

SOPHOS

Sophos Control Center 4.1 Guía de actualización

Versión: 4.1

Edición: febrero de 2011



Contenido

- 1 Acerca de esta guía.....3
- 2 Novedades en Sophos Control Center 4.....4
- 3 Requisitos del sistema.....5
- 4 Preparar la actualización.....6
- 5 Actualizar Sophos Control Center.....8
- 6 Comprobar que los ordenadores están protegidos.....9
- 7 Configurar el cortafuegos.....10
- 8 Configurar la restricción de aplicaciones.....11
- 9 Configurar el control de dispositivos.....13
- 10 Soporte técnico.....16
- 11 Copyright.....17

1 Acerca de esta guía

Esta guía de actualización de Sophos Control Center 4.1 describe cómo:

- Actualizar Sophos Control Center versiones 2.0 y 2.5 a Sophos Control Center versión 4.1.
- Actualizar Sophos Anti-Virus y Sophos Client Firewall (si su licencia incluye el cortafuegos) a Sophos Endpoint Security and Control.

Si dispone de una versión anterior de Sophos PureMessage y su licencia incluye actualización a la última versión de Sophos PureMessage, vea la *Guía de actualización de Sophos PureMessage*.

- Configurar las nuevas funciones de seguridad.

Hallará información sobre el resto de opciones de configuración de Sophos Control Center, que no se incluyen en esta guía, en la *Ayuda de Sophos Control Center*.

La documentación de Sophos está disponible en <http://esp.sophos.com/support/docs/>.

2 Novedades en Sophos Control Center 4

La nueva versión de Sophos Control Center incluye las siguientes funciones:

Sophos Control Center 4.1

Sistemas operativos compatibles

Sophos Control Center versión 4.1 sólo es compatible con los siguientes sistemas operativos:

- Windows Server 2008 R2,
- Windows 7.

Nota: Sophos Control Center versión 4.0 es compatible con sistemas operativos Windows más antiguos. Para más información sobre los requisitos del sistema, consulte [Requisitos del sistema](#) en la página 5.

Sophos Control Center 4.0

Compatibilidad con la protección más reciente en las estaciones

La nueva versión de Sophos Control Center permite utilizar Sophos Endpoint Security and Control en las estaciones para disponer de la protección más completa en estaciones con Windows 2000 y posterior.

Panel de control

Sophos Control Center dispone de un panel de control con información detallada sobre el estado de la protección en la red. Puede configurar los umbrales de aviso y alertas para los diferentes parámetros de seguridad. Para más información sobre cómo configurar el panel de control, vea la Ayuda de Sophos Control Center.

Restricción de aplicaciones

Sophos Control Center permite detectar y bloquear aplicaciones que no desea permitir en su red. Para más información sobre cómo restringir aplicaciones, consulte [Configurar la restricción de aplicaciones](#) en la página 11.

Control de dispositivos

El sistema de control de dispositivos permite evitar el uso de dispositivos no autorizados, como memoria externa o dispositivos inalámbricos. Para más información sobre el control de dispositivos, consulte [Configurar el control de dispositivos](#) en la página 13.

Integración con Sophos PureMessage y Sophos para Microsoft SharePoint

Si dispone de Sophos PureMessage o Sophos para Microsoft SharePoint en el mismo ordenador que Sophos Control Center, podrá acceder a los mismos desde la consola de Sophos Control Center.

3 Requisitos del sistema

Consulte la página de requisitos del sistema en la web de Sophos
<http://esp.sophos.com/products/all-sysreqs.html>.

Además, debe disponer de acceso a Internet para descargar el software desde la web de Sophos.

Sophos Control Center y los componentes del servidor tienen los siguientes requisitos:

- Acceso a todos los ordenadores de la red en ambas direcciones.
- Se recomienda el uso de un sistema operativo de servidor (por ejemplo, Windows Server 2003 o Windows Small Business Server 2011). De lo contrario el rendimiento de Sophos Control Center podría verse afectado.

4 Preparar la actualización

Nota:

- Se recomienda realizar copias de seguridad de su versión de Sophos Control Center antes de la actualización.
- Tenga en cuenta que tras completar la actualización deberá reiniciar la sesión.
- Si desea instalar Sophos Client Firewall (siempre que su licencia lo incluya), deberá reiniciar cada estación afectada para que se active el cortafuegos.

Las alertas del cortafuegos en la versión anterior de Sophos Control Center no estarán disponibles al actualizarse a Sophos Control Center versión 4.0. Sophos recomienda resolver las alertas pendientes del cortafuegos antes de realizar la actualización.

4.1 Requisitos previos

Antes de comenzar con la actualización de Sophos Control Center, que se completará con la actualización de la protección en la red, asegúrese de que cumple los siguientes requisitos:

- Su sistema reúne los requisitos mínimos de hardware y software que se enumeran en [Requisitos del sistema](#) en la página 5.
- Dispone de derechos de administrador en el ordenador en el que va a actualizar Sophos Control Center.

Preparar estaciones Windows

Para estaciones Windows:

- Desactive el uso compartido simple de archivos en ordenadores con Windows XP.
Para saber cómo hacerlo, consulte <http://esp.sophos.com/support/knowledgebase/article/12837.html>.
- Elimine el cortafuegos de otros proveedores, excepto el Firewall de Windows, de todos los equipos con Windows 2000 y posterior en los que desea instalar Sophos Client Firewall.

Preparar estaciones en las que **NO** desea instalar Sophos Client Firewall

Si dispone de estaciones con Windows XP Service Pack 2 en las que **no** desea instalar Sophos Client Firewall, y que tienen activado el Firewall de Windows:

- Active Compartir archivos e impresoras para redes Microsoft.
Para saber cómo hacerlo, consulte <http://esp.sophos.com/support/knowledgebase/article/11738.html>.
- Asegúrese de que los puertos TCP 8192, 8193 y 8194 estén abiertos
- Añada la siguiente excepción: C:\Archivos de programa\Sophos\Remote Management System\RouterNT.exe
Para saber cómo hacerlo, consulte <http://esp.sophos.com/support/knowledgebase/article/11075.html>.

- Reinicie los equipos para aplicar los cambios.

5 Actualizar Sophos Control Center

Para actualizar Sophos Control Center y mantener la configuración existente, inicie la sesión como administrador o administrador del dominio, según sea necesario, en el ordenador donde tiene instalado Sophos Control Center y haga lo siguiente:

1. Cierre las aplicaciones de Sophos que puedan estar abiertas.
2. Visite la página de descargas en la web de Sophos <http://esp.sophos.com/support/updates/> e introduzca las credenciales suministradas por Sophos.

Descargue el programa de instalación correspondiente de Sophos Control Center y ejecútelos.

3. Para la extracción (**Programa de instalación de Sophos Small Business Edition**) confirme la ruta (debe encontrarse en el mismo ordenador en el que está instalando Sophos Control Center) y haga clic en **Instalar**.
4. En la página de **bienvenida**, haga clic en **Siguiente**.

El asistente de instalación le guiará en el proceso de instalación. Acepte los valores predeterminados.

5. Cuando se complete la actualización, haga clic en **Finalizar** para cerrar la sesión. Si no desea cerrar la sesión en ese momento, desactive la opción **Cerrar sesión** y haga clic en **Finalizar**.

En ciertos casos será necesario reiniciar el sistema. Un mensaje le informará de esta situación y le dará a elegir la acción a realizar.

6. Al reiniciar la sesión, utilice el mismo usuario.

Tras la instalación de Sophos Control Center, las estaciones se actualizarán de forma automática con la nueva protección descargada desde Sophos.

Nota: en estaciones con Windows 98 o Mac OS X tendrá que actualizar Sophos Anti-Virus de forma manual. Para más información sobre cómo proteger ordenadores de forma manual, consulte la *Guía de inicio* de *Sophos Control Center*.

6 Comprobar que los ordenadores están protegidos

Podrá comprobar en todo momento que los ordenadores de la red se encuentran protegidos y actualizados.

El panel de control ofrece una visión general del estado de seguridad de la red. Puede configurar los umbrales de aviso y alertas para los diferentes parámetros de seguridad.

Para mostrar u ocultar el panel de control, haga clic en el botón **Panel de control**.

Para más información sobre la configuración del panel de control y de los iconos utilizados, vea la ayuda de Sophos Control Center.

7 Configurar el cortafuegos

La instalación inicial de Sophos Client Firewall permite todo el tráfico de red. Debe configurar el cortafuegos para permitir/bloquear el tráfico necesario.

Para más información sobre la configuración inicial del cortafuegos, vea la *Ayuda de Sophos Control Center* .

Nota: Sophos Client Firewall no es compatible con IPv6. La versión 1 admite los paquetes de IPv6, pero las versiones 1.5 y 2.0 pueden permitirlos o bloquearlos, según la configuración.

8 Configurar la restricción de aplicaciones

Sophos Control Center permite detectar y bloquear "aplicaciones restringidas", es decir, aplicaciones legítimas que no suponen una amenaza para la seguridad, pero cuyo uso no considere adecuado en el entorno empresarial. Entre estas aplicaciones se incluyen programas de mensajería instantánea, de voz sobre IP (VoIP), de fotografía digital, reproductores multimedia o complementos del navegador.

Nota: Esta opción sólo está disponible en Sophos Endpoint Security and Control para Windows 2000 y posterior.

Sophos proporciona la lista actualizada de aplicaciones restringidas de forma regular. No es posible añadir aplicaciones a la lista, pero puede enviar una solicitud a Sophos para que incluya una aplicación legítima nueva que desee restringir en su red. Para más información, consulte el artículo 35330 de la base de conocimiento (<http://esp.sophos.com/support/knowledgebase/article/35330.html>).

Para más información sobre los eventos de la restricción de aplicaciones, vea la Ayuda de Sophos Control Center.

8.1 Configurar la restricción de aplicaciones

Puede configurar Sophos Control Center para detectar aplicaciones cuyo uso desea restringir en su red.

1. En el panel de la izquierda, en **Configuración**, haga clic en **Configurar la restricción de aplicaciones**.
Se mostrará el cuadro de diálogo **Configurar la restricción de aplicaciones**.
2. En la ficha **Escaneado**, configure las opciones de la forma siguiente:
 - Para activar el escaneado en acceso, active la casilla **Activar el escaneado en acceso**. Si no desea bloquear las aplicaciones detectadas, active la opción **Detectar pero permitir ejecución**.
 - Para activar los escaneados en demanda y programado, active la casilla **Activar el escaneado en demanda y programado**.

Nota: la política antivirus y HIPS determina los archivos a escanear (extensiones y exclusiones).

3. Abra la ficha **Autorización** y seleccione las aplicaciones que desea restringir.

Para más información sobre cómo añadir aplicaciones, vea [Seleccionar las aplicaciones que desea restringir](#) en la página 12.

8.2 Seleccionar las aplicaciones que desea restringir

Por defecto, todas las aplicaciones están permitidas. Para seleccionar las aplicaciones que desea restringir:

1. En el panel de la izquierda, en **Configuración**, haga clic en **Configurar la restricción de aplicaciones**.
2. En el cuadro de diálogo **Configurar la restricción de aplicaciones**, abra la ficha **Autorización**.
3. Seleccione el **Tipo de aplicación**, por ejemplo, **Intercambio de archivos**.

La lista **Autorizadas** contiene todas las aplicaciones incluidas en ese grupo.

- Para bloquear una aplicación, selecciónela y muévela a la lista **Bloqueadas** haciendo clic en el botón "Añadir".



- Para bloquear todas las aplicaciones nuevas que Sophos añade a ese tipo en lo sucesivo, mueva **Todas las añadidas por Sophos en el futuro** a la lista **Bloqueadas**.

- Para bloquear todas las aplicaciones de ese tipo, muévalas todas desde la lista **Autorizadas** a la lista **Bloqueadas** haciendo clic en el botón "Añadir todas".



Para más información sobre cómo desinstalar aplicaciones restringidas, vea la Ayuda de Sophos Control Center.

9 Configurar el control de dispositivos

Importante: No debe utilizar el control de dispositivos de Sophos junto con otros programas de terceros para el mismo propósito.

El control de dispositivos permite impedir el uso de dispositivos de hardware externos no autorizados, medios de almacenamiento extraíbles y tecnologías de conexión inalámbrica en los equipos. Esto puede reducir de forma significativa el riesgo de pérdida accidental de datos y la entrada de programas externos.

Los dispositivos de almacenamiento extraíbles, unidades ópticas y disquetes también se pueden configurar para que tenga acceso de sólo lectura.

Por defecto, el control de dispositivos está desactivado y se permite el uso de todos los dispositivos.

Si desea activar el control de dispositivos por primera vez, Sophos recomienda:

- Seleccionar los tipos de dispositivo que desea controlar.
- Detectar los dispositivos pero sin bloquearlos.
- Configurar alertas del control de dispositivos.
- Detectar y bloquear, o permitir sólo la lectura de dispositivos de almacenamiento.

Para más información sobre los eventos del control de dispositivos, vea la Ayuda de Sophos Control Center.

9.1 Dispositivos que se pueden controlar

El sistema de control de dispositivos permite bloquear tres tipos de dispositivos: *almacenamiento, red y corto alcance*.

Almacenamiento

- Dispositivos extraíbles de almacenamiento (como memoria USB, dispositivos PC Card o discos duros externos)
- Unidades ópticas (unidades de CD-ROM, DVD o Blu-ray)
- Disqueteras
- Dispositivos seguros de almacenamiento extraíbles (por ejemplo, unidades de memoria USB con cifrado por hardware SanDisk Cruzer Enterprise, SanDisk Cruzer Enterprise FIPS Edition, Kingston Data Traveler Vault - Privacy Edition, Kingston Data Traveler BlackBox y IronKey Enterprise Basic Edition)

Mediante la categoría de dispositivos seguros de almacenamiento extraíbles, puede permitir el uso de dispositivos compatibles, a la vez que bloquea otros dispositivos de almacenamiento extraíbles. Para ver una lista actualizada de los dispositivos seguros de almacenamiento extraíbles, visite el sitio web de Sophos (esp.sophos.com).

Red

- Módems

- Inalámbricos (Wi-Fi, 802.11 estándar)

Para las interfaces de red, puede configurar un nivel de acceso adicional con el modo Bloquear puente. Permite la activación de los dispositivos de red (como adaptadores Wi-Fi), cuando el equipo está físicamente desconectado de la red. Seleccione la opción Bloquear puente al configurar los niveles de acceso para los dispositivos de red.

Nota: De esta forma evitará posibles interacciones entre redes (por ejemplo, entre la red empresarial y otras externas). El modo Bloquear puente está disponible tanto para módems como dispositivos inalámbricos. Este modo funciona desactivando el adaptador de red inalámbrico o módem cuando una estación está conectada a una red física (normalmente, mediante una conexión Ethernet). Cuando el ordenador se desconecta de la red de la empresa, podrá volver a utilizar los dispositivos inalámbricos o módem.

Corto alcance

- Bluetooth
- Infrarrojos (IrDA)

El control se extiende tanto a dispositivos internos como externos. Por ejemplo, al bloquear interfaces de Bluetooth, se bloquearán:

- El dispositivo Bluetooth integrado en el ordenador
- Cualquier dispositivo Bluetooth USB que se conecte.

9.2 Configurar el control de dispositivos

Puede configurar Sophos Control Center para detectar dispositivos cuyo uso desea controlar en su red.

1. En el panel de la izquierda, en **Configuración**, haga clic en **Configurar el control de dispositivos**.

Aparecerá el cuadro de diálogo **Política de control de dispositivos**.

2. En la ficha **Configuración**:

- Seleccione la opción **Activar el control de dispositivos**. Si no desea bloquear los dispositivos detectados, active la opción **Detectar pero no bloquear**.
- Para establecer el nivel de acceso a un dispositivo, haga clic en la columna **Estado** para desplegar la lista de selección. Seleccione el tipo de acceso que desea permitir.

Por defecto, los dispositivos tienen acceso total. Para los dispositivos de almacenamiento extraíbles, unidades ópticas y disquetes, puede cambiarlo por "Bloqueado" o "Sólo lectura". Para los dispositivos seguros de almacenamiento extraíbles, puede cambiarlo por "Bloqueado".

Para más información sobre cómo configurar las alertas del control de dispositivos, vea la Ayuda de Sophos Control Center.

9.3 Excluir un dispositivo

Es posible excluir dispositivos de las políticas de control de dispositivos.

Puede excluir un dispositivo determinado ("sólo este dispositivo") o un modelo de dispositivos ("todos los dispositivos de este modelo"). No configure ambos tipos de excepciones. Si se definen ambas, la excepción del dispositivo determinado tendrá preferencia.

Para excluir un dispositivo:

1. En el menú **Ver**, haga clic en **Eventos del control de dispositivos**.
Aparece el cuadro de diálogo **Visualizador de eventos del control de dispositivos**.
2. Si sólo desea mostrar ciertos eventos, en el panel **Criterio de búsqueda**, configure los filtros que necesite y haga clic en **Buscar** para mostrar los eventos.
3. Seleccione la entrada del dispositivo que desea excluir y haga clic en **Excepciones**.
Aparece el cuadro de diálogo **Excepción de dispositivos**. En **Detalles del dispositivo**, aparece el tipo, el modelo y el ID del dispositivo.

10 Soporte técnico

Para obtener asistencia técnica sobre cualquier producto de Sophos, puede:

- Visitar el fórum SophosTalk en <http://community.sophos.com/> para consultar casos similares.
- Visitar la base de conocimiento de Sophos en <http://esp.sophos.com/support/>
- Descargar la documentación correspondiente desde <http://esp.sophos.com/support/docs/>
- Enviar un email a support@sophos.com indicando la versión del producto de Sophos, el sistema operativo y parches aplicados, y el texto exacto de cualquier mensaje de error.

11 Copyright

Copyright © 2011 Sophos Limited. Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, mecánico, grabación, fotocopia o cualquier otro sin la correspondiente licencia del producto, bajo dichos términos, o sin la previa autorización escrita por parte del propietario.

Sophos y Sophos Anti-Virus son marcas registradas de Sophos Limited. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

El software de Sophos descrito en este documento incluye o puede incluir software con licencia (o sublicencia) de público común (CPL) que, entre otros derechos, permiten al usuario tener acceso al código fuente. Las licencias de dichos programas, que se distribuyen al usuario en formato de código de objeto, exigen que el código fuente esté disponible. Para cualquiera de tales programas que se distribuya junto con el producto de Sophos, el código fuente se ofrece a petición por correo; envíe su solicitud a Sophos por email a support@sophos.com o por Internet desde <http://esp.sophos.com/support/queries/enterprise.html>. Para ver los términos de la licencia CPL, visite <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/>