

SOPHOS

simple + secure

Sophos Enterprise Manager Help

Product version: 4.7

Document date: July 2011



Contents

1 About Sophos Enterprise Manager.....	3
2 Guide to the Enterprise Manager interface.....	4
3 Getting started.....	12
4 Setting up Enterprise Manager.....	14
5 Protecting computers.....	31
6 Updating computers.....	46
7 Configuring policies.....	60
8 Setting up alerts and messages.....	114
9 Generating reports.....	123
10 Copying or printing data from Enterprise Manager.....	133
11 Troubleshooting.....	135
12 Glossary.....	142
13 Technical support.....	145
14 Legal notices.....	146

1 About Sophos Enterprise Manager

Sophos Enterprise Manager, version 4.7, is a single, automated console that manages and updates Sophos security software on Windows, Mac and Linux computers. Enterprise Manager enables you to:

- Protect your network against viruses, Trojans, worms, spyware, malicious websites, and unknown threats, as well as adware and other potentially unwanted applications.
- Manage client firewall protection on 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.

To learn how Enterprise Manager and associated licenses differ from other Sophos's products and licenses, see Sophos support knowledgebase article 113711 (<http://www.sophos.com/support/knowledgebase/article/113711.html>).

2 Guide to the Enterprise Manager interface

2.1 User interface layout

The Enterprise Manager 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.

For more information, see [Toolbar buttons](#) (page 5).

Dashboard

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

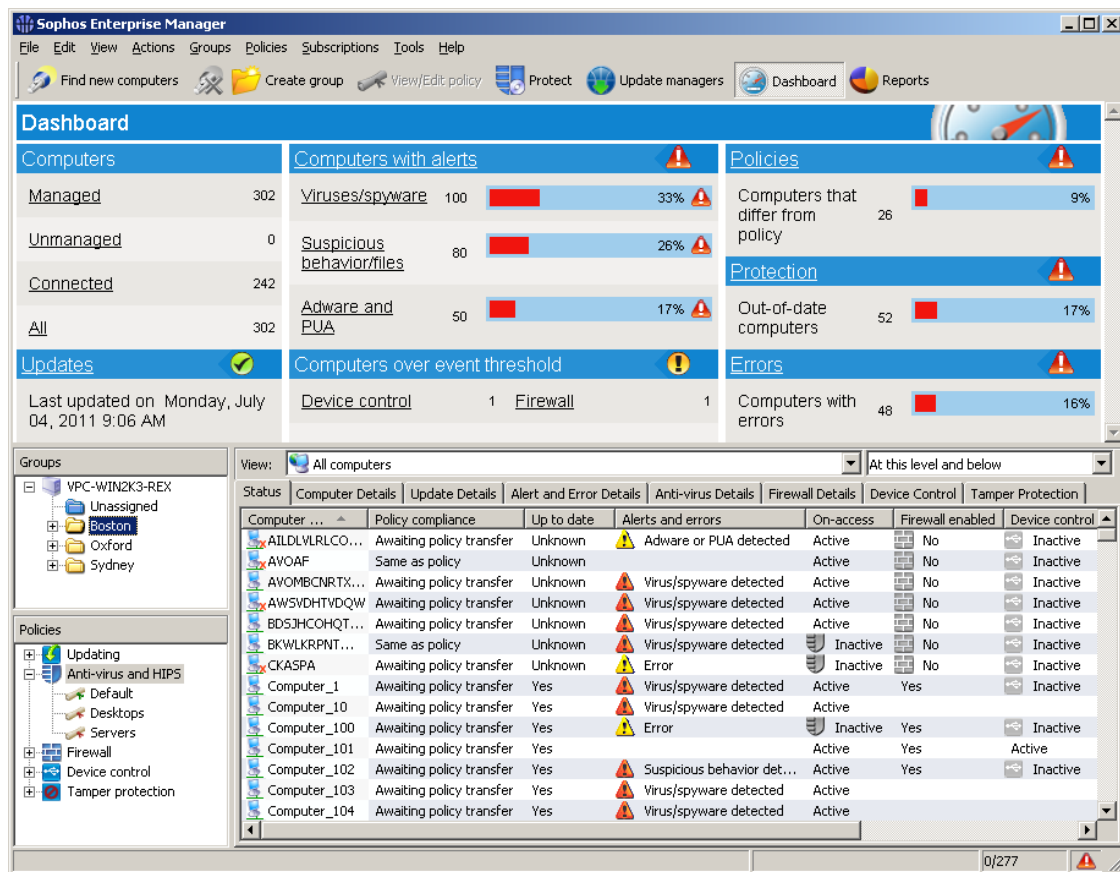
For more information, see [Dashboard panels](#) (page 6).

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. For more information, see [Navigating the Endpoints view](#) (page 9).
- **Update managers** view displays the computer where Sophos Update Manager is installed. For more information, see [Navigating the Update managers view](#) (page 11).

The screenshot below shows the computer list in the **Endpoints** view.



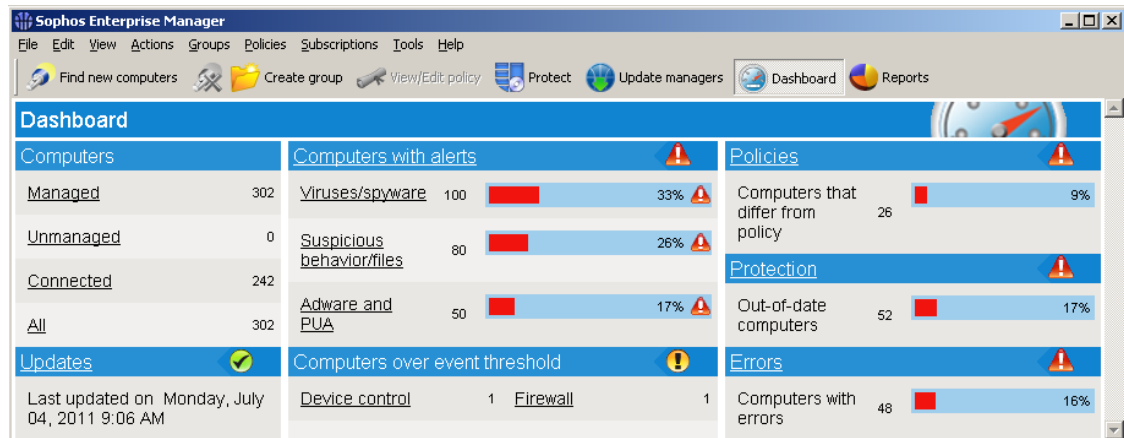
2.2 Toolbar buttons

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.

Toolbar Button	Description
Find new computers	Searches for computers on the network and add them to the console. For more information, see Choose how to find computers (page 26) and the other topics in the <i>Setting up Enterprise Manager > Finding computers on the network</i> section.
Create group	Creates a new group for computers. For more information, see Create a group (page 19).
View/Edit policy	Opens the policy selected in the Policies pane for editing. For more information, see Edit a policy (page 25).

Toolbar Button	Description
Protect	Installs anti-virus and firewall software on the computers selected in the computer list. For more information, see Protect computers (page 33).
Endpoints	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. For more information, see Navigating the Endpoints view (page 9).
Update managers	Switches to the Update managers view in the computer list. The Update managers view displays the computer where Sophos Update Manager is installed. For more information, see Navigating the Update managers view (page 11).
Dashboard	Shows or hides the Dashboard . The Dashboard provides an at-a-glance view of your network's security status. For more information, see Dashboard panels (page 6).
Reports	Starts Report Manager so that you can generate reports about alerts and events on your network. For more information, see About reports (page 123) and the other topics in the Generating reports section.

2.3 Dashboard panels






The **Dashboard** contains the following panels:

Dashboard Panel	Description
Computers	<p>Displays the total number of computers on the network and the number of connected, managed and unmanaged computers.</p> <p>To view a list of managed, unmanaged, connected, or all computers, click a link in the Computers area.</p>
Updates	<p>Displays the status of the update manager.</p>
Computers with alerts	<p>Displays the number and percentage of managed computers with alerts about:</p> <ul style="list-style-type: none"> ■ Known and unknown viruses and spyware ■ Suspicious behavior and files ■ Adware and other potentially unwanted applications <p>To view a list of managed computers with outstanding alerts, click the panel title Computers with alerts.</p>
Computers over event threshold	<p>Displays the number of computers with events over the threshold within the last seven days.</p> <p>To view a list of computers with device control or firewall events, click a link in the Computers over event threshold panel.</p>
Policies	<p>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.</p> <p>To view a list of managed computers that differ from policy, click the panel title Policies.</p>
Protection	<p>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.</p> <p>To view a list of managed connected out-of-date computers, click the panel title Protection.</p>
Errors	<p>Displays the number and percentage of managed computers with outstanding scanning, updating, or firewall errors.</p> <p>To view a list of managed computers with outstanding Sophos product errors, click the panel title Errors.</p>

2.4 Security status icons

The following table describes the security status icons displayed in the **Dashboard** and the Enterprise Manager status bar.

Security Status icon	Description
	<p>Normal</p> <p>The number of affected computers is below the warning level.</p>
	<p>Warning</p> <p>The warning level has been exceeded.</p>
	<p>Critical</p> <p>The critical level has been exceeded.</p>

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 particular 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 Enterprise Manager status bar. It shows the overall security status of your network.

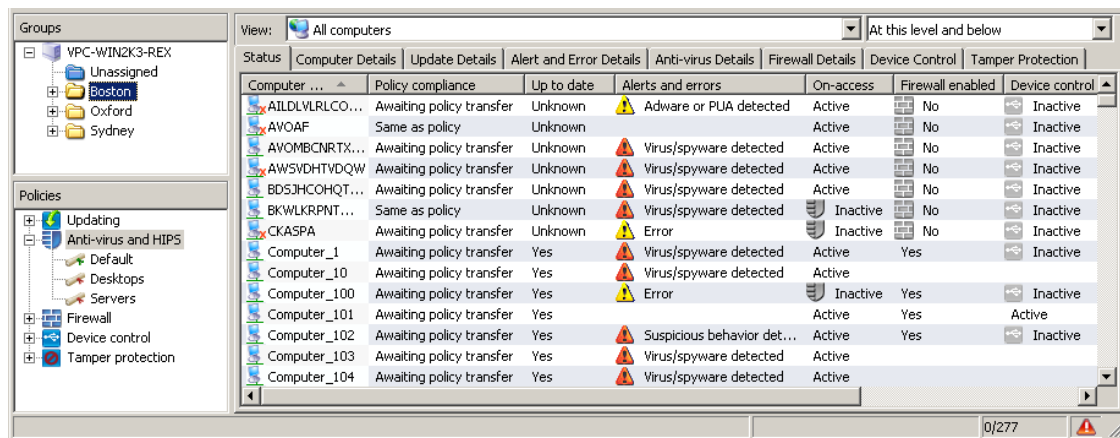
The network health icon shows the status of the **Dashboard** panel with the most severe status, that is:

- 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**.

When you first install Enterprise Manager, the **Dashboard** uses the default warning and critical levels. To configure your own warning and critical levels, see [Configure the Dashboard](#) (page 35).

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. For instructions, see [Set up network status email alerts](#) (page 118).

2.5 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.

For an explanation of the icons displayed in the computer list, see [Computer list icons](#) (page 10).

You can copy or print data displayed in the computer list. For more information, see [Copy data from the computer list](#) (page 133) and the other topics in the section *Copying or printing data from Enterprise Manager*.

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 Manager computer groups.

For more information, see [What are groups for?](#) (page 18) and the other topics in the *Setting up Enterprise Manager > Creating and using groups* section.

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. For more information, see the following:

- [About policies](#) (page 22) and the other topics in the *Setting up Enterprise Manager > Creating and using policies* section

- The *Configuring policies* section

2.6 Computer list icons




Alerts

Icon	Explanation
	A red warning sign displayed in the Alerts and errors column on the Status tab means that a virus, worm, Trojan, spyware, or suspicious behavior has been detected.
	<p>A yellow warning sign displayed in the Alerts and errors column on the Status tab indicates one of the following problems:</p> <ul style="list-style-type: none"> ■ A suspicious file has been detected. ■ An adware or other potentially unwanted application has been detected. ■ An error has occurred. <p>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.</p>







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)

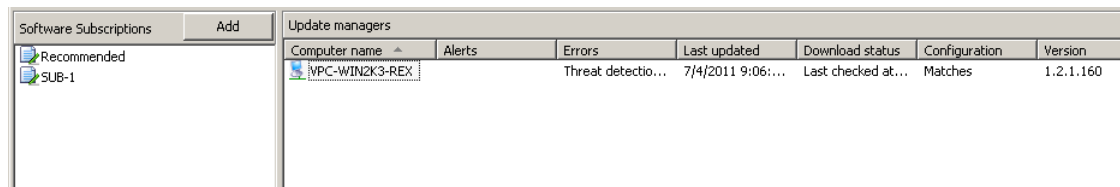
Protection disabled or out of date

Icon	Explanation
	A gray shield means that on-access scanning is inactive.
	A gray firewall sign means that the firewall is disabled.
	A clock icon means that the software is out of date.

Computer status

Icon	Explanation
	A blue computer sign means that the computer is managed by Enterprise Manager.
	A computer sign with a yellow arrow means that installation of anti-virus and firewall software is pending.
	A computer sign with a green arrow means that installation is in progress.
	A computer sign with an hourglass means that the automatic updating component of the endpoint security software has been installed and is now downloading the latest version of the product.
	A gray computer sign means that the computer is not managed by Enterprise Manager.
	A computer sign with a red cross beside it means that the computer that is usually managed by Enterprise Manager is disconnected from the network. (Unmanaged disconnected computers are not shown.)

2.7 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 the update manager.

The computer list displays the computer 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.

3 Getting started

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

We recommend that you refer to the *Sophos Enterprise Manager policy setup guide* for advice on best practices for using and managing Sophos security software. Sophos documentation is published at <http://www.sophos.com/support/docs/>.

If you haven't completed the **Download Security Software Wizard**, see [Run the Download Security Software Wizard](#) (page 54).

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 Enterprise Manager computer groups.

If you want to import Active Directory containers, see [Import containers and computers from Active Directory](#) (page 27). We recommend that you first import containers from Active Directory without computers, then assign group policies to the groups, and then add computers to the groups.

For information about creating groups manually, see [What are groups for?](#) (page 18) and other topics in the subsection *Creating and using groups* under the *Setting up Enterprise Manager* section.

2. Set up policies.

Enterprise Manager 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. To configure the firewall policy, run the **Firewall policy** wizard. See [Set up a basic firewall policy](#) (page 76).

3. Find 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. Otherwise, see [Choose how to find computers](#) (page 26) and other topics in the subsection *Finding computers on the network* under the *Setting up Enterprise Manager* section.

4. Protect computers.

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. See [Protect computers](#) (page 33) and other topics in the section *Protecting computers*.

5. Check that computers are protected.

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 Enterprise Manager. For more information, see [How do I check that my network is protected?](#) (page 35).

6. Clean up computers.

If a virus, unwanted application, or other issue has been detected on your network, clean up affected computers as described in [Clean up computers now](#) (page 42).

Additional protection and administration options

By default, Sophos Endpoint Security and Control detects viruses, Trojans, worms and spyware and analyzes behavior of the programs running on the system. You can add further protection, for example, protection against adware, potentially unwanted applications (PUAs), suspicious or unwanted behavior, or accidental data loss from workstations. For more detail, see the following sections:

- [Scan for suspicious files](#) (page 62)
- [Scan for adware and PUAs](#) (page 65)
- [About device control](#) (page 104)
- [About tamper protection](#) (page 111)

You can set up role-based access to Enterprise Manager by assigning Windows users and groups to the four preconfigured roles - System Administrator, Administrator, Helpdesk, and Guest. The System Administrator role that includes the Sophos Full Administrators Windows group has full rights and does not require setting up. For more information, see [About roles](#) (page 14).

4 Setting up Enterprise Manager

4.1 Managing roles

4.1.1 About roles

Important: If you already use role-based administration, you must have the **Role-based administration** right to set up roles. The System Administrator role that includes the Sophos Full Administrators Windows group has full rights and does not require setting up. For more information, see [What are the preconfigured roles?](#) (page 14) and [What tasks do the rights authorize?](#) (page 15).

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

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

Note: If you want to allow a user to use a remote or additional Enterprise Manager, see [How can another user use Enterprise Manager?](#) (page 18).

You can edit and use preconfigured roles, but you cannot create your own 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 Enterprise Manager.

4.1.2 What are the preconfigured roles?

There are four preconfigured roles in Enterprise Manager. The roles can be edited, but they cannot be renamed or deleted.

Role	Description
System Administrator	A preconfigured role that has full rights to manage Sophos security software on the network and roles in Enterprise Manager.
Administrator	A preconfigured role that has rights to manage Sophos security software on the network, but cannot manage roles in Enterprise Manager.

Role	Description
Helpdesk	A preconfigured role that has remediation rights only, for example, to clean up or update computers.
Guest	A preconfigured role that has read-only access to Enterprise Manager.

4.1.3 Edit a role

If you already use role-based administration, you must have the **Role-based administration** right to perform this task. For more information, see [About roles](#) (page 14).

1. On the **Tools** menu, click **Manage Roles**.
2. In the **Manage roles** 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 **Users and groups** pane, add Windows users or groups to the role or remove existing users or groups as appropriate.

4.1.4 View user or group roles

To view the roles a Windows user or group has been assigned to:

1. On the **Tools** menu, click **Manage Roles**.
2. In the **Manage roles** 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 you want to view and click **OK**.

4.1.5 What tasks do the rights authorize?

Right	Tasks
Computer search, protection and groups	Start search, stop search and find domains for Network search, IP range search and Active Directory search
	Import computers and groups from Active Directory; import groups from Active Directory
	Import computers from a file

Right	Tasks
	Delete a computer
	Protect a computer
	Move a computer
	Create a group
	Rename a group
	Move a group
	Delete a group
	Assign a policy to a group
Policy setting - anti-virus and HIPS	Create an anti-virus and HIPS policy
	Duplicate an anti-virus and HIPS policy
	Rename an anti-virus and HIPS policy
	Edit an anti-virus and HIPS policy
	Restore default anti-virus and HIPS settings
	Delete an anti-virus and HIPS policy
	Add or remove entry from threat master list
Policy setting - device control	Create a device control policy
	Duplicate a device control policy
	Rename a device control policy
	Edit a device control policy
	Restore default device control settings
	Delete a device control policy
Policy setting - firewall	Create a firewall policy
	Duplicate a firewall policy
	Rename a firewall policy
	Edit a firewall policy
	Restore default firewall settings

Right	Tasks
	Delete a firewall policy
Policy setting - tamper protection	Create a tamper protection policy
	Duplicate a tamper protection policy
	Rename a tamper protection policy
	Edit a tamper protection policy
	Restore default tamper protection settings
	Delete a tamper protection policy
Policy setting - updating	Create an updating policy
	Duplicate an updating policy
	Rename an updating policy
	Edit an updating policy
	Restore default updating settings
	Delete an updating policy
	Create a subscription
	Edit a subscription
	Rename a subscription
	Duplicate a subscription
	Delete a subscription
	Configure the update manager
Remediation - cleanup	Clean up detected items
	Acknowledge alerts
	Acknowledge errors
Remediation - updating and scanning	Update computers now
	Run a full system scan of a computer
	Make computers comply with the group policy
Report configuration	Create, edit, or delete a report

Right	Tasks
Role-based administration	Add a user or group to a role
	Remove a user or group from a role
System configuration	Modify SMTP server settings; test SMTP server settings; modify email alert recipients
	Configure dashboard thresholds
	Configure reporting; configure database alert purging; set the company name displayed in reports

4.1.6 How can another user use Enterprise Manager?

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

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

- a member of the Sophos Console Administrators group,
- assigned to at least one Enterprise Manager role.

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 a Enterprise Manager role, on the **Tools** menu, click **Manage Roles**. For more information about roles, see [About roles](#) (page 14).

To use a remote or additional Enterprise Manager, a user must:

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

4.2 Creating and using groups

4.2.1 What are groups for?

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

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, 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.

4.2.2 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 Enterprise Manager.

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.

4.2.3 What is the Unassigned group?

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

You cannot:

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

4.2.4 Create a group

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task. For more information, see [About roles](#) (page 14).

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, firewall, device control, and tamper protection policies are applied to the new group automatically. You can edit these policies, or apply different policies. See [Edit a policy](#) (page 25) or [Assign a policy to a group](#) (page 24).

Note: If the new group is a subgroup, it initially uses the same settings as the group it is within.

4.2.5 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. For more information, see [About roles](#) (page 14).

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.

4.2.6 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. For more information, see [About roles](#) (page 14).

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

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

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 **Find new computers** icon on the toolbar. These computers will not be shown as managed until they are restarted.

4.2.7 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. For more information, see [About roles](#) (page 14).

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**.

4.2.8 Delete a group

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task. For more information, see [About roles](#) (page 14).

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.

4.2.9 Rename a group

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task. For more information, see [About roles](#) (page 14).

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

4.2.10 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. For more information, see [About roles](#) (page 14).

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.

4.2.11 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.

4.3 Creating and using policies

4.3.1 About policies

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

When you install Enterprise Manager, 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.

You can also create up to four new policies of each type. Once you have reached this limit, the **Create Policy** and **Duplicate Policy** options will be disabled.

You can apply the same policy to more than one group.

There are the following types of policy in Enterprise Manager:

- 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 behaviour and suspicious files, and how it cleans them up.
- The **Firewall** policy specifies how the firewall protects computers.
- The **Device control** policy specifies which storage and networking devices are not authorized for use on workstations.
- The **Tamper protection** policy specifies the password that allows authorized endpoint users to re-configure, disable or uninstall Sophos security software.

4.3.2 What are the default policies?

When you install Enterprise Manager, default policies are created for you.

Updating policy

The default updating policy 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 provides:

- On-access scanning for viruses and spyware (but not suspicious files and adware and other potentially unwanted applications).
- Analysis of the execution of programs running on the system (Sophos Anti-Virus and Sophos Endpoint Security and Control for Windows 2000 and later).

- Security alerts displayed on the desktop of the affected computer and added to the event log.

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. See [Set up a basic firewall policy](#) (page 76).

For a full list of the default firewall settings, see Sophos support knowledgebase article 57757 (<http://www.sophos.com/support/knowledgebase/article/57757.html>).

Device control policy

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

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.

4.3.3 Do I need to create my own policies?

When you install Enterprise Manager, “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 device 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. For more information, see [About roles](#) (page 14).

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, configure update policies as described in [About updating policy](#) (page 54).

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/suspicious applications or behavior, you may want to create new policies, or change the default policy. See [About the anti-virus and HIPS policy](#) (page 60).

Firewall policy

To allow bona-fide applications access to a network, configure firewall policies as described in [Set up a basic firewall policy](#) (page 76).

Device control

By default, device control is turned off. To restrict allowed hardware devices, configure device control policies as described in [About device control](#) (page 104).

Tamper protection

By default, tamper protection is turned off. To enable tamper protection, configure tamper policies as described in [About tamper protection](#) (page 111).

4.3.4 Create a policy

If you use role-based administration, you must have a respective **Policy setting** right to perform this task. For more information, see [About roles](#) (page 14).

You can create up to four new policies of each type. Once you have reached this limit, the **Create Policy** and **Duplicate Policy** options will be disabled.

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.

4.3.5 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. For more information, see [About roles](#) (page 14).

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.

4.3.6 Edit a policy

If you use role-based administration, you must have a respective **Policy setting** right to perform this task. For more information, see [About roles](#) (page 14).

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.

4.3.7 Rename a policy

If you use role-based administration, you must have a respective **Policy setting** right to perform this task. For more information, see [About roles](#) (page 14).

Note: 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**.

4.3.8 Delete a policy

If you use role-based administration, you must have a respective **Policy setting** right to perform this task. For more information, see [About roles](#) (page 14).

Note: You cannot delete a “Default” policy.

To delete a policy:

1. In the **Policies** pane, right-click the policy you want to delete and select **Delete Policy**.
2. Any groups that use the deleted policy will revert to using the default policy.

4.3.9 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.

4.3.10 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.

If you want your computers to comply with their group policies, see [Make computers use the group policy](#) (page 26).

4.3.11 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. For more information, see [About roles](#) (page 14).

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 computer(s) 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**.

4.4 Finding computers on the network

4.4.1 Choose how to find computers

You can use the “Find new computers” function and choose among several options that allow you to find networked computers and add them to Enterprise Manager. There are the following options:

- [Import containers and computers from Active Directory](#) (page 27)
- [Find computers with Active Directory](#) (page 27)
- [Find computers by browsing the network](#) (page 28)
- [Find computers by IP range](#) (page 28)
- [Import computers from a file](#) (page 29)

If you use role-based administration, you must have the **Computer search, protection and groups** right to add computers to the console. For more information, see [About roles](#) (page 14).

4.4.2 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. For more information, see [About roles](#) (page 14).

Importing groups from Active Directory retrieves the Active Directory container structure and copies it into Enterprise Manager 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.

To import groups from Active Directory:

1. On the toolbar, click the **Find new computers** icon.
2. In the **Find new 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 container(s) 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 groups** or **Groups only**, depending on what you want to import.

After you have imported containers from Active Directory, apply policies to the groups. See [About policies](#) (page 22).

4.4.3 Find computers with Active Directory

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task. For more information, see [About roles](#) (page 14).

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

1. On the toolbar, click the **Find new computers** icon.
2. In the **Find new computers** dialog box, select **Find 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 be a domain administrator’s account, or have full administrative rights over the target XP computers.

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

4. In the **Find 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.

4.4.4 Find 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. For more information, see [About roles](#) (page 14).

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

1. On the toolbar, click the **Find new computers** icon.
2. In the **Find New Computers** dialog box, select **Find 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 be a domain administrator's account or 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.

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

4. In the **Find 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.

4.4.5 Find computers by IP range

If you use role-based administration, you must have the **Computer search, protection and groups** right to perform this task. For more information, see [About roles](#) (page 14).

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

Note: You cannot use IPv6 addresses.

1. On the toolbar, click the **Find new computers** icon.
2. In the **Find new computers** dialog box, select **Find 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 be a domain administrator's account, or have full administrative rights over the target XP machines.

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 **Find 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.

4.4.6 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. For more information, see [About roles](#) (page 14).

To enable Enterprise Manager to list your computers, you can import the computer names from a file.

The file that contains the computer names must be one of the following:

- A file that uses the conventions listed below.
- An SGR file exported from Sophos SAVAdmin.

You can create a file using entries like this:

```
[GroupName1]
Domain1 | Windows7 | ComputerName1
Domain1 | WindowsServer2008R2 | 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.

Note: Valid operating system names are: Windows2000, Windows2000Server, WindowsXP, Windows2003, WindowsVista, Windows7, WindowsServer2008, WindowsServer2008R2, MACOSX, and Linux.

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.

5 Protecting computers

5.1 Prepare for installation of anti-virus 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.

To prepare for installation of anti-virus software:

1. On Windows 7/Vista computers:
 - a) On Windows 7, in Control Panel, open Network and Sharing Center. For the **Work network** location, ensure that the options are configured as below:
 - Network discovery: On
 - File and printer sharing: On
 - File sharing connections: Enable file sharing for devices that use 40- or 56-bit encryption
 - Password protected sharing: Off
 - b) On Windows Vista, in Control Panel, open Network and Sharing Center. Ensure that the options are configured as below:
 - Network discovery: On
 - File sharing: On
 - Printer sharing: On
 - Password protected sharing: Off
 - c) Ensure that the Remote Registry service is started and that its startup type is set to Automatic. This service is not on by default on Windows 7/Vista.
 - d) On Windows 7, set User Account Control to **Never notify**. When installation is complete, you should reset this to **Default**.
 - e) On Windows Vista, turn off User Account Control. When installation is complete, you should turn this back on.
 - f) Turn off Sharing Wizard.
 - g) Open Windows Firewall with Advanced Security, using the **Administrative Tools** item in Control Panel. Ensure that **Inbound connections** are allowed.
 - h) Change the **Inbound rules** to enable the processes below. When installation is complete, disable them again:
 - Remote Administration (NP-In) Domain
 - Remote Administration (NP-In) Private

Remote Administration (RPC) Domain

Remote Administration (RPC) Private

Remote Administration (RPC-EPMAP) Domain

Remote Administration (RPC-EPMAP) Private

2. On Windows 2003/XP Pro/2000 computers:
 - a) Ensure that the Remote Registry, Server, Computer Browser, and Task Scheduler services are started.
 - b) Ensure that the C\$ admin share is enabled.
 - c) Ensure that Simple File Sharing is turned off (XP only).
3. On Windows XP SP2 or later computers:
 - a) Ensure that the Remote Registry, Server, Computer Browser, and Task Scheduler services are started.
 - b) Ensure that the C\$ admin share is enabled.
 - c) Ensure that Simple File Sharing is turned off.
 - d) Enable File and Printer Sharing for Microsoft Networks.
 - e) Ensure that TCP ports 8192, 8193, and 8194 are open.
 - f) Restart the computer to make the changes effective.

5.2 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.

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.

5.3 Protect computers

Before you protect computers from the console:

- You must apply an updating policy to the group before you can protect computers in that group.
- If you want to protect Windows XP computers automatically from the console, make sure that "Simple File Sharing" is turned off.
- If you use role-based administration, you must have the **Computer search, protection and groups** right to protect computers. For more information, see [About roles](#) (page 14).

Automatic installation using Enterprise Manager is not possible on Mac and Linux computers. For information about how to protect these operating systems, see the *Sophos Enterprise Manager startup guide*. Sophos documentation is published at <http://www.sophos.com/support/docs/>.

To protect computers:

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.

2. Follow the instructions in the wizard. On the **Select features** page, select the features you want.

The anti-virus protection is always selected and must be installed. You can also select to install the following features:

■ **Sophos Client Firewall**

The client firewall is available only if your license includes it, and only for Windows 2000 or later.

You cannot install the firewall on computers running server operating systems or Windows Vista Starter.

■ **Third-Party Security Software Detection**

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.

3. On the **Protection summary** page, any problems with installation are shown in the **Protection issues** column. Troubleshoot the installation (see [Sophos Endpoint Security and Control installation failed](#) (page 137)), or carry out manual installation on these computers (see the *Sophos Enterprise Manager startup guide*). Click **Next**.

4. On the **Credentials** page, enter details of an account which can be used to install software. This account is typically a domain administrator account. It must:

- Have local administrator rights on computers you want to protect.
- Be able to log on to the computer where you installed the management server.
- Have read access to the Primary server location specified in the **Updating** policy. See [About update server locations](#) (page 55) and other topics in section *Configuring update server locations*.

Note: 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 Enterprise Administrator account in Active Directory instead.

5.4 View bootstrap locations

If Enterprise Manager is unable to install the anti-virus or firewall 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.

If your license includes the firewall, you can install it along with the anti-virus on Windows 2000 or later computers.

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

5.5 Checking whether your network is protected

5.5.1 How do I check that my network is protected?

For an overview of the network's security status, use the Dashboard. For more information, see [Dashboard panels](#) (page 6) and [Configure the Dashboard](#) (page 35).

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 installed or have alerts that need attention. For more information, see [Check that computers are protected](#) (page 36), [Check that computers are up to date](#) (page 36), and [Find computers with problems](#) (page 37).

You can also check whether all the computers in a group comply with the policies for that group, as described in [Check whether computers use the group policy](#) (page 26).

5.5.2 Configure the Dashboard

If you use role-based administration, you must have the **System configuration** right to configure the Dashboard. For more information, see [About roles](#) (page 14).

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 particular 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. For instructions, see [Set up network status email alerts](#) (page 118).

5.5.3 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 device control, check the status in the respective column.

For information about how to check that computers are up to date, see [Check that computers are up to date](#) (page 36).

For information about how to find computers with problems using the computer list filters, see [Find computers with problems](#) (page 37).

5.5.4 Check that computers are up to date

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

To check that computers are up to date:

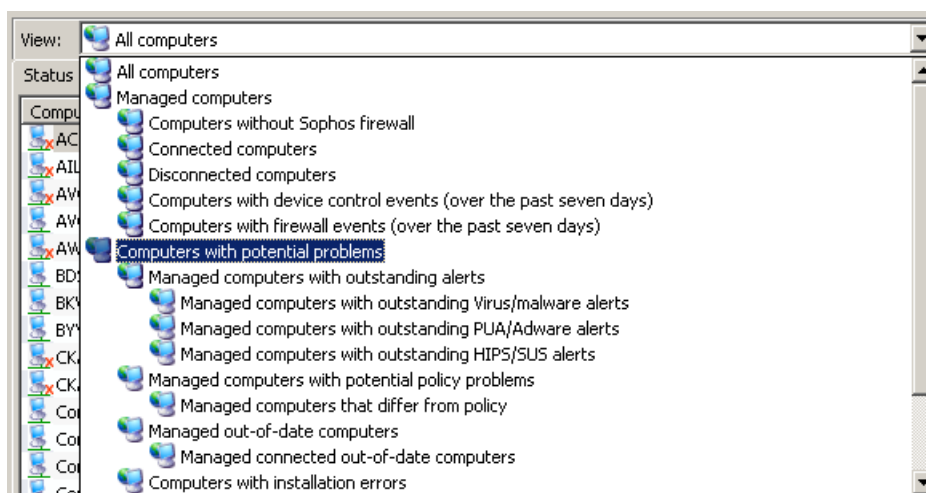
1. Select the group of computers you want to check.
2. If you want to check computers in any subgroups, select **At this level and below** in the drop-down list.
3. On the **Status** tab, look in the **Up to date** column, or go to the **Update details** tab.
 - If you see “Yes” in the **Up to date** 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.

For information about updating such out-of-date computers, see [Update out-of-date computers](#) (page 59).

5.5.5 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.

For information about dealing with protection problems, see [Computers are not running on-access scanning](#) (page 135) and other topics in the *Troubleshooting* section.

5.6 Dealing with alerts and errors



5.6.1 What do the alert icons mean?

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.

Below is a key to the alert icons. The other topics in this section give advice on dealing with alerts.

Note: Warnings are also displayed in the console if software is disabled or out of date. For information on this, see [How do I check that my network is protected?](#) (page 35).

Alert icons

Icon	Explanation
	A red warning sign displayed in the Alerts and errors column means that a virus, worm, Trojan, spyware, or suspicious behavior has been detected.
	<p>A yellow warning sign displayed in the Alerts and errors column indicates one of the following problems:</p> <ul style="list-style-type: none"> ■ A suspicious file has been detected. ■ An adware or other potentially unwanted application has been detected. ■ An error has occurred. <p>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.</p>

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)

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

5.6.2 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. For more information, see [About roles](#) (page 14).

To take action against 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. 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.

Cleanup status	Description and actions to take
Cleanable	You can remove the item. To do this, select the alert or alerts and click Cleanup .
Threat type not cleanable	This type of detected item, for example, suspicious file or suspicious behavior, 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. For more information, see Find information about detected items (page 40).
Not cleanable	This item cannot be cleaned up from the console. For more information about the item and actions you can take against it, see Find information about detected items (page 40).
Full scan required	This item may be cleanable, but a full scan of the endpoint is required before the cleanup can be carried out. For instructions, see Scan computers now (page 41).
Restart required	The item has been partially removed, but the endpoint needs to be restarted to complete the cleanup. Note: Endpoints must be restarted locally, not from Enterprise Manager.
Cleanup failed	The item could not be removed. Manual cleanup may be required. For more information, see Deal with detected items if cleanup fails (page 43).
Cleanup in progress (started <time>)	Cleanup is in progress.

Cleanup status	Description and actions to take
Cleanup timed out (started <time>)	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.

If you decided to allow an item, see [Authorize adware and PUAs](#) (page 65) or [Authorize suspicious items](#) (page 62).

5.6.3 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 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 (<http://www.sophos.com/security/analyses/>), go to the tab for the type of item you want to find, and either type the name of the item in the search box or look for the item in the list of items.

5.6.4 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. For more information, see [About roles](#) (page 14).

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 computer(s) 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.

For information about clearing update manager alerts from the console, see [Clear update manager alerts from the console](#) (page 41).

5.6.5 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. For more information, see [About roles](#) (page 14).

To clear update manager alerts from the console:

1. In the **Update managers** view, select the update manager. 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.

5.7 Scanning computers

5.7.1 About scanning

By default, Sophos Endpoint Security and Control detects known and unknown viruses, Trojans, worms, and spyware automatically as soon as a user attempts to access files that contain them. It also analyzes behavior of the programs running on the system.

You can also configure Sophos Endpoint Security and Control to:

- Scan computers for suspicious files. See [Scan for suspicious files](#) (page 62).
- Scan for adware and other potentially unwanted applications. See [Scan for adware and PUAs](#) (page 65).
- Scan computers at set times. See [Scan computers at set times](#) (page 69).

For more information about configuring scanning, see [About the anti-virus and HIPS policy](#) (page 60).

This section describes how to perform a full system scan of selected computers immediately.

5.7.2 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. For more information, see [About roles](#) (page 14).

Note: Only Windows 2000 or later 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**.
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 Enterprise Manager. This is because further scanning could enable the threat to spread. You must clean up the threat before running the scan again.

5.8 Cleaning up computers

5.8.1 Clean up computers now

You can immediately clean up Windows 2000 and later 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. For more information, see [About roles](#) (page 14).

Note: To clean up Mac or Linux computers, you can either set up automatic cleanup from the console (see [Set up automatic cleanup](#) (page 43)) or clean up the computers individually as described in [Deal with detected items if cleanup fails](#) (page 43).

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**. For more information, see [Partially detected item](#) (page 139).

To clean up computers immediately:

1. In the computer list, **Endpoints** view, right-click the computer(s) 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. See [Deal with detected items if cleanup fails](#) (page 43).

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.

5.8.2 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 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.

5.8.3 Set up automatic cleanup

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can have computers cleaned up automatically as soon as a virus or other item is found. To do this, you change the settings for on-access scanning and scheduled scanning as described below.

Note: On-access scanning cannot clean up adware and other potentially unwanted applications (PUAs). You should deal with these as described in [Clean up computers now](#) (page 42) or enable automatic cleanup of adware and PUA for scheduled scans.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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. Set up automatic cleanup for *on-access scanning*.
 - a) In the **Configure anti-virus and HIPS** panel, click the **On-access scanning** button.
 - b) In the **On-access scan settings** dialog box, click the **Cleanup** tab.
 - c) Set the options as described below.

Viruses/spyware

Select **Automatically clean up items that contain a virus/spyware**. 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 <UNC path>**

Notes

- If you select **Deny access and move to** and specify a location, Mac OS X computers will still move infected items to the default location.
- The **Deny access and move to default location** and **Deny access and move to** settings do not apply to Linux computers and will be ignored by them.

Suspicious files

Note: These settings only apply to Windows 2000 and later.

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 <UNC path>**

4. Set up automatic cleanup for *scheduled scanning*.

- a) In the **Anti-virus and HIPS policy** dialog box, in the **Scheduled scanning** panel, highlight the scan, and then click **Edit**.
- b) In the **Scheduled scan settings** dialog box, click **Configure**.
- c) In the **Scanning and cleanup settings** dialog box, click the **Cleanup** tab.
- d) Set the options as described below.

Viruses/spyware

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

- **Log only**
- **Delete**
- **Move to default location** or **Move to <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

Note: This setting only applies to Windows 2000 and later.

Select **Automatically clean up adware and PUA**, if you want to.

Suspicious files

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

- **Log only**
- **Delete**
- **Move to default location** or **Move to <UNC path>**

Notes

- These settings only apply to Windows 2000 and later.
- Moving an executable file reduces the likelihood of it being run.
- You cannot automatically move a multi-component infection.

6 Updating computers

6.1 Configuring the update manager

6.1.1 What is the update manager?

The update manager enables you to set up automatic updating of Sophos security software from a Sophos website.

Enterprise Manager supports only a single update manager. That update manager is installed with and managed from Enterprise Manager.

The update manager is configured when you run the **Download Security Software Wizard** which starts automatically when you open Enterprise Manager for the first time after the installation.

You can change the update manager configuration at a later time, for example, if you want to distribute downloaded Sophos software to additional shares on your network.

6.1.2 How does the update manager work?

Once you have configured the 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.

6.1.3 View or edit update manager configuration

If you use role-based administration, you must have the **Policy setting - updating** right to configure the update manager. For more information, see [About roles](#) (page 14).

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 computer list, select the update manager. 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 as described in the following topics:
 - [Select an update source for the update manager](#) (page 47).
 - [Select which software to download](#) (page 47).
 - [Specify where the software is placed](#) (page 48).
 - [Create or edit an update schedule](#) (page 49).
 - [Configure the update manager log](#) (page 50).
 - [Configure the self-updating of the update manager](#) (page 51).

For information about clearing update manager alerts from the console, see [Clear update manager alerts from the console](#) (page 41).

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

6.1.4 Select an update source for the update manager

If you use role-based administration, you must have the **Policy setting - updating** right to configure the update manager. For more information, see [About roles](#) (page 14).

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

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 computer list, select the update manager. 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, select **Sophos** to download software and updates directly from Sophos.
5. In the **Username** and **Password** fields, enter the download credentials supplied by Sophos.
6. If you access the internet 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.

6.1.5 Select which software to download

If you use role-based administration, you must have the **Policy setting - updating** right to configure the update manager. For more information, see [About roles](#) (page 14).

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 computer list, select the update manager. 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.
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.



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



For more information about subscriptions, see [About software subscriptions](#) (page 53).

6.1.6 Specify where the software is placed

If you use role-based administration, you must have the **Policy setting - updating** right to configure the update manager. For more information, see [About roles](#) (page 14).

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 **SophosUpdateMgr** account has read rights to the shares.

For a list of platforms on which network shares are supported, see [On what platforms are network shares supported?](#) (page 49)

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 computer list, select the update manager. 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 Enterprise Manager knows about.

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.

6.1.7 On what platforms are network shares supported?

Network shares on the following platforms are supported:

- Shares on Windows NT and later.
- Samba shares hosted on a Linux server, for example, SUSE Linux Enterprise 10 (SLES 10).
- Samba shares hosted on Netware 5.1 SP3 and Netware 6.5 SP3 to SP7, Netware kernel.
- Samba shares hosted on Mac OSX 10.2 or later.
- Samba shares hosted on Unix.
- Novell Storage Services (NSS) shares, supporting NDS authentication, hosted on Novell Open Enterprise Server 1 and 2, Linux kernel.
- Netware File System (NFS) shares, supporting NDS authentication, hosted on Netware 5.1 SP3 and Netware 6.5 SP3 to SP7, Netware kernel.
- NetApp filers.
- Samba shares hosted on Novell Open Enterprise Server 1 and 2.
- Novell Storage Services (NSS) shares, supporting NDS authentication, hosted on Netware 5.1 SP3 and Netware 6.5 SP3 to SP7, Netware kernel.

6.1.8 Create or edit an update schedule

If you use role-based administration, you must have the **Policy setting - updating** right to configure the update manager. For more information, see [About roles](#) (page 14).

By default, the 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, the 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.

Note: 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 computer list, select the update manager. 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.

6.1.9 Configure the update manager log

If you use role-based administration, you must have the **Policy setting - updating** right to configure the update manager. For more information, see [About roles](#) (page 14).

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 computer list, select the update manager. 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.

6.1.10 Configure the self-updating of the update manager

If you use role-based administration, you must have the **Policy setting - updating** right to configure the update manager. For more information, see [About roles](#) (page 14).

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 computer list, select the update manager. 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.

Enterprise Manager supports only the “recommended” version of the update manager. This means that the update manager will always be upgraded to the version that is labeled as such at Sophos. The actual update manager version will change.

6.1.11 Make the 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. For more information, see [About roles](#) (page 14).

After you have configured the 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 the 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 computer list, select the update manager, right-click and click **Update Now**.

6.1.12 Monitor the 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 computer list, look in the **Alerts** and **Errors** columns for any possible problems.
3. If there is an alert or error displayed next to the update manager, right-click the 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 particular update manager status and for information on how to resolve it, follow the link in the **Description** column.

Note: The **Updates** section of the dashboard does not report an alert or error if the 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 set in [Configure the Dashboard](#) (page 35).

6.1.13 Make the update manager comply with the configuration settings

If you use role-based administration, you must have the **Remediation - updating and scanning** right to perform this task. For more information, see [About roles](#) (page 14).

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 computer list, select the update manager, right-click and click **Comply with Configuration**.

6.1.14 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 Enterprise Manager, 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.
3. Specify usernames and passwords to prevent unauthorized access to this folder on the web server.

Note: The documentation for your web server should describe how to share a folder over the web and how to set up usernames and passwords for it. For more information about how to do this, contact your web server vendor.

6.2 Configuring software subscriptions

6.2.1 About 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 and ensures that your software is kept up to date automatically.

If you selected all the platforms you wish to protect in the wizard, you do not need to configure software subscriptions. If you want to add protection for a new platform, configure the subscription as described in [Subscribe to security software](#) (page 53).

If you haven't completed the wizard after you installed Enterprise Manager, see [Run the Download Security Software Wizard](#) (page 54).

6.2.2 Subscribe to security software

If you use role-based administration, you must have the **Policy setting - updating** right to edit a software subscription. For more information about role-based administration, see [About roles](#) (page 14).

To subscribe to security software:

1. On the **View** menu, click **Update Manager**.
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. For each of the selected platforms, click in the **Version** field next to the platform and then click again. In the drop-down list of available versions, select the recommended version, for example, *9.7 Recommended*.

Important: Select a fixed version (for example, *9.7.1*) only if advised to by Sophos technical support.

If you created a new software subscription, configure the update manager to maintain it as described in [View or edit update manager configuration](#) (page 46).

You can set up software subscription email alerts. For more information about subscription email alerts, see [Set up software subscription alerts](#) (page 114).

6.2.3 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**. For more information, see [About roles](#) (page 14).

If you haven't completed the **Download Security Software Wizard** after you installed Enterprise Manager, 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.

6.2.4 See which updating policies use the software subscription

To see which updating policies 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 policies that use the subscription.

6.3 Configuring the updating policy

6.3.1 About updating policy

Updating policies enable you to keep your computers up to date with your chosen security software. Enterprise Manager 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, follow the instructions in the following topics:

- [Select a subscription](#) (page 55)
- [About update server locations](#) (page 55)
- [Schedule updates](#) (page 57)
- [Select a different source for initial installation](#) (page 58)
- [Log updates](#) (page 58)

Note: If you use role-based administration, you must have the **Policy setting - updating** right to configure an updating policy. For more information about role-based administration, see [About roles](#) (page 14).

6.3.2 Select a subscription

If you use role-based administration, you must have the **Policy setting - updating** right to configure an updating policy. For more information, see [About roles](#) (page 14).

A subscription specifies which versions of endpoint software are downloaded from Sophos for each platform. The default subscription includes the latest software for Windows 2000 and later.

To select a subscription:

1. Check which updating policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.

6.3.3 Configuring update server locations

6.3.3.1 About update server locations

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 and enable location roaming. 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 HTTP URLs from Update Manager on your network. The secondary update server location may alternatively be set to get updates directly from Sophos over the internet via HTTP.

Note: Update Manager may have multiple distribution shares available, depending on how you have set it up.

6.3.3.2 About 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) location(s) 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. See [Specify where the software is placed](#) (page 48).

Location roaming is only usable where:

- There is a single common Enterprise Manager for both roaming and fixed endpoints.
- The fixed endpoints use the same software subscription as the roaming laptops.
- Enterprise Manager is version 4.7 or later and Endpoint Security and Control is version 9.7 or later on both fixed and roaming endpoints.
- Any third-party firewalls are configured to allow update location queries and responses. The port used is normally 51235 but is configurable; for details see <http://www.sophos.com/support/knowledgebase/article/110371.html>.

You enable location roaming as part of specifying sources for updates. For information on how to do this, see [Change primary server credentials](#) (page 56).

6.3.3.3 Change primary server credentials

If you use role-based administration, you must have the **Policy setting - updating** right to configure an updating policy. For more information, see [About roles](#) (page 14).

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.
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.

6.3.3.4 Set the secondary update server location

If you use role-based administration, you must have the **Policy setting - updating** right to configure an updating policy. For more information, see [About roles](#) (page 14).

To set the secondary update server location:

1. Check which updating policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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**.

Important: If you choose an HTTP URL or a share that is not maintained by a managed Update Manager, Enterprise Manager 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 HTTP, 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.

Note: If the username needs to be qualified to indicate the domain, use the form domain\username. For information about how to check a Windows user account, see Sophos support knowledgebase article 11637

(<http://www.sophos.com/support/knowledgebase/article/11637.html>).

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 HTTP 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.

6.3.4 Schedule updates

If you use role-based administration, you must have the **Policy setting - updating** right to configure an updating policy. For more information, see [About roles](#) (page 14).

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

Note: If the computers download updates directly from Sophos, this update interval does not apply. Computers running Sophos PureMessage can check for updates every 15 minutes. Computers that are not running Sophos 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. See [Check which policies a group uses](#) (page 21).
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.

6.3.5 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. For more information, see [About roles](#) (page 14).

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.

Note:

This setting applies only to Windows 2000 and later.

If your primary server is an HTTP (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 group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.

6.3.6 Log updates

If you use role-based administration, you must have the **Policy setting - updating** right to configure an updating policy. For more information, see [About roles](#) (page 14).

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. See [Check which policies a group uses](#) (page 21).
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.

6.4 Update out-of-date computers

If you use role-based administration, you must have the **Remediation - updating and scanning** right to update computers. For more information, see [About roles](#) (page 14).

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 up-to-dateness.
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 particular 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 manager**. 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**.

7 Configuring policies

7.1 Configuring the anti-virus and HIPS policy

7.1.1 About the anti-virus and HIPS policy

An anti-virus and HIPS policy enables you to detect and clean up viruses, Trojans, worms, spyware as well as adware and other potentially unwanted applications. Using it, you can also scan your computers for suspicious behavior, suspicious files, and rootkits. You can use different settings for each set of computers.

By default, Sophos Endpoint Security and Control detects known and unknown viruses, Trojans, worms, and spyware automatically as soon as a user attempts to access files that contain them. It also analyzes behavior of the programs running on the system.

You can also configure Sophos Endpoint Security and Control to:

- [Scan for suspicious files](#) (page 62)
- [Scan for adware and PUAs](#) (page 65)
- [Scan computers at set times](#) (page 69)

You can also have computers cleaned up automatically as soon as a virus or other threat is found. To do this, you change the settings for on-access scanning as described in [Set up automatic cleanup](#) (page 43).

Note: If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to edit an anti-virus and HIPS policy. For more information about role-based administration, see [About roles](#) (page 14).

Note: Enterprise Manager 4.7 cannot perform scheduled scans on Macs. Use an alternative scanning option or refer to the *Sophos Anti-Virus for Mac OS X Help* for more scanning options.

7.1.2 Scan for viruses, Trojans, worms, and spyware

By default, Sophos Endpoint Security and Control detects known and unknown viruses, Trojans, worms, and spyware automatically as soon as a user attempts to access files that contain them.

7.1.3 Suspicious behavior and file detection (HIPS)

7.1.3.1 What is HIPS?

Host Intrusion Prevention System (HIPS) is a security technology that protects computers from suspicious files, unidentified viruses, and suspicious behavior. There are two HIPS methods: suspicious behavior detection and suspicious file detection.

Note: HIPS options apply only to Sophos Endpoint Security and Control for Windows 2000 and later.

Suspicious behavior detection

Suspicious behavior detection is the dynamic analysis 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 includes buffer overflow detection, which dynamically analyzes the behavior of all programs running on the system in order to detect buffer overflow attacks.

Note: The “buffer overflow detection” feature is not available for Windows Vista, Windows 2008, Windows 7, and 64-bit versions of Windows. These operating systems are protected against buffer overflows by Microsoft’s Data Execution Prevention (DEP) feature.

For information about configuring suspicious behavior detection, see [Detect and block suspicious behavior](#) (page 61).

Suspicious file detection

Sophos Endpoint Security and Control can scan for suspicious files. These contain certain characteristics that are common to malware but not sufficient for the files to be identified as new pieces of malware.

For information about configuring suspicious file detection, see [Scan for suspicious files](#) (page 62).

7.1.3.2 Detect and block suspicious behavior

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

By default, Sophos Endpoint Security and Control analyzes behavior of the programs running on the system, but does not block programs exhibiting suspicious behavior.

We recommend that you run Sophos Endpoint Security and Control in this alert-only mode for a time and authorize the programs you need before enabling automatic blocking of suspicious behavior. When suspicious behavior or buffer overflow is detected, you can either remove or authorize the suspicious item. See [Clean up computers now](#) (page 42) and [Authorize suspicious items](#) (page 62). After you have authorized all the programs you need, enable blocking of suspicious behavior.

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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 **Suspicious behavior** button.

The **Suspicious Behavior Detection** dialog box is displayed. By default, all three options (**Detect suspicious behavior**, **Detect buffer overflows**, and **Alert only**) are enabled.

4. Clear the **Alert only** check box.

7.1.3.3 Scan for suspicious files

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

Suspicious file is a file that contains certain characteristics that are common to malware but not sufficient for the file to be identified as a new piece of malware (for example, a file containing dynamic decompression code commonly used by malware).

Note: This option applies only to Sophos Endpoint Security and Control for Windows 2000 and later.

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, set the options as follows:

■ On-access scanning

To configure on-access scanning, in the **Configure anti-virus and HIPS** panel, make sure the **Enable on-access scanning** check box is selected. Click the **Configure** button next to the check box.

On the **Scanning** tab, in the **Scanning options** panel, select the **Scan for suspicious files** check box. Click **OK**.

■ Scheduled scanning

To configure scheduled scans, in the **Scheduled scanning** panel, click **Add** (or select an existing scan and click **Edit**).

In the **Scheduled scan settings** dialog box, enter your settings and then click **Configure**.

In the **Scanning and cleanup settings** dialog box, on the **Scanning** tab, in the **Scanning options** panel, select the **Scan for suspicious files** check box. Click **OK**.

When a suspicious file is detected, you can either remove or authorize the file. See [Clean up computers now](#) (page 42) and [Authorize suspicious items](#) (page 62).

7.1.3.4 Authorize suspicious items

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

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 group(s) of computers you want to configure.
See *Check which policies a group uses* (page 21).
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. In the **Authorization Manager** dialog box, click the tab for the type of behavior that has been detected, for example, "Buffer overflow."
 - To authorize a program that has been detected, find the program in the **Known** list and move it from the **Known** list to the **Authorized** list.
 - To allow an item that Sophos Endpoint Security and Control has *not* yet classified as suspicious, click **New entry**. Browse to the item and select it to add it to the **Authorized** list.

If you want to remove an item from the list, select the item and click **Delete entry**. If you have authorized the item, removing it from the list effectively blocks it again, so use this option only if you are sure that it does not need to be authorized. This option does not delete the item from disk.

7.1.4 Sophos Live Protection

7.1.4.1 About 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 the anti-virus scan on an endpoint computer has identified a file as suspicious, but cannot further identify it as either clean or malicious based on the threat identity (IDE) files stored on the computer, certain file 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.

■ 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. 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).

Important: You must ensure that Sophos domain to which the file data is sent is trusted in your web filtering solution. For details, see support knowledgebase article 62637 (<http://www.sophos.com/support/knowledgebase/article/62637.html>).

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.

7.1.4.2 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. For more information, see [About roles](#) (page 14).

By default, Endpoint Security and Control sends file data such as checksums to Sophos, but does not send sample files. To take full advantage of Sophos Live Protection, you must enable both Sophos Live Protection options.

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.
See [Check which policies a group uses](#) (page 21).
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:
 - To turn the sending of file data to Sophos on or off, select or clear the **Enable Live Protection** check box.
 - To turn the sending of sample files to Sophos on or off, select or clear the **Automatically send file samples to Sophos** check box.

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

7.1.5 Adware and PUAs

7.1.5.1 Scan for adware and PUAs

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

Note: This option applies only to Sophos Endpoint Security and Control for Windows 2000 and later.

We recommend that you begin by using a scheduled scan to detect potentially unwanted applications. This lets you deal safely with applications that are *already* running on your network. You can then enable on-access detection to protect your computers in future.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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 **Scheduled scanning** panel, click **Add** to create a new scan, or double-click a scan in the list to edit it.
4. In the **Scheduled scan settings** dialog box, click **Configure** (at the bottom of the page).
5. In the **Scanning and cleanup settings** dialog box, on the **Scanning** tab, under **Scanning options**, select **Scan for adware and PUA**. Click **OK**.

When the scan is carried out, Sophos Endpoint Security and Control may report some adware or other potentially unwanted applications.

6. If you want your computers to run the applications, you must authorize them (see [Authorize adware and PUAs](#) (page 65)). Otherwise, remove them (see [Clean up computers now](#) (page 42)).
7. If you want to enable on-access detection, open the **Anti-Virus and HIPS policy** dialog box again. In the **Configure anti-virus and HIPS** panel, make sure the **Enable on-access scanning** check box is selected. Click the **Configure** button next to the check box. In the **On-access scan settings** dialog box, select **Scan for adware and PUA**.

Note: Some applications "monitor" files and attempt to access them frequently. If you have on-access scanning enabled, it detects each access and sends multiple alerts. See [Frequent alerts about potentially unwanted applications](#) (page 139).

7.1.5.2 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. For more information, see [About roles](#) (page 14).

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 want.

To authorize such applications:

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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. In the **Authorization manager** dialog box, on the **Adware and PUAs** tab, in the **Known adware and PUAs** list, select the application you want. Click **Add** to add it to the **Authorized adware and PUAs** list.
5. If you cannot see the application you want to authorize, click **New entry**.

The **Add new adware or PUA** dialog box is displayed.

6. Go to the Sophos security analyses web page, <http://www.sophos.com/security/analyses>. On the **Adware and PUAs** tab, find the application you want to authorize.
7. In Enterprise Manager, in the **Add new adware or PUA** dialog box, enter the name of the application you want to authorize and click **OK**.

The application is added to the **Known adware and PUAs** list.

8. Select the application and click **Add** to add it to the **Authorized adware and PUAs** list.

If you want to remove an application from the list, select the application and click **Delete entry**.

7.1.6 Web protection

7.1.6.1 About web protection

Web protection provides enhanced protection against web threats by preventing access to locations that are known to host malware. It blocks endpoints access to such sites by performing a real-time lookup against Sophos's online database of malicious websites.

Web protection:

- Blocks network access to malicious websites.
- Scans data and files downloaded with Internet Explorer.

For information on how to enable web scanning, see [Enable web protection](#) (page 66).

7.1.6.2 Enable web protection

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

To enable web protection:

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, next to **Block access to malicious websites**, select **On**. This option is enabled by default.

For information on how to authorize specific websites, see [Authorize websites](#) (page 67).

4. To scan data and files downloaded by Internet Explorer, next to **Download scanning**, select **On**.

You can also select **As on access**, if you want to disable or enable on-access scanning and download scanning simultaneously.

7.1.6.3 Authorize websites

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).



Caution: Authorizing a website that has been classified as malicious could expose you to threats, ensure it is safe to access the website before you authorize it.

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

Note: If you have download scanning enabled and use Internet Explorer to visit a website that contains a threat, access to the site will be blocked even if it is listed as a authorized website.

To authorize a website:

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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. In the **Authorization manager** dialog box, on the **Websites** tab, click **Add** to add a website using one of the available options.

You can add a website by entering its domain name, IP address, or IP address with subnet mask.

If you want to edit or remove a website from the list, select the website and click **Edit** or **Remove** accordingly.

To view a list of recently blocked websites on an endpoint computer, see [View blocked websites](#) (page 121).

7.1.7 On-access scanning

7.1.7.1 Change when on-access scanning occurs

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can specify whether files are scanned when you open them (“on read”), save them (“on write”) or rename them.

Note:

Scanning files “on write” or “on rename” can have an impact on the computers’ performance. These options are not usually recommended.

These options apply to Windows computers only.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, in the **On-access scanning** panel, click the **Configure** button.
4. In the **On-access scan settings** dialog box, on the **Scanning** tab, under **Check files on**, select the options you want.

7.1.7.2 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. For more information, see [About roles](#) (page 14).

You can exclude items from on-access scanning.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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 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. See [Items that can be excluded from scanning](#) (page 75).

7.1.7.3 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. For more information, see [About roles](#) (page 14).

By default, Sophos 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.

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

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.

See [Check which policies a group uses](#) (page 21).

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. To turn off on-access scanning, clear the **Enable on-access scanning** check box. Then, in the **Scheduled scanning** panel, click **Add** and set up a scheduled scan.

If you later want to restart on-access scanning, select the **Enable on-access scanning** check box again.

7.1.8 Scheduled scanning

7.1.8.1 Scan computers at set times

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can have computers scanned at set times.

Note: Scheduled scans will run only on Windows and Linux computers.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.

See [Check which policies a group uses](#) (page 21).

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, in the **Scheduled scanning** panel, click **Add**.
4. In the **Scheduled scan settings** dialog box, enter a name for the scanning job. Select the items to scan (by default, all local hard disks or mounted filesystems are scanned). Select the days and times at which you want the scan to run.
5. If you want to change other scanning options or configure this scan to clean up computers, click **Configure** at the bottom of the dialog box.

For instructions on how to change the options for a scheduled scan, see [Change scheduled scan settings](#) (page 70).

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 Enterprise Manager. This is because further scanning could enable the threat to spread. You must clean up the threat before running the scan again.

7.1.8.2 Change scheduled scan settings

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

To change the settings for scheduled scanning:

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, in the **Scheduled scanning** panel, change settings as appropriate.

You can change two different kinds of setting:

- To change the types of files scanned by *all* scheduled scans, click **Extensions and Exclusions**.
- To change settings specific to each scan (what is scanned, times, scanning options, cleanup), highlight the scan and click **Edit**. Then in the **Scheduled scan settings** dialog box, click **Configure**.

Note: For full details of how to use scanning options, see [Scan for suspicious files](#) (page 62), [Scan for adware and PUAs](#) (page 65), and [Scan inside archive files](#) (page 73). For details of how to use cleanup options, see [Set up automatic cleanup](#) (page 43).

7.1.8.3 Exclude items from scheduled scanning

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can exclude items from scheduled scanning.

Note:

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. See [Scan computers now](#) (page 41).

Scheduled scans are not supported on Mac computers.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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 **Scheduled scanning** panel, click **Extensions and Exclusions**.
4. Click the **Windows Exclusions** or **Linux 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. See [Items that can be excluded from scanning](#) (page 75).

7.1.9 Scanning options

7.1.9.1 Change types of file scanned

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

By default, Sophos Endpoint Security and Control scans file types that are vulnerable to viruses. You can scan additional file types or choose to exempt some file types from scanning.

The file types scanned by default differ between operating systems and change as the product is updated. To see a list of the file types, go to a computer with the relevant operating system, open the Sophos Endpoint Security and Control or Sophos Anti-Virus window and look for the “Extensions” configuration page.

Note:

These options apply to Windows computers only.

On Windows 2000 or later, you can change these settings separately for on-access and scheduled scanning.

You can make changes on Mac OS X computers with the Sophos Update Manager, a utility supplied with Sophos Anti-Virus for Mac OS X. To open Sophos Update Manager, on a Mac OS X computer, in a **Finder** window, browse to the Sophos Anti-Virus:ESOSX folder. Double-click **Sophos Update Manager**. For further details, see Sophos Update Manager Help.

You can make changes on Linux computers using the `savconfig` and `savscan` commands as described in the Sophos Anti-Virus for Linux user manual.

To change types of files scanned:

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, set the options as follows:
 - To configure on-access scanning, in the **Configure anti-virus and HIPS** panel, make sure the **Enable on-access scanning** check box is selected. Click the **Configure** button next to the check box.
 - To configure scheduled scans, in the **Scheduled scanning** panel, click **Extensions and Exclusions**.
4. On the **Extensions** tab, select **Scan executable and infectable files**.
 - To scan additional file types, click **Add** and type the file extension, for example, PDF, in the **Extension** field.
 - To exempt some of the file types that are usually scanned by default, click **Exclude**. This opens the **Exclude extensions** dialog box. Enter the file extension.

By default, files with no extension are scanned.

Note: You can also select to scan all files, although this will affect computer performance.

7.1.9.2 Scan Macintosh files

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can enable Sophos Endpoint Security and Control to scan Macintosh files stored on Windows computers.

Note: This option applies only to Sophos Endpoint Security and Control for Windows 2000 and later.

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, set the options as follows:

■ **On-access scanning**

To configure on-access scanning, in the **On-access scanning** panel, make sure the **Enable on-access scanning** check box is selected. Click the **Configure** button next to the check box.

On the **Scanning** tab, under **Scan for**, select the **Macintosh viruses** check box.

■ **Scheduled scanning**

To configure scheduled scans, in the **Scheduled scanning** panel, click **Add** (or select an existing scan and click **Edit**).

In the **Scheduled scan settings** dialog box, enter your settings and then click **Configure**.

In the **Scanning and cleanup settings** dialog box, on the **Scanning** tab, under **Scan for**, select the **Macintosh viruses** check box.

7.1.9.3 Scan for rootkits

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

Scanning for rootkits is always performed when you run a full system scan of a computer (see [Scan computers now](#) (page 41)). However, if you want to change the setting for a scheduled scan, do as follows.

Note: This option applies only to Sophos Endpoint Security and Control for Windows 2000 and later.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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, in the **Scheduled scanning** panel, click **Add** (or select an existing scan and click **Edit**).
4. In the **Scheduled scan settings** dialog box, enter your settings and then click **Configure**.
5. In the **Scanning and cleanup settings** dialog box, on the **Scanning** tab, under **Scan for**, select the **Rootkits** check box. Click **OK**.

7.1.9.4 Scan inside archive files

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

Note: Scanning inside archive files makes scanning significantly slower and is generally not required. Even if you do not select the option, when you attempt to access a file extracted from

the archive file, the extracted file is scanned. Sophos therefore does not recommend selecting this option.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, in the **Scheduled scanning** panel, click **Add** (or select an existing scan and click **Edit**).
4. In the **Scheduled scan settings** dialog box, enter your settings and then click **Configure** (at the bottom of the page).
5. In the **Scanning and cleanup settings** dialog box, on the **Scanning** tab, under *Other scanning options*, select **Scan inside archive files**. Click **OK**.

7.1.9.5 Scan system memory

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can enable Endpoint Security and Control for Windows to scan system memory for threats. *System memory* is the memory that is used by the operating system. Endpoint Security and Control can scan system memory periodically in the background while on-access scanning is enabled and as part of a scheduled scan.

To scan system memory:

1. Check which anti-virus and HIPS policy is used by the group or groups of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, set the options as follows:

- **On-access scanning**

To configure on-access scanning, in the **On-access scanning** panel, make sure the **Enable on-access scanning** check box is selected. Click the **Configure** button next to the check box.

On the **Scanning** tab, in the **Other scanning options** panel, select the **Scan system memory** check box.

■ Scheduled scanning

To configure scheduled scans, in the **Scheduled scanning** panel, click **Add** (or select an existing scan and click **Edit**).

In the **Scheduled scan settings** dialog box, enter your settings and then click **Configure**.

In the **Scanning and cleanup settings** dialog box, on the **Scanning** tab, in the **Other scanning options** panel, select the **Scan system memory** check box.

Note: If you have set up automatic cleanup of viruses that are detected by on-access scanning, the cleanup of some viruses causes a full system scan to be run, which tries to clean up *all* the viruses on the computer. This might take a long time.

7.1.9.6 Run scan at lower priority

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can configure a custom scan to run at a lower priority so that it has minimal impact on user applications.

Note: This option applies only to Sophos Endpoint Security and Control for Windows Vista and later.

1. Check which anti-virus and HIPS policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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, in the **Scheduled scanning** panel, click **Add** (or select an existing scan and click **Edit**).
4. In the **Scheduled scan settings** dialog box, enter your settings and then click **Configure**.
5. In the **Scanning and cleanup settings** dialog box, on the **Scanning** tab, under *Other scanning options*, select the **Run scan at lower priority** check box. Click **OK**.

7.1.9.7 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 2000 and later

On Windows 2000 and later, you can exclude drives, folders and files.

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.

For further details, see the section “Using Sophos Anti-Virus” in Help for the endpoint software, Sophos Endpoint Security and Control version 9.7.

Mac OS X

On Mac OS X, you can exclude volumes, folders, and files.

Although wildcard characters are not supported, you can specify which items are excluded by prefixing or suffixing the exclusion with a slash or double slash.

For further details, see the help files or user manual for Sophos Anti-Virus for Mac OS X.

Linux

On Linux, you can exclude directories and files by specifying a path (with or without wildcards).

Note: Enterprise Manager supports only path-based Linux 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 instructions, see the *Sophos Anti-Virus for Linux user manual*.

If you set up another path-based exclusion on a managed Linux computer, this computer will be reported to the console as differing from the group policy.

7.2 Configuring the firewall policy

7.2.1 Basic firewall configuration

7.2.1.1 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 Manager policy setup guide* for detailed advice.

For more information about the default firewall settings, see Sophos support knowledgebase article 57756 (<http://www.sophos.com/support/knowledgebase/article/57756.html>).

For information about preventing network bridging, see [About device control](#) (page 104).

Important: 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. For more information about role-based administration, see [About roles](#) (page 14).

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:

Mode	Description
Block inbound and outbound traffic	<ul style="list-style-type: none"> ■ Default level. Offers the highest security. ■ Only allows essential traffic through the firewall and authenticates the identity of applications using checksums. ■ To allow applications commonly used in your organization to communicate through the firewall, click Trust. For more information, see About trusting applications (page 83).
Block inbound and allow outbound traffic	<ul style="list-style-type: none"> ■ Offers a lower security level than Block inbound and outbound traffic. ■ Allows your computers to access the network and internet without you having to create special rules. ■ All applications are allowed to communicate through the firewall.
Monitor	<ul style="list-style-type: none"> ■ 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. ■ Enables you to collect information about your network, and to then create suitable rules before deploying the firewall to your computers. For more information, see About using monitor mode (page 78).

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**. For details, see [View firewall events](#) (page 120).

The number of computers with events over a specified threshold within the last seven days is also displayed on the Dashboard.

7.2.1.2 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, as described in [Create a firewall event rule](#) (page 80).

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. For details, see [About interactive mode](#) (page 82) and the other topics in the "Working in interactive mode" section.

7.2.1.3 Add and trust an application

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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. Check which firewall policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
2. In the **Policies** pane, double-click **Firewall**, and then double-click the policy you want to change.
3. On the **Operational mode** page of the **Firewall Policy** wizard, click **Trust**.

The **Firewall Policy** dialog box appears.

4. Click **Add**.

The **Firewall policy - Add trusted 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.

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. 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.

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**.

The application is added to the firewall policy and marked as **Trusted**.

7.2.1.4 Allow all traffic on a LAN

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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

1. Check which firewall policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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.

Notes

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

7.2.1.5 Allow file and printer sharing

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

To allow computers to share local printers and folders on the network:

1. Check which firewall policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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**.

7.2.1.6 Allow flexible control of file and printer sharing

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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:

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

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

1. Check which firewall policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.

7.2.1.7 Block unwanted file and printer sharing

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.

7.2.1.8 Create a firewall event rule

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

You can create rules for all firewall events except the “modified memory” events.

To create a firewall event rule:

1. On the **View** 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: If you want to create an application rule directly from a firewall policy, using the advanced firewall policy configuration pages, see [Create an application rule from a firewall policy](#) (page 97).

7.2.1.9 Temporarily disable the firewall

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

By default, the firewall is enabled. Occasionally, you may need to temporarily disable the firewall for maintenance or troubleshooting, and then re-enable it.

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. See [Check which policies a group uses](#) (page 21).
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.

7.2.2 Advanced firewall configuration

7.2.2.1 Open the advanced configuration pages

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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.

7.2.2.2 Working in interactive mode

7.2.2.2.1 About interactive mode

In interactive mode, the firewall 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.

7.2.2.2.2 Enable interactive mode

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

The firewall can work in interactive mode, asking the user how to deal with detected traffic. For more information, see [About interactive mode](#) (page 82).

To put the firewall in interactive mode on a group of computers:

1. Check which firewall policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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. On the **General** tab, under **Working mode**, click **Interactive**.

7.2.2.2.3 Change to a non-interactive mode

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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. In the **Policies** pane, double-click **Firewall**, and then double-click the 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 that you want to configure.
4. Click the **General** tab.
5. Under **Working mode**, click **Allow by default** or **Block by default**.

7.2.2.3 Configuring the firewall

7.2.2.3.1 About trusting applications

To help provide security for your computers, the firewall blocks traffic from unrecognised 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. For information on how to do this, see [Create an application rule](#) (page 96) and other topics in the section *Application rules*.

7.2.2.3.2 Add an application to a firewall policy

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

To add an application to a firewall policy:

1. Check which firewall policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.

6. Click **Add**.

The **Firewall Policy - Add application** dialog box appears.

7. 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.

8. 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.

9. 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.

10. Click **Search** to display a list of application events.

11. 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.

7.2.2.3.3 Remove an application from a firewall policy

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

To remove an application from a firewall policy:

1. Check which firewall policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.
6. Select the application in the list, and then click **Remove**.

7.2.2.3.4 Trust an application

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

To trust an application on a group of computers:

1. Check which firewall policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).

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, follow the instructions in [Add an application to a firewall policy](#) (page 83) to add it.
 6. 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.
- [Create an application rule](#) (page 96)
 - [Apply preset application rules](#) (page 98)

7.2.2.3.5 Trust an application using the Firewall Event Viewer

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 **View** 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. See [Add an application checksum](#) (page 88).
 - You can also add an application as trusted directly in a firewall policy, using the advanced firewall policy configuration pages. See [Create an application rule from a firewall policy](#) (page 97).

7.2.2.3.6 Block an application

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

To block an application on a group of computers:

1. Check which firewall policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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, follow the instructions in [Add an application to a firewall policy](#) (page 83) to add it.

6. Select the application in the list, and then click **Block**.

7.2.2.3.7 Allow applications to launch hidden processes

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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:

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 upper 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 of a certain type, in the **Event type** field, click the drop-down arrow and select the event type.

8. 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.
9. Click **Search** to display a list of application events.
10. 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. For details, see [Enable interactive mode](#) (page 82).

7.2.2.3.8 Allow applications to use rawsockets

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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:

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 of a certain type, in the **Event type** field, click the drop-down arrow and select the event type.
8. 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.
9. Click **Search** to display a list of application events.

10. 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. For details, see [Enable interactive mode](#) (page 82).

7.2.2.3.9 Add an application checksum

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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. For details, see [Enable interactive mode](#) (page 82).

7.2.2.3.10 Turn blocking of modified processes on or off

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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.
- Only the modified process is blocked. The modifying program is not blocked from accessing the network.

7.2.2.3.11 Filter ICMP messages

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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

You should only filter ICMP messages if you are familiar with networking protocols. For explanations of the ICMP message types, see [Explanation of ICMP message types](#) (page 90).

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.

7.2.2.3.12 Explanation of ICMP message types

Echo Request, Echo Reply	Used to test destination accessibility and status. A host sends an Echo Request and listens for a corresponding Echo Reply . This is most commonly done using the ping command.
Destination Unreachable, Echo Reply	Sent by a router when it cannot deliver an IP datagram. A datagram is the unit of data, or packet, transmitted in a TCP/IP network.
Source Quench	Sent by a host or router if it is receiving data too quickly for it to handle. The message is a request that the source reduce its rate of datagram transmission.
Redirect	Sent by a router if it receives a datagram that should have been sent to a different router. The message contains the address to which the source should direct future datagrams. This is used to optimize the routing of network traffic.
Router Advertisement, Router Solicitation	Allow hosts to discover the existence of routers. Routers periodically broadcast their IP addresses via Router Advertisement messages. Hosts may also request a router address by broadcasting a Router Solicitation message to which a router replies with a Router Advertisement .
Time Exceeded for a Datagram	Sent by a router if the datagram has reached the maximum limit of routers through which it can travel.
Parameter Problem for a Datagram	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.
Timestamp Request, Timestamp Reply	Used to synchronize the clocks between hosts and to estimate transit time.
Information Request, Information Reply	Obsolete. These messages were used earlier by hosts to determine their inter-network addresses, but are now considered outdated and should not be used.
Address Mask Request, Address Mask Reply	Used to find the mask of the subnet (i.e. what address bits define the network). A host sends an Address Mask Request to a router and receives an Address Mask Reply in return.

7.2.2.4 Firewall rules

7.2.2.4.1 About firewall rules

Global rules

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

Application rules

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

7.2.2.4.2 About the order in which rules are applied

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

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

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

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

Connection	Port	Range
TCP	Remote	137-139 or 445
TCP	Local	137-139 or 445
UDP	Remote	137 or 138
UDP	Local	137 or 138

If the network address is *not* listed on the **LAN** tab, other firewall rules are checked in the following order:

1. Any **NetBIOS** traffic that has not been allowed using the **LAN** tab is dealt with according to the setting of the **Block file and printer sharing for other networks** check box:
 - If the check box is selected, the traffic is blocked.
 - If the check box is cleared, the traffic is processed by the remaining rules.
2. The high-priority global rules are checked, in the order in which they are listed.
3. If the connection has not already had rules applied to it, the application rules are checked.

4. If the connection has still not been handled, the normal-priority global rules are checked, in the order in which they are listed.
5. If no rules have been found to handle the connection:
 - In **Allow by default** mode, the traffic is allowed (if it is outbound).
 - In **Block by default** mode, the traffic is blocked.
 - In **Interactive** mode, the user is asked to decide.

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

7.2.2.4.3 About local network detection

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.

7.2.2.4.4 Global rules

7.2.2.4.4.1 Default global rule settings

This topic describes the conditions and actions for the default global rules. Use these settings if you want to create a new default global rule.

Allow DNS Resolving (TCP)

- Protocol: TCP
- Direction: Outbound
- Remote port: DOMAIN
- Action: Allow

Allow DNS Resolving (UDP)

- Protocol: UDP
- Direction: Outbound
- Remote port: DNS
- Action: Allow Stateful inspection

Allow Outgoing DHCP

- Protocol: UDP

- Local port: BOOTPS,BOOTPC,546,547

- Action: Allow

Allow Inbound Identification

- Protocol: TCP

- Direction: Inbound

- Local port: AUTH

- Action: Allow

Allow Loopback

- Protocol: TCP

- Direction: Inbound

- Local port: 127.0.0.0 (255.255.255.0)

- Action: Allow

Allow GRE Protocol

- Protocol: TCP

- Protocol type: Outbound

- Action: Allow

Allow PPTP Control Connection

- Protocol: TCP

- Direction: Outbound

- Remote port: PPTP

- Local port: 1024-65535

- Action: Allow

Block RPC Call (TCP)

- Protocol: TCP

- Direction: Inbound

- Local port: DCOM

- Action: Block

Block RPC Call (UDP)

- Protocol: UDP

- Local port: 135

- Action: Block

Block Server Message Block Protocol (TCP)

- Protocol: TCP
- Direction: Inbound
- Local port: MICROSOFT_DS
- Action: Block

Block Server Message Protocol (UDP)

- Protocol: TCP
- Local port: 445
- Action: Block

Allow Localhost UDP Connection

- Protocol: UDP
- Remote host: 255.255.255.255 (0.0.0.0)
- Local host: 255.255.255.255 (0.0.0.0)
- Where the local port is equal to the remote port: True
- Action: Allow

7.2.2.4.4.2 *Create a global rule*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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

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

To create a global rule:

1. 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.
For information on the order in which rules are applied, see [About the order in which rules are applied](#) (page 91).
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**.
11. Under **Rule description**, click an underlined value. For example, if you click the **TCP** link, the **Select Protocol** dialog box opens.

7.2.2.4.4.3 Edit a global rule

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

Important: 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 [Default global rule settings](#) (page 92).

7.2.2.4.4.4 Copy a global rule

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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**.

7.2.2.4.4.5 *Delete a global rule*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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**.

7.2.2.4.4.6 *Change the order in which global rules are applied*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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**.

7.2.2.4.5 **Application rules**

7.2.2.4.5.1 *Create an application rule*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 the arrow next to **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. To intelligently allow replies from the remote computer based on the initial connection, select **Stateful inspection**.
11. Under **Rule description**, click an underlined value. For example, if you click the **TCP** link, the **Select Protocol** dialog box opens.

7.2.2.4.5.2 Create an application rule from a firewall policy

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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.

7.2.2.4.5.3 *Edit an application rule*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 the arrow next to **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. To intelligently allow replies from the remote computer based on the initial connection, select **Stateful inspection**.
11. Under **Rule description**, click an underlined value. For example, if you click the **TCP** link, the **Select Protocol** dialog box opens.

7.2.2.4.5.4 *Apply preset application rules*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 the arrow next to **Custom**.

6. Point to **Add rules from preset**, and then click a preset.

7.2.2.4.5.5 *Copy an application rule*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 the arrow next to **Custom**.
6. In the **Application Rules dialog box**, click **Copy**.

7.2.2.4.5.6 *Delete an application rule*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 the arrow next to **Custom**.
6. In the **Application Rules dialog box**, click **Remove**.

7.2.2.4.5.7 *Change the order in which application rules are applied*

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 the arrow next to **Custom**.

6. 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**.

7.2.2.5 Location awareness

7.2.2.5.1 About 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.

7.2.2.5.2 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**.

Important: 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.

7.2.2.5.3 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:

Option	Description
DNS lookup	You create a list of domain names and expected IP addresses that correspond to your primary locations.
MAC address detection	You create a list of gateway MAC addresses that correspond to your primary locations.

6. Follow the instructions on the screen.

7.2.2.5.4 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. For information on how to do this, see the *Configuring the firewall* section.



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.

7.2.2.5.5 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:

Option	Description
Apply the configuration for the detected location	The firewall applies either the primary or secondary configuration to each network connection according to the detection settings for location awareness (as described in About setting up location awareness (page 100)).
Apply the configuration for the primary location	The firewall applies the primary configuration to all network connections.
Apply the configuration for the secondary location	The firewall applies the secondary configuration to all network connections.

7.2.2.6 Firewall reporting

7.2.2.6.1 About firewall reporting

By default, the firewall on an endpoint computer reports state changes, events, and errors to Enterprise Manager.

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 Enterprise Manager. In that case, you can choose **not** to send "differs from policy" alerts to Enterprise Manager when you make changes to certain parts of your firewall configuration.

For more information, see [Turn reporting of local changes on or off](#) (page 102).

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 Enterprise Manager.

For more information, see [Turn off reporting of unknown network traffic](#) (page 103)

7.2.2.6.2 Turn reporting of local changes on or off

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

If the firewall configuration on endpoint computers differs from policy, you can **turn reporting of local changes off**.

Turning reporting of local changes off stops the firewall sending "differs from policy" alerts to Enterprise Manager 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.

7.2.2.6.3 Turn off reporting of unknown network traffic

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

You can prevent the firewall on endpoint computers from reporting unknown network traffic to Enterprise Manager. 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 Enterprise Manager:

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.

7.2.2.6.4 Turn off reporting of firewall errors

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

To prevent the firewall on endpoint computers from reporting errors to Enterprise Manager:

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.

7.2.2.7 Import or export firewall configuration

Note: If you use role-based administration, you must have the **Policy setting - firewall** right to configure a firewall policy. For more information, see [About roles](#) (page 14).

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 group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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**.

7.3 Configuring the device control policy

7.3.1 About device control

Important: 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 Manager policy setup guide*.

Note: If you use role-based administration, you must have the **Policy setting - device control** right to configure a device control policy. For more information, see [About roles](#) (page 14).

7.3.2 About device control events

When a device control event occurs, for example, a removable storage device has been blocked, the event is sent to Enterprise Manager and can be viewed in the **Device Control - Event Viewer** dialog box.

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. For details, see [View device control events](#) (page 119) and [Export the list of events to a file](#) (page 122).

You can use device control events to add exemptions for specific devices or device models to the device control policies. For more information about exempting devices, see [Exempt a device from a single policy](#) (page 109) or [Exempt a device from all policies](#) (page 108).

The number of computers with device control events over a specified threshold within the last seven days is displayed on the Dashboard. For information on how to set up the threshold, see [Configure the Dashboard](#) (page 35).

You can also set up alerts to be sent to your chosen recipients when a device control event has occurred. For details, see [Set up device control alerts and messages](#) (page 117).

7.3.3 What types of device can be controlled?

Device control enables you to block three types of device: *storage*, *network*, and *short range*.

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 (SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault - Privacy Edition, Kingston Data Traveler BlackBox, and IronKey Enterprise Basic Edition USB flash drives with hardware encryption)

Using the secure removable storage category, you can easily allow the use of supported secure removable storage devices while blocking other removable storage devices. For an up-to-date list of supported secure removable storage devices, see Sophos support knowledgebase article 63102 (<http://www.sophos.com/support/knowledgebase/article/63102.html>).

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

7.3.4 Select device types to control

If you use role-based administration, you must have the **Policy setting - device control** right to edit a device control policy. For more information, see [About roles](#) (page 14).

Important: You should not block Wi-Fi connections on computers that are managed by Enterprise Manager via Wi-Fi.

1. Check which device control policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.”
Click **OK**.

7.3.5 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. For more information, see [About roles](#) (page 14).

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.

For information about viewing device control events, see [View device control events](#) (page 119).

To detect devices without blocking them:

1. Check which device control policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.” (For details, see [Select device types to control](#) (page 107).)
Click **OK**.

7.3.6 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. For more information, see [About roles](#) (page 14).

1. Check which device control policy is used by the group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).
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.” (For details, see [Select device types to control](#) (page 107).)
Click **OK**.

7.3.7 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. For more information, see [About roles](#) (page 14).

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 device model (“all devices of this model”). Do not set exemptions at both the model and device instance level. If both are defined, the device instance level will take precedence.

To exempt a device from all device control policies:

1. On the **View** 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.

For more information, see [View device control events](#) (page 119).

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, and 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 of this model.
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**.

7.3.8 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. For more information, see [About roles](#) (page 14).

You can exempt a specific device from a device control policy.

You can exempt a device instance (“this device only”) or a device model (“all devices of this model”). Do not set exemptions at both the model and device instance level. 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 group(s) of computers you want to configure. See [Check which policies a group uses](#) (page 21).

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.
For more information, see [View device control events](#) (page 119).
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, and 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 of this model.
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**.

7.3.9 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. For more information, see [About roles](#) (page 14).

To view or edit the list of exempt devices:

1. Check which device control policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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 of that model, 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**. For more information, see [Exempt a device from a single policy](#) (page 109).
- 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.

7.4 Configuring the tamper protection policy

7.4.1 About tamper protection

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. (For more information, see [About the anti-virus and HIPS policy](#) (page 60).)

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).
- Uninstall Sophos SafeGuard Disk Encryption.

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.

Note: If you use role-based administration, you must have the **Policy setting - tamper protection** right to configure a tamper protection policy. For more information, see [About roles](#) (page 14).

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 Enterprise Manager. For details, see [View tamper protection events](#) (page 121).

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.

7.4.2 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. For more information, see [About roles](#) (page 14).

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.
See [Check which policies a group uses](#) (page 21).
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.

7.4.3 Change 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. For more information, see [About roles](#) (page 14).

To change the tamper protection password:

1. Check which tamper protection policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).

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.

8 Setting up alerts and messages

8.1 About alerts and messages

There are several alerting methods used in Enterprise Manager.

■ 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 Enterprise Manager. The alert is displayed in the computer list. For more information about dealing with such alerts, see [Deal with alerts about detected items](#) (page 39).

These alerts are always displayed. You do not need to set them up.

■ Events displayed in the console

When a firewall, 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 Enterprise Manager 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 a device control event occurs, a message is displayed on the computer desktop.

You can also set up email alerts or SNMP messages for administrators.

This section describes how to set up alerts to be sent to your chosen recipients.

8.2 Set up software subscription alerts

If you use role-based administration, you must have the **System configuration** right to perform this task. For more information, see [About roles](#) (page 14).

Enterprise Manager displays alerts raised by the update manager in the **Alerts** column in the **Update managers** view.

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 two 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 has been retired at Sophos.

8.3 Set up anti-virus and HIPS email alerts

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can have email alerts sent to particular users if a virus, suspicious behavior, an unwanted application or an error is encountered on any of the computers in a group.

Important: Mac OS X computers can send email alerts to only one address.

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, in the **Configure anti-virus and HIPS** panel, 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.

Note: The **Suspicious behavior detection**, **Suspicious file detection**, and **Adware and PUA detection and cleanup** settings apply only to Windows 2000 and later. The **Other errors** setting applies only to Windows.

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.

Important: 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.
 - In the **SMTP server** text box, type the host name or IP address of the SMTP server. Click **Test** to send a test email alert.
 - In the **SMTP sender address** text box, type an email address to which bounces and non-delivery reports can be sent.
 - 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.
Note: Linux computers will ignore the SMTP sender and reply-to addresses and use the address `root@<hostname>`.
 - In the **Language** panel, click the drop-down arrow, and select the language in which email alerts should be sent.

8.4 Set up anti-virus and HIPS SNMP messaging

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

You can have SNMP messages sent to particular users if a virus or error is encountered on any of the computers in the group.

Note: These settings apply only to Windows 2000 and later.

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, in the **Configure anti-virus and HIPS** panel, 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.

8.5 Configure anti-virus and HIPS desktop messaging

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

By default, desktop messages are displayed on the computer on which a virus, suspicious item or potentially unwanted application is found. You can 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, in the **Configure anti-virus and HIPS** panel, 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 2000 and later.
4. In the **User-defined message** text box, you can type a message that will be added to the end of the standard message.

8.6 Set up device control alerts and messages

If you use role-based administration, you must have the **Policy setting - device control** right to edit a device control policy. For more information, see [About roles](#) (page 14).

Enterprise Manager uses events and messages to report when a controlled device is detected or blocked.

For information about device control policies and events, see [About device control](#) (page 104).

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 Enterprise Manager and can be viewed in the **Device Control - Event Viewer**. (To open the event viewer, on the **View** menu, click **Device Control Events**.)
- 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 Enterprise Manager to send the following messages:

Email alerts	An email message is sent to the recipients that you specify.
SNMP messages	An SNMP message is sent to the recipients specified in your anti-virus and HIPS policy settings.

To set up device control messaging:

1. Check which device control policy is used by the group(s) of computers you want to configure.
See [Check which policies a group uses](#) (page 21).
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, `About Sophos`.

- *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 via the anti-virus and HIPS policy.

8.7 Set up network status email alerts

If you use role-based administration, you must have the **System configuration** right to configure the network status email alerts. For more information, see [About roles](#) (page 14).

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.

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.

8.8 Configure Windows event logging

If you use role-based administration, you must have the **Policy setting - anti-virus and HIPS** right to perform this task. For more information, see [About roles](#) (page 14).

By default, Sophos Endpoint Security and Control adds alerts to the Windows 2000 or later 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.

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, in the **Configure anti-virus and HIPS** panel, 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.

8.9 Viewing events

8.9.1 About events

When a firewall, 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 Enterprise Manager and can be viewed in the respective event viewer.

Using the event viewers, you can investigate events occurred on the network. You can also generate a list of events based on a filter you configure, for example, a list of all device 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). For information on how to set up the threshold, see [Configure the Dashboard](#) (page 35).

You can also set up alerts to be sent to your chosen recipients when an event has occurred. For more information, see [About alerts and messages](#) (page 114).

8.9.2 View device control events

To view device control events:

1. On the **View** 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.

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. For details, see [Exempt a device from all policies](#) (page 108).

You can export the list of device control events to a file. For details, see [Export the list of events to a file](#) (page 122).

8.9.3 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 **View** 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 as described in [Create a firewall event rule](#) (page 80).

You can export the list of firewall events to a file. For details, see [Export the list of events to a file](#) (page 122).

8.9.4 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 **View** 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. For details, see [Export the list of events to a file](#) (page 122).

8.9.5 View blocked websites

You can view the list of websites that have recently been blocked on an endpoint computer.

To view recently blocked websites:

1. In the **Endpoints** view, in the computer list, double-click the computer for which you want to view the blocked websites.
2. In the **Computer details** dialog box, scroll to the **Latest blocked websites** section.

You can also view the number of websites that have been blocked for a user by generating a report. For more information, see [Configure the Events by user report](#) (page 129).

8.9.6 Export the list of events to a file

You can export the list of firewall, device control, or tamper protection events to a comma separated value (csv) file.

1. On the **View** 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.

For more information, see [View device control events](#) (page 119), [View firewall events](#) (page 120), or [View tamper protection events](#) (page 121).

3. Click **Export**.
4. In the **Save As** dialog box, enter a file name and browse to select a destination for the file.

9 Generating reports

9.1 About 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. For more information about role-based administration, see [About roles](#) (page 14).

9.2 Create a new report

If you use role-based administration, you must have the **Report configuration** right to perform this task. For more information, see [About roles](#) (page 14).

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.

9.3 Configure the Alert and event history report

If you use role-based administration, you must have the **Report configuration** right to perform this task. For more information, see [About roles](#) (page 14).

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.

9.4 Configure the Alert summary report

If you use role-based administration, you must have the **Report configuration** right to perform this task. For more information, see [About roles](#) (page 14).

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.

9.5 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. For more information, see [About roles](#) (page 14).

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.

9.6 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. For more information, see [About roles](#) (page 14).

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.

9.7 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. For more information, see [About roles](#) (page 14).

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.

9.8 Configure the Endpoint policy non-compliance report

If you use role-based administration, you must have the **Report configuration** right to perform this task. For more information, see [About roles](#) (page 14).

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.

9.9 Configure the Events by user report

If you use role-based administration, you must have the **Report configuration** right to perform this task. For more information, see [About roles](#) (page 14).

The **Events by user** report shows firewall and device control events along with blocked websites 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.

9.10 Configure the Managed endpoint protection report

If you use role-based administration, you must have the **Report configuration** right to perform this task. For more information, see [About roles](#) (page 14).

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.

9.11 Updating hierarchy report

The **Updating hierarchy** report shows the update manager on your network, update shares that it maintains, and the number of computers that update from these shares.

You cannot configure the **Updating hierarchy** report. You can run the report as described in [Run a report](#) (page 131).

9.12 Schedule a report

If you use role-based administration, you must have the **Report configuration** right to perform this task. For more information, see [About roles](#) (page 14).

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.

9.13 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.

9.14 View a report as a table or chart

Some report 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.

9.15 Print a report

To print a report, click the **Print** icon on the toolbar at the top of the report.



9.16 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**.

9.17 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.

10 Copying or printing data from Enterprise Manager

10.1 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.

10.2 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**.

10.3 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.

10.4 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**.

11 Troubleshooting

11.1 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.
For details, see [Check which policies a group uses](#) (page 21).
2. Ensure that on-access scanning is enabled in that policy and that the computers comply with the policy.
For details, see [Turn on-access scanning on or off](#) (page 69) and [Make computers use the group policy](#) (page 26).

11.2 The firewall is disabled

If there are computers with the firewall disabled:

1. Check which firewall policy is used by those computers.
For details, see [Check which policies a group uses](#) (page 21).
2. Ensure that the firewall is enabled in that policy and that the computers comply with the policy.
For details, see [Temporarily disable the firewall](#) (page 81) and [Make computers use the group policy](#) (page 26).

11.3 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. For more information, see [About roles](#) (page 14).

Before you attempt to install the client firewall on endpoint computers check that:

- Your license includes the firewall.
- The computers are running Windows 2000 or later.

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.

If the problem persists, contact Sophos technical support.

11.4 Computers have outstanding alerts

- If there are computers with a virus, or an application you do not want, see [Clean up computers now](#) (page 42).
- If there are computers with an adware or other potentially unwanted application that you do want, see [Authorize adware and PUAs](#) (page 65).
- If there are out-of-date computers, see [Update out-of-date computers](#) (page 59) for help with diagnosing and fixing the problem.

Note: If you do not need the alert displayed any more, you can clear it. Select the computer(s) with alerts, right-click and select **Resolve Alerts and Errors**. You must have the **Remediation - cleanup** right to acknowledge (clear) alerts and errors.

11.5 Computers are not managed by the console

Computers should be managed by Enterprise Manager, so that they can be updated and monitored.

Note: New computers added to the network are not displayed or managed by the console automatically. Click **Find new 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. Select any computers that are listed. Right-click and select **Protect computers** to install a managed version of Sophos Endpoint Security and Control.
3. If there are computers on which Enterprise Manager cannot install Sophos Endpoint Security and Control automatically, carry out a manual installation.

For details, see the *Sophos Enterprise Manager startup guide*.

11.6 Cannot 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.

11.7 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:

- Enterprise Manager 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 Manager 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.

If installation of Compliance Agent fails or there is an error during installation, you can view the Compliance Agent installation log. The log is in the %tmp% folder.

For a full list of requirements for the Sophos Endpoint Security and Control features, see the system requirements page on the Sophos website (<http://www.sophos.com/products/all-sysreqs.html>).

11.8 Computers are not updated

See [Update out-of-date computers](#) (page 59) for help with diagnosing and fixing the problem.

11.9 Cannot create a new policy

If the **Create Policy** and **Duplicate Policy** options are disabled, that means that you have reached the maximum number of policies you can create. You can create a maximum of four new policies of each type (that is, four new updating policies, four new anti-virus and HIPS policies, and so on).

11.10 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.

You can change anti-virus settings on Mac computers with Sophos Update Manager, a utility supplied with Sophos Anti-Virus for Mac. To open Sophos Update Manager, on a Mac computer, in a **Finder** window, browse to the Sophos Anti-Virus:ESOSX folder. Double-click **Sophos Update Manager**. For further details, see Sophos Update Manager Help.

11.11 Anti-virus settings do not take effect on Linux

Some anti-virus settings cannot be applied to Linux 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 user manual*.

11.12 Linux 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.

11.13 New scan appears unexpectedly on Windows 2000 or later

If you look at the local copy of Sophos Endpoint Security and Control on Windows 2000 or later 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.

11.14 Connectivity and timeout problems

If the communications between Enterprise Manager 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 Enterprise Manager. 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.

11.15 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. See [Scan for adware and PUAs](#) (page 65).
- The applications are on a computer running Windows 2000 or later.

11.16 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 2000 or later, 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. See [Scan for adware and PUAs](#) (page 65).

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 (see [Exclude items from on-access scanning](#) (page 68)). 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.

11.17 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 Endpoint Security and Control 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). See [Authorize adware and PUAs](#) (page 65).
- Clean up the computer(s), removing applications that you have not authorized. See [Clean up computers now](#) (page 42).

11.18 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. See [Scan computers now](#) (page 41).
- Some drives or folders that contain item components are excluded from scanning. Check the items excluded from scanning (see [Exclude items from on-access scanning](#) (page 68)). If there are some items on the list, remove them from the list.
- You have insufficient access rights.
- It cannot 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 2000 or later).

11.19 Recover from virus side-effects

Cleanup can remove a virus from computers, but it cannot 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.

11.20 Recover from application side-effects

Cleanup can remove unwanted applications, but it cannot 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.

12 Glossary

Application manager	A dialog box that enables you to allow or create new rules for applications that have been blocked by Sophos Client Firewall.
controlled device	A device that is subject to device control.
critical level	A value that triggers the change of an item's security status to Critical.
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.
database	The component of Sophos Enterprise Manager that stores details about computers on the network.
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.
exempt device	A device that is explicitly excluded from device control.
group	A group of managed computers defined in Sophos Enterprise Manager.
health indicator	Generic term for icons depicting security status of a dashboard section or item, or the overall health status of the network.
Host Intrusion Prevention System (HIPS)	A security technology that protects computers from suspicious files, unidentified viruses, and suspicious behavior.
managed computer	A computer that has Remote Management System (RMS) installed and on which Sophos Enterprise Manager can report and install and update software.
management console	The component of Sophos Enterprise Manager that enables you to protect and manage computers.
management server	The component of Sophos Enterprise Manager that handles updating and communications with networked computers.
out-of-date computer	A computer that has not got up-to-date Sophos software.
policy	A group of settings, for example, for updating, applied to a group or groups of computers.

potentially unwanted application (PUA)	An application that is not inherently malicious but is generally considered unsuitable for the majority of business networks.
right	A set of permissions to perform certain tasks in Enterprise Manager.
role	A set of rights that determines access to Enterprise Manager.
role-based administration	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.
server root node	The topmost node of the group tree in the Groups pane, which includes the Unassigned group.
Sophos Live Protection	A feature that uses in-the-cloud technology to instantly decide whether a suspicious file is a threat and take action specified in the Sophos anti-virus cleanup configuration.
Sophos Update Manager (SUM)	A program that downloads Sophos security software and updates from Sophos or another update server to shared update locations.
software subscription	A set of versions of software for a variety of platforms, selected by the user, that Update Manager will download and keep updated. One version can be specified for each supported platform (for example, “Latest” for Windows 2000 and later).
suspicious behavior detection	Dynamic analysis of the behavior of all programs running on the system in order to detect and block activity which appears to be malicious.
suspicious file	A file that exhibits a combination of characteristics that are commonly, but not exclusively, found in viruses.
System Administrator	<p>A preconfigured role that has full rights to manage Sophos security software on the network and roles in Enterprise Manager.</p> <p>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.</p>
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.

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.
update manager	See <i>Sophos Update Manager</i> .
warning level	A value that triggers the change of an item's security status to Warning.

13 Technical support

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

- Visit the SophosTalk community at <http://community.sophos.com/> and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at <http://www.sophos.com/support/>.
- Download the product documentation at <http://www.sophos.com/support/docs/>.
- Send an email to support@sophos.com, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

14 Legal notices

Copyright © 2011 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 licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

ACE™, TAO™, CIAO™, and CoSMIC™

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

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

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹² around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

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

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets,

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

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

If you have any suggestions, additions, comments, or questions, please let me²¹ know.

Douglas C. Schmidt²²

References

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

Apache

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

Common Public License

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

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991–2000 iMatix Corporation
<http://www.imatix.com>.

OpenSSL cryptographic toolkit

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

OpenSSL license

Copyright © 1998–2008 The OpenSSL Project. All rights reserved.

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

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

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Original SSLeay license

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

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

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

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

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

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

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

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

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

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

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

Index

A

- access to console 18
- acknowledge alerts 40
- acknowledge errors 40
- Active Directory
 - importing from 27
- adding applications 78, 83
- adding computers 26
- adding computers to groups 20
- adware 65
- adware/PUA
 - authorize 65
- alert icons 38
- alerts 38, 114
 - acknowledge 40
 - clear 40
 - dealing with 39
 - email 115
 - information about detected items 40
 - network status 118
 - resolving 39
 - subscriptions 114
 - update manager 41
- allow file and printer sharing 79
- allowing
 - file and printer sharing 80
 - hidden processes 86
 - LAN traffic 79
 - rawsockets 87
- alternative update source 55
- anti-virus 60
- anti-virus and HIPS policy 60
- applications
 - adding 78, 83
 - blocking 86
 - trusting 78, 83–85
- applying policies 21, 24
- archive files 73
- assigning policies 21, 24
- authorize
 - adware/PUA 65

- authorize (*continued*)
 - suspicious items 62
 - website 67
- automatic cleanup 43
- automatic disinfection 43
- automatic updating 54

B

- bandwidth
 - limiting 55–56
- blocking
 - applications 86
 - file and printer sharing 80
- bootstrap locations 34
- buffer overflow 61

C

- central reporting, configuring 102
- checksums 88
- cleanup 39, 42
 - automatic 43
 - failed 140
 - manual 43
- cleanup status 39
- computer details
 - copying 133
 - printing 134
- computer list
 - copying data from 133
 - printing data from 133
- computers with problems 37
- configurations, applying 101
- configuring
 - central reporting 102
 - policies 23
- configuring Dashboard 35
- configuring update manager 46
- connectivity problems 138
- console access 18
- copying
 - computer details 133
 - computer list data 133
- creating groups 19
- creating policies 24

creating reports 123

D

Dashboard

configuring 35

panels 6

security status icons 7

dealing with alerts 39

default global rules

further information 92

deleting a group 21

deleting policies 25

desktop messaging 116

device control

blocking devices 108

blocking network bridging 106

controlled devices 106

detecting and blocking devices 108

detecting devices without blocking 107

events 105, 119

exempting a device from a policy 109

exempting a device from all policies 108

list of exempt devices 110

messaging 117

overview 104

selecting device types 107

disconnected computers 10

disinfection 42

automatic 43

manual 43

dual location 76, 100

E

editing policies 25

editing roles 15

email alerts

anti-virus and HIPS 115

network status 118

enable

web protection 66

Endpoints view 9

copying data from 133

printing data from 133

errors

acknowledge 40

clear 40

event logging 119

events 119

device control 119

exporting to a file 122

firewall 120

tamper protection 121

exclusions 75

on-access scanning 68

scheduled scanning 70

exporting reports 132

extensions 71

F

failed cleanup 140

file and printer sharing

allowing 79

file and printer sharing, allowing 80

file and printer sharing, blocking 80

file sharing, allowing 80

file sharing, blocking 80

file types scanned 71

filtering ICMP messages 89

find computers

by IP range 28

import from file 29

on the network 28

with Active Directory 27

finding computers 26

Active Directory 27

firewall

adding applications 78, 83

adding checksums 88

advanced configuration 82

advanced options 82

allow file and printer sharing 79

creating a rule 80, 97

disabling 81

enabling 81

events 120

setting up 76

trusting applications 78, 83–85

firewall configuration
 exporting 104
 importing 104
full system scan 41

G

getting started 12
global rules
 setting 94, 96, 99
glossary 142
groups 18–19
 adding computers 20
 creating 19
 cutting and pasting 20
 deleting 21
 importing from Active Directory 27
 policies used 21
 removing computers 20
 renaming 21
 Unassigned group 19

H

hidden processes, allowing 86
HIPS 60
HIPS alerts
 email 115
HIPS messaging
 desktop 116
 SNMP 116
Host Intrusion Prevention System 60

I

ICMP messages
 filtering 89
 information about 90
icons 10
immediate scan 41
immediate updating 59
import computers
 from file 29
in-the-cloud technology 63
initial installation source 58

installation failure
 Sophos Endpoint Security and Control 137
interactive mode, about 82
interactive mode, enabling 82

L

LAN traffic, allowing 79
location awareness
 about 100
 setting up 100
 using two network adapters 100
location roaming 55

M

Mac viruses 72
Macintosh files
 scan 72
Macintosh viruses 72
managed computers 10
manual cleanup 43
manual disinfection 43
manual updating 59
messaging 114
 desktop 116
 SNMP 116
monitor mode 78

N

network shares
 supported 49
network status alerts 118
new user 18
non-interactive mode, changing to a 82

O

on-access scanning
 cleanup 43
 disable 69
 enable 69
 exclude items from 68
 on read 68
 on rename 68

on-access scanning (*continued*)

- on write 68
- turn off 69
- turn on 69

out-of-date computers 137

- finding 36
- updating 59

P

partially detected item 139

policies

- anti-virus and HIPS 60
- applying 21, 24
- assigning 21, 24
- checking 26
- configuring 23
- creating 24
- default 22
- deleting 25
- editing 25
- enforcing 26
- overview 22
- renaming 25
- which groups use 25

potentially unwanted applications 65

pre-authorize

- suspicious items 62
- website 67

preconfigured roles 14

primary locations, defining 101

primary server 55

- changing credentials 56

printer sharing, allowing 80

printer sharing, blocking 80

printing

- computer details 134
- computer list data 133

printing reports 132

priority, scanning 75

Protect computers wizard

- credentials 33
- selecting features 33

protected computers 35–36

protected network 35

protecting computers

- credentials 33
- pre-requisites 31
- preparing for installation 31
- Protect computers wizard 33
- selecting features 33

protection, check 35

PUA 65

- frequent alerts 139
- not detected 139
- side-effects 140

publishing software on a web server 52

R

rawsockets, allowing 87

removal tool

- third-party security software 32

removing computers from groups 20

renaming groups 21

renaming policies 25

reports

- alert and event history 124
- alert summary 125
- alerts and events by item name 125
- alerts and events by time 126
- alerts and events per location 127
- creating 123
- displaying as table 131
- endpoint policy non-compliance 128
- endpoint protection by time 130
- events by user 129
- exporting 132
- layout 132
- managed endpoint protection 130
- overview 123
- policy non-compliance by time 128
- printing 132
- running 131
- scheduling 131
- updating hierarchy 131

resolving alerts

- actions to take 39–40
- cleanup status 39
- information about detected items 40

rights 15

- roles 14
 - adding users and groups to 15
 - editing 15
 - modifying 15
 - preconfigured 14
- rootkits
 - scanning for 73
- rule
 - set 95–96
- rule priority 91
- run scan at lower priority 75
- running reports 131
- runtime behavior analysis 61

S

- scan now 41
- scanning
 - exclusions 75
 - scheduled 70
- scanning computers 41
 - immediately 41
- scheduled scanning 69–70
 - exclude items from 70
- scheduling reports 131
- scheduling updates 57
- secondary configurations, creating 101
- secondary server 55–56
- selecting software 47
- selecting subscriptions 55
- setting a rule 95–96
- setting global rules 94, 96, 99
- setup 12
- SNMP messaging 116
- software
 - selecting 47
 - subscribing to 53
- software distribution 48
- Sophos Endpoint Security and Control installation failure 137
- Sophos Enterprise Manager 3
- Sophos Live Protection
 - disabling 64
 - enabling 64
 - in-the-cloud technology 63
 - overview 63

- Sophos Live Protection (*continued*)
 - turning off 64
 - turning on 64
- Sophos Update Manager 46
- sorting computer list
 - computers with problems 37
 - unprotected computers 37
- spyware 60
- subscribing to software 53
- subscription alerts 114
- subscription usage 54
- subscriptions 53
 - adding 53
 - selecting 55
- supported network shares 49
- suspicious behavior
 - blocking 61
 - detecting 61
- suspicious files 62
- suspicious items
 - allow 62
 - authorize 62
 - pre-authorize 62
- system memory scanning 74

T

- tamper protection
 - changing password 112
 - disabling 112
 - enabling 112
 - events 111, 121
 - overview 111
 - turning off 112
 - turning on 112
- third-party security software removal tool 32
- timeout 138
- toolbar buttons 5
- Trojans 60
- troubleshooting
 - cannot create a new policy 137
 - cleanup 140
 - connectivity problems 138
 - Create Policy grayed out 137
 - disabled Create Policy 137
 - disabled Duplicate Policy 137

troubleshooting (*continued*)

- Duplicate Policy grayed out 137
 - firewall disabled 135
 - firewall not installed 135
 - Linux 138
 - Mac 137
 - on-access scanning 135
 - out-of-date computers 137
 - outstanding alerts 136
 - partially detected item 139
 - PUA, frequent alerts 139
 - PUA, not detected 139
 - PUA, side-effects 140
 - Sophos Endpoint Security and Control installation failure 137
 - timeout 138
 - Unassigned group 136
 - unmanaged computers 136
 - virus, side-effects 140
 - Windows 2000 or later 138
- trusting applications 78, 83–85
- two network adapters
using 100

U

- Unassigned group 19, 136
- unmanaged computers 136
- unprotected computers 37
- up-to-date computers
checking 36
- update manager 46
 - alerts 41
 - complying with configuration 52
 - configuring 46
 - logging 50
 - monitoring 51
 - scheduling 49
 - selecting update source 47
 - self-updating 51
 - software distribution 48
 - supported network shares 49
 - updating 51
 - viewing configuration 46
- Update managers view 11
- update schedule 49

- update server 46
- update source 47
 - alternative 55
 - primary 55
 - secondary 55–56
 - web server 52
- updating
 - automatic 54
 - immediate 59
 - initial installation source 58
 - limiting bandwidth 55–56
 - location roaming 55
 - logging 58
 - manual 59
 - out-of-date computers 59
 - primary server 55
 - primary update source 55
 - proxy details 55–56
 - publishing software on a web server 52
 - scheduling 57
 - secondary server 55–56
 - secondary update source 55–56
- user interface 4–5
 - Endpoints view 9
 - Update managers view 11
- user roles
viewing 15

V

- virus
 - side-effects 140
- virus alerts
email 115
- virus messaging
desktop 116
SNMP 116
- viruses 60

W

- warning signs 10
- web protection 66
- website
 - allow 67
 - authorize 67

website (*continued*)
pre-authorize 67

working mode, changing to interactive 82
worms 60