

SOPHOS

Sophos Helpdesk Console user manual

Document date: February 2008



Contents

1	Introduction to Helpdesk Console	6
	About the interface.....	6
	What is a group?.....	8
	What is a policy?.....	8
	What do the icons mean?.....	9
2	How do I protect computers?	12
	Protect computers.....	12
	Protect computers that require manual installation.....	13
	Protect computers by using a login script.....	14
	Add the firewall to protected computers.....	17
3	How do I check whether my network is protected?	19
	Which computers are protected?.....	19
	Which computers are up to date?.....	20
	Find computers that are unprotected.....	21
	Find computers without the firewall installed.....	22
	Find computers with alerts that need attention.....	22
	Find out-of-date computers.....	23
	Find computers not managed by the console.....	24
	Find computers disconnected from the network.....	24
4	How do I update computers?	26
	Update computers now.....	26
5	How do I ensure that computers comply with policies?	27
	Check whether computers comply with policies.....	27

	Make computers comply with policies.....	27
6	How do I scan computers?.....	29
	Scan computers now.....	29
7	How do I deal with alerts?.....	30
	What do the alert icons mean?.....	30
	Deal with virus and spyware alerts.....	31
	Deal with suspicious behavior alerts.....	32
	Deal with suspicious file alerts.....	32
	Deal with firewall alerts.....	32
	Deal with adware/PUA alerts.....	33
	Deal with controlled application alerts.....	33
	Clear alerts from the console.....	33
8	How do I clean up computers?.....	35
	Clean up computers now.....	35
	Deal with detected items if cleanup fails.....	36
9	How do I generate reports?.....	37
	Generate a report.....	37
	Display a report as a table.....	38
	Display a report as a chart.....	38
	Show the number of alerts per item name.....	38
	Show the number of alerts per location.....	40
	Show the rate of alerts.....	41
	Show history of alerts.....	43
	Print a report.....	44
	Export a report to a file.....	44
	Change the report layout.....	45

10	Troubleshooting	46
	Cannot start Helpdesk Console.....	46
	Groups not shown.....	46
	Sophos Anti-Virus installation failed.....	47
	Computers are not updated.....	47
	Partially detected item.....	48
	Cleanup failed.....	49
	Recover from virus side-effects.....	49
	Recover from application side-effects.....	50
11	Glossary	52
	Index	56

1 Introduction to Helpdesk Console

Sophos Helpdesk Console enables IT help desk staff to monitor and manage Sophos software.

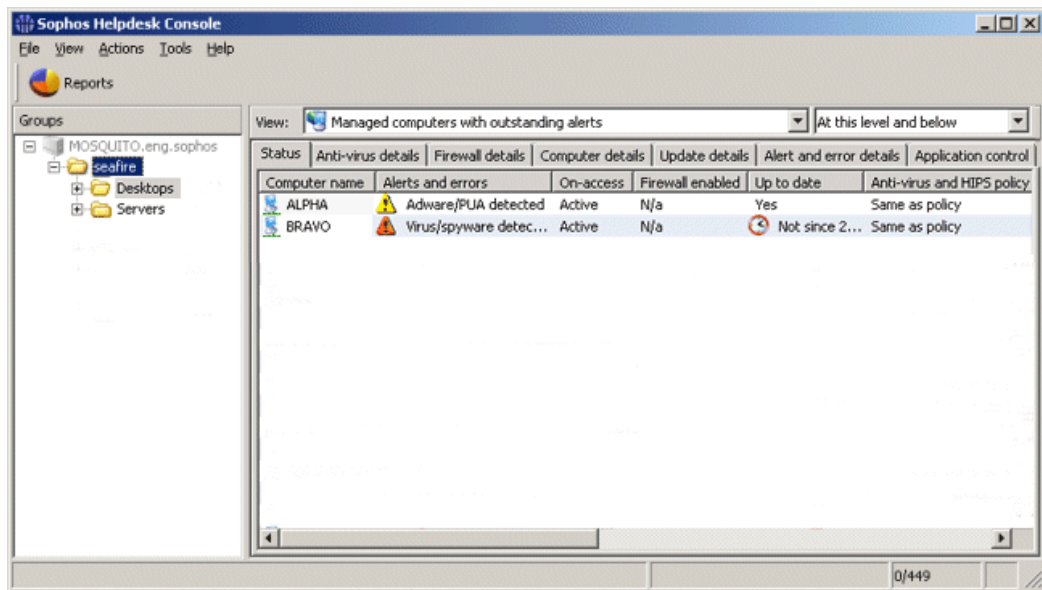
Using Helpdesk Console, you can manage computer groups that your network administrator has given you access to. You can protect computers, ensure that they are up to date, view any threats, potential threats, or unwanted applications that are detected and clean them up.

This section gives you an overview of the interface and key features of Helpdesk Console.

- [About the interface](#)
- [What is a group?](#)
- [What is a policy?](#)
- [What do the icons mean?](#)

About the interface

The main features of the Helpdesk Console interface are described below.



The Groups pane

In the **Groups** pane, you can see the groups of computers that you can manage. Select a group to display a list of the computers.



Your administrator has decided which groups of computers you can see from Helpdesk Console. If you think that you need access to different groups, contact the administrator.

The computer list

The computer list (right-hand pane) displays the computers in the selected group.



If you have Linux computers managed from the console, make sure a unique hostname is configured for each computer. Otherwise, each computer will be displayed in the console with the default name "localhost."

The **Status** tab shows whether the computers are protected by on-access scanning, whether the firewall is enabled, and whether the software is up to date. This page 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 [What do the icons mean?](#)

The toolbar

Reports enables you to generate reports about alerts on your networks.

What is a group?

A group  is a folder that holds a number of computers.

Your administrator decides which groups of computers you can manage from Helpdesk Console. If you think that you need access to different groups, contact the administrator.

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

A group can contain sub-groups.

What is a policy?

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

The network administrator creates the policies. As a Helpdesk Console user, you cannot create or edit policies, but you can ensure that computers comply with the policies that the administrator has created.

The policies are as follows.

- The **Updating** policy specifies how computers are updated with new software.
- The **Anti-virus and HIPS** policy specifies how Sophos Anti-Virus scans for known and unknown viruses, Trojans, worms, spyware, adware and other potentially unwanted applications and detects suspicious behavior and files. It also specifies how Sophos Anti-Virus cleans up computers.
- The **Application control** policy specifies how Sophos Anti-

Virus handles applications you want to control.



- The **Firewall** policy specifies how Sophos Client Firewall protects computers.

What do the icons mean?

In the list of computers, icons are used to indicate:

- alerts
- protection disabled or out of date
- the status of each computer, e.g. whether software is being installed.

Alerts

Sign	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. • A controlled application has been detected. • The firewall has blocked an application. • An error has occurred. <p>A yellow warning sign displayed in the Anti-virus and HIPS policy, Firewall policy, Updating policy, or Application control policy column means that the computer is not using the same 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.





Priority of alerts



1. Virus/spyware alerts
2. Suspicious behavior alerts
3. Suspicious file alerts
4. Firewall alerts
5. Adware/PUA alerts
6. Controlled application alerts
7. Sophos Anti-Virus, updating, and Sophos Client Firewall errors

Protection disabled or out of date

Sign	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

Sign	Explanation
	A blue computer sign means that the computer is managed by Helpdesk Console.
	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 Sophos Anti-Virus has been installed and is now downloading the latest version of the product.

Sign	Explanation
	A gray computer sign means that the computer is not managed by Helpdesk Console.
	A computer sign with a red cross beside it means that the computer is disconnected.

2 How do I protect computers?

This section describes how to install Sophos Anti-Virus and Sophos Client Firewall on networked computers.

- [Protect computers](#)
- [Protect computers that require manual installation](#)
- [Protect computers by using a login script](#)
- [Add the firewall to protected computers](#)

Protect computers

You can protect Windows computers automatically as follows.



Automatic installation is not possible on Windows 95/98/Me computers. Use [manual installation](#) instead.

1. Select the computer(s). Right-click and select **Protect computers**. The **Protect computers wizard** is launched.
2. On the **Welcome** page of the wizard, click **Next**.
3. On the **Select security software** page, select the software you want.

Sophos 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.

Click **Next**.

4. On the **Protection summary** page, any problems with installation are shown in the **Protection issues** column. See the [troubleshooting](#) section, or carry out [manual installation](#) for these computers. Click **Next**.
5. 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 on the computer where you installed the management server
- have read access to the Primary server location specified in the **Updating** policy.



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

Protect computers that require manual installation

If Helpdesk Console is unable to install anti-virus or firewall software on certain computers automatically, you can perform the installation manually.

Helpdesk Console will subsequently manage and update these installations, provided that the computers are in a group or groups.



Alternatively, you can perform the installation automatically by using a script. See [Protect computers by using a login script](#).



If you have a previous version of Sophos Anti-Virus on Windows 95, 98 or Me, you must uninstall it before installing the latest version.

You install manually as follows.

1. In Helpdesk Console, select the computer(s) where you want to make a manual installation. Click the **Update details** tab and look in the **Primary server** column. This shows you the directory that each computer will update from.

If you are using the default directories, the folders from which each product is installed and updated are as follows:

Sophos Endpoint Security and Control for Windows 2000/XP/2003/Vista	\\Servername\InterChk\SAVSCFXP
Sophos Anti-Virus for Windows 2000/XP/2003/Vista	\\Servername\InterChk\ESXP
Sophos Anti-Virus for Windows NT	\\Servername\InterChk\ESNT
Sophos Anti-Virus for Windows 95/98/Me	\\Servername\InterChk\ES9x

Sophos Anti-Virus for Mac OS X	\\Servername\InterChk\ESOSX
Sophos Anti-Virus for Linux	\\Servername\InterChk\savlinux



The directory for "Sophos Endpoint Security and Control" contains the installer for Sophos Anti-Virus and Sophos Client Firewall.

2. Go to the computer and browse to the directory that it will update from.

On a **Windows** computer, double-click setup.exe.

To protect Windows 2000 or later computers with the firewall, as well as anti-virus software, open a command prompt and run setup.exe with the appropriate qualifier:

setup.exe -sav installs anti-virus only

setup.exe -scf installs anti-virus and firewall

On a **Mac OS X** computer, double-click Sophos Anti-Virus.mpkg.

On a **Linux** computer, install Sophos Anti-Virus using the distribution package, as described in the *Sophos Endpoint Security and Control Network Startup Guide*.



If you have Linux computers managed from the console, make sure a unique hostname is configured for each computer. Otherwise, each computer will be displayed in the console with the default name "localhost."

Protect computers by using a login script

You can protect computers with anti-virus software (and with the firewall if your license includes it) by running the installation program with a script or a program like Microsoft SMS.



Helpdesk Console will subsequently manage and update these installations, provided that the computers are in a group or groups.

This page describes:

- Finding the installation program you need

- [Protecting Windows 2000 or later computers](#)
- [Protecting Windows 95/98/Me computers](#)
- [Protecting Mac OS X computers](#)
- [Protecting Linux computers](#)

Finding the installation program you need

The installation program is in the directory that holds Sophos updates. To check which directory this is, look in the computer list and find the computer(s) you want to protect. Click the **Update details** tab and look in the **Primary server** column.

If you are using the default directories, the folders from which each product is installed and updated are as follows:

Sophos Endpoint Security and Control for Windows 2000/XP/2003/Vista	\\Servername\InterChk\SAVSCFXP
Sophos Anti-Virus for Windows 2000/XP/2003/Vista	\\Servername\InterChk\ESXP
Sophos Anti-Virus for Windows NT	\\Servername\InterChk\ESNT
Sophos Anti-Virus for Windows 95/98/Me	\\Servername\InterChk\ES9x
Sophos Anti-Virus for Mac OS X	\\Servername\InterChk\ESOSX
Sophos Anti-Virus for Linux	\\Servername\InterChk\savlinux



The directory for "Sophos Endpoint Security and Control" contains the installer for Sophos Anti-Virus and Sophos Client Firewall.

Protecting Windows 2000 or later computers

If you want to protect Windows 2000 or later computers with the firewall, as well as anti-virus software, you must:

- Ensure that you use the correct setup program. This is the setup program for Sophos Endpoint Security and Control and it is in a directory called SAVSCFXP.
- Run the setup program with the -scf qualifier.


Protecting Windows 95/98/Me computers

To protect Windows 95/98/Me computers with a login script, do as follows.

1. If you do not already know it, find the location of the directory that contains the installation program.
2. Add the following line to the login script:


```
[Path]\setup.exe -user [domain\name] -pwd [password] -login -s
```

where [Path] is the location of the directory that contains the installation program (e.g. \\Servername\InterChk\ES9x), and the username and password are for an account that is able to log on to your Windows 95/98/Me computers, and has read access to the CID share (in this example \\Servername\InterChk).

 If you have any Windows 95 computers, you must run a small utility on them before installation. From the Sophos Endpoint Security and Control Network Install CD, copy the file Tools/Utils/w95ws2setup.exe to your server. Then insert a line in the login script, before the line shown above, to run this utility.

The user account you specify must

- be able to log on to the computers you want to protect
- have administrator rights on the computers you want to protect
- have read access to the Primary server location specified in the **Updating** policy.

 If you do not want to manage the computers with Helpdesk Console, you should add the parameter -mng no

The next time your users log in, their computers will install the anti-virus software.

Protecting Mac OS X computers

For Mac OS X computers, use Apple Remote Desktop. Go to the central installation directory and copy the installer to the computer running Apple Remote Desktop before using it.

Protecting Linux computers

For information about installing Sophos Anti-Virus on Linux computers, see the *Sophos Anti-Virus for Linux Startup Guide*.



If you have Linux computers managed from the console, make sure a unique hostname is configured for each computer. Otherwise, each computer will be displayed in the console with the default name "localhost."

Add the firewall to protected computers

If you have already protected your computers with Sophos Anti-Virus, you can install the Sophos Client Firewall on them, provided that your license includes the firewall.



The firewall can be installed only on computers running Windows 2000 or later.



You cannot install the firewall on computers running server operating systems.

1. Select the computer(s) where you want to install the firewall. Right-click and select **Protect computers**. A wizard is launched.
2. On the **Welcome** page of the wizard, click **Next**.
3. On the **Select security software** page, select **Install Sophos Client Firewall**.
4. On the **Protection summary** page, any problems with installation are shown in the **Protection issues** column. See the [troubleshooting](#) section, or carry out [manual installation](#) for these computers. Click **Next**.
5. On the **Credentials** page, enter details of an account which can

be used to install software. This account is typically a domain administrator account.

3 How do I check whether my network is protected?


This section describes how to ensure that computers are properly protected. It also tells you how to identify computers with a problem using the computer list filters and take action to resolve the problem.

- [Which computers are protected?](#)
- [Which computers are up to date?](#)
- [Find computers that are unprotected](#)
- [Find computers without the firewall installed](#)
- [Find computers with alerts that need attention](#)
- [Find out-of-date computers](#)
- [Find computers not managed by the console](#)
- [Find computers disconnected from the network](#)

You can also check whether all the computers in a group comply with the anti-virus and HIPS, updating, firewall, and application control settings for that group as described in [Check whether computers comply with policies](#).

Which 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.


 On-access scanning may have been deliberately disabled by the administrator on certain types of computer, e.g. file servers.

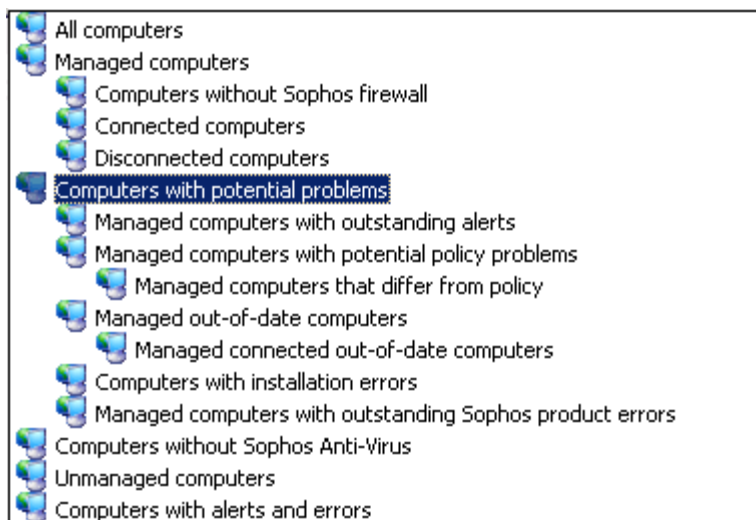
To check that computers are protected:

1. Select the group of computers you want to check.
2. If you want to check computers in sub-groups of the group,

select **At this level and below** in the drop-down list.

3. In the list of computers, 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 computer has firewall protection.
5. Next look in the **Up to date** column. If you see "Yes", the computer is up to date. If you see a clock icon and a date, it is not.

 You can display a list of computers that are not properly protected or have other protection-related problems. Go to the **View** drop-down list and select **Computers with potential problems**. You can also select a subentry of this entry, to display computers affected by a specific problem (e.g. computers that differ from group policy or where a Sophos product error has occurred).



Which computers are up to date?

If your administrator has set up the Sophos security software as recommended, computers should receive updates automatically.

1. Select the group of computers you want to check.

2. If you want to check computers in any sub-groups, select **At this level and below** in the drop-down list.
3. Look in the **Up to date** column.

If you see "Yes", 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.



To update computers immediately, select the computers. Right-click and select **Update computers now**.

Find computers that are unprotected

A computer is not properly protected if it is not running on-access scanning or if the firewall (where installed) is disabled.



On-access scanning may have been deliberately disabled by the administrator on certain types of computer, e.g. file servers.

If a computer is not running on-access scanning, a gray shield and the word "Inactive" are displayed in the **On-access** column on the **Status page**.

If the firewall is disabled, a gray firewall icon (a brick wall) is displayed in the **Firewall enabled** column.

To display all computers that are not properly protected, do as follows:

1. Select the group where you want to find the computers.
2. On the toolbar, in the **View** drop-down list, select **Computers with potential problems**. You can also select a subentry of this entry, to display computers affected by a specific problem (e.g. computers that differ from group policy or where a Sophos product 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**.
4. Any computers that have protection problems will be listed.

Find computers without the firewall installed

If a computer does not have the firewall installed, a gray firewall icon (brick wall) is displayed in the **Firewall enabled** column on the **Status page**.

To display all such computers and fix the problem, do as follows:

1. Select the group where you want to find computers with alerts.
2. On the toolbar, in the **View** drop-down list, select **Computers without Sophos firewall**.
3. If the group contains subgroups, select also whether you want to find computers **At this level only** or **At this level and below**.
4. If there are computers on which you want to install the firewall, select them, right-click and select **Protect computers**. When prompted to select software, select **Install Sophos Client Firewall**.

Find computers with alerts that need attention

If a computer has an alert that needs your attention, there is an alert icon in the **Alerts and errors** column on the **Status page**.

A red warning sign indicates a virus or spyware. A yellow sign indicates suspicious behavior or file, an adware or other potentially unwanted application, an application blocked by the firewall, a controlled application, or an error.

To display the computers that have alerts that still need attention, do as follows:

1. Select the group where you want to find computers with alerts.
2. On the toolbar, in the **View** drop-down list, select **Managed computers with outstanding alerts**.
3. If the group contains subgroups, select also whether you want to find computers **At this level only** or **At this level and below**.

4. If there are computers with a virus or an application you do not want, see Clean up computers now.

If there are computers with an adware or other potentially unwanted application that you **do** want, ask your administrator to authorize it.

If the firewall has blocked an application you **do** want to run, ask your administrator to authorize it.

If there are out-of-date computers, see Find out-of-date computers for help with diagnosing and fixing the problem.



If you do not need the alert displayed any more, you can clear it. Select the computer(s) with alerts, right-click and select **Acknowledge alerts and errors**.

Find out-of-date computers

If a computer has out-of-date anti-virus software, a clock icon is displayed in the **Up to date** column on the **Status** page. 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.

This section tells you how to diagnose the problem and update the computers.

1. Select the group where you want to find out-of-date computers.
2. On the **Status** tabbed page, click on the **Up to date** column 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 select **Update computers now**.

If all are out of date, the problem could be with the directory. Ask your network administrator to ensure that the directory has the latest Sophos software.

Find computers not managed by the console

Windows, Mac, and Linux computers should be managed by Helpdesk Console, so that they can be updated and monitored.

If a computer is not managed, its details on the **Status** tabbed page are grayed out.

You find and fix unmanaged computers as follows.

1. On the toolbar, 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 Anti-Virus.
3. If there are computers on which Helpdesk Console cannot install Sophos Anti-Virus automatically, carry out a manual installation.

Find computers disconnected from the network

If a computer is disconnected from the network, a red cross appears by the icon next to its name on the **Status** page.

To display a list of the computers that are disconnected, do as follows:

1. Select the group where you want to find disconnected computers.
2. On the toolbar, in the **View** drop-down list, select **Disconnected computers**.

3. If the group contains subgroups, select also whether you want to find computers **At this level only** or **At this level and below**



"Disconnected computers" here means computers that are usually managed by Helpdesk Console, but are disconnected. Unmanaged disconnected computers are not shown.

4 How do I update computers?

Computers are usually configured to update with the latest Sophos software automatically. However, you can update computers manually at any time, as described in this section.

- Update computers now

Update computers now

You can update a computer or computers immediately, without waiting for the next automatic update.

Select the computer(s) you want to update. Right-click and select **Update computers now**.

5 How do I ensure that computers comply with policies?

This section tells you how to ensure that all the computers in a group use the same anti-virus and HIPS, updating, firewall and application control settings.

- [Check whether computers comply with policies](#)
- [Make computers comply with policies](#)

Check whether computers comply with policies

You can check whether all the computers in a group comply with the anti-virus and HIPS, updating, firewall, and application control settings for that group.

1. Select the group which you want to check.
2. On the **Status** page, look in the **Anti-virus and HIPS policy**, **Updating policy**, **Firewall policy**, and **Application control policy** columns. If the computer does not use the same settings as the rest of the group, you see a warning sign and the words "Differs from policy".

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

Make computers comply with policies

If you find computers that do not comply with the anti-virus and HIPS, updating, firewall, or application control settings for their group, you can apply the group settings to that computer.

1. Select the computer(s) that do not comply with group settings.
2. Right-click and select **Comply with**. Then select **Group anti-virus and HIPS policy**, **Group updating policy**, **Group firewall policy**, **Group application control policy**, or **All**

group policies as appropriate.

6 How do I scan computers?

By default, Sophos Anti-Virus detects known and unknown viruses, Trojans, worms, and spyware automatically as soon as a user attempts to access files that contain them. Sophos Anti-Virus 7 and later for Windows 2000 and later also analyzes behavior of the programs running on the system.

You can also perform a full system scan of selected computers immediately.

Scan computers now

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



Only Windows computers running Sophos Anti-Virus 7 or later can perform immediate full system scans originated from the console.

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.

7 How do I deal with alerts?

This section describes how to deal with alerts.


It includes:

- [What do the alert icons mean?](#)
- [Deal with virus and spyware alerts](#)
- [Deal with suspicious behavior alerts](#)
- [Deal with suspicious file alerts](#)
- [Deal with firewall alerts](#)
- [Deal with adware/PUA alerts](#)
- [Deal with controlled application alerts](#)
- [Clear alerts from the console](#)


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** page in Helpdesk Console.

Below is a key to the alert icons. In the other pages in this section, you can find advice on dealing with alerts.

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

Alert icons

Sign	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.


Sign	Explanation
	<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. • A controlled application has been detected. • The firewall has blocked an application. • An error has occurred. <p>A yellow warning sign displayed in the Anti-virus and HIPS policy, Firewall policy, Updating policy, or Application control policy column means that the computer is not using the same 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.

Priority of alerts

1. Virus/spyware alerts
2. Suspicious behavior alerts
3. Suspicious file alerts
4. Firewall alerts
5. Adware/PUA alerts
6. Controlled application alerts
7. Sophos Anti-Virus, updating, and Sophos Client Firewall errors


Deal with virus and spyware alerts

If a virus or spyware is detected, you see a red warning triangle 

and the words "Virus/spyware detected" on the **Status** page.


For more details, click the **Alert and error details** tab. To deal with the virus or spyware, follow the instructions in [Clean up computers now](#).

Deal with suspicious behavior alerts

If suspicious behavior or buffer overflow is detected during runtime behavior analysis, you see a red warning triangle  and the words "Suspicious behavior detected" on the **Status** page.

For more details, click the **Alert and error details** tab. To remove the suspicious item, follow the instructions in [Clean up computers now](#). If you want to authorize it, ask your administrator.


Deal with suspicious file alerts

If a suspicious file is detected, you see a yellow warning triangle  and the words "Suspicious file detected" on the **Status** page.

For more details, click the **Alert and error details** tab. The name of the file is shown in the **Item detected** column.

To remove the file, see [Clean up computers now](#). To authorize the file, ask your administrator.

Deal with firewall alerts

If the firewall blocks an application, you see a yellow warning triangle  and the words "Firewall alert" on the **Status** page.





This icon can also indicate an adware/PUA alert from Sophos Anti-Virus. Then the words "Adware/PUA detected" are displayed next to the icon.

For more details, click the **Alert and error details** tab. The name of the application blocked by the firewall is shown in the **Item detected** column.

If you want to allow the application, or to make a new rule for it, ask your administrator.

Deal with adware/PUA alerts


If an adware or other potentially unwanted application (PUA) is detected, you see a yellow warning triangle  and the words "Adware/PUA detected" on the **Status** page.

 This icon can also indicate a firewall alert. Then the words "Firewall alert" are displayed next to the icon.

For more details, click the **Alert and error details** tab. The name of the application is shown in the **Item detected** column.


To remove the application, see [Clean up computers now](#). To authorize the application, ask your administrator.

Deal with controlled application alerts

If a controlled application is detected, you see a yellow warning triangle  and the words "Controlled application detected" on the **Status** page.

For more details, click the **Alert and error details** tab. The name of the application is shown in the **Item detected** column.

To remove the application, you need to go to each computer and run the uninstaller for that product.

 Sophos security software may interfere with uninstallation, as on-access scanning for controlled applications blocks the programs used to install and uninstall applications. You should consult your administrator.

Clear alerts from the console

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

console.



You cannot clear alerts about installation errors. These are cleared only when Sophos Anti-Virus is installed successfully on the computer.

1. Select the computer(s) for which you want to clear alerts. Right-click and select **Acknowledge alerts and errors**.
2. The **Acknowledge alerts and errors** dialog box is displayed.

To clear alerts from the console, in the **Acknowledge alerts and errors** dialog box, on the **Alerts** tab, select the alerts you want to clear and click **OK**. Acknowledged (cleared) alerts are no longer displayed in the console.

To clear Sophos product errors from the console, in the **Acknowledge alerts and errors** dialog box, go to the **Sophos Anti-Virus errors** or **Firewall errors** tab, select the errors you want to clear from the console and click **OK**.

8 How do I clean up computers?


This section describes how to clean up computers that are infected with a virus or have unwanted applications on them.

You can:


- [Clean up computers now](#)
- [Deal with detected items if cleanup fails](#)

Clean up computers now

From Helpdesk Console, you can immediately clean up computers that are infected with a virus or have unwanted applications on them.

 This option applies only to Windows 2000 and later computers running Sophos Anti-Virus 6 or later.

To clean up Windows 95/98/Me and NT4, Mac or Linux computers, you can ask your administrator to set up automatic cleanup, or you can clean up the computers individually as described in [Deal with detected items if cleanup fails](#).

 Sophos Anti-Virus may report that an item (e.g. a Trojan or potentially unwanted application) is "partially detected". This means that it has not found all the component parts of that application. Before you can clean up the item, you will need to find its other components by carrying out a full system scan of the computer(s) affected. For more information, see [Partially detected item](#).

1. In the list of computers, right-click the computer(s) that you want to clean up. Select **Clean up detected items**.
2. In the **Clean up detected items** dialog box, select the check box for each item you want to clean up, or click **Select all**.
3. Click **OK** to clean the computer(s).
4. If the cleanup is successful, the alert(s) 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](#).

Deal with detected items if cleanup fails

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

1. In the computer list, click the **Alert and error details** tab. In the **Item detected** column, look for the name of the item.
2. On the **Help** menu, click **View item information**. This connects you to the Sophos website, where you can search for the item and find advice on how to clean up the computer.
3. Go to each computer and carry out the cleanup manually.



The Sophos website provides special downloadable disinfectors for certain viruses and worms.

9 How do I generate reports?

You can generate reports about alerts on your network.

To do this, you click the **Reports** icon on the toolbar and then use the **Reporting** options as described in this section.

You can:

- Generate a report
- Display a report as a table
- Display a report as a chart
- Show the number of alerts per item name
- Show the number of alerts per location
- Show the rate of alerts
- Show history of alerts
- Print a report
- Export a report to a file
- Change the report layout

Generate a report

To create a report, do as follows.

1. Click the **Reports** icon on the toolbar.
2. In the **Reporting** dialog box, in the drop-down menu, select the type of report that you want.
 - **Alerts by item name** shows the number of alerts for each item (such as a virus or unwanted application) detected on your network.
 - **Alerts per location** shows the number of alerts for each computer or group of computers.

- **Alerts by time** shows the rate of alerts occurring during a set time.
- **Alert History** shows full details of each alert.
- On the **Configuration** tab, you can customize the report.

Then click the **Table** or **Chart** tab to view the report.

Display a report as a table

1. Click the **Reports** icon on the toolbar.
2. In the **Reporting** dialog box, in the drop-down menu, select the type of report you want to create. On the **Configuration** tab, configure the report. Then click the **Table** tab.
3. The table is displayed. The **Report Description** summarizes the criteria (e.g. the length of time covered) used to create the report.

Display a report as a chart



The chart view is not available for 'Alert history' reports.

1. Click the **Reports** icon on the toolbar.
2. In the **Reporting** dialog box, in the drop-down menu, select the type of report you want to create. On the **Configuration** tab, configure the report. Then click the **Chart** tab.
3. The chart is displayed. The **Report Description** summarizes the criteria (e.g. the length of time covered) used to create the report.

Show the number of alerts per item name

1. Click the **Reports** icon on the toolbar.
2. In the **Reporting** dialog box, in the drop-down menu, select **Alerts by item name**.

3. On the **Configuration** tab, you can select the options described below. When you have finished, click one of the other tabs to display the report as a chart or table.

Reporting Period

In the **Period** text box, click the drop-down arrow and select a time period. You can either select a fixed period, e.g. **Last month**, or select **Custom** and specify your own time period in the **Start** and **End** boxes.

Location

Click **Group of computers** or **Individual computer**. Then click the drop-down arrow to specify a group or computer name.

Filter

By default, the report shows all alerts and the number of occurrences for each. You can change the types of alert shown to one of the following:

- All (except controlled applications)
- Viruses/spyware only
- Suspicious behavior only
- Suspicious files only
- Firewall only
- Adware/PUA only
- Controlled applications only

You can also configure the report to show only:

- the top n alerts (where n is a number you specify), or
- alerts with m occurrences or more (where m is a number you specify).

Sort by

By default, the report lists alerts in order of decreasing number of occurrences. Select **Alert name** if you want them listed by name in alphabetical order.

Show the number of alerts per location

1. Click the **Reports** icon on the toolbar.
2. In the **Reporting** dialog box, in the drop-down menu, select **Alerts per location**.
3. On the **Configuration** tab, you can select the options described below. When you have finished, click one of the other tabs to display the report as a chart or table.

Reporting Period

In the **Period** text box, click the drop-down arrow and select a time period. You can either select a fixed period, e.g. **Last month**, or select **Custom** and specify your own time period in the **Start** and **End** boxes.

Location

Click **Computers** to show alerts per computer or **Group** to show alerts for each group of computers.

Filter

By default, the report shows all alerts and the number of occurrences for each. You can change the types of alert shown to one of the following:

- All (except controlled applications)
- Viruses/spyware only
- Suspicious behavior only
- Suspicious files only
- Firewall only

- Adware/PUA only
- Controlled applications only

Alternatively, you can configure the report to show only locations that have reported a particular alert. To specify a single alert, click the drop-down arrow and click an alert name in the list. To specify more than one alert, 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/.

By default, the report shows all computers or groups (depending on the selection made for **Location**). However, you can configure it to show only:

- the top n locations that have recorded the most alerts (where n is a number you specify), or
- locations with m alerts or more (where m is a number you specify).

Sort by

By default, the report lists locations in order of decreasing number of alerts per location. Select **Location** if you want them sorted by name in alphabetical order.

Show the rate of alerts

1. Click the **Reports** icon on the toolbar.
2. In the **Reporting** dialog box, in the drop-down menu, select **Alerts by time**.
3. On the **Configuration** tab, you can select the options described below. When you have finished, click one of the other tabs to display the report as a chart or table.

Reporting Period

In the **Period** text box, click the drop-down arrow and select a

time period. You can either select a fixed period, e.g. **Last month**, or select **Custom** and specify your own time period in the **Start** and **End** boxes.

Location

Click **Group of computers** or **Individual computer**. Then click the drop-down arrow to specify a group or computer name.

Filter

By default, the report shows all alerts and the number of occurrences for each. You can change the types of alert shown to one of the following:

- All (except controlled applications)
- Viruses/spyware only
- Suspicious behavior only
- Suspicious files only
- Firewall only
- Adware/PUA only
- Controlled applications only

If you want the report to show statistics only for a particular alert or group of alerts, use the **Show only alerts like** text box. To specify a single alert, click the drop-down arrow and click an alert name in the list. To specify more than one alert, 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/.

Intervals at which the rate is measured

To specify the intervals of time at which the rate of alerts is measured, e.g. each hour or each day, click the drop-down arrow and select an interval.

Show history of alerts

1. Click the **Reports** icon on the toolbar.
2. In the **Reporting** dialog box, in the drop-down menu, select **Alert History**.
3. On the **Configuration** tab, you can select the options described below. When you have finished, click the **Table** tab to display the report.

Reporting period

In the **Period** text box, click the drop-down arrow and select a time period. You can either select a fixed period, e.g. **Last month**, or select **Custom** and specify your own time period in the **Start** and **End** boxes.

Location

Select **Group of computers** or **Individual computer**. Then click the drop-down arrow to specify a group or computer name.

Filter

By default, the report shows all alerts and the number of occurrences for each. You can change the types of alert shown to one of the following:

- All (except controlled applications)
- Viruses/spyware only
- Suspicious behavior only
- Suspicious files only
- Firewall only
- Adware/PUA only
- Controlled applications only

If you want the report to show statistics only for a particular

alert or group of alerts, use the **Show only alerts like** text box. To specify a single alert, click the drop-down arrow and click an alert name in the list. To specify more than one alert, 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/.

Sort by

By default, alert details are sorted according to **Alert name**. However, reports can also be sorted by **Computer name**, computer **Group name**, or **Date and time**.

Print a report

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



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**.

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 Troubleshooting

This section describes how to deal with problems that might arise when using Helpdesk Console.

- Cannot start Helpdesk Console
- Groups not shown
- Sophos Anti-Virus installation failed
- Computers are not updated
- Partially detected item
- Cleanup failed
- Recover from virus side-effects
- Recover from application side-effects

Cannot start Helpdesk Console

When you try to start Helpdesk Console, the error message "Cannot start Helpdesk Console" may be displayed. This occurs for one of the following reasons.

- The administrator has not made you a member of the Sophos Console Administrators group on the server that is running Enterprise Console. You should ask the administrator to ensure that you are added to this group and the Sophos DB Users group.
- Helpdesk Console Configuration Utility has not been used to configure the Helpdesk Console computer. You should ask the administrator to do this.

Groups not shown

If you cannot see the groups you expect, or you can see no groups at all, there are two possible reasons:

- Your administrator has not configured Helpdesk Console to display the groups.
- Your administrator has renamed the groups since configuring Helpdesk Console.

Ask your administrator to reconfigure Helpdesk Console so that you can manage the groups.

Sophos Anti-Virus installation failed

If the Protect computers wizard fails to install Sophos Anti-Virus on computers, it could be because:

- Helpdesk Console does not know which operating system the computers are running. This is probably because the administrator did not enter their username in the correct format when using Sophos Enterprise Console to find computers. You should ask the administrator to repeat this process, entering their username in the format domain\user.
- The computers are running a firewall (usually this is the case on Windows XP SP2 and Windows Vista computers).
- "Simple File Sharing" hasn't been turned off on Windows XP computers.

A full list of requirements for the anti-virus and firewall software is on the Sophos website, at www.sophos.com/products/all-sysreqs.html

Computers are not updated

If a computer has out-of-date anti-virus software, a clock icon is displayed in the **Up to date** column on the **Status** page. 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.

This section tells you how to diagnose the problem and update the computers.

1. Select the group where you want to find out-of-date computers.
2. On the **Status** tabbed page, click on the **Up-to-date column** 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 select **Update computers now**.

If all are out of date, the problem could be with the directory. Ask your network administrator to ensure that the directory has the latest Sophos software.

Partially detected item

Sophos Anti-Virus may report that an item (e.g. 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 Sophos Anti-Virus 7 for Windows 2000/XP/2003/Vista, you can do this by selecting the computer(s), right-clicking and selecting **Full system scan**.

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, ask your administrator to check the list of items excluded from scanning and remove any items on the list. Then scan your computer again.

Sophos Anti-Virus may not be able to fully detect or remove adware and other potentially unwanted applications with components installed on network drives.

For advice, contact your administrator.

Cleanup failed

If Helpdesk Console fails in an attempt to clean up items ("Cleanup failed"), the reason could be:

- It has not found all the components of a multi-component item. Run a full system scan of the computer(s) to find the other components.
- Some drives or folders that contain item components are excluded from scanning. Ask your administrator to check the items excluded from scanning and remove any items on 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).

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 item 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 your network administrator for advice.

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 Anti-Virus cannot always restore all settings. For example, if an application changed the browser home page, Sophos Anti-Virus 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 Anti-Virus 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 item 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/PUA's side-effects, contact your network administrator.

11 Glossary

[A](#) | [B](#) | [C](#) | [D](#) | [E](#) | [F](#) | [G](#) | [H](#) | [I](#) | [J](#) | [K](#) | [L](#) | [M](#) | [N](#) | [O](#) | [P](#) | [Q](#) | [R](#) | [S](#) | [T](#) | [U](#) | [V](#) | [W](#) | [X](#) | [Y](#) | [Z](#)

[-A-](#)

adware

A program that displays advertising - such as pop-up messages - which affects user productivity and system efficiency.

Application Control

A feature in Sophos Anti-Virus that enables you to block or authorize execution of legitimate applications, according to your organization's policy.

[^ Top of page](#)

[-C-](#)

comma-separated values (CSV)

Another name for the comma-delimited format, a type of data format in which each piece of data is separated by a comma. This is a popular format for transferring data from one application to another, because most database systems are able to import and export comma-delimited data. For example, a .csv file can be imported into Microsoft Excel for further analysis.

controlled application

A legitimate application that is not a security threat, but that you decide is unsuitable for use in your office environment. Controlled applications may include games, instant messaging (IM) clients, Voice over Internet Protocol (VoIP) clients, digital imaging

software, media players, or browser plug-ins.

[^ Top of page](#)

-H-

Host Intrusion Prevention System (HIPS)

Security technology that protects computers from suspicious files, unidentified viruses, and suspicious behavior.

[^ Top of page](#)

-N-

Network Access Control (NAC)

A system that reduces the security threat from unauthorized, non-compliant, or infected computers by restricting their access to network resources.

[^ Top of page](#)

-P-

potentially unwanted application (PUA)

A program that is not inherently malicious, but is generally considered unsuitable for the majority of business networks. Potentially unwanted applications perform actions such as displaying advertising, tracking web sites visited, or changing the configuration of a computer. They include a wide range of programs such as adware, dialers, remote administration tools, and hacking tools.

[^ Top of page](#)

-R-

runtime behavior analysis

Dynamic analysis of the behavior of the programs running on the system performed by the "suspicious behavior detection" and "buffer overflow detection" features.

[^ Top of page](#)

-S-

spyware

A program that installs itself onto a user's computer by stealth, subterfuge or social engineering and sends information from that computer to a third party without the user's permission or knowledge. Spyware includes key loggers, backdoor Trojans, password stealers, and botnet worms, which cause corporate data theft, financial loss and network damage.

suspicious behavior

Behavior normally attributed to malware, exhibited by an application that had not been identified as malicious before it was run.

suspicious file

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).

[^ Top of page](#)

-U-

unidentified virus

A virus for which there is no identity; an unknown virus.

^ [Top of page](#)

-V-

virus

A program which can spread across computers and networks by attaching itself to another program and making copies of itself.

^ [Top of page](#)

Index

A

- acknowledge alerts 33
- acknowledge errors 33
- adware alerts 33
- alerts 22
- anti-virus and HIPS policy 8
- anti-virus protection 14
- application control policy 8

C

- cleanup 49
- cleanup:failed 49
- cleanup:manual 36
- clear alerts 33
- clear errors 33
- Console Administrators group 46
- console GUI 6
- controlled application alerts 33

D

- disconnected computers 24
- disinfection 35
- disinfection:manual 36

E

- error message 46

- export report 44

F

- failed cleanup 49
- firewall 22
- firewall alerts 32
- firewall policy 8
- full system scan 29

G

- glossary 52
- group 8
- group policy 27
- group policy:enforce 27
- groups 46

H

- Helpdesk Console:overview 6

I

- icons 9
- immediate scan 29
- interface 6

M

- manual cleanup 36
- manual disinfection 36
- manual installation 13
- manual updating 26

missing groups 46

O

out-of-date computers 47

outstanding alerts 22

P

partially detected 48

policy 27

potentially unwanted application alerts 33

print report 44

protect computers 12

protect computers:firewall 17

protect computers:manually 13

protect computers:with login script 14

protected computers 19

protected network 19

PUA:side-effects 50

R

report 37

report:display as chart 38

report:display as table 38

report:export 44

report:generate 37

report:history of alerts 43

report:layout 45

report:print 44

report:rate of alerts 41

report:show alerts per item name 38

report:show alerts per location 40

runtime behavior analysis alerts 32

S

scan 29

scan now 29

Sophos Anti-Virus installation failure 47

sort computers 24

spyware alerts 31

suspicious behavior alerts 32

suspicious file alerts 32

T

troubleshooting 46

U

unmanaged computers 24

unprotected computers 21

updating 26

updating policy 8

updating:manual 26

up-to-date computers 20

V

virus alerts 31

virus:side-effects 49

W

warning signs 9

Copyright © 2005-2007 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

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