to the location that you want to configure.
4. On the **General** tab, under **Working mode**, click **Interactive**.

**Related concepts**
Managing roles and sub-estates (page 15)
Interactive mode (page 123)

Change to a non-interactive mode
If you use role-based administration:
- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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 on a group of computers:
1. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
2. Under **Configurations**, click **Configure** next to the location that you want to configure.
3. Click the **General** tab.
4. Under **Working mode**, click **Allow by default** or **Block by default**.

**Related concepts**
Managing roles and sub-estates (page 15)
8.9.3 Configuring the firewall

About trusting applications

To help provide security for your computers, the firewall blocks traffic from unrecognized applications on your computers. However, applications commonly used in your organization may be blocked, thus preventing users from performing their everyday tasks.

You can trust these applications, so that they can communicate through the firewall. Trusted applications are allowed full and unconditional access to the network and the internet.

Note
For greater security, you can apply one or more application rules to specify the conditions under which the application can run.

Related tasks
Create an application rule from a firewall policy (page 138)

Add an application to a firewall policy

If you use role-based administration:

• You must have the Policy setting - firewall right to configure a firewall policy.
• You cannot edit a policy if it is applied outside your active sub-estate.

To add an application to a firewall policy:

1. Under Configurations, click Configure next to the location that you want to configure.
2. Click the Applications tab.
3. Click Add.
   The Firewall Policy - Add application dialog box appears.
4. In the Search period field, click the drop-down arrow and select the period for which you want to display application events.
   You can either select a fixed period, for example, Within 24 hours, or select Custom and specify your own time period by selecting the starting and ending dates and times.
5. If you want to view application events of a certain type, in the Event type field, click the drop-down arrow and select the event type.
6. If you want to view application events for a certain file, in the File name field, enter the file name.
   If you leave this field empty, application events for all files will be displayed.
   You can use wildcards in this field. Use ? for any single character and * for any string of characters.
7. Click Search to display a list of application events.
8. Select an application event, and then click OK.
   • The application is added to the firewall policy and marked as Trusted.
   • The application’s checksum is added to the list of allowed checksums.
Related concepts
Managing roles and sub-estates (page 15)

Remove an application from a firewall policy

If you use role-based administration:

- You must have the Policy setting - firewall right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To remove an application from a firewall policy:

1. Under Configurations, click Configure next to the location that you want to configure.
2. Click the Applications tab.
3. Select the application in the list, and then click Remove.

Related concepts
Managing roles and sub-estates (page 15)

Trust an application

If you use role-based administration:

- You must have the Policy setting - firewall right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To trust an application on a group of computers:

1. Under Configurations, click Configure next to the location that you want to configure.
2. Click the Applications tab.
   - If the application is not in the list, add it.
3. Select the application in the list, and then click Trust.
   - The application is added to the firewall policy and marked as Trusted.
   - The application’s checksum is added to the list of allowed checksums.

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.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Add an application to a firewall policy (page 125)
Apply preset application rules (page 140)
Create an application rule (page 137)

Trust an application using the Firewall Event Viewer

If you use role-based administration:

- You must have the Policy setting - firewall right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.
If the firewall reports an unknown application or blocks an application on your networked computers, an event is displayed in the Firewall Event Viewer. This topic describes how to trust an application from the Firewall Event Viewer and apply the new rule to your chosen firewall policies.

To find details of reported or blocked applications in the Firewall Event Viewer, and trust them or create new rules for them:

1. On the **Events** menu, click **Firewall Events**.
2. In the **Firewall - Event Viewer** dialog box, select the entry for the application you want to trust or create a rule for, and then click **Create Rule**.
3. In the dialog box that appears, select whether to trust the application or create a rule for it using an existing preset.
4. From the list of firewall policies, select the firewall policies to which you want to apply the rule. To apply the rule to all policies, click **Select All** and then click **OK**.
   - If you are using checksums, you may have to add the application's checksum to the list of allowed checksums.
   - You can also add an application as trusted directly in a firewall policy, using the advanced firewall policy configuration pages.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Add an application checksum (page 129)
Create an application rule from a firewall policy (page 138)

**Block an application**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To block an application on a group of computers:

1. Check which firewall policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Firewall**, and then double-click the policy you want to change.
3. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
4. Under **Configurations**, click **Configure** next to the location that you want to configure.
5. Click the **Applications** tab.
   - If the application is not in the list, add it.
6. Select the application in the list, and then click **Block**.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Check which policies a group uses (page 27)
Add an application to a firewall policy (page 125)

**Allow applications to launch hidden processes**

If you use role-based administration:
You must have the **Policy setting - firewall** right to configure a firewall policy.

You cannot edit a policy if it is applied outside your active sub-estate.

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.

To allow applications to launch hidden processes, follow these steps.

**Note**

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

1. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
2. Under **Configurations**, click **Configure** next to the location for which you want to configure the firewall.
3. Click the **Processes** tab.
4. In the upper area, click **Add**. The **Firewall Policy - Add application** dialog box appears.
5. In the **Search period** field, click the drop-down arrow and select the period for which you want to display application events.
6. If you want to view application events for a certain file, in the **File name** field, enter the file name.
7. If you leave this field empty, application events for all files will be displayed.
   You can use wildcards in this field. Use ? for any single character and * for any string of characters.
8. Click **Search** to display a list of application events.
9. Select an application event, and then click **OK**.

If you enable interactive mode, the firewall can display a learning dialog on the endpoint computer when it detects a new launcher. The interactive mode is not available on Windows 8 and later.

**Related concepts**

Managing roles and sub-estates (page 15)

**Related tasks**

Enable interactive mode (page 124)

**Allow applications to use rawsockets**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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.

To allow applications to access the network through rawsockets, follow these steps.
1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the Processes tab.
5. In the lower area, click Add.
   The Firewall Policy - Add application dialog box appears.
6. In the Search period field, click the drop-down arrow and select the period for which you want to display application events.
   You can either select a fixed period, for example, Within 24 hours, or select Custom and specify your own time period by selecting the starting and ending dates and times.
7. If you want to view application events for a certain file, in the File name field, enter the file name.
   If you leave this field empty, application events for all files will be displayed.
   You can use wildcards in this field. Use ? for any single character and * for any string of characters.
8. Click Search to display a list of application events.
9. Select an application event, and then click OK.

If you enable interactive mode, the firewall can display a learning dialog on the endpoint computer when a rawsocket is detected.

Related concepts
Managing roles and sub-estates (page 15)
Related tasks
Enable interactive mode (page 124)

Add an application checksum

If you use role-based administration:
• You must have the Policy setting - firewall right to configure a firewall policy.
• You cannot edit a policy if it is applied outside your active sub-estate.

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.

To add a checksum to the list of allowed checksums:
1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Click the Checksums tab.
4. Click Add.
   The Firewall Policy - Add application checksum dialog box appears.
5. In the **Search period** field, click the drop-down arrow and select the period for which you want to display application events.

   You can either select a fixed period, for example, **Within 24 hours**, or select **Custom** and specify your own time period by selecting the starting and ending dates and times.

6. In the **Event type** field, click the drop-down arrow and select whether you want to add a checksum for a modified application or a new application.

7. If you want to view application events for a certain file, in the **File name** field, enter the file name.

   If you leave this field empty, application events for all files will be displayed.

   You can use wildcards in this field. Use ? for any single character and * for any string of characters.

8. Click **Search** to display a list of application events.

9. Select the application event for which you want to add a checksum, and then click **OK**.

The application checksum is added to the list of allowed checksums in the **Firewall Policy** dialog box.

If you enable interactive mode, the firewall can display a learning dialog on the endpoint computer when it detects a new or modified application.

**Related concepts**

Managing roles and sub-estates (page 15)

**Related tasks**

Enable interactive mode (page 124)

---

**Turn blocking of modified processes on or off**

If you use role-based administration:

- **You must have the Policy setting - firewall** right to configure a firewall policy.
- **You cannot edit a policy if it is applied outside your active sub-estate.**

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. Double-click the firewall policy you want to change.
2. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
3. Under **Configurations**, click **Configure** next to the location for which you want to configure the firewall.
4. On the **General** tab, under **Blocking**, clear the **Block processes if memory is modified by another application** 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 and on Windows 8 and later. On Windows 8 and later it is handled automatically by the Sophos Anti-Virus HIPS technology.

• Only the modified process is blocked. The modifying program is not blocked from accessing the network.

Related concepts
Managing roles and sub-estates (page 15)

Turn the use of checksums on or off

By default, the firewall uses checksums to authenticate applications. When you trust or block applications, they are identified by 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. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. On the General tab, under Blocking, select or clear the Use checksums to authenticate applications check box.

Allow or block IPv6 packets

To allow or block IPv6 packets:

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. On the General tab, under Blocking, clear or select the Block IPv6 packets check box.

Filter ICMP messages

If you use role-based administration:

• You must have the Policy setting - firewall right to configure a firewall policy.

• You cannot edit a policy if it is applied outside your active sub-estate.

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.

To filter ICMP messages:

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. On the **ICMP** tab, select the **In** or **Out** check box to allow incoming or outgoing messages of the specified type.

**Related concepts**
- Managing roles and sub-estates (page 15)
- Explanation of ICMP message types (page 132)

**Explanation of ICMP message types**

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Echo Request, Echo Reply</strong></td>
<td>Used to test destination accessibility and status. A host sends an <strong>Echo Request</strong> and listens for a corresponding <strong>Echo Reply</strong>. This is most commonly done using the <strong>ping</strong> command.</td>
</tr>
<tr>
<td><strong>Destination Unreachable, Echo Reply</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Source Quench</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Redirect Message</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Router Advertisement, Router Solicitation</strong></td>
<td>Allow hosts to discover the existence of routers. Routers periodically broadcast their IP addresses via <strong>Router Advertisement</strong> messages. Hosts may also request a router address by broadcasting a <strong>Router Solicitation</strong> message to which a router replies with a <strong>Router Advertisement</strong>.</td>
</tr>
<tr>
<td><strong>Time Exceeded</strong></td>
<td>Sent by a router if the datagram has reached the maximum limit of routers through which it can travel.</td>
</tr>
<tr>
<td><strong>Parameter Problem</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Timestamp Request, Timestamp Reply</strong></td>
<td>Used to synchronize the clocks between hosts and to estimate transit time.</td>
</tr>
<tr>
<td><strong>Information Request, Information Reply</strong></td>
<td>Obsolete. These messages were used earlier by hosts to determine their inter-network addresses, but are now considered outdated and should not be used.</td>
</tr>
<tr>
<td><strong>Address Mask Request, Address Mask Reply</strong></td>
<td>Used to find the mask of the subnet (i.e. what address bits define the network). A host sends an <strong>Address Mask Request</strong> to a router and receives an <strong>Address Mask Reply</strong> in return.</td>
</tr>
</tbody>
</table>
8.9.4 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.

For information about the settings for the default global and application rules, see knowledge base article 57757.

Related information
knowledge base article 57757

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>
<tr>
<td>TCP</td>
<td>Local</td>
<td>137-139 or 445</td>
</tr>
<tr>
<td>UDP</td>
<td>Remote</td>
<td>137 or 138</td>
</tr>
<tr>
<td>UDP</td>
<td>Local</td>
<td>137 or 138</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:
   a) In **Allow by default** mode, the traffic is allowed (if it is outbound).

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

6. In **Block by default** mode, the traffic is blocked.
7. In **Interactive** mode, the user is asked to decide. This mode is not available on Windows 8 and later.

**Local network detection**

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

You can assign the local network for a computer to firewall rules. When the firewall starts, it determines the computer's local network, 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 secondary configurations. If the 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.

**8.9.5 Global rules**

**Create a global rule**

If you use role-based administration:
- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

**CAUTION**
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. Double-click the firewall policy you want to change.
2. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.

4. Click the Global Rules tab.

5. Click Add.

6. 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.

7. To apply the rule before any application rules or normal priority global rules, select the High priority rule check box.

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 actions 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.

    Note
    This option is only available for TCP rules, which are stateful by default.

    • To intelligently allow replies from the remote computer based on the initial connection, select Stateful inspection.

    Note
    This option is only available for UDP and IP rules.

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

11. Under Rule description, click an underlined value. For example, if you click the Stateful TCP link, the Select Protocol dialog box opens.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
The order in which rules are applied (page 133)

Edit a global rule

If you use role-based administration:

• You must have the Policy setting - firewall right to configure a firewall policy.

• You cannot edit a policy if it is applied outside your active sub-estate.

CAUTION
We recommend that you change global rules only if you are familiar with networking protocols.
To edit a global rule:
1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the Global Rules tab.
5. In the Rule list, select the rule that you want to edit.
6. Click Edit.

For information on the global rule settings, see knowledge base article 57757.

Related concepts
Managing roles and sub-estates (page 15)
Related information
knowledge base article 57757

Copy a global rule

If you use role-based administration:
• You must have the Policy setting - firewall right to configure a firewall policy.
• You cannot edit a policy if it is applied outside your active sub-estate.

To copy a global rule and append it to the list of rules:
1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the Global Rules tab.
5. In the Rule list, select the rule that you want to copy.
6. Click Copy.

Related concepts
Managing roles and sub-estates (page 15)

Delete a global rule

If you use role-based administration:
• You must have the Policy setting - firewall right to configure a firewall policy.
• You cannot edit a policy if it is applied outside your active sub-estate.
1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the Global Rules tab.
5. In the Rule list, select the rule that you want to delete.
6. Click Remove.
Change the order in which global rules are applied

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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. Double-click the firewall policy you want to change.
2. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
3. Under **Configurations**, click **Configure** next to the location for which you want to configure the firewall.
4. Click the **Global Rules** tab.
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**.

Related concepts
Managing roles and sub-estates (page 15)

---

8.9.6 Application rules

Create an application rule

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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

1. Double-click the firewall policy you want to change.
2. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
3. Under **Configurations**, click **Configure** next to the location for which you want to configure the firewall.
4. Click the **Applications** tab.
5. Select the application in the list, and then click **Custom**.
6. In the **Application Rules** dialog box, click **Add**.
7. 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.
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 actions 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**.

**Note**
This option is only available for TCP rules, which are stateful by default.

To intelligently allow replies from the remote computer based on the initial connection, select **Stateful inspection**.

**Note**
This option is only available for UDP and IP rules.

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

11. Under **Rule description**, click an underlined value. For example, if you click the **Stateful TCP** link, the **Select Protocol** dialog box opens.

**Related concepts**
**Managing roles and sub-estates** (page 15)

**Create an application rule from a firewall policy**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can create an application rule directly from a firewall policy using the advanced firewall policy configuration pages.

To create an application rule from a firewall policy:

1. Double-click the policy you want to change.
2. On the welcome page of the **Firewall Policy** wizard, click the **Advanced firewall policy** button.
3. In the **Firewall Policy** dialog box that appears, click **Configure** next to the location for which you want to configure the firewall.
4. Do one of the following:
   - If you want to add an application to the firewall policy, in the dialog box that appears, go to the **Applications** tab and click **Add**.
   - If you want to allow an application to launch hidden processes, go to the **Processes** tab and click **Add** in the upper area.
   - If you want to allow an application to access the network using rawsockets, go to the **Processes** tab and click **Add** in the lower area.

The **Firewall policy - Add application** dialog box appears.

5. If you are adding an application, in the **Event type** box, select whether you want to add a modified application, a new application, or an application for which there is no application rule set up in the firewall policy.
6. Select an entry for the application you want to add or allow to launch hidden processes or use rawsockets, and click OK.
   The application is added to the firewall policy.

If you added an application on the Applications tab, the application is added as trusted. If you want, you can block it or create a custom rule for it.

Related concepts
Managing roles and sub-estates (page 15)

Edit an application rule

If you use role-based administration:

- You must have the Policy setting - firewall right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the Applications tab.
5. Select the application in the list, and then click Custom.
6. In the Application Rules dialog box, click Edit.
7. 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.
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 actions 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.
      
      Note
      This option is only available for TCP rules, which are stateful by default.
    
    - To intelligently allow replies from the remote computer based on the initial connection, select Stateful inspection.
      
      Note
      This option is only available for UDP and IP rules.

Note
On Windows 8 and later, these options do not apply as Stateful inspection is always used and Concurrent connections are not supported.
11. Under **Rule description**, click an underlined value. For example, if you click the **Stateful TCP** link, the **Select Protocol** dialog box opens.

**Related concepts**
Managing roles and sub-estates (page 15)

**Apply preset application rules**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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

1. Double-click the firewall policy you want to change.
2. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
3. Under **Configurations**, click **Configure** next to the location for which you want to configure the firewall.
4. Click the **Applications** tab.
5. Select the application in the list, and then click **Custom**.
6. Point to **Add rules from preset**, and then click a preset.

**Related concepts**
Managing roles and sub-estates (page 15)

**Copy an application rule**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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

1. Double-click the firewall policy you want to change.
2. On the **Welcome** page of the **Firewall Policy** wizard, click **Advanced firewall policy**.
3. Under **Configurations**, click **Configure** next to the location for which you want to configure the firewall.
4. Click the **Applications** tab.
5. Select the application in the list, and then click **Custom**.
6. In the **Application Rules** dialog box, select the rule you want to copy and click **Copy**.

**Related concepts**
Managing roles and sub-estates (page 15)

**Delete an application rule**

If you use role-based administration:

- You must have the **Policy setting - firewall** right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.
1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the Applications tab.
5. Select the application in the list, and then click Custom.
6. In the Application Rules dialog box, select the rule you want to remove and click Remove.

Related concepts
Managing roles and sub-estates (page 15)

Change the order in which application rules are applied

If you use role-based administration:

- You must have the Policy setting - firewall right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

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. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the Applications tab.
5. Select the application in the list, and then click Custom.
6. In the Application Rules dialog box, in the Rule list, click the rule that you want to move up or down in the list.
7. Click Move Up or Move Down.

Related concepts
Managing roles and sub-estates (page 15)

8.9.7 Location awareness

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

The most common scenario in which this feature is used is where an employee has a company laptop and works from home. They are using two network connections simultaneously:

- For work use, they connect to the office network through a VPN client and a virtual network adapter.
- For personal use, they connect to their 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 requires sufficient rules to allow the "virtual" office connection to be established.

About setting 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 to 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 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.

Note
The secondary configuration switches from Interactive mode to Block by default mode on a computer when both the following conditions are met:
• Both locations are active.
• The primary configuration is not interactive.

Define your primary locations
1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the Location detection tab.
5. 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>

6. Follow the instructions on the screen.
Create a secondary configuration

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Select the Add configuration for a second location check box.

Now set up your secondary configuration.

CAUTION
We strongly advise caution when using local network rules as part of secondary configurations. If the 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.

Choose a configuration to apply

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. 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.</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>

Related concepts
Managing roles and sub-estates (page 15)
8.9.8 Firewall reporting

By default, the firewall on an endpoint computer reports state changes, events, and errors to Sophos Enterprise 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 Sophos Enterprise Console. In that case, you can choose not to send "differs from policy" alerts to Sophos Enterprise Console when you make changes to certain parts of your firewall configuration.

Firewall events

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

You can prevent the firewall from reporting events to Sophos Enterprise Console.

Related tasks

Turn reporting of local changes on or off (page 144)
Turn off reporting of unknown network traffic (page 145)

Turn reporting of local changes on or off

If you use role-based administration:

• You must have the Policy setting - firewall right to configure a firewall policy.
• You cannot edit a policy if it is applied outside your active sub-estate.

If the firewall configuration on endpoint computers differs from policy, you can turn reporting of local changes off.

Note

This option is not supported on Windows 8 and later.

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

If the firewall configuration on endpoint computers is intended to conform to policy, you should turn reporting of local changes on.
To turn reporting of local changes off:

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the General tab.
5. Under Reporting, do one of the following:
   • To turn reporting of local changes on, select 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, clear the Display an alert in the management console if local changes are made to the global rules, applications, processes or checksums check box.

Related concepts
Managing roles and sub-estates (page 15)

Turn off reporting of unknown network traffic

If you use role-based administration:

- You must have the Policy setting - firewall right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can prevent the firewall on endpoint computers from reporting unknown network traffic to Sophos Enterprise Console. The firewall regards traffic as unknown if there is no rule for it.

To prevent the firewall on endpoint computers from reporting unknown network traffic to Sophos Enterprise Console:

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the General tab.
5. Under Blocking, select the Use checksums to authenticate applications check box.
6. Under Reporting, clear the Report unknown applications and traffic to the management console check box.

Related concepts
Managing roles and sub-estates (page 15)

Turn off reporting of firewall errors

**CAUTION**
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 on endpoint computers from reporting errors to Enterprise Console:

1. Double-click the firewall policy you want to change.
2. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
3. Under Configurations, click Configure next to the location for which you want to configure the firewall.
4. Click the General tab.
5. Under Reporting, clear the Report errors to the management console check box.

8.9.9 Import or export firewall configuration

If you use role-based administration:

- You must have the Policy setting - firewall right to configure a firewall policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can import or export the firewall general settings and rules as a configuration file (*.conf). You can use this feature to do the following:

- Back up and restore your firewall configuration.
- Import application rules created on one computer and use them to create a policy for other computers running the same set of applications.
- Merge configurations created on several different computers to create a policy that is valid for one or more groups of computers on the network.

To import or export firewall configuration:

1. Check which firewall policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Firewall, and then double-click the policy you want to import to or export from.
3. On the Welcome page of the Firewall Policy wizard, click Advanced firewall policy.
4. In the Firewall Policy dialog box, on the General tab, under Managing configuration, click Import or Export.

Related concepts
Managing roles and sub-estates (page 15)

8.10 Application control policy

Sophos Enterprise Console enables you to detect and block "controlled applications", that is, legitimate applications that are not a security threat, but that you decide are unsuitable for use in your office environment. Such applications may include instant messaging (IM) clients, Voice over Internet Protocol (VoIP) clients, digital imaging software, media players, or browser plug-ins.

**Warning**
This option applies only to Sophos Endpoint Security and Control for Windows.

Applications can be blocked or authorized for different groups of computers with complete flexibility. For example, VoIP can be switched off for office-based desktop computers, yet authorized for remote computers.

The list of controlled applications is supplied by Sophos and updated regularly. You cannot add new applications to the list, but you can submit a request to Sophos to include a new legitimate application you would like to control on your network, see knowledge base article 63656.
This section describes how to select the applications you want to control on your network and set up scanning for controlled applications.

If you use role-based administration:

- You must have the **Policy setting - application control** right to configure an application control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

### Application control events

When an application control event occurs, for example, a controlled application has been detected on the network, the event is written in the application control event log that can be viewed from Sophos Enterprise Console.

The number of computers with events over a specified threshold within the last seven days is displayed on the Dashboard.

You can also set up alerts to be sent to your chosen recipients when an application control event has occurred.

**Related concepts**

- Managing roles and sub-estates (page 15)

**Related tasks**

- View application control events (page 198)
- Set up application control alerts and messages (page 191)

You can send messages to specific users when a controlled application is found.

**Related information**

- knowledge base article 63656

### 8.10.1 Select the applications you want to control

By default, all applications are allowed. You can select the applications you want to control.

If you use role-based administration:

- You must have the **Policy setting - application control** right to configure an application control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To control applications:

1. Check which application control policy is used by the group(s) of computers you want to configure.
2. In the **Policies** pane, double-click **Application control**. Then double-click the policy you want to change.
3. In the **Application control policy** dialog box, click the **Authorization** tab.
4. Select an **Application type**, for example, **File sharing**.

A full list of the applications included in that group is displayed in the **Authorized** list below.

- To block an application, select it and move it to the **Blocked** list by clicking the “Add” button.

- To block any new applications that Sophos adds to that type in the future, move **All added by Sophos in the future** to the **Blocked** list.
To block all applications of that type, move all applications from the **Authorized** list to the **Blocked** list by clicking the “Add all” button.

5. On the **Scanning** tab of the **Application control policy** dialog box, make sure that scanning for controlled applications is enabled. Click **OK**.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)
- Scan for applications you want to control (page 148)

### 8.10.2 Scan for applications you want to control

If you use role-based administration:

- You must have the **Policy setting - application control** right to configure an application control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can configure Sophos Endpoint Security and Control to scan for applications you want to control on your network on access.

1. Check which application control policy is used by the group(s) of computers you want to configure.
2. In the **Policies** pane, double-click **Application control**. Then double-click the policy you want to change.

   The **Application control policy** dialog box is displayed.

3. On the **Scanning** tab, set the options as follows:
   - To enable on-access scanning, select the **Enable on-access scanning** check box. If you want to detect applications but do not want to block them on access, select the **Detect but allow to run** check box.
   - To enable on-demand and scheduled scanning, select the **Enable on-demand and scheduled scanning** check box.

   **Warning**
   - Your anti-virus and HIPS policy settings determine which files are scanned (that is, the extensions and exclusions).

You can also have alerts sent to specific users if a controlled application is found on any of the computers in the group.

**Related concepts**
- Managing roles and sub-estates (page 15)
- Uninstall controlled applications you do not want (page 149)

**Related tasks**
- Check which policies a group uses (page 27)
- Set up application control alerts and messages (page 191)
You can send messages to specific users when a controlled application is found.

8.10.3 Uninstall controlled applications you do not want

Before you uninstall controlled applications, ensure that on-access scanning for controlled applications is disabled. This type of scanning blocks the programs used to install and uninstall applications, so it may interfere with uninstallation.

You can remove an application in one of two ways:

- Go to each computer and run the uninstaller for that product. You can usually do this by opening the Windows Control Panel and using Add/Remove Programs.
- At the server, use your usual script or administration tool to run the uninstaller for that product on your networked computers.

Now you can enable on-access scanning for controlled applications.

8.11 Data control policy

**Note**

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

Data control enables you to reduce accidental data loss from workstations by monitoring and restricting the transfer of files containing sensitive data. You do this by creating data control rules and then adding the rules to the Data control policies.

You can monitor and control the transfer of files to specified storage devices (e.g. removable storage device or optical drive) or by specified applications (e.g. email client or web browser).

To enable you to quickly define and roll out a data control policy, SophosLabs maintain a library of sensitive data definitions (Content Control Lists). The main focus for this library is personally identifiable information, but it also covers other common data structures. You can use Content Control Lists in Sophos Enterprise Console, as described further in this section.

**Related information**

Sophos product comparison

8.11.1 How does data control work?

Data control identifies accidental data loss that is typically caused by employees mishandling sensitive data. For example, a user sends a file containing sensitive data home via web-based email.

Data control enables you to monitor and control the transfer of files from computers to storage devices and applications connected to the internet.

- **Storage devices**: Data control intercepts all files copied onto monitored storage devices using Windows Explorer (this includes the Windows desktop). However, direct saves from within applications, such as Microsoft Word, or transfers made using the command prompt are not intercepted.

  It is possible to force all transfers onto monitored storage devices to be made using Windows Explorer by using either the **Allow transfer on acceptance by user and log event** action or the **Block transfer and log event** action. In either case, any attempt to save directly from within
an application or transfer files using the command prompt are blocked by data control, and a
desktop alert is displayed to the user requesting that they use Windows Explorer to complete the
transfer.

When a data control policy only contains rules with the **Allow file transfer and log event** action, direct saves from within applications and transfers using the command prompt are
not intercepted. This behavior enables users to use storage devices without any restrictions.
However, data control events are still logged for transfers made using Windows Explorer.

**Note**
This restriction does not apply to application monitoring.

- **Applications**: To ensure only file uploads by users are monitored, some system file locations are
  excluded from data control monitoring. This significantly reduces the risk of data control events
  being generated by applications opening configuration files as opposed to users uploading files.

**Note**
If you experience erroneous events generated by an application opening configuration files, the
problem can usually be solved by adding custom location exclusions or by configuring a data
control rule to be less sensitive. For more information, see [knowledge base article 113024](#).

**Note**
On-access scanning exclusions do not always apply to data control.

**When does data control use on-access scanning exclusions?**

Depending on how and where you copy or move files, data control may or may not take into account
the on-access scanning exclusions you have set up in the anti-virus and HIPS policy.

Data control uses on-access scanning exclusions when files are uploaded or attached using a
monitored application, for example, an email client, a web browser, or an instant messaging (IM)
client.

**Restriction**
If you have excluded remote files from on-access scanning, data control won’t scan files that you
upload or attach from a network location to a monitored application, for example, email or web
browser.

Data control doesn’t use on-access scanning exclusions when files are copied or moved using
Windows Explorer. So the exclusions won’t work, for example, if you copy files to a storage device
such as a USB, or copy or move files to a network location. All files will be scanned, even though you
may have excluded remote files from on-access scanning.

**Note**
If you are copying or moving archive files to a network location, the process may take some time,
for example over a minute per 100 MB of data, depending on your network connection. This is
because scanning of archive files takes longer than scanning of non-archived files.
Data control policies

Data control enables you to monitor and control the transfer of files by defining data control policies and applying them to groups of computers on your network.

**Restriction**

Data control is not supported on Windows 2008 Server Core and must be disabled on computers running this operating system. To exclude Windows 2008 Server Core computers from data control scanning, put them in a group that has a data control policy with data control scanning disabled.

Data control policies include one or more rules that specify conditions and actions to be taken when the rule is matched. A data control rule can be included in multiple policies. When a data control policy contains several rules, a file that matches any of the rules in the data control policy violates the policy.

Data control rule conditions

The data control rule conditions include destination, file name and extension, file type, or file content. Destination includes devices (for example, removable storage devices, such as USB flash drives) and applications (for example, internet browsers and email clients).

The matching of file content is defined using a Content Control List. This is an XML based description of structured data. SophosLabs provide an extensive set of Content Control Lists which can be used within your data control rules.
Data control rule actions

When data control detects all the conditions specified in a rule, the rule is matched, and data control takes the action specified in the rule and logs the event. You can specify one of the following actions:

- Allow file transfer and log event
- Allow transfer on acceptance by user and log event
- Block transfer and log event

If a file matches two data control rules that specify different actions, the rule that specifies the most restrictive action is applied. Data control rules that block file transfer take priority over the rules that allow file transfer on user acceptance. Rules that allow file transfer on user acceptance take priority over the rules that allow file transfer.

By default, when the rule is matched and file transfer is blocked or user confirmation of file transfer is required, a message is displayed on the endpoint computer's desktop. The rule that has been matched is included in the message. You can add your own custom messages to the standard messages for user confirmation of file transfer and for blocked file transfer.

Related concepts
Data control does not scan uploaded or attached files (page 229)
About data control rules (page 152)
About Content Control Lists (page 153)

Related tasks
Exclude items from on-access scanning (page 92)
Turn data control on or off (page 154)

By default, data control is turned off and no rules are specified to monitor or restrict the transfer of files over the network.

Set up data control alerts and messages (page 192)
Sophos Enterprise Console uses events and messages to report when the transfer of sensitive data is detected or blocked.

Related information
knowledge base article 113024

8.11.2 About data control rules

Data control rules specify conditions for data control scanning to detect, actions to be taken if rules are matched, and any files to be excluded from scanning.

You can create your own rules or use the sample rules provided. We provide a number of preconfigured data control rules that you can use unmodified or customize to your own needs. These rules are provided as examples only and are not updated.

There are two types of data control rule: file matching rule and content rule.

File matching rules

A file matching rule specifies action to be taken if a user attempts to transfer a file with the specified file name or of the specified file type (true file type category, e.g. a spreadsheet) to the specified destination, for example, block the transfer of databases to removable storage devices.
Data control includes true file type definitions for over 150 different file formats. We may add additional true file types from time to time. The newly added types will be automatically added to any data control rules that use the relevant true file type category.

File types not covered by a true file type definition can be identified using their file extensions.

Content rules

A content rule is a rule that contains one or more Content Control Lists and specifies action to be taken if a user attempts to transfer data that matches all the Content Control Lists in the rule to the specified destination.

8.11.3 About Content Control Lists

A Content Control List (CCL) is a set of conditions that describe structured file content. A Content Control List may describe a single type of data (for example, a postal address or social security number) or a combination of data types (for example, a project name near to the term "confidential").

You can use SophosLabs Content Control Lists that are provided by Sophos or create your own Content Control Lists.

SophosLabs Content Control Lists provide expert definitions for common financial and personally identifiable data types, for example, credit card numbers, social security numbers, postal addresses, or email addresses. Advanced techniques, such as checksums, are used in SophosLabs Content Control Lists to increase the accuracy of sensitive data detection.

You can’t edit SophosLabs Content Control Lists, but you can submit a request to Sophos to create a new SophosLabs Content Control List. For details, see knowledge base article 51976.

Note

Double-byte characters (for example, Japanese or Chinese characters) are not officially supported in the current version of Content Control Lists. However, you can enter double-byte characters in the Content Control List editor.

Setting up the quantity for SophosLabs Content Control Lists

Most SophosLabs Content Control Lists have quantity assigned to them.

A quantity is the volume of the Content Control List key data type that must be found in a file before the Content Control List is matched. You can edit the quantity of a SophosLabs Content Control List in a content rule that includes that Content Control List.

Using quantity, you can fine-tune your data control rules and avoid blocking documents that do not contain sensitive information (for example, a document containing one postal address or one or two telephone numbers, possibly in the letterhead, footer or signature). If you search for a single postal address, thousands of documents may match the rule and trigger a data control event. However, if you want to prevent the loss of a customer list, you may want to only detect the transfer of documents containing, for example, more than 50 postal addresses. In other cases, however, it may be advisable to search for a single instance of content, for example, a credit card number.

Related information
knowledge base article 51976
8.11.4 About data control events

When a data control event occurs, for example, the copying of a file containing sensitive data to a USB flash drive, the event is sent to Sophos Enterprise Console and can be viewed in the Data Control - Event Viewer. The event is also logged locally on the endpoint computer and can be viewed, with the appropriate permissions, in Sophos Endpoint Security and Control.

**Note**
An endpoint computer can send to Sophos Enterprise Console a maximum of 50 data control events per hour. All events are logged locally on the endpoint computer.

In the Data Control - Event Viewer dialog box, you can use filters to display only the events you are interested in. You can also export the list of data control events to a file.

The number of computers with data control events over a specified threshold within the last seven days is displayed on the Dashboard.

You can also set up alerts to be sent to your chosen recipients when a data control event has occurred.

**Related concepts**
About data control events (page 154)

**Related tasks**
Export the list of events to a file (page 206)
Set up data control alerts and messages (page 192)

Sophos Enterprise Console uses events and messages to report when the transfer of sensitive data is detected or blocked.

**Related reference**
Dashboard panels (page 6)

8.11.5 Turn data control on or off

By default, data control is turned off and no rules are specified to monitor or restrict the transfer of files over the network.

If you use role-based administration:

- You must have the **Policy setting - data control** right to configure a data control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To turn data control on:

1. Check which data control policy is used by the group or groups of computers you want to configure.
2. In the Policies pane, double-click **Data control**. Then double-click the policy you want to change. The Data control policy dialog box is displayed.
3. On the Policy Rules tab, select the **Enable data control scanning** check box.
4. Click the Add Rule button. In the Data Control Rule Management dialog box, select the rules you want to add to the policy and click **OK**.
Note
If you do not add any data control rules, data control will not monitor or restrict the transfer of files until you do so.

If you later want to disable data control scanning, clear the Enable data control scanning check box.

Related concepts
Data control policy (page 149)

Related tasks
Check which policies a group uses (page 27)

8.11.6 Create a file matching rule

If you use role-based administration:

- You must have the Data control customization right to create or edit data control rules.
- You must have the Policy setting - data control right to set up data control policies.
- You cannot edit a policy if it is applied outside your active sub-estate.

To create a file matching rule and add it to a data control policy:

1. Check which data control policy is used by the group or groups of computers you want to configure.
   a) Alternatively, you can create a rule from the Tools menu and add it to a policy or policies later.
      On the Tools menu, point to Manage Data Control, and then click Data control rules and perform steps 4 to 10.
2. In the Policies pane, double-click Data control. Then double-click the policy you want to change.
3. In the Data control policy dialog box, on the Policy Rules tab, make sure the Enable data control scanning check box is selected and click Manage Rules.
4. In the Data Control Rule Management dialog box, click the Add File Matching Rule button.
5. In the Create a File Matching Rule dialog box, under Rule name, type a name for the rule.
6. Under Rule description (optional), enter the rule’s description, if you wish.
7. Under Select the rule’s conditions, select conditions for the rule.
   The destination condition is preselected and must be included in the rule.
   By default, all file types are scanned. If you want to scan only certain file types, select Where the file type is. You can then set up this condition as described in step 10.
8. Under Select the action to take if the rule is matched, select the action.
9. If you want to exclude some files from data control scanning, under Select files to exclude, select the Where file name matches or Where the file type is check box.
10. Under Rule content, click each underlined value and set up the rule’s conditions.
    For example, if you click Select destination, the Match Destination Type Condition dialog box opens, where you can select the devices and/or applications to which you want to restrict the transfer of data.
    a) Select or enter conditions for each underlined value.
b) Click **OK**.

The new rule appears in the **Data Control Rule Management** dialog box.

11. To add the rule to the policy, select the check box next to the rule's name and click **OK**.

The rule is added to the data control policy.

You can set up alerts and messages that will be sent to the user when a rule in the data control policy is matched.

**Related concepts**
- Managing roles and sub-estates (page 15)
- About data control rules (page 152)

**Related tasks**
- Check which policies a group uses (page 27)
- Set up data control alerts and messages (page 192)
Sophos Enterprise Console uses events and messages to report when the transfer of sensitive data is detected or blocked.

8.11.7 Create a content rule

If you use role-based administration:

- You must have the **Data control customization** right to create or edit data control rules and Content Control Lists.
- You must have the **Policy setting - data control** right to set up data control policies.
- You can't edit a policy if it is applied outside your active sub-estate.

To create a content rule and add it to a data control policy:

1. Check which data control policy is used by the group or groups of computers you want to configure.
   Alternately, you can create a rule from the **Tools** menu and add it to a policy or policies later. On the **Tools** menu, point to **Manage Data Control**, and then click **Data control rules** and perform steps 4 to 13.
2. In the **Policies** pane, double-click **Data control**. Then double-click the policy you want to change.
3. In the **Data control policy** dialog box, on the **Policy Rules** tab, make sure the **Enable data control scanning** check box is selected and click **Manage Rules**.
4. In the **Data Control Rule Management** dialog box, click the **Add Content Rule** button.
5. In the **Create a Content Rule** dialog box, under **Rule name**, type a name for the rule.
6. Under **Rule description (optional)**, enter the rule's description, if you wish.
7. Under **Select the rule's conditions**, the file content and destination conditions are already selected. You must set up both conditions for a content rule.
8. Under **Select the action to take if the rule is matched**, select the action.
9. If you want to exclude some files from data control scanning, under **Select files to exclude**, select the **Where file name matches** or **Where the file type is** check box.
10. Under **Rule content**, click the “select file content” underlined value.
11. In the **Content Control List Management** dialog box, select the Content Control Lists you want to include in the rule.
   - If you want to add SophosLabs Content Control Lists, select one for each country you need.

   **Tip**
   Do not select a global Content Control List if you do not need support for all countries. Instead, select Content Control Lists only for the countries you need. This can significantly reduce scanning time as well as reduce the risk of unwanted, coincidental matches.

   - Create a new Content Control List.
     a) Click **OK**.
12. If you want to change quantity assigned to a SophosLabs Content Control List, under **Rule content**, click the “quantity” underlined value (“n or more matches”) that you want to change. In the **Quantity editor** dialog box, enter a new quantity.
13. Under **Rule content**, select or enter conditions for the rest of the underlined values.
a) Click OK.

The new rule appears in the Data Control Rule Management dialog box.

14. To add the rule to the policy, select the check box next to the rule’s name and click OK.

The rule is added to the data control policy.

You can set up alerts and messages that will be sent to the user when a rule in the data control policy is matched.

Related concepts
Managing roles and sub-estates (page 15)
About Content Control Lists (page 153)

Related tasks
Check which policies a group uses (page 27)
Create or edit a simple Content Control List (page 161)
Create or edit an advanced Content Control List (page 162)
Set up data control alerts and messages (page 192)
Sophos Enterprise Console uses events and messages to report when the transfer of sensitive data is detected or blocked.

### 8.11.8 Add a data control rule to a policy

You can add data control rules to policies.

If you use role-based administration:
- You must have the **Policy setting - data control** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

To add a data control rule to a policy:
1. Check which data control policy is used by the group or groups of computers you want to configure.
2. In the **Policies** pane, double-click **Data control**. Then double-click the policy you want to change. The **Data control policy** dialog box is displayed.
3. On the **Policy Rules** tab, click **Add Rule**. The **Data Control Rule Management** dialog box is displayed.
4. Select the rules you want to add to the policy and click **OK**.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

### 8.11.9 Remove a data control rule from a policy

If you use role-based administration:
- You must have the **Policy setting - data control** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

To remove a data control rule from a policy:
1. Check which data control policy is used by the group or groups of computers you want to configure.
2. In the **Policies** pane, double-click **Data control**. Then double-click the policy you want to change. The **Data control policy** dialog box is displayed.
3. On the **Policy Rules** tab, select the rule you want to remove and click **Remove Rule**.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Check which policies a group uses (page 27)

### 8.11.10 Exclude files or file types from data control

If you use role-based administration, you must have the **Data control customization** right to exclude files from data control.

You can exclude files and file types from data control by setting up exclusions in a data control rule.
To exclude a file or file type from data control, exclude it in a rule with the highest priority (that is, specifying the most restrictive action).

To exclude files or file types from data control:

1. On the **Tools** menu, point to **Manage Data Control**, and then click **Data Control Rules**.
2. In the **Data Control Rule Management** dialog box, select the rule you want to edit and click **Edit**, or create a new rule by clicking the **Add file matching rule** or **Add content rule** button.
3. To exclude files from data control, in the **Rule Editor** dialog box, under **Select files to exclude**, select the **Where file name matches** check box.
4. Under **Rule content**, click the underlined value to specify excluded file names.
5. In the **Exclude File Name Condition** dialog box, click **Add** and specify the names of the files you want to exclude.

You can use the wildcards * and ?

The wildcard ? can be used only in a filename or extension. It generally matches any single character. However, when used at the end of a filename or extension, it matches any single character or no characters. For example file???.txt matches file.txt, file1.txt and file12.txt but not file123.txt.

The wildcard * can be used only in a filename or extension, in the form [filename].* or *. [extension]. For example, file*.txt, file.txt* and file.*,txt are invalid.
6. To exclude file types from data control, in the **Rule Editor** dialog box, under **Select files to exclude**, select the **Where the file type is** check box.
7. Under **Rule content**, click the underlined value to specify excluded file types.
8. In the **Exclude File Type Condition** dialog box, select the file types you want to exclude and click **OK**.

**Related concepts**

Managing roles and sub-estates (page 15)

### 8.11.11 Import or export a data control rule

If you use role-based administration, you must have the **Data control customization** right to import or export a data control rule.

Data control rules can be imported into or exported from Sophos Enterprise Console as XML files.

To import or export a data control rule:

1. On the **Tools** menu, point to **Manage Data Control**, and then click **Data control rules**.
2. In the **Data Control Rule Management** dialog box, click **Import** or **Export**.
   - If you want to import a rule, in the **Import** dialog box, browse to the rule you want to import, select it and click **Open**.
   - If you want to export a rule, in the **Export** dialog box, browse to select a destination for the file, type a name for the file and click **Save**.

**Related concepts**

Managing roles and sub-estates (page 15)
8.11.12 Create or edit a simple Content Control List

If you use role-based administration, you must have the **Data control customization** right to create a Content Control List.

To create or edit a Content Control List:

1. On the **Tools** menu, point to **Manage Data Control**, and then click **Data Control Content Control Lists**.
2. In the **Content Control List Management** dialog box, click **Add** to create a new Content Control List, or select an existing Content Control List and click **Edit**.
3. In the **Add Content Control List** dialog box, in the **Name** field, enter a name for the Content Control List.
4. In the **Description** field, enter a description for the Content Control List, if you wish.
5. If you want to add tags or edit the tags assigned to the Content Control List, click **Change** next to the **Tags** field.
   
   You can assign tags to identify the Content Control List's type and region where it applies.
6. In the **Edit Content Control List Tags** dialog box, in the **Available tags** list, select the tags you want to assign and move them to the **Selected tags** list. Click **OK**.
7. In the **Scan for content matching** section, select a search condition (“Any of these terms”, “All of these terms”, or “Exactly this phrase”) and enter the search terms you want to find in documents, separated by a space. Click **OK**.

   **Note**
   The search is case insensitive.

   Quotation marks are not supported in simple Content Control Lists. Use the “Exactly this phrase” condition to scan for an exact phrase.

   To create more complex expressions, use the advanced Content Control List editor.

The new content control list appears in the **Content Control List Management** dialog box.

**Examples**

<table>
<thead>
<tr>
<th>Search condition</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match any term</td>
<td>confidential secret</td>
<td>Matches documents containing either “confidential” or “secret”.</td>
</tr>
<tr>
<td>Match all terms</td>
<td>project confidential</td>
<td>Matches documents containing both ”project” and ”confidential”.</td>
</tr>
<tr>
<td>Exact match</td>
<td>for internal use only</td>
<td>Matches documents containing the phrase ”for internal use only”.</td>
</tr>
</tbody>
</table>

Now you can add the new Content Control List to a content rule.

Managing roles and sub-estates (page 15) About Content Control Lists (page 153) Create or edit an advanced Content Control List (page 162)
8.11.13 Create or edit an advanced Content Control List

If you use role-based administration, you must have the **Data control customization** right to create a Content Control List.

You can create a Content Control List that consists of one or more regular expressions and a trigger score. To do this, use the advanced editor.

To create or edit a Content Control List using the advanced editor:

1. On the **Tools** menu, point to **Manage Data Control**, and then click **Data Control Content Control Lists**.
2. In the **Content Control List Management** dialog box, click **Add** to create a new Content Control List, or select an existing Content Control List and click **Edit**.
3. In the **Add Content Control List** dialog box, in the **Name** field, enter a name for the Content Control List.
4. In the **Description** field, enter a description for the Content Control List, if you wish.
5. If you want to add tags or edit the tags assigned to the Content Control List, click **Change** next to the **Tags** field.

   You can assign tags to identify the Content Control List's type and region where it applies.
6. In the **Edit Content Control List Tags** dialog box, in the **Available tags** list, select the tags you want to assign and move them to the **Selected tags** list. Click **OK**.
7. Click the **Advanced** button.
8. In the **Advanced** pane, click **Create** to create a new expression, or select an existing expression and click **Edit**.
9. In the **Content Control List - Advanced** dialog box, enter a Perl 5 regular expression.

   For a description of Perl 5 regular expressions, refer to Perl documentation or go to **Perl syntax**.
10. In the **Expression score** field, enter the number that will be added to the total score for a Content Control List when the regular expression is matched.
11. In the **Maximum count** field, enter the maximum number of matches for the regular expression that can be counted towards the total score.

    For example, an expression with the score of 5 and the maximum count of 2 can add the maximum of 10 to the total score of the Content Control List. If the expression is found 3 times, it still adds 10 to the total score.

   a) Click **OK**.
12. Repeat steps 5 to 11 if you want to add more regular expressions to the Content Control List.
13. In the **Trigger score** field, enter the number of times a regular expression must be matched before the Content Control List is matched.

    For example, consider a Content Control List that has the trigger score of 8 and consists of 3 expressions (A, B, and C) with the following scores and maximum counts:

```
<table>
<thead>
<tr>
<th>Expression</th>
<th>Score</th>
<th>Maximum count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expression A</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Expression B</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Expression C</td>
<td>1</td>
<td>5</td>
</tr>
</tbody>
</table>
```
This Content Control List is matched if data control finds 2 matches of expression A or 1 match of expression A and 1 match of expression B, or 1 match of expression B and 5 matches of expression C.

Click OK.

The new Content Control List appears in the **Content Control List Management** dialog box.

**Regular expression example**

```
(?i)\b[a-ceghj-npr-tw-z][a-ceghj-npr-tw-z]\s?\d{2}\s?\d{2}\s?\d{2}\s?[abcd]?\b
```

This regular expression matches UK National Insurance numbers, for example, AA 11 11 11 A.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>(?i)</code></td>
<td>Makes the match case-insensitive.</td>
</tr>
<tr>
<td><code>\b</code></td>
<td>Matches a boundary between a word character and a non-word character.</td>
</tr>
<tr>
<td><code>[a-ceghj-npr-tw-z]</code></td>
<td>Matches any single character in the range of characters (A to C E G H J to N P R to T W to Z).</td>
</tr>
<tr>
<td><code>?</code></td>
<td>Matches the preceding element zero or one time.</td>
</tr>
<tr>
<td><code>\s?</code></td>
<td>Matches zero or one whitespace.</td>
</tr>
<tr>
<td><code>\d{2}</code></td>
<td>Matches two digits.</td>
</tr>
<tr>
<td><code>[abcd]</code></td>
<td>Matches any single character from the list (A, B, C, or D).</td>
</tr>
</tbody>
</table>

Now you can add the new Content Control List to a content rule.

**Related concepts**

- Managing roles and sub-estates (page 15)
- About Content Control Lists (page 153)

**Related information**

- Perl syntax

**8.11.14 Import or export a Content Control List**

If you use role-based administration, you must have the **Data control customization** right to import or export a Content Control List.

Content Control Lists can be imported into or exported from Sophos Enterprise Console as XML files. You can share Content Control Lists between Sophos products that support them.

**Note**

- SophosLabs Content Control Lists cannot be exported.

To import or export a Content Control List:
1. On the **Tools** menu, point to **Manage Data Control**, and then click **Data control content control lists**.

2. In the **Content Control List Management** dialog box, click **Import** or **Export**.
   - If you want to import a Content Control List, in the **Import** dialog box, browse to the Content Control List you want to import, select it and click **Open**.
   - If you want to export a Content Control List, in the **Export** dialog box, browse to select a destination for the file, type a name for the file and click **Save**.

**Related concepts**

*Managing roles and sub-estates* (page 15)

## 8.12 Device control policy

**Note**

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

**Warning**

Sophos device control should not be deployed alongside device control software from other vendors.

Device control enables you to prevent users from using unauthorized external hardware devices, removable storage media, and wireless connection technologies on their computers. This can help to significantly reduce your exposure to accidental data loss and restrict the ability of users to introduce software from outside of your network environment.

Removable storage devices, optical disk drives, and floppy disk drives can also be set to provide read-only access.

Using device control, you can also significantly reduce the risk of network bridging between a corporate network and a non-corporate network. The **Block bridged** mode is available for both wireless and modem types of device. 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.

By default, device control is turned off and all devices are allowed.

If you want to enable device control for the first time, we recommend that you:

- Select device types to control.
- Detect devices without blocking them.
- Use device control events to decide which device types to block and which, if any, devices should be exempt.
- Detect and block devices or allow read-only access to storage devices.

For more information about the recommended settings for device control, see the Sophos Enterprise Console policy setup guide.

If you use role-based administration:

- You must have the **Policy setting - device control** right to configure a device control policy.
- You can't edit a policy if it is applied outside your active sub-estate.
8.12.1 About device control events

When a device control event occurs, for example, a removable storage device has been blocked, the event is sent to Sophos Enterprise Console and can be viewed in the Device Control - Event Viewer dialog box.

Note
If you set optical disk drives to "Read only", events for these disk drives are not sent to Sophos Enterprise Console or logged locally. This prevents unwanted reports of events.

In the Device Control - Event Viewer dialog box, you can use filters to display only the events you are interested in. You can also export the list of device control events to a file.

You can use device control events to add exemptions for specific devices or device models to the device control policies.

The number of computers with device control events over a specified threshold within the last seven days is displayed on the Dashboard.

You can also set up alerts to be sent to your chosen recipients when a device control event has occurred.

8.12.2 What types of device can be 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 knowledge base 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).

**Related information**
knowledge base article 63102

### 8.12.3 Select device types to control

You can control which device types are allowed on your network.

If you use role-based administration:
- You must have the **Policy setting - device control** right to edit a device control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.
Note
You should not block Wi-Fi connections on computers that are managed by Sophos Enterprise Console using Wi-Fi.

To control devices:

1. Check which device control policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Device control. Then double-click the policy you want to change.
3. In the Device control policy dialog box, on the Configuration tab, under Storage, select the type of storage device you want to control.
4. Click in the Status column next to the device type, and then click the drop-down arrow that appears. Select the type of access that you want to allow.
   By default, devices have full access. For removable storage devices, optical disk drives and floppy disk drives, you can change that to “Blocked” or “Read only.” For secure removable storage devices, you can change that to “Blocked.”
5. Under Network, select the type of network device you want to block.
6. Click in the Status column next to the type of network device, and then click the drop-down arrow that appears.
   - Select “Blocked” if you want to block the device type.
   - Select “Block bridged” if you want to prevent network bridging between a corporate network and a non-corporate network. The device type will be blocked when an endpoint is connected to a physical network (typically through an Ethernet connection). Once the endpoint is disconnected from the physical network, the device type will be re-enabled.
7. Under Short Range, select the type of short-range device you want to block. In the Status column next to the device type, select “Blocked.”
   a) Click OK.
8. To block media devices that connect to a computer using Media Transfer Protocol (MTP) or Picture Transfer Protocol (PTP), such as mobile phones, tablets, digital cameras or media players, under Media, select MTP/PTP. In the Status column, select “Blocked.”

Related concepts
Managing roles and sub-estates (page 15)
Related tasks
Check which policies a group uses (page 27)

8.12.4 Detect devices without blocking them

If you use role-based administration:

- You must have the Policy setting - device control right to edit a device control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

You can detect devices without blocking them. This is useful if you intend to block devices in future, but want to detect and exempt the devices you need first.

To detect devices without blocking them, enable device control scanning in a device control policy and turn on the detection-only mode. Change the status of the devices you want to detect to “Blocked.” This will generate events for devices used on endpoint computers when the policy would have been infringed, but the devices will not be blocked.
To detect devices without blocking them:
1. Check which device control policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Device control. Then double-click the policy you want to change.
3. In the Device control policy dialog box, on the Configuration tab, select Enable device control scanning.
4. Select Detect but do not block devices.
5. If you haven’t done so already, change the status of devices you want to detect to “Blocked.”
   a) Click OK.

Related concepts
Managing roles and sub-estates (page 15)
About device control events (page 165)

Related tasks
Check which policies a group uses (page 27)
Select device types to control (page 166)

You can control which device types are allowed on your network.

8.12.5 Detect and block devices

If you use role-based administration:
• You must have the Policy setting - device control right to edit a device control policy.
• You cannot edit a policy if it is applied outside your active sub-estate.
1. Check which device control policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Device control. Then double-click the policy you want to change.
3. In the Device control policy dialog box, on the Configuration tab, select the Enable device control scanning check box.
4. Clear the Detect but do not block devices check box.
5. If you haven’t done so already, change the status of devices you want to block to “Blocked.”
   a) Click OK.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)
Select the applications you want to control (page 147)

By default, all applications are allowed. You can select the applications you want to control.

8.12.6 Exempt a device from all policies

If you use role-based administration:
• You must have the Policy setting - device control right to edit a device control policy.
• You cannot edit a policy if it is applied outside your active sub-estate.
You can exempt a device from all policies, including the default one. That exception will then be added to all new policies you create.

You can exempt a device instance ("this device only") or a specific device model ("all devices with this model ID"). Do not set multiple exemptions for the same device at both the model ID and device instance levels. If both are defined, the device instance level will take precedence.

To exempt a device from all device control policies:

1. On the Events menu, click Device Control Events. The Device Control - Event Viewer dialog box appears.
2. If you want to display only certain events, in the Search criteria pane, set the filters as appropriate and click Search to display the events.
3. Select the entry for the device that you want to exempt from the policies, and then click Exempt Device.
   The Exempt device dialog box appears. Under Device details, you see the type, model, model ID and device ID of the device. Under Exemption details > Scope, you see the words "All policies."

Note
If there is no event for the device you want to exempt, for example, an integral CD or DVD drive on an endpoint computer, go to the computer containing the device and enable the device in the Device Manager. (To access Device Manager, right-click My Computer, click Manage, and then click Device Manager.) This will generate a new “block” event that will appear in the Device Control - Event Viewer dialog box. You can then exempt the device as described earlier in this step.

4. Select whether you want to exempt this device only or all devices with this model ID.
5. Select whether you want to allow full access or read-only access to the device.
6. In the Comment field, enter a comment, if you wish. For example, you can specify who requested to exempt the device.
7. Click OK.

Related concepts
Managing roles and sub-estates (page 15)
About device control events (page 165)
Related tasks
Check which policies a group uses (page 27)

8.12.7 Exempt a device from a single policy

If you use role-based administration:

• You must have the Policy setting - device control right to edit a device control policy.
• You cannot edit a policy if it is applied outside your active sub-estate.

You can exempt a specific device from a device control policy.

You can exempt a device instance ("this device only") or a specific device model ("all devices with this model ID"). Do not set multiple exemptions for the same device at both the model ID and device instance levels. If both are defined, the device instance level will take precedence.

To exempt a device from a policy:
1. Check which device control policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Device control. Then double-click the policy you want to change.
3. In the Device control policy dialog box, on the Configuration tab, click Add exemption. The Device Control - Event Viewer dialog box appears.
4. If you want to display only certain events, in the Search criteria pane, set the filters as appropriate and click Search to display the events.
5. Select the entry for the device that you want to exempt from the policy, and then click Exempt Device.
   The Exempt device dialog box appears. Under Device details, you see the type, model, model ID and device ID of the device. Under Exemption details, Scope, you see the words “This policy only.”

   **Note**
   If there is no event for the device you want to exempt, for example, an integral CD or DVD drive on an endpoint computer, go to the computer containing the device and enable the device in the Device Manager. (To access Device Manager, right-click My Computer, click Manage, and then click Device Manager.) This will generate a new “block” event that will appear in the Device Control - Event Viewer dialog box. You can then exempt the device as described earlier in this step.

6. Select whether you want to exempt this device only or all devices with this model ID.
7. Select whether you want to allow full access or read-only access to the device.
8. In the Comment field, enter a comment, if you wish. For example, you can specify who requested to exempt the device.
9. Click OK.

**Related concepts**
Managing roles and sub-estates (page 15)
About device control events (page 165)

**Related tasks**
Check which policies a group uses (page 27)

### 8.12.8 View or edit the list of exempt devices

If you use role-based administration:

- You must have the Policy setting - device control right to edit a device control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To view or edit the list of exempt devices:

1. Check which device control policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Device control. Then double-click the policy you want to change.
3. In the Device control policy dialog box, on the Configuration tab, select the type of device for which you want to view exemptions, for example, optical drive. Click View Exemptions.
   The <Device type> exemptions dialog box is displayed. If an exemption is for all devices with that model ID, the Device ID field is blank.
4. If you want to edit the list of exempt devices, do one of the following:
• If you want to add an exemption, click **Add**.

• If you want to edit an exemption, select the exemption and click **Edit**. Edit the settings in the **Exempt device** dialog box as appropriate.

• If you want to remove an exemption, select the exempt device and click **Remove**. This will remove the exempt device from the policy you are editing. If you want to remove the device from other policies, repeat the steps in this task for each policy.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Check which policies a group uses (page 27)
Exempt a device from a single policy (page 169)

## 8.13 Tamper protection policy

Tamper protection enables you to prevent 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.

**Note**
Tamper protection is not designed to protect against users with extensive technical knowledge. Nor does it protect against malware which has been specifically designed to subvert the operating system to avoid detection. This type of malware is only detected by scanning for threats and suspicious behavior.

After you enable tamper protection and create a tamper-protection password, a member of the SophosAdministrator group on the endpoint who does not know the password will not be able to:

• Re-configure on-access scanning or suspicious behavior detection settings in Sophos Endpoint Security and Control.

• Disable tamper protection.

• Uninstall the Sophos Endpoint Security and Control components (Sophos Anti-Virus, Sophos Client Firewall, Sophos AutoUpdate, or Sophos Remote Management System).

If you want to enable SophosAdministrators to perform these tasks, you must provide them with the tamper protection password so that they can authenticate themselves with tamper protection first.

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.

If you use role-based administration:

• You must have the **Policy setting - tamper protection** right to configure a tamper protection policy.

• You can’t edit a policy if it is applied outside your active sub-estate.
Tamper protection events

When a tamper protection event occurs, for example, an unauthorized attempt to uninstall Sophos Anti-Virus from an endpoint computer has been prevented, the event is written in the event log that can be viewed from Sophos Enterprise Console.

There are two types of tamper protection 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.

Related concepts
Anti-virus and HIPS policy (page 85)
Managing roles and sub-estates (page 15)

Related tasks
View tamper protection events (page 201)

8.13.1 Turn tamper protection on or off

If you use role-based administration:

- You must have the Policy setting - tamper protection right to configure a tamper protection policy.
- You can't edit a policy if it is applied outside your active sub-estate.

To turn tamper protection on or off:

1. Check which tamper protection policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Tamper protection. Then double-click the policy you want to change.
3. In the Tamper Protection Policy dialog box, select or clear the Enable tamper protection check box.
   If you want to enable tamper protection for the first time, click Set under the Password box. In the Tamper Protection Password dialog box, enter and confirm a password.

   Tip
   We recommend that the password should be at least eight characters long and contain mixed-case letters and numbers.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)
8.13.2 Change the tamper protection password

To change the tamper protection password:

1. Check which tamper protection policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Tamper protection. Then double-click the policy you want to change.
3. In the Tamper Protection Policy dialog box, click Change under the Password box. 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 mixed-case letters and numbers.

Related concepts
Managing roles and sub-estates (page 15)
Related tasks
Check which policies a group uses (page 27)

8.13.3 About enhanced tamper protection

Enhanced tamper protection builds on the functionality of tamper protection. If enhanced tamper protection is enabled, the following actions are blocked for Sophos Anti-Virus, Sophos AutoUpdate, Sophos Management Communication System, Sophos Remote Management System and Sophos Endpoint Defense:

• Stopping services from the Services UI
• Killing services from the Task Manager UI
• Changing service configuration from the Services UI
• Stopping services/editing service configuration from the command line
• Uninstalling
• Reinstalling
• Killing processes from the Task Manager UI
• Deleting or modifying protected files or folders
• Deleting or modifying protected registry keys

CAUTION
To enable enhanced tamper protection, tamper protection must be enabled. If tamper protection is disabled, enhanced tamper protection will automatically be disabled.

8.13.4 Enhanced tamper protection settings

1. In the Policies pane, double-click Tamper protection. Then double-click the policy you want to change.
2. In the **Tamper Protection Policy** dialog box, make sure the **Enable tamper protection** check box is ticked then select the **Enable enhanced tamper protection** check box.

3. If this is a new install or an upgrade, in the **Tamper Protection Policy** dialog box, click **Set** under the **Password** box.

   If tamper protection is already enabled, click **Change** under the **Password** box. In the **Tamper Protection Password** dialog box, enter and confirm a password.

   **Note**
   The same password is used for tamper protection and enhanced tamper protection. When enhanced tamper protection is enabled, it overrides tamper protection. This is why the password must be changed when the tamper protection password has already been set.

   We recommend that you use a different password for each policy.

### 8.14 Patch policy

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

Sophos Enterprise Console enables you to check that your computers have the most up-to-date security patches installed.

Before using patch, you must install the patch agent on your networked computers so that they can perform patch assessments and communicate status to Sophos Enterprise Console. You can install this using the **Protect Computers Wizard**.

This section assumes that you have installed the patch agent.

If you use role-based administration:

- You must have the **Policy setting - patch** right to configure a patch policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

**Related concepts**
**Managing roles and sub-estates** (page 15)

**Related tasks**
**Protect computers automatically** (page 50)

**Related information**
**Sophos product comparison**

### 8.14.1 How does patch assessment work?

Patch assessment is disabled in the default policy. Once patch assessment is enabled, computers begin an assessment. This can take several minutes. Subsequent assessments occur at the interval set in policy, which is daily by default.
Note
If computers run an assessment before Sophos Enterprise Console has downloaded patch data from Sophos for the first time, the Patch Event viewer displays no results. The download can take several hours. To check if this has completed, see the Patch updates field in Events > Patch Assessment Events.

If the patch agent cannot update from Sophos Enterprise Console, for any reason, it will continue to assess computers against the previously downloaded patch detections.

Computers are only assessed for security patches on software that is installed on the computer. If a new patch is released that supersedes an older patch, then patch assessment will no longer check for the presence of the older patch. Only the new patch will be assessed.

What are superseded patches?
If a vendor releases a patch that replaces an earlier patch, the new patch is called a superseding patch. The patch it replaces is referred to as the superseded patch.

Sophos recommends you install the superseding patch to keep your computers up-to-date.

Example: If you search for virusX and see that the fix for the virus is available in patch P01, which is superseded by patch P02, Sophos recommends you install P02.

8.14.2 About patch assessment events
When a patch assessment event occurs, for example, a computer is missing a patch, the event is sent to Sophos Enterprise Console and can be viewed in the Patch Assessment - Event Viewer.

In the Patch Assessment - Event Viewer, you can use filters to display only the events you are interested in. You can also export the list of patch assessment events to a file.

Related concepts
Patch assessment events (page 201)
Related tasks
Export the list of events to a file (page 206)

8.14.3 Turn patch assessment on or off
If you use role-based administration:

- You must have the Policy setting - patch right to configure a patch policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To turn patch assessment on or off:
1. Check which patch policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Patch. Then double-click the policy you want to change.
3. In the Patch Policy dialog box, select or clear the Enable patch assessments check box, and click OK.

Related concepts
Managing roles and sub-estates (page 15)
8.14.4 Select the patch assessment interval

If you use role-based administration:

- You must have the Policy setting - patch right to configure a patch policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To set the patch assessment interval:

1. Check which patch policy is used by the group(s) of computers you want to configure.
2. In the Policies pane, double-click Patch. Then double-click the policy you want to change.
3. In the Patch Policy dialog box, click the drop-down arrow of the Assess for missing patches field, and select the appropriate interval. Click OK.

To assess at this interval, patch assessment must be enabled in the policy.

8.15 Web control policy

**Note**

This feature is not included with all licenses. If you want to use it, you might need to change your license. For more information, see Products.

By default, the web control policy is turned off in Sophos Enterprise Console. Selecting Enable web control allows you to choose one of the following policy options:

- **Inappropriate Website Control**: This basic web control option includes 14 essential site categories. It is designed to protect users from visiting websites for which your organization could be legally liable.

- **Full Web Control**: This option applies a comprehensive, full-featured policy that covers more than 50 website categories. It requires a Sophos Web Appliance, Sophos Management Appliance, or Sophos UTM appliance (version 9.2 or later) to synchronize with endpoints to distribute policy updates and collect web activity data.

When using Inappropriate Website Control, you can either edit an existing web control policy, or create a new policy. You can set the various site categories to Block, Warn, or Allow. Web control status and web events are displayed in Sophos Enterprise Console.

If, instead, you are using the Full Web Control policy, Sophos Enterprise Console requires the location of the Web, UTM, or Management Appliance from which the full web-filtering policy is configured, together with a shared key to secure communication between the appliance and Sophos Enterprise Console. When the Full Web Control policy is selected, most of the reporting and monitoring is shifted to the appliance; however, websites scanned and assessed by Sophos Endpoint Security and Control's live URL-filtering are displayed in Sophos Enterprise Console as web events.
If you use role-based administration:

- You must have the **Policy setting - web control** right to edit a web control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

**Related concepts**
- Full Web Control (page 181)
- Web protection (page 106)
- Inappropriate Website Control (page 177)
- Managing roles and sub-estates (page 15)

**Related tasks**
- Create a policy (page 32)
- View web events (page 204)

**Related information**

**8.15.1 Inappropriate Website Control**

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

With this basic form of website control, you can filter the web activity of users, based on 14 website categories. There is a default action for each category, but, if necessary, you can select a different action.

Users can be blocked from visiting restricted websites. An event is triggered that is shown to the user and sent to Sophos Enterprise Console.

Alternatively, users can be warned by means of a notification when visiting controlled websites; even if the user does not proceed, a warning event is triggered. If the user proceeds and views a site despite the warning, a second event is triggered and sent to Sophos Enterprise Console.

**Note**
Although HTTP and HTTPS sites are both filtered in all supported web browsers, user notifications are different, depending on whether the URL is HTTP or HTTPS. With HTTP sites, users see notification pages for sites in categories set to **Block** or **Warn**. For HTTPS, users only see **Block** notifications, and they are displayed as a balloon tip in the Windows System Tray. HTTPS **Warn** actions are neither displayed to the user nor are they logged. Instead, users are allowed to continue to the requested page, and the event is logged as a Proceed in Sophos Enterprise Console.

If you select the **Allow** action for a website category, users can access all websites within this category, unless website exceptions are specified. Allow events are not logged when **Inappropriate Website Control** is selected.

**Note**
Allowed sites are still scanned and assessed by Sophos Endpoint Security and Control's live URL-filtering (Web protection) feature.
Turn on Inappropriate Website Control

Perform the following steps to turn on web control in Sophos Enterprise Console and use Inappropriate Website Control.

If you use role-based administration:
- You must have the Policy setting - web control right to edit a web control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To turn on Inappropriate Website Control:

1. Check which web control policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Web control. Then double-click the policy you want to change.
   The Web Control Policy dialog box is displayed.
3. On the General tab, select Enable web control.
   The Inappropriate Website Control policy is displayed. Although there is a default action for each of the 14 site categories, you can set a different action.

About website categories

By selecting Inappropriate Website Control, you can configure 14 website categories, controlling the internet content that users can access through a web browser.

The website categories described below are filtered. The default action for each category is indicated in brackets. Each category can be configured as Block, Warn, or Allow. Selecting Allow gives users access to all sites within that category.

- Adult Sexually Explicit (Block): This category includes sites for adult products including sex toys, CD-ROMs, and videos; child pornography and pedophilia (including the IWF list); adult services including video-conferencing, escort services, and strip clubs; erotic stories and textual descriptions of sexual acts; explicit cartoons and animation; online groups, including newsgroups and forums that are sexually explicit in nature; sexually-oriented or erotic sites with full or partial nudity; depictions or images of sexual acts, including with animals or inanimate objects used in a sexual manner; sexually exploitive or sexually violent text or graphics; bondage, fetishes, genital piercing; naturist sites that feature nudity; and erotic or fetish photography that depicts nudity.

  Note
  We do not include sites regarding sexual health, breast cancer, or sexually transmitted diseases (except those with graphic examples).
• **Alcohol and Tobacco (Warn):** This category includes sites that promote or distribute alcohol or tobacco products for free or for a charge.

• **Anonymizer Proxies (Block):** This category includes sites for remote proxies or anonymous surfing, search engine caches that circumvent filtering, and web-based translation sites that circumvent filtering.

• **Criminal Activity (Block):** This category includes sites for advocating, instructing, or giving advice on performing illegal acts; tips on evading law enforcement; and lock-picking and burglary techniques.

• **Gambling (Warn):** This category includes sites of online gambling or lottery websites that invite the use of real or virtual money; information or advice for placing wagers, participating in lotteries, gambling, or running numbers; virtual casinos and offshore gambling ventures; sports picks and betting pools; and virtual sports and fantasy leagues that offer large rewards or request significant wagers.

• **Hacking (Block):** This category includes sites for the promotion, instruction, or advice on the questionable or illegal use of equipment and software for purpose of hacking passwords, creating viruses, gaining access to other computers and computerized communication systems; sites that provide instruction or work-arounds for filtering software; cracked software and information sites; warez; pirated software and multimedia download sites; and computer crime sites.

• **Illegal Drugs (Block):** This category includes sites for recipes, instructions or kits for manufacturing or growing illicit substances for purposes other than industrial usage; glamorizing, encouraging, or instructing on the use of or masking the use of alcohol, tobacco, illegal drugs, or other substances that are illegal to minors; information on "legal highs", including glue sniffing, misuse of prescription drugs, or abuse of other legal substances; distributing illegal drugs free or for a charge; and displaying, selling, or detailing the use of drug paraphernalia.

• **Intolerance and Hate (Block):** This category includes sites that advocate or incite degradation or attack of specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation; sites that promote a political or social agenda that is supremacist in nature and exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation; holocaust revisionist or denial sites and other revisionist sites that encourage hate; coercion or recruitment for membership in a gang or cult; militancy and extremist sites; and flagrantly insensitive or offensive material, including those with a lack of recognition or respect for opposing opinions and beliefs.

**Note**
We do not include news, historical, or press incidents that may include the above criteria (except in graphic examples).

\(^1\) A gang is defined as a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol, and whose members individually or collectively engage in criminal activity in the name of the group.

\(^2\) A cult is defined as a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers' personalities and behavior are altered; a group in which leadership is all-powerful, ideology is totalistic, and the will of the individual is subordinate to the group; and a group that sets itself outside of society.

• **Phishing and Fraud (Block):** This category includes sites involved in phishing and telephone scams, service theft advice sites, and plagiarism and cheating sites, including the sale of research papers.

• **Spam URLs (Block):** This category includes URLs found in spam, particularly on these topics: computing, finance and stocks, entertainment, games, health and medicine, humor and novels, personal and dating, products and services, shopping, and travel.
• **Spyware (Block)**: This category includes sites that provide or promote information gathering or tracking that is unknown to, or done without the explicit consent of, the end user or the organization, including sites that carry malicious executables or viruses, third party monitoring, and other unsolicited commercial software, spyware, and malware “phone home” destinations.

• **Tasteless and Offensive (Warn)**: This category includes sites that feature offensive or violent language, including through jokes, comics, or satire, and excessive use of profanity or obscene gesticulation.

• **Violence (Warn)**: This category includes sites portraying, describing or advocating physical assault against humans, animals, or institutions; depicting torture, mutilation, gore, or horrific death; advocating, encouraging, or depicting self-endangerment, or suicide, including through eating disorders or addictions; instructions, recipes, or kits for making bombs or other harmful or destructive devices; sites promoting terrorism; and excessively violent sports or games, including videos and online games.

  **Note**
  We do not block news, historical, or press incidents that may include the above criteria, except those that include graphic examples.

• **Weapons (Warn)**: This category includes sites with online purchasing or ordering information, including lists of prices and dealer locations; any page or site predominantly containing, or providing links to, content related to the sale of guns, weapons, ammunition or poisonous substances; displaying or detailing the use of guns, weapons, ammunition or poisonous substances; and clubs which offer training on machine guns, automatics, other assault weapons, and sniper training.

  **Note**
  Weapons are defined as something (such as a club, knife, or gun) used to injure, defeat, or destroy.

**Related concepts**
Inappropriate Website Control (page 177)

**Related tasks**
Select a website category action (page 180)

**Select a website category action**

With web control turned on and the *Inappropriate Website Control* policy selected, you can configure the action for each website category. You can also create a new policy that is based on the default policy.

To select a site category action:

1. On the **General** tab, on the drop-down list next to the site category or categories that you want to configure, select one of the following:

   • **Block**: Prevents users from viewing sites in this category. If it is an HTTP web page, a block notification is displayed to the user, explaining why the site was blocked. If it is an HTTPS page, a balloon tip is displayed to the users in the Windows System Tray.

   • **Warn**: Warns users that they are at risk of violating their organization’s web use policy, but allows them to proceed. If it is an HTTP page, a warn notification is displayed to users, cautioning them about proceeding to the site. If it is an HTTPS page, the user does not receive
a notification, and is allowed to continue to the website. The event is logged as a Proceed in Sophos Enterprise Console.

- **Allow**: Lets users view sites in this category. The event is not logged.

2. Click OK.

**Related tasks**

Create a policy (page 32)

**Manage website exceptions**

If you have selected the Inappropriate Website Control policy, you can create exceptions to the Block and Warn actions. You can exempt websites from filtering by adding them to the Websites to Allow or Websites to Block list. Entries can take the form of IP addresses and domain names. You can also edit existing website entries, and remove websites from a list.

**Note**

If there are conflicting or overlapping entries in the Block and Allow lists, the entries in the Block list will always take precedence. For example, if the same IP address is included in the Block list and the Allow list, the website is blocked. Furthermore, if a domain is included in the Block list, but a subdomain of that same domain is included in the Allow list, the Allow entry is ignored, and the domain and all of its subdomains are blocked.

To add a website exception:

1. On the Website Exceptions tab, click the Add button next to the Websites to Allow or Websites to Block text box.
2. In the Add Website to Allow dialog box, click Domain name, IP address with subnet mask, or IP address. Examples of each format are displayed above the associated text box.
3. In the text box, enter the domain name or IP address for the website you want to allow or block.
4. Click OK.

If you want to edit a website or remove it from a list, select the website, and click Edit or Remove accordingly.

**8.16 Full Web Control**

**Note**

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

If you have a Sophos Web Appliance, Sophos Management Appliance, or Sophos UTM appliance (version 9.2 or later) you can distribute an appliance-based policy to your users by way of Sophos Enterprise Console.

Endpoint computers communicate with Sophos Enterprise Console in the same way as when the Inappropriate Website Control policy is selected, but the web-filtering rules and web activity logs are synchronized with the appliance that you specify. The policy is stored on endpoint computers and applied, based on the latest Sophos data.

Users are blocked, warned or allowed, according to the web control policy. You can view user activity data using the Reports and Search features on the Web Appliance or Management Appliance, or Logging & Reporting > Web Protection option on the UTM appliance. Web control
events are all recorded on the appliance; however, sites scanned and assessed by Sophos Endpoint Security and Control's live URL-filtering (Web protection) are recorded as web events in Sophos Enterprise Console.

Note
Although HTTP and HTTPS sites are both filtered in all supported web browsers, in a Web Appliance or Management Appliance user notifications are different, depending on whether the URL is HTTP or HTTPS. With HTTP sites, users see notification pages for sites in categories set to Block or Warn. For HTTPS, users only see Block notifications, and they are displayed as a balloon tip in the Windows System Tray. HTTPS Warn actions are not displayed to users, nor are they logged. Instead, users are allowed to continue to the requested page, and it is logged as a Proceed event in the Sophos Web Appliance or Security Management Appliance.

UTM appliance uses a central cloud-based service called Sophos LiveConnect for protecting and monitoring endpoint computers. LiveConnect allows you to always manage all of your endpoints, whether they are on your local network, at remote sites, or with traveling users—policy updates are distributed to users, and reporting data from endpoint computers is uploaded, even when users are not connected from within the network.

When using Management Appliance or Web Appliance, endpoints can communicate with the appliance either directly or through Sophos LiveConnect.

With Full Web Control selected, a full-featured policy takes effect. Full Web Control offers the following benefits over basic web control, depending on the appliance you use:

- Users are warned or blocked, based on over 50 categories of URLs.
- Differentiated Special Hours policies can be applied.
- Numerous additional policies can be used as per-user or per-group exceptions to the default and Special Hours policies.
- Detailed logs and reports are available on the Sophos Web Appliance, Security Management Appliance, or UTM appliance.
- LiveConnect allows distribution of policy updates and uploading of report data, even when users connect remotely.
- Users can submit feedback regarding the handling of blocked URLs.
- Customized notification pages that include your logo, and text that is specific to your organization, can be displayed to users. For more information, see the Sophos Web Appliance documentation.
- Users are automatically restricted from browsing to inappropriate sites from within popular search engines when SafeSearch is enabled.

For more information on configuring a full Web Appliance policy, see Sophos Web Appliance documentation.

Related information
Sophos product comparison
Sophos Web Appliance documentation
UTM appliance documentation
8.16.1 Turn on Full Web Control

Note
The following procedure assumes that you have a Sophos Web Appliance, Sophos Management Appliance, or Sophos UTM appliance (version 9.2 or later) that is configured, fully functioning, and using endpoint web control.

By default, the web control policy is turned off. Perform the following steps to enable web control and use the Full Web Control policy.

If you use role-based administration:
- You must have the Policy setting - web control right to edit a web control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To turn on Full Web Control:
1. Check which web control policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Web control. Then double-click the policy you want to change. The Web Control Policy dialog box is displayed.
3. On the General tab, click Enable web control.
4. Select Full Web Control.
5. In the Settings panel, enter the Appliance Hostname and Security Key for Policy Exchange.
   - For a Web Appliance or Management Appliance, you must provide a fully qualified hostname. The security key must match the one that is displayed on the Endpoint Web Control page of the appliance.
   - For UTM, enter the Hostname and the Shared Key of the Sophos LiveConnect broker used by UTM. They can be found in the UTM administrative interface WebAdmin, on the Endpoint Protection > Computer Management > Advanced tab, in the Sophos LiveConnect – Registration section under SEC Information.
6. Optionally, select Block browsing if the website category cannot be determined. If an endpoint computer is unable to retrieve data about website categorization, URLs that cannot be categorized are blocked until the service is restored.
   - This check box is not selected by default, which allows users to continue browsing if the categorization service fails.
7. Click OK.
   Sophos Enterprise Console reconfigures endpoint computers to communicate with the Web Appliance, Management Appliance, or Sophos LiveConnect broker used by UTM.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)

Related information
Sophos Web Appliance documentation
UTM appliance documentation
8.17 Exploit prevention policy

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

Exploit prevention lets you:

- Protect document files from ransomware (CryptoGuard).
- Protect against attacks on the boot sector (WipeGuard).

**Warning**
This functionality is not currently available for servers.

- Protect critical functions in web browsers (Safe Browsing).
- Mitigate exploits. This protects the applications most vulnerable to exploitation by malware, such as Java applications.
- Protect against process hollowing attacks.
- Protect against loading .DLL files from untrusted folders.
- Protect against processor branch tracing.

By default, exploit prevention and all exploit prevention options are turned on.

**Warning**
If you upgrade your license to include Exploit Prevention, it is not automatically installed on the computers you already manage. You need to reprotect the computers to install it.

You can exclude applications from exploit prevention. Note that they will still be protected by CryptoGuard and Safe Browsing.

For more information about the recommended settings for exploit prevention, see the Sophos Enterprise Console policy setup guide.

If you use role-based administration:

- You must have the **Policy setting - exploit prevention** right to configure an exploit prevention policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

**HitmanPro.Alert and policy updates**

HitmanPro.Alert detects applications, on endpoints, that need protection. It reports the detected application to the Sophos Enterprise Console server. The server collates the applications that require protection and every 120 minutes merges the new application data into the policy. The server distributes the updated policy to the endpoints and provides the list of applications to be protected.

**Related concepts**
Managing roles and sub-estates (page 15)
8.17.1 Turn exploit prevention on or off

If you use role-based administration:

- You must have the **Policy setting - exploit prevention** right to configure an exploit prevention policy.
- You can't edit a policy if it is applied outside your active sub-estate.

**Note**

By default, exploit prevention is turned on and all exploit prevention options are turned on.

To turn exploit prevention on or off:

1. Check which exploit prevention policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Exploit prevention**. Then double-click the policy you want to change.
3. In the **Protection Settings** tab of the **Exploit Prevention Policy** dialog box, select or clear the **Enable exploit prevention** check box.
4. Select or clear the **Protect document files from ransomware (CryptoGuard)** check box.
   - You can also choose whether to protect against remotely run ransomware (only on 64-bit endpoints).
5. Select or clear the **Disk and boot record protection (WipeGuard)** check box.
6. Select or clear the **Protect critical functions in web browsers (Safe Browsing)** check box.
7. Select or clear the **Mitigate exploits in vulnerable applications** check box.
   - You can also choose the types of applications you want to protect against exploitation, for example Microsoft Office applications.
8. Select or clear the **Prevent process hollowing attacks** check box.
9. Select or clear the **Prevent DLLs loading from untrusted folders** check box.
10. Select or clear the **CPU branch tracing** check box.
11. Click **OK**.

You can exclude applications from exploit prevention. Note that they will still be protected by CryptoGuard and Safe Browsing, if these options are selected.

You can also exclude exploit events from exploit prevention.

**Related concepts**

Managing roles and sub-estates (page 15)

**Related tasks**

Check which policies a group uses (page 27)
Exclude exploit events from exploit prevention (page 186)
Exclude applications from exploit prevention (page 186)
8.17.2 Exclude applications from exploit prevention

If you use role-based administration:

- You must have the **Policy setting - exploit prevention** right to configure an exploit prevention policy.
- You can't edit a policy if it is applied outside your active sub-estate.

**Warning**
Vulnerable applications are protected by default. You should be careful when excluding applications from exploit prevention. They will still be protected by CryptoGuard and Safe Browsing.

You can exclude applications from exploit prevention. You can also protect previously excluded applications.

To exclude applications:

1. Check which exploit prevention policy is used by the groups of computers you want to configure.
2. In the **Policies** pane, double-click **Exploit prevention**. Then double-click the policy you want to change.
3. In the **Application Exclusions** tab of the **Exploit Prevention Policy** dialog box, select the applications you want to exclude in the **Protected Applications** list and click **Exclude**. This moves the selected applications to the **Excluded Applications** list.
4. To protect applications that are currently excluded from checking, go to the **Excluded Applications** list, select the applications and click **Include**.
5. Click **OK**.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Turn exploit prevention on or off (page 185)
Check which policies a group uses (page 27)

8.17.3 Exclude exploit events from exploit prevention

If you use role-based administration:

- You must have the **Policy setting - exploit prevention** right to configure an exploit prevention policy.
- You can't edit a policy if it is applied outside your active sub-estate.
- When you exclude an exploit event, only the specific exploit will be excluded, not the complete application.
- If an exploit event is part of an application that has already been excluded, you do not need to exclude the exploit event.

You can exclude exploit events from exploit prevention. You can also protect previously excluded exploit events.

To exclude exploit events:
1. Check which exploit prevention policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Exploit prevention. Then double-click the policy you want to change.
3. In the Exploit Exclusions tab of the Exploit Prevention Policy dialog box, select the exploit events you want to exclude in the Detected exploit events list and click Exclude. This moves the selected exploit events to the Excluded exploit events list.
4. To protect exploit events that are currently excluded from checking, go to the Excluded exploit events list, select the events and click Include.
5. Click OK.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Check which policies a group uses (page 27)
9 Setting up alerts and messages

There are several alerting methods used in Sophos Enterprise Console.

- **Alerts displayed in the console**: If an item that requires attention is found on a computer, or an error has occurred, Sophos Endpoint Security and Control sends an alert to Sophos Enterprise Console. The alert is displayed in the computer list. These alerts are always displayed. You do not need to set them up.

- **Events displayed in the console**: When an application control, firewall, patch assessment, web, data control, device control or tamper protection event occurs on an endpoint computer, for example, an application has been blocked by the firewall, that event is sent to Sophos Enterprise Console and can be viewed in the respective event viewer.

- **Alerts and messages sent by the console to your chosen recipients**: By default, when an item is found on a computer, a message is displayed on the computer desktop and an entry is added to the Windows event log. When an application control, data control, or device control event occurs, a message is displayed on the computer desktop.

  **Note**  
  Optional user-defined desktop messages are not displayed on computers running Windows 8 or later.

You can also set up email alerts or SNMP messages for administrators.

  **Note**  
  If you want to use authenticated SMTP for email alerts, see knowledge base article 113780.

This section describes how to set up alerts to be sent to your chosen recipients.

**Related tasks**
Deal with alerts about detected items (page 56)

**Related information**
knowledge base article 113780

9.1 Set up software subscription alerts

Sophos Enterprise Console displays alerts raised by the update manager in the **Alerts** column in the **Update managers** view.

If you use role-based administration, you must have the **System configuration** right to perform this task.

If you subscribed to a fixed version of software, an alert will be displayed when that version is nearing retirement or is retired. An alert will also be displayed if your product license has changed.

If you are subscribed to a fixed version of software and have chosen to **Automatically upgrade fixed version software when it is no longer supported by Sophos**, your subscription will be upgraded automatically.

If you have chosen not to be upgraded automatically, you will be instructed to change your subscription.
Note
Running unsupported software leaves you unprotected against new security threats. We recommend that you upgrade to a supported version as soon as possible.

You can also set up email alerts to be sent to your chosen recipients when the product version you are subscribed to is nearing retirement or is retired.

1. On the **Tools** menu, select **Configure email alerts**.
   The **Configure email alerts** dialog box is displayed.
2. If SMTP settings have not been configured, or if you want to view or change the settings, click **Configure**.
   In the **Configure SMTP settings** dialog box, enter the details as described below.
   a) In the **Server address** text box, type the host name or IP address of the SMTP server.
   b) In the **Sender** text box, type an email address to which bounces and non-delivery reports can be sent.
   c) Click **Test** to test the connection.
3. In the **Recipients** panel, click **Add**.
   The **Add a new email alert recipient** dialog box appears.
4. In the **Email address** field, enter the address of your recipient.
5. In the **Language** field, select the language in which email alerts should be sent.
6. In the **Subscriptions** pane, select “Software subscriptions” email alerts you want to send to this recipient. There are three alerts you can subscribe to:
   • A software subscription includes a version of a product that is shortly to be retired at Sophos.
   • A software subscription includes a version of a product which is no longer available.
     This alert is sent if the product you are subscribed to has been retired, or your license has changed and the new license does not include that product.
   • The Sophos license information has been updated. Product features may have changed.

Related concepts
**Managing roles and sub-estates** (page 15)

9.2 Set up anti-virus and HIPS email alerts

You can send email alerts to specific users if a virus, suspicious behavior, an unwanted application or an error is encountered on any of the computers in a group.

If you use role-based administration:
- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

**Warning**
Mac OS X computers can send email alerts to only one address.

To send alerts:
1. In the **Policies** pane, double-click the anti-virus and HIPS policy you want to change.
2. In the Anti-virus and HIPS policy dialog box, click Messaging.
3. In the Messaging dialog box, go to the Email alerting tab and select Enable email alerting.
4. In the Messages to send panel, select the events for which you want to send email alerts.

**Warning**
The Suspicious behavior detection, Suspicious file detection, Adware and PUA detection and cleanup, and Other errors settings apply only to Windows computers.

5. In the Recipients panel, click Add or Remove to add or remove, respectively, email addresses to which email alerts should be sent. Click Rename to change an email address you have added.

**Warning**
Mac OS X computers will send messages only to the first recipient in the list.

6. Click Configure SMTP to change the settings for the SMTP server and the language of the email alerts.
7. In the Configure SMTP settings dialog box, enter the details as described below.
   a) In the SMTP server text box, type the host name or IP address of the SMTP server. Click Test to test the connection.
   b) In the SMTP sender address text box, type an email address to which bounces and non-delivery reports can be sent.
   c) In the SMTP reply-to address text box, you can type in the text box an email address to which replies to email alerts can be sent. Email alerts are sent from an unattended mailbox.
   d) In the Language panel, click the drop-down arrow, and select the language in which email alerts should be sent.

**Related concepts**
Managing roles and sub-estates (page 15)

9.3 Set up anti-virus and HIPS SNMP messaging

You can send SNMP messages to specific users if a virus or error is encountered on any of the computers in the group.

If you use role-based administration:
- You must have the Policy setting - anti-virus and HIPS right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

**Warning**
These settings apply only to Windows computers.

1. In the Policies pane, double-click the anti-virus and HIPS policy you want to change.
2. In the Anti-virus and HIPS policy dialog box, click Messaging.
3. In the Messaging dialog box, go to the SNMP messaging tab and select Enable SNMP messaging.
4. In the Messages to send panel, select the types of event for which you want Sophos Endpoint Security and Control to send SNMP messages.
5. In the **SNMP trap destination** text box, enter the IP address of the recipient.
6. In the **SNMP community name** text box, enter the SNMP community name.

**Related concepts**

Managing roles and sub-estates (page 15)

### 9.4 Configure anti-virus and HIPS desktop messaging

By default, desktop messages are displayed on the computer on which a virus, suspicious item or potentially unwanted application is found.

If you use role-based administration:

- You must have the **Policy setting - anti-virus and HIPS** right to perform this task.
- You cannot edit a policy if it is applied outside your active sub-estate.

To configure these messages:

1. In the **Policies** pane, double-click the anti-virus and HIPS policy you want to change.
2. In the **Anti-virus and HIPS policy** dialog box, click **Messaging**.
3. In the **Messaging** dialog box, click the **Desktop messaging** tab.

   By default, **Enable desktop messaging** and all the options in the **Messages to send** panel are selected. Edit these settings, if appropriate.

   **Note**

   The **Suspicious behavior detection**, **Suspicious file detection**, and **Adware and PUA detection** settings apply only to Windows computers.

4. In the **User-defined message** text box, you can type a message that will be added to the end of the standard message.

   **Note**

   User-defined desktop messages are not displayed on computers running Windows 8 or later.

### 9.5 Set up application control alerts and messages

You can send messages to specific users when a controlled application is found.

If you use role-based administration:

- You must have the **Policy setting - application control** right to configure an application control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

To send messages:

1. In the **Policies** pane, double-click the application control policy you want to change.
2. In the **Application control policy** dialog box, go to the **Messaging** tab.
In the **Messaging** panel, the **Enable desktop messaging** check box is enabled by default. When an unauthorized controlled application is detected by on-access scan and blocked, a desktop message will be displayed to the user informing them that the application has been blocked.

3. In the **Message text** box, type a message that will be added to the end of the standard desktop message.

**Note**
User-defined desktop messages are not displayed on computers running Windows 8 or later.

4. If you want to send email alerts about detected controlled applications, select the **Enable email alerting** check box.

5. Select the **Enable SNMP messaging** check box, if you want to send SNMP messages.

**Warning**
Your anti-virus and HIPS policy settings determine email and SNMP messaging configuration and recipients.

**Related concepts**
Managing roles and sub-estates (page 15)

**Related tasks**
Set up anti-virus and HIPS SNMP messaging (page 190)

You can send SNMP messages to specific users if a virus or error is encountered on any of the computers in the group.

### 9.6 Set up data control alerts and messages

Sophos Enterprise Console uses events and messages to report when the transfer of sensitive data is detected or blocked.

If you use role-based administration:

- You must have the **Policy setting - data control** right to configure a data control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

When data control is enabled, the following events and messages are logged or displayed by default:

- Data control events are logged on the workstation.
- Data control events are sent to Sophos Enterprise Console and can be viewed in the **Data Control - Event Viewer**. (To open the event viewer, on the **Events** menu, click **Data Control Events**.)

**Note**
Each computer can send to Sophos Enterprise Console a maximum of 50 data control events per hour.

- The number of computers with data control events over a specified threshold within the last seven days is displayed on the Dashboard.
- Desktop messages are displayed on the workstation.
You can also configure Sophos Enterprise Console to send the following messages:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email alerts</td>
<td>An email message is sent to the recipients that you specify.</td>
</tr>
<tr>
<td>SNMP messages</td>
<td>An SNMP message is sent to the recipients specified in your anti-virus and HIPS policy settings.</td>
</tr>
</tbody>
</table>

To set up data control messaging:

1. Check which data control policy is used by the group or groups of computers you want to configure.
2. In the Policies pane, double-click Data control. Then double-click the policy you want to change. The Data control policy dialog box is displayed.
3. In the Data control policy dialog box, go to the Messaging tab. Desktop messaging is enabled by default and Include matched rules in messages is selected.
4. Type messages that will be added to the standard messages for user confirmation of file transfer and for blocked file transfer, if you wish.

   You can enter a maximum of 100 characters. You can also add an HTML link to the message, for example, `<a href="http://www.sophos.com">About Sophos</a>.

   Note
   User-defined desktop messages are not displayed on computers running Windows 8 or later.

5. To enable email alerting, select the Enable email alerting check box. In the Email recipients field, enter the email addresses of the recipients. Separate each address with a semicolon (;).
6. To enable SNMP messaging, select the Enable SNMP messaging check box.

   The email server and SNMP trap settings are configured via the anti-virus and HIPS policy.

**Related concepts**
Managing roles and sub-estates (page 15)
Data control policy (page 149)

**Related tasks**
Check which policies a group uses (page 27)

### 9.7 Set up device control alerts and messages

Sophos Enterprise Console uses events and messages to report when a controlled device is detected or blocked.

If you use role-based administration:

- You must have the **Policy setting - device control** right to edit a device control policy.
- You cannot edit a policy if it is applied outside your active sub-estate.

When device control is enabled, the following events and messages are logged or displayed by default:

- Device control events are logged on the workstation.
- Device control events are sent to Sophos Enterprise Console and can be viewed in the **Device Control - Event Viewer**. (To open the event viewer, on the **Events** menu, click **Device Control Events**.)
Sophos Enterprise Console

- The number of computers with device control events over a specified threshold within the last seven days is displayed on the Dashboard.
- Desktop messages are displayed on the workstation.

You can also configure Sophos Enterprise Console to send the following messages:

<table>
<thead>
<tr>
<th>Message Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email alerts</td>
<td>An email message is sent to the recipients that you specify.</td>
</tr>
<tr>
<td>SNMP messages</td>
<td>An SNMP message is sent to the recipients specified in your anti-virus and HIPS policy settings.</td>
</tr>
</tbody>
</table>

To set up device control messaging:

1. Check which device control policy is used by the groups of computers you want to configure.
2. In the Policies pane, double-click Device control. Then double-click the policy you want to change.
3. In the Device control policy dialog box, on the Messaging tab, desktop messaging is enabled by default. To further configure messaging, do the following:
   - To enter a message text for desktop messaging, in the Message text box, type a message that will be added to the end of the standard message.
     You can enter a maximum of 100 characters. You can also add an HTML link to the message, for example, `<a href="http://www.sophos.com">About Sophos</a>`.

   **Note**
   User-defined desktop messages are not displayed on computers running Windows 8 or later.

   - To enable email alerting, select the Enable email alerting check box. In the Email recipients field, enter the email addresses of the recipients. Separate each address with a semicolon (;).
   - To enable SNMP messaging, select the Enable SNMP messaging check box.

   The email server and SNMP trap settings are configured using the anti-virus and HIPS policy.

**Related concepts**
- Managing roles and sub-estates (page 15)
- Device control policy (page 164)

**Related tasks**
- Check which policies a group uses (page 27)

**9.8 Set up network status email alerts**

You can set up email alerts to be sent to your chosen recipients when a warning or critical level has been exceeded for a dashboard section.

If you use role-based administration, you must have the System configuration right to configure the network status email alerts.

To set up alerts:

1. On the Tools menu, select Configure email alerts.
   The Configure email alerts dialog box is displayed.
2. If SMTP settings have not been configured, or if you want to view or change the settings, click Configure. In the Configure SMTP settings dialog box, enter the details as described below.
   a) In the Server address text box, type the host name or IP address of the SMTP server.
   b) In the Sender text box, type an email address to which bounces and non-delivery reports can be sent.
   c) Click Test to test the connection.

3. In the Recipients panel, click Add. The Add a new email alert recipient dialog box appears.

4. In the Email address field, enter the address of your recipient.

5. In the Language field, select the language in which email alerts should be sent.

6. In the Subscriptions pane, select “warning level exceeded” and “critical level exceeded” email alerts you want to send to this recipient.

Related concepts
Managing roles and sub-estates (page 15)

9.9 Set up Active Directory synchronization email alerts

You can set up email alerts to be sent to your chosen recipients about new computers and groups discovered during synchronizations with Active Directory.

If you use role-based administration, you must have the System configuration right to configure the Active Directory synchronization email alerts.

If you choose to protect computers in synchronized groups automatically, you can also set up alerts about automatic protection failures.

To set up alerts:
1. On the Tools menu, select Configure email alerts. The Configure email alerts dialog box is displayed.
2. If SMTP settings have not been configured, or if you want to view or change the settings, click Configure.
   In the Configure SMTP settings dialog box, enter the details as described below.
   a) In the Server address text box, type the host name or IP address of the SMTP server.
   b) In the Sender text box, type an email address to which bounces and non-delivery reports can be sent.
   c) Click Test to test the connection.
3. In the Recipients panel, click Add. The Add a new email alert recipient dialog box appears.
4. In the Email address field, enter the address of your recipient.
5. In the Language field, select the language in which email alerts should be sent.
6. In the Subscriptions pane, select “Active Directory synchronization” email alerts you want to send to this recipient.
   “Active Directory synchronization” email alerts:
   • New groups discovered
   • New computers discovered
• Automatic computer protection has failed

Related concepts
Managing roles and sub-estates (page 15)

9.10 Configure Windows event logging

By default, Sophos Endpoint Security and Control adds alerts to the Windows event log when a virus or spyware is detected or cleaned up, suspicious behavior or file is detected, or adware or PUA is detected or cleaned up.

If you use role-based administration:

• You must have the Policy setting - anti-virus and HIPS right to perform this task.
• You cannot edit a policy if it is applied outside your active sub-estate.

To edit these settings:
1. In the Policies pane, double-click the anti-virus and HIPS policy you want to change.
2. In the Anti-virus and HIPS policy dialog box, click Messaging.
3. In the Messaging dialog box, go to the Event log tab.
   By default, event logging is enabled. Edit the settings, if appropriate.
   Scanning errors include instances when Sophos Endpoint Security and Control is denied access to an item that it attempts to scan.

Related concepts
Managing roles and sub-estates (page 15)

9.11 Turn sending feedback to Sophos on or off

Sophos Enterprise Console will send Sophos a report periodically. These reports will help Sophos to understand how its products are being used and help to improve our products and services.

If you use role-based administration, you must have the System configuration right to turn sending feedback to Sophos on or off.

More details about the types of information collected and the way in which your information is processed can be found in the Sophos End User License Agreement (EULA) and the Sophos Privacy Policy located here: http://www.sophos.com/legal.

Some of the information reported is optional and some is mandatory, as further described in the EULA and the Privacy Policy. You can opt out of the optional information reporting at any time by changing the Feedback to Sophos setting.

By default, sending feedback to Sophos is enabled. You are given the option of disabling it when installing or upgrading the console, in the Sophos Enterprise Console installation wizard.

If you want to turn sending feedback to Sophos on or off after the installation, do the following:
1. On the Tools menu, click Feedback to Sophos.
2. In the Feedback to Sophos dialog box, you can enable or disable sending feedback to Sophos.
   • If you want to enable sending feedback to Sophos, read the agreement and select the I agree check box if you agree to the terms.
• If you want to disable sending feedback to Sophos, clear the I agree check box.

Related concepts
Managing roles and sub-estates (page 15)
10 Viewing events

When an application control, data control, device control, firewall, patch assessment, tamper protection, web control or exploit prevention event occurs on an endpoint computer, for example, an application has been blocked by the firewall, that event is sent to Enterprise Console and can be viewed in the respective event viewer.

Using the event viewers, you can investigate events that have occurred on the network. You can also generate a list of events based on a filter you configure, for example, a list of all data control events for the past seven days generated by a certain user.

The number of computers with events over a specified threshold within the last seven days is displayed on the Dashboard (except for tamper protection events).

You can also set up alerts to be sent to your chosen recipients when an event has occurred.

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Configure the Dashboard (page 53)

10.1 View application control events

To view application control events:

1. On the Events menu, click Application Control Events. The Application Control - Event Viewer dialog box appears.

2. In the Search period field, click the drop-down arrow and select the period for which you want to display the events.
   You can either select a fixed period, for example, Within 24 hours, or select Custom and specify your own time period by selecting the starting and ending dates and times.

3. If you want to view events for a certain user or computer, enter the name in the respective field.
   If you leave the fields empty, events for all users and computers will be displayed.
   You can use wildcards in these fields. Use ? for any single character and * for any string of characters.

4. If you want to view events for a certain application type, in the Application type field, click the drop-down arrow and select the application type.
   By default, the event viewer displays events for all application types.

5. Click Search to display a list of events.

You can export the list of application control events to a file.

Related tasks
Export the list of events to a file (page 206)
10.2 View data control events

Note
This feature will be unavailable if your license doesn't include Data Control.

If you use role-based administration, you must have the Data control events right to view data control events in Sophos Enterprise Console.

To view data control events:

1. On the Events menu, click Data Control Events. The Data Control - Event Viewer dialog box appears.
2. In the Search period field, click the drop-down arrow and select the period for which you want to display the events.
   You can either select a fixed period, for example, Within 24 hours, or select Custom and specify your own time period by selecting the starting and ending dates and times.
3. If you want to view events for a certain user, computer, or file, enter the name in the respective field.
   If you leave the fields empty, events for all users, computers, and files will be displayed.
   You can use wildcards in these fields. Use ? for any single character and * for any string of characters.
4. If you want to view events for a certain rule, in the Rule name field, click the drop-down arrow and select the rule name.
   By default, the event viewer displays events for all rules.
5. If you want to view events for a certain file type, in the File type field, click the drop-down arrow and select the file type.
   By default, the event viewer displays events for all file types.
6. Click Search to display a list of events.

You can export the list of data control events to a file

Related concepts
Managing roles and sub-estates (page 15)

Related tasks
Export the list of events to a file (page 206)

10.3 View device control events

To view device control events:

1. On the Events menu, click Device Control Events. The Device Control - Event Viewer dialog box appears.
2. In the Search period field, click the drop-down arrow and select the period for which you want to display the events.
   You can either select a fixed period, for example, Within 24 hours, or select Custom and specify your own time period by selecting the starting and ending dates and times.
3. If you want to view events for a certain device type, in the **Device type** field, click the drop-down arrow and select the device type.

   By default, the event viewer displays events for all device types.

   **Note**
   If you set optical disk drives to “Read only”, events for these devices are not seen in the event viewer.

4. If you want to view events for a certain user or computer, enter the name in the respective field.

   If you leave the fields empty, events for all users and computers will be displayed.

   You can use wildcards in these fields. Use ? for any single character and * for any string of characters.

5. Click **Search** to display a list of events.

In the **Device Control - Event Viewer** dialog box, you can exempt a device from the device control policies.

You can export the list of device control events to a file.

**Related tasks**
- Exempt a device from all policies (page 168)
- Export the list of events to a file (page 206)

10.4 View firewall events

Firewall events are sent only once from an endpoint computer to the console. Identical events from different endpoints are grouped together in the **Firewall - Event Viewer**. In the **Count** column, you can see the total number of times that an event has been sent from different endpoints.

To view firewall events:

1. On the **Events** menu, click **Firewall Events**.

   The **Firewall - Event Viewer** dialog box appears.

2. In the **Search period** field, click the drop-down arrow and select the period for which you want to display the events.

   You can either select a fixed period, for example, **Within 24 hours**, or select **Custom** and specify your own time period by selecting the starting and ending dates and times.

3. If you want to view events of a certain type, in the **Event type** field, click the drop-down arrow and select the event type.

   By default, the event viewer displays all types of events.

4. If you want to view events for a certain file, in the **File name** field, enter the file name.

   If you leave this field empty, events for all files will be displayed.

   You can use wildcards in this field. Use ? for any single character and * for any string of characters.

5. Click **Search** to display a list of events.

In the **Firewall - Event Viewer** dialog box, you can create a firewall rule.

You can export the list of firewall events to a file.
10.5 View tamper protection events

There are two types of tamper protection 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.

To view tamper protection events:

1. On the Events menu, click Tamper Protection Events. The Tamper Protection - Event Viewer dialog box appears.
2. In the Search period field, click the drop-down arrow and select the period for which you want to display the events.
   You can either select a fixed period, for example, Within 24 hours, or select Custom and specify your own time period by selecting the starting and ending dates and times.
3. If you want to view events of a certain type, in the Event type field, click the drop-down arrow and select the type of event.
   By default, the event viewer displays events of all types.
4. If you want to view events for a certain user or computer, enter the name in the respective field.
   If you leave the fields empty, events for all users and computers will be displayed.
   You can use wildcards in these fields. Use ? for any single character and * for any string of characters.
5. Click Search to display a list of events.
   You can export the list of events to a file.

Related tasks
Export the list of events to a file (page 206)

10.6 Patch assessment events

Note
This feature will be unavailable if your license doesn't include Patch Assessment.

The Patch Assessment - Event Viewer contains information about security patches and results of patch assessments.

The Patch updates field displays the download status of patch information. It displays one of the following status messages:

- Not downloaded indicates patch information is not downloaded or you do not have the license to use the Patch feature.
- Downloading indicates the first download, after install, is in progress.
- **OK** indicates patch information is up-to-date.
- **Out of date** indicates that there has not been a fully successful update of patch data in the past 72 hours. Typically this status is displayed if Sophos Enterprise Console is not up-to-date, due to issues with network connectivity. It may also be displayed if you change your license from a SEC that has the Patch feature, to another without it. It is possible that a partial update may have occurred when this status message is displayed.

The Patch Assessment - Event Viewer has the following tabs:

**Patches by rating**: This tab by default displays missing patches. Each patch is displayed, along with a count of the computers missing the patch, and the threats and vulnerabilities linked to the patch. You can use filters to show a full list of all the supported patches with a count of the number of computers missing them.

**Computers missing patches**: This tab displays patch assessment status by computer. Each computer is displayed, along with its missing patches. Computers are listed multiple times if missing more than one patch.

### 10.7 View patch assessment events

To view patch assessment events:

1. On the **Events** menu, click **Patch Assessment Events**. The **Patch Assessment - Event Viewer** dialog box appears.
2. Click on one of the tabs **Patches by rating** or **Computers missing patches**.
3. In the search panel, if you want to view events for a certain patch by its name, computer, threat, or vulnerability, enter the information in the respective field. Available criteria are based on the information displayed in the tab.
   
   If you leave the fields empty, events for all patch names, patch IDs, and computer names will be displayed.
   
   You can use wildcards in these fields. Use ? for any single character and * for any string of characters.
4. If you want to view events for a certain patch by its status, rating, vendor, group, or release date, click the drop-down arrow of the respective field and select the appropriate option. Available criteria are based on the information displayed in the tab.
   
   By default, the event viewer displays events for the threat ratings, vendors, groups, threats, and patch names for the missing patches.
5. Click **Search** to display a list of patch assessment events.

You can right-click on an individual hyperlink to copy its name, or use Ctrl+C to copy a patch assessment event row to the Clipboard.

You can export the list of patch assessment events.

You can view details about a specific patch by clicking the provided link.

**Related concepts**

- Patch assessment events (page 201)
- Search result categories (page 203)

**Related tasks**

- Export the list of events to a file (page 206)
- View patch, threat, or vulnerability details (page 203)
10.8 View patch, threat, or vulnerability details

To view patch, threat, or vulnerability details:

1. On the **Events** menu, click **Patch Assessment Events**. The **Patch Assessment - Event Viewer** dialog box appears.

2. Click on one of the tabs **Patches by rating** or **Computers missing patches**, select the required options, and click **Search** to display a list of events.

3. Click the patch name for which you want to view additional details.

4. In the **Patch Detail** dialog box, you can view a description of the patch and information about the threats and vulnerabilities it protects against. If available, you can:
   - Click the patch name to open a web browser and view vendor information about a patch.
   - Click the threat to open a web browser and view the Sophos threat analysis and recommendations.
   - Click the vulnerability to open a web browser and view common vulnerabilities and exposures (CVE) information.
   - Click the patch name in the **Previously addressed by** column to open a web browser and view vendor information about a patch that has been superseded.

The list is sorted alphabetically by threat and then by vulnerability.

**Related concepts**

*Search result categories (page 203)*

10.9 Search result categories

The search results are displayed in different categories based on the tab:

- Patches by rating.
- Computers missing patches.

**Related concepts**

*Patches by rating (page 203)*

The search results are displayed based on the following categories:

**Computers missing patches (page 204)**

The search results are displayed based on the following categories:

10.9.1 Patches by rating

The search results are displayed based on the following categories:

- **Threats**: A threat can be a virus, Trojan, worm, spyware, malicious website as well as adware and other potentially unwanted applications. You can click on the threat name to view the Sophos threat analysis and recommendations in a web browser.

- **Vulnerabilities**: A vulnerability is a software weakness which can be exploited by an attacker. The potential damage that could be caused by the exploitation is dependent upon the nature of the vulnerability, and the affected software. Patches are provided to fix vulnerabilities so
that exploitation is no longer possible. You can click on the vulnerability name to view common vulnerabilities and exposures (CVE) information in a web browser.

- **Patch name**: Displays the name of the patch. You can click on the patch name to open a web browser and view vendor information about a patch.
- **Vendor**: Displays the name of the vendor that published the patch.
- **Computers**: Displays the number of computers that are affected. If one or more computers are affected, you can click on the number to view the details in the Computers missing patches tab. If a "-" is displayed, it indicates that the patch is not assessed.
- **Superseded by**: Displays the names of any superseding patches. You can click on the patch name to open the Patch detail dialog box to view information about the superseding patch.
- **Release date**: Displays the patch release date.

### 10.9.2 Computers missing patches

The search results are displayed based on the following categories:

- **Computer**: Displays the name of the computer that is affected.
- **Patch name**: Displays the name of the patch. You can click on the patch name to open a web browser and view vendor information about a patch.
- **Superseded by**: Displays the name(s) of any superseding patches. You can click on the patch name to open the Patch detail dialog box to view information about the superseding patch.
- **Last assessment**: Displays the date when a computer was last assessed for missing patches.
- **Vendor**: Displays the name of the vendor that published the patch.
- **Release date**: Displays the patch release date.
- **Group**: Displays the group name to which the computer belongs.

### 10.10 View web events

**Note**
This feature will be unavailable if your license doesn't include Web Control.

If you use role-based administration, you must have the Web events right to view web events in Sophos Enterprise Console.

You can view the following web events in the Web Event Viewer:

- Malicious websites blocked by the Web Protection feature in the Anti-virus and HIPS policy.
- Web control events, if you use the web control feature.

Web control events are displayed differently, depending on which web control policy is selected. Although the Web Event Viewer can be used in both policy modes, the content is different.

When the Inappropriate Website Control policy option is selected, you can view any Block and Warn actions. Visited HTTPS sites categorized as Warn are logged as Proceed events because Sophos Endpoint Security and Control responds differently to HTTPS (see the note in Inappropriate Website Control).

When Full Web Control is selected, events are displayed on the appliance.
Sophos Enterprise Console

- For Sophos Web Appliance or Security Management Appliance, you can view browsing activity using the **Reports** and **Search** features. Block, Warn, and Allow actions are all shown. Visited HTTPS sites categorized as Warn are displayed as Proceed events because Sophos Endpoint Security and Control responds differently to HTTPS (see the note in Full Web Control).

- For UTM, use the **Logging & Reporting > Web Protection > Web Usage Report** page. There you can see actions showing whether the website has been delivered to the client (passed), whether it has been blocked by an application control rule, or whether a user gained access to a blocked page using the bypass blocking feature (overridden), as well as other information.

**Note**

Regardless of which policy you select, websites scanned and assessed by live URL-filtering in Sophos Endpoint Security and Control are displayed as web events in Sophos Enterprise Console.

To view web events:

1. On the **Events** menu, click **Web Events**. The **Web - Event Viewer** dialog box appears.
2. In the **Search period** box, click the drop-down arrow, and select the period for which you want to display the events.
   
   You can either select a fixed period, for example, **Within 24 hours**, or select **Custom** and specify your own time period by selecting the starting and ending dates and times.
3. If you want to view events for a certain **User** or **Computer**, enter the name in the respective field.
   
   If you leave the fields empty, events for all users and computers will be displayed.
   
   You can use wildcards in these fields. Use ? for any single character and * for any string of characters.
4. If you want to view events associated with a certain action, in the **Action** field, click the drop-down arrow and select the action.
5. If you want to view events associated with a specific domain, enter it in the **Domain** field.
6. If you want to view events that were triggered for a specific **Reason**, click the drop-down arrow and select the reason.
7. Click **Search** to display a list of events.

You can export the list of web events to a file.

**Related concepts**

- Managing roles and sub-estates (page 15)
- Inappropriate Website Control (page 177)
- Full Web Control (page 181)
- Web protection (page 106)

**Related tasks**

- Export the list of events to a file (page 206)

### 10.10.1 View latest web events on a computer

You can view the last 10 events for which an action was taken on an endpoint computer, for example, recently blocked websites.

To view the latest web events:

1. In the **Endpoints** view, in the computer list, double-click the computer for which you want to view activity.
2. In the **Computer details** dialog box, scroll down to the **Latest web events** section.

You can also view the number of events for a user by generating a report.

**Related tasks**
- Configure the **Events by user report** (page 213)

### 10.11 View exploit prevention events

**Note**

This feature will be unavailable if your license doesn't include Exploit Prevention.

If you use role-based administration, you must have the **Exploit Prevention** right to view exploit prevention events in Sophos Enterprise Console.

**To view exploit prevention events:**

1. On the **Events** menu, click **Exploit Prevention**.

   The **Exploit Prevention - Event Viewer** dialog box appears.

2. In the **Search period** box, click the drop-down arrow, and select the period for which you want to display the events.

   You can either select a fixed period, for example, **Within 24 hours**, or select **Custom** and specify your own time period by selecting the starting and ending dates and times.

3. If you want to view events for a certain **User** or **Computer**, enter the name in the respective field.

   If you leave the fields empty, events for all users and computers will be displayed.

   You can use wildcards in these fields. Use ? for any single character and * for any string of characters.

4. If you want to view events associated with a certain type, in the **Type** field, click the drop-down arrow and select the type.

5. Click **Search** to display a list of events.

   - You can export the list of exploit prevention events to a file.
   - You can exclude exploit prevention events from exploit prevention.

**Related concepts**
- Managing roles and sub-estates (page 15)

**Related tasks**
- Export the list of events to a file (page 206)
- Exclude events from exploit prevention (page 207)

### 10.12 Export the list of events to a file

You can export the list of application control, data control, device control, firewall, patch assessment, tamper protection, web events or exploit prevention events to a comma separated value (CSV) file.

You can also export the list of patch assessment events to a PDF file.

1. On the **Events** menu, click one of the “events” options, depending on which event list you want to export.

   The **Event Viewer** dialog box appears.
2. If you want to display only certain events, in the **Search criteria** pane, set the filters as appropriate and click **Search** to display the events.

3. Click **Export**.

4. In the **Save As** window, browse to select a destination for the file, enter a file name in the **File name** dialog box, and select a file type in the **Save as type** dialog box.

5. Click **Save**.

---

**10.13 Exclude events from exploit prevention**

You can exclude applications and exploit prevention events from exploit prevention by selecting specific events from the event viewer.

1. On the **Events** menu, click **Exploit Prevention Events**. The **Event Viewer** dialog box appears.

2. If you want to display only certain events, in the **Search criteria** pane, set the filters as appropriate and click **Search** to display the events.

3. Click on an event then click **Exclude**. The **Exploit Prevention Exclusions** dialog box appears.

4. Click the policy you want to change. To change the settings for all policies, click **Select All**.

5. Under the **Exploit event** or **Application** section, click **Exclude**.

6. Click **OK**.

The exploit prevention event or application will be excluded from exploit prevention for the policies selected.

---

**Related tasks**

- View exploit prevention events (page 206)
11 Generating reports

Reports provide textual and graphical information on a variety of aspects of your network's security status.

Reports are available via the Report Manager. Using the Report Manager, you can quickly create a report based on an existing template, change configuration of an existing report, and schedule a report to run at regular intervals, with the results being sent to your chosen recipients as an email attachment. You can also print reports and export them in a number of formats.

Sophos provides a number of reports that you can use out of the box or configure to tailor your needs. These reports are:

- Alert and event history
- Alert summary
- Alerts and events by item name
- Alerts and events by time
- Alerts and events per location
- Endpoint policy non-compliance
- Events by user
- Managed endpoint protection
- Updating hierarchy

Reports and role-based administration

If you use role-based administration, you must have the Report configuration right to create, edit, or delete a report. If you do not have this right, you can only run a report.

A report can only include data from the active sub-estate. You cannot share reports between sub-estates. The default reports are not copied from the Default sub-estate to new sub-estates you create.

When you delete a sub-estate, all reports in that sub-estate are also deleted.

Related concepts
Managing roles and sub-estates (page 15)

11.1 Create a new report

If you use role-based administration, you must have the Report configuration right to perform this task.

To create a report:
1. Click the Reports icon on the toolbar.
2. In the Report Manager dialog box, click Create.
3. In the Create new report dialog box, select a report template and click OK.
   A wizard guides you through creating a report based on your chosen template.
If you do not want to use the wizard, in the **Create new report** dialog box, clear the **Use the wizard to create report** check box. You can then configure your new report in the report properties dialog box. For more information, see the topic on configuring the relevant report.

**Related concepts**
Managing roles and sub-estates (page 15)

### 11.2 Configure the Alert and event history report

If you use role-based administration, you must have the **Report configuration** right to perform this task.

The **Alert and event history** report shows alerts and events per specified reporting period.

1. Click the **Reports** icon on the toolbar.
2. In the **Report Manager** dialog box, select **Alert and event history** and click **Properties**.
3. In the **Alert and Event History Properties** dialog box, on the **Configuration** tab, set up the options you want.
   a) In the **Report details** panel, edit the name and description of the report, if you wish.
   b) In the **Reporting period** panel, in the **Period** text box, click the drop-down arrow and select a time period.
      You can either select a fixed period, for example, **Last month**, or select **Custom** and specify your own time period in the **Start** and **End** boxes.
   c) In the **Report location** panel, click **Group of computers** or **Individual computer**. Then click the drop-down arrow to specify a group or computer name.
   d) In the **Alert and event types to include** panel, select alert and event types you want to include in the report.
      By default, the report shows all alert and event types.
      Alternatively, you can configure the report to show only locations that have reported a particular alert or event. To specify a single alert or event, click **Advanced** and click an alert or event name in the list. To specify more than one alert or event, type a name in the text box, using wildcards. Use ? for any single character in the name, and * for any string of characters. For example, W32/* would specify all viruses with names beginning W32/.
4. On the **Display options** tab, select how you want to sort the alerts and events.
   By default, alert and event details are sorted according to **Alert and event name**. However, reports can also be sorted by **Computer name**, computer **Group name**, or **Date and time**.
5. On the **Schedule** tab, select **Schedule this report** if you want to run the report at regular intervals, with the results being sent to your chosen recipients as email attachments. Enter the start date and time and the frequency with which the report will be generated, specify the output file format and language, and enter the email addresses of the recipients of the report.

**Related concepts**
Managing roles and sub-estates (page 15)
11.3 Configure the Alert summary report

If you use role-based administration, you must have the Report configuration right to perform this task.

The Alert summary report provides statistics on the overall health and status of your network.

1. Click the Reports icon on the toolbar.
2. In the Report Manager dialog box, select Alert summary and click Properties.
3. In the Alert Summary Properties dialog box, on the Configuration tab, set up the options you want.
   a) In the Report details panel, edit the name and description of the report, if you wish.
   b) In the Reporting period panel, in the Period text box, click the drop-down arrow and select a time period.
      You can either select a fixed period, for example, Last month, or select Custom and specify your own time period in the Start and End boxes.
4. In the Display options tab, under Display results per, specify the intervals of time at which the non-compliance is measured, for example, each hour or each day, click the drop-down arrow and select an interval.
5. On the Schedule tab, select Schedule this report if you want to run the report at regular intervals, with the results being sent to your chosen recipients as email attachments. Enter the start date and time and the frequency with which the report will be generated, specify the output file format and language, and enter the email addresses of the recipients of the report.

Related concepts
Managing roles and sub-estates (page 15)

11.4 Configure the Alerts and events by item name report

If you use role-based administration, you must have the Report configuration right to perform this task.

The Alerts and events by item name report provides statistics on all alerts and events from all computers over a selected period, grouped by item name.

To configure the report:

1. Click the Reports icon on the toolbar.
2. In the Report Manager dialog box, select Alerts and events by item name and click Properties.
3. In the Alerts and Events by Item Name Properties dialog box, on the Configuration tab, set up the options you want.
   a) In the Report details panel, edit the name and description of the report, if you wish.
   b) In the Reporting period panel, in the Period text box, click the drop-down arrow and select a time period.
      You can either select a fixed period, for example, Last month, or select Custom and specify your own time period in the Start and End boxes.
c) In the **Report location** panel, click **Group of computers** or **Individual computer**. Then click the drop-down arrow to specify a group or computer name.

d) In the **Alert and event types to include** panel, select alert and event types you want to include in the report.

By default, the report shows all alert and event types.

4. On the **Display options** tab, under **Display**, choose which alerts and events you want the report to show.

By default, the report shows all alerts and events and the number of occurrences for each.

You can also configure the report to show only:

- the top \( n \) alerts and events (where \( n \) is a number you specify), or
- alerts and events with \( m \) occurrences or more (where \( m \) is a number you specify).

5. Under **Sort by**, select whether you want to sort alerts and events by the number or name.

By default, the report lists alerts and events in order of decreasing number of occurrences.

6. On the **Schedule** tab, select **Schedule this report** if you want to run the report at regular intervals, with the results being sent to your chosen recipients as email attachments. Enter the start date and time and the frequency with which the report will be generated, specify the output file format and language, and enter the email addresses of the recipients of the report.

**Related concepts**

Managing roles and sub-estates (page 15)

### 11.5 Configure the Alerts and events by time report

If you use role-based administration, you must have the **Report configuration** right to perform this task.

The **Alerts and events by time** report shows alerts and events summarized at specified intervals.

1. Click the **Reports** icon on the toolbar.
2. In the **Report Manager** dialog box, select **Alerts and events by time** and click **Properties**.
3. In the **Alerts and Events by Time Properties** dialog box, on the **Configuration** tab, set up the options you want.

   a) In the **Report details** panel, edit the name and description of the report, if you wish.

   b) In the **Reporting period** panel, in the **Period** text box, click the drop-down arrow and select a time period.

       You can either select a fixed period, for example, **Last month**, or select **Custom** and specify your own time period in the **Start** and **End** boxes.

   c) In the **Report location** panel, click **Group of computers** or **Individual computer**. Then click the drop-down arrow to specify a group or computer name.

   d) In the **Alert and event types to include** panel, select alert and event types you want to include in the report.

       By default, the report shows all alert and event types.

       Alternatively, you can configure the report to show only locations that have reported a particular alert or event. To specify a single alert or event, click **Advanced** and click an alert or event name in the list. To specify more than one alert or event, type a name in the text.
box, using wildcards. Use ? for any single character in the name, and * for any string of characters. For example, W32/* would specify all viruses with names beginning W32/.

4. On the Display options tab, specify the intervals of time at which the rate of alerts and events is measured, for example, each hour or each day, click the drop-down arrow and select an interval.

5. On the Schedule tab, select Schedule this report if you want to run the report at regular intervals, with the results being sent to your chosen recipients as email attachments. Enter the start date and time and the frequency with which the report will be generated, specify the output file format and language, and enter the email addresses of the recipients of the report.

Related concepts
Managing roles and sub-estates (page 15)

11.6 Configure the Alerts and events per location report

If you use role-based administration, you must have the Report configuration right to perform this task.

The Alerts and events per location report provides statistics on all alerts from all computers over a selected period, grouped by location.

1. Click the Reports icon on the toolbar.
2. In the Report Manager dialog box, select Alerts and events per location and click Properties.
3. In the Alerts and Events per Location Properties dialog box, on the Configuration tab, set up the options you want.
   a) In the Report details panel, edit the name and description of the report, if you wish.
   b) In the Reporting period panel, in the Period text box, click the drop-down arrow and select a time period.
      You can either select a fixed period, for example, Last month, or select Custom and specify your own time period in the Start and End boxes.
   c) In the Report location panel, click Computers to show alerts per computer or Group to show alerts for each group of computers.
   d) In the Alert and event types to include panel, select alert and event types you want to include in the report.
      By default, the report shows all alert and event types.
      Alternatively, you can configure the report to show only locations that have reported a particular alert or event. To specify a single alert or event, click Advanced and click an alert or event name in the list. To specify more than one alert or event, type a name in the text box, using wildcards. Use ? for any single character in the name, and * for any string of characters. For example, W32/* would specify all viruses with names beginning W32/.
4. On the Display options tab, under Display, choose which locations you want the report to show.
   By default, the report shows all computers and groups and the number of occurrences for each. You can configure it to show only:
   • the top \( n \) locations that have recorded the most alerts and events (where \( n \) is a number you specify), or
   • locations with \( m \) alerts and events or more (where \( m \) is a number you specify).
5. Under Sort by, select whether you want to sort locations by the number of items detected or name.
By default, the report lists locations in order of decreasing number of alerts and events per location. Select Location if you want them sorted by name in alphabetical order.

6. On the Schedule tab, select Schedule this report if you want to run the report at regular intervals, with the results being sent to your chosen recipients as email attachments. Enter the start date and time and the frequency with which the report will be generated, specify the output file format and language, and enter the email addresses of the recipients of the report.

Related concepts
Managing roles and sub-estates (page 15)

11.7 Configure the Endpoint policy non-compliance report

If you use role-based administration, you must have the Report configuration right to perform this task.

The Endpoint policy non-compliance report shows the percentage or number of computers that do not comply with their group policy, summarized at specified intervals.

1. Click the Reports icon on the toolbar.
2. In the Report Manager dialog box, select Endpoint policy non-compliance and click Properties.
3. In the Endpoint Policy Non-Compliance Properties dialog box, on the Configuration tab, set up the options you want.
   a) In the Report details panel, edit the name and description of the report, if you wish.
   b) In the Reporting period panel, in the Period text box, click the drop-down arrow and select a time period.
      You can either select a fixed period, for example, Last month, or select Custom and specify your own time period in the Start and End boxes.
   c) In the Show panel, select the policies you want to show in the report. By default, only Anti-virus and HIPS policy is selected.
4. In the Display options tab, under Display results per, specify the intervals of time at which the non-compliance is measured, for example, each hour or each day, click the drop-down arrow and select an interval.
5. Under Display results as, select whether you want to display results as percentages or numbers.
6. On the Schedule tab, select Schedule this report if you want to run the report at regular intervals, with the results being sent to your chosen recipients as email attachments. Enter the start date and time and the frequency with which the report will be generated, specify the output file format and language, and enter the email addresses of the recipients of the report.

Related concepts
Managing roles and sub-estates (page 15)

11.8 Configure the Events by user report

If you use role-based administration, you must have the Report configuration right to perform this task.
The Events by user report shows application control, firewall, data control, and device control events, along with web events, grouped by user.

1. Click the Reports icon on the toolbar.
2. In the Report Manager dialog box, select Events by user and click Properties.
3. In the Events by User Properties dialog box, on the Configuration tab, set up the options you want.
   a) In the Report details panel, edit the name and description of the report, if you wish.
   b) In the Reporting period panel, in the Period text box, click the drop-down arrow and select a time period.
      You can either select a fixed period, for example, Last month, or select Custom and specify your own time period in the Start and End boxes.
   c) Under Event types to include, select the features for which you want to show events.
4. On the Display options tab, under Display, choose which users you want the report to show.
   By default, the report shows all users and the number of events for each. You can configure it to show only:
   • the top \( n \) users that have recorded the most events (where \( n \) is a number you specify), or
   • users with \( m \) events or more (where \( m \) is a number you specify).
5. Under Sort by, select whether you want to sort users by the number of events or name.
   By default, the report lists users in order of decreasing number of events per user. Select User if you want them sorted by name in alphabetical order.
6. On the Schedule tab, select Schedule this report if you want to run the report at regular intervals, with the results being sent to your chosen recipients as email attachments. Enter the start date and time and the frequency with which the report will be generated, specify the output file format and language, and enter the email addresses of the recipients of the report.

Related concepts
Managing roles and sub-estates (page 15)

11.9 Configure the Managed endpoint protection report

If you use role-based administration, you must have the Report configuration right to perform this task.

The Managed endpoint protection report shows the percentage or number of protected computers, summarized at specified intervals.

1. Click the Reports icon on the toolbar.
2. In the Report Manager dialog box, select Managed endpoint protection and click Properties.
3. In the Managed Endpoint Protection Properties dialog box, on the Configuration tab, set up the options you want.
   a) In the Report identity panel, edit the name and description of the report, if you wish.
   b) In the Reporting period panel, in the Period text box, click the drop-down arrow and select a time period.
      You can either select a fixed period, for example, Last month, or select Custom and specify your own time period in the Start and End boxes.
c) In the **Show** panel, select the features you want to show in the report.

4. In the **Display options** tab, under **Display results per**, specify the intervals of time at which the non-compliance is measured, for example, each hour or each day, click the drop-down arrow and select an interval.

5. Under **Display results as**, select whether you want to display results as percentages or numbers.

6. On the **Schedule** tab, select **Schedule this report** if you want to run the report at regular intervals, with the results being sent to your chosen recipients as email attachments. Enter the start date and time and the frequency with which the report will be generated, specify the output file format and language, and enter the email addresses of the recipients of the report.

**Related concepts**

Managing roles and sub-estates (page 15)

### 11.10 Updating hierarchy report

The **Updating hierarchy** report shows update managers on your network, update shares that they maintain, and the number of computers that update from these shares.

You cannot configure the **Updating hierarchy** report. You can run the report.

**Related tasks**

Run a report (page 215)

### 11.11 Schedule a report

If you use role-based administration, you must have the **Report configuration** right to perform this task.

You can schedule a report to run at regular intervals, with the results being sent to your chosen recipients as email attachments.

1. Click the **Reports** icon on the toolbar.
2. In the **Report Manager** dialog box, select the report you want to schedule and click **Schedule**.
3. In the dialog box that appears, on the **Schedule** tab, select **Schedule this report**.
4. Enter the start date and time and the frequency with which the report will be generated.
5. Specify the output file format and language.
6. Enter the email addresses of the recipients of the report.

**Related concepts**

Managing roles and sub-estates (page 15)

### 11.12 Run a report

1. Click the **Reports** icon on the toolbar.
2. In the **Report Manager** dialog box, select the report you want to run and click **Run**.
   The **Reporting** window, showing the report, is displayed.

You can change the report layout, print the report or export it to a file.
11.13 View a report as a table or chart

Some reports can be viewed both as a table and as a chart. If this is the case, you will see two tabs, Table and Chart in the Reporting window displaying the report.

1. Click the Reports icon on the toolbar.
2. In the Report Manager dialog box, select the report you want to run, for example, Alerts and events per location, and click Run.
   The Reporting window, showing the report, is displayed.
3. To view the report as a table or chart, go to the respective tab.

11.14 Print a report

To print a report, click the Print icon on the toolbar at the top of the report.

11.15 Export a report to a file

To export a report to a file:

1. Click the Export icon in the toolbar at the top of the report.
2. In the Export report dialog box, select the type of document or spreadsheet you would like to export the report to. The options are:
   - PDF (Acrobat)
   - HTML
   - Microsoft Excel
   - Microsoft Word
   - Rich Text Format (RTF)
   - Comma separated values (CSV)
   - XML
3. Click the File Name browse button to select a location. Then enter a name. Click OK.

11.16 Change the report layout

You can change the page layout used for reports. For example, you can display a report in landscape (wide-page) format.

1. Click the page layout icon in the toolbar at the top of the report.
2. In the Page Setup dialog box, specify page size, orientation and margins. Click OK.
The report is then displayed with these page settings.
These page settings are also used when you print or export the report.
12 Auditing

Auditing enables you to monitor changes in Enterprise Console configuration and other user or system actions. You can use this information for regulatory compliance and troubleshooting or, in the case of malicious activity, during a forensic analysis.

By default, auditing is disabled. After you enable auditing, an audit entry is written to the auditing database whenever certain configuration settings are changed or certain actions are performed.

Note
If you use role-based administration, you must have the Auditing right to enable or disable auditing.

The audit entry includes the following information:

- Action performed
- User who performed the action
- User's computer
- User's sub-estate
- Date and time of the action

Both successful and failed attempts at actions are audited, so the audit entries can show who performed actions on the system and who started actions that did not complete successfully.

Audited actions include:

<table>
<thead>
<tr>
<th>Category</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer actions</td>
<td>Acknowledge/resolve alerts and errors, protect a computer, update a computer, delete a computer, perform a full system scan on a computer.</td>
</tr>
<tr>
<td>Computer group management</td>
<td>Create a group, delete a group, move a group, rename a group, assign a computer to a group.</td>
</tr>
<tr>
<td>Policy management</td>
<td>Create a policy, rename a policy, duplicate a policy, edit a policy, assign a policy to a computer, reset a policy to factory defaults, delete a policy.</td>
</tr>
<tr>
<td>Role management</td>
<td>Create a role, delete a role, rename a role, duplicate a role, add a user to a role, remove a user from a role, add a right to a role, remove a right from a role.</td>
</tr>
<tr>
<td>Update manager management</td>
<td>Update an update manager, make an update manager comply with configuration, acknowledge alerts, delete an update manager, configure an update manager, add a new software subscription, delete a software subscription, rename a software subscription, edit a software subscription, duplicate a software subscription.</td>
</tr>
<tr>
<td>System events</td>
<td>Enable auditing, disable auditing.</td>
</tr>
</tbody>
</table>

You can use third-party programs, such as Microsoft Excel, Microsoft Access, Microsoft SQL Server Reporting Services, or Crystal Reports, to access and analyze data stored in the auditing database.
For information about how to view audit entries, see the Sophos Enterprise Console auditing user guide.

**Related concepts**
Managing roles and sub-estates (page 15)

### 12.1 Enable or disable auditing

If you use role-based administration, you must have the **Auditing** right to enable or disable auditing.

To enable or disable auditing:

1. On the **Tools** menu, click **Manage Auditing**.
2. In the **Manage Auditing** dialog box, select or clear the **Enable auditing** check box to enable or disable auditing. The option is disabled by default.

**Related concepts**
Managing roles and sub-estates (page 15)
13 Copying or printing data from Sophos Enterprise Console

13.1 Copy data from the computer list

You can copy information displayed in the computer list, in the Endpoints view, to the Clipboard and then paste it into another document in a tab-separated format.

1. In the Endpoints view, in the Groups pane, select the group of computers for which you want to copy data.
2. In the View drop-down list, select which computers you want to display, for example, Computers with potential problems.
3. If the group contains subgroups, select also whether you want to display computers At this level only or At this level and below.
4. In the computer list, go to the tab you want to display, for example, Anti-Virus Details.
5. Click anywhere in the computer list to bring the focus to it.
6. On the Edit menu, click Copy to copy the data to the Clipboard.

13.2 Print data from the computer list

You can print information displayed in the computer list, in the Endpoints view.

1. In the Endpoints view, in the Groups pane, select the group of computers for which you want to print data.
2. In the View drop-down list, select which computers you want to display, for example, Computers with potential problems.
3. If the group contains subgroups, select also whether you want to display computers At this level only or At this level and below.
4. In the computer list, go to the tab you want to display, for example, Anti-Virus Details.
5. Click anywhere in the computer list to bring the focus to it.
6. On the File menu, click Print.

13.3 Copy computer details for a computer

You can copy information from the Computer details dialog box to the Clipboard and then paste it into another document. The information includes computer name, computer's operating system, versions of the security software installed on the computer, any outstanding alerts and errors, update status, and so on.

1. In the Endpoints view, in the computer list, double-click the computer for which you want to copy the data.
2. In the Computer details dialog box, click Copy to copy the data to the Clipboard.
13.4 Print computer details for a computer

You can print information from the Computer details dialog box. The information includes computer name, computer’s operating system, versions of the security software installed on the computer, any outstanding alerts and errors, update status, and so on.

1. In the Endpoints view, in the computer list, double-click the computer for which you want to print the data.
2. In the Computer details dialog box, click Print.
14 Troubleshooting

When you run the Protect computers wizard, installation of security software can fail for a number of reasons.

• Automatic installation is not possible on that operating system. Perform a manual installation. For other operating systems (if your license permits you to protect them), see the Sophos Enterprise Console startup guide for Linux and UNIX.

• Operating system could not be determined. This may be because you did not enter your username in the format domain\username when finding computers.

• Firewall rules are blocking access needed to deploy the security software.

14.1 Computers are not running on-access scanning

If there are computers not running on-access scanning:

1. Check which anti-virus and HIPS policy is used by those computers.
2. Ensure that on-access scanning is enabled in that policy and that the computers comply with the policy.

Related tasks
Check which policies a group uses (page 27)
Turn on-access scanning on or off (page 89)
Make computers use the group policy (page 34)

14.2 The firewall is disabled

If there are computers with the firewall disabled:

1. Check which firewall policy is used by those computers.
2. Ensure that the firewall is enabled in that policy and that the computers comply with the policy.

Related tasks
Check which policies a group uses (page 27)
Temporarily disable the firewall (page 122)
Make computers use the group policy (page 34)

14.3 The firewall is not installed

Note
If you use role-based administration, you must have the Computer search, protection and groups right to install the firewall.
Before you attempt to install the client firewall on endpoint computers, check that the computers are running a Windows client operating system.

**Note**

You cannot install the firewall on computers running server operating systems or Windows Vista Starter.

If there are computers on which you want to install the firewall:

1. Select the computers, right-click and select **Protect Computers**.

   The **Protect Computers Wizard** appears. Click **Next**.

2. When prompted to select features, select **Firewall**. Complete the wizard.

3. Click **Next**.

4. When prompted to select features, select **Firewall**.

5. Complete the wizard.

If the problem persists, contact Sophos technical support.

**Related concepts**

*Managing roles and sub-estates* (page 15)

### 14.4 Computers have outstanding alerts

- You need to clean up computers, if there are computers with a virus, or an application you do not want.
- You need to authorize adware and PUAs, if there are computers with an adware or other potentially unwanted application that you do want.
- You can diagnose and update out-of-date computers.

**Note**

If you do not need the alert displayed any more, you can clear it. Select the computers with alerts, right-click and select **Resolve Alerts and Errors**. You must have the **Remediation - cleanup** right to acknowledge (clear) alerts and errors.

**Related tasks**

*Clean up computers now* (page 59)

*Authorize adware and PUAs* (page 113)

*Update out-of-date computers* (page 83)

### 14.5 Computers are not managed by the console

Windows, Mac, Linux, and UNIX computers should be managed by Sophos Enterprise Console, so that they can be updated and monitored.
Note
Unless you use Active Directory synchronization, new computers added to the network are not
displayed or managed by the console automatically. Click **Discover computers** in the toolbar to
search for them and place them in the **Unassigned** group.

If a computer is not managed, its details on the **Status** tab are grayed out.

To start managing unmanaged computers:

1. In the **View** drop-down list, select **Unmanaged computers**.
2. Do one of the following:
   - If the unmanaged computers are in the **Unassigned** group, select the computers and drag and
drop them onto the group where you want to place them. The **Protect Computers Wizard** is
launched to help you protect them.
   - If the computers are already in a group, select them, right-click and select **Protect Computers**
to install a managed version of Sophos Endpoint Security and Control.
3. If there are computers on which Sophos Enterprise Console cannot install Sophos Endpoint
Security and Control automatically, carry out a manual installation.

Automatic installation using the **Protect Computers Wizard** is only available for Windows
computers. If you need to protect Macs, Linux or UNIX computers, install the software manually.

For information about protecting Macs or Windows computers manually, see the **Sophos
Enterprise Console advanced startup guide**.

For information about protecting Linux or UNIX, see the **Sophos Enterprise Console startup
guide for Linux and UNIX**.

**Related concepts**

**Managing roles and sub-estates** (page 15)

**14.6 Can't protect computers in the Unassigned group**

The **Unassigned** group is only for holding computers that are not yet in groups created by you, to
which policies can be applied. You cannot protect computers until you place them in such a group.

**14.7 Sophos Endpoint Security and Control installation failed**

If the **Protect Computers Wizard** fails to install Sophos Endpoint Security and Control on
computers, it could be because:

- Sophos Enterprise Console does not know which operating system the computers are running.
  This is probably because you did not enter your username in the format domain\user when finding
computers.
- Automatic installation is not possible on that operating system. Perform a manual installation. For
instructions, see the **Sophos Enterprise Console advanced startup guide**.
- The computers are running a firewall.
• “Simple File Sharing” has not been turned off on Windows XP computers.
• The “Use Sharing Wizard” option has not been turned off on Windows Vista computers.
• You selected to install a feature that is not supported on the computers’ operating systems.

For a full list of requirements for the Sophos Endpoint Security and Control features, see the system requirements page on the Sophos website.

**Related information**
Sophos system requirements

### 14.8 Computers are not updated

See [Update out-of-date computers](#) (page 83) for help with diagnosing and fixing the problem.

### 14.9 Anti-virus settings do not take effect on Macs

Some anti-virus settings cannot be applied to Mac computers. In this case, there is a warning on that page of settings.

For more information about anti-virus and HIPS policy settings that apply to Macs, see [knowledge base article 118859](#).

**Related information**
knowledge base article 118859

### 14.10 Anti-virus settings do not take effect on Linux or UNIX

Some anti-virus settings can't be applied to Linux or UNIX computers. In this case, there is a warning on that page of settings.

You can change anti-virus settings on Linux computers using the `savconfig` and `savscan` commands as described in the [Sophos Anti-Virus for Linux configuration guide](#).

You can change anti-virus settings on UNIX computers using the `savscan` command as described in the [Sophos Anti-Virus for UNIX configuration guide](#).

### 14.11 Linux or UNIX computer does not comply with policy

If you use a corporate configuration file in the CID, and the file contains a configuration value which conflicts with the policy, the computer is shown as not complying with the policy.

Selecting the **Comply with policy** option brings the computer in compliance only temporarily, until the CID-based configuration is reapplied.

To resolve the problem, review the corporate configuration file and, where possible, replace by console-based configuration.
14.12 New scan appears unexpectedly on a Windows computer

If you look at the local copy of Sophos Enterprise Console on Windows computers, you may see that a new “Available scan” is listed, even though the user has not created one. This new scan is actually a scheduled scan that you have set up from the console. You should not delete it.

14.13 Connectivity and timeout problems

If the communications between Sophos Enterprise Console and a networked computer become slow or the computer becomes unresponsive, there may be a connectivity problem.

Check the Sophos Network Communications Report that presents an overview of the current state of communications between a computer and Sophos Enterprise Console. To view the report, go to the computer where the problem occurred. On the taskbar, click the Start button, select All Programs > Sophos > Sophos Endpoint Security and Control, and then click View Sophos Network Communications Report.

The report shows possible problem areas and, if a problem is detected, remedial actions.

14.14 Adware and PUAs are not detected

If adware and other potentially unwanted applications (PUAs) are not detected, you should check that:

- Detection has been enabled.
- The applications are on a computer running Windows.

Related tasks
Configure on-access scanning (page 87)

14.15 Partially detected item

Sophos Endpoint Security and Control may report that an item (for example, a Trojan or potentially unwanted application) is “partially detected”. This means that it has not found all the component parts of that application.

To find the other components, you need to carry out a full system scan of the computer(s) affected. On computers running Windows, you can do this by selecting the computer(s), right-clicking and selecting Full system scan. You can also set up a scheduled scan for adware and other potentially unwanted applications.

If the application has still not been fully detected, it may be because:

- you have insufficient access rights
- some drives or folders on the computer, containing the application’s components, are excluded from scanning.
If the latter is the case, check the list of items excluded from scanning. If there are some items on the list, remove them from the list and scan your computer again.

Sophos Endpoint Security and Control may not be able to fully detect or remove adware and other potentially unwanted applications with components installed on network drives.

For advice, contact Sophos technical support.

**Related tasks**
- Configure on-access scanning (page 87)
- Create a scheduled scan (page 93)
- Exclude items from on-access scanning (page 92)

### 14.16 Frequent alerts about potentially unwanted applications

You may receive very large numbers of alerts about potentially unwanted applications, including multiple reports of the same application.

This can occur because some types of potentially unwanted application "monitor" files, trying to access them frequently. If you have on-access scanning enabled, Sophos Enterprise Console detects each file access and sends an alert.

You should do one of the following:
- Disable on-access scanning for adware and PUA. You can use a scheduled scan instead.
- Authorize the application (if you want to have it running on your computers).
- Clean up the computers, removing applications that you have not authorized.

**Related tasks**
- Authorize adware and PUAs (page 113)
- Clean up computers now (page 59)

### 14.17 Cleanup failed

If Sophos Endpoint Security and Control fails in an attempt to clean up items ("Cleanup failed"), the reason could be:
- It has not found all the components of a multi-component item. Run a full system scan of the computer(s) to find the other components.
- Some drives or folders that contain item components are excluded from scanning. Check the items excluded from scanning. If there are some items on the list, remove them from the list.
- You have insufficient access rights.
- It can't clean up that type of item.
- It has found a virus fragment, rather than an exact virus match.
- The item is on a write-protected floppy disk or CD.
- The item is on a write-protected NTFS volume (Windows).
14.18 Recover from virus side-effects

Cleanup can remove a virus from computers, but it can't always reverse the side-effects.

Some viruses leave no side-effects. Others may make changes or corrupt data in ways that are hard to detect. To deal with this, you should:

• On the Help menu, click View Security Information. This connects you to the Sophos website, where you can read the virus analysis.

• Use backups or original copies of programs to replace infected programs. If you did not have backup copies before the infection, create them now 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.

14.19 Recover from application side-effects

Cleanup can remove unwanted applications, but it can't always reverse the side-effects.

Some applications modify the operating system, e.g. by changing your internet connection settings. Sophos Endpoint Security and Control cannot always restore all settings. For example, if an application changed the browser home page, Sophos Endpoint Security and Control cannot know what the previous home page setting was.

Some applications install utilities, such as .dll or .ocx files, on your computer. If a utility is harmless (that is, does not possess the qualities of a potentially unwanted application), e.g. a language library, and is not integral to the application, Sophos Endpoint Security and Control may not detect it as part of the application. In this case, cleanup won't remove the file from your computer.

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

You should:

• On the Help menu, click View Security Information. This connects you to the Sophos website, where you can read the application analysis.

• Use backups to restore your system settings or programs you want to use. If you did not have backup copies before, create them now in case of future incidents.

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

14.20 Data control does not detect files uploaded via embedded browsers

Data control intercepts documents which are uploaded via standalone web browsers. It does not intercept documents uploaded via browsers embedded in third-party applications (for example,
Lotus Notes). If you have a third-party application with an embedded browser and want to monitor all uploaded documents, you must configure the application to launch an external browser.

14.21 Data control does not scan uploaded or attached files

If data control does not scan files uploaded or attached from a network location using a monitored application (for example, an email client, a web browser, or an instant messaging (IM) client), it may be because you excluded remote files from on-access scanning in the anti-virus and HIPS policy. In this case, data control uses the same set of exclusions as the Sophos Anti-Virus on-access scanner (InterCheck™), so if remote file scanning is disabled, it will not send any remote files for a data control check.

Note
Data control does not use on-access scanning exclusions when files are copied or moved using Windows Explorer. In this case, data control will intercept the transfer of files onto monitored storage devices from a network location, for example, copying files to a removable storage device or burning data onto optical media.

Related tasks
Exclude items from on-access scanning (page 92)

14.22 Uninstalled update manager is displayed in the console

After you uninstall an additional update manager, it may still be displayed in Sophos Enterprise Console, Update managers view.

To remove the update manager from the console, select it, right-click, and then click Delete.
15 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.
• Visit the Sophos support knowledge base at www.sophos.com/en-us/support.aspx.
• Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.
### 16 Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Active Directory synchronization event</strong></td>
<td>An event that occurs during synchronization with Active Directory.</td>
</tr>
<tr>
<td><strong>active sub-estate</strong></td>
<td>A sub-estate displayed in the Groups pane.</td>
</tr>
<tr>
<td><strong>advanced Content Control List editor</strong></td>
<td>An editor that enables a user to create a custom Content Control List that consists of a score, maximum count, regular expression, and a trigger score that must be reached before the Content Control List is matched.</td>
</tr>
<tr>
<td><strong>Application manager</strong></td>
<td>A dialog box that enables you to allow or create new rules for applications that have been blocked by Sophos Client Firewall.</td>
</tr>
<tr>
<td><strong>auditing</strong></td>
<td>A feature that enables you to monitor changes in Sophos Enterprise Console configuration and other user and system actions.</td>
</tr>
<tr>
<td><strong>automatic protection</strong></td>
<td>Deployment of security software (installation and policy enforcement) on all the computers in an Active Directory container as soon as they are synchronized with Sophos Enterprise Console.</td>
</tr>
<tr>
<td><strong>category</strong></td>
<td>A specific tag that is used to classify SophosLabs Content Control Lists according to their type, regulation that defines their contents, or region they apply to.</td>
</tr>
<tr>
<td><strong>Content Control List (CCL)</strong></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><strong>content rule</strong></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><strong>controlled application</strong></td>
<td>A non-malicious application that an organization might want to detect or block because it undermines productivity or network performance.</td>
</tr>
<tr>
<td><strong>controlled data</strong></td>
<td>Files that meet data control conditions.</td>
</tr>
<tr>
<td><strong>controlled device</strong></td>
<td>A device that is subject to device control.</td>
</tr>
<tr>
<td><strong>critical level</strong></td>
<td>A value that triggers the change of an item’s security status to Critical.</td>
</tr>
<tr>
<td><strong>custom Content Control List</strong></td>
<td>A Content Control List that has been created by a Sophos customer. There are two ways to create a custom Content Control List: create a simple list of search terms with a specified search condition,</td>
</tr>
</tbody>
</table>
### Dashboard
An at-a-glance view of the network’s security status.

### Dashboard event
An event in which a dashboard health indicator exceeds critical level. An email alert is generated when a dashboard event occurs.

### 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 loss prevention (DLP)
See data control.

### database
The component of Sophos Enterprise Console that stores details about computers on the network.

### Default sub-estate
A sub-estate that has as its root the server root node of the group tree and the **Unassigned** group. It is displayed by default when you open Sophos Enterprise Console for the first time.

### 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.

### estate
See **IT estate**.

### exempt device
A device that is explicitly excluded from device control.

### expression
See **regular expression**.

### file matching rule
A rule that specifies the action that is taken if the user attempts to transfer a file with the specified file name or of the specified file type to the specified destination, for example, block the transfer of databases to removable storage devices.

### group
A group of managed computers defined in Sophos Enterprise Console.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>health indicator</td>
<td>Generic term for icons depicting security status of a dashboard section or item, or the overall health status of the network.</td>
</tr>
<tr>
<td>Host Intrusion Prevention System (HIPS)</td>
<td>A security technology that protects computers from suspicious files, unidentified viruses, and suspicious behavior.</td>
</tr>
<tr>
<td>IT estate</td>
<td>The company IT environment, including computers, network, and so on.</td>
</tr>
<tr>
<td>Malicious Traffic Detection</td>
<td>A feature that detects communications between compromised computers and attackers' command and control servers.</td>
</tr>
<tr>
<td>managed computer</td>
<td>A computer that has Remote Management System (RMS) installed and on which Sophos Enterprise Console can report and install and update software.</td>
</tr>
<tr>
<td>management console</td>
<td>The component of Sophos Enterprise Console that enables you to protect and manage computers.</td>
</tr>
<tr>
<td>management server</td>
<td>The component of Sophos Enterprise Console that handles updating and communications with networked computers.</td>
</tr>
<tr>
<td>maximum count</td>
<td>The maximum number of matches for a regular expression that can be counted towards the total score.</td>
</tr>
<tr>
<td>out-of-date computer</td>
<td>A computer that has not got up-to-date Sophos software.</td>
</tr>
<tr>
<td>patch assessment</td>
<td>Evaluates computers for installed patches and identifies missing patches.</td>
</tr>
<tr>
<td>policy</td>
<td>A group of settings, for example, for updating, applied to a group or groups of computers.</td>
</tr>
<tr>
<td>potentially unwanted application (PUA)</td>
<td>An application that is not inherently malicious but is generally considered unsuitable for the majority of business networks.</td>
</tr>
<tr>
<td>quantity</td>
<td>The volume of the Content Control List key data type that must be found in a file before the Content Control List is matched.</td>
</tr>
<tr>
<td>quantity key</td>
<td>The key type of data defined in a Content Control List, to which the quantity setting is applied. For example, for a Content Control List containing credit or debit card numbers, the quantity specifies how many credit or debit card numbers must be found in a file before the Content Control List is matched.</td>
</tr>
<tr>
<td>region</td>
<td>The scope of a SophosLabs Content Control List. The region either specifies the country the Content Control List applies to (for country-specific Content Control Lists) or shows “global” (for global Content Control Lists that apply to all countries).</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>regular expression</td>
<td>A search string that uses special characters to match a text pattern in a file. Data control uses Perl 5 regular expression syntax.</td>
</tr>
<tr>
<td>right</td>
<td>A set of permissions to perform certain tasks in Sophos Enterprise Console.</td>
</tr>
<tr>
<td>role</td>
<td>A set of rights that determines access to Sophos Enterprise Console.</td>
</tr>
<tr>
<td>role-based administration</td>
<td>A feature that allows you to specify which computers a user can access and which tasks they can carry out, depending on their role in your organization.</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>rule</td>
<td>A rule specifies the action that is taken if a file meets certain conditions. There are two types of data control rule: file matching rule and content rule.</td>
</tr>
<tr>
<td>score</td>
<td>The number that is added to the total score for a Content Control List when a regular expression is matched.</td>
</tr>
<tr>
<td>server root node</td>
<td>The topmost node of the group tree in the Groups pane, which includes the Unassigned group.</td>
</tr>
<tr>
<td>Sophos Live Protection</td>
<td>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.</td>
</tr>
<tr>
<td>Sophos Update Manager (SUM)</td>
<td>A program that downloads Sophos security software and updates from Sophos or another update server to shared update locations.</td>
</tr>
<tr>
<td>Sophos-defined rule</td>
<td>A rule that has been provided by Sophos as an example. Sophos-defined rules are not updated by Sophos.</td>
</tr>
<tr>
<td>SophosLabs Content Control List</td>
<td>A Content Control List that has been provided and is managed by Sophos. Sophos can update SophosLabs Content Control Lists or create new Content Control Lists and make them available in Sophos Enterprise Console. The contents of SophosLabs Content Control Lists cannot be edited. However, the quantity can be set for each such Content Control List.</td>
</tr>
<tr>
<td>sub-estate</td>
<td>A named part of the IT estate, containing a subset of the computers and groups.</td>
</tr>
<tr>
<td>sub-estate administration</td>
<td>A feature that restricts the computers and groups that are available to perform operations on.</td>
</tr>
<tr>
<td>software subscription</td>
<td>A set of versions of software for a variety of platforms, selected by the user, that Update Manager will download and keep updated. One</td>
</tr>
</tbody>
</table>
**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.

**synchronization interval**
The period after which a synchronization point in Sophos Enterprise Console is synchronized with the selected Active Directory container.

**synchronization point (for an Active Directory tree)**
A Sophos Enterprise Console group into which the contents of a selected Active Directory container (groups and computers or groups only) will be added for synchronization, their structure preserved.

**synchronization with Active Directory**
a one-way synchronization of Sophos Enterprise Console group(s) with Active Directory organizational units, or containers.

**synchronized group**
Any group below the synchronization point.

**System Administrator**
A preconfigured role that has full rights to manage Sophos security software on the network and roles in Sophos Enterprise Console.

The System Administrator role cannot be deleted or have its rights or name changed, and the Sophos Full Administrators Windows group cannot be removed from it. Other users and groups can be added to or removed from the role.

**tag**
A descriptor applied to a SophosLabs Content Control List to identify the contents or scope of the Content Control List. There are three types of tag: type, regulation, and region.

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

**threshold level**
A value that triggers the change of an item’s security status to Warning or Critical.

**total score**
The sum of the scores for a Content Control List, according to the content that has been matched.

**trigger score**
The number of times a regular expression must be matched before a Content Control List is matched.

**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.
| **type** | The criteria according to which SophosLabs Content Control Lists are classified, for example, a Content Control List defining passport details, postal addresses, or email addresses belongs to the Personally Identifiable Information type. |
| **update manager** | See Sophos Update Manager. |
| **warning level** | A value that triggers the change of an item’s security status to Warning. |
| **web control** | A feature that allows you to set and enforce web access policies for your organization, and to view reports on web browsing usage. You can allow or block user access to certain categories of websites, and users can also be warned whether visiting a website will violate your policies. |
| **web protection** | A feature that detects threats in web pages. This feature blocks sites that have hosted malicious content in the past and also prevents malicious downloads. Web protection is part of the anti-virus and HIPS policy. |
17 Legal notices

Copyright © 2009 - 2020 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.

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