

SOPHOS

Sophos Endpoint Security and Control 9.5

Guía rápida de inicio

Edición: junio de 2010



Contenido

- 1 Acerca de esta guía.....3
- 2 Productos instalados.....3
- 3 Pasos clave.....3
- 4 Comprobar los requisitos del sistema.....4
- 5 Preparación de la instalación.....5
- 6 Descargar los programas de instalación.....6
- 7 Instalar Enterprise Console.....6
- 8 Descargar el software de seguridad.....7
- 9 Instalar NAC Manager.....7
- 10 Crear grupos de ordenadores.....8
- 11 Configurar políticas de seguridad.....8
- 12 Buscar ordenadores.....9
- 13 Proteger ordenadores.....9
- 14 Comprobar el estado de la red.....11
- 15 Solución de problemas.....11
- 16 Ayuda para tareas habituales.....12
- 17 Soporte técnico.....12
- 18 Aviso legal.....13

1 Acerca de esta guía

En esta guía se explica cómo proteger redes con el software de seguridad de Sophos.

Si es la primera vez que instala software de Sophos, léala.

Si va a actualizar el software, vaya al **Centro de actualizaciones de Endpoint Security and Control 9.5** en <http://esp.sophos.com/support/upgrades/>

Nota: si cuenta con una red muy grande, tenga en cuenta las opciones de instalación descritas en la *Guía avanzada de inicio de Sophos Endpoint Security and Control*.

2 Productos instalados

Se instalan dos herramientas de administración:

- **Sophos Enterprise Console.** Permite instalar y administrar software de seguridad en los equipos.
- **Sophos NAC Manager.** Permite utilizar el “control de acceso a la red”, que puede evitar el acceso de equipos no autorizados o que no cumplen los estándares de seguridad.

La instalación de NAC Manager es optativa.

Nota: las herramientas se instalan por separado mediante dos programas de instalación diferentes.

Nota: puede instalar ambas herramientas en el mismo servidor. Sin embargo, si tiene más de 1.000 equipos, es aconsejable instalar las herramientas en servidores diferentes. El procedimiento es el mismo.

3 Pasos clave

Los pasos a realizar son:

- Comprobar los requisitos del sistema.
- Preparar la instalación.
- Descargar los programas de instalación.
- Instalar Enterprise Console.
- Descargar el software de seguridad.
- Instalar NAC Manager.
- Crear grupos de ordenadores.
- Configurar políticas de seguridad.
- Buscar ordenadores.
- Proteger los equipos.

- Comprobar el estado de la red.

4 Comprobar los requisitos del sistema

Antes de comenzar la instalación, compruebe que se cumplen los requisitos de hardware y software.

4.1 Hardware y sistema operativo

Los requisitos del sistema dependen de las herramientas que instale.

Estas son algunas recomendaciones. Aquí se asume que todas las herramientas de gestión se instalan un solo servidor para administrar un máximo de 1.000 ordenadores en la red.

Es necesario acceso a Internet en todos los casos.

Nota: estos requisitos hacen referencia exclusiva a sistemas operativos de servidores. Para más información sobre los requisitos del sistema, visite

<http://esp.sophos.com/products/all-sysreqs.html>.

Sólo Enterprise Console

Procesador	Espacio en disco	Memoria	Sistema operativo
Pentium a 2 GHz o equivalente	Hasta 2 GB para la base de datos	512 MB	Windows Server 2008 R2 Windows Server 2008 (32 ó 64 bits) Windows Server 2008 Hyper-V Windows Server 2003 R2 Windows Server 2003 SP1+ (32 ó 64 bits) VMWare ESX 3.0 ó 3.5 VMWare Workstation 6.5

Enterprise Console y NAC Manager

Procesador	Espacio en disco	Memoria	Sistema operativo
Pentium a 2 GHz o equivalente	Hasta 3 GB para la base de datos	1 GB	Windows Server 2008 R2 Windows Server 2008 (32 ó 62 bit) Windows Server 2003 R2 Windows Server 2003 SP1+ (32 ó 64 bits)

4.2 Software de Microsoft

El sistema debe disponer de los siguientes componentes de Microsoft para poder instalar Enterprise Console:

- Microsoft Windows Installer versión 4.5, con el parche KB958655
- Actualización de seguridad para Microsoft XML Core Services 6.0
- Microsoft .NET Framework 3.5 SP1
- Microsoft SQL Server 2005 Express

Si no dispone de estos productos, el programa de instalación de Enterprise Console los instalará.

Notas

El programa de instalación instala SQL Server 2008 Express, a menos que disponga de SQL Server 2005 Express o posterior. SQL Server 2008 Express no es compatible con Windows Server 2003 SP1 ni Windows Essential Business Server 2008.

El programa de instalación no puede instalar .NET Framework 3.5 en Windows Server 2008 R2. Debe añadirlo desde el Administrador del servidor.

Tras instalar el software adicional, puede que tenga que reiniciar el sistema. Para más información sobre los casos en los que se debe reiniciar el sistema, vea el artículo 65190 en la base de conocimiento de Sophos

(<http://esp.sophos.com/support/knowledgebase/article/65190.html>).

5 Preparación de la instalación

En un servidor que cumpla los requisitos del sistema:

- Compruebe que cuenta con una conexión a Internet.
- Compruebe que cuenta con los CD-ROM de Windows y de los Service Packs. Puede que los necesite durante la instalación.
- Si dispone de Microsoft SQL Server 2000 o MSDE 2000 con una instancia que no sea "SOPHOS", actualícese a Microsoft SQL Server 2005.
- Si el servidor utiliza Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinicielo.

Nota: puede activarlo de nuevo después de instalar el software y descargar los productos de seguridad.

6 Descargar los programas de instalación

Descargue los programas de instalación de Sophos en el servidor en el que desea instalar las herramientas de administración.

1. Vaya a <http://esp.sophos.com/support/updates/>.
2. Escriba el nombre de usuario y la contraseña de MySophos.
3. En la página de descargas de **Endpoint Security and Data Protection**:
 - Descargue el programa de instalación de Enterprise Console.
 - Si desea utilizar NAC Manager, descargue el programa de instalación de Sophos NAC.

Si tiene intención de instalar NAC Manager en un servidor diferente al de Enterprise Console, descargue el programa de instalación en dicho servidor.

7 Instalar Enterprise Console

Para instalar Enterprise Console:

1. Inicie sesión como administrador:
 - Si el ordenador se encuentra en un dominio, inicie la sesión como administrador del dominio.
 - Si el ordenador se encuentra en un grupo de trabajo, inicie la sesión como administrador local.
2. Busque el programa de instalación de Enterprise Console que descargó antes.
Consejo: el nombre del archivo del programa de instalación incluye "sec".
3. Haga doble clic en el programa de instalación.
4. En el cuadro de diálogo del **programa de instalación en red de Sophos Endpoint Security and Control 9.5**, haga clic en **Instalar**.

Los archivos de instalación se copian en el equipo y se inicia el asistente para la instalación.

5. En el cuadro de diálogo **Sophos Enterprise Console**, haga clic en **Siguiente**.
6. Un asistente le guiará durante la instalación. Haga lo siguiente:
 - a) Utilice las opciones predeterminadas si es posible.
 - b) Seleccione la instalación **Completa**.
7. Tras la instalación puede que tenga que reiniciar el sistema. Haga clic en **Sí** o **Finalizar**.

8 Descargar el software de seguridad

Al volver a iniciar sesión o reiniciar el equipo tras la instalación, Enterprise Console se abre de forma automática y se inicia un asistente.

Nota: si utilizó Remote Desktop para la instalación, la consola no se abre automáticamente. Ábrala desde el menú Inicio.

El asistente le guiará durante la selección y descarga del software de seguridad. Haga lo siguiente:

1. En la página **Cuenta de descarga desde Sophos**, introduzca el nombre de usuario y la contraseña que aparecen impresos en el anexo de la licencia. Si utiliza un servidor proxy para acceder a Internet, active la opción **Acceder a través de un proxy**.
2. En la página **Selección de plataformas**, seleccione sólo las plataformas que necesita proteger ahora.

Al hacer clic en **Siguiente**, Enterprise Console empieza a descargar el software.

3. En la página **Descarga del software**, puede ver el progreso de la descarga. Haga clic en **Siguiente** en cualquier momento.
4. En el cuadro de diálogo **Importar ordenadores desde Active Directory**, seleccione la opción **Crear grupos de ordenadores** si desea que Enterprise Console utilice los grupos existentes de Active Directory.

Si desactivó el Control de cuentas de usuario antes de la instalación, ya puede volver a activarlo.

9 Instalar NAC Manager

Compruebe que cuenta con los CD-ROM de Windows y de los Service Packs. Puede que los necesite durante la instalación.

Nota: si instala NAC Manager en un servidor diferente al de Enterprise Console, instale primero una base de datos de SQL Server 2005 o posterior de forma manual.

1. Inicie sesión como administrador.
 - Si el ordenador se encuentra en un dominio, inicie la sesión como administrador del dominio.
 - Si el ordenador se encuentra en un grupo de trabajo, inicie la sesión como administrador local.
2. Busque el programa de instalación de Sophos NAC que descargó antes.

Consejo: el nombre del archivo del programa de instalación incluye "nac".
3. Haga doble clic en el programa de instalación.
4. En el cuadro de diálogo de **Sophos NAC Manager**, haga clic en **Instalar**.
5. Un asistente le guiará durante la instalación.

10 Crear grupos de ordenadores

Si utilizó el **asistente para la descarga de software de seguridad** para configurar los grupos de ordenadores (basados en los grupos de Active Directory), pase a la sección siguiente. Vaya a [Configurar políticas de seguridad](#) en la página 8.

Para proteger y administrar ordenadores, debe crear grupos.

1. Si Enterprise Console no está abierta, ábrala.
2. En el panel **Grupos** (en la parte izquierda de la consola), compruebe que está seleccionado el nombre del primer servidor de la lista.
3. En la barra de herramientas, haga clic en el icono **Crear grupo**.
Un "Nuevo grupo" se añadirá a la lista y se destacará su nombre.
4. Escriba un nombre para el grupo.

Para crear más grupos, vaya al panel de la izquierda. Seleccione el servidor en lo más alto para crear un grupo de primer nivel. Si desea crear un subgrupo, seleccione el grupo en el que se incluirá. Después, cree el grupo como antes.

11 Configurar políticas de seguridad

Enterprise Console aplica políticas de seguridad predeterminadas a los grupos de ordenadores. No es obligatorio modificarlas, pero:

- Deberá configurar una política cortafuegos inmediatamente.
- Para utilizar estas funciones, modifique las políticas de control de acceso a la red, restricción de aplicaciones y control de dispositivos. Puede hacerlo en cualquier momento.

11.1 Configurar una política de cortafuegos

Nota: durante la instalación del cortafuegos, se desconectarán los adaptadores de red de forma temporal. La interrupción puede provocar la desconexión de aplicaciones de red, como el Escritorio remoto.

Por defecto, el cortafuegos bloquea todas las conexiones no esenciales. Por eso, deberá configurar el cortafuegos antes de proteger los ordenadores.

1. En el panel **Políticas**, haga doble clic en **Cortafuegos**.
2. Haga doble clic en la política **Predeterminada** para modificarla. Se inicia un asistente.

3. En el **Asistente de políticas del cortafuegos**, se recomienda seleccionar las opciones siguientes.
 - a) En la página **Configurar cortafuegos**, seleccione **Ubicación única**, a menos que desee que el cortafuegos utilice una configuración diferente según la ubicación desde la que se utilice.
 - b) En la página **Modo operativo**, seleccione **Bloquear el tráfico de entrada y permitir el de salida**.
 - c) En la página **Uso compartido de archivos e impresoras**, seleccione **Permitir el uso compartido de archivos e impresoras**.

12 Buscar ordenadores

Para que Enterprise Console pueda proteger y administrar ordenadores, primero deberá buscarlos en la red.

1. Haga clic en el icono **Buscar ordenadores** de la barra de herramientas.
2. Seleccione el método que desea utilizar para buscar ordenadores.
3. Escriba los datos de la cuenta y especifique dónde quiere buscar.

Si utiliza alguna de las opciones **Buscar**, los equipos se colocan en la carpeta **No asignados**.

13 Proteger ordenadores

Para proteger equipos:

- Prepárelos.
- Proteja los ordenadores de Windows de forma automática.
- Proteja los ordenadores Windows o Mac OS X de forma manual.

13.1 Preparación para proteger ordenadores

Antes de proteger ordenadores:

Preparar la eliminación de software de terceros

Si quiere que el programa de instalación de Sophos elimine cualquier programa de seguridad instalado:

- Si los equipos cuentan con software de otros proveedores, compruebe que la interfaz está cerrada.
- Si los equipos cuentan con un cortafuegos o un producto HIPS de otro proveedor, compruebe que está desactivado o que permite la ejecución del programa de instalación de Sophos.

Si los equipos utilizan una herramienta de actualización de otro proveedor, puede que desee eliminarla. Consulte el apartado "Eliminar software de seguridad de terceros" de la sección "Proteger ordenadores" de la Ayuda de Enterprise Console.

Comprobar que tiene una cuenta que puede utilizar para instalar software

Deberá introducir los datos de una cuenta que pueda utilizar para instalar software de seguridad (como una cuenta de administrador de dominio). Deberá:

- Tener derechos de administrador local para los equipos que desee proteger.
- Poder iniciar sesión en los equipos en los que instaló Enterprise Console.
- Tener derechos de lectura en la ubicación desde la que se actualizan los ordenadores. Para comprobar la ubicación, en el panel **Políticas**, haga doble clic en **Actualización** y, a continuación, haga doble clic en **Predeterminada**.

Preparar la instalación del control de acceso a la red

Para poder instalar el control de acceso a la red:

- Especifique la dirección web del equipo en el que instaló NAC Manager. En Enterprise Console, seleccione **Herramientas** > **Configurar dirección de NAC**.

13.2 Proteger los ordenadores de Windows de forma automática

Para proteger ordenadores:

1. Seleccione los ordenadores que desea proteger.
2. Haga clic en **Proteger ordenadores**.
 - Nota:** si los equipos se encuentran en el grupo **No asignados**, arrástrelos a los grupos que desee.
3. Un asistente le guiará durante la instalación del software de seguridad de Sophos. Haga lo siguiente:
 - a) En la página **Seleccionar funciones**, puede seleccionar los productos que desee instalar. Seleccione **Control del cumplimiento** si desea disponer de control de acceso a la red.
 - b) En la página **Resumen de protección**, podrá ver cualquier problema de instalación. Si necesita ayuda, consulte [Solución de problemas](#) en la página 11.
 - c) En la página **Credenciales**, indique la cuenta que se utilizará para instalar el software en los ordenadores.

La instalación se realiza por fases, por lo que el proceso puede no completarse en todos los equipos durante algún tiempo.

Cuando termine la instalación, vuelva a mirar la lista de equipos. En la **columna En acceso**, **Activo** indica que el equipo está ejecutando el escaneo de virus en acceso.

13.3 Proteger los ordenadores Windows o Mac OS X de forma manual

Si cuenta con ordenadores que no se pueden proteger de forma automática, protéjalos ejecutando un programa de instalación desde un directorio central.

Para saber en qué directorio se encuentra el programa, abra Enterprise Console y seleccione **Ver > Ubicación de archivos de inicio**.

1. Vaya a cada uno de los ordenadores e inicie una sesión con derechos de administrador local.
2. Busque y haga doble clic en el programa de instalación del directorio de instalación central.
 - Para Windows, el programa se denomina setup.exe.
 - Para Mac OS X, el programa se denomina Sophos Anti-Virus.mpkg.
3. Un asistente le guiará durante la instalación.

14 Comprobar el estado de la red

Para comprobar el estado de la red desde Enterprise Console:

1. En la barra de menús, haga clic en el icono del **panel de control** (si no está ya a la vista).
El panel de control indica cuántos ordenadores:
 - Tienen amenazas detectadas.
 - No están actualizados.
 - No cumplen las políticas.
2. Si utiliza NAC, también puede:
 - a) Seleccionar **Archivo > Abrir > NAC**.
 - b) En NAC Manager, seleccione **Report > Compliance**.
Aquí se muestra si los ordenadores cumplen la política NAC.

15 Solución de problemas

Al ejecutar el asistente para proteger ordenadores, se pueden producir errores en la instalación del software de seguridad por diferentes motivos:

- La instalación automática no se puede realizar en ese sistema operativo. Realice una instalación manual. Consulte [Proteger los ordenadores Windows o Mac OS X de forma manual](#) en la página 11 . Para más información sobre otros sistemas operativos, consulte la *Guía avanzada de inicio de Sophos Endpoint Security and Control*.
- No se puede determinar el sistema operativo. Esto puede ocurrir si, al buscar ordenadores, no introduce su nombre de usuario con el formato dominio\usuario.

- Los equipos tienen un cortafuegos activado.

16 Ayuda para tareas habituales

En esta sección se indica dónde encontrar información para llevar a cabo tareas habituales.

SESC = Sophos Endpoint Security and Control

Tarea	Documento
Proteger equipos Linux	Guía de inicio de SESC 9.5 para Linux, NetWare y UNIX: "Proteger ordenadores Linux"
Proteger ordenadores independientes	Guía avanzada de inicio SESC 9.5: "Proteger ordenadores independientes"
Configurar antivirus y HIPS	Ayuda de Enterprise Console: "Configurar la política antivirus y HIPS"
Configurar la restricción de aplicaciones	Ayuda de Enterprise Console: "Configurar la política de restricción de aplicaciones"
Configurar el control de datos	Ayuda de Enterprise Console: "Configurar la política de control de datos"
Configurar el control de dispositivos	Ayuda de Enterprise Console: "Configurar la política de control de dispositivos"
Configurar la protección contra manipulaciones	Ayuda de Enterprise Console: "Configurar la política de protección contra manipulaciones"
Configurar NAC	Ayuda de NAC Manager: "Gestión"
Conceder acceso a la red a usuarios invitados	Guía de configuración del agente de cumplimiento de Sophos: "Agente soluble"
Alertas	Ayuda de Enterprise Console: "Alertas y errores"
Limpiar ordenadores	Ayuda de Enterprise Console: "Limpiar ordenadores"
Generar informes de SEC	Ayuda de Enterprise Console: "Generar informes"
Generar informes de NAC	Ayuda de NAC Manager: "Informes"

17 Soporte técnico

Para obtener soporte técnico sobre esta edición beta:

1. Complete el formulario online de comentarios (la dirección se incluye en el mensaje que Sophos le envió) y envíelo al equipo de soporte técnico.
2. Acceda al fórum Sophos Beta (la dirección y detalles se incluye en el mensaje que Sophos le envió) para buscar casos similares.
3. Si necesita ayuda con los pasos anteriores, escríbanos a betaprogram@sophos.com.

18 Aviso legal

Copyright © 2010 Sophos Group. Reservados todos los derechos. 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 Plc y Sophos Group. Todos los demás nombres de productos o empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.

El software de Sophos descrito en este documento incluye o puede incluir software bajo licencia (o sublicencia) Common Public License (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 el usuario. 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 correo, por email a support@sophos.com o por Internet desde <http://esp.sophos.com/support/queries/enterprise.html>. Puede encontrar una copia de los términos de licencia en <http://opensource.org/licenses/cpl1.0.php>