

# SOPHOS

## Sophos Endpoint Security and Control 9.5 Guía avanzada de inicio para Windows y Mac OS X

Edición: junio de 2010



# Contenido

- 1 Acerca de esta guía.....3
- 2 Planificar la instalación.....4
- 3 Requisitos del sistema.....8
- 4 Dónde instalar las herramientas administrativas.....9
- 5 Instalar las herramientas administrativas con las bases de datos en un servidor diferente.....13
- 6 Instalar las herramientas administrativas con un gestor de actualización adicional en un servidor diferente.....24
- 7 Publicar el software de seguridad en un servidor web.....40
- 8 Crear grupos de ordenadores.....41
- 9 Configurar políticas de seguridad.....42
- 10 Buscar ordenadores.....46
- 11 Proteger ordenadores Windows y Mac.....47
- 12 Comprobar el estado de la red.....52
- 13 Proteger ordenadores independientes.....53
- 14 Soporte técnico.....54
- 15 Aviso legal.....55

## 1 Acerca de esta guía

En esta guía se describe el procedimiento avanzado para la instalación del software de Sophos Endpoint Security and Control en redes complejas o que cuenten con más de 1.000 estaciones. Cubre la instalación en Windows y Mac.

Para realizar la instalación en una red sencilla de menos de 1.000 estaciones Windows y Mac, consulte la *Guía rápida de inicio de Sophos Endpoint Security and Control 9.5*.

Para realizar la instalación en estaciones Linux, NetWare o UNIX, además de esta guía debe consultar también la *Guía de inicio de Sophos Endpoint Security and Control 9.5 para Linux, NetWare y UNIX*.

Para la actualización, visite el **Centro de actualizaciones para Endpoint Security and Control 9.5** en <http://esp.sophos.com/support/upgrades/>.

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

## 2 Planificar la instalación

Para proteger los ordenadores, es necesario seguir estos pasos:

1. Instalar las herramientas de administración de Sophos.
2. Publicar el software de seguridad en un servidor web, si lo desea.
3. Crear grupos de ordenadores.
4. Establecer las políticas de seguridad para esos grupos.
5. Buscar los ordenadores en la red y ponerlos en los grupos.
6. Proteger los equipos.
7. Comprobar el estado de la red.
8. Proteger los ordenadores independientes.

**Nota:** si utiliza Active Directory, algunos pasos se pueden realizar de forma automática.

Esta sección le ayudará a tomar decisiones en cada etapa.

### 2.1 Planificar la instalación de herramientas de administración

Las herramientas administrativas de Sophos son:

- **Sophos Enterprise Console (SEC).** Permite instalar y administrar software de seguridad en los equipos.
- **Servidor de Sophos NAC.** 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.

**Importante:** se recomienda que los servidores en los que se instala SEC estén en el mismo bosque de Active Directory que en los que se instala el servidor NAC.

#### 2.1.1 Planificar la instalación de Enterprise Console

Sophos Enterprise Console incluye cuatro componentes:

<b>Consola de administración</b>	Para proteger y administrar los equipos.
<b>Servidor de administración</b>	Para la actualización y funciones de comunicación.
<b>Base de datos</b>	Para el almacenamiento de datos.
<b>Gestor de actualización</b>	Para la descarga de software y actualizaciones de Sophos de forma automática en una ubicación central.

**Importante:** si instala los componentes en diferentes servidores, se recomienda que los servidores se encuentren en el mismo dominio.

## Consola de administración

Si lo desea, puede instalar otra instancia de la consola de administración en otro servidor para administrar las estaciones en red más cómodamente, dependiendo de cómo desee configurar el acceso administrado a la consola y cómo quiera dividir el entorno informático en subentornos:

- Para un *acceso administrado* a la consola de administración, es necesario configurar roles, agregarles derechos y asignar usuarios y grupos de Windows a dichos roles. Por ejemplo, un técnico de soporte puede actualizar y limpiar ordenadores, pero no puede configurar políticas, de lo que es responsable el administrador.
- Los *subentornos* se pueden utilizar para restringir los equipos y grupos en los que los usuarios pueden realizar operaciones. El entorno informático se puede dividir en subentornos, a los que se asignan grupos de equipos de la consola de administración. De esta forma, es posible controlar el acceso a los subentornos mediante la asignación de usuarios y grupos de Windows a los mismos. El subentorno predeterminado contiene todos los grupos de la consola de administración y el grupo **No asignados**.

En esta guía se explica cómo instalar una consola de administración adicional. Para más información sobre la configuración del acceso administrado y la creación de subentornos, vaya a <http://esp.sophos.com/support/bestpractice/esc>.

## Base de datos

La base de datos se puede instalar en otro servidor si:

- Necesita más espacio.
- Cuenta con un servidor SQL Server dedicado.
- Desea repartir la carga de procesos entre varios servidores.

En esta guía se explica cómo instalar la base de datos en el mismo servidor que el resto de componentes de Enterprise Console o en el mismo servidor que las bases de datos de NAC.

## Gestor de actualización

El gestor de actualización permite crear unidades compartidas que contengan el software que desea distribuir en las estaciones. Los ordenadores que desee proteger se actualizan desde estas unidades compartidas. Al instalar Enterprise Console, se instala siempre un gestor de actualización. Pero, si lo desea, puede instalar gestores de actualización adicionales en otros servidores y crear unidades compartidas adicionales para descargar y distribuir el software en redes más grandes. En esta guía se explica cómo instalar un gestor de actualización adicional y cómo crear unidades compartidas. Para más información sobre la organización de administradores de actualización y unidades compartidas en grandes redes, vaya a <http://esp.sophos.com/support/bestpractice/esc>.

### 2.1.2 Planificar la instalación del servidor NAC

Si desea utilizar Sophos Network Access Control (NAC), deberá instalar el servidor NAC. Está formado por dos componentes:

<b>Sophos NAC Manager</b>	Permite administrar y configurar NAC en la red.
<b>Bases de datos de Sophos NAC</b>	Almacenan datos de NAC sobre la red, que pueden visualizarse con NAC Manager.

**Importante:** si instala los componentes en diferentes servidores, los servidores deben compartir el mismo dominio.

Las bases de datos se pueden instalar en otro equipo si:

- Necesita más espacio.
- Cuenta con un servidor SQL Server dedicado.
- Desea repartir la carga de procesos entre varios equipos.

Las tablas siguientes contienen los tamaños aproximados de las bases de datos:

Número de estaciones	Tamaño de ReportStore
1.500	300 MB
3.000	379 MB
5.000	485 MB
7.500	616 MB
10.000	748 MB
15.000	1011 MB
20.000	1274 MB
25.000	1536 MB

Número de estaciones	Tamaño del registro de ReportStore
1.500	150 MB
3.000	206 MB
5.000	281 MB
7.500	374 MB
10.000	467 MB
15.000	653 MB
20.000	839 MB
25.000	1024 MB

En esta guía se explica cómo instalar las bases de datos en el mismo servidor que NAC Manager o en el mismo servidor que la base de datos de Enterprise Console.

NAC es compatible con la comunicación HTTPS entre el servidor NAC y Sophos Compliance Agent. El agente de cumplimiento se instala en las estaciones y comprueba que cumplen las políticas. Si desea activar HTTPS con NAC, póngase en contacto con el soporte técnico de Sophos. Para más información sobre cómo ponerse en contacto con el soporte técnico, consulte [Soporte técnico](#) en la página 54. Hágalo antes de empezar la instalación.

## 2.2 Planificar los grupos de ordenadores

Decida cómo desea agrupar los ordenadores que va a proteger. Para más información, vaya a <http://esp.sophos.com/support/bestpractice/esc>.

## 2.3 Planificar las políticas de seguridad

Una *política de seguridad* es un conjunto de parámetros que pueden aplicarse a los ordenadores de un grupo.

Al crear grupos, Enterprise Console les aplica las políticas predeterminadas. Si lo desea, puede modificar estas políticas o crear políticas nuevas, según se explica en esta guía. Para más información sobre qué configuración utilizar, consulte la *Guía de configuración de Sophos Endpoint Security and Control 9.5*.

## 2.4 Planificar la búsqueda de ordenadores en red

Para poder instalar el software de seguridad en ordenadores en red, es necesario añadirlos a la lista de ordenadores de Enterprise Console. Para más información sobre cómo buscar ordenadores para añadirlos a la lista de ordenadores, consulte la Ayuda de Enterprise Console.

## 2.5 Planificar la protección de ordenadores

Puede instalar el software de seguridad de forma automática desde Enterprise Console en estaciones con Windows 2000 o posterior.

**Nota:** no es posible instalar Sophos Client Firewall ni Sophos Compliance Agent en un sistema operativo de servidor.

Si dispone de otros sistemas operativos en su red, deberá instalar el software de forma manual o usando scripts, o mediante otro método (como Active Directory). En esta guía se describe el proceso de instalación manual en los siguientes sistemas operativos:

- Windows
- Mac OS X

Para otros sistemas operativos, consulte la *Guía de inicio de Sophos Endpoint Security and Control 9.5 para Linux, NetWare y UNIX*.

### 3 Requisitos del sistema

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 Edition

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

Antes de instalar las bases de datos de NAC, compruebe que tiene instalada la versión adecuada del servidor SQL:

- Para redes de hasta 1.500 estaciones, se recomienda utilizar SQL Server 2005/2008 Express. Estas bases de datos están limitadas a 4 GB.
- Para redes de más de 1.500 estaciones, se recomienda utilizar SQL Server 2005/2008.

Para ver los requisitos del sistema de Sophos Enterprise Console y Sophos Network Access Control, consulte las notas de la edición de dichos productos.

Para otros productos, visite la página de requisitos del sistema en el sitio web de Sophos (<http://esp.sophos.com/products/all-sysreqs.html>).

#### 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. En Windows Server 2008 R2 Datacenter, debe subir el nivel funcional del dominio a Windows Server 2003, como se describe en <http://support.microsoft.com/kb/322692>.

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>).

## 4 Dónde instalar las herramientas administrativas

Las herramientas de administración de Sophos son Sophos Enterprise Console (SEC) y el servidor NAC.

SEC incluye cuatro componentes:

<b>Consola de administración</b>	Para proteger y administrar los equipos.
<b>Servidor de administración</b>	Para la actualización y funciones de comunicación.
<b>Base de datos</b>	Para el almacenamiento de datos.
<b>Gestor de actualización</b>	Para la descarga de software y actualizaciones de Sophos de forma automática en una ubicación central.

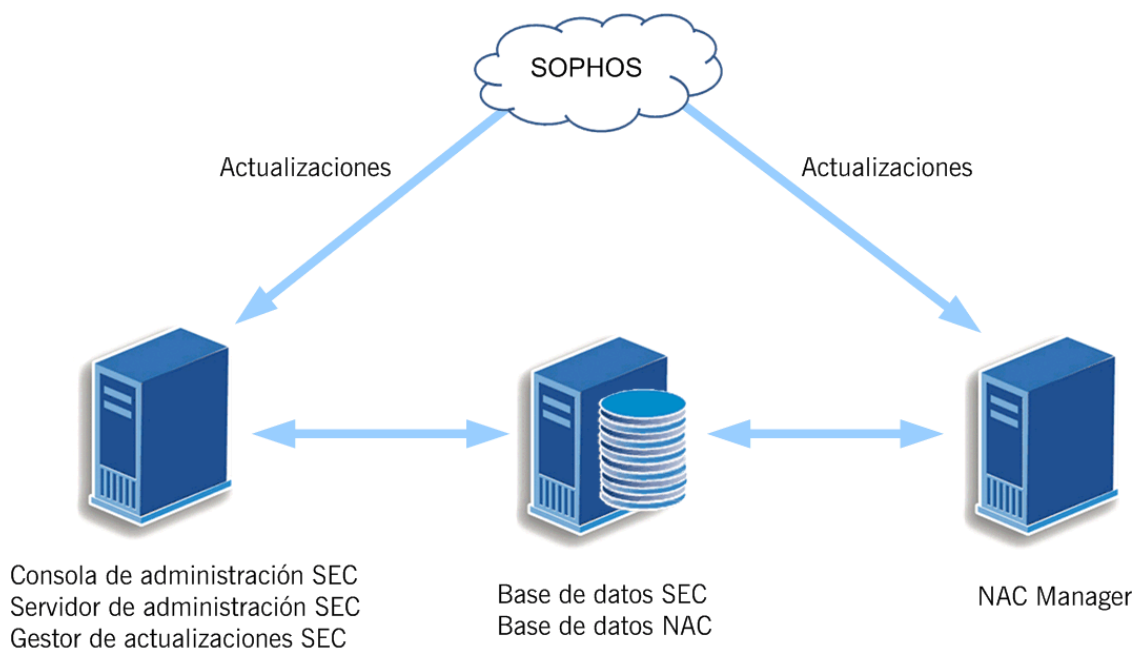
El servidor NAC incluye dos componentes:

<b>Sophos NAC Manager</b>	Permite administrar y configurar NAC en la red.
<b>Bases de datos de Sophos NAC</b>	Almacenan datos de NAC sobre la red, que pueden visualizarse con NAC Manager.

**Nota:** si no desea utilizar el control de acceso a la red, no es necesario que instale los componentes de servidor NAC.

En esta guía se describen dos situaciones de instalación. En cada una de ellas, los componentes de las herramientas administrativas se distribuyen a la red de forma diferente.

### Bases de datos instaladas en otro servidor



**Nota:** los servidores en los que se instalan las bases de datos de NAC y NAC Manager deben estar vinculados al mismo dominio.

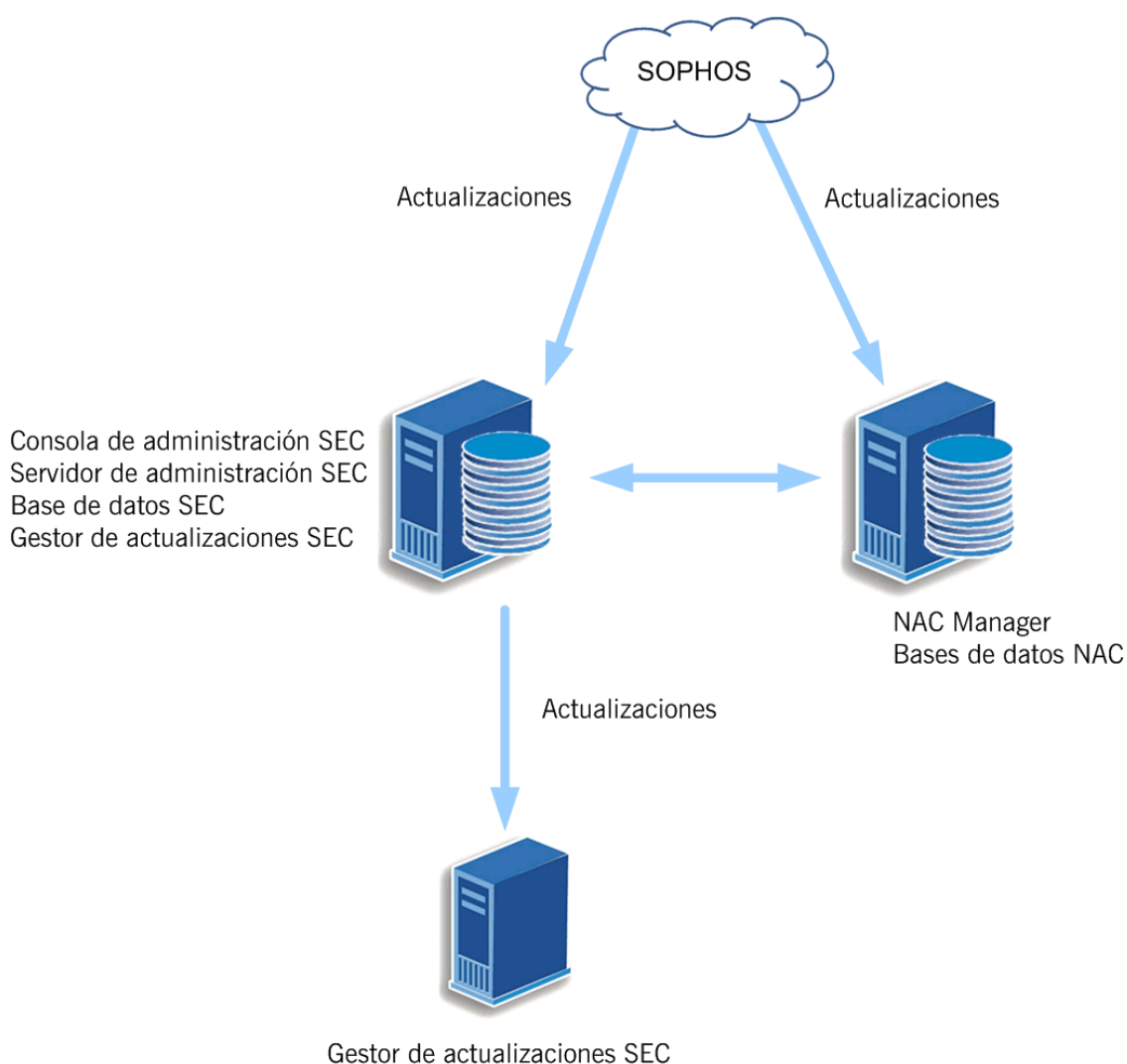
Para seguir las instrucciones para esta situación, consulte [Instalar las herramientas administrativas con las bases de datos en un servidor diferente](#) en la página 13.

### Gestor de actualización adicional instalado en otro servidor

En esta situación, las fuentes de actualización de los gestores de actualización se pueden configurar de dos formas.

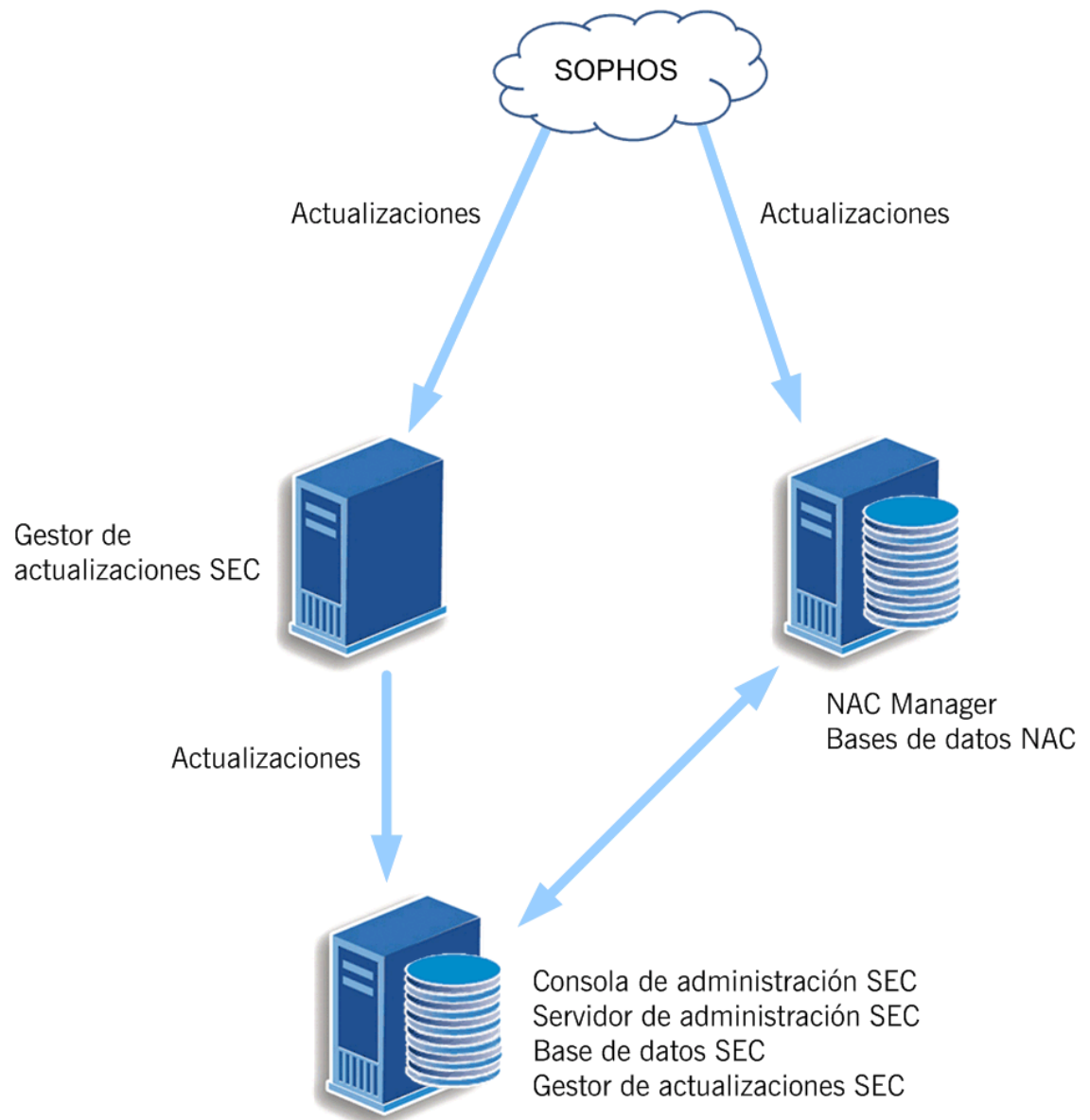
El primer método consiste en:

- Configurar el gestor de actualización principal instalado con la consola SEC para que se actualice directamente desde Sophos.
- Configurar el gestor de actualización adicional para que se actualice desde el gestor de actualización principal.



El segundo método consiste en:

- Configurar el gestor de actualización adicional para que se actualice directamente desde Sophos.
- Configurar el gestor de actualización principal instalado con la consola SEC para que se actualice desde el gestor de actualización adicional.



Independientemente del método que elija, en una situación como esta, consulte [Instalar las herramientas administrativas con un gestor de actualización adicional en un servidor diferente](#) en la página 24.

## 5 Instalar las herramientas administrativas con las bases de datos en un servidor diferente

### 5.1 Descargar los programas de instalación

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.
4. Descargue el programa de instalación de NAC Manager.
5. Descargue el programa de instalación de Sophos Compliance Dissolvable Agent.
6. Compruebe que se puede acceder a los programas de instalación desde los servidores en los que quiere instalar el software.  
Si lo prefiere, puede copiarlos en un CD-ROM o DVD.

### 5.2 Instalar las bases de datos de NAC

El asistente de instalación de NAC le guiará durante la instalación de los requisitos del sistema de NAC. Durante la instalación de NAC, tenga a mano el CD-ROM del sistema operativo correspondiente para instalar determinados requisitos del sistema. El asistente de instalación de NAC instala de forma automática otros requisitos.

1. En el controlador del dominio, cree una cuenta estándar de dominio en la que la contraseña no caduca y el usuario no la puede cambiar.  
El asistente para la instalación de NAC añade esta cuenta al grupo de administradores locales del servidor de NAC Manager para que NAC Manager pueda acceder a las bases de datos de NAC.
2. Vaya al servidor en el que desea instalar las bases de datos.
3. Haga doble clic en el programa de instalación de NAC que descargó anteriormente.  
Se inicia el asistente para la instalación.
4. Haga clic en **Install**.
5. En la página de **bienvenida**, haga clic en **Next**.
6. En el cuadro de diálogo **Select Features**, haga clic en **Advanced**.
7. Desactive todas las opciones y active la opción **Sophos NAC Databases**. Haga clic en **Next**.  
Si desea cambiar la carpeta en la que se instalan los scripts que crean las bases de datos de NAC, haga clic en **Browse**. Si desea cambiar la instancia del servidor SQL que utilizará NAC, haga clic en **Select**. Este botón sólo aparecerá si el programa de instalación de NAC detecta más de una instancia del servidor SQL.

8. En el cuadro de diálogo **Service Account Information**, escriba los datos de la cuenta del servicio en los campos correspondientes. Haga clic en **Next**.  
Esta es la cuenta de dominio necesaria para las bases de datos de NAC y NAC Manager. Esta cuenta de servicio se creó en el paso 1.
9. En el cuadro de diálogo **Sophos Download Account Details**, introduzca los datos de la cuenta de descargas de Sophos en los campos correspondientes. Haga clic en **Next**.  
Los datos de la cuenta de descargas de Sophos se proporcionan al adquirir Sophos NAC. El nombre de usuario y la contraseña son necesarios para descargar los datos más recientes de detección para las aplicaciones de seguridad. Si se equivoca al introducir los datos, puede corregirlos más tarde con NAC Manager. Para más información, consulte la Ayuda de NAC Manager.
10. En el cuadro de diálogo **Ready to Install**, haga clic en **Install** para que empiece la instalación.  
Aparece la barra de evolución de la instalación y configuración de las bases de datos de NAC. Ciertas tareas durante la instalación pueden tardar bastante y la barra de evolución no se moverá. No cancele la instalación.
11. Haga clic en **Finish**.  
**Importante:** si se produce algún error durante la instalación, consulte el registro de eventos de la aplicación. Si falla la instalación de las bases de datos, deberá borrar las siguientes bases de datos: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore y SecurityStore. Tras borrar las bases de datos podrá volver a intentar la instalación.

## 5.3 Cambiar el tamaño de las bases de datos de NAC

En las instalaciones de hasta 1.500 estaciones, el proceso de instalación de NAC ajusta de forma automática el tamaño de las bases de datos de NAC. Puede pasar a la sección siguiente.

En las instalaciones de más estaciones, es necesario aumentar el tamaño de las bases de datos de NAC: la base de datos ReportStore y el registro de ReportStore, como se explica en esta sección.

### 5.3.1 Guía para establecer el tamaño de las bases de datos ReportStore

Utilice esta tabla como guía para establecer el tamaño de la base de datos ReportStore.

Número de estaciones	Tamaño de ReportStore
1.500	300 MB
3.000	379 MB
5.000	485 MB
7.500	616 MB
10.000	748 MB

Número de estaciones	Tamaño de ReportStore
15.000	1011 MB
20.000	1274 MB
25.000	1536 MB

### 5.3.2 Guía para establecer el tamaño de los registros de ReportStore

Utilice esta tabla como guía para establecer el tamaño del registro de ReportStore.

Número de estaciones	Tamaño del registro de ReportStore
1.500	150 MB
3.000	206 MB
5.000	281 MB
7.500	374 MB
10.000	467 MB
15.000	653 MB
20.000	839 MB
25.000	1024 MB

### 5.3.3 Cambiar el tamaño de la base de datos de NAC: SQL Server 2005/2008

1. En el menú **Inicio** de SQL Server, señale **Microsoft SQL Server 2005** o **Microsoft SQL Server 2008** y haga clic en **SQL Server Management Studio**.
2. En SQL Server Management Studio, haga clic con el botón derecho en la base de datos ReportStore de la carpeta Databases y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades**, seleccione **Archivos**.
4. Busque el archivo ReportStore\_Data. En el campo **Tamaño inicial (MB)** indique el tamaño deseado para la base de datos.
5. Busque el archivo ReportStore\_Log. En el campo **Tamaño inicial (MB)** indique el tamaño deseado para el registro.
6. Haga clic en **Aceptar**.
7. Cierre SQL Server Management Studio.

## 5.4 Instalar la base de datos de SEC

La base de datos de SEC se instala en el mismo servidor donde instaló las bases de datos de NAC.

Si el servidor utiliza Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinícielo. Puede activarlo de nuevo después de instalar la base de datos.

Si el servidor se encuentra en un *dominio*, inicie la sesión como administrador del dominio.

Si el servidor se encuentra en un *grupo de trabajo*, inicie la sesión como administrador local.

1. Haga doble clic en el programa de instalación del Enterprise Console que descargó anteriormente.
2. Extraiga los archivos de instalación en la carpeta de destino sugerida o en otra que prefiera. La carpeta debe encontrarse en el propio ordenador.

Se inicia el asistente para la instalación.

3. En el cuadro de diálogo **Sophos Enterprise Console**, haga clic en **Siguiente**.

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

En el cuadro de diálogo **Tipo de instalación**, seleccione **Personalizada**.

En el cuadro de diálogo **Instalación personalizada**, compruebe que está seleccionada la opción **Base de datos**, pero no **Consola de administración** ni **Servidor de administración**.

En la página **Datos de la cuenta de conexión a la base de datos**, utilice una cuenta que con acceso a este servidor y al servidor en el que instaló el servicio de administración de Enterprise Console. Si los servidores se encuentran en un *dominio*, utilice una cuenta de dominio. Si los servidores se encuentran en un *grupo de trabajo*, utilice una cuenta local que exista en ambos servidores.

Cuando se complete el asistente de instalación de Enterprise Console, reinicie el servidor si así se indica.

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

## 5.5 Instalar NAC Manager

Vaya al servidor en el que desea instalar NAC Manager. Compruebe que está conectado a Internet.

Inicie sesión con una cuenta de dominio con permisos de administrador local.

El asistente de instalación de NAC le guiará durante la instalación de los requisitos del sistema de NAC. Durante la instalación de NAC, tenga a mano el CD-ROM del sistema operativo correspondiente para instalar determinados requisitos del sistema. El asistente de instalación de NAC instala de forma automática otros requisitos.

1. Haga doble clic en el programa de instalación del NAC que descargó anteriormente.

Se inicia el asistente para la instalación.

2. Haga clic en **Install**.
3. En la página de **bienvenida**, haga clic en **Next**.
4. Después, siga uno de los procedimientos siguientes:
  - Si aparece un mensaje para indicar que el servidor de NAC es el único servidor NAC que se puede instalar, haga clic en **OK**. En el cuadro de diálogo **Select Features**, haga clic en **Next**.
  - Si aparece el cuadro de diálogo **Select Features** directamente, haga clic en **Advanced**. Desactive todas las opciones y active la opción **Sophos NAC Application Server**. Haga clic en **Next**.

Si desea modificar la carpeta en la que se instalarán los archivos de NAC Manager, haga clic en **Browse**.
5. En el cuadro de diálogo **Service Account Information**, escriba los datos de la cuenta del servicio en los campos correspondientes. Haga clic en **Next**.

Esta es la cuenta de dominio necesaria para las bases de datos de NAC y NAC Manager. La cuenta del servicio se creó durante el primer paso de la instalación de las bases de datos de NAC.
6. En el cuadro de diálogo **Sophos Database Server**, escriba el nombre del servidor de la base de datos de NAC. Haga clic en **Next**.

Si cambió la instancia del servidor SQL que utilizará NAC al instalar las bases de datos de NAC, introduzca también el nombre de la instancia, con este formato:

```
servidor\instancia
```
7. En la página **Server Proxy Settings**, si utiliza un servidor proxy para acceder a Internet, haga clic en **Use Proxy**. Puede utilizar el mismo proxy que para Enterprise Console. Haga clic en **Next**.

El nombre de usuario y la contraseña son obligatorios cuando NAC Manager utiliza un proxy autenticado.
8. En la página **Ready to Install**, haga clic en **Install** para que empiece la instalación.

NAC Manager se configura y aparece el progreso de la instalación. Ciertas tareas durante la instalación pueden tardar bastante y la barra de evolución no se moverá. No cancele la instalación.
9. Haga clic en **Finish**.

**Nota:** si se produce algún error durante la instalación, consulte el registro de eventos de la aplicación.

## 5.6 Instalar el agente soluble de cumplimiento en un servidor web

Sophos Compliance Dissolvable Agent es un componente de NAC que evalúa el cumplimiento de las estaciones. Está diseñado para los usuarios que no tienen instalado Sophos Compliance Agent, como trabajadores temporales o invitados. Para usarlo, es necesario instalar primero el agente soluble de cumplimiento en un servidor web de Windows al que puedan acceder los usuarios. Una vez instalado, los usuarios descargan el agente soluble de cumplimiento desde un navegador.

**Nota:** si lo desea, puede instalarlo en el mismo servidor en el que instaló NAC Manager o las bases de datos de NAC.

1. Haga doble clic en el programa de instalación del agente soluble de cumplimiento que descargó anteriormente.  
Se inicia el asistente para la instalación.
2. En la página de **bienvenida**, haga clic en **Next**.
3. En el cuadro de diálogo **Destination Folder**, conserve la carpeta predeterminada o haga clic en **Change** para seleccionar una carpeta diferente para la instalación. Haga clic en **Next**.
4. En el cuadro de diálogo **Sophos Server**, escriba la dirección IP o el nombre del DNS del servidor en el que instaló NAC Manager.

**Nota:** si cambia la dirección del servidor de NAC Manager más adelante, deberá volver a instalar el agente soluble de cumplimiento en el servidor web y especificar la dirección nueva durante la instalación.

5. Si utiliza HTTPS con NAC, seleccione la opción **Secure Sophos Server (use HTTPS)**.  
La dirección IP o nombre del DNS del certificado web debe ser la misma que la del servidor de NAC Manager.
6. Haga clic en **Next**.
7. En el cuadro de diálogo **Ready to Install**, haga clic en **Install** para que empiece la instalación.
8. Haga clic en **Finish**.

**Nota:** si se produce algún error durante la instalación, consulte el registro de eventos de la aplicación.

Si instala el agente soluble de cumplimiento en la carpeta predeterminada, las estaciones pueden acceder con la dirección siguiente: `http(s)://dirección IP o nombre DNS/agentesoluble`. La dirección IP o nombre DNS corresponde al servidor donde instaló el agente soluble de cumplimiento. Por ejemplo:

```
http://www.ejemplo.com/agentesoluble  
https://192.0.2.0/agentesoluble
```

## 5.7 Instalar SEC: consola de administración, servidor de administración, gestor de actualización

Vaya al servidor en el que instaló la consola de administración, el servidor de administración y el gestor de actualización de Enterprise Console. Compruebe que está conectado a Internet.

Para permitir que la consola se comuniquen con las estaciones administradas, abra los puertos 8192 y 8194 del servidor. Para permitir que el gestor de actualización descargue software de seguridad desde Sophos, abra el puerto 80 del servidor.

El nombre de este equipo debe ser diferente al del resto de servidores en los que instale el gestor de actualización.

Si el servidor utiliza Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinícelo. Puede volver a activarlo después de instalar Enterprise Console y suscribirse a las actualizaciones de Sophos.

Si el servidor se encuentra en un *dominio*, inicie la sesión como administrador del dominio.

Si el servidor se encuentra en un *grupo de trabajo*, inicie la sesión como administrador local.

1. Haga doble clic en el programa de instalación del Enterprise Console que descargó anteriormente.
2. Extraiga los archivos de instalación en la carpeta de destino sugerida o en otra que prefiera. La carpeta debe encontrarse en el propio ordenador.

Se inicia el asistente para la instalación.

3. En el cuadro de diálogo **Sophos Enterprise Console**, haga clic en **Siguiente**.

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

En el cuadro de diálogo **Tipo de instalación**, seleccione **Personalizada**.

En el cuadro de diálogo **Instalación personalizada**, compruebe que están seleccionadas las opciones **Consola de administración** y **Servidor de administración**, pero no **Base de datos**.

En el cuadro **Detalles de la base de datos**, introduzca la ubicación y el nombre de la base de datos de Enterprise Console que creó en el otro servidor.

En la página **Datos de la cuenta de conexión a la base de datos**, utilice una cuenta que con acceso a este servidor y al servidor en el que instaló la base de datos de Enterprise Console. Si los servidores se encuentran en un *dominio*, utilice una cuenta de dominio. Si los servidores se encuentran en un *grupo de trabajo*, utilice una cuenta local que exista en ambos servidores.

Cuando termine la instalación, cierre la sesión o reinicie el servidor (indicado en el último cuadro de diálogo del asistente). Al volver a iniciar sesión, Enterprise Console se abre de forma automática y se inicia el asistente para descargar el software de seguridad. Cancelelo y ejecútelo más adelante, cuando se indique en esta guía.

## 5.8 Instalar una consola de administración de SEC adicional

Si lo desea, puede instalar otra instancia de la consola de administración en otro servidor para administrar las estaciones en red más cómodamente. Si no, pase a la sección siguiente.

Si el servidor utiliza Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinícelo. Puede activarlo de nuevo después de instalar la consola de administración.

Si el servidor se encuentra en un *dominio*, inicie la sesión como administrador del dominio.

Si el servidor se encuentra en un *grupo de trabajo*, inicie la sesión como administrador local.

1. Haga doble clic en el programa de instalación del Enterprise Console que descargó anteriormente.

2. Extraiga los archivos de instalación en la carpeta de destino sugerida o en otra que prefiera. La carpeta debe encontrarse en el propio ordenador.

Se inicia el asistente para la instalación.

3. En el cuadro de diálogo **Sophos Enterprise Console**, haga clic en **Siguiente**.

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

En el cuadro de diálogo **Tipo de instalación**, seleccione **Personalizada**.

En el cuadro **Instalación personalizada**, compruebe que está seleccionada **Consola de administración**, pero no **Servidor de administración** ni **Base de datos**.

En el cuadro **Servidor de administración**, escriba el nombre del servidor en el que instaló el servidor de administración SEC.

Cuando termine el asistente, cierre la sesión o reinicie el servidor (según se indique al final del asistente). Al volver a iniciar sesión, Enterprise Console se abre de forma automática. Si se inicia el asistente para descargar el software de seguridad, ciérrelo.

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

Para permitir a otros usuarios el control de la nueva consola de administración:

- Añada los usuarios a los grupos Sophos Console Administrators y Distributed COM Users en el ordenador donde ha instalado la consola de administración.
- Asigne a cada usuario algún subentorno de Enterprise Console.

Para poder crear informes, usuario debe pertenecer también al grupo Sophos DB Users en el servidor con la base de datos de Enterprise Console.

## 5.9 Crear un directorio para Sophos Anti-Virus para NetWare

Para proteger servidores de NetWare, es necesario crear un directorio en el que el gestor de actualización colocará el software más reciente de Sophos Anti-Virus para NetWare, en cada servidor de NetWare que quiera proteger.

Para crear un directorio para Sophos Anti-Virus para NetWare:

1. En un equipo de Windows con software de administrador de NetWare, o en uno de los servidores de Netware que desee proteger, cree el directorio `\\servidor de NetWare\SYS\SWEET\NLMINST` siendo *servidor de NetWare* el nombre del servidor de Netware.
2. Comparta el directorio para que puedan acceder a él todos los servidores en los que ha instalado un gestor de actualización.
3. Repita el procedimiento en todos los servidores de NetWare que desee proteger.

La instalación de Sophos Anti-Virus en NetWare se describe en la *Guía de inicio de Sophos Endpoint Security and Control 9.5 para Linux, NetWare y UNIX*.

## 5.10 Descargar software de seguridad

Para descargar software de seguridad en una ubicación central para distribuirla a las estaciones, es necesario configurar el gestor de actualización instalado. Siga uno de estos dos métodos.

La sección [Configurar el gestor de actualización de forma automática](#) en la página 21 describe cómo ejecutar el asistente que permite descargar:

- Sólo la versión más reciente.
- Sólo las subcarpetas de la unidad compartida `\\servidor\SophosUpdate`, siendo *servidor* el servidor en el que está instalado el gestor de actualización.

La sección [Configurar el gestor de actualización de forma manual](#) en la página 22 describe cómo configurar el gestor de actualización directamente para poder descargar:

- Versiones anteriores.
- A otras unidades compartidas, como en otros servidores.

**Nota:** utilice este método para descargar Sophos Anti-Virus para NetWare.

Para más información sobre otros tipos de versiones disponibles, consulte la sección sobre la configuración de suscripciones de la Ayuda de Enterprise Console.

### 5.10.1 Configurar el gestor de actualización de forma automática

1. En Enterprise Console, en el menú **Acciones**, haga clic en **Asistente para descargar el software de seguridad**.
2. 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**.
3. En la página **Selección de plataformas**, seleccione las plataformas que desea proteger.  
Al hacer clic en **Siguiente**, Enterprise Console empieza a descargar el software.
4. En la página **Descarga del software**, puede ver el progreso de la descarga. Haga clic en **Siguiente** en cualquier momento.
5. 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.

**Nota:** si un equipo se añade a más de un contenedor de Active Directory, se intercambiarán mensajes continuamente entre el equipo y Enterprise Console.

El software seleccionado se descarga en la unidad compartida `\\servidor\SophosUpdate`, siendo *servidor* el nombre del servidor en el que está instalado el gestor de actualización.

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

Ahora, configure el gestor de actualización de forma manual, si es necesario. A continuación, vaya a [Publicar el software de seguridad en un servidor web](#) en la página 40.

## 5.10.2 Configurar el gestor de actualización de forma manual

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

1. En Enterprise Console, en el menú **Ver**, seleccione **Gestores de actualización**.
2. Si *no* ha configurado el gestor de actualización de forma automática, configúrelo para que utilice Sophos como fuente de actualización:
  - a) En el panel **Gestores de actualización**, seleccione el gestor de actualización que está instalado en este servidor. Haga clic con el botón derecho y seleccione **Ver/editar configuración**.
  - b) En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Fuentes**, haga clic en **Añadir**.
  - c) En el cuadro de diálogo **Detalles de la fuente**, en el cuadro **Dirección**, seleccione **Sophos**. En los cuadros **Nombre de usuario** y **Contraseña**, escriba las credenciales de descarga proporcionadas por Sophos.
  - d) Si accede a la fuente de actualización a través de un servidor proxy, seleccione la opción **Usar servidor proxy**. Introduzca la **dirección** y el número de **puerto** del servidor proxy. En los cuadros **Nombre de usuario** y **Contraseña**, escriba las credenciales necesarias para acceder al servidor proxy. Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma dominio\usuario.
  - e) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Detalles de la fuente**.  
**Sophos** aparece en la lista de la ficha **Fuentes** del cuadro de diálogo **Configuración del gestor de actualización**.
  - f) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración del gestor de actualización**.
3. Suscríbase al software que desea descargar:
  - a) En el panel **Suscripciones**:
    - Haga doble clic en la suscripción que desea cambiar.
    - Para añadir una suscripción, haga clic en **Añadir** en la parte superior del panel.  
**Importante:** para suscribirse a Sophos Anti-Virus para NetWare, es necesario añadir una suscripción nueva exclusiva. No incluya ningún otro software.
  - b) En el cuadro de diálogo **Suscripción de software**, si va a añadir una suscripción nueva, indique el **Nombre de la suscripción**.
  - c) En la lista de plataformas, seleccione el software y la versión que desee.

La suscripción **Recomendada** garantiza la actualización automática del software. Para más información sobre otros tipos de versiones disponibles, consulte la sección sobre la configuración de suscripciones de la Ayuda de Enterprise Console.

- d) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Suscripción de software**.
  - e) Repita estos pasos con todas las suscripciones que desee cambiar o añadir.
4. Configure el gestor de actualización para que utilice estas suscripciones:
- a) En el panel **Gestores de actualización**, seleccione el gestor de actualización que está instalado en este servidor. Haga clic con el botón derecho y seleccione **Ver/editar configuración**.
  - b) En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Suscripciones**, compruebe que las suscripciones están en la lista **Suscrito**. De lo contrario, seleccione las suscripciones en la lista **Disponibles** y haga clic en el botón > para moverlas a la lista **Suscritas**.
5. Si desea realizar las descargas en otras unidades compartidas que no sean \\servidor\SophosUpdate, como las unidades creadas en los servidores de NetWare:
- a) Abra la ficha **Distribución**.
  - b) No olvide seleccionar en la lista de la parte superior de la ficha la suscripción que desea utilizar.
  - c) Haga clic en **Añadir**.
  - d) Desde el cuadro de diálogo **Buscar carpeta**, vaya a una de las unidades compartidas. Haga clic en **Aceptar**.
  - e) Seleccione la unidad compartida en la lista **Disponibles** y haga clic en el botón > para moverla a la lista **Actualizar en**.
  - f) Para introducir una descripción de la unidad compartida o las credenciales, seleccione la unidad compartida y haga clic en **Configurar**. En el cuadro de diálogo **Gestor de unidades compartidas**, escriba la descripción y las credenciales.
  - g) Repita estos pasos con cada unidad compartida.
6. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración del gestor de actualización**.

El software seleccionado se descarga en las unidades compartidas especificadas.

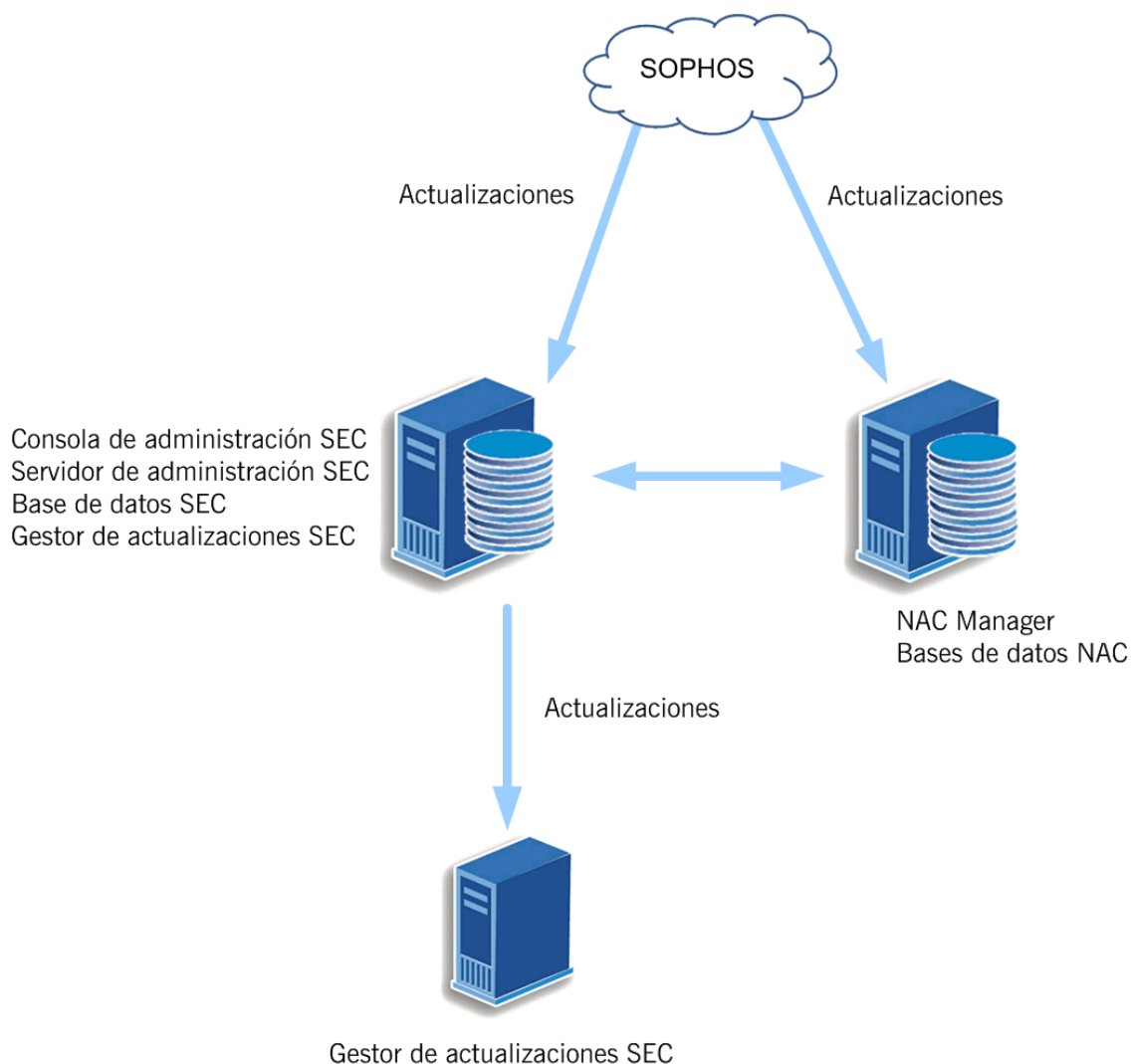
El proceso de instalación de las herramientas administrativas finaliza aquí. Ahora vaya a [Publicar el software de seguridad en un servidor web](#) en la página 40.

## 6 Instalar las herramientas administrativas con un gestor de actualización adicional en un servidor diferente

En esta situación, las fuentes de actualización de los gestores de actualización se pueden configurar de dos formas.

El primer método consiste en:

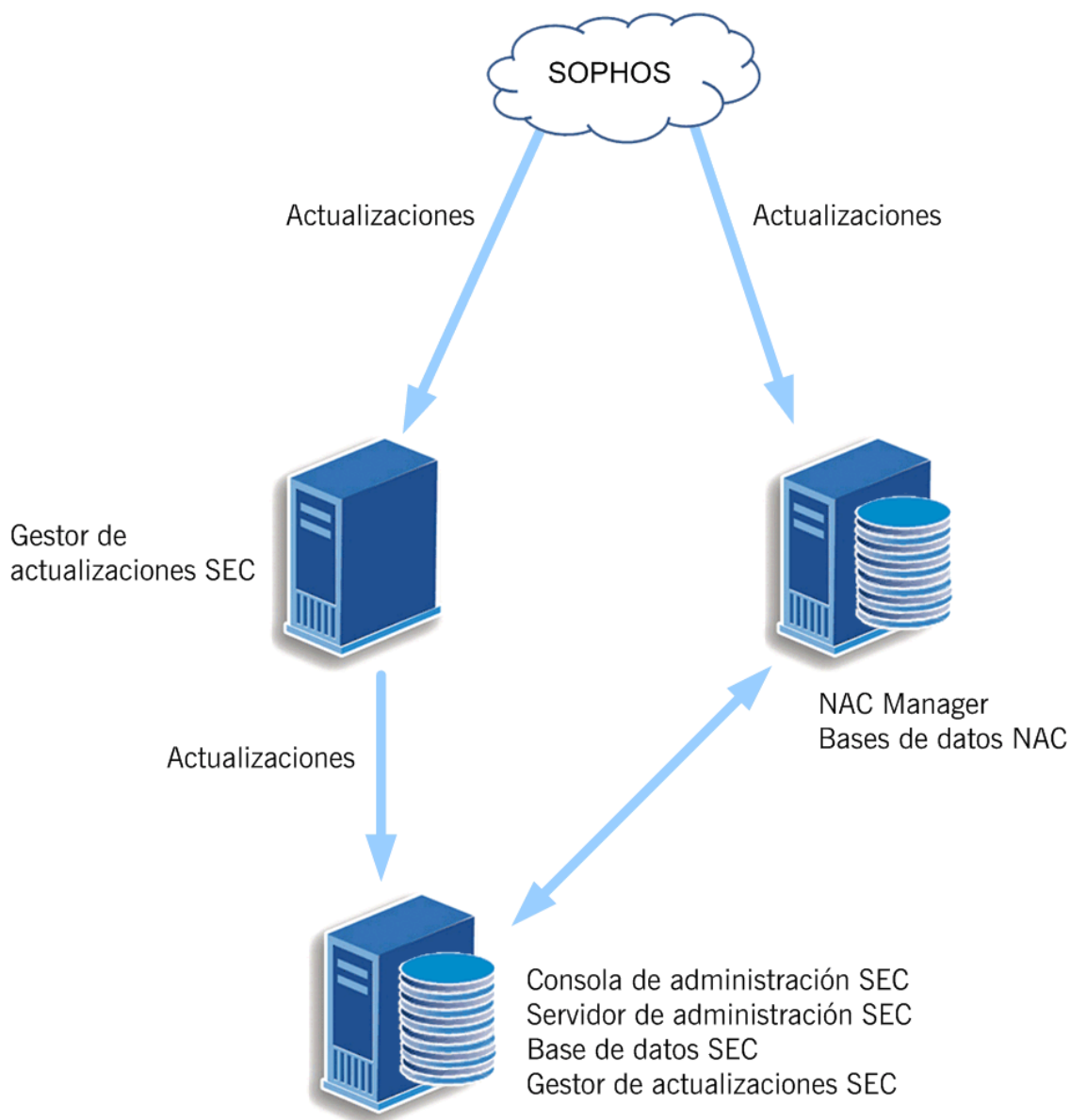
- Configurar el gestor de actualización principal instalado junto a la consola de administración para que se actualice directamente desde Sophos.
- Configurar el gestor de actualización adicional para que se actualice desde el gestor de actualización principal.



El segundo método consiste en:

- Configurar el gestor de actualización adicional para que se actualice directamente desde Sophos.

- Configurar el gestor de actualización instalado junto a la consola de administración para que se actualice desde el gestor de actualización adicional.



Utilice el segundo método si no quiere conectar el servidor principal de Enterprise Console a Internet.

El método elegido determina:

- Los servidores que necesita conectar a Internet. En la sección siguientes sobre la instalación, se indica cuándo el servidor en el que realiza la instalación necesita estar conectado a Internet.
- El método elegido para descargar software de seguridad en una ubicación central para distribuirla a las estaciones. Elija la sección adecuada cuando llegue el momento.

## 6.1 Descargar los programas de instalación

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.
4. Descargue el programa de instalación de NAC Manager.
5. Descargue el programa de instalación de Sophos Compliance Dissolvable Agent.
6. Compruebe que se puede acceder a los programas de instalación desde los servidores en los que quiere instalar el software.  
Si lo prefiere, puede copiarlos en un CD-ROM o DVD.

## 6.2 Instalar NAC Manager y las bases de datos de NAC

Vaya al servidor en el que desea instalar NAC Manager y las bases de datos de NAC. Compruebe que está conectado a Internet.

Para la instalación de NAC, es necesario que inicie sesión como se describe a continuación:

- Si el servidor se encuentra en un dominio, inicie la sesión como administrador del dominio.
- Si el servidor se encuentra en un grupo de trabajo, inicie la sesión como administrador local.

El asistente de instalación de NAC le guiará durante la instalación de los requisitos del sistema de NAC. Durante la instalación de NAC, tenga a mano el CD-ROM del sistema operativo correspondiente para instalar determinados requisitos del sistema. El asistente de instalación de NAC instala de forma automática otros requisitos.

1. Haga doble clic en el programa de instalación del NAC que descargó anteriormente.  
Se inicia el asistente para la instalación.

2. Haga clic en **Install**.
3. En la página de **bienvenida**, haga clic en **Siguiente**.
4. En el cuadro de diálogo **Select Features**, haga clic en **Next**.
5. En el cuadro de diálogo **Sophos Download Account Details**, introduzca los datos de la cuenta de descargas de Sophos en los campos correspondientes. Haga clic en **Next**.  
Los datos de la cuenta de descargas de Sophos se proporcionan al adquirir Sophos NAC. El nombre de usuario y la contraseña son necesarios para descargar los datos más recientes de detección para las aplicaciones de seguridad. Si se equivoca al introducir los datos, puede corregirlos más tarde con NAC Manager. Para más información, consulte la Ayuda de NAC Manager.
6. En la página **Server Proxy Settings**, si utiliza un servidor proxy para acceder a Internet, haga clic en **Use Proxy**. Puede utilizar el mismo proxy que para Enterprise Console. Haga clic en **Next**.

El nombre de usuario y la contraseña son obligatorios cuando NAC Manager utiliza un proxy autenticado.

7. En el cuadro de diálogo **Preparado para instalar el programa**, haga clic en **Install** para que empiece la instalación.  
 NAC se configura y aparece el progreso de la instalación. Ciertas tareas durante la instalación pueden tardar bastante y la barra de evolución no se moverá. No cancele la instalación.
8. Haga clic en **Finish**.  
**Importante:** si se produce algún error durante la instalación, consulte el registro de eventos de la aplicación. Si falla la instalación de las bases de datos, deberá borrar las siguientes bases de datos: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore y SecurityStore. Tras borrar las bases de datos podrá volver a intentar la instalación.

## 6.3 Cambiar el tamaño de las bases de datos de NAC

En las instalaciones de hasta 1.500 estaciones, el proceso de instalación de NAC ajusta de forma automática el tamaño de las bases de datos de NAC. Puede pasar a la sección siguiente.

En las instalaciones de más estaciones, es necesario aumentar el tamaño de las bases de datos de NAC: la base de datos ReportStore y el registro de ReportStore, como se explica en esta sección.

### 6.3.1 Guía para establecer el tamaño de las bases de datos ReportStore

Utilice esta tabla como guía para establecer el tamaño de la base de datos ReportStore.

Número de estaciones	Tamaño de ReportStore
1.500	300 MB
3.000	379 MB
5.000	485 MB
7.500	616 MB
10.000	748 MB
15.000	1011 MB
20.000	1274 MB
25.000	1536 MB

### 6.3.2 Guía para establecer el tamaño de los registros de ReportStore

Utilice esta tabla como guía para establecer el tamaño del registro de ReportStore.

Número de estaciones	Tamaño del registro de ReportStore
1.500	150 MB
3.000	206 MB
5.000	281 MB
7.500	374 MB
10.000	467 MB
15.000	653 MB
20.000	839 MB
25.000	1024 MB

### 6.3.3 Cambiar el tamaño de la base de datos de NAC: SQL Server 2005/2008

1. En el menú **Inicio** de SQL Server, señale **Microsoft SQL Server 2005** o **Microsoft SQL Server 2008** y haga clic en **SQL Server Management Studio**.
2. En SQL Server Management Studio, haga clic con el botón derecho en la base de datos ReportStore de la carpeta Databases y haga clic en **Propiedades**.
3. En el cuadro de diálogo **Propiedades**, seleccione **Archivos**.
4. Busque el archivo ReportStore\_Data. En el campo **Tamaño inicial (MB)** indique el tamaño deseado para la base de datos.
5. Busque el archivo ReportStore\_Log. En el campo **Tamaño inicial (MB)** indique el tamaño deseado para el registro.
6. Haga clic en **Aceptar**.
7. Cierre SQL Server Management Studio.

## 6.4 Instalar el agente soluble de cumplimiento en un servidor web

Sophos Compliance Dissolvable Agent es un componente de NAC que evalúa el cumplimiento de las estaciones. Está diseñado para los usuarios que no tienen instalado Sophos Compliance Agent, como trabajadores temporales o invitados. Para usarlo, es necesario instalar primero el agente soluble de cumplimiento en un servidor web de Windows al que puedan acceder los usuarios. Una vez instalado, los usuarios descargan el agente soluble de cumplimiento desde un navegador.

**Nota:** si lo desea, puede instalarlo en el mismo servidor en el que instaló NAC Manager o las bases de datos de NAC.

1. Haga doble clic en el programa de instalación del agente soluble de cumplimiento que descargó anteriormente.

Se inicia el asistente para la instalación.

2. En la página de **bienvenida**, haga clic en **Next**.
3. En el cuadro de diálogo **Destination Folder**, conserve la carpeta predeterminada o haga clic en **Change** para seleccionar una carpeta diferente para la instalación. Haga clic en **Next**.
4. En el cuadro de diálogo **Sophos Server**, escriba la dirección IP o el nombre del DNS del servidor en el que instaló NAC Manager.

**Nota:** si cambia la dirección del servidor de NAC Manager más adelante, deberá volver a instalar el agente soluble de cumplimiento en el servidor web y especificar la dirección nueva durante la instalación.

5. Si utiliza HTTPS con NAC, seleccione la opción **Secure Sophos Server (use HTTPS)**. La dirección IP o nombre del DNS del certificado web debe ser la misma que la del servidor de NAC Manager.
6. Haga clic en **Next**.
7. En el cuadro de diálogo **Ready to Install**, haga clic en **Install** para que empiece la instalación.
8. Haga clic en **Finish**.

**Nota:** si se produce algún error durante la instalación, consulte el registro de eventos de la aplicación.

Si instala el agente soluble de cumplimiento en la carpeta predeterminada, las estaciones pueden acceder con la dirección siguiente: `http(s)://dirección IP o nombre DNS/agentesoluble`. La dirección IP o nombre DNS corresponde al servidor donde instaló el agente soluble de cumplimiento. Por ejemplo:

```
http://www.ejemplo.com/agentesoluble
https://192.0.2.0/agentesoluble
```

## 6.5 Instalar SEC: todos los componentes

Vaya al servidor en el que desea instalar todos los componentes de Enterprise Console. Si quiere que se actualice directamente desde Sophos, el servidor debe estar conectado a Internet.

Para permitir que la consola se comuniquen con las estaciones administradas, abra los puertos 8192 y 8194 del servidor. Para permitir que el gestor de actualización descargue el software de seguridad desde Sophos o desde otro gestor de actualización mediante HTTP, abra el puerto 80 del servidor. Para permitir que el gestor de actualización descargue el software de seguridad desde otro gestor de actualización mediante una ruta UNC, abra los puertos 137, 138, 139 y 445 del servidor.

El nombre de este equipo debe ser diferente al del resto de servidores en los que instale el gestor de actualización.

Si el servidor utiliza Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinícielo. Puede volver a activarlo después de instalar Enterprise Console y suscribirse a las actualizaciones de Sophos.

Si el servidor se encuentra en un *dominio*, inicie la sesión como administrador del dominio.

Si el servidor se encuentra en un *grupo de trabajo*, inicie la sesión como administrador local.

1. Haga doble clic en el programa de instalación del Enterprise Console que descargó anteriormente.
2. Extraiga los archivos de instalación en la carpeta de destino sugerida o en otra que prefiera. La carpeta debe encontrarse en el propio ordenador.

Se inicia el asistente para la instalación.

3. En el cuadro de diálogo **Sophos Enterprise Console**, haga clic en **Siguiente**.

Un asistente le guiará durante la instalación. Acepte las opciones predeterminadas y compruebe que está seleccionada la configuración **Completa**.

Cuando termine la instalación, cierre la sesión o reinicie el servidor (indicado en el último cuadro de diálogo del asistente). Al volver a iniciar sesión, Enterprise Console se abre de forma automática y se inicia el asistente para descargar el software de seguridad. Cancelelo y ejecútelo más adelante, cuando se indique en esta guía.

## 6.6 Instalar una consola de administración de SEC adicional

Si lo desea, puede instalar otra instancia de la consola de administración en otro servidor para administrar las estaciones en red más cómodamente. Si no, pase a la sección siguiente.

Si el servidor utiliza Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinícielo. Puede activarlo de nuevo después de instalar la consola de administración.

Si el servidor se encuentra en un *dominio*, inicie la sesión como administrador del dominio.

Si el servidor se encuentra en un *grupo de trabajo*, inicie la sesión como administrador local.

1. Haga doble clic en el programa de instalación del Enterprise Console que descargó anteriormente.
2. Extraiga los archivos de instalación en la carpeta de destino sugerida o en otra que prefiera. La carpeta debe encontrarse en el propio ordenador.

Se inicia el asistente para la instalación.

3. En el cuadro de diálogo **Sophos Enterprise Console**, haga clic en **Siguiente**.

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

En el cuadro de diálogo **Tipo de instalación**, seleccione **Personalizada**.

En el cuadro **Instalación personalizada**, compruebe que está seleccionada **Consola de administración**, pero no **Servidor de administración** ni **Base de datos**.

En el cuadro **Servidor de administración**, escriba el nombre del servidor en el que instaló el servidor de administración SEC.

Cuando termine el asistente, cierre la sesión o reinicie el servidor (según se indique al final del asistente). Al volver a iniciar sesión, Enterprise Console se abre de forma automática. Si se inicia el asistente para descargar el software de seguridad, ciérrelo.

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

Para permitir a otros usuarios el control de la nueva consola de administración:

- Añada los usuarios a los grupos Sophos Console Administrators y Distributed COM Users en el ordenador donde ha instalado la consola de administración.
- Asigne a cada usuario algún subentorno de Enterprise Console.

Para poder crear informes, usuario debe pertenecer también al grupo Sophos DB Users en el servidor con la base de datos de Enterprise Console.

## 6.7 Instalar un gestor de actualización adicional

Vaya al servidor en el que quiere instalar un gestor de actualización adicional. Si quiere que se actualice directamente desde Sophos, el servidor debe estar conectado a Internet.

Para permitir que el gestor de actualización descargue el software de seguridad desde Sophos o desde otro gestor de actualización mediante HTTP, abra el puerto 80 del servidor. Para permitir que el gestor de actualización descargue el software de seguridad desde otro gestor de actualización mediante una ruta UNC, abra los puertos 137, 138, 139 y 445 del servidor.

El nombre de este equipo debe ser diferente al del resto de servidores en los que instale el gestor de actualización.

Si el servidor tiene instalada la detección de redes de Windows pero está desactivada, tendrá que activarla y reiniciar el sistema.

Si el servidor utiliza Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinícielo. Puede volver a activarlo después de instalar el gestor de actualización y suscribirse a las actualizaciones de Sophos.

Si el servidor se encuentra en un *dominio*, inicie la sesión como administrador del dominio.

Si el servidor se encuentra en un *grupo de trabajo*, inicie la sesión como administrador local.

1. Busque la carpeta compartida SUMInstallSet en el servidor en el que instaló Enterprise Console.
2. Haga doble clic en Setup.exe para ejecutar el programa de instalación.
3. En el cuadro de diálogo **Sophos Update Manager**, haga clic en **Siguiente**.

Un asistente le guiará durante la instalación. Acepte los valores predeterminados.

El gestor de actualización está instalado y se administra desde Enterprise Console.

## 6.8 Crear un directorio para Sophos Anti-Virus para NetWare

Para proteger servidores de NetWare, es necesario crear un directorio en el que el gestor de actualización colocará el software más reciente de Sophos Anti-Virus para NetWare, en cada servidor de NetWare que quiera proteger.

Para crear un directorio para Sophos Anti-Virus para NetWare:

1. En un equipo de Windows con software de administrador de NetWare, o en uno de los servidores de Netware que desee proteger, cree el directorio `\\servidor de NetWare\SYS\SWEET\NLMINST` siendo *servidor de NetWare* el nombre del servidor de Netware.
2. Comparta el directorio para que puedan acceder a él todos los servidores en los que ha instalado un gestor de actualización.
3. Repita el procedimiento en todos los servidores de NetWare que desee proteger.

La instalación de Sophos Anti-Virus en NetWare se describe en la *Guía de inicio de Sophos Endpoint Security and Control 9.5 para Linux, NetWare y UNIX*.

## 6.9 Descargar software de seguridad

Según lo descrito anteriormente, en esta situación, las fuentes de actualización de los gestores de actualización se pueden configurar de dos formas. Elija la que sea más apropiada:

- [Gestor de actualización principal con actualización desde Sophos](#) en la página 32
- [Gestor de actualización adicional con actualización desde Sophos](#) en la página 36

### 6.9.1 Gestor de actualización principal con actualización desde Sophos

#### Configurar el gestor de actualización principal para que se actualice desde Sophos

Configure el gestor de actualización principal que instaló junto a la consola de administración de SEC para que se actualice directamente desde Sophos. Siga uno de estos dos métodos.

La sección [Configurar el gestor de actualización principal de forma automática](#) en la página 33 describe cómo ejecutar el asistente que permite descargar:

- Sólo la versión más reciente.
- Sólo las subcarpetas de la unidad compartida `\\servidor\SophosUpdate`, siendo *servidor* el servidor en el que está instalado el gestor de actualización principal.

La sección [Configurar el gestor de actualización principal de forma manual](#) en la página 33 describe cómo configurar el gestor de actualización principal directamente para poder descargar:

- Versiones anteriores.
- A otras unidades compartidas, como en otros servidores.

**Nota:** utilice este método para descargar Sophos Anti-Virus para NetWare.

Para más información sobre otros tipos de versiones disponibles, consulte la sección sobre la configuración de suscripciones de la Ayuda de Enterprise Console.

## Configurar el gestor de actualización adicional para que se actualice desde el gestor de actualización principal

La sección [Configurar el gestor de actualización adicional](#) en la página 35 explica cómo configurar el gestor de actualización adicional para que se actualice desde el gestor de actualización principal.

### 6.9.1.1 Configurar el gestor de actualización principal de forma automática

1. En Enterprise Console, en el menú **Acciones**, haga clic en **Asistente para descargar el software de seguridad**.
2. 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**.
3. En la página **Selección de plataformas**, seleccione las plataformas que desea proteger. Al hacer clic en **Siguiente**, Enterprise Console empieza a descargar el software.
4. En la página **Descarga del software**, puede ver el progreso de la descarga. Haga clic en **Siguiente** en cualquier momento.
5. 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.

**Nota:** si un equipo se añade a más de un contenedor de Active Directory, se intercambiarán mensajes continuamente entre el equipo y Enterprise Console.

El software seleccionado se descarga en la unidad compartida `\\servidor\SophosUpdate`, siendo *servidor* el nombre del servidor en el que está instalado el gestor de actualización.

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

Ahora, configure el gestor de actualización de forma manual, si es necesario. A continuación, vaya a [Configurar el gestor de actualización adicional](#) en la página 35.

### 6.9.1.2 Configurar el gestor de actualización principal de forma manual

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

1. En Enterprise Console, en el menú **Ver**, seleccione **Gestores de actualización**.

2. Si *no* ha configurado el gestor de actualización de forma automática, configúrelo para que utilice Sophos como fuente de actualización:
  - a) En el panel **Gestores de actualización**, seleccione el gestor de actualización que está instalado en este servidor. Haga clic con el botón derecho y seleccione **Ver/editar configuración**.
  - b) En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Fuentes**, haga clic en **Añadir**.
  - c) En el cuadro de diálogo **Detalles de la fuente**, en el cuadro **Dirección**, seleccione **Sophos**. En los cuadros **Nombre de usuario** y **Contraseña**, escriba las credenciales de descarga proporcionadas por Sophos.
  - d) Si accede a la fuente de actualización a través de un servidor proxy, seleccione la opción **Usar servidor proxy**. Introduzca la **dirección** y el número de **puerto** del servidor proxy. En los cuadros **Nombre de usuario** y **Contraseña**, escriba las credenciales necesarias para acceder al servidor proxy. Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma dominio\usuario.
  - e) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Detalles de la fuente**.  
**Sophos** aparece en la lista de la ficha **Fuentes** del cuadro de diálogo **Configuración del gestor de actualización**.
  - f) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración del gestor de actualización**.
3. Suscríbase al software que desea descargar:
  - a) En el panel **Suscripciones**:
    - Haga doble clic en la suscripción que desea cambiar.
    - Para añadir una suscripción, haga clic en **Añadir** en la parte superior del panel.

**Importante:** para suscribirse a Sophos Anti-Virus para NetWare, es necesario añadir una suscripción nueva exclusiva. No incluya ningún otro software.
  - b) En el cuadro de diálogo **Suscripción de software**, si va a añadir una suscripción nueva, indique el **Nombre de la suscripción**.
  - c) En la lista de plataformas, seleccione el software y la versión que desee.  
La suscripción **Recomendada** garantiza la actualización automática del software. Para más información sobre otros tipos de versiones disponibles, consulte la sección sobre la configuración de suscripciones de la Ayuda de Enterprise Console.
  - d) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Suscripción de software**.
  - e) Repita estos pasos con todas las suscripciones que desee cambiar o añadir.

4. Configure el gestor de actualización para que utilice estas suscripciones:
  - a) En el panel **Gestores de actualización**, seleccione el gestor de actualización que está instalado en este servidor. Haga clic con el botón derecho y seleccione **Ver/editar configuración**.
  - b) En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Suscripciones**, compruebe que las suscripciones están en la lista **Suscrito**. De lo contrario, seleccione las suscripciones en la lista **Disponibles** y haga clic en el botón > para moverlas a la lista **Suscritas**.
5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración del gestor de actualización**.

El software seleccionado se descarga en el gestor de actualización que está instalado en este servidor.

### 6.9.1.3 Configurar el gestor de actualización adicional

1. En Enterprise Console, en el menú **Ver**, seleccione **Gestores de actualización**.
2. Configure el gestor de actualización adicional para que utilice el gestor de actualización como fuente de actualización:
  - a) En el panel **Gestores de actualización**, seleccione el gestor de actualización adicional. Haga clic con el botón derecho y seleccione **Ver/editar configuración**.
  - b) En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Fuentes**, haga clic en **Añadir**.
  - c) En el cuadro de diálogo **Detalles de la fuente**, en el cuadro **Dirección**, seleccione la unidad compartida en la que el gestor de actualización principal descarga el software.

Los cuadros **Nombre de usuario** y **Contraseña** se rellenan de forma automática con las credenciales necesarias para acceder a esta unidad compartida.
  - d) Si accede a la fuente de actualización a través de un servidor proxy, seleccione la opción **Usar servidor proxy**. Introduzca la **dirección** y el número de **puerto** del servidor proxy. En los cuadros **Nombre de usuario** y **Contraseña**, escriba las credenciales necesarias para acceder al servidor proxy. Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma dominio\usuario.
  - e) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Detalles de la fuente**.

La unidad compartida en la que el gestor de actualización principal descarga el software aparece en la lista de la ficha **Fuentes** del cuadro de diálogo **Configuración del gestor de actualización**.
3. Configure el gestor de actualización para que utilice las suscripciones configuradas anteriormente:
  - En la ficha **Suscripciones**, compruebe que las suscripciones están en la lista **Suscritas**. De lo contrario, seleccione las suscripciones en la lista **Disponibles** y haga clic en el botón > para moverlas a la lista **Suscritas**.

4. Si desea realizar las descargas en otras unidades compartidas que no sean \\servidor\SophosUpdate, como las unidades creadas en los servidores de NetWare:
  - a) Abra la ficha **Distribución**.
  - b) No olvide seleccionar en la lista de la parte superior de la ficha la suscripción que desea utilizar.
  - c) Haga clic en **Añadir**.
  - d) Desde el cuadro de diálogo **Buscar carpeta**, vaya a una de las unidades compartidas. Haga clic en **Aceptar**.
  - e) Seleccione la unidad compartida en la lista **Disponibles** y haga clic en el botón > para moverla a la lista **Actualizar en**.
  - f) Para introducir una descripción de la unidad compartida o las credenciales, seleccione la unidad compartida y haga clic en **Configurar**. En el cuadro de diálogo **Gestor de unidades compartidas**, escriba la descripción y las credenciales.
  - g) Repita estos pasos con cada unidad compartida.
5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración del gestor de actualización**.

El software seleccionado se descarga en las unidades compartidas especificadas durante la próxima actualización programada.

El proceso de instalación de las herramientas administrativas finaliza aquí. Ahora vaya a [Publicar el software de seguridad en un servidor web](#) en la página 40.

## 6.9.2 Gestor de actualización adicional con actualización desde Sophos

La sección [Configurar el gestor de actualización adicional](#) en la página 36 describe cómo configurar el gestor de actualización adicional para que se actualice directamente desde Sophos.

La sección [Configurar el gestor de actualización principal](#) en la página 38 describe cómo configurar el gestor de actualización principal instalado junto con la consola de SEC para que se actualice desde el gestor de actualización adicional.

### 6.9.2.1 Configurar el gestor de actualización adicional

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

1. En Enterprise Console, en el menú **Ver**, seleccione **Gestores de actualización**.

2. Configure el gestor de actualización adicional para que utilice Sophos como fuente de actualización:
  - a) En el panel **Gestores de actualización**, seleccione el gestor de actualización adicional. Haga clic con el botón derecho y seleccione **Ver/editar configuración**.
  - b) En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Fuentes**, haga clic en **Añadir**.
  - c) En el cuadro de diálogo **Detalles de la fuente**, en el cuadro **Dirección**, seleccione **Sophos**. En los cuadros **Nombre de usuario** y **Contraseña**, escriba las credenciales de descarga proporcionadas por Sophos.
  - d) Si accede a la fuente de actualización a través de un servidor proxy, seleccione la opción **Usar servidor proxy**. Introduzca la **dirección** y el número de **puerto** del servidor proxy. En los cuadros **Nombre de usuario** y **Contraseña**, escriba las credenciales necesarias para acceder al servidor proxy. Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma dominio\usuario.
  - e) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Detalles de la fuente**.  
**Sophos** aparece en la lista de la ficha **Fuentes** del cuadro de diálogo **Configuración del gestor de actualización**.
  - f) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración del gestor de actualización**.
3. Suscríbase al software que desea descargar:
  - a) En el panel **Suscripciones**:
    - Haga doble clic en la suscripción que desea cambiar.
    - Para añadir una suscripción, haga clic en **Añadir** en la parte superior del panel.**Importante:** para suscribirse a Sophos Anti-Virus para NetWare, es necesario añadir una suscripción nueva exclusiva. No incluya ningún otro software.
  - b) En el cuadro de diálogo **Suscripción de software**, si va a añadir una suscripción nueva, indique el **Nombre de la suscripción**.
  - c) En la lista de plataformas, seleccione el software y la versión que desee.  
La suscripción **Recomendada** garantiza la actualización automática del software. Para más información sobre otros tipos de versiones disponibles, consulte la sección sobre la configuración de suscripciones de la Ayuda de Enterprise Console.
  - d) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Suscripción de software**.
  - e) Repita estos pasos con todas las suscripciones que desee cambiar o añadir.
4. Configure el gestor de actualización para que utilice estas suscripciones:
  - a) En el panel **Gestores de actualización**, seleccione el gestor de actualización adicional. Haga clic con el botón derecho y seleccione **Ver/editar configuración**.
  - b) En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Suscripciones**, compruebe que las suscripciones están en la lista **Suscrito**. De lo

contrario, seleccione las suscripciones en la lista **Disponibles** y haga clic en el botón > para moverlas a la lista **Suscritas**.

5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración del gestor de actualización**.

El software seleccionado se descarga en el gestor de actualización adicional.

### 6.9.2.2 Configurar el gestor de actualización principal

1. En Enterprise Console, en el menú **Ver**, seleccione **Gestores de actualización**.
2. Configure el gestor de actualización principal para que utilice el gestor de actualización adicional como fuente de actualización:
  - a) En el panel **Gestores de actualización**, seleccione el gestor de actualización que está instalado en este servidor. Haga clic con el botón derecho y seleccione **Ver/editar configuración**.
  - b) En el cuadro de diálogo **Configuración del gestor de actualización**, en la ficha **Fuentes**, haga clic en **Añadir**.
  - c) En el cuadro de diálogo **Detalles de la fuente**, en el cuadro **Dirección**, seleccione la unidad compartida en la que el gestor de actualización adicional descarga el software.

Los cuadros **Nombre de usuario** y **Contraseña** se rellenan de forma automática con las credenciales necesarias para acceder a esta unidad compartida.

- d) Si accede a la fuente de actualización a través de un servidor proxy, seleccione la opción **Usar servidor proxy**. Introduzca la **dirección** y el número de **puerto** del servidor proxy. En los cuadros **Nombre de usuario** y **Contraseña**, escriba las credenciales necesarias para acceder al servidor proxy. Si el nombre de usuario tiene que indicar el dominio para su validación, use la forma dominio\usuario.
  - e) Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Detalles de la fuente**.

La unidad compartida en la que el gestor de actualización adicional descarga el software aparece en la lista de la ficha **Fuentes** del cuadro de diálogo **Configuración del gestor de actualización**.
3. Configure el gestor de actualización para que utilice las suscripciones configuradas anteriormente:
    - En la ficha **Suscripciones**, compruebe que las suscripciones están en la lista **Suscritas**. De lo contrario, seleccione las suscripciones en la lista **Disponibles** y haga clic en el botón > para moverlas a la lista **Suscritas**.

4. Si desea realizar las descargas en otras unidades compartidas que no sean \\servidor\SophosUpdate, como las unidades creadas en los servidores de NetWare:
  - a) Abra la ficha **Distribución**.
  - b) No olvide seleccionar en la lista de la parte superior de la ficha la suscripción que desea utilizar.
  - c) Haga clic en **Añadir**.
  - d) Desde el cuadro de diálogo **Buscar carpeta**, vaya a una de las unidades compartidas. Haga clic en **Aceptar**.
  - e) Seleccione la unidad compartida en la lista **Disponibles** y haga clic en el botón > para moverla a la lista **Actualizar en**.
  - f) Para introducir una descripción de la unidad compartida o las credenciales, seleccione la unidad compartida y haga clic en **Configurar**. En el cuadro de diálogo **Gestor de unidades compartidas**, escriba la descripción y las credenciales.
  - g) Repita estos pasos con cada unidad compartida.
5. Haga clic en **Aceptar** para cerrar el cuadro de diálogo **Configuración del gestor de actualización**.

El software seleccionado se descarga en las unidades compartidas especificadas durante la próxima actualización programada.

El proceso de instalación de las herramientas administrativas finaliza aquí. Ahora vaya a [Publicar el software de seguridad en un servidor web](#) en la página 40.

## 7 Publicar el software de seguridad en un servidor web

Si lo desea, puede publicar el software de seguridad de Sophos en un servidor web para los equipos que acceden a través de HTTP.

Para publicar el software de seguridad en un servidor web:

1. Para averiguar la ruta a la carpeta compartida en la que se ha descargado el software de seguridad, conocida como ubicación de archivos de inicio:
  - a) En Enterprise Console, en el menú **Ver**, seleccione **Ubicación de archivos de inicio**.  
En el cuadro de diálogo **Ubicación de archivos de inicio**, la columna **Ubicación** muestra la ubicación de los archivos de inicio de cada plataforma.
  - b) Anote la ruta sin incluir la carpeta de los CID. Por ejemplo:  
`\\servidor\SophosUpdate`
2. Permita que la ubicación de los archivos de inicio, incluidas las subcarpetas, estén disponibles desde el servidor web.
3. Especifique nombres de usuario y contraseñas para evitar el acceso no autorizado a esta carpeta del servidor web.

**Nota:** la documentación para su servidor web le explicará cómo compartir una carpeta en su sitio web y cómo configurar credenciales para ella. Para más información sobre cómo hacerlo, póngase en contacto con el proveedor del servidor web.

## 8 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 42.

Para proteger y administrar ordenadores, debe crear grupos.

1. Si no puede ver el panel **Grupos** (en la parte izquierda de la ventana), en el menú **Ver**, haga clic en **Estaciones**.
2. Haga clic en cualquier lugar del panel **Grupos**.
3. En el menú **Grupos**, haga clic en **Crear grupo**.  
Se añadirá un **Nuevo grupo** en el panel de la izquierda.
4. Escriba el nombre que desee utilizar para el grupo.
5. Para crear otro grupo en el nivel más alto, seleccione el servidor que aparece en la parte superior del panel **Grupos** y repita los pasos 3 y 4.

Para crear un subgrupo de un grupo existente, selecciónelo y repita los pasos 3 y 4.

## 9 Configurar políticas de seguridad

Una *política de seguridad* es un conjunto de parámetros que pueden aplicarse a los ordenadores de un grupo.

Enterprise Console aplica políticas predeterminadas a los grupos de ordenadores. En esta sección se explica:

- Cuáles son las políticas predeterminadas y cuándo es necesario modificarlas.
- Cómo crear o editar una política.
- Cómo aplicar una política a los grupos de ordenadores.

### 9.1 Políticas predeterminadas

Esta sección describe las políticas predeterminadas y cómo debe modificarlas. Para más información sobre la configuración recomendada de la política, consulte la *Guía de configuración de políticas de Sophos Endpoint Security and Control 9.5*.

#### 9.1.1 Política de actualización

Por defecto, las estaciones se actualizan desde la unidad compartida predeterminada creada en el servidor en el que está instalado el gestor de actualización correspondiente.

Si lo desea, puede:

- Especificar una fuente de actualización alternativa para los equipos que no están siempre conectados a la red de la empresa, como los portátiles.
- Especificar la dirección del software publicado en un servidor web.

Para cambiar la forma en la que se actualiza el software de la estación, es necesario modificar la política de actualización. Puede hacerlo en cualquier momento.

#### 9.1.2 Política antivirus y HIPS

Por defecto, Sophos Endpoint Security and Control:

- Impide acceder a archivos que contengan virus o programas espía.
- Detecta comportamientos sospechosos de los programas en ejecución.
- Bloquea el acceso a sitios web maliciosos.
- Utiliza la protección activa de Sophos para mejorar la detección de nuevas amenazas.
- Envía una alerta a Enterprise Console cuando se detecta cualquier amenaza.

Si lo desea, puede:

- Desactivar el escaneo en acceso en servidores de Exchange o en otros servidores cuyo rendimiento se pueda ver afectado. Para más información, consulte el artículo 12421 de la base de conocimiento de Sophos (<http://esp.sophos.com/support/knowledgebase/article/12421.html>).

- Bloquear comportamientos sospechosos.
- Detectar archivos sospechosos.
- Detectar programas publicitarios y aplicaciones no deseadas.
- Detectar amenazas en descargas de Internet.
- Activar el envío de muestras a Sophos para sacar el mayor partido de la protección activa.

Para modificar el funcionamiento del software en las estaciones, es necesario modificar la política antivirus y HIPS. Puede hacerlo en cualquier momento.

### 9.1.3 Política de restricción de aplicaciones

La restricción de aplicaciones está desactivada de forma predeterminada. Para utilizar esta función, modifique la política de restricción de aplicaciones. Puede hacerlo en cualquier momento.

### 9.1.4 Política cortafuegos

Por defecto, Sophos Client Firewall bloquea todas las conexiones no esenciales. Por eso, para que la conectividad de la red no se vea perjudicada, es necesario modificar la política de cortafuegos antes de proteger los ordenadores.

### 9.1.5 Política NAC

Por defecto, los ordenadores pueden acceder a la red. Si desea utilizar esta función, modifique y aplique alguna de las políticas de NAC. Puede hacerlo en cualquier momento.

### 9.1.6 Política de control de datos

Por defecto, el control de datos está desactivado y no existen reglas para el control o para la restricción de transferencias de archivos a través de Internet o a dispositivos de almacenamiento. Para utilizar esta función, modifique la política de control de datos. Puede hacerlo en cualquier momento.

### 9.1.7 Política de control de dispositivos

Por defecto, el control de dispositivos está desactivado y se permiten todos los dispositivos. Para utilizar esta función, modifique la política de control de dispositivos. Puede hacerlo en cualquier momento.

### 9.1.8 Política de protección contra manipulaciones

Por defecto, la protección la protección contra manipulaciones se encuentra desactivada y no se requiere ninguna contraseña para configuración, desactivar o desinstalar Endpoint Security and Control. Para utilizar esta función, modifique la política de protección contra manipulaciones. Puede hacerlo en cualquier momento.

## 9.2 Crear o editar políticas, excepto NAC

1. En Enterprise Console, si no puede ver el panel **Políticas** (en la parte inferior izquierda de la ventana), en el menú **Ver**, haga clic en **Estaciones**.
2. En el panel **Políticas**, siga uno de estos pasos:
  - Para crear una política nueva, haga clic con el botón derecho del ratón en el tipo de política que desea crear, como **Actualización**, y haga clic en **Crear política**.
  - También puede editar la política predeterminada, haciendo doble clic en el tipo de política correspondiente. A continuación, seleccione **Predeterminada**.

Al crear una política, se añade una **Nueva política** a la lista. Escriba el nombre que desee utilizar para la política.

3. Haga doble clic en la política. Introduzca los parámetros que desee.

Después de crear una política, aplíquela a un grupo de ordenadores.

## 9.3 Editar una política NAC

1. Si todavía no ha utilizado NAC Manager:
  - a) Abra su navegador web.

Sophos sólo es compatible de forma oficial con Internet Explorer versiones 7 y 8, y Firefox versiones 3 y 3.5.
  - b) Añada la dirección del servidor donde instaló NAC Manager como sitio web de confianza.

**Nota:** esto no es necesario en Internet Explorer 7.
  - c) Permite las ventanas emergentes para la dirección donde instaló NAC Manager.
2. En Enterprise Console, si no puede ver el panel **Políticas** (en la parte inferior izquierda de la ventana), en el menú **Ver**, haga clic en **Estaciones**.
3. En el panel **Políticas**, haga doble clic en NAC. A continuación, haga doble clic en la política que desea editar.

NAC Manager aparece en el navegador predeterminado.

4. Inicie sesión con la cuenta predeterminada u otra creada.

La primera vez que utilice NAC Manager, utilice el nombre y la contraseña siguientes:

- Nombre de cuenta = admin
- Contraseña = la que prefiera

**Nota:** guarde la contraseña, ya que es el único acceso a NAC Manager que tendrá hasta que cree otras cuentas de usuario.

5. En la página de NAC Manager de la política que quiere editar, introduzca la configuración que desee.

Asegúrese de que la política se aplica a un grupo de ordenadores.

## **9.4 Aplicar una política a un grupo**

- ❖ En el panel **Políticas**, arrastre la política al grupo al que desea aplicar la política.

## 10 Buscar ordenadores

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

1. Si no puede ver el panel **Grupos** (en la parte izquierda de la ventana), en el menú **Ver**, haga clic en **Estaciones**.
2. En el menú **Acciones**, haga clic en **Buscar ordenadores**.
3. Seleccione el método que desea utilizar para buscar ordenadores.
4. Escriba los datos de la cuenta y especifique dónde quiere buscar.

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

## 11 Proteger ordenadores Windows y Mac

Para proteger ordenadores Windows y Mac:

- Prepare la protección de los ordenadores
- Proteja los ordenadores de Windows de forma automática.
- Proteja los ordenadores Windows o Mac de forma manual.

### 11.1 Preparación para proteger ordenadores

#### 11.1.1 Preparar la eliminación de software de terceros

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

1. En los equipos con programas antivirus de otros proveedores instalados, asegúrese de que la interfaz de usuario del software antivirus está cerrada.
2. En los equipos que utilizan cortafuegos o productos HIPS de otros proveedores, compruebe que están desactivados o configurados para permitir la ejecución del programa de instalación de Sophos.

Si los equipos utilizan una herramienta de actualización de otro proveedor, puede que desee eliminarla. Para más información, consulte la Ayuda de Sophos Enterprise Console.

#### 11.1.2 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).

Compruebe que dispone de una cuenta que:

- Tenga derechos de administrador local para los equipos que desee proteger.
- Pueda iniciar sesión en el equipo en el que instaló Enterprise Console.
- Tenga 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**.

**Nota:** si no puede ver el panel **Políticas** (en la parte inferior izquierda de la ventana), en el menú **Ver**, haga clic en **Estaciones**.

#### 11.1.3 Preparación para la instalación del software antivirus

Además de asegurarse de que los ordenadores cumplen los requisitos generales del sistema, es necesario realizar algunos pasos más para instalar el software de forma automática.

Para preparar la instalación del software antivirus:

1. En equipos con Windows Vista o Windows 7:
  - a) En Windows 7, en el Panel de control, abra el Centro de redes y recursos compartidos. Compruebe que están configuradas las opciones siguientes en la ubicación de la **Red de trabajo**:
    - Detección de redes: Activado
    - Uso compartido de archivos e impresoras: Activado
    - Conexiones de uso compartido de archivos: Habilitar el uso compartido de archivos para dispositivos que usan el cifrado de 40 o 56 bits
    - Uso compartido con protección por contraseña: Desactivado
  - b) En Windows Vista, en el Panel de control, abra el Centro de redes y recursos compartidos. Compruebe que están configuradas las opciones siguientes:
    - Detección de redes: Activado
    - Intercambio de archivos: Activado
    - Uso compartido de impresora: Activado
    - Uso compartido con protección por contraseña: Desactivado
  - c) Compruebe que el servicio de registro remoto está activado y que el tipo de inicio es Automático. Este servicio no está activado por defecto en Windows 7 o Vista.
  - d) En Windows 7, configure **No notificar** en el Control de cuentas de usuario. Una vez finalizada la instalación, vuelva a configurar la opción **Predeterminada**.
  - e) En Windows Vista, desactive el control de cuentas de usuario. Debería volver a activarlo cuando termine la instalación.
  - f) Desactive el asistente para compartir.
  - g) Abra el Firewall de Windows con seguridad avanzada desde las **Herramientas administrativas** del Panel de control. Compruebe que las **Conexiones entrantes** están permitidas.
  - h) Cambie las **Reglas de entrada** para activar lo siguiente. Cuando finalice la instalación, vuelva a desactivarlas:
    - Administración remota (NP-In) Dominio
    - Administración remota (NP-In) Privado
    - Administración remota (RPC) Dominio
    - Administración remota (RPC) Privado
    - Administración remota (RPC-EPMAP) Dominio
    - Administración remota (RPC-EPMAP) Privado

2. En equipos con Windows 2003/XP Pro/2000:
  - a) Compruebe que están iniciados los servicios Registro remoto, Servidor, Examinador de equipos y Programador de tareas.
  - b) Compruebe que el recurso compartido C\$ está activado.
  - c) Compruebe que el uso compartido simple de archivos está desactivado (sólo XP).
3. En equipos con Windows XP SP2 o posterior:
  - a) Compruebe que están iniciados los servicios Registro remoto, Servidor, Examinador de equipos y Programador de tareas.
  - b) Compruebe que el recurso compartido C\$ está activado.
  - c) Compruebe que el uso compartido simple de archivos está desactivado.
  - d) Active Compartir archivos e impresoras para redes Microsoft.
  - e) Asegúrese de que los puertos TCP 8192, 8193 y 8194 están abiertos.
  - f) Reinicie el ordenador para que los cambios surtan efecto.

#### 11.1.4 Preparación para la instalación del agente de cumplimiento

Sophos Compliance Agent es un componente de NAC que evalúa el cumplimiento de las estaciones. Se instala al proteger los ordenadores de Windows.

Para preparar la instalación de agente de cumplimiento:

- ❖ Especifique la dirección web del equipo en el que instaló NAC Manager. En Enterprise Console, en el menú **Herramientas**, haga clic en **Configurar dirección de NAC**.

### 11.2 Proteger los ordenadores de Windows de forma automática

**Nota:** al instalar Sophos Client Firewall, se desconectan de forma temporal todos los adaptadores de red. Se perderán todas las conexiones de red durante unos 20 segundos.

1. En Enterprise Console, seleccione los ordenadores que desea proteger.
2. Haga clic con el botón derecho en la selección y seleccione **Proteger ordenadores**.

**Nota:** si los equipos se encuentran en el grupo **No asignados**, arrástrelos a los grupos que desee.

Un asistente le guiará durante la instalación del software de seguridad de Sophos. Acepte las opciones predeterminadas, excepto las siguientes.

En el cuadro de diálogo **Seleccionar funciones**, seleccione la opción **Control de cumplimiento** si desea instalar NAC.

En la página **Resumen de protección**, podrá ver cualquier problema de instalación. Si necesita ayuda, consulte [Solución de problemas](#) en la página 50.

En la página **Credenciales**, indique la cuenta que se utilizará para instalar el software en los ordenadores.

Los equipos seleccionados están protegidos con el software de seguridad. La instalación se realiza por fases, por lo que el proceso puede no completarse en todos los equipos durante algún tiempo. Algunos ordenadores puede que tengan que reiniciarse para completar la instalación.

Cuando termine la instalación, vuelva a mirar la lista de equipos. En la columna **En acceso, Activo** quiere decir que el escaneado en acceso está activado.

### 11.2.1 Solución de problemas

Al intentar proteger ordenadores Windows de forma automática, se pueden producir errores en la instalación del software de seguridad por diferentes motivos:

- No es posible llevar a cabo la instalación automática en ese sistema operativo. Realice una instalación manual. Consulte [Proteger los ordenadores Windows o Mac de forma manual](#) en la página 50. Para otros sistemas operativos, consulte las secciones siguientes de esta guía.
- No se pudo 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.
- En estaciones con Windows XP, no se ha desactivado el uso compartido simple de archivos.
- En estaciones con Windows Vista, no se ha desactivado el asistente para compartir.
- Ha seleccionado alguna función que no es compatible con el sistema operativo.

Si se produce un error en la instalación del agente de cumplimiento, consulte el registro de la instalación del agente de cumplimiento. El registro se encuentra en la carpeta %tmp%.

## 11.3 Proteger los ordenadores Windows o Mac de forma manual

Si cuenta con equipos que no puede proteger de forma automática, puede protegerlos ejecutando el programa de instalación desde la carpeta compartida en la que se descargó el software de seguridad, conocida como la ubicación de los archivos de inicio.

Para llevar a cabo este procedimiento, es necesario utilizar una cuenta de administrador en los equipos que desee proteger.

Para proteger los ordenadores Windows o Mac de forma manual:

1. Para averiguar la ubicación de los archivos de inicio:
  - a) En Enterprise Console, en el menú **Ver**, seleccione **Ubicación de archivos de inicio**.  
En el cuadro de diálogo **Ubicación de archivos de inicio**, la columna **Ubicación** muestra la ubicación de los archivos de inicio de cada plataforma.
  - b) Anote las rutas correspondientes.
2. En el equipo en el que están alojados los archivos de inicio, cree una cuenta de usuario de solo lectura.

3. En todos los ordenadores que desee proteger, haga doble clic en el programa de instalación en la ubicación de los archivos de inicio.

- El programa de instalación para los ordenadores de Windows se denomina setup.exe.
- El programa de instalación para los ordenadores Mac se denomina Sophos Anti-Virus.mpkg.

Un asistente le guiará durante la instalación del software de seguridad de Sophos. Acepte las opciones predeterminadas, excepto las que se explican a continuación.

En la página **Datos de la cuenta de usuario**, escriba la información de la cuenta creada en el paso 2.

4. Una vez finalizada la instalación, ejecute una actualización:

- En los ordenadores de Windows, haga clic con el botón derecho en el icono de Sophos de la bandeja del sistema y haga clic en **Actualizar**.
- En los equipos Mac, haga clic en el icono de Sophos Anti-Virus en la parte derecha de la barra de menús y seleccione **Actualizar** en el menú contextual.

## 12 Comprobar el estado de la red

Para comprobar el estado de la red desde Enterprise Console:

1. Consulte el panel de control de Enterprise Console.  
Si aún no está a la vista, en el menú **Ver**, haga clic en **Panel de control**.  
El panel de control indica cuántos ordenadores:
  - Tienen amenazas detectadas.
  - No están actualizados.
  - No cumplen las políticas.
2. Si utiliza NAC, también puede comprobar si los equipos cumplen la política de NAC:
  - a) En el menú **Herramientas**, haga clic en **Administrar NAC**.
  - b) En NAC Manager, en el menú **Report**, haga clic en **Compliance**.

## 13 Proteger ordenadores independientes

Algunos ordenadores están siempre fuera de la red y no es fácil acceder a ellos, como los usados fuera de la oficina. Para protegerlos, cada usuario debe instalar el software de seguridad de Sophos usando un programa de instalación “independiente”. El software se actualiza a través de Internet. Existen tres planteamientos posibles:

- El usuario puede descargar el software desde Sophos, que se actualizará de forma automática desde la misma ubicación. Consulte el artículo de la base de conocimiento 41141 (<http://esp.sophos.com/support/knowledgebase/article/41141.html>).
- Puede ofrecer el software y las actualizaciones posteriores en su propio sitio web, desde donde el usuario descargará el programa y sus actualizaciones. Para más información sobre cómo volver a publicar las actualizaciones de Sophos en su sitio web, consulte el artículo de soporte de la base de conocimiento 12134 (<http://esp.sophos.com/support/knowledgebase/article/12134.html>) de Sophos.
- Puede copiar el software en un CD-ROM y enviarlo al usuario. El usuario instalará el programa y lo configurará para actualizarse desde la ubicación que prefiera. Consulte el artículo de la base de conocimiento de Sophos 13093 (<http://esp.sophos.com/support/knowledgebase/article/13093.html>).

### 13.1 Enviar información necesaria a usuarios independientes

Envíe la información siguiente a los usuarios que no estén en la red:

- La ubicación desde la que pueden descargar el software de seguridad (salvo que les entregue el programa en un CD-ROM).
- La *Guía de inicio independiente de Sophos Endpoint Security and Control 9.5*.
- El nombre de usuario y la contraseña que necesitan (tanto si lo descargan directamente de Sophos como desde su sitio web).

Al enviar el nombre de usuario y la contraseña:

- No los envíe por correo electrónico si el ordenador está infectado, ya que pueden ser robadas.
- Si es necesario, envíelos por fax o por correo postal ordinario.

## 14 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](mailto: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.

## 15 Aviso legal

Copyright © 2009–2010 Sophos Group. 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 Plc y Sophos Group. Todos los demás nombres de productos o empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.

### **ACE™, TAO™, CIAO™, and CoSMIC™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source<sup>10</sup>, 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 us<sup>11</sup> know so we can promote your project in the DOC software success stories<sup>12</sup>.

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 companies<sup>13</sup> 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 ACE<sup>14</sup>, TAO<sup>15</sup>, CIAO<sup>16</sup>, and CoSMIC<sup>17</sup> web sites are maintained by the DOC Group<sup>18</sup> at the Institute for Software Integrated Systems (ISIS)<sup>19</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>20</sup> for the development of open-source software as part of the open-source software community<sup>21</sup>. 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 me<sup>22</sup> know.

Douglas C. Schmidt<sup>23</sup>

### **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. <http://www.the-it-resource.com/Open-Source/Licenses.html>
11. [mailto:doc\\_group@cs.wustl.edu](mailto:doc_group@cs.wustl.edu)
12. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
13. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
14. <http://www.cs.wustl.edu/~schmidt/ACE.html>
15. <http://www.cs.wustl.edu/~schmidt/TAO.html>
16. <http://www.dre.vanderbilt.edu/CIAO/>
17. <http://www.dre.vanderbilt.edu/cosmic/>
18. <http://www.dre.vanderbilt.edu/>
19. <http://www.isis.vanderbilt.edu/>
20. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
21. <http://www.opensource.org/>
22. <mailto:d.schmidt@vanderbilt.edu>
23. <http://www.dre.vanderbilt.edu/~schmidt/>

### **Apache**

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license

agreement for any such included software can be found at <http://www.apache.org/licenses/LICENSE-2.0>.

### **Common Public License**

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to [support@sophos.com](mailto:support@sophos.com) or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

### **ConvertUTF**

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

### **iMatix SFL**

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

### **OpenSSL cryptographic toolkit**

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998–2006 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:  
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).  
This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

#### **Original SSLeay license**

Copyright © 1995–1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)) All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]