

SOPHOS

Sophos Helpdesk Console manual del usuario

Edición: Febrero de 2008



Contenido

1	Introducción a Helpdesk Console.....	4
2	Proteger ordenadores.....	8
3	Comprobar que la red está protegida.....	14
4	Actualizar ordenadores.....	20
5	Hacer que los ordenadores se ciñan a las políticas.....	21
6	Escanear ordenadores.....	22
7	Qué hacer ante una alerta.....	23
8	Limpiar ordenadores.....	27
9	Generar informes.....	29
10	Solución de problemas.....	37
11	Glosario.....	42

1 Introducción a Helpdesk Console

Sophos Helpdesk Console permite al departamento informático monitorizar y administrar el software de seguridad de Sophos.

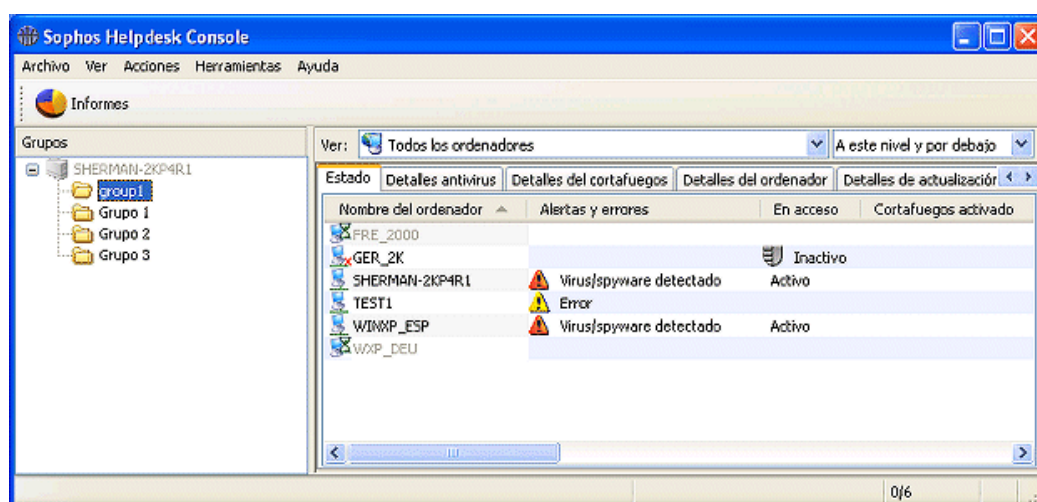
Desde Helpdesk Console podrá administrar los grupos de ordenadores a los que le dé acceso el administrador central. Podrá proteger ordenadores, comprobar que están actualizados, recibir alertas y limpiar amenazas y aplicaciones no deseadas detectadas en la red.

Esta sección describe la interfaz y las funciones principales de Helpdesk Console.

- [Acerca de la interfaz](#)
- [Qué es un grupo](#)
- [Qué son las políticas](#)
- [Significado de los iconos](#)

Acerca de la interfaz

A continuación se describen las principales funciones de Helpdesk Console.



El panel Grupos

En el panel **Grupos** podrá ver los grupos de ordenadores que se le permite administrar. Seleccione un grupo para ver los ordenadores que contiene.



El administrador central decide los grupos de ordenadores a los que tendrá acceso desde Helpdesk Console. Si necesita acceso a algún otro grupo, póngase en contacto con su administrador.

La lista de ordenadores

La lista de ordenadores (panel de la derecha) muestra los ordenadores que forman parte del grupo seleccionado.



Si gestiona equipos Linux desde la consola, configure un nombre de servidor exclusivo para cada uno. De lo contrario, aparecerán todos en la consola con el nombre predeterminado "localhost".


La ficha **Estado** muestra si los equipos están protegidos mediante escaneado en acceso, si el cortafuegos está activado y si el software está actualizado. Esta página también muestra las alertas. El resto de fichas aportan más datos sobre cada uno de los siguientes aspectos.

Para ver una explicación de los iconos que aparecen en la lista de ordenadores, vea la sección [Significado de los iconos](#).

La barra de herramientas

Informes permite generar informes sobre alertas en sus redes.

Qué es un grupo

Un grupo  es una carpeta que incluye un cierto número de ordenadores.

El administrador central decide los grupos de ordenadores que podrá administrar desde Helpdesk Console. Si necesita acceso a algún otro grupo, póngase en contacto con su administrador.

Cada grupo puede disponer de su propia configuración antivirus y HIPS, de actualización, cortafuegos y restricción de aplicaciones. Generalmente, todos los ordenadores de un grupo usan estos parámetros de configuración, que constituyen una "política".

Un grupo puede contener subgrupos.

Qué son las políticas

Una política es el conjunto de normas y opciones de configuración que rigen cada grupo.

El administrador central crea estas políticas. Como usuario de Helpdesk Console, no podrá crear ni modificar políticas, pero puede hacer que los ordenadores cumplan con las políticas establecidas.

Estos son los tipos de política:


- La política de **actualización** define la configuración de actualización de nuevo software.
- La política **antivirus y HIPS** define la configuración del escaneo de Sophos Anti-Virus. También define las opciones de limpieza.
- La política de **restricción de aplicaciones** define las opciones de bloqueo de aplicaciones desde Sophos Anti-Virus.
- La política **cortafuegos** define cómo Sophos Client Firewall protege los ordenadores.

Significado de los iconos

En la lista de ordenadores, los iconos se usan para indicar:

- las alertas
- protección desactivada u obsoleta
- el estado de cada ordenador, por ejemplo si se está instalando un programa.

Alertas

Símbolo	Significado
	La detección de virus, gusanos, troyanos, programas espía o comportamientos sospechosos se indica mediante iconos de aviso rojos en la columna Alertas y errores .



Los iconos de aviso amarillos que aparecen en la columna **Alertas y errores** indican uno de los problemas siguientes:

- Se ha detectado un archivo sospechoso.
- Se ha detectado un programa publicitario o aplicación no deseada.
- Se ha detectado una aplicación restringida.
- El cortafuegos ha bloqueado una aplicación.
- Se ha producido un error.

Los iconos de aviso amarillos que aparecen en las columnas **Política antivirus y HIPS**, **Política cortafuegos**, **Política de actualización** o **Política de restricción de aplicaciones** indican que el equipo no está utilizando las mismas políticas que el resto de equipos de su grupo.

Si existen varias alertas o errores en un equipo, el icono de la alerta más importante aparecerá en la columna **Alertas y errores**. A continuación se enumeran los tipos de alertas en orden descendente de prioridad.

Prioridad de alertas

1. Alertas de virus/spyware
2. Alertas de comportamientos sospechosos
3. Alertas de archivos sospechosos
4. Alertas del cortafuegos
5. Alertas de adware/PUA
6. Alertas de aplicaciones restringidas
7. Sophos Anti-Virus, actualizaciones y errores de Sophos Client Firewall

Protección desactivada u obsoleta

Símbolo	Significado
	Un escudo gris indica que el escaneo en acceso se encuentra inactivo.



Un icono de cortafuegos de color gris indica que el cortafuegos está desactivado.



Un icono de un reloj indica que el software está obsoleto.

Estado del ordenador

Símbolo	Significado
	Un icono de un ordenador azul indica que el ordenador es administrado por Helpdesk Console.
	Un icono de un ordenador con una flecha amarilla indica que la instalación del software antivirus y del cortafuegos está pendiente.
	Un icono de un ordenador con una flecha verde indica que la instalación está en progreso.
	Un icono de un ordenador con un reloj de arena indica que el componente de actualización automática de Sophos Anti-Virus ha sido instalado y en ese momento está descargando la última versión del producto.
	Un icono de un ordenador gris indica que el ordenador no es administrado por Helpdesk Console.
	Un icono de un ordenador con una cruz roja indica que el ordenador está desconectado.


2 Proteger ordenadores

En esta sección se describe cómo instalar Sophos Anti-Virus y Sophos Client Firewall en ordenadores en red.

- Proteger ordenadores
- Proteger ordenadores que requieren instalación manual
- Proteger ordenadores mediante un archivo de inicio de sesión
- Añadir el cortafuegos a los ordenadores protegidos

Proteger ordenadores

Puede proteger ordenadores Windows de forma automática como se describe a continuación.


 No es posible la instalación automática en estaciones con Windows 95/98/Me. Vea cómo realizar la [instalación manual](#).

1. Seleccione los ordenadores nuevos. Haga clic con el botón derecho y seleccione **Proteger ordenadores**. Se inicia el **Asistente para proteger ordenadores**.
2. En la página inicial, haga clic en **Siguiente**.
3. En la página **Seleccionar el software de seguridad**, seleccione el programa que desee.

Sophos Client Firewall está sólo disponible si su licencia lo incluye, y sólo para Windows 2000 o posterior. No es posible instalar el cortafuegos en un sistema operativo de servidor.

Haga clic en **Siguiente**.

4. En la página **Resumen de protección**, cualquier problema con la instalación aparecerá en la columna **Problemas de protección**. Consulte la sección de [resolución de problemas](#), o realice una [instalación manual](#) para esos ordenadores. Haga clic en **Siguiente**.
5. En la página **Credenciales**, introduzca los datos de una cuenta que pueda utilizarse para instalar software. Normalmente, esta cuenta es una cuenta de administrador de dominio. Debe tener:
 - § derecho de administrador local en las estaciones a proteger
 - § acceso al servidor de administración
 - § derecho de lectura al **servidor primario** especificado en la política de actualización.

 Si usa una cuenta de dominio, debe introducir un nombre de usuario en el formato dominio\usuario.

Proteger ordenadores que requieren instalación manual

Si Helpdesk Console no puede instalar el software antivirus o el cortafuegos de forma automática en ciertos equipos, podrá hacerlo de

forma manual.

Helpdesk Console administrará y actualizará dichos ordenadores según el grupo al que pertenezcan.



Si lo prefiere, podrá realizar la instalación mediante un archivo de inicio de sesión. Consulte Proteger ordenadores mediante un archivo de inicio de sesión.



Si dispone de una versión previa de Sophos Anti-Virus para Windows 95, 98 o Me, deberá desinstalarla antes de instalar la última versión.

Para realizar una instalación manual, haga lo siguiente.

1. En Helpdesk Console, seleccione los ordenadores en los que desea realizar una instalación manual. Haga clic en la ficha **Detalles de la actualización** y mire en la columna **Servidor primario**. Aquí se muestra el directorio que utiliza cada ordenador para actualizarse.

(Si utiliza la estructura predeterminada)

Sophos Endpoint Security and Control para Windows 2000/XP/2003/Vista	\\Nombredelservidor\InterChk\SAVSCFXP
Sophos Anti-Virus para Windows 2000/XP/2003/Vista	\\Nombredelservidor\InterChk\ESXP
Sophos Anti-Virus para Windows NT	\\Nombredelservidor\InterChk\ESNT
Sophos Anti-Virus para Windows 95/98/Me	\\Nombredelservidor\InterChk\ES9X
Sophos Anti-Virus para Mac OS X	\\Nombredelservidor\InterChk\ESOSX
Sophos Anti-Virus para Linux	\\Nombredelservidor\InterChk\savlinux



El directorio para "Sophos Endpoint Security and Control" contiene el programa de instalación para Sophos Anti-Virus y Sophos Client Firewall.

2. Vaya al ordenador y busque el directorio desde donde se actualiza.

En estaciones **Windows**, haga doble clic en setup.exe.

Para proteger equipos Windows 2000 o posteriores con el cortafuegos, así como el software antivirus, abra la línea de comandos y ejecute setup.exe con el modificador adecuado:
setup.exe -sav instala sólo el antivirus
setup.exe -scf instala el antivirus y el cortafuegos

En estaciones **Mac OS X**, haga doble clic en Sophos Anti-Virus.mpkg.

En estaciones **Linux**, instale Sophos Anti-Virus mediante el paquete de distribución, como se describe en la *Guía de inicio en red de Sophos Endpoint Security and Control*.



Si gestiona equipos Linux desde la consola, configure un nombre de servidor exclusivo para cada uno. De lo contrario, aparecerán todos en la consola con el nombre predeterminado "localhost".

Proteger ordenadores mediante un archivo de inicio de sesión

Puede proteger ordenadores con el software antivirus (y el cortafuegos si lo incluye su licencia) si ejecuta el programa de instalación con un script o un programa como Microsoft SMS.



Helpdesk Console administrará y actualizará dichos ordenadores según el grupo al que pertenezcan.

Aquí encontrará información sobre cómo:

- Encontrar el programa de instalación adecuado
- [Proteger ordenadores Windows 2000 o posteriores](#)
- [Proteger ordenadores Windows 95/98/Me](#)
- [Proteger ordenadores Mac OS X](#)
- [Proteger ordenadores Linux](#)


Encontrar el programa de instalación adecuado

El programa de instalación se encuentra en el directorio con las actualizaciones de Sophos. Para comprobar de qué directorio se trata, en la lista de ordenadores busque el equipo que desea proteger. Haga clic en la ficha **Detalles de la actualización** y mire en la columna **Servidor primario**.

(Si utiliza la estructura predeterminada)

Sophos Endpoint Security and Control para \\Nombredelservidor\InterChk\SAVSCFXP
Windows 2000/XP/2003/Vista

Sophos Anti-Virus para Windows 2000/XP/2003/Vista	\\Nombredelservidor\InterChk\ESXP
Sophos Anti-Virus para Windows NT	\\Nombredelservidor\InterChk\ESNT
Sophos Anti-Virus para Windows 95/98/Me	\\Nombredelservidor\InterChk\ES9X
Sophos Anti-Virus para Mac OS X	\\Nombredelservidor\InterChk\ESOSX
Sophos Anti-Virus para Linux	\\Nombredelservidor\InterChk\savlinux

 El directorio para "Sophos Endpoint Security and Control" contiene el programa de instalación para Sophos Anti-Virus y Sophos Client Firewall.

Proteger ordenadores Windows 2000 o posteriores

Si desea proteger ordenadores Windows 2000 o posteriores con el cortafuegos, así como con el software antivirus, deberá:

- Asegurarse de que está usando el programa de configuración adecuado. Éste es el programa de configuración para Sophos Endpoint Security and Control y se encuentra en un directorio llamado SAVSCFXP.
- Ejecutar el programa de configuración con el modificador -scf.


Proteger ordenadores Windows 95/98/Me

Para proteger ordenadores con Windows 95/98/Me con un archivo de inicio de sesión, siga los siguientes pasos:

1. Si aún la desconoce, busque la ubicación del directorio que contiene el programa de instalación.
2. Añada la siguiente línea al archivo de inicio de sesión:


```
[Ruta]\setup.exe -usuario [dominio\nombre] -pwd [contraseña] -login -s
```

donde [Ruta] es la ubicación del directorio con el programa de instalación (por ejemplo, \\servidor\InterChk\ES9x) y el nombre de usuario y la contraseña corresponden a una cuenta con acceso a sus ordenadores con Windows 95/98/Me y a la unidad compartida (en este ejemplo, \\servidor\InterChk).

 Si dispone de algún ordenador con Windows 95, deberá ejecutar una pequeña aplicación antes de realizar la instalación. Desde el CD-ROM de instalación en red de Sophos Endpoint Security and Control, copie el archivo Tools/Utils/w95ws2setup.exe a su servidor. A continuación, inserte una línea en el archivo de inicio de sesión, antes de la línea mostrada anteriormente, para ejecutar esta aplicación.

La cuenta de usuario que va a determinar debe:

- § poder iniciar la sesión en los ordenadores que desea proteger
- § derecho de administrador local en las estaciones a proteger
- § derecho de lectura al **servidor primario** especificado en la política de actualización.

 Si no desea administrar los ordenadores con Helpdesk Console, añada el parámetro -mng no.


La próxima vez que los ordenadores se inicien, se instalará el programa antivirus.

Proteger ordenadores Mac OS X

Para ordenadores Mac OS X, use Apple Remote Desktop. Vaya al directorio de instalación central y copie el programa de instalación en el ordenador ejecutando Apple Remote Desktop antes de utilizarlo.

Proteger ordenadores Linux

Para más información sobre cómo instalar Sophos Anti-Virus en ordenadores Linux, consulte la *Guía de inicio de Sophos Anti-Virus para Linux*.

 Si gestiona equipos Linux desde la consola, configure un nombre de servidor exclusivo para cada uno. De lo contrario, aparecerán todos en la consola con el nombre predeterminado "localhost".

Añadir el cortafuegos a los ordenadores protegidos

Si sus ordenadores ya están protegidos con Sophos Anti-Virus, puede

instalar Sophos Client Firewall en ellos si dispone de la licencia correspondiente.



El cortafuegos puede instalarse solamente en ordenadores con Windows 2000 o posterior.



No es posible instalar el cortafuegos en un sistema operativo de servidor.

1. Seleccione los ordenadores donde desea instalar el cortafuegos. Haga clic con el botón derecho y seleccione **Proteger ordenadores**. Se iniciará un asistente.
2. En la página inicial, haga clic en **Siguiente**.
3. En la página **Seleccionar el software de seguridad**, seleccione **Instalar Sophos Client Firewall**.
4. En la página **Resumen de protección**, cualquier problema con la instalación aparecerá en la columna **Problemas de protección**. Consulte la sección de [resolución de problemas](#), o realice una [instalación manual](#) para esos ordenadores. Haga clic en **Siguiente**.
5. En la página **Credenciales**, introduzca los datos de una cuenta que pueda utilizarse para instalar software. Normalmente, esta cuenta es una cuenta de administrador de dominio.

3 Comprobar que la red está protegida

En esta sección se describe cómo comprobar que los ordenadores están protegidos. También explica cómo identificar equipos con problemas mediante los filtros de listas de equipos y qué hacer para resolver dichos problemas.

- [Qué ordenadores están protegidos](#)
- [Qué ordenadores están actualizados](#)
- [Identificar ordenadores no protegidos](#)
- [Identificar ordenadores sin el cortafuegos instalado](#)
- [Identificar ordenadores con alertas pendientes](#)
- [Identificar ordenadores con protección obsoleta](#)

- Identificar ordenadores no administrados por la consola
- Identificar ordenadores desconectados de la red

También puede comprobar si todos los equipos de un grupo cumplen las opciones de antivirus y HIPS, actualización, cortafuegos y restricción de aplicaciones de dicho grupo, según se describe en Comprobar que los ordenadores cumplen las políticas.

Qué ordenadores están protegidos

Los ordenadores están protegidos si tienen activado el escaneo en acceso y el cortafuegos (si lo ha instalado). Para una protección completa, el software debe estar actualizado.



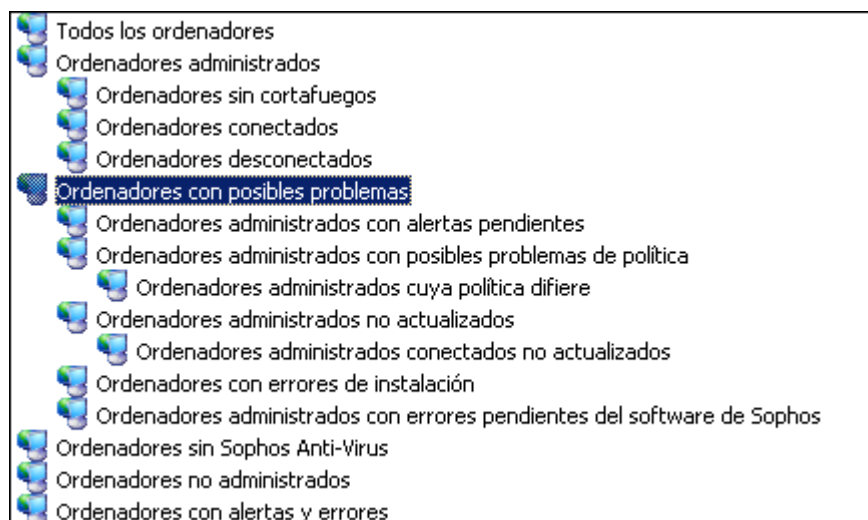
El administrador puede haber desactivado el escaneo en acceso a propósito, por ejemplo en servidores.

Para comprobar que los ordenadores están protegidos:

1. Seleccione el grupo de ordenadores que desea comprobar.
2. Si desea comprobar ordenadores en subgrupos, seleccione **A este nivel y por debajo** en la lista desplegable.
3. En la lista de ordenadores, mire en la columna **En acceso**. Si aparece "Activo", el equipo dispone de escaneo en acceso. Si aparece un escudo en gris y el texto "Inactivo", el escaneo en acceso no está funcionando en ese equipo.
4. Si instaló el cortafuegos, compruebe la columna **Cortafuegos activado**. Si aparece "Sí", el ordenador tiene protección cortafuegos.
5. A continuación, mire en la columna **Actualizado**. Si aparece "Sí", el ordenador está actualizado. De lo contrario, el equipo no estará actualizado.



Puede ver una lista de los equipos que no están protegidos adecuadamente o que tienen problemas relacionados con la protección. Vaya al menú desplegable **Ver** y seleccione **Ordenadores con posibles problemas**. También puede seleccionar una entrada secundaria de ésta para ver los equipos afectados por un problema específico (como equipos con una política de grupo diferente o errores en los productos de Sophos).




Qué ordenadores están actualizados

Si el software de seguridad de Sophos se configuró de la forma recomendada, los ordenadores recibirán las actualizaciones de forma automática.

1. Seleccione el grupo de ordenadores que desea comprobar.
2. Si desea comprobar ordenadores en subgrupos, seleccione **A** este nivel y por debajo en la lista desplegable.
3. Mire en la columna **Actualizado**.


Si aparece "Sí", el ordenador está actualizado.

De lo contrario, el equipo no estará actualizado. Se indicará el tiempo que lleva sin actualizarse.

 Para actualizar los ordenadores, selecciónelos. Haga clic con el botón derecho y seleccione **Actualizar ordenadores ahora**.

Identificar ordenadores no protegidos

Un ordenador no está protegido correctamente si no tiene activado el escaneo en acceso o el cortafuegos (en caso de tenerlo instalado).

 El administrador puede haber desactivado el escaneo en acceso a propósito, por ejemplo en servidores.

Si un ordenador no tiene el escaneado en acceso activo, aparecerá un escudo gris y la palabra "Inactivo" en la columna **En acceso** en la ficha **Estado**.

Si el cortafuegos está desactivado, se mostrará un icono de cortafuegos (una pared de ladrillos) de color gris en la columna **Cortafuegos activado**.

Para mostrar todos los ordenadores que no están correctamente protegidos, haga lo siguiente:

1. Seleccione el grupo de ordenadores.
2. En la barra de herramientas, en el cuadro de lista desplegable **Ver**, seleccione **Ordenadores con posibles problemas**. También puede seleccionar una entrada secundaria de ésta para ver los equipos afectados por un problema específico (como equipos con una política de grupo diferente o errores en los productos de Sophos).
3. Si el grupo contiene subgrupos, seleccione **Sólo a este nivel o A este nivel y por debajo**.
4. En la lista aparecerán los ordenadores que tengan problemas de protección.

Identificar ordenadores sin el cortafuegos instalado

Si un ordenador no tiene instalado el cortafuegos, aparecerá un icono de cortafuegos de color gris (una pared de ladrillos) en la columna **Cortafuegos activado** de la ficha **Estado**.

Para mostrar todos estos ordenadores y solucionar sus problemas, haga lo siguiente:

1. Seleccione el grupo de ordenadores.
2. En el cuadro de lista desplegable **Ver**, seleccione **Ordenadores sin cortafuegos**.
3. Si el grupo contiene subgrupos, seleccione **Sólo a este nivel o A este nivel y por debajo**.
4. Si no existen ordenadores en los que desea instalar el cortafuegos, haga clic con el botón derecho y seleccione **Proteger ordenadores**. Cuando se le pida seleccionar el

software, seleccione **Instalar Sophos Client Firewall**.

Identificar ordenadores con alertas pendientes

Si algún ordenador tiene alertas pendientes, mostrará un icono de alerta en la columna **Alertas y errores** en la ficha **Estado**.

El icono de aviso rojo informa sobre un virus o un programa espía. El icono amarillo informa sobre comportamientos o archivos sospechosos, programas publicitarios u otras aplicaciones no deseadas, una aplicación bloqueada por el cortafuegos, una aplicación restringida o un error.

Para mostrar los ordenadores con alertas que aún requieren atención:

1. Seleccione el grupo de ordenadores.
2. En el cuadro de lista desplegable **Ver**, seleccione **Ordenadores administrados sin alertas pendientes**.
3. Si el grupo contiene subgrupos, seleccione **Sólo a este nivel o A este nivel y por debajo**.
4. Si hay ordenadores con un virus o una aplicación que no desea, consulte [Realizar una limpieza inmediata](#).

Si hay aplicaciones detectadas que desea utilizar, póngase en contacto con su administrador central para su autorización.

Si el cortafuegos ha bloqueado alguna aplicación que desea utilizar, póngase en contacto con su administrador central para su autorización.

Si tiene algún ordenador con protección obsoleta, vaya a [Identificar ordenadores con protección obsoleta](#) para saber cómo identificar y resolver el problema.



Una vez resuelto el problema, puede borrar la alerta. Seleccione los ordenadores con alertas, haga clic con el botón derecho y seleccione **Quitar alertas y errores**.

Identificar ordenadores con protección obsoleta

Si algún ordenador tiene la protección antivirus obsoleta, aparecerá un icono de un reloj en la columna **Actualizado** en la ficha **Estado**. Se

indicará el tiempo que lleva sin actualizarse.

Un ordenador puede tener una protección obsoleta por dos razones:

- El ordenador no ha podido recoger una actualización desde el servidor.
- El servidor no dispone de las últimas actualizaciones del software de Sophos.

Esta sección explica cómo identificar el problema y actualizar los ordenadores.

1. Seleccione el grupo de ordenadores.
2. En la ficha **Estado**, haga clic en la columna **Actualizado** para ordenar los equipos por la fecha en la que su protección pasó a ser obsoleta.
3. Haga clic en la ficha **Detalles de la actualización** y mire en la columna **Servidor primario**. Aquí se muestra el directorio que utiliza cada ordenador para actualizarse.
4. Observe los ordenadores que se actualizan desde un directorio en concreto.

Si algunos de ellos tienen una protección obsoleta y otros no, el problema radica en los equipos individuales. Selecciónelos, haga clic con el botón derecho y seleccione **Actualizar ordenadores ahora**.

Si todos tienen una protección obsoleta, el problema podría estar en el directorio de actualización. El administrador central podrá comprobar que el directorio de instalación dispone de la última actualización del software de seguridad de Sophos.

Identificar ordenadores no administrados por la consola

Los ordenadores Windows, Macintosh y Linux deben gestionarse mediante Helpdesk Console, de manera que puedan actualizarse y monitorizarse.

Si algún ordenador no está administrado, las estaciones aparecerán en gris en la ficha **Estado**.

Para identificar ordenadores no administrados y gestionarlos, siga los

siguientes pasos:

1. En el cuadro de lista desplegable **Ver**, seleccione **Ordenadores no administrados**.
2. Seleccione cualquier ordenador que aparezca en la lista. Haga clic con el botón derecho y seleccione **Proteger ordenadores** para instalar una versión administrada de Sophos Anti-Virus.
3. Si hay ordenadores en los que Helpdesk Console no puede instalar Sophos Anti-Virus de forma automática, realice una instalación manual.

Identificar ordenadores desconectados de la red

Si algún ordenador está desconectado de la red, aparecerá una cruz roja junto al icono al lado de su nombre en la ficha **Estado**.

Para identificar estos ordenadores:

1. Seleccione el grupo de ordenadores.
2. En el cuadro de lista desplegable **Ver**, seleccione **Ordenadores desconectados**.
3. Si el grupo contiene subgrupos, seleccione **Sólo a este nivel o A este nivel y por debajo**.



"Ordenadores desconectados" hace referencia a los ordenadores que normalmente están gestionados por Helpdesk Console, pero que están desconectados. No se mostrarán los ordenadores desconectados no administrados.

4 Actualizar ordenadores

Los ordenadores, con la configuración predeterminada, se actualizan de forma automática, aunque también puede actualizarlos cuando sea necesario.

- Actualizar ordenadores al instante

Actualizar ordenadores al instante

Puede actualizar ordenadores de forma inmediata entre actualizaciones programadas.

Seleccione los ordenadores que desea actualizar. Haga clic con el botón derecho y seleccione **Actualizar ordenadores ahora**.

5 Hacer que los ordenadores se ciñan a las políticas

En esta sección se explica cómo garantizar que todos los equipos de un mismo grupo utilicen las mismas opciones de antivirus y HIPS, actualización, cortafuegos y restricción de aplicaciones.

- Comprobar que los ordenadores cumplen las políticas
- Hacer que los ordenadores se ciñan a las políticas

Comprobar que los ordenadores cumplen las políticas

Podrá comprobar que todos los ordenadores de un grupo disponen de la misma configuración antivirus y HIPS, de actualización, de cortafuegos y de restricción de aplicaciones.

1. Seleccione el grupo que desea comprobar.
2. En la página **Estado**, observe las columnas **Política antivirus y HIPS**, **Política de actualización**, **Política cortafuegos** y **Política de restricción de aplicaciones**. Si algún ordenador no dispone de la configuración del grupo, verá un icono de aviso y el mensaje "Diferente de la política".

Si quiere que los equipos cumplan las políticas de los grupos a los que pertenecen, consulte Hacer que los ordenadores se ciñan a las políticas.

Hacer que los ordenadores se ciñan a las políticas

Si encuentra algún ordenador que no se ajusta a la configuración antivirus y HIPS, de actualización, de cortafuegos o de restricción de aplicaciones del grupo, puede forzar el cambio en dicho ordenador.

1. Seleccione los ordenadores que no cumplen con la configuración del grupo.
2. Haga clic con el botón derecho del ratón y seleccione **Cumplir con**. Después, seleccione **Política antivirus y HIPS del grupo**, **Política de actualización del grupo**, **Política cortafuegos del grupo**, **Política de restricción de aplicaciones del grupo** o **Todas las políticas del grupo** según sea adecuado.

6 Escanear ordenadores

Por defecto, Sophos Anti-Virus detecta virus, troyanos, gusanos y programas espía de forma automática tan pronto como un usuario intenta acceder a un archivo infectado. Sophos Anti-Virus 7 y posterior para Windows 2000 y posterior también permite analizar el comportamiento de programas y procesos.

También es posible realizar escaneos remotos desde la consola de administración.

Escaneo remoto

Puede escanear ordenadores de forma inmediata sin necesidad de esperar hasta el siguiente escaneo programado.



Sólo es posible realizar escaneos remotos en sistemas Windows con Sophos Anti-Virus 7 o posterior.

1. Seleccione los ordenadores que desea escanear. Haga clic con el botón derecho del ratón y seleccione **Escaneo remoto**.

También encontrará este comando en el menú **Acciones**.

2. Para iniciar el escaneo, en el cuadro de diálogo **Escaneo remoto**, compruebe la lista de ordenadores a escanear y haga clic en **Aceptar**.

7 Qué hacer ante una alerta

En esta sección se describe qué hacer ante una alerta.

Comprende lo siguiente:

- [Significado de los iconos de alerta](#)
- [Alertas de virus y programas espía](#)
- [Alertas de comportamientos sospechosos](#)
- [Alertas de archivos sospechosos](#)
- [Qué hacer ante una alerta de cortafuegos](#)
- [Programas publicitarios y aplicaciones no deseadas](#)
- [Alertas de aplicaciones restringidas](#)
- [Borrar las alertas desde la consola](#)

Significado de los iconos de alerta


Si se detecta un elemento sospechoso, un programa publicitario u otra aplicación no deseada, aparecen iconos de alerta en la página Estado de Helpdesk Console.

Más abajo se incluye una explicación de los iconos de alerta. En el resto de páginas de esta sección, hallará información sobre qué hacer ante una alerta.



También se mostrarán avisos en la consola si el programa está desactivado u obsoleto. Para más información, consulte la sección [Comprobar que la red está protegida](#).

Iconos de alerta

Símbolo	Significado
	La detección de virus, gusanos, troyanos, programas espía o comportamientos sospechosos se indica mediante iconos de aviso rojos en la columna Alertas y errores .



Los iconos de aviso amarillos que aparecen en la columna **Alertas y errores** indican uno de los problemas siguientes:

- Se ha detectado un archivo sospechoso.
- Se ha detectado un programa publicitario o aplicación no deseada.
- Se ha detectado una aplicación restringida.
- El cortafuegos ha bloqueado una aplicación.
- Se ha producido un error.

Los iconos de aviso amarillos que aparecen en las columnas **Política antivirus y HIPS**, **Política cortafuegos**, **Política de actualización** o **Política de restricción de aplicaciones** indican que el equipo no está utilizando las mismas políticas que el resto de equipos de su grupo.

Si existen varias alertas o errores en un equipo, el icono de la alerta más importante aparecerá en la columna **Alertas y errores**. A continuación se enumeran los tipos de alertas en orden descendente de prioridad.

Prioridad de alertas


1. Alertas de virus/spyware
2. Alertas de comportamientos sospechosos
3. Alertas de archivos sospechosos
4. Alertas del cortafuegos
5. Alertas de adware/PUA
6. Alertas de aplicaciones restringidas
7. Sophos Anti-Virus, actualizaciones y errores de Sophos Client Firewall

Alertas de virus y programas espía

Si se detecta un virus o un programa espía, aparecerá un triángulo rojo de advertencia y el mensaje "Virus/spyware detectado" en la página **Estado**.

Para más información, abra la ficha **Detalles de alertas y errores**. Para desinfectar un virus o programa espía, siga las instrucciones en Realizar una limpieza inmediata.

Alertas de comportamientos sospechosos

Si se detectan comportamientos sospechosos o desbordamientos del búfer durante el análisis de comportamientos sospechosos, aparecerá un triángulo rojo de aviso  y el mensaje "Comportamiento sospechoso detectado" en la página Estado.

Para más información, abra la ficha **Detalles de alertas y errores**. Para eliminar el elemento sospechoso, siga las instrucciones del apartado Realizar una limpieza inmediata. Sólo el administrador central puede autorizar elementos sospechosos.

Alertas de archivos sospechosos

Si se detecta un archivo sospechoso, aparecerá un triángulo amarillo de advertencia  y el mensaje "Archivo sospechoso detectado" en la página Estado.

Para más información, abra la ficha **Detalles de alertas y errores**. El nombre del archivo se muestra en la columna **Elemento detectado**.

Para eliminar el archivo, consulte el apartado Realizar una limpieza inmediata. Sólo el administrador central puede autorizar archivos.

Qué hacer ante una alerta de cortafuegos

Si el cortafuegos bloquea una aplicación, aparecerá un triángulo de aviso amarillo  y el mensaje "Alerta del cortafuegos" en la página Estado.




Este icono puede aparecer también por alertas de programas publicitarios y aplicaciones no deseadas de Sophos Anti-Virus. A continuación, el mensaje "Adware/PUA detectado" aparece junto al icono.

Para más información, abra la ficha **Detalles de alertas y errores**. El

nombre de la aplicación bloqueada por el cortafuegos se muestra en la columna **Elemento detectado**.

Sólo el administrador central puede autorizar aplicaciones.

Programas publicitarios y aplicaciones no deseadas

Si se detecta un programa publicitario o una aplicación no deseada (PUA), aparecerá una señal de aviso amarilla  y el mensaje "Adware/PUA detectado" en la página Estado.




Este icono también puede indicar una alerta de cortafuegos. A continuación, aparece el mensaje "Alerta del cortafuegos" junto al icono.

Para más información, abra la ficha **Detalles de alertas y errores**. El nombre de la aplicación se muestra en la columna **Elemento detectado**.

Para eliminar la aplicación, consulte [Realizar una limpieza inmediata](#). Sólo el administrador central puede autorizar aplicaciones.

Alertas de aplicaciones restringidas

Si se detecta una aplicación restringida, aparecerá un triángulo amarillo de advertencia  y el mensaje "Aplicación restringida detectada" en la página Estado.

Para más información, abra la ficha **Detalles de alertas y errores**. El nombre de la aplicación se muestra en la columna **Elemento detectado**.

Para eliminar la aplicación tendrá que ir a cada ordenador y ejecutar el programa de desinstalación de dicho producto.



El software de seguridad de Sophos podría interferir con la desinstalación, ya que es posible que el escaneo en acceso de aplicaciones restringidas bloquee los archivos de instalación/desinstalación. Consulte con su administrador central.

Borrar las alertas desde la consola

Una vez resuelto el problema que hubiera causado la alarma ya puede borrarla de la consola.



No se pueden borrar alertas sobre errores de instalación. Estas alertas solamente se borrarán cuando Sophos Anti-Virus se instale de forma satisfactoria en el ordenador.

1. Seleccione los ordenadores con alertas ya resueltas. Haga clic con el botón derecho del ratón y seleccione **Quitar alertas y errores**.
2. Se abre el cuadro de diálogo **Quitar alertas y errores**.

Para borrar alertas de la consola, en el cuadro de diálogo **Quitar alertas y errores**, en la ficha **Alertas**, seleccione las alertas que quiere borrar y haga clic en **Aceptar**. Las alertas reconocidas dejan de mostrarse en la consola.

Para borrar errores de productos de Sophos, en el cuadro de diálogo **Quitar alertas y errores**, vaya a las fichas **Errores de Sophos Anti-Virus** o **Errores del cortafuegos**, seleccione los errores que quiere borrar de la consola y haga clic en **Aceptar**.

8 Limpiar ordenadores

Esta sección describe cómo limpiar ordenadores infectados con un virus o que contienen una aplicación no deseada.

Podrá:

- Realizar una limpieza inmediata
- Eliminar elementos detectados si falla la limpieza

Realizar una limpieza inmediata

Desde Helpdesk Console, podrá limpiar de forma remota los ordenadores afectados por virus o aplicaciones no deseadas.



Esta opción sólo se aplica a ordenadores Windows 2000 o posterior con Sophos Anti-Virus 6 o posterior.

Para limpiar ordenadores con Windows 95/98/Me, NT4, Mac o Linux, el administrador central puede activar la limpieza automática. De lo contrario, tendrá que limpiar cada ordenador como se describe en la sección [Eliminar elementos detectados si falla la limpieza](#).



Sophos Anti-Virus podría informar de la detección parcial de algún elemento (como troyanos o aplicaciones no deseadas). Esto significa que no ha identificado todos los componentes de la aplicación. Para limpiar un elemento, tendrá que encontrar todos sus componentes mediante un escaneo remoto del ordenador afectado. Para más información, consulte [Elemento detectado de forma parcial](#).

1. En la lista de ordenadores, haga clic con el botón derecho del ratón en el ordenador que desea limpiar. Seleccione **Limpiar elementos detectados**.
2. En el cuadro de diálogo **Limpiar elementos detectados**, marque la casilla de los elementos que desee limpiar o **Seleccionar todo**.
3. Haga clic en **Aceptar** para limpiar el ordenador.
4. Si la limpieza se realiza de forma satisfactoria, las alertas que se muestran en la lista de ordenadores desaparecerán.

Si alguna alerta permanece en la lista, debería limpiar los ordenadores de forma manual. Consulte [Eliminar elementos detectados si falla la limpieza](#).

Eliminar elementos detectados si falla la limpieza

Si no puede limpiar ordenadores desde la consola, puede proceder a la limpieza manual de la siguiente manera.

1. En la vista principal de la consola, abra la ficha **Detalles de alertas y errores**. En la columna **Elemento detectado**, busque el nombre del elemento.
2. En el menú **Ayuda**, seleccione **Ver información del elemento**. Se abrirá la web de Sophos, donde podrá obtener información detallada sobre el elemento detectado, incluyendo el modo de desinfección.
3. Proceda a la limpieza manual en cada ordenador.



En la web de Sophos se ofrecen herramientas para la desinfección automática de ciertos virus y gusanos.

9 Generar informes

Puede generar informes sobre incidentes víricos en su red.

Haga clic en el icono **Informes** de la barra de herramientas y utilice el generador de **Informes** como se describe en esta sección.

Podrá:

- Generar informes
- Mostrar informes en modo de tabla
- Mostrar informes en modo gráfico
- Mostrar el número de alertas por nombre de elemento
- Mostrar el número de alertas por ubicación
- Mostrar la tasa de alertas
- Mostrar historial de alertas
- Imprimir informes
- Exportar informes
- Cambiar el diseño del informe

Generar informes

Para crear un informe, haga lo siguiente.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Informes**, seleccione el tipo de informe que desea generar.
 - § **Alertas por nombre** muestra el número de alertas de cada elemento (como virus o aplicaciones no deseadas) detectadas en la red.
 - § **Alertas por ubicación** mostrará el número de alertas por cada

ordenador o grupo.

- § **Alertas por fecha** mostrará la tasa de alertas de virus durante un período de tiempo.
- § **Historial de alertas** muestra información completa de cada alerta.

En la ficha **Configuración**, puede personalizar el informe.

A continuación, abra las fichas **Tabla** o **Gráfico** para ver el informe.

Mostrar informes en modo de tabla

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Informes**, seleccione el tipo de informe que desea generar. En la ficha **Configuración**, configure el informe. A continuación, abra la ficha **Tabla**.
3. Se mostrará el informe en modo de tabla. En la **Descripción del informe** se resumen los parámetros utilizados para regenerar el informe (como el período analizado).

Mostrar informes en modo gráfico



El modo gráfico no está disponible para informes de 'Detalles de alertas'.

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Informes**, seleccione el tipo de informe que desea generar. En la ficha **Configuración**, configure el informe. A continuación, abra la ficha **Gráfico**.
3. Se mostrará el informe en modo gráfico. En la **Descripción del informe** se resumen los parámetros utilizados para regenerar el informe (como el período analizado).

Mostrar el número de alertas por nombre de elemento

1. Haga clic en el icono **Informes** de la barra de herramientas.

2. En el cuadro de diálogo **Informes** seleccione **Alertas por nombre**.
3. En la ficha **Configuración**, dispondrá de las opciones descritas a continuación. Tras concluir la configuración, abra la ficha **Tabla** o **Gráfico** para ver el informe.

Periodo del informe

En el cuadro de lista **Periodo**, seleccione el tiempo que desee cubrir. Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.

Ubicación

Haga clic en **Grupo de ordenadores** o en **Ordenador individual**. Después, seleccione un grupo o un ordenador en la lista desplegable.

Filtro

Por defecto, el informe mostrará todas las alertas y el número de veces que se ha producido cada una. Si lo desea, puede cambiar el tipo de alertas que se muestran por uno de los siguientes:

- § Todo (excepto aplicaciones restringidas)
- § Sólo virus/spyware
- § Sólo comportamiento sospechoso
- § Sólo archivos sospechosos
- § Sólo cortafuegos
- § Sólo adware/PUA
- § Sólo aplicaciones restringidas

También puede configurar el informe para que sólo muestre:

- § las principales n alertas (siendo n el número que usted especifique) o
- § alertas generadas m veces o más (siendo m el número que usted especifique).

Ordenar por

Por defecto, el informe mostrará las alertas en orden descendente de número de veces que se han producido. Seleccione **Nombre de la alerta** si desea la lista en orden alfabético.

Mostrar el número de alertas por ubicación

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Informes**, seleccione **Alertas por ubicación**.
3. En la ficha **Configuración**, dispondrá de las opciones descritas a continuación. Tras concluir la configuración, abra la ficha **Tabla** o **Gráfico** para ver el informe.

Periodo del informe

En el cuadro de lista **Periodo**, seleccione el tiempo que desee cubrir. Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.

Ubicación

Seleccione **Ordenadores** para mostrar las alertas por ordenador o **Grupo** para mostrar las alertas para cada grupo de ordenadores.

Filtro

Por defecto, el informe mostrará todas las alertas y el número de veces que se ha producido cada una. Si lo desea, puede cambiar el tipo de alertas que se muestran por uno de los siguientes:

- § Todo (excepto aplicaciones restringidas)
- § Sólo virus/spyware
- § Sólo comportamiento sospechoso
- § Sólo archivos sospechosos
- § Sólo cortafuegos

§ Sólo adware/PUA

§ Sólo aplicaciones restringidas

Además, puede generar un informe en el que se muestren sólo los ordenadores o grupos en los que se hayan detectado determinadas amenazas. Para especificar una alerta, selecciónela en la lista. Para especificar más de una alerta, escriba el nombre utilizando caracteres comodín. Use ? para sustituir un sólo carácter y * para sustituir toda una cadena de caracteres. Por ejemplo, W32/* incluye a todos los virus que comienzan con W32/.

Por defecto, el informe mostrará todos los ordenadores o grupos (dependiendo de la opción seleccionada en **Región**). Puede configurar el informe para mostrar sólo

§ Los principales n ordenadores o grupos que hayan generado más alertas (siendo n el número que usted indique) o

§ ordenadores o grupos con m alertas o más (siendo m el número que usted indique).

Ordenar por

Por defecto, el informe mostrará los ordenadores o grupos en orden decreciente por número de alertas. Seleccione **Ubicación** si desea la lista en orden alfabético.

Mostrar la tasa de alertas

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Informes**, seleccione **Alertas por fecha**.
3. En la ficha **Configuración**, dispondrá de las opciones descritas a continuación. Tras concluir la configuración, abra la ficha **Tabla** o **Gráfico** para ver el informe.

Periodo del informe

En el cuadro de lista **Periodo**, seleccione el tiempo que desee cubrir. Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.

Ubicación

Haga clic en **Grupo de ordenadores** o en **Ordenador individual**. Después, seleccione un grupo o un ordenador en la lista desplegable.

Filtro

Por defecto, el informe mostrará todas las alertas y el número de veces que se ha producido cada una. Si lo desea, puede cambiar el tipo de alertas que se muestran por uno de los siguientes:

- § Todo (excepto aplicaciones restringidas)
- § Sólo virus/spyware
- § Sólo comportamiento sospechoso
- § Sólo archivos sospechosos
- § Sólo cortafuegos
- § Sólo adware/PUA
- § Sólo aplicaciones restringidas

Si desea un informe sobre algún virus o tipo de alerta en particular, utilice la opción **Mostrar sólo alertas como**. Para especificar una alerta, selecciónela en la lista. Para especificar más de una alerta, escriba el nombre utilizando caracteres comodín. Use ? para sustituir un sólo carácter y * para sustituir toda una cadena de caracteres. Por ejemplo, W32/* incluye a todos los virus que comienzan con W32/.

Frecuencia de medición

Seleccione la frecuencia de medición en la lista desplegable, por ejemplo, mensual.

Mostrar historial de alertas

1. Haga clic en el icono **Informes** de la barra de herramientas.
2. En el cuadro de diálogo **Informes**, seleccione **Historial de alertas**.

3. En la ficha **Configuración**, dispondrá de las opciones descritas a continuación. Cuando haya acabado, haga clic en la ficha **Tabla** para mostrar el informe.

Periodo del informe

En el cuadro de lista **Periodo**, seleccione el tiempo que desee cubrir. Puede seleccionar los periodos de tiempo ofrecidos, como **Este mes**, o utilizar **Personalizar** para indicar las fechas de **Inicio** y **Fin**.

Ubicación

Haga clic en **Grupo de ordenadores** o en **Ordenador individual**. Después, seleccione un grupo o un ordenador en la lista desplegable.

Filtro

Por defecto, el informe mostrará todas las alertas y el número de veces que se ha producido cada una. Si lo desea, puede cambiar el tipo de alertas que se muestran por uno de los siguientes:

- § Todo (excepto aplicaciones restringidas)
- § Sólo virus/spyware
- § Sólo comportamiento sospechoso
- § Sólo archivos sospechosos
- § Sólo cortafuegos
- § Sólo adware/PUA
- § Sólo aplicaciones restringidas

Si desea un informe sobre algún virus o tipo de alerta en particular, utilice la opción **Mostrar sólo alertas como**. Para especificar una alerta, selecciónela en la lista. Para especificar más de una alerta, escriba el nombre utilizando caracteres comodín. Use **?** para sustituir un sólo carácter y ***** para sustituir toda una cadena de caracteres. Por ejemplo, **W32/*** incluye a todos los virus que comienzan con **W32/**.

Ordenar por

Por defecto, los detalles de alertas se ordenarán por **Nombre de la alerta**. Seleccione otra opción si desea ordenarlos por **Nombre del ordenador**, **Nombre del grupo** o **Fecha y hora**.

Imprimir informes

Para imprimir un informe, haga clic en el icono **Imprimir** en la barra de herramientas al visualizar el informe.



Exportar informes

Para exportar un informe:

1. Haga clic en el icono **Exportar** en la barra de herramientas al visualizar el informe.



2. En el cuadro de diálogo **Exportar informe**, seleccione el formato en el que desea guardar el informe. Las opciones son:

- § PDF (Acrobat)
- § HTML
- § Microsoft Excel
- § Microsoft Word
- § Texto enriquecido (RTF)
- § Valores separados por comas
- § XML

3. Seleccione el **Nombre de archivo** con el botón de Examinar. Escriba un nombre. Haga clic en **Aceptar**.

Cambiar el diseño del informe

Puede cambiar el diseño de la página en la que se muestran los

informes. Por ejemplo, puede mostrar los informes de forma apaisada.

1. Haga clic en el icono de diseño de página en la barra de herramientas al visualizar el informe.



2. En el cuadro de diálogo **Configurar página**, especifique el tamaño, orientación y los márgenes de la hoja. Haga clic en **Aceptar**. El informe se mostrará con la nueva configuración de página.

Esta configuración se utilizará también al imprimir o exportar el informe.

10 Solución de problemas

En esta sección se describe cómo solucionar posibles problemas con Helpdesk Console.

- [No se inicia Helpdesk Console](#)
- [Grupos que no aparecen](#)
- [Fallo de la instalación de Sophos Anti-Virus](#)
- [Los ordenadores no se actualizan](#)
- [Elemento detectado de forma parcial](#)
- [Falló la limpieza](#)
- [Recuperación tras una infección](#)
- [Recuperación de los efectos secundarios de una aplicación](#)

No se inicia Helpdesk Console

Al intentar iniciar Helpdesk Console, puede aparecer el mensaje de error "No se inicia Helpdesk Console". Esto puede ocurrir por alguna de las siguientes razones:

- No pertenece al grupo Sophos Console Administrators en el servidor donde se ejecuta Enterprise Console. Consulte con el administrador para saber si pertenece a este grupo y a Sophos DB Users.
- Todavía no se ha utilizado la herramienta de configuración de Sophos Helpdesk Console para incluir su ordenador. El administrador puede realizar esta tarea.

Grupos que no aparecen

Si no ve los grupos que debería o no ve ninguno, puede deberse a dos motivos:

- El administrador no ha configurado Helpdesk Console para que muestre los grupos.
- El administrador ha cambiado el nombre de los grupos desde que configuró Helpdesk Console.

Pídale al administrador que vuelva a configurar Helpdesk Console para poder administrar los grupos.

Fallo de la instalación de Sophos Anti-Virus

Si el Asistente para proteger ordenadores falla al instalar Sophos Anti-Virus en las estaciones, puede deberse a dos razones:

- Helpdesk Console desconoce el sistema operativo de los ordenadores. Esto puede deberse a que el administrador no introdujo el nombre de usuario en el formato dominio\usuario cuando buscó los ordenadores. El administrador tendrá que repetir el proceso, especificando el nombre de usuario de la forma dominio\usuario.
- Los ordenadores tienen activado un cortafuegos (normalmente, éste es el caso de ordenadores Windows XP SP2 y Windows Vista).
- No se ha desactivado el uso compartido simple de archivos en los ordenadores con Windows XP.

En la web de Sophos encontrará lista de requisitos para el software antivirus y cortafuegos: www.esp.sophos.com/products/all-sysreqs.html

Los ordenadores no se actualizan

Si algún ordenador tiene la protección antivirus obsoleta, aparecerá un icono de un reloj en la columna **Actualizado** en la ficha **Estado**. Se indicará el tiempo que lleva sin actualizarse.

Un ordenador puede tener una protección obsoleta por dos razones:

- El ordenador no ha podido recoger una actualización desde el servidor.
- El servidor no dispone de las últimas actualizaciones del software de Sophos.

Esta sección explica cómo identificar el problema y actualizar los ordenadores.

1. Seleccione el grupo de ordenadores.
2. En la ficha **Estado**, haga clic en la columna **Actualizado** para ordenar los equipos por la fecha en la que su protección pasó a ser obsoleta.
3. Haga clic en la ficha **Detalles de la actualización** y mire en la columna **Servidor primario**. Aquí se muestra el directorio que utiliza cada ordenador para actualizarse.
4. Observe los ordenadores que se actualizan desde un directorio en concreto.

Si algunos de ellos tienen una protección obsoleta y otros no, el problema radica en los equipos individuales. Selecciónelos, haga clic con el botón derecho y seleccione **Actualizar ordenadores ahora**.

Si todos tienen una protección obsoleta, el problema podría estar en el directorio de actualización. El administrador central podrá comprobar que el directorio de instalación dispone de la última actualización del software de seguridad de Sophos.

Elemento detectado de forma parcial

Sophos Anti-Virus podría informar de la detección parcial de algún elemento (como troyanos o aplicaciones no deseadas). Esto significa que no ha identificado todos los componentes de la aplicación.

Para identificar el resto de componentes, será necesario realizar un escaneo exhaustivo del ordenador en cuestión. En ordenadores con Sophos Anti-Virus 7 para Windows 2000/XP/2003/Vista, lo podrá hacer desde la consola: seleccione el ordenador, haga clic con el botón derecho del ratón y seleccione **Escaneo remoto**.

Si la aplicación sigue siendo detectada de forma parcial, se puede deber a lo siguiente:

- no tiene suficientes derechos de acceso
- algunas unidades o carpetas del ordenador, que contienen los componentes de la aplicación, están excluidas del escaneo.

En este último caso, consulte con su administrador central y vuelva a escanear el ordenador.

Es posible que Sophos Anti-Virus no pueda detectar o eliminar completamente programas publicitarios y aplicaciones no deseadas con componentes instalados en unidades de red.

Consulte con su administrador central.

Falló la limpieza

Si Helpdesk Console no consigue limpiar algún elemento ("Falló la limpieza"), puede deberse a varias razones:

- No ha identificado todos los componentes de un elemento multicomponente. Ejecute un escaneo exhaustivo del ordenador para identificar el resto de componentes.
- Algunas unidades o carpetas que contienen componentes del elemento son excluidas del escaneo. Consulte con su administrador central para revisar la lista.
- No tiene suficientes derechos de acceso.
- No puede limpiar ese tipo de elemento.

- En vez de obtener una correspondencia exacta del virus, ha identificado sólo un fragmento de virus.
- El elemento está en un disquete o CD-ROM protegido contra escritura.
- El elemento está en un volumen NTFS protegido contra escritura (Windows 2000 o posterior).

Recuperación tras una infección

La limpieza puede eliminar un virus del ordenador, pero no siempre puede deshacer el daño que el virus haya podido causar.

Algunos virus no tienen efectos secundarios. Otros pueden realizar cambios o corromper datos en formas que son difíciles de detectar. Para saber qué hacer ante cada caso, deberá:

- En el menú **Ayuda**, seleccione **Ver información del elemento**. Desde aquí será dirigido al sitio web de Sophos, donde podrá consultar el análisis del virus.
- Utilice copias de seguridad o copias originales de programas para sustituir programas infectados. Si no dispone de copias de seguridad, créelas para minimizar el impacto de una posible infección.

A veces es posible recuperar datos en discos dañados por un virus. Sophos proporciona herramientas para reparar el daño creado por ciertos virus. Póngase en contacto con el administrador para que le aconseje.

Recuperación de los efectos secundarios de una aplicación

La limpieza puede eliminar aplicaciones no deseadas del ordenador, pero no siempre puede deshacer el daño que hayan podido causar.

Algunas aplicaciones modifican el sistema operativo, por ejemplo cambiando la configuración de la conexión a Internet. Sophos Anti-Virus no siempre puede recuperar todos los parámetros de configuración. Por ejemplo, si una aplicación ha cambiado la página de inicio del navegador web, Sophos Anti-Virus no puede saber qué

página de inicio estaba configurada previamente.

Algunas aplicaciones instalan herramientas, como archivos .dll o .ocx, en su ordenador. Si una herramienta es inofensiva (es decir, si no posee las cualidades de una aplicación no deseada), como por ejemplo una biblioteca de idiomas, y no es integral para la aplicación, es posible que Sophos Anti-Virus no pueda detectarla como parte de una aplicación. En este caso, la limpieza no eliminará el archivo de su ordenador.

A menudo, una aplicación, como el adware, forma parte de un programa que ha instalado a propósito, y su presencia es necesaria para ejecutar el programa. Si elimina la aplicación, es posible que el programa deje de funcionar en su ordenador.

Haga lo siguiente:

- En el menú **Ayuda**, seleccione **Ver información del elemento**. Desde aquí será dirigido al sitio web de Sophos, donde podrá consultar el análisis de la aplicación.
- Utilice copias de seguridad para recuperar la configuración de su sistema o los programas que desea usar. Si no dispone de copias de seguridad, créelas para minimizar el impacto de futuros incidentes.

Para obtener más información o recomendaciones sobre cómo recuperarse de los efectos secundarios de un programa publicitario o de una aplicación no deseada, póngase en contacto con el administrador de la red.

11 Glosario

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

-A-

adware

Programa que muestra publicidad, como mensajes emergentes, y que afecta a la productividad del usuario y a la eficacia del sistema.

aplicaciones no deseadas (PUA)

Programa no malicioso en sí mismo, pero normalmente considerado inadecuado para la mayoría de redes empresariales. Las aplicaciones no deseadas realizan acciones como mostrar publicidad, controlar los sitios web visitados o cambiar la configuración de los equipos. Entre ellas, se incluyen programas maliciosos, marcadores telefónicos, herramientas de administración y ataque remoto.

aplicación restringida

Aplicación que no supone una amenaza para la seguridad, pero cuyo uso se considera inadecuado en el entorno empresarial. Entre estas aplicaciones se pueden incluir juegos, programas de mensajería instantánea, programas de voz sobre IP (VoIP), programas de fotografía digital, reproductores multimedia o complementos del navegador.

archivo sospechoso

Archivo con ciertas características propias de programas maliciosos pero sin ser suficientes para clasificarlo como tal (por ejemplo, un archivo con código de descompresión dinámica, normalmente utilizado por programas maliciosos).

^ [Subir](#)

-C-

comportamiento sospechoso

Comportamiento de una aplicación antes de ejecutarse y normalmente atribuida a programas maliciosos.

^ [Subir](#)

-D-

detección por análisis de comportamiento

Análisis dinámico del comportamiento de los programas en ejecución en el sistema, realizado por las funciones de "detección de comportamiento sospechoso" y "detección de desbordamiento de búfer".

^ [Subir](#)

-H-

HIPS (sistema de prevención contra intrusiones)

Tecnología de seguridad que protege los equipos contra archivos sospechosos, virus no identificados y comportamiento sospechoso.

^ [Subir](#)

-P-

programas espía

Programa que se instala en el equipo de otro usuario y envía información desde ese equipo a otro sin conocimiento ni autorización del usuario. Entre los programas espía se incluyen grabadores de pulsaciones del teclado, troyanos de puerta trasera, ladrones de contraseñas y gusanos de redes de bots, que pueden provocar robos de datos corporativos, pérdidas económicas y daños en las redes.

^ [Subir](#)

-R-

restricción de aplicaciones

Función de Sophos Anti-Virus que permite bloquear o autorizar la ejecución de aplicaciones, según la política de su empresa.

^ [Subir](#)

-V-

valores separados por comas

Nombre utilizado para el formato delimitado por comas, en el que los datos se separan mediante comas. Es un formato muy habitual para transferir datos de una aplicación a otra, ya que la mayor parte de sistemas de bases de datos pueden importar y exportar datos delimitados con comas. Por ejemplo, un archivo .csv puede importarse a Microsoft Excel para analizarlo.

virus

Programa que se propaga por equipos y redes adjuntándose a otros programas y creando copias de sí mismo.

virus no identificado

Virus para el que no se ha definido una identidad, desconocido.

^ [Subir](#)

Índice

A

- actualización manual 21
- actualización:manual 21
- actualizar 20
- alertas 18
- alertas de aplicaciones no deseadas 26
- alertas de aplicaciones restringidas 26
- alertas de archivos sospechosos 25
- alertas de comportamientos sospechosos 25
- alertas de programas espía 24
- alertas de programas publicitarios 26
- alertas de virus 24
- alertas del cortafuegos 25
- alertas por análisis de comportamiento 25

B

- borrar alertas 27
- borrar errores 27

C

- cortafuegos 17

D

- desinfección 27
- desinfección manual 28

- desinfección:manual 28
- detectado de forma parcial 40

E

- escaneado inmediato 22
- escaneado remoto 22
- escanear 22
- exportar informes 36

F

- fallo de la instalación de Sophos Anti-Virus 38
- fallo de la limpieza 40

G

- glosario 42
- grupo 5
- grupo de usuarios Console Administrators 37
- grupos 38
- grupos que no aparecen 38

H

- Helpdesk Console:introducción 4

I

- iconos 6
- imprimir informes 36
- informe 29

informe:diseño 36
informe:en modo de tabla 30
informe:en modo gráfico 30
informe:exportar 36
informe:generar 29
informe:historial de alertas 34
informe:imprimir 36
informe:mostrar alertas por nombre de elemento 30
informe:número de alertas por ubicación 32
informe:tasa de alertas 33
instalación manual 9
interfaz 4
interfaz gráfica de la consola 4

L

limpieza 40
limpieza manual 28
limpieza:fallo 40
limpieza>manual 28

M

mensaje de error 37

O

ordenadores actualizados 16
ordenadores con alertas 18
ordenadores desconectados 20
ordenadores no actualizados 39
ordenadores no administrados 19

ordenadores no protegidos 16
ordenadores protegidos 15
ordenar ordenadores 20

P

política 21
política antivirus y HIPS 6
política cortafuegos 6
política de actualización 6
política de grupos 21
política de restricción de aplicaciones 6
políticas de grupo:imponer 22
protección antivirus 11
proteger ordenadores 9
proteger ordenadores:con un archivo de inicio de sesión 11
proteger ordenadores:cortafuegos 13
proteger ordenadores:de forma manual 9
PUA:efectos secundarios 41

Q

quitar alertas 27
quitar errores 27

R

red protegida 14

S

símbolos de aviso 6

solución de problemas 37

V

virus:efectos secundarios 41