

SOPHOS

Sophos Control Center Guía de inicio

Versión: 4.1

Edición: febrero de 2011



Contenido

- 1 Acerca de esta guía.....3
- 2 Requisitos del sistema.....4
- 3 Instalación.....5
- 4 Proteger ordenadores en red.....8
- 5 Comprobar que los ordenadores están protegidos.....11
- 6 Configurar las alertas por email.....12
- 7 Detectar aplicaciones no deseadas.....13
- 8 Desinfectar virus.....15
- 9 Configurar el cortafuegos.....16
- 10 Soporte técnico.....18
- 11 Copyright.....19

1 Acerca de esta guía

En esta guía encontrará la información necesaria para proteger su red (con estaciones Windows y Mac) contra virus (incluyendo programas espía) y aplicaciones no deseadas.

Si dispone de ordenadores que no se conectan a la red, consulte también la *Guía de inicio de usuario independiente de Sophos Endpoint Security and Control*.

Si está actualizando una versión anterior de Sophos Control Center, consulte la *Guía de actualización de Sophos Control Center*.

Para más información sobre todas las opciones de configuración de Sophos Control Center que no se tratan en esta guía, consulte la Ayuda de Sophos Control Center.

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

2 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.

Importante: si va a instalar Sophos Control Center en Windows 2008 Small Business Server (SBS), asegúrese de que Windows Live OneCare no se encuentra instalado. Si necesita desinstalar Windows Live OneCare, hágalo desde el Panel de control.

Si desea utilizar SQL Server 2008 (en lugar de SQL Server 2005 Express, incluido en los productos de Sophos), asegúrese de que está instalado y cree una instancia "SOPHOS". Para más información, consulte la documentación de SQL o póngase en contacto con soporte técnico de Microsoft.

3 Instalación

3.1 Preparar la instalación de Sophos Control Center

Antes de instalar Sophos Control Center, asegúrese de que:

- Tiene a mano las credenciales proporcionadas por Sophos.
- Inicia sesión como administrador o administrador del dominio, según sea necesario, en el equipo en el que desea instalar Sophos Control Center.

Nota: para proteger equipos que pertenezcan a un grupo de trabajo, en todas las plataformas Windows, es necesario realizar los pasos adicionales que se describen en el artículo:

<http://esp.sophos.com/support/knowledgebase/article/29728.html>.

3.2 Preparar las estaciones

Antes de instalar el software de seguridad en las estaciones, compruebe que:

- Se ha eliminado el software antivirus de otros proveedores en las estaciones en las que desea instalar Sophos Anti-Virus.
- El sistema operativo está configurado correctamente.

3.2.1 Windows Vista y posterior

Los siguientes requisitos adicionales son necesarios para Sophos Anti-Virus en equipos con Windows Vista y posterior:

- Compruebe que el servicio **Registro remoto** está activado y que el tipo de inicio es **Automático**. Este servicio no está activado por defecto en Windows Vista. Para configurarlo, haga clic en **Inicio|Panel de control|Herramientas administrativas|Servicios**. Haga doble clic en el servicio **Registro remoto** que aparece en la lista. En el cuadro de diálogo de **Propiedades del registro remoto**, en la ficha **General**, en el campo **Tipo de inicio**, abra la lista desplegable y seleccione **Automático**. Haga clic en **Aplicar**. Haga clic en **Iniciar** y haga clic en **Aceptar**.
- Desactive el **Control de cuentas de usuario**. Para acceder a él, vaya a **Inicio|Panel de control|Cuentas de usuario** y active o desactive el **Control de cuentas de usuario**. Debería volver a activarlo cuando termine la instalación.
- Abra **Firewall de Windows con seguridad avanzada**: Para configurarlo, haga clic en **Inicio|Panel de control|Herramientas administrativas**. Cambie las **Reglas de entrada** para activar lo siguiente:

Regla	Perfil
Administración remota (NP-In)	Dominio
Administración remota (NP-In)	Privado

Regla	Perfil
Administración remota (RPC)	Dominio
Administración remota (RPC)	Privado
Administración remota (RPC-EPMAP)	Dominio
Administración remota (RPC-EPMAP)	Privado

Nota: es aconsejable desactivar de nuevo estos procesos una vez que haya terminado la instalación.

3.2.2 Windows XP

Realice los pasos siguientes en todos los equipos con Windows XP, con o sin service packs:

- Elimine el cortafuegos de otros proveedores, excepto el cortafuegos de Windows, de todos los equipos con Windows XP en los que desea instalar Sophos Client Firewall.
- Desactive el uso compartido simple de archivos.

Para saber cómo hacerlo, consulte

<http://esp.sophos.com/support/knowledgebase/article/12837.html>.

Windows XP Service Pack 2

En los equipos con Windows XP Service Pack 2, si el Firewall de Windows está activado y **no** tiene intención de instalar Sophos Client Firewall:

- Active Compartir archivos e impresoras para redes Microsoft.
- 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>.

3.2.3 Windows Server 2003 con Service Pack 1

Si tiene activado el Firewall de Windows, deberá hacer lo siguiente:

- Active Compartir archivos e impresoras para redes Microsoft.
- 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>.

3.2.4 Windows 2000

- Elimine el cortafuegos de otros proveedores, excepto el cortafuegos de Windows, de todos los equipos con Windows 2000/XP en los que desea instalar Sophos Client Firewall.

3.2.5 Windows 98 SE

- Desinstale cualquier versión anterior de Sophos Anti-Virus. Utilice Agregar o quitar programas del Panel de control de Windows.

3.3 Instalar Sophos Control Center

Desde Sophos Control Center podrá descargar, distribuir y administrar la protección antivirus para el resto de la red.

1. 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 de soluciones de Sophos para PYMES y ejecútelo.

2. 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**.
3. En la página de **bienvenida**, haga clic en **Siguiente**.

Un asistente le guiará durante la instalación. Acepte las opciones predeterminadas, excepto las siguientes.

4. En la página **Tipo de instalación**, seleccione **Completa** para instalar todas las funciones del programa.

Nota: si desea administrar el software de seguridad desde otro equipo, puede copiar el programa de instalación a dicho equipo, ejecutarlo y seleccionar **Sólo consola de administración**.

Haga clic en **Siguiente** y siga el asistente con las opciones predeterminadas.

5. Cuando se complete la instalación, 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. El Asistente de Sophos para proteger su red se iniciará de forma automática.

Para más información sobre la protección de estaciones en red, consulte [Proteger ordenadores en red](#) en la página 8.

4 Proteger ordenadores en red

Al iniciar sesión por primera vez después de realizar la instalación, Sophos Control Center se abre de forma automática y se inicia el asistente para la protección de la red de Sophos. Este asistente permite proteger ordenadores en red.

1. En la página de **bienvenida**, haga clic en **Siguiente**.
2. En la página **Datos de cuenta de descarga desde Sophos**, introduzca el Nombre de usuario y la Contraseña proporcionados por Sophos y haga clic en **Siguiente**.

Sophos Control Center descargará el software a una unidad compartida en el mismo ordenador, desde donde se distribuirá al resto de estaciones. La carpeta utilizada depende del sistema operativo:

- Windows 2000, XP y 2003:
C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager\Update Manager\CIDs\
- Windows Vista y posterior:
C:\ProgramData\Sophos\Update Manager\Update Manager\CIDs\

Si utiliza un servidor proxy para conectarse a Internet, seleccione **Acceder a través de un proxy** e introduzca los datos del proxy.

3. En el cuadro de diálogo **Selección de plataformas**, seleccione el software correspondiente para los sistemas operativos en sus ordenadores.
 - La opción **Windows 2000 y posterior** está seleccionada por defecto.
 - Si dispone de estaciones con Mac OS X, seleccione la opción Mac OS X. Esto le permitirá instalar más tarde el software antivirus en los equipos.
4. Comenzará la descarga y preparación del software (una barra de evolución indicará el progreso). Sophos Control Center completará la descarga del software. A continuación, haga clic en **Siguiente**.
5. En la página **Datos de cuenta de Windows**, especifique una cuenta con derechos de administrador en las estaciones de la red y que será utilizada para instalar el software. Ésta no es la misma cuenta de Sophos utilizada anteriormente. Es probable que pueda utilizar la misma cuenta que utilizó para la instalación inicial de la consola.
6. En la página **Proteger ordenadores**, el asistente busca los ordenadores en los que el software se puede instalar de forma automática.

Sólo se mostrarán ordenadores con Windows 2000 y posterior ya que no es posible la instalación automática en Windows 98 ni Macs.

Todos los ordenadores están seleccionados por defecto para protegerse. Desactive la casilla de los equipos que no desee proteger. Para seleccionar o deseleccionar todos, utilice la casilla de activación en el encabezado de la columna **Proteger**.

7. En el cuadro de diálogo **Seleccionar funciones**, seleccione las funciones que desea instalar:

- Protección antivirus (seleccionada por defecto).
- Protección de Sophos Client Firewall (si está incluido en la licencia).

Nota: para activar el cortafuegos, reinicie los equipos en los que lo haya instalado.

- Herramienta de eliminación de software de la competencia.

Haga clic en **Siguiente**.

8. En la página **Ordenadores que requieren protección manual**, haga clic en **Imprimir** si desea disponer de una copia impresa, haga clic en **Guardar como** si desea guardar la lista en un archivo, o simplemente anote el nombre de los ordenadores. Haga clic en **Siguiente** y siga el asistente.

Sophos Control Center instala el software de forma automática en los equipos seleccionados.

A medida que se aplica la protección antivirus y del cortafuegos a cada equipo, aparece un icono de un ordenador azul junto al nombre del equipo y se puede leer **Sí** en la columna **Actualizado**.

Para más información sobre cómo proteger ordenadores de forma manual, consulte [Proteger ordenadores en red de forma manual](#) en la página 9.

4.1 Proteger ordenadores en red de forma manual

Si lo desea, puede proteger los ordenadores de forma manual.

1. Vaya a cada ordenador de la lista. Vaya a la carpeta en la que Sophos Control Center coloca el software y las actualizaciones del antivirus y el cortafuegos. Por defecto, las carpetas son:

Operating System	Carpeta
Windows 2000 y posterior	\\[servidor]\sophosUpdate\CIDs\Sxxx\EECSXP
Windows 98	\\[servidor]\sophosUpdate\CIDs\Sxxx\ES9X
Mac OS X	smb://[servidor]/sophosUpdate/CIDs/Sxxx/ESCOSX

Donde:

[servidor] es el nombre del equipo en el que instaló Sophos Control Center.

[Sxxx] es el número generado en la descarga, por ejemplo, S000.

2. En el directorio adecuado, haga doble clic en setup.exe (en Windows) o Sophos Anti-Virus.mpkg (en Mac OS X).

Si realiza la instalación en un ordenador con Mac OS X 10.3 o posterior, copie Sophos Anti-Virus.mpkg en el Mac y realice allí la instalación.

También puede proteger equipos que no estén siempre en la red ([Proteger ordenadores sin conexión permanente a la red](#) en la página 10).

4.2 Proteger ordenadores sin conexión permanente a la red

Los ordenadores que no siempre están conectados a la red (como portátiles que se utilizan tanto dentro como fuera de la empresa) estarán protegidos en todo momento.

Todos los ordenadores en los que ha instalado el software antivirus ya están configurados para actualizarse directamente desde Sophos por Internet cuando no estén dentro de la red de la empresa.

Los ordenadores que no siempre están conectados a la red y en los que todavía no ha instalado la protección antivirus deberían configurarse cuando se conectan a la red. Para más información, consulte la Ayuda de Sophos Control Center en la sección sobre la protección de nuevos ordenadores.

5 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.

6 Configurar las alertas por email

Las alertas de escritorio sólo se muestran en el ordenador en el que se detecta una amenaza. Puede configurar Sophos Control Center para enviar alertas por email cuando se detecte alguna amenaza.

Para configurar las alertas por email:

1. En el panel de la izquierda, en **Configuración**, haga clic en **Configurar escaneado**.
2. En el cuadro de diálogo **Configurar escaneado**, haga clic en **Notificación**.

Se abrirá el cuadro de diálogo **Notificación**.

3. En la ficha **Alerta por email**, seleccione **Activar alerta por email** para recibir alertas por email.
4. En el panel **Notificar**, seleccione los eventos de los que desea que se envíen alertas.

Nota: las opciones Detección de comportamiento sospechoso, Detección de archivos sospechosos y Detección y limpieza de adware/PUA sólo son compatibles con Windows 2000 y posterior. La opción Otros errores sólo se aplica a sistemas Windows.

5. En el panel **Destinatarios**, haga clic en **Añadir** o **Eliminar** para modificar la lista de direcciones de email a las que se enviarán las alertas. Haga clic en **Editar** para cambiar una dirección ya introducida.

Nota: desde ordenadores Mac OS X sólo se enviarán los mensajes al primer destinatario.

6. Haga clic en **Configurar correo SMTP** para cambiar la dirección de su servidor de correo SMTP y el idioma de las alertas.
7. En el cuadro de diálogo **Configuración de correo SMTP**, seleccione las opciones correspondientes según se describe a continuación:

- En el cuadro de texto **Servidor SMTP**, escriba el nombre o la dirección IP del servidor de SMTP. Haga clic en Probar para enviar un mensaje de prueba.
- En el cuadro de texto **Dirección remitente**, escriba una dirección de email a la que se puedan enviar los mensajes devueltos o no entregados.
- En el cuadro de texto **Dirección de respuesta**, puede introducir una dirección de correo a la que se puedan enviar las respuestas a las alertas. Las alertas se envían desde un buzón desatendido.

Nota: los sistemas Linux y UNIX no tienen en cuenta la dirección remitente y la dirección de respuesta, y en su lugar utilizarán la dirección raíz@<host>.

- En el panel **Idioma**, abra la lista desplegable y seleccione el idioma en el que desea que se envíen las alertas.

También puede configurar Sophos Control Center para enviar alertas por email según el estado del Panel de control, para más información consulte la Ayuda de Sophos Control Center.

7 Detectar aplicaciones no deseadas

Por defecto, Sophos Anti-Virus detecta virus, troyanos, programas espía y gusanos. También se puede configurar para detectar aplicaciones no deseadas.

Nota: esta opción se aplica sólo a Sophos Anti-Virus en Windows 2000 o posterior.

Sophos recomienda que en primer lugar use un escaneo programado para detectar aplicaciones no deseadas. Esto le permitirá gestionar de forma segura las aplicaciones que ya se ejecutan en su red. A continuación, puede activar el escaneo en acceso de aplicaciones no deseadas para proteger los equipos en un futuro.

7.1 Realizar un escaneo programado

1. En el panel de la izquierda, en **Configuración**, haga clic en **Configurar escaneo**.
2. En el cuadro de diálogo **Configurar escaneo**, en la sección **Escaneo programado**, haga clic en **Añadir** para crear un nuevo escaneo, o haga clic en **Editar** para modificar el escaneo seleccionado.
3. En el cuadro de diálogo **Escaneo programado**, haga clic en **Configurar** (en la parte inferior).
4. En el cuadro de diálogo **Configuración de escaneo y limpieza**, abra la ficha **Escaneo**. En el panel **Opciones de escaneo**, active la opción **Detectar adware/PUA** y haga clic en **Aceptar**.

Cuando se lleve a cabo el escaneo, es posible que Sophos Anti-Virus notifique algunas "aplicaciones no deseadas". Puede autorizar las aplicaciones o eliminarlas de los equipos.

7.2 Autorizar aplicaciones que desea utilizar

Si lo desea, puede autorizar aplicaciones que se hayan detectado como programas publicitarios o aplicaciones no deseadas durante un escaneo programado.

Para autorizar una aplicación:

1. En el panel de la izquierda, en **Configuración**, haga clic en **Configurar escaneo**.
2. En el cuadro de diálogo **Configurar escaneo**, haga clic en **Gestor de autorización**.
3. En el cuadro de diálogo **Gestor de autorización**, siga uno de estos pasos:
 - Seleccione la aplicación que desea autorizar. Haga clic en **Añadir** para añadirla a la lista de aplicaciones autorizadas.
 - Si no encuentra la aplicación, haga clic en **Nueva**. Haga clic en el enlace de la lista de posibles aplicaciones no deseadas de Sophos en el cuadro de diálogo que se abre. Localice la aplicación que desea autorizar y escriba su nombre en el campo **Nombre**.

7.3 Limpiar aplicaciones que no desea utilizar

Si lo desea, puede limpiar aplicaciones que se hayan detectado como programas publicitarios o aplicaciones no deseadas durante un escaneo programado.

Para limpiar aplicaciones:

1. En el panel izquierdo, en **Acción**, haga clic en **Resolver alertas y errores**.
Se abre el cuadro de diálogo **Resolver alertas y errores**.
2. Active las casillas de las aplicaciones que desea eliminar o haga clic en **Seleccionar todo** y haga clic en **Limpiar**.

De esta forma se eliminarán todos los componentes de las aplicaciones detectadas en los ordenadores de la red. El proceso de limpieza puede durar unos instantes.

Nota: existen ciertas aplicaciones que no se pueden eliminar desde Sophos Control Center. En estos casos tendrá que ir al equipo afectado y utilizar Sophos Anti-Virus para eliminar la aplicación no deseada.

Para completar la eliminación de ciertas amenazas con múltiples componentes, es posible que tenga que reiniciar el sistema. En este caso, se muestra un aviso en el ordenador afectado en el que se da la oportunidad de reiniciar el sistema en ese momento o más adelante. El proceso de limpieza continua al reiniciar el sistema.

Para más información sobre cualquier aplicación detectada, en el cuadro de diálogo **Resolver alertas y errores**, haga clic en el nombre de la aplicación.

Al hacer clic en **Quitar**, las aplicaciones seleccionadas se eliminan de la lista, pero no se eliminan ni se autorizan.

7.4 Activar la detección en acceso de aplicaciones no deseadas y programas publicitarios

1. En el panel de la izquierda, en **Configuración**, haga clic en **Configurar escaneado**.
Aparece el cuadro de diálogo **Configurar escaneado**.
2. Haga clic en **Escaneado en acceso**.
Aparece el cuadro de diálogo **Configuración del escaneado en acceso**.
3. En el panel **Opciones de escaneado**, active la casilla **Detectar adware/PUA**. Haga clic en **Aceptar**.

Algunas aplicaciones controlan archivos e intentan acceder a ellos con frecuencia. Si ha activado el escaneado en acceso, éste detectará cada intento de acceso y enviará múltiples alertas.

8 Desinfectar virus

Si se detecta algún virus en las estaciones de su red, podrá desinfectarlo de la siguiente manera:

1. En Sophos Control Center, en el **Panel de control**, haga clic en el enlace **Virus/spyware**

En el cuadro de diálogo **Resolver alertas y errores** se mostrará la lista de ordenadores infectados y detalles de los virus detectados.

2. Seleccione los virus que desea desinfectar y haga clic en **Limpiar**.

Se elimina el virus del archivo o sector de arranque infectado. Sin embargo, la limpieza de documentos se recomienda sólo como medida temporal, ya que no soluciona cualquier otro cambio realizado por el virus en el documento; sustituya después los programas utilizando los discos originales o copias de seguridad limpias. El proceso de limpieza puede durar unos instantes.

Existen ciertos virus que no se pueden eliminar desde Sophos Control Center. En estos casos tendrá que ir al equipo afectado y utilizar Sophos Anti-Virus para eliminar dicho virus.

Antes de intentar la eliminación de amenazas con múltiples componentes, Sophos recomienda un escaneado programado completo del sistema.

Para más información sobre cualquier virus detectado, en el cuadro de diálogo **Resolver alertas y errores**, haga clic en el nombre del virus.

9 Configurar el cortafuegos

Al instalar Sophos Client Firewall por primera vez, la configuración predeterminada permite el tráfico esencial entrante y saliente.

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.

9.1 Configurar el cortafuegos

El cortafuegos se puede configurar para permitir o bloquear el tráfico según sea necesario. Por defecto, el cortafuegos está configurado para permitir el tráfico entrante esencial y todo el tráfico saliente.

Para configurar el cortafuegos:

1. En el panel de la izquierda, en **Configuración**, haga clic en **Configurar cortafuegos**.
2. En el asistente de configuración del cortafuegos, haga clic en **Siguiente**.
3. En la página **Configurar cortafuegos**, seleccione la opción necesaria:

- **Ubicación única**

Seleccione esta opción para los equipos que estén siempre en la red, como los ordenadores de escritorio.

- **Ubicación dual**

Seleccione esta opción si desea que el cortafuegos utilice una configuración diferente según la ubicación de los equipos, por ejemplo, en la oficina o fuera de ella. La ubicación dual es aconsejable para los equipos portátiles.

- **Permitir todo el tráfico**

Seleccione esta opción para desactivar el cortafuegos.

4. Si selecciona **Ubicación dual**, en el cuadro de diálogo **Identificación de red**, configure la identificación del DNS o puerta de enlace de la red.

Nota: la página **Identificación de red** sólo aparece si selecciona **Ubicación dual**.

Sophos Control Center aplicará una configuración diferente del cortafuegos a los equipos, dependiendo de si están en la red o no.

5. En la página **Modo operativo**, especifique el comportamiento del cortafuegos ante tráfico entrante y saliente.

- **Bloquear el tráfico de entrada y permitir el de salida**

Permite a las estaciones acceder a la red y a Internet pero bloquea el tráfico que proviene de fuera. En este modo, las aplicaciones no se autentican.

- **Bloquear el tráfico de entrada y el de salida**

Si selecciona este modo, el cortafuegos bloqueará todo el tráfico saliente, excepto para las aplicaciones que especifique. Haga clic en **Confianzas** a la derecha de la opción para añadir aplicaciones. Para las aplicaciones de confianza se permite todo el tráfico de red.

■ Monitorizar

Este modo aplica las reglas especificadas a los ordenadores y permite el acceso a la red y a Internet del tráfico desconocido. Este modo envía información a la consola. Utilice este modo para recoger información sobre la red y crear reglas adecuadas.

■ Personalizado

Permite aplicar una configuración personalizada. Haga clic en **Avanzadas** para ver las opciones de configuración avanzada.

Nota: sólo debería modificar las opciones avanzadas si entiende los efectos que los cambios pueden conllevar.

Para más información sobre las opciones avanzadas, consulte la Ayuda de *Sophos Endpoint Security and Control*.

6. En la página **Uso compartido de archivos e impresoras**, seleccione **Permitir el uso compartido de archivos e impresoras** si desea que las estaciones en la red puedan compartir carpetas e impresoras.
7. Si seleccionó **Ubicación dual**, tendrá que configurar el modo operativo y el uso compartido de archivos e impresoras (según se describe en los pasos 5 y 6) para la ubicación secundaria (fuera de la red).

Puede utilizar de nuevo este asistente cuando desee modificar cualquiera de las opciones.

Tras configurar el cortafuegos, puede utilizar el **Visualizador de eventos del cortafuegos** para monitorizar el comportamiento (por ejemplo, aplicaciones bloqueadas por el cortafuegos). Para más información, consulte la Ayuda de Sophos Control Center.

9.2 Elementos bloqueados por el cortafuegos

Es posible que Sophos Control Center bloquee aplicaciones o procesos que desee ejecutar. En ese caso:

1. En Sophos Control Center, en el **Panel de control**, haga clic en el enlace **Cortafuegos**
2. En el cuadro de diálogo **Visualizador de eventos del cortafuegos**, seleccione la entrada de la aplicación para la que desea crear una regla o que desea autorizar. Haga clic en **Crear regla**.
3. En el cuadro de diálogo que aparece, seleccione si desea permitir la aplicación o crear una regla para que utilice una configuración existente.

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/>

iMatix SFL

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