

SOPHOS

Sophos Control Center 4.1 upgrade guide

Product version: 4.1

Document date: February 2011



Contents

1 About this guide.....	3
2 What's new in Sophos Control Center 4.....	4
3 System requirements.....	5
4 Preparing to upgrade.....	6
5 Upgrading Sophos Control Center.....	8
6 Checking computers are protected.....	9
7 Setting up the firewall.....	10
8 Setting up application control.....	11
9 Setting up device control.....	13
10 Technical Support.....	16
11 Copyright.....	17

1 About this guide

This Sophos Control Center 4.1 upgrade guide describes how to:

- Upgrade from Sophos Control Center versions 2.0 and 2.5 to Sophos Control Center version 4.1.
- Upgrade from Sophos Anti-Virus and Sophos Client Firewall (if your license includes firewall) to Sophos Endpoint Security and Control.

If you use a previous version of Sophos PureMessage and your license includes an upgrade to the latest version of Sophos PureMessage, for instructions on how to upgrade, see *Sophos PureMessage upgrade guide*.

- Set up the new security features.

You can find details of all other configuration options of Sophos Control Center, which are not covered in this guide, in the *Sophos Control Center Help*.

Sophos documentation is published at <http://www.sophos.com/support/docs/>.

2 What's new in Sophos Control Center 4

The new version of Sophos Control Center has the following salient features:

Sophos Control Center 4.1

Operating system compatibility

Sophos Control Center version 4.1 is compatible with the following operating systems only:

- Windows Server 2008 R2,
- Windows 7.

Note: Sophos Control Center version 4.0 is compatible with older Windows operating systems. For full system requirements, see the following section, [System requirements](#) (page 5).

Sophos Control Center 4.0

Support for latest endpoint security software

The new version of Sophos Control Center lets you use Sophos Endpoint Security and Control for endpoint computers which provides latest version of anti-virus and firewall software for Windows 2000 and later.

Dashboard

Sophos Control Center interface now provides a dashboard that lets you get an at-a-glance view of the network's security status. You can configure the threshold values for the dashboard to warn and send alert messages when a threshold value is reached. For information on how to configure dashboard, see Sophos Control Center Help.

Application control

Sophos Control Center lets you detect and block applications that you decide are unsuitable for use in your office environment. For more information on application control, see [Setting up application control](#) (page 11).

Device control

Device control lets you prevent users from using unauthorized external hardware devices, removable storage media, and wireless connection technologies on their computers. For more information on device control, see [Setting up device control](#) (page 13).

Launching Sophos PureMessage and Sophos for Microsoft SharePoint

If Sophos PureMessage or Sophos for Microsoft SharePoint console is installed on the same computer as Sophos Control Center, you can launch them from Sophos Control Center console.

3 System requirements

For system requirements, see the system requirements page of the Sophos website <http://www.sophos.com/products/all-sysreqs.html>.

In addition, you must have internet access to download the software from the Sophos website.

Sophos Control Center and server components have the following other requirements:

- You must have access to and from the other computers on the network.
- It is recommended that a server operating system is used (such as, Windows Server 2003 or Windows Small Business Server 2011). Otherwise, the performance of Sophos Control Center is impacted.

4 Preparing to upgrade

Note:

- It is recommended that you back up your existing version of Sophos Control Center prior to upgrading it.
- After completing the Sophos Control Center Installation Wizard, you will need to either log off from the computer where you upgraded Sophos Control Center and then log on again, or restart the computer.
- If you choose to install Sophos Client Firewall (if it is included in your license), you must restart each computer where you have installed firewall software to activate it.

The firewall alerts generated in the previous version of Sophos Control Center will not be available after you upgrade to Sophos Control Center 4.0. Sophos recommends that you resolve all the firewall alerts before upgrading.

4.1 Prerequisites

Before you upgrade Sophos Control Center, and subsequently upgrade the software on your networked computers managed by it, you must meet the following prerequisites:

- You have met all the hardware and software requirements listed in [System requirements](#) (page 5).
- You are an administrator on the computer where you are upgrading Sophos Control Center.

Preparing endpoint computers that have Windows operating system

For endpoint computers with Windows operating system, you must do the following:

- Disable Simple File Sharing on all Windows XP computers.
To find out how to do this, see <http://www.sophos.com/support/knowledgebase/article/12837.html>.
- Remove any other vendor's firewall software, except Windows Firewall, from all Windows 2000 and later computers on which you want to install Sophos Client Firewall.

Preparing endpoint computers on which you **DO NOT** want to install Sophos Client Firewall

If you have Windows XP Service Pack 2 workstations on which you **do not** want to install Sophos Client Firewall and these computers have Windows Firewall turned on, you must do the following:

- Enable File and Printer Sharing for Microsoft Networks.
To find out how to do this, see <http://www.sophos.com/support/knowledgebase/article/11738.html>.
- Make sure TCP ports 8192 , 8193 and 8194 are open.

- Add the following program exception: C:\Program Files\Sophos\Remote Management System\RouterNT.exe

To find out how to do this, see <http://www.sophos.com/support/knowledgebase/article/11075.html>.

- Restart the computers for the changes to take effect.

5 Upgrading Sophos Control Center

To upgrade Sophos Control Center retaining your settings, log on as an administrator or domain administrator, as appropriate, at the computer where the previous version of Sophos Control Center is installed and do the following:

1. Close all open Sophos applications, if any.
2. Visit the Sophos product download page at <http://www.sophos.com/support/updates/> and type the username and password supplied to you by Sophos.

Follow the links to download your Sophos Control Center Installer, then run it.

3. On the extractor (**Sophos Small Business Edition installer**) confirm the path for extraction of installation files (this must be on the same computer where you are installing Sophos Control Center) then click **Install**.
4. On the **Welcome** page, click **Next**.

The Installation Wizard guides you through installation. Accept the default options.

5. When upgrade is complete, click **Finish** to log off automatically. If you want to log off later, clear the **Log off now** check box before you click **Finish**.

Sometimes, it is necessary to restart Windows instead of simply logging off. In this case, the check box is not displayed, and a subsequent message asks you if you want to restart Windows now or later.

6. When you log on again, log on as the same user.

After the installation of Sophos Control Center is complete, the endpoint computers will automatically update once the download of the new endpoint software version is complete.

Note: On endpoint computers with Windows 98 and Mac OS X you will have to upgrade Sophos Anti-Virus manually. For information on protecting computers manually, see the *Sophos Control Center startup guide*.

6 Checking computers are protected

You can check that your networked computers are protected against threats by using the Dashboard.

Dashboard provides an at-a-glance view of the network's security status. You can configure the threshold values for the dashboard to warn and send alert messages when a threshold value is reached.

To show or hide the dashboard, click the **Dashboard** button on the toolbar.

For information on how to configure dashboard and a complete list of icons that are displayed and their status, see Sophos Control Center Help.

7 Setting up the firewall

When you first install Sophos Client Firewall it is configured to allow all traffic. You can configure it to allow or block only required traffic.

If you are setting up the firewall for the first time, for information on how to configure the firewall, see *Sophos Control Center Help*.

Note: Sophos Client Firewall does not support IPv6. Version 1 lets IPv6 packets through; versions 1.5 and 2.0 either block all or allow all IPv6 packets depending on configuration.

8 Setting up 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>).

For information on application control events, see Sophos Control Center Help.

8.1 Set up application 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 applications to control](#) (page 11).

8.2 Select 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.



For information on how to uninstall controlled applications, see Sophos Control Center Help.

9 Setting up 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.

For information on device control events, see Sophos Control Center Help.

9.1 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).

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.

9.2 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.”

For information on how to set up device control alerts, see the Sophos Control Center Help.

9.3 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.
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.

10 Technical Support

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

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

11 Copyright

Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

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

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 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™

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

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

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

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

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

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

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

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

Douglas C. Schmidt²²

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>

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