

# SOPHOS

## Sophos Control Center Help

Product version: 4.1  
Document date: March 2010



# Contents

1 About Sophos Control Center.....	3
2 Introduction to Sophos Control Center.....	4
3 Checking if the network is protected.....	8
4 Protecting new computers.....	10
5 Updating computers.....	12
6 Resolving alerts and threats.....	14
7 Reprotecting computers.....	17
8 Monitoring protected computers.....	18
9 Viewing events.....	21
10 Configuring a scan.....	24
11 Configuring updates.....	32
12 Configuring the firewall.....	35
13 Configuring application control.....	39
14 Configuring device control.....	41
15 Managing notifications.....	44
16 Managing reports.....	48
17 Troubleshooting.....	53
18 Technical Support.....	54
19 Copyright.....	55

# 1 About Sophos Control Center

Using Sophos Control Center, you can:

- Install anti-virus and firewall software on your network.

The Sophos Security Suite and Sophos Computer Security licenses include the firewall; the Sophos Anti-Virus license does not.

- Keep the software updated automatically via the internet.
- Centrally configure detection and cleanup of viruses, worms, Trojans, spyware, and potentially unwanted applications, such as, adware, dialers, remote administration tools, and hacking tools.
- Control which applications can run on the network.
- Prevent users from using unauthorized devices on endpoint computers.
- Centrally configure the firewall, application control, and device control for computers on your network.
- Monitor the network and check that computers are protected and comply with central configuration.
- Provide a summary of threats.
- Generate reports on threat trends.

You can use Sophos Control Center to protect:

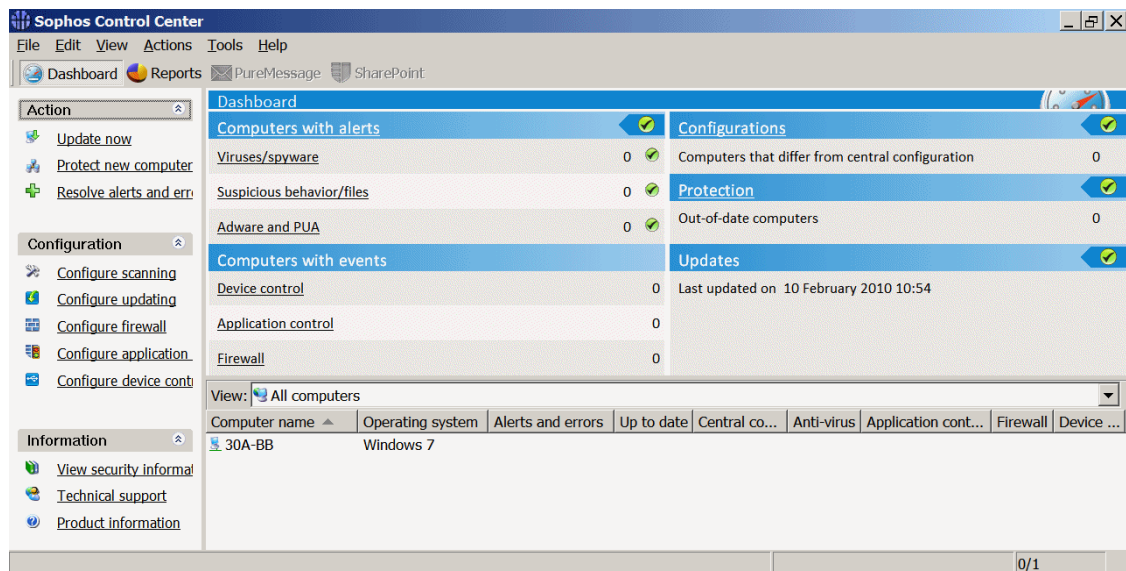
- Windows 2000 and later computers
- Windows 98 (SE) computers
- Mac OS X computers

**Note:** Sophos Control Center version 4.1 is only compatible with Windows 7 and Windows Server 2008 R2.

## 2 Introduction to Sophos Control Center

### 2.1 About the interface

You can use and configure Sophos Anti-Virus and Sophos Client Firewall software via the Sophos Control Center interface, which is the window you are now looking at. The main features are described below:



#### Action menu

This menu enables you to update anti-virus and (if your license includes it) firewall software, protect new computers, and resolve threats.

#### Configuration menu

This menu enables you to configure anti-virus and firewall software and set up alerts about threats.

#### Information menu

This menu gives you access to the threat information on the Sophos website, technical support, and product information.

#### Toolbar

##### ■ Reports

Click this button to open the **Report Manager** dialog box. For instructions on how to generate reports, see [Generate a report](#) (page 48).

##### ■ PureMessage

If you are a PureMessage user, by clicking this button you can launch PureMessage console. The button is enabled only if PureMessage console is installed on the same computer as Sophos Control Center.

#### ■ **SharePoint**

If you are a Sophos for Microsoft SharePoint user, by clicking this button you can launch Sophos for Microsoft SharePoint. The button is enabled only if Sophos for Microsoft SharePoint is installed on the same computer as Sophos Control Center.

### **Dashboard**

The **Dashboard** provides an at-a-glance view of the network's security status. To show or hide the dashboard, click the **Dashboard** button on the toolbar. For more information on dashboard, see [The dashboard overview](#) (page 8).

### **The computer list**

This enables you to see:

- Whether anti-virus and firewall protection is active, inactive, or not installed.
- Whether computers comply with the configuration set centrally via Sophos Control Center.
- Where alerts occur.

For an explanation of the icons displayed in the computer list, see [What do the icons mean?](#) (page 5).

To sort the computer list by a column, click the heading of the column you want to sort by.


To view details for a computer, such as versions and status of anti-virus and firewall software, outstanding alerts, and threat detection history, double-click the computer in the list, to display the **Computer details** window. Alternatively, highlight the computer, right-click, and select **View computer details**.


## **2.2 What do the icons mean?**

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




- alerts
- protection is disabled or out of date
- the status of each computer, such as, whether software is being installed

### **Alerts**






Icon	Description
	A red warning sign displayed in the <b>Alerts and errors</b> column indicates that a virus, worm, Trojan, spyware, or suspicious behavior has been detected.


Icon	Description
	<p>A yellow warning sign displayed in the <b>Alerts and errors</b> column indicates one of the following problems:</p> <ul style="list-style-type: none"> <li>■ A suspicious file has been detected.</li> <li>■ An adware or other potentially unwanted application has been detected.</li> <li>■ An error has occurred.</li> </ul> <p>A yellow warning sign displayed in the <b>Central configuration</b> column indicates the computer is not complying with the central configuration as other computers in its network.</p>

### Protection disabled or out of date



Icon	Description
	A gray shield and the word "Inactive" in the <b>Anti-virus</b> column in the computer list means that on-access scanning is inactive.
	A gray firewall sign and the word "Inactive" in the <b>Firewall</b> column means that the firewall is disabled.
	A clock icon and the word "No" in the <b>Up to date</b> column means that the software is out of date.

### Computer status

Icon	Description
	A blue computer sign means that the computer is managed by Sophos Control Center.
	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 updating component of Sophos Anti-Virus 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 Sophos Control Center.

Icon	Description
	A computer sign with a red cross beside it means that the computer is disconnected.

### Dashboard Status

Icon	Description
	A green icon corresponds to the "normal" status. The number of affected computers is below the set threshold level.
	A red icon indicates the set threshold level has been exceeded for the corresponding category.

## 2.3 Priority of alerts

If there are multiple alerts on a computer, the icon of an alert that has the highest priority will be displayed in the computer list. 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)

## 3 Checking if the network is protected

### 3.1 The dashboard overview

You can use the dashboard to check your network's security status. To show or hide the dashboard, click the **Dashboard** button on the toolbar.

Dashboard	
<b>Computers with alerts</b> (0 alerts, green checkmark)	<b>Configurations</b> (1 warning, red warning icon)
Viruses/spyware: 0 (green checkmark)	Computers that differ from central configuration: 1
Suspicious behavior/files: 0 (green checkmark)	<b>Protection</b> (1 warning, red warning icon)
Adware and PUA: 0 (green checkmark)	Out-of-date computers: 1
<b>Computers over event threshold</b> (0 events, green checkmark)	<b>Updates</b> (1 update, green checkmark)
Device control: 0 (green checkmark)	Last updated at: Not available
Application control: 0 (green checkmark)	
Firewall: 0 (green checkmark)	

The dashboard interface consists of five sections with security status indicators displaying the status of each section based on the threshold value:

#### Computers with alerts

This section displays the number of managed computers with alerts about:

- Known and unknown viruses and spyware
- Suspicious behavior and files
- Adware and other potentially unwanted applications

To view a list of managed computers with outstanding alerts, click the section title, **Computers with alerts**.

#### Computers over event threshold

The section displays the number of events encountered under device control, controlled application, and applications blocked by firewall with status indicators displaying the status of each category.

#### Configurations

This section displays the number of managed computers that do not match the central configuration.

To view a list of managed computers that differ from central configuration, click the section title, **Configurations**.

### Protection

This section displays the number of managed and connected computers on which Sophos Anti-Virus is out of date or uses unknown detection data.

To view a list of managed connected out-of-date computers, click the section title, **Protection**.

### Updates

This section displays the date and time of the last update from Sophos.

## 3.2 Configure dashboard

The dashboard displays 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. If a level is exceeded, the dashboard status indicator changes.

To configure dashboard to indicate the status:

1. On the **Tools** menu, select **Configure Dashboard**.

The **Configure Dashboard** dialog box is displayed.

2. Change the threshold values in the level text boxes as required.
  - a) Under **Computers with outstanding alerts**, enter a percentage of managed computers affected by a particular problem to trigger the change of respective indicator.
  - b) Under **Computers with events**, enter the number of events after which the warnings must be triggered.
  - c) Under **Configuration and protection**, enter a percentage of managed computers affected to trigger the change of respective indicator.
  - d) Under **Latest protection from Sophos**, enter the number of hours since last successful update from Sophos should be received. This will trigger the change of the "Updates" indicator.
  - e) 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 the threshold value is reached. For information, see [Set up network status email alerts](#) (page 45).

## 4 Protecting new computers

### 4.1 Protect new computers

If new computers are added to your network, you must protect them with anti-virus and (if your license includes it) firewall software.

**Note:** Only Windows 2000 and later computers are located for installation, since automatic installation or upgrade is not possible on Windows 98 or Mac OS X computers.

If you have computers that run a different operating system (such as Windows 98 or Mac OS X) from those you have used before, see [Protect new operating systems](#) (page 11).

To protect new computers:

1. In Sophos Control Center, on the **Actions** menu, click **Protect new computers**.  
The **Sophos network protection wizard** starts.
2. On the **Windows user account details** page, enter the details of the administrator account that can be used to install the software on the computers on your network.
3. On the **Protect computers** page, wait for the computers to be located.  
In the **Protect** column, select the computers that you want to protect and click **Next**.
4. In the **Select features** page, select the features that you want to install on the computers.
  - Anti-virus software is selected for installation on all the computers by default.
  - If you want to install the firewall, select the **Firewall** check box.  
Sophos Client Firewall can be installed only on workstations running Windows 2000 or later; it cannot be installed on computers running server operating systems. The firewall requires Sophos Anti-Virus.  
**Note:** You must restart each computer if you choose to install and activate Sophos Client Firewall.
  - If you want to remove any third-party security software, select the **Competitor removal** check box.
5. If there are computers listed on the **Computers you must protect manually** page, click **Print** to print a list of the unprotected computers.  
Alternatively, click **Save as** to save a copy of the list, or make a note of the computers.
6. On the last page of the wizard, click **Finish**.  
After you close the wizard, Sophos Control Center will install the software automatically on as many of the selected computers as possible. You will see the computers listed in Sophos Control Center, with information about their status.

7. Go to each computer on the list of unprotected computers and install the software manually.  
For information on how to perform manual installation, see the Sophos Control Center Startup Guide.

## 4.2 Protect new operating systems

If you add a new type of computer to your network, for example, if you add Windows 98 or Mac OS X computers for the first time, you must enable Sophos Control Center to download anti-virus software for that type of computer.

Sophos Endpoint Security and Control can be installed only on computers running Windows 2000 or later.

To protect new operating systems:

1. In the left pane, under **Configuration**, click **Configure updating**.
2. In the **Configure updating** dialog box, on the **Software** tab, select the operating system or systems that you want to protect.
3. Return to the Sophos Control Center main window. On the **Actions** menu, click **Update now**.
4. Go to each computer of the new type and install the software. For information on how to install manually, see the *Sophos Control Center startup guide*.

## 5 Updating computers

### 5.1 How updating works

Sophos Control Center checks for updates from Sophos every 60 minutes and, if new updates are available, downloads them.

This software is then available on the computer where you run Sophos Control Center. Computers that are managed by Sophos Control Center update themselves automatically from this central copy (by default, they check for updates every 5 minutes).

The time of the last update from Sophos is displayed on the dashboard of the Sophos Control Center.

### 5.2 Did the update succeed?

Updating security software involves two steps:

1. Sophos Control Center downloads updates from Sophos.
2. Networked computers update from your server.

If either step fails, you are alerted as follows:

#### ■ Sophos Control Center fails to download updates

If downloading fails, a message is displayed on the dashboard of Sophos Control Center. You can set to receive an alert when download fails. For information, see [Set up network status email alerts](#) (page 45).

#### ■ Computers fail to update themselves

In the list of computers, the word "No" is displayed in the **Up to date** column next to any out-of-date computer. To force a computer to update, highlight and right-click the computer you want to update. In the menu, click **Update computers now**.

### 5.3 Get alerts about the last update

You can configure Sophos Control Center to alert you if there are problems downloading updates from Sophos.

To get alerts about the last update:

1. On the **Tools** menu, click **Configure Email Alerts**.
2. In the **Configure email alerts** dialog box, click **Configure** and enter details of your SMTP server.

3. Click **Add** and type the email address and set the language to which alerts will be sent in the specified language.
4. In the **Subscriptions** section under **Level exceeded**, ensure you have the **Time since last update from Sophos** option selected, and then click **OK**.

## 5.4 Update the network manually

You can choose to update your security software manually.

To update your security software manually:

1. On the **Actions** menu, click **Update now**.
2. Sophos Control Center displays a message, asking you to confirm that you want to perform an update. Click **Yes**.

Sophos Control Center contacts Sophos and downloads the latest version of the anti-virus and (if you have selected this option) firewall software. All the computers on your network then update themselves automatically the next time they check for updates on your server.

## 5.5 Update an individual computer

If an individual computer is shown as out of date ("No" is displayed in the **Up to date** column), you can prompt it to update.

- ❖ In the computer list, highlight and right-click the computer you want to update. In the menu, click **Update computers now**.

## 6 Resolving alerts and threats

### 6.1 What happens when a threat is found?

If a threat was found on your network, and it has not been cleaned automatically:

- Sophos Control Center will send you an alert, if scanning alerts are enabled. For information, see [Set up anti-virus and HIPS alerts](#) (page 44).
- In Sophos Control Center, in the computer list, an alert icon will be displayed against the name of the infected computer. To find out what caused an alert, highlight the computer in the computer list, right-click, and select **View Computer Details**. For information about the alert icons, see [What do the icons mean?](#) (page 5)
- In Sophos Control Center, in the **Dashboard** pane, the total number of viruses and spyware found on your network will be displayed.

### 6.2 Clean up your computer

To deal with threats, viruses and spyware, and PUAs found on your computers, do the following:

1. On the **Actions** menu, click **Resolve Alerts and Errors**.  
Alternatively, you can click on the alert type links on the Dashboard.  
The **Resolve alerts and errors** dialog box is displayed.
2. In the **Alerts** tab, in the **Show** drop-down select one of the options.  
Based on the selection, information about each infected computer is shown in the columns. such as the name of the infected computer, date and time when the first threat was found on the computer, type of alert, status of the alert, and so on.
3. Based on the selection, **Status** column displays one of the following:
  - **Cleanable**  
In this case, clean up the infected items by using the **Cleanup** button as described later in this topic.
  - **Not Cleanable**  
To clean up the items that appear as "not cleanable" in Sophos Control Center, go to the infected computer and carry out the cleanup manually. If the threat has not been removed, see [Cleanup failed](#) (page 53).
  - **Cleanup in progress (started <time>)**  
Indicates Cleanup process has started.
  - **Cleanup timed out (started <time>)**  
Indicates the cleanup operation has timed out, and the threat may not have been cleaned up. Can be caused when computer is not connected to the network. Make sure the computer is connected to the network and try to clean up the computer again.

- **Restart required**  
Indicates the alert has been partially cleaned up but a restart is required to complete the cleanup.
- **Full scan required**  
Indicates the alert may be cleanable, but a full scan is required to complete the cleanup.
- **Cleanup failed**  
Indicates alert failed to be cleaned up. Manual cleanup may be required.
- **Threat type not cleanable**  
Indicates the item cannot be cleaned up because the alert type is not cleanable.

4. Use the options described below to perform the corresponding action:

- **Select all/Clear all**  
Click these buttons to select or clear all the entries. This enables you to perform the same action on a group of entries. To select or clear a particular entry, click the check box to the left of it.
- **Acknowledge**  
Click this to remove selected entries from the list, if you consider it safe. This action does not delete the items from disk.
- **Cleanup**  
Click this to clean up threats, viruses, spyware, or PUAs from the selected computers.

**Note:** You should subsequently replace cleaned programs from the original disks or a clean backup.

Sophos recommends that before you attempt to clean multi-component threats from the computers, you run a full scan of the computers to determine all components of multi-component threats. For information on scanning computers at set times, see [Scan computers at set times](#) (page 29).

To fully clean some threats consisting of several components from a computer, you may need to restart the computer. If this is the case, a message will appear on the affected computer, giving an option to restart the computer immediately or later. The final cleanup steps will be performed after the computer is restarted.

**Note:** When cleaning up a threat on a computer, the action will be marked as failed if a response is not received from the computer within one hour (measured from the time when an instruction to carry out the action was sent from Sophos Control Center to the computer).

## 6.3 Find information about threats

If a threat is reported, you can find information about its effects, and advice on cleanup.

To find information about threats:

1. In Sophos Control Center, in the computer list, highlight the computer where the threat was found, right-click, and select **View Computer Details**.

2. In the **Computer details** window, scroll down to **Outstanding alerts and errors** and click the threat's name.

Sophos Control Center will connect you to the analysis of the threat on the Sophos website.

Alternatively, you can also go to the Sophos website and browse to the analysis of the threat you want to learn about. To do so, on the **Help** menu, click **View Item Information**.

## 6.4 Deal with error alerts

Information about outstanding scanning and firewall errors that occurred over the last 30 days are displayed in the Errors tab. In particular, you can view the name of the computer where the error was encountered, date and time when the error occurred, and type, code and description of the error.

To deal with anti-virus and firewall errors:

1. On the **Actions** menu, click **Resolve Alerts and Errors**.
2. In the **Resolve alerts and errors** dialog box, click **Errors** tab.
3. Use the options described below to perform the corresponding action:

- **Select all/Clear all**

Click these buttons to select or clear all the entries. This enables you to perform the same action on a group of entries. To select or clear a particular entry, click the check box to the left of it.

- **Acknowledge**

Click this to mark errors as dealt with. Acknowledged alerts are no longer displayed.

## 7 Reprotecting computers

### 7.1 Reprotect computers

You can reinstall anti-virus and firewall software (if your license includes it), which was originally installed on any computers on your network.

To reprotect computers:

1. In the computer list, highlight the computers where you want to reinstall the software.
2. Open the **Tools** menu and select **Reprotect Computers**.

The **Reprotect computers wizard** starts. It guides you through the process of reinstalling software.

For information on how to protect computers manually, see the Sophos Control Center Startup guide.

## 8 Monitoring protected computers

### 8.1 Identify computers that comply with central configuration

Sophos Control Center lets you create a group of settings (for example, for updating) centrally and apply it to endpoint computers, which is referred as central configuration.

To check whether all the computers comply with the anti-virus, updating, firewall, application, and device control configuration set centrally via Sophos Control Center.

Look in the computer list. In the **Central configuration** column, the word "Ok" shows that the computer complies with the central configuration.

- If a computer does not comply with the central configuration (for example, if the computer's configuration has been changed from the computer itself, and it is not marked as locally configured in Sophos Control Center), you will see a yellow warning sign and the word "Changed" in the **Central configuration** column.
- If no security software is installed on a computer, the **Central configuration** column will not display any status (it will be blank) for that computer. If the software is configured locally, you will see "Locally configured". If a computer is waiting for central configuration from Sophos Control Center, you will see "Pending" displayed in this column.

To reapply central configuration to a computer, highlight the computer, right-click and select **Reapply central configuration**.

### 8.2 Identify computers configured locally

You can identify computers on which the anti-virus and firewall software is configured locally in two ways:

- **Display locally configured computers only**

You can display the locally configured computers only.

On the **View** drop-down list, select **Locally configured computers**.

- **Check individual computers**

To see if an individual computer is configured locally, right-click the computer name, if the **Use central configuration** is not selected, the computer is configured locally.

### 8.3 Check computers are protected

In Sophos Control Center a list of computers is displayed with their status.

- In the **Up to date** column, the word "Yes" shows that Sophos protection is up to date on that computer. A clock icon and the word "No" show that it is not.

To arrange the computers according to whether they are up-to-date or not, click the heading of the **Up to date** column.

- In the **Anti-virus** column, the word "Active" shows that on-access scanning is protecting the computer. A grayed-out shield and the word "Inactive" show that it is not.

**Note:** As long as your users' computers are protected by on-access scanning, you do not normally need to run on-access scanning on file servers.

If the software is not installed on the computer, you will see "Not installed" displayed in this column.

- In the **Application control** column, the word "Active" shows when application control is enabled on the computer. A grayed-out icon shield and the word "Inactive" show that it is not.
- In the **Firewall** column, the word "Active" shows that firewall is protecting the computer. A grayed-out firewall icon and the word "Inactive" show that it is not. If the software is not installed on the computer, the column will not display any status (it will be blank) for that computer.

## 8.4 Locate deleted computers

You can retrieve a computer that has been deleted from the list of computers in Sophos Control Center.

To retrieve a computer that has been deleted, you must locate the deleted computer as a new computer. For information on how to locate computers, see [Protect new computers](#) (page 10).

## 8.5 Display computers based on their status

You can display a list of the computers based on their status.

To view a computer based on its status:

- ❖ In Sophos Control Center, in the **View** drop-down list, select a status. The following table displays the list of statuses:

Option	Description
<b>All computers</b>	Displays a list of computers currently connected to the network and managed by Sophos Control Center.
<b>Computers with alerts and errors</b>	Displays a list of the computers that have alerts. To find out what caused an alert, highlight the computer in the computer list, right-click, and select <b>View Computer Details</b> .
<b>Unmanaged computers</b>	Displays a list of computers that are not managed by Sophos Control Center.

Option	Description
<b>Managed out-of-date computers</b>	Displays a list of computers that are managed with out-of-date software.  To update an individual computer, right-click its entry in the computer list and select <b>Update Computers Now</b> .
<b>Managed computers</b>	Displays a list of computers currently managed by Sophos Control Center.
<b>Locally configured computers</b>	Displays a list of computers that are locally configured.  To make the computer use the central configuration again, right-click the computer name and select <b>Use Central Configuration</b> .
<b>Connected computers</b>	Displays a list of computers that are managed and currently available.
<b>Disconnected computers</b>	Displays a list of computers that are managed but currently unavailable, e.g computer is shutdown.

If there are multiple alerts on a computer, the icon of an alert that has the highest priority will be displayed. For information on priority of icons, see [Priority of alerts](#) (page 7).

## 8.6 Print the summary of threats and computer list

You can print the summary of threats on your computers and the computer list for a selected view.

To print the summary of threats and computer list:

1. In the Sophos Control Center window, in the **File** menu, click **Print**.

The **Print** dialog box is displayed.

2. Set up the printing options and click **OK**. The resulting document will include the following information:

- Company name
- Date and time of printing
- Data displayed in the computer list for the selected view

---

## 9 Viewing events

### 9.1 About events

When an application control, firewall, or device control event occurs on an endpoint computer, for example, an application has been blocked by the firewall, that event is sent to Sophos Control Center 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 application control events for the past 24 hours generated by a certain user.

The number of computers with events over a specified threshold within the last 24 hours is displayed on the Dashboard. For information on how to set up the threshold, see [Configure dashboard](#) (page 9).

You can also set up alerts to be sent to your chosen recipients when an event has occurred. For more information, see [Set up anti-virus and HIPS alerts](#) (page 44).

### 9.2 View application control events

To view application control events:

1. On the **View** menu, click **Application Control Events**.  
Alternatively, click on the **Application control** link on the dashboard.  
The **Application Control - Event Viewer** dialog box appears.
2. In the **Search period** field, click the drop-down arrow and select the period for which you want to display the events.  
You can either select a fixed period, for example, **Within 24 hours**, or select **Custom** and specify your own time period by selecting the starting and ending dates and times.
3. Click **Search** to display a list of events.

You can export the list of application control events to a file. For details, see [Export the list of events to a file](#) (page 23).

You can also copy events to the Clipboard. For details, see [Copy events to the Clipboard](#) (page 23).

## 9.3 View device control events

To view device control events:

1. On the **View** menu, click **Device Control Events**.  
Alternatively, click on the **Device control** link on the dashboard.  
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.
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](#) (page 43).

You can export the list of device control events to a file. For details, see [Export the list of events to a file](#) (page 23).

You can also copy events to the Clipboard. For details, see [Copy events to the Clipboard](#) (page 23).

## 9.4 View firewall events

To view firewall events:

1. On the **View** menu, click **Firewall Events**.  
Alternatively, click on the **Firewall** link on the dashboard.  
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. Click **Search** to display a list of events.

In the **Firewall - Event Viewer** dialog box, you can customize a firewall rule as described in [Set up the firewall](#) (page 35).

You can export the list of firewall events to a file. For details, see [Export the list of events to a file](#) (page 23).

You can also copy events to the Clipboard. For details, see [Copy events to the Clipboard](#) (page 23).

## 9.5 Export the list of events to a file

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

1. On the **View** menu, click one of the “events” option, 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 application control events](#) (page 21), [View device control events](#) (page 22), or [View firewall events](#) (page 22).
3. Click **Export**.
4. In the **Save As** dialog box, enter a file name and browse to select a destination for the file.

## 9.6 Copy events to the Clipboard

You can copy application control, firewall, or device control events to the Clipboard and then paste into another document in a tab-separated format. You can copy all events in the list or one event.

1. On the **View** menu, click one of the “events” option, 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 application control events](#) (page 21), [View device control events](#) (page 22), or [View firewall events](#) (page 22).
3. In the **Event Viewer** dialog box, click **Copy** to copy the list of events to the Clipboard.  
If you want to copy one event, select the event and click **Copy**.

## 10 Configuring a scan

### 10.1 Scan for viruses, Trojans, spyware and worms

By default, Sophos Anti-Virus detects viruses, Trojans, spyware and worms automatically as soon as a user attempts to access files that contain them.

To scan your computer:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, in the **Configure anti-virus and HIPS** panel, ensure **Enable on-access scanning** check box is selected.

### 10.2 Scan for potentially unwanted applications

By default, Sophos Anti-Virus detects viruses, Trojans, spyware and worms. You can also configure it to detect potentially unwanted applications.

**Note:** This option applies only to Sophos Endpoint Security and Control running on Windows 2000 or later.

Sophos recommends 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.

To scan for potentially unwanted applications:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, in the **Scheduled scanning** panel, click **Add** to create a new scan, or select a scan in the list and click **Edit** to edit it.
3. In the **Scheduled scan settings** dialog box, click **Configure** (at the bottom of the page).
4. In the **Scanning and cleanup settings** dialog box, click the **Scanning** tab. In the **Other scanning options** panel, make sure that **Scan for adware and PUA** is selected. Click **OK**.
5. When the scan is carried out, Sophos Anti-Virus may report some "potentially unwanted applications."

If you want your computers to run the applications, you must authorize them. For information on how to authorize application, see [Authorize applications for use](#) (page 29).

6. If you want to enable on-access detection, in the **Configure scanning** dialog box, click **On-access scanning**.

In the **On-access scan settings** dialog box that appears, under **Other Scanning options**, select **Scan for adware and PUA**.

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 53).

## 10.3 Set up on-access scanning options

To set up on-access scanning options:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, click **On-access scanning**.
3. In the **On-access scan settings** dialog box, select the options, as required.
  - **Scan inside archive files**

You can scan inside archive files. However, before enabling this option, consider the following:

    - On-access scanning automatically checks files in an archive when you access those files. Scanning inside archives is therefore optional.
    - Scanning inside archives has an impact on computers' performance and is not recommended for use with on-access scanning.
  - **Scan for Macintosh viruses**

Select to scan Macintosh files stored on Windows computers during on-access scanning.
  - **Scan for adware and PUA**

By default, Sophos Endpoint Security and Control detects viruses, Trojans and worms. You can also configure it to detect potentially unwanted applications.
  - **Scan for suspicious files (HIPS)**

Select to scan for suspicious files during on-access scanning.
4. Under **On-access scanning behavior**, select the files to scan when the user is carrying out operations.
  - **On read**, Sophos Anti-Virus software scans files automatically "on access". By default, this means when the user opens the file ("on read").
  - **On write**, if you want files checked as they are closed.
  - **On rename**, if you want files checked as they are renamed.

These options give greater protection against viruses that write to the computer's hard drive and/or rename files. However, the increased activity may affect the computer's performance.

5. Under **Removable media**, select **Allow access to drives with infected boot sectors** to allow access. For example, to copy files from a floppy disk infected with a boot sector virus.

By default, Sophos Anti-Virus prevents access to removable disks whose boot sectors are infected.

## 10.4 Change types of files scanned

The file types scanned by default differ between operating systems and change as the product is updated.

### ■ On Mac

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.

### ■ On Windows

By default, Sophos Anti-Virus scans file types that are vulnerable to viruses. You can scan additional file types or choose to exempt some file types from scanning. To see a list of the file types, go to a computer with the relevant operating system, open the Sophos Anti-Virus window and look for the "Extensions" configuration page.

**Note:** On Windows 98 computers, changes made in the scheduled scan settings apply to on-access scanning also.

To change types of files scanned:

1. In the left pane, under **Configuration**, click **Configure scanning**. The **Configure scanning** dialog box is displayed.
  - To configure on-access scanning, under **Configure anti-virus and HIPS**, click **On-access Scanning**.
  - To configure scheduled scans, under Scheduled scanning, click **Extensions and Exclusions**.
2. In the **Extensions** tab:
  - To scan additional file types, click **Add** and type the file extension, such as PDF, in the Extension field.
  - **Scan files with no extension**. By default files with no extension are scanned.
  - 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.

## 10.5 Enable web scanning

Web scanning scans data and files downloaded by Internet Explorer. By default, web scanning is disabled.

To enable web scanning:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, next to **Web scanning is:**, select **On**.

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

## 10.6 Exclude items from on-access scanning

This topic tells you how to exclude items (for example, drives, folders, or files) from on-access scanning.

You can exempt some of the file types from scanning, by adding the file extensions to the **Excluded extension list**. For instructions on how to do this, see [Change types of files scanned](#) (page 26).

- The "exclude items" options apply only to Windows 2000 or later and Mac OS X computers.
  - To exclude items on Windows 98 computers, see [Exclude items from scheduled scanning](#) (page 31).
1. In the left pane, under **Configuration**, click **Configure scanning**.
  2. In the **Configure scanning** dialog box, click **On-access scanning**.
  3. In the **On-access scan settings** dialog box, click the **Windows exclusions** or **Mac exclusions** tab.
    - Click **Add**, to add items to the list by entering the full path in the **Exclude item** dialog box.
    - Select **Exclude remote files**, if you want to prevent Sophos Anti-Virus from scanning files on network drives.

## 10.7 Setting up automatic cleanup

### 10.7.1 About automatic cleanup

You can have computers cleaned up automatically as soon as a virus is found. To do this, you must change the scanning settings as described.

**Note:** On-access scanning cannot clean up potentially unwanted applications, however, you can enable automatic cleanup of unauthorized applications during a scheduled scanning, as described later in this topic.

## 10.7.2 Clean up viruses automatically

You can clean up viruses automatically during on-access and scheduled scanning.

To clean up viruses automatically:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. To change the settings for on-access scanning, in the **Configure scanning** dialog box, click **On-access scanning** button. In the **On-access scan settings** dialog box, click the **Cleanup** tab.
3. To change the settings for a scheduled scan, in the **Configure scanning** dialog box, under **Scheduled scanning**, select a scan and click **Edit**.

In the **Scheduled scan settings** dialog box, click **Configure**. In the **Scanning and cleanup settings** dialog box, click **Cleanup** tab.

4. Select **Automatically clean up items that contain a virus/spyware**.
5. You can also specify what should be done if cleanup fails. The options are:
  - Deny access only
  - Delete
  - Deny access and move to a default location
  - Deny access and move to UNC

**Note:** If you select **Move to** and specify a location, Mac OS X computers will still move infected items to the default location.

## 10.7.3 Clean up potentially unwanted applications automatically

**Note:** This option applies only to Sophos Endpoint Security and Control running on Windows 2000 or later.

You can clean up potentially unwanted applications automatically only during a scheduled scanning.

To clean up potentially unwanted applications automatically:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, under **Scheduled scanning**, select a scan and click **Edit**.
3. In the **Scheduled scan settings** dialog box, click **Configure**.
4. In the **Scanning and cleanup settings** dialog box, click the **Cleanup** tab.

5. Under Adware and PUA, select **Automatically clean up adware and PUA**.

This will enable Sophos Anti-Virus to remove from your computers potentially unwanted applications.

6. You can also specify the action to be taken on suspicious files. The options are:

- Deny access only
- Delete
- Deny access and move to a default location
- Deny access and move to UNC

**Note:** If you select **Move to** and specify a location, Mac OS X computers will still move infected items to the default location.

## 10.8 Authorize applications for use

If you have enabled Sophos Anti-Virus to detect potentially unwanted applications, it may prevent the use of an application that you want.

To authorize applications:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, click **Authorization**.
3. In the **Authorization Manager** dialog box, in the **Known adware and PUAs** list, select the application you want to authorize. Click **Add** to add it to the list of authorized applications. Repeat for each application you want to authorize. Click **OK**.
4. If you cannot see the application you want to authorize, click **New Entry**. In the **Add New Adware or PUA** dialog box, enter the name of the new adware or PUA you want to authorize and click **OK**.

## 10.9 Scan computers at set times

You can configure computers to scan at set times.

To scan computers at set times:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, in the **Scheduled scanning** panel, click **Add**.
3. In the **Scheduled scan settings** dialog box, enter a name for the scanning job.
4. Select the items to scan:
  - Local hard disks
  - Floppy disk and removable drives
  - CD drives

By default, all local hard disks are scanned.

5. Select the days and times at which you want the scan to run.

If you want to change the default scanning or cleanup options for the scan, click **Configure** at the bottom of the **Scheduled scan settings** dialog box. For more information, see [Set up scheduled scanning options](#) (page 30) or [Clean up viruses automatically](#) (page 28).

To learn how to change types of files scanned or exclude certain items from scheduled scanning, see [Change types of files scanned](#) (page 26) or [Exclude items from scheduled scanning](#) (page 31).

## 10.10 Set up scheduled scanning options

You can choose to configure your scheduled scanning options.

To set up options for a scheduled scan:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, select a scheduled scan and click **Edit**.
3. In the **Scheduled scan settings** dialog box, click **Configure**.
4. In the **Scanning and cleanup settings** dialog box, under the **Scanning** tab, select the desired options.

### ■ Scan inside archive files

You can scan inside archive files. However, before enabling this option, consider the following:

- On-access scanning automatically checks files in an archive when you access those files. Scanning inside archives is therefore optional.
- Scanning inside archives has an impact on computers' performance and is not recommended for use with on-access scanning.

### ■ Scan for Macintosh viruses

Select to scan Macintosh files stored on Windows computers during a scheduled scan.

### ■ Scan for adware and PUA

By default, Sophos Endpoint Security and Control detects viruses, Trojans and worms. You can also configure it to detect potentially unwanted applications. The option is selected by default for a scheduled scan.

### ■ Scan for suspicious files (HIPS)

By default, scanning for suspicious files is enabled during a scheduled scan.

### ■ Enable rootkit scan

Scanning for rootkits is always performed when you run a full system scan of a computer. The option can also be enabled for a scheduled scan.

For information on cleanup options, see [About automatic cleanup](#) (page 27) and the other topics in the Setting up automatic cleanup section.

## 10.11 Exclude items from scheduled scanning

This topic tells you how to exclude items (for example, drives, folders, or files) from scheduled scanning.

You can also exempt some of the file types from scanning, by adding the file extensions to the **Excluded extension list**. For instructions on how to do this, see [Change types of files scanned](#) (page 26).

**Note:** On Windows 98 computers changes made in the scheduled scan settings apply to on-access scanning too.


To exclude items from scheduled scanning:

1. In the left pane, under **Configuration**, click **Configure scanning**. The **Configure scanning** dialog box is displayed.
2. In the **Scheduled scanning** panel, click **Extensions and Exclusions**.
3. In the **Scheduled scan extensions and exclusions** dialog box, click **Windows Exclusions** or **Mac Exclusions** tab based on the operating system files that should be excluded from scanning. To add items to the list, click **Add** and enter the full path in the **Exclude item** dialog box.

## 10.12 Configure scanning on individual computers

You can configure certain computers to use options different from those set centrally at the Sophos Control Center.

To configure scanning on individual computers

1. In the computer list, highlight the computer or computers. Right-click and deselect **Use central configuration**.
2. Now go to the individual computer(s) and configure the anti-virus options.  
  
To configure scanning on an individual computer, right-click the Sophos Endpoint Security and Control taskbar icon .
3. Click **Open Sophos Endpoint Security and Control**. In **Sophos Endpoint Security and Control** window, click **Configure anti-virus and HIPS**. Under **Configure**, click **On-access scanning** and edit the settings.

For more information on how to configure scanning on individual computers, refer to Sophos Endpoint Security and Control Help.

## 11 Configuring updates

### 11.1 Change what is updated

You can change the software that is updated. You need to do this if:

- You add computers with a different operating system, such as Mac OS X, to your network and you need Sophos Anti-Virus for that system.
- You take all the computers of a particular operating system off your network.

To change the software downloaded:

1. In the left pane, under **Configuration**, click **Configure updating**.
2. In the **Configure updating** dialog box, click the **Software** tab. Then select the operating system or systems for which you need Sophos Anti-Virus and click **OK**.

If you selected operating systems you have not protected before (Windows 98 or Mac OS X), continue to steps 3 and 4.

3. Return to the Sophos Control Center main window. On the **Actions** menu, click **Update now** to download the new software.
4. Go to each computer of the new type and install Sophos Anti-Virus. For information on how to install manually, see the Sophos Control Center Startup guide.

### 11.2 Update via a proxy server

If you use a proxy server to access the internet, you must enable Sophos Control Center to download updates via the proxy.

To update via a proxy server:

1. In the left pane, under **Configuration**, click **Configure updating**.
2. In the **Configure updating** dialog box, click the **Proxy** tab. Type the proxy address and port number. Type the username and password for an account that has access to the proxy (your network administrator can give you these details).

### 11.3 Change the user ID for updating

You can change the user ID that is used to download updates.

To change the user ID for updating:

1. In the left pane, under **Configuration**, click **Configure updating**.
2. In the **Configure updating** dialog box, click the **User ID** tab. Type in the username and password supplied to you by Sophos.

## 11.4 Turn off automatic updating

If you need to turn off automatic updating (for example, you have a dial-up connection), do as follows:

**Note:** If you turn off automatic updating, ensure you check for updates regularly. For information on checking for updates manually, see [Update the network manually](#) (page 13).

To turn off automatic updating:

1. In the left pane, under **Configuration**, click **Configure updating**.
2. In the **Configure updating** dialog box, click the **Schedule** tab. Clear **Enable networked computers to use Sophos updates automatically** check box.

## 11.5 Change how often computers update

By default, computers on your network check every 10 minutes to see if there is updated security software available.

To change the frequency of update:

1. In the left pane, under **Configuration**, click **Configure updating**.
2. In the **Configure updating** dialog box, click the **Schedule** tab. Make sure that the check box **Enable networked computers to use Sophos updates automatically** is selected. In the field below the check box enter a time interval in minutes.

## 11.6 Update computers not always on the network

By default, networked computers update themselves from an updates folder on the computer where you run Sophos Control Center. If this folder becomes unavailable to a computer, for example, when it is not connected to a company network but connected to the internet, the computer will update directly from Sophos.

To update computers not always on the network:

1. In the left pane, under **Configuration**, click **Configure updating**.
2. In the **Configure updating** dialog box, click the **Alternative source** tab, the following options are displayed:

■ **From Sophos**

Select this option if you have computers that are not always connected to the company network, for example, laptops. The computers will use the same credentials that your copy of Sophos Control Center uses.

■ **None**

This is the default option. Does not specify an alternative source.

■ **From your company**

Select this option if you want your networked computers to update from a company website or directory, if the primary updating location becomes unavailable. Enter the address of a network folder (UNC path) or a website (HTTP address).

If necessary, enter the username and password of an account that your computers can use to access the folder or website. This account should have read rights to the directory you entered in the address field above. If the username needs to be qualified to indicate the domain, use the form domain\username.

**Note:** If you specify a folder on your company network or website, you must ensure that regularly updated copies of the security software are available in that folder. You can do this by installing Sophos Control Center. You can also arrange to publish copies of the updates folder.

## 12 Configuring the firewall

### 12.1 Set up the firewall

You can configure the firewall to block or allow traffic based on your requirements. By default, the firewall blocks all non-essential traffic.

For a complete list of the firewall factory settings, go to:

<http://www.sophos.com/support/knowledgebase/article/16608.html>

To configure the firewall:

1. In the left pane, under **Configuration**, click **Configure firewall**.
  2. On the Firewall configuration wizard, click **Next**.
  3. On the **Configure firewall** page, choose any of the following options:
    - Select **Allow all traffic** if you want to turn off the firewall and allow all traffic.
    - 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 the office. You may want to set up dual location for laptops.
  4. If you selected **Dual location** on the previous page, on the **Network identification** page, configure DNS or Gateway identification of your network.
- Note:** The **Network identification** page appears only if you select **Dual location**.
- Sophos Control Center will then apply different firewall settings to the computers depending on whether they are on the network or not.
5. On the **Operational Mode** page, select how the firewall should handle inbound and outbound traffic.

- **Learning mode**

This allows your computers to access the network and internet and reports the information back to console.

- **Block inbound and allow outbound traffic**

This allows your computers to access the network and internet but blocks any inbound traffic.

- **Block inbound and outbound traffic**

If you select this option, the firewall will block all outbound traffic, except for the applications you specify by clicking the **Trust** button to the right of this option. For a "trusted" application, all network activity is allowed.

6. Click **Advanced** to open advanced configuration for firewall.

**Note:** This is an advanced option, and you should only use it if you understand the effects of the changes you make.

For information on advanced firewall configuration, see the Sophos Endpoint Security and Control Help.

7. On the **File and print sharing** page, select **Allow file and print sharing** if you want to allow other computers on the local area network to access printers and shared folders on your computer.
8. If you selected **Dual location**, you will be prompted to configure the inbound and outbound traffic, and file and printer sharing (as mentioned in step 5 and 7) for the secondary (off the network) location.

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 22).

You can choose to run the wizard again, if you choose to modify any of the settings later.

The number of computers with events over a specified threshold within the last 24 hours is also displayed on the Dashboard.

## 12.2 Turn the firewall off

### 12.2.1 To turn the firewall off at the Sophos Control Center

You can choose to turn the firewall off for all the computers that are managed from Sophos Control Center.

For day-to-day use, Sophos recommends that you keep your firewall enabled.

To turn the firewall off at the Sophos Control Center:

1. In the left pane, under **Configuration**, click **Configure firewall**.

The **Firewall configuration wizard** starts.

2. In the **Configure firewall wizard**, go to the **Configure firewall** page and select **Allow all traffic**.

### 12.2.2 To turn the firewall off on an individual computer

You can choose to turn off firewall for selected computers.

To turn the firewall off on an individual computer:

1. In the computer list, highlight the computer(s). Right-click and deselect **Use central configuration**.

**Note:** If you set the computer not to use central configuration, along with firewall, you can configure Sophos Anti-Virus locally as well.

2. Now go to the individual computer(s) and turn off the firewall by locating the Sophos Endpoint Security and Control shield icon .
  - a) Right-click the icon to display a menu, and select **Open Sophos Endpoint Security and Control**.
  - b) In the **Firewall** section, click **Configure firewall**.  
The firewall configuration window is displayed.
  - c) Click the **General** tab and select **Allow all traffic**. Click **OK**.

## 12.3 Allow applications that have been blocked

If the firewall blocks an application on your networked computers, an event is logged in the firewall log.

To find details of blocked applications, and allow them or create new rules for them:

1. On the **View** menu, point to **Events** and then click **Firewall events**.
2. In the **Firewall - Event Viewer** dialog box, select the entry for the application you want to allow or create a rule for. Click **Create Rule**.
3. In the dialog box that appears, select whether to allow 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**.

## 12.4 Configure the firewall on individual computers

If you want certain computers to use options different from those set centrally at the Sophos Control Center, do the following:

1. In the computer list, highlight the computer(s). Right-click and deselect **Use central configuration**.

2. Go to the individual computer(s) and configure the firewall options there as follows:
  - a) On the computer, locate the Sophos Endpoint Security and Control shield icon .
  - b) Right-click the icon to display a menu, and select **Open Sophos Endpoint Security and Control**.
  - c) In the **Firewall** section, click **Configure firewall**.  
The firewall configuration window is displayed.

## 13 Configuring application control

### 13.1 About application control

Sophos Control Center enables you to detect and block "controlled applications", that is, legitimate applications that are not a security threat, but that you decide are unsuitable for use in your office environment. Such applications may include instant messaging (IM) clients, Voice over Internet Protocol (VoIP) clients, digital imaging software, media players, or browser plug-ins.

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

The list of controlled applications is supplied by Sophos and updated regularly. You cannot add new applications to the list, but you can submit a request to Sophos to include a new legitimate application you would like to control on your network. For details, see Sophos support knowledgebase article 35330 (<http://www.sophos.com/support/knowledgebase/article/35330.html>).

#### Application control events

When an application control event occurs, for example, a controlled application has been detected on the network, the event is written in the application control event log that can be viewed from Sophos Control Center. For details, see [View application control events](#) (page 21).

By default, the number of computers with events over a specified threshold within the last 24 hours is displayed on the Dashboard.

You can also set up alerts to be sent to your chosen recipients when an application control event has occurred. For details, see [Set up application control alerts](#) (page 46).

### 13.2 Set up applications control

You can configure Sophos Control Center to scan for applications you want to control on your network on access.

1. In the left pane, under **Configuration**, click **Configure application control**.

The **Configure application control** dialog box is displayed.

2. On the **Scanning** tab, set the options as follows:

- To enable on-access scanning, select the **Enable on-access scanning** check box. If you want to detect applications but do not want to block them on access, select the **Detect but allow to run** check box.
- To enable on-demand and scheduled scanning, select the **Enable on-demand and scheduled scanning** check box.

**Note:** Your anti-virus and HIPS policy settings determine which files are scanned (that is, the extensions and exclusions).

3. Click the **Authorization** tab and select the applications you want to control.

For information on how to select applications, see [Select the applications to control](#) (page 40).

If you want to remove controlled applications found on your networked computers, follow the instructions in [Uninstall controlled applications](#) (page 40).

You can also have alerts sent to particular users if a controlled application is found on any of the computers in the group. For information, see [Set up application control alerts](#) (page 46).

### 13.3 Select the applications to control

By default, all applications are allowed. You can select the applications you want to control as follows:

1. In the left pane, under **Configuration**, click **Configure application control**.
2. In the **Configure application control** dialog box, click the **Authorization** tab.
3. Select the **Application type**, for example, **File sharing**.

A full list of the applications included in that group is displayed in the **Authorized** list.

- To block an application, select it and move it to the **Blocked** list by clicking the "Add" button.



- To block any new applications that Sophos adds to that type in the future, move **All added by Sophos in the future** to the **Blocked** list.
- To block all applications of that type, move all applications from the **Authorized** list to the **Blocked** list by clicking the "Add all" button.



### 13.4 Uninstall controlled applications

Before you uninstall controlled applications, ensure that on-access scanning for controlled applications is disabled. This type of scanning blocks the programs used to install and uninstall applications, so it may interfere with uninstallation.

You can remove an application in one of two ways:

- Go to each computer and run the uninstaller for that product. You can usually do this by opening the Windows Control Panel and using Add/Remove Programs.
- At the server, use your usual script or administration tool to run the uninstaller for that product on your networked computers.

Now you can enable on-access scanning for controlled applications.

## 14 Configuring device control

### 14.1 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.

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

If you want to enable device control for the first time, Sophos recommends that you:

- Select device types to control.
- Detect devices without blocking them.
- Set up device control alerts.
- Detect and block devices or allow read-only access to storage devices.

#### Device control events

When a device control event occurs, for example, a removable storage device has been blocked, the event is written in the device control event log that can be viewed from Sophos Control Center. For details, see [View device control events](#) (page 22).

By default, the number of computers with events over a specified threshold within the last 24 hours is displayed on the Dashboard.

You can also set up alerts to be sent to your chosen recipients when a device control event has occurred. For details, see [Set up device control alerts](#) (page 46).

### 14.2 What types of devices 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 disk drives (CD-ROM/DVD drives/Blu-ray drives)
- Floppy disk drives

- Secure removable storage devices (for example, 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, visit the Sophos website ([www.sophos.com](http://www.sophos.com)).

## Network

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

For network interfaces, you can set an additional access level of Block Bridged mode. It allows network device to become enabled (i.e. Modem or Wi-Fi adapters) when the computer is physically disconnected from the network. Select the Block bridged option when setting access levels for network devices.

**Note:** The Block bridged mode prevents network bridging, for example, between a corporate network and a non-corporate network. The mode is available for both wireless and modem types of devices. 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, blocking Bluetooth interfaces will block both:

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

## 14.3 Set up device control

You can configure Sophos Control Center to scan for devices you want to control on your network on access.

1. In the left pane, under **Configuration**, click **Configure device control**.

The **Device control policy** dialog box is displayed.

2. On the **Configuration** tab, set the options as follows:
  - To enable device control, select the **Enable device control scanning** check box. If you want to detect devices but do not want to block them, select the **Detect but not block devices** check box.
  - To set the access-level for each type of device, 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.”

## 14.4 Exempt a device

You can exempt a device from device control policies.

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:

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 22).
3. Select the entry for the device that you want to exempt, and then click **Exempt Device**.

The **Exempt device** dialog box appears. Under **Device details**, you see the type, model, and ID of the device.

## 15 Managing notifications

### 15.1 Configure notifications

You can configure Sophos Control Center to send alerts when threats are found in your network and/or when there is a change in your network status. Sophos Control Center also lets you choose how you want to handle old alerts.

E-mail alerts in Sophos Control Center are divided into two categories:

- An alert sent to your chosen recipients if a virus, a suspicious behavior, an unwanted application, or an error is encountered in any of the computers on the network. These alerts are configured through the **Configure scanning > Messaging** options. For information, see [Set up anti-virus and HIPS alerts](#) (page 44).
- An alert sent to your chosen recipients when a level set on the Dashboard has been exceeded. It is configured in any of the two ways:
  - **Tools > Configure email alerts**
  - **Tools > Configure dashboard > Email alerts**

For information, see [Set up network status email alerts](#) (page 45).

### 15.2 Set up anti-virus and HIPS alerts

Sophos Control Center can display an alert on the desktop or send an email alert if a virus or a potentially unwanted application is found on any of the computers on your network.

To set up scanning alerts:

1. In the left pane, under **Configuration**, click **Configure scanning**.
2. In the **Configure scanning** dialog box, click **Messaging**.
3. In the **Messaging** panel, by default, **Enable desktop messaging** and all the options in the **Messages to send** panel are selected. You can modify these settings, if appropriate.

In the User-defined message text box, you can type a message that will be added to the end of the standard message.

4. In the **Email alerting** tab, select **Enable email alerting** to receive alerts by email.

**Note:** No email alerts are sent for items that are blocked by the firewall.

5. 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.

6. 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.  
**Note:** Mac OS X computers will send messages only to the first recipient in the list.
7. Click **Configure SMTP** to change the settings for the SMTP server and the language of the email alerts.
8. 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 and UNIX 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.

### 15.3 Set up network status email alerts

You can set up email alerts to be sent to your chosen recipients when a threshold value is reached in the Dashboard.

To set up email alerts:

1. On the **Tools** menu, select **Configure email alerts**.  
The **Configure email alerts** dialog box is displayed.
2. If SMTP settings have not been configured, or if you want to view or change the settings, click **Configure**. In the **Configure SMTP settings** dialog box, enter the details as described below:
  - a) In the **Server address** text box, type the host name or IP address of the SMTP server.
  - b) In the **Sender** text box, type an email address to which bounces and non-delivery reports can be sent.
  - c) Click **Test** to test the connection.
3. In the **Recipients** panel, click **Add**.  
The **Add a new email alert recipient** dialog box is displayed.
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 the options that must be sent as an email alert to the recipient when a threshold level is exceeded.

For information on how to modify the threshold values, see [Configure dashboard](#) (page 9).

## 15.4 Set up application control alerts

You can send alerts to particular users when a controlled application is found.

1. In the left pane, under **Configuration**, click **Configure application control**.

The **Configure application control** dialog box is displayed.

2. On the **Messaging** tab, set the options as described below:

- a) In the **Messaging** panel, the **Enable desktop messaging** check box is enabled by default.

When an unauthorized controlled application is detected by on-access scan and blocked, a desktop message will be displayed to the user informing them that the application has been blocked.

- b) In the **Message text** box, type a message that you want to be added to the end of the standard desktop message.

- c) Select the **Enable email alerting** check box to enable Sophos Anti-Virus to send email alerts. For more information on configuring email alerts, see [Set up anti-virus and HIPS alerts](#) (page 44).

## 15.5 Set up device control alerts

You can send alerts to particular users when a device control event is encountered.

1. In the left pane, under **Configuration**, click **Configure device control**.

The **Configure device control** dialog box is displayed.

2. On the **Messaging** tab, set the options as described below:

- a) In the **Messaging** panel, the **Enable desktop messaging** check box is enabled by default.

When an unauthorized device is detected by on-access scan and blocked, a desktop message will be displayed to the user informing them that the device has been blocked.

- b) In the **Message text** box, type a message that you want to be added to the end of the standard desktop message.

- c) Select the **Enable email alerting** check box to enable Sophos Control Center to send email alerts.

In the **Email recipients** box, enter the email addresses to which you want to send the alerts.

## 15.6 Delete old alerts

You can set up Sophos Control Center to delete old alerts automatically. By default, alerts are stored in the database for 12 months and then deleted.

**Note:** Outstanding alerts are never purged.

To delete old alerts:

1. On the **Tools** menu select **Configure Reporting**.

The **Configure Reporting** dialog box is displayed.

2. Click the **Purge** tab.

Depending on your reporting requirements, choose how you want to handle old alerts.

- **Do not purge old alerts.**
- **Purge alerts older than  $n$  months** (where  $n$  is a number you specify).

## 16 Managing reports

### 16.1 Generate a report

You can generate an existing report using the reporting manager.

To generate a report:

1. In the Sophos Control Center window, on the toolbar, click **Reports**.

The **Reporting Manager** dialog box is displayed.

2. Select the type of report that you want to generate.

For information on how to create a new report, see [Create a new report](#) (page 48).

3. Click **Run**.

A report is displayed summarizing the criteria used to create the report.

4. Choose one of the following tabs to view the report in desired format:

**Note:** Based on the report criteria, some of the reports may have only one format to display data.

- **Chart**
- **Table**

### 16.2 Create a new report

You can create a new report using reporting manager.

To create a new report:

1. In the Sophos Control Center window, on the toolbar, click **Reports**.

The **Reporting Manager** dialog box is displayed.

2. Click **Create**.

The **Create a new report** window is displayed.

- **Using wizard:** In the drop-down menu, select the report template you want to use and click **OK**.

The wizard guides you through the process of creating a report based on the template selected.

- **Using Properties window:** Clear the **Use the wizard to create report** check box and click **OK**.

A **Properties** window is displayed with options to create a report.

## 16.3 Set up scheduled reports

Sophos Control Center can send reports with the number and details of threats found during the period you specify.

The recipients will receive an email report with the following information:

- Date of report
- Company name (Click on **Tools > Configure Reporting** to set your company name)
- Number of suspicious files/behavior
- Number of adware/potentially unwanted applications detected
- Number of viruses/spyware detected.
- List of detected threats in chronological order, displaying the name of the threat and the number of infections
- List of blocked applications in chronological order, displaying the name of the application and the number of affected computers. You can include Blocked by firewall, Controlled applications and Device control alerts.

To set up scheduled reports:

1. In the Sophos Control Center window, on the toolbar, click **Reports**.

The **Reporting Manager** dialog box is displayed.

2. Select an existing report and click **Schedule**.

The **Report name properties** dialog box is displayed (where *Report name* is the name of your report).

3. In the **Schedule** tab, set the options as required:

- a) Select **Schedule this report**.

- b) Under the Schedule section, set the **Start at** and **On** fields to the desired time and date at which you want to generate report.

In the **Repeat** drop-down set the frequency at which you want the report to be generated.

- c) In the **Output** section, set the **Format** in which you want to send the email attachment.

- d) Set the **Language** in which you want to receive the report.

- e) Select the email address to which you want to send the email and add them to recipients.

You must configure SMTP server settings to send emails. For information on how to configure settings, see [Set up network status email alerts](#) (page 45).

## 16.4 Modify report

You can modify an existing report and generate data.

To modify an existing report:

1. In the Sophos Control Center window, on the toolbar, click **Reports**.
2. In the **Reporting Manager** dialog box, select the report you want to modify and click **Properties**.

**Note:** Based on the selected criteria, only some or all of the fields may appear in the tabs.

3. In the **Configuration** tab select any of the following options to modify:

- **Report details**

Enter the **Name** to save the report by that name. By default, the **Description** box contains description based on the selections that have been made.

- **Reporting period**

In the **Period** drop-down list, select a defined time period. Select **Custom** to specify a time period using the **Start** and **End** boxes.

- **Report location**

Select **All computers** or **Individual computer** drop-down to specify a computer name.

- **Alert types to include**

Select the alert types you want to include.

You can also configure the report to show only computers that have reported a particular threat. To specify a single threat, click **Advanced**.

In the **Advanced Configuration** window, select which alerts to include in the report. You can enter a name of the threat in the **Expression** text box, or to specify more than one threat, 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. In the **Display Options** tab select any of the following options to modify:
  - By default, the **Display Options** lists all the items selected. However, you can configure the report to show:
    - Only the top  $n$  alerts (where  $n$  is a number you specify).
    - Only alerts with  $n$  or more occurrences.
  - **Display results per**  
By default, results are displayed per **Day**. You can also choose to set it for **Hour**, **Week**, or **Month**.
  - **Display results as**  
By default results are displayed as **Percentages**. You can also choose to display results as **Numbers**.
  - **Sort by**  
By default, the report lists threats in order of decreasing number of alerts per threat. You can also choose to sort them by **Alert name**, **Computer name**, or **Date and time**.
5. In the Schedule tab, select the options to modify schedule:
  - a) Select **Schedule this report**.
  - b) Under the Schedule section, set the **Start at** and **On** fields to the desired time and date at which you want to generate report.  
The **Repeat** drop-down lets you choose the frequency at which you want to repeat the task.
  - c) In the **Output** section, select a **File format** in which you want to send the email attachment.
  - d) Set the **Language** in which you want to receive the report.
  - e) Select the email address to which you want to send the email and add them to recipients.  
For information to configure or add email addresses, see [Set up network status email alerts](#) (page 45).

## 16.5 Export a report to a file

You can export a report in several formats after the report is generated.

To export a report to a file:

1. In the Sophos Control Center window, on the toolbar, click **Reports**.  
The **Reporting Manager** dialog box is displayed.
2. Select a report that you want to export and click **Run**.

3. In the **Reporting** window, on the toolbar, click the **Export** icon.



4. In the **Export report** dialog box, select the type of document or spreadsheet you would like to export the report.
5. Click the **File Name** browse button to select a location.
6. In the **Save As** dialog box, browse to a location where you want to save the report, enter a name for the report, and then click **Save**.
7. In the **Export report** dialog box, click **OK**.

## 16.6 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.

To change the report layout:

1. In the Sophos Control Center window, on the toolbar, click **Reports**.  
The **Reporting Manager** dialog box is displayed.
2. Select a report and click **Run**.
3. In the **Reporting** window, on the toolbar, click the page layout icon.



4. In the **Page Setup** dialog box, specify page size, orientation and margins. Click **OK**. The report is then displayed with these page settings.
5. These page settings are also used when you print or export the report.

---

## 17 Troubleshooting

### 17.1 Cleanup failed

If it is not possible to remove a threat centrally, go to the infected computer and carry out the cleanup manually.

If the threat has not been removed and you require assistance in dealing with it, you should:

1. Make a note of the threat's name.
2. In the left pane, under **Information**, click **View threat information** to connect to the threat analyses page of the Sophos website.
3. On the threat analyses page, search for the threat. Follow the links for advice on cleanup.

If you cannot eliminate the threat yourself, under **Information**, click **Technical support**.

Enter the name of the threat and details of the computer(s) affected and send an email.

### 17.2 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 Anti-Virus detects each file access and sends an alert.

You should do one of the following:

- Disable on-access scanning for potentially unwanted applications. You can use a scheduled scan instead.
- Authorize the application if you want to have it running on your computers. For information, see [Authorize applications for use](#) (page 29).
- Clean up applications that you have not authorized. For information, see [Clean up your computer](#) (page 14).

## 18 Technical Support

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

- Visit the SophosTalk forum 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](mailto:support@sophos.com), including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

## 19 Copyright

Copyright © 2010 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.

The Sophos software that is described 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](mailto: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>

### **ACE™, TAO™, CIAO™, and CoSMIC™**

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

Since DOC software is open-source<sup>10</sup>, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us<sup>11</sup> know so we can promote your project in the DOC software success stories<sup>12</sup>.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies<sup>13</sup> around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

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

The ACE<sup>14</sup>, TAO<sup>15</sup>, CIAO<sup>16</sup>, and CoSMIC<sup>17</sup> web sites are maintained by the DOC Group<sup>18</sup> at the Institute for Software Integrated Systems (ISIS)<sup>19</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>20</sup> for the development of open-source software as part of the open-source software community<sup>21</sup>. 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 me<sup>22</sup> know.

Douglas C. Schmidt<sup>23</sup>

The ACE home page is <http://www.cs.wustl.edu/ACE.html>

## **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. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>

14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>
17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>

## Index

### A

- acknowledge
  - alerts 16
  - errors 16
- alerts
  - anti-virus 44
  - application control 46
  - configure 44
  - dashboard 45
  - delete 47
  - device control 46
  - HIPS 44
  - network status 45
- application control 39
  - alerts 46
  - events 21
- authorize applications 29
- automatic cleanup 27
  - PUAs 28
  - viruses 28

### B

- block
  - controlled applications 39

### C

- central configuration 18
- change
  - proxy 32
  - user ID 32
- check network 18
- cleanup 14
  - failed 53
- complying with configuration 18
- computer status 19
- configure files
  - Mac 26
  - Windows 26
- configure on-access scan 24

- configure scan 31
- configuring Dashboard 9
- controlled applications
  - block 39
  - select applications 40
- create
  - reports 48

### D

- Dashboard
  - configuring 9
  - overview 8
- desktop messaging 44
- device control
  - alerts 46
  - block bridge 41
  - device types 41
  - enable device control 42
  - events 22
  - exempting a device 43
  - network
    - short range 41
  - overview 41
  - storage 41
- disconnected computers 5
- disinfection 14
- display computers 19

### E

- enable on-access scan 24
- Endpoints view 4
- events 21
  - application control 21
  - copying to the Clipboard 23
  - device control 22
  - exporting to a file 23
  - firewall 22
- exclude from scan 27
- export
  - reports 51

### F

- failed cleanup 53

**firewall**

- allowing applications 37
- configure on individual computers 37
- disable at Sophos Control Center 36
- disable on an individual computer 36
- events 22
- setting up 35

**G****generate**

- reports 48

**I****icons** 5**immediate updating** 13**interface**

- Endpoints view 4
- Update managers view 4

**L****last update** 12**layout**

- reports 52

**locally configured** 18**locate deleted computers** 19**M****managed computers** 5**manual updating** 13**modify**

- reports 50

**O****on-access scan options** 25**out-of-date computers**

- updating 13

**P****print summary** 20**priority of alerts** 7**Protect computers wizard** 10**protected computers** 18**protected network** 18**protecting computers**

- Protect computers wizard 10

**protecting operating systems** 11**PUA**

- frequent alerts 53

**R****Reapply central configuration** 18**reports**

- create 48
- export 51
- generate 48
- layout 52
- modify 50
- schedule 49

**reprotecting computers** 17**resolve**

- alerts 16
- errors 16
- threats 14

**S****scan**

- on-access 24, 25
- PUA 24

**scan individual computers** 31**scan options**

- exclude file 26
- include extension 26

**schedule**

- reports 49

**schedule options** 30**schedule scan** 24, 29**schedule scan exclude** 31**Sophos Control Center** 3, 4**Sophos Control Center interface** 4**suspicious files** 28**T****threat information** 15

troubleshooting

- cleanup 53
- frequent alerts 53
- PUA 53

turn off

- automatic updates 33
- firewall
  - individual computer 36
  - Sophos Control Center 36

**U**

uninstall

- controlled applications 40

uninstall controlled applications 40

updating

- automatic 33
- interval 33

updating (*continued*)

- off network 33
- proxy 32
- select applications 32
- user ID 32

updating individual computer 13

updating network 13

updating process 12

**V**

verifying update 12

**W**

warning signs 5

web scanning 27