

**SOPHOS**

Security made simple.

# Sophos Enterprise Console

## Guía avanzada de inicio

En el caso de SEC distribuido:

Versión: 5.5



# Contenido

1	Acerca de esta guía.....	4
2	Planificar la instalación.....	5
2.1	Planificar la instalación de Enterprise Console.....	5
2.2	Planificar la seguridad de la base de datos.....	7
2.3	Planificar los grupos de ordenadores.....	7
2.4	Planificar las políticas de seguridad.....	7
2.5	Planificar la búsqueda de ordenadores en red.....	8
2.6	Planificar la protección de ordenadores.....	8
3	Requisitos del sistema.....	9
3.1	Hardware y sistema operativo.....	9
3.2	Software de Microsoft.....	9
3.3	Requisitos de puertos.....	10
4	Cuentas necesarias.....	11
4.1	Cuenta de la base de datos.....	11
4.2	Cuenta del gestor de actualización.....	11
5	Dónde instalar los componentes de Enterprise Console.....	13
5.1	Bases de datos instaladas en otro servidor.....	14
5.2	Gestor de actualización adicional instalado en otro servidor.....	14
6	Problema 1: Bases de datos instaladas en otro servidor.....	16
6.1	Descargar el programa de instalación.....	16
6.2	Instalar la base de datos de SEC.....	16
6.3	Instalar SEC: consola de administración, servidor de administración, gestor de actualización.....	17
6.4	Instalar una consola de administración de SEC adicional.....	18
6.5	Descargar software de seguridad.....	19
7	Problema 2: Gestor de actualización adicional instalado en otro servidor.....	22
7.1	Descargar el programa de instalación.....	22
7.2	Instalar SEC: todos los componentes.....	23
7.3	Instalar una consola de administración de SEC adicional.....	23
7.4	Instalar un gestor de actualización adicional.....	24
7.5	Descargar software de seguridad.....	25
8	Publicar el software de seguridad en un servidor web.....	32
9	Crear grupos de ordenadores.....	33
10	Configurar políticas de seguridad.....	34
10.1	Políticas predeterminadas.....	34

10.2	Configurar una política de cortafuegos.....	34
10.3	Crear o editar una política.....	35
10.4	Aplicar una política a un grupo.....	35
11	Buscar ordenadores.....	36
12	Preparación para proteger ordenadores.....	37
12.1	Preparar la eliminación de software de terceros.....	37
12.2	Comprobar que tiene una cuenta que puede utilizar para instalar software.....	37
12.3	Preparar la instalación del software antivirus.....	38
13	Proteger ordenadores.....	39
13.1	Proteger ordenadores Windows de forma automática.....	39
13.2	Proteger los ordenadores Windows o Mac de forma manual.....	40
13.3	Proteger equipos Linux y UNIX.....	40
14	Comprobar el estado de la red.....	41
15	Proteger ordenadores independientes.....	42
15.1	Enviar información necesaria a usuarios independientes.....	42
16	Soporte técnico.....	43
17	Aviso legal.....	44

# 1 Acerca de esta guía

En esta guía se describe la instalación inicial del software de seguridad de Sophos en redes complejas o que cuenten con más de 1.000 estaciones. Cubre la instalación en Windows y Mac.

**Nota:** las funciones que no se incluyan en su licencia no estarán disponibles.

Para realizar la instalación en una red sencilla de menos de 1.000 estaciones con Windows y Mac, es preferible que consulte la Guía rápida de inicio *de Sophos Enterprise Console* en vez de esta guía.

Para realizar la instalación en estaciones Linux o UNIX, además de esta guía debe consultar también la *Guía de inicio de Sophos Enterprise Console para Linux y UNIX*.

Para realizar una actualización, consulte la *Guía de actualización de Sophos Enterprise Console*.

La documentación de Sophos Enterprise Console se encuentra publicada en [www.sophos.com/es-es/support/documentation/enterprise-console.aspx](http://www.sophos.com/es-es/support/documentation/enterprise-console.aspx).

## 2 Planificar la instalación

Para proteger los ordenadores, es necesario:

1. Instalar Sophos Enterprise Console.
2. Descargar el software de seguridad a una unidad compartida en la red.
3. Publicar el software de seguridad en un servidor web.
4. Crear grupos de ordenadores.
5. Establecer las políticas de seguridad para esos grupos.
6. Buscar los ordenadores en la red y ponerlos en los grupos.
7. Proteger los ordenadores.
8. Comprobar el estado de la red.
9. 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 Enterprise Console

Sophos Enterprise Console permite instalar y administrar software de seguridad en los equipos.

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>Bases 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.

#### 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 la administración delegada a la consola y cómo quiera dividir el entorno informático en subentornos:

- La *administración delegada* de la consola de administración requiere 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 administración delegada y la creación de subentornos, vaya a [www.sophos.com/es-es/support/knowledgebase/63556.aspx](http://www.sophos.com/es-es/support/knowledgebase/63556.aspx).

## Bases 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 las bases de datos en el mismo servidor que los demás componentes de Enterprise Console o en un servidor dedicado diferente.

**Nota:** si necesita instalar las bases de datos en un servidor seguro con un script o en un clúster SQL, consulte [www.sophos.com/es-es/support/knowledgebase/33980.aspx](http://www.sophos.com/es-es/support/knowledgebase/33980.aspx).

**Importante:** la base de datos de Sophos Auditing, **SophosSecurity**, debe encontrarse activa con las otras bases de datos de Enterprise Console, incluso si no desea hacer uso de la auditoría. Esto se debe a que esta base de datos también se utiliza para el control de acceso mejorado.

## 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. De forma predeterminada, el gestor coloca el software para estaciones y las actualizaciones en la unidad compartida UNC SophosUpdate. 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.

Como norma general, se recomienda instalar un gestor de actualización adicional por cada 25 000 ordenadores cliente en la red. También se aconseja instalar un gestor de actualización adicional en una ubicación remota para ahorrar ancho de banda al actualizar unidades compartidas de actualización en dicha ubicación y evitar que queden incompletas si se pierde la conexión.

Las rutas UNC configuradas como unidades compartidas de actualización deben utilizarse para un máximo de 1000 ordenadores, a menos que se encuentren en servidores de archivos dedicados. Con una ubicación web, es posible actualizar hasta alrededor de 10 000 ordenadores.

## 2.2 Planificar la seguridad de la base de datos

### Audite la base de datos

Además de la protección integral de las bases de datos de Enterprise Console, se recomienda establecer un control de la instancia del servidor SQL para auditar la actividad en la base de datos SophosSecurity.

Por ejemplo, si utiliza SQL Server 2008 Enterprise Edition , puede utilizar la función SQL Server Audit. Versiones anteriores de SQL Server disponen de auditoría de inicio de sesión, de cambios y eventos.

Para más información sobre estas funciones, consulte la documentación de SQL Server. Por ejemplo:

- [SQL Server Audit \(motor de base de datos\)](#)
- [Auditoría \(motor de base de datos\), SQL Server 2008 R2](#)
- [Auditoría en SQL Server 2008](#)
- [Auditoría \(motor de base de datos\), SQL Server 2008](#)

### Cifre la conexión a la base de datos

Se recomienda cifrar la comunicación entre los clientes y las bases de datos de Enterprise Console. Para más información, consulte la documentación de SQL Server:

- [Habilitar conexiones cifradas en el motor de base de datos \(Administrador de configuración de SQL Server\)](#)
- [Cifrar conexiones a SQL Server 2008 R2](#)
- [Cómo habilitar el cifrado SSL para una instancia de SQL Server mediante Microsoft Management Console](#)

### Controle el acceso a las copias de seguridad de la base de datos

Imponga un control de acceso restrictivo a las copias de seguridad o copias de la base de datos. De esta forma evitará el acceso no autorizado a los archivos.

**Nota:** Los enlaces en esta sección llevan a sitios web de terceros y se incluyen como ayuda. El contenido de estas páginas podría cambiar sin nuestro conocimiento.

## 2.3 Planificar los grupos de ordenadores

Decida cómo desea agrupar los ordenadores que va a proteger. Para más información, consulte [www.sophos.com/es-es/support/knowledgebase/63556.aspx](http://www.sophos.com/es-es/support/knowledgebase/63556.aspx).

## 2.4 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 políticas de Sophos Enterprise Console*.

## 2.5 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.

## 2.6 Planificar la protección de ordenadores

Puede instalar el software de seguridad de forma automática desde Enterprise Console en estaciones de trabajo con sistema operativo Windows.

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

Si dispone de otros sistemas operativos en su red, deberá instalar el software de forma manual, 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 Enterprise Console para Linux y UNIX*.

## 3 Requisitos del sistema

**Consejo:** utilice el programa de instalación de Enterprise Console para comprobar los requisitos de instalación, aunque no desee realizar la instalación en ese momento. En la página **Comprobación de las propiedades del sistema** del asistente podrá se ofrece la información necesaria. Si no desea continuar con la instalación, haga clic en **Cancelar** para cerrar el asistente. Para más información sobre la comprobación de requisitos, consulte <http://www.sophos.com/es-es/support/knowledgebase/113945.aspx>.

### 3.1 Hardware y sistema operativo

Consulte la página de requisitos del sistema en la web de Sophos ([www.sophos.com/es-es/products/all-system-requirements.aspx](http://www.sophos.com/es-es/products/all-system-requirements.aspx)).

### 3.2 Software de Microsoft

Enterprise Console requiere ciertos productos de Microsoft (por ejemplo, base de datos).

El programa de instalación de Enterprise Console intentará instalar el software necesario. Sin embargo, en ciertos casos el software puede no ser compatible con su sistema operativo o es necesario instalarlo de forma manual.

**Nota:** Tras instalar el software adicional, puede que tenga que reiniciar el sistema. Para más información, vea <https://www.sophos.com/es-es/support/knowledgebase/65190.aspx>.

#### Instalación del servidor SQL

El programa de instalación intenta instalar SQL Server 2012 Express Edition SP2, a menos que disponga de SQL Server 2005 Express o posterior. Tenga en cuenta que:

- No se recomienda instalar SQL Server en un controlador de dominio.
- Si desea instalar las bases de datos de Enterprise Console en otro servidor, asegúrese de que dispone de acceso remoto al servidor SQL. Para más información, vea <https://www.sophos.com/es-es/support/knowledgebase/118473.aspx>.

#### Instalación de .NET Framework

El programa de instalación instala .NET Framework 4.5.2, a menos que ya esté instalada una versión 4.x.

**Importante:** Durante la instalación de .NET Framework 4.5.2 se reinician ciertos servicios del sistema (como IIS Admin Service).

Puede que se solicite reiniciar el sistema tras instalar .NET Framework 4.5.2. Si es así, se recomienda hacerlo lo antes posible.

## Instalación de Microsoft Message Queuing

El programa de instalación intentará instalar Microsoft Message Queuing (MSMQ), a menos que ya esté instalado.

**Importante:** Durante la instalación de MSMQ se detienen de forma temporal los siguientes servicios: MSDTC, MSSQLServer, SQLSERVERAGENT. Esto interrumpirá el acceso a la base de datos predeterminada del servidor SQL. Asegúrese de que los servicios se pueden interrumpir de forma segura. Compruebe a continuación que los servicios se reinician correctamente.

### 3.3 Requisitos de puertos

Enterprise Console requiere acceso a través de ciertos puertos. Para más información, vea [www.sophos.com/es-es/support/knowledgebase/38385.aspx](http://www.sophos.com/es-es/support/knowledgebase/38385.aspx).

## 4 Cuentas necesarias

Antes de instalar el software de Sophos, debe crear las cuentas necesarias:

- **Cuenta de la base de datos.** Esta cuenta de Windows permite al servicio de administración de Enterprise Console acceder a la base de datos. Otros servicios de Sophos también utilizan esta cuenta.

Se recomienda utilizar una cuenta con el nombre **SophosManagement**.

- **Cuenta del gestor de actualización.** Esta cuenta de Windows permite a las estaciones acceder a las actualizaciones del software.

Se recomienda utilizar una cuenta con el nombre **SophosUpdateMgr**.

### 4.1 Cuenta de la base de datos

La cuenta de la base de datos debe:

- Permitir el inicio de sesión en el equipo con el servidor de administración de Sophos (componente de Enterprise Console).
- Disponer de acceso de lectura y escritura en el directorio temporal del sistema, como "windows\temp". Por defecto, miembros del grupo "Usuarios" disponen de estos permisos.
- Disponer de nombre principal de usuario (UPN), si se trata de una cuenta de dominio.

El resto de permisos y pertenencia de grupos se realiza de forma automática durante la instalación.

Sophos recomienda que la cuenta:

- No tenga fecha de caducidad ni ninguna otra restricción para el inicio de sesión.
- No sea una cuenta de administrador.
- No se modifique tras la instalación.
- Tenga el nombre **SophosManagement**.

Para obtener recomendaciones e instrucciones paso a paso, vaya a <https://www.sophos.com/es-es/support/knowledgebase/113954.aspx>.

### 4.2 Cuenta del gestor de actualización

La cuenta del gestor de actualización debe disponer de acceso de lectura a la carpeta de actualización del software. Por defecto es: \\[servidor]\SophosUpdate

Sophos recomienda que la cuenta:

- No tenga fecha de caducidad ni ninguna otra restricción para el inicio de sesión.
- No sea una cuenta de administrador.
- Dispone de nombre principal de usuario (UPN), si se trata de una cuenta de dominio.
- Tenga el nombre **SophosUpdateMgr**.

Para obtener recomendaciones e instrucciones paso a paso, vaya a <https://www.sophos.com/es-es/support/knowledgebase/113954.aspx>.

## 5 Dónde instalar los componentes de Enterprise Console

Sophos Enterprise Console (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>Bases 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.

Si instala los componentes de SEC en diferentes servidores, se recomienda que los servidores se encuentren en el mismo dominio.

No se recomienda instalar las bases de datos de SEC en un controlador de dominio.

En esta guía se describen dos situaciones de instalación:

- Bases de datos instaladas en otro servidor
- Gestor de actualización adicional instalado en otro servidor

En cada una de ellas, los componentes de SEC se distribuyen a la red de forma diferente.

## 5.1 Bases de datos instaladas en otro servidor

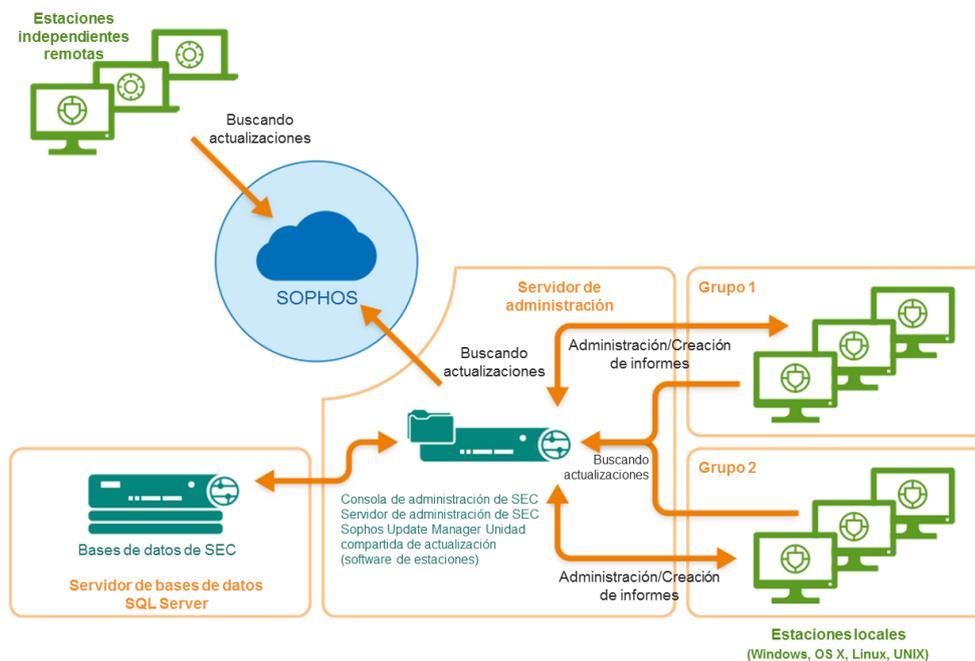


Figura 1: Implementación de ejemplo: bases de datos instaladas en otro servidor

En este caso, consulte [Problema 1: Bases de datos instaladas en otro servidor](#) en la página 16.

## 5.2 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.

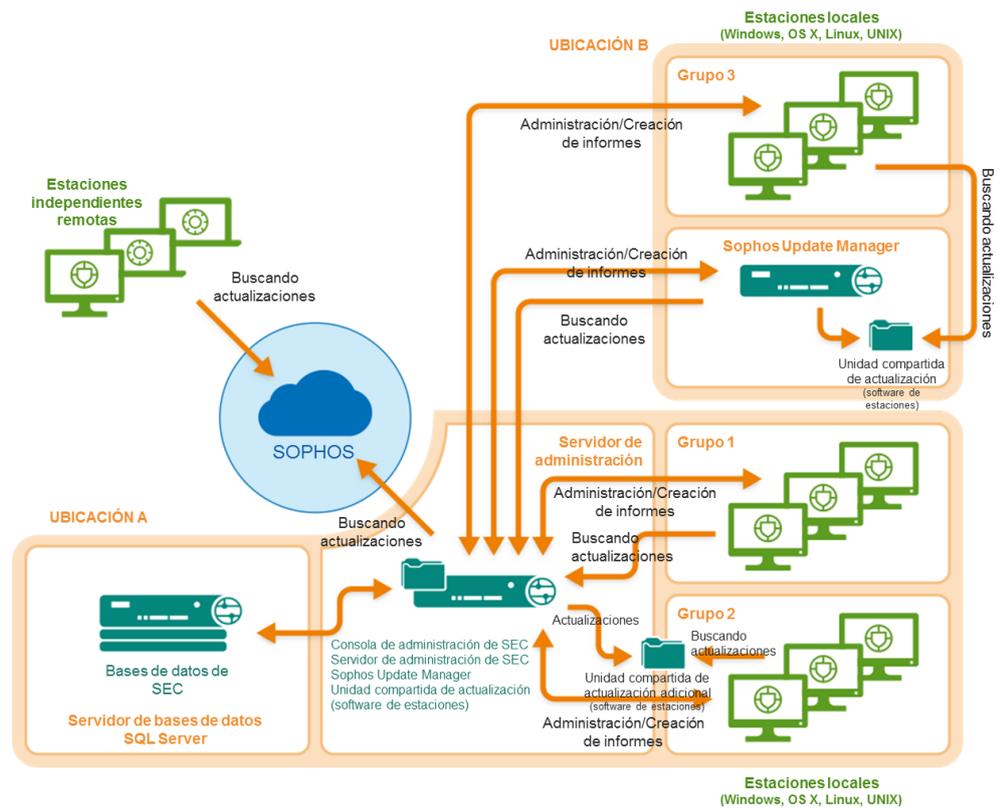


Figura 2: Implementación de ejemplo: gestor de actualización adicional actualizado desde el gestor de actualización principal

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 [Problema 2: Gestor de actualización adicional instalado en otro servidor](#) en la página 22.

## 6 Problema 1: Bases de datos instaladas en otro servidor

### 6.1 Descargar el programa de instalación

**Nota:** Puede descargar los programas de instalación desde cualquier ordenador y después copiarlos al ordenador donde desea utilizarlos.

1. Inicie sesión en <https://www.sophos.com/es-es/support/downloads.aspx> con su Sophos ID.

**Nota:** Si necesita ayuda con su Sophos ID, consulte el [artículo de la base de conocimiento de Sophos 111195](#).

2. Si ha iniciado sesión para las descargas anteriormente, verá la página **Descargas y actualizaciones de productos**.

**Nota:** Si es la primera vez, verá su perfil. Haga clic en **Endpoint and Server Protection** y luego en **Descargas y actualizaciones**.

3. En **Console**, haga clic en el enlace para **Sophos Enterprise Console** y descargue el programa de instalación.

### 6.2 Instalar la base de datos de SEC

**Nota:** si necesita instalar las bases de datos en un servidor seguro con un script o en un clúster SQL, consulte [www.sophos.com/es-es/support/knowledgebase/33980.aspx](http://www.sophos.com/es-es/support/knowledgebase/33980.aspx).

En Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinicie el sistema.. Puede activarlo de nuevo después de instalar la base de datos.

Inicie sesión como administrador.

- Si el servidor se encuentra en un dominio, utilice una cuenta de dominio con derechos de administrador local.
- Si el servidor se encuentra en un grupo de trabajo, utilice una cuenta local con derechos de administrador.

1. Haga doble clic en el programa de instalación de 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.

El asistente de instalación le guiará en el proceso de instalación. Acepte las opciones predeterminadas, excepto las siguientes:

- a) En el cuadro de diálogo **Selección de componentes**, compruebe que está seleccionada la opción **Base de datos**, pero no **Consola de administración** ni **Servidor de administración**.
- b) En la página **Detalles de 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. No debería utilizar una cuenta de administrador.

**Nota:** la cuenta de la base de datos se creó en [Cuenta de la base de datos](#) en la página 11.

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.

## 6.3 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.

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

En Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinicie el sistema.. Puede volver a activarlo después de instalar Enterprise Console y suscribirse a las actualizaciones de Sophos.

Inicie sesión como administrador.

- Si el servidor se encuentra en un dominio, utilice una cuenta de dominio con derechos de administrador local.
- Si el servidor se encuentra en un grupo de trabajo, utilice una cuenta local con derechos de administrador.

1. Haga doble clic en el programa de instalación de 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.

El asistente de instalación le guiará en el proceso de instalación. Acepte las opciones predeterminadas, excepto las siguientes:

- a) En el cuadro de diálogo **Selección de componentes**, compruebe que están seleccionadas las opciones **Consola de administración** y **Servidor de administración**, pero no **Base de datos**.
- b) 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. Introduzca una cuenta 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. No debería utilizar una cuenta de administrador.

**Nota:** la cuenta de la base de datos se creó en [Cuenta de la base de datos](#) en la página 11.

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.

## 6.4 Instalar una consola de administración de SEC adicional

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

**Importante:** Debe instalar la misma versión de Enterprise Console que se esté ejecutando en su servidor de administración.

**Nota:** La consola nueva necesita acceder al equipo con el servidor de administración de Enterprise Console. Si dicho equipo utiliza un cortafuegos, configure el cortafuegos para permitir el acceso. Para obtener instrucciones sobre cómo añadir una regla de cortafuegos para permitir el tráfico DCOM de la consola remota al servidor de administración, consulte el [artículo de la base de conocimiento 49028](#).

Para instalar una consola de administración adicional:

En Windows Server 2008 o posterior y Windows Vista o posterior, desactive el Control de cuentas de usuario y reinicie el sistema.. Puede activarlo de nuevo después de instalar la consola de administración.

Inicie sesión como administrador.

- Si el equipo se encuentra en un dominio, utilice una cuenta de dominio con derechos de administrador local.
  - Si el equipo se encuentra en un grupo de trabajo, utilice una cuenta local con derechos de administrador.
1. Haga doble clic en el programa de instalación de 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.  
El asistente de instalación le guiará en el proceso de instalación. Acepte las opciones predeterminadas, excepto las siguientes:
    - a) En el cuadro **Selección de componentes**, compruebe que está seleccionada **Consola de administración**, pero no **Servidor de administración** ni **Base de datos**.
    - b) En el cuadro **Servidor de administración**, escriba el nombre del servidor en el que instaló el servidor de administración Enterprise Console.  
**Nota:** Si cambió el puerto durante la instalación del servidor de administración, especifique ahora el mismo puerto.
    - c) Si se encuentra en un entorno de dominio, introduzca la cuenta de usuario que se utiliza para acceder a las bases de datos de Enterprise Console.

Esta es la cuenta que indicó al instalar la base de datos de Enterprise Console. Es la misma que utiliza el servicio Sophos Management Host en el servidor con el servidor de administración de Enterprise Console.

Cuando termine el asistente, cierre la sesión o reinicie el equipo (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.

## 6.5 Descargar software de seguridad

Para descargar software de seguridad en una ubicación central para distribuirlo 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 19 describe cómo ejecutar el asistente que permite descargar:

- Software de seguridad para todas las plataformas compatibles.
- Solo la versión recomendada en la actualidad.
- Solo 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 20 describe cómo configurar el gestor de actualización directamente para poder descargar:

- Software de seguridad para todas las plataformas compatibles.
- Versiones de avance o anteriores.
- A otras unidades compartidas, como en otros servidores.

### 6.5.1 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**, se iniciará la descarga del 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 32.

## 6.5.2 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.
  - 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:`
  - 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 continúe en [Publicar el software de seguridad en un servidor web](#) en la página 32.

## 7 Problema 2: 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 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 las secciones 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 distribuirlo a las estaciones. Elija la sección adecuada cuando llegue el momento.
- Si puede utilizar la función de parches en Enterprise Console. Para poder utilizar esta función debe seleccionar el primer método.

### 7.1 Descargar el programa de instalación

**Nota:** Puede descargar los programas de instalación desde cualquier ordenador y después copiarlos al ordenador donde desea utilizarlos.

1. Inicie sesión en <https://www.sophos.com/es-es/support/downloads.aspx> con su Sophos ID.

**Nota:** Si necesita ayuda con su Sophos ID, consulte el [artículo de la base de conocimiento de Sophos 111195](#).

2. Si ha iniciado sesión para las descargas anteriormente, verá la página **Descargas y actualizaciones de productos**.

**Nota:** Si es la primera vez, verá su perfil. Haga clic en **Endpoint and Server Protection** y luego en **Descargas y actualizaciones**.

3. En **Console**, haga clic en el enlace para **Sophos Enterprise Console** y descargue el programa de instalación.

## 7.2 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.

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

En Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinicie el sistema.. Puede volver a activarlo después de instalar Enterprise Console y suscribirse a las actualizaciones de Sophos.

Inicie sesión como administrador.

- Si el servidor se encuentra en un dominio, utilice una cuenta de dominio con derechos de administrador local.
- Si el servidor se encuentra en un grupo de trabajo, utilice una cuenta local con derechos de administrador.

1. Haga doble clic en el programa de instalación de 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.

El asistente de instalación le guiará en el proceso de instalación. Acepte las opciones predeterminadas, excepto las siguientes:

- a) En la página **Selección de componentes**, seleccione *todos* los componentes.
- b) En la página **Detalles de la base de datos**, introducir los datos de una cuenta en este servidor. Si el servidor se encuentra en un *dominio*, utilice una cuenta de dominio. Si el servidor se encuentra en un *grupo de trabajo*, utilice una cuenta local del servidor. No debería utilizar una cuenta de administrador.

**Nota:** la cuenta de la base de datos se creó en [Cuenta de la base de datos](#) en la página 11.

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.

## 7.3 Instalar una consola de administración de SEC adicional

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

**Importante:** Debe instalar la misma versión de Enterprise Console que se esté ejecutando en su servidor de administración.

**Nota:** La consola nueva necesita acceder al equipo con el servidor de administración de Enterprise Console. Si dicho equipo utiliza un cortafuegos, configure el cortafuegos para permitir el acceso. Para obtener instrucciones sobre cómo añadir una regla de cortafuegos

para permitir el tráfico DCOM de la consola remota al servidor de administración, consulte el [artículo de la base de conocimiento 49028](#).

Para instalar una consola de administración adicional:

En Windows Server 2008 o posterior y Windows Vista o posterior, desactive el Control de cuentas de usuario y reinicie el sistema.. Puede activarlo de nuevo después de instalar la consola de administración.

Inicie sesión como administrador.

- Si el equipo se encuentra en un dominio, utilice una cuenta de dominio con derechos de administrador local.
- Si el equipo se encuentra en un grupo de trabajo, utilice una cuenta local con derechos de administrador.

1. Haga doble clic en el programa de instalación de 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.

El asistente de instalación le guiará en el proceso de instalación. Acepte las opciones predeterminadas, excepto las siguientes:

- a) En el cuadro **Selección de componentes**, compruebe que está seleccionada **Consola de administración**, pero no **Servidor de administración** ni **Base de datos**.
- b) En el cuadro **Servidor de administración**, escriba el nombre del servidor en el que instaló el servidor de administración Enterprise Console.

**Nota:** Si cambió el puerto durante la instalación del servidor de administración, especifique ahora el mismo puerto.

- c) Si se encuentra en un entorno de dominio, introduzca la cuenta de usuario que se utiliza para acceder a las bases de datos de Enterprise Console.

Esta es la cuenta que indicó al instalar la base de datos de Enterprise Console. Es la misma que utiliza el servicio Sophos Management Host en el servidor con el servidor de administración de Enterprise Console.

Cuando termine el asistente, cierre la sesión o reinicie el equipo (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.

## 7.4 Instalar un gestor de actualización adicional

**Importante:** si desea instalar una consola de administración de SEC adicional en el mismo equipo en el que desea instalar un gestor de actualización adicional, debe instalar primero la consola, como se describe en [Instalar una consola de administración de SEC adicional](#) en la página 23.

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.

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

En Windows Server 2008 o posterior, active la Detección de redes y reinicie el sistema.

En Windows Server 2008 o posterior, desactive el Control de cuentas de usuario y reinicie el sistema.. Puede volver a activarlo después de instalar el gestor de actualización y suscribirse a las actualizaciones de Sophos.

Inicie sesión como administrador.

- Si el servidor se encuentra en un dominio, utilice una cuenta de dominio con derechos de administrador local.
  - Si el servidor se encuentra en un grupo de trabajo, utilice una cuenta local con derechos de administrador.
1. Localice 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.  
El asistente de instalación le guiará en el proceso de instalación. Acepte los valores predeterminados.

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

## 7.5 Descargar software de seguridad

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 25
- [Gestor de actualización adicional con actualización desde Sophos](#) en la página 29

### 7.5.1 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 26 describe cómo ejecutar el asistente que permite descargar:

- Software de seguridad para todas las plataformas compatibles.
- 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 26 describe cómo configurar el gestor de actualización principal directamente para poder descargar:

- Software de seguridad para todas las plataformas compatibles.
- Versiones anteriores.
- A otras unidades compartidas, como en otros servidores.

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 28 describe cómo configurar el gestor de actualización adicional para que se actualice desde el gestor de actualización principal.

### 7.5.1.1 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**, se iniciará la descarga del 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 28.

### 7.5.1.2 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.
  - 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.

### 7.5.1.3 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 **Suscrito**. 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:`
  - 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 continúe en [Publicar el software de seguridad en un servidor web](#) en la página 32.

## 7.5.2 Gestor de actualización adicional con actualización desde Sophos

La sección [Configurar el gestor de actualización adicional](#) en la página 29 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 30 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.

### 7.5.2.1 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.
  - 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.

### 7.5.2.2 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 **Suscrito**. 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:
  - 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 continúe en [Publicar el software de seguridad en un servidor web](#) en la página 32.

## 8 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. Esto puede ser especialmente útil para aquellos ordenadores que no siempre están conectados a la red.

- Para publicar el software de seguridad en un servidor web, consulte [www.sophos.com/es-es/support/knowledgebase/38238.aspx](http://www.sophos.com/es-es/support/knowledgebase/38238.aspx).

## 9 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 34.

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**. Asegúrese de que el grupo **No asignados** no se encuentra seleccionado.
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.

## 10 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.

### 10.1 Políticas predeterminadas

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

- Deberá configurar una política cortafuegos inmediatamente.
- Para utilizar estas funciones, modifique las políticas de restricción de aplicaciones, control de dispositivos, protección contra manipulaciones, parches, prevención de vulnerabilidades o control web. Puede hacerlo en cualquier momento.

Para más información sobre las opciones de las políticas, consulte la Guía de configuración de políticas de Sophos Enterprise Console.

### 10.2 Configurar una política de cortafuegos

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

1. En , en el panel **Políticas**, haga clic con el botón derecho en **Cortafuegos** y seleccione **Crear política**.

Una **Nueva política** se añadirá a la lista y se destacará su nombre. Escriba el nombre que desee utilizar para la política.

2. Haga doble clic en la política para modificarla.

Se inicia un asistente.

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

## 10.3 Crear o editar una política

1. En Enterprise Console, si no se muestra 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.

## 10.4 Aplicar una política a un grupo

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

**Nota:** si lo prefiere, haga clic con el botón derecho del ratón en el grupo y seleccione **Ver/editar políticas del grupo**. A continuación, puede seleccionar las políticas para ese grupo desde los menús desplegables.

# 11 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 **Detectar 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 **Detectar**, los equipos se colocan en el grupo **No asignados**.

## 12 Preparación para proteger ordenadores

### 12.1 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.
 

**Nota:** es posible que HitmanPro.Alert ya esté instalado como producto independiente o desde Sophos Central. Debe eliminar HitmanPro.Alert antes de aplicar la administración local desde Sophos Enterprise Console.
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.

### 12.2 Comprobar que tiene una cuenta que puede utilizar para instalar software

Deberá introducir los datos de una cuenta de Windows que permita instalar el software de seguridad Deberá:

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

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

Recomendamos que la cuenta:

- No sea una cuenta de administrador de dominio ni esté configurada para la delegación restringida.
- No tenga derechos administrativos o cualquier privilegio adicional en los ordenadores en los que Enterprise Console gestiona las actualizaciones adicionales o donde están instalados los repetidores de mensajes.
- Tenga derechos de escritura o de modificar permisos en la ubicación desde la que se actualizan los ordenadores.
- Se utiliza únicamente para proteger los ordenadores y no se usa para tareas administrativas generales.
- Cambia su contraseña con frecuencia.

## 12.3 Preparar la instalación del software antivirus

Puede que tenga que preparar los equipos antes de instalar el software antivirus. Para obtener asesoramiento, consulte la guía de implementación de Sophos en estaciones de trabajo ([https://docs.sophos.com/esg/enterprise-console/tools/deployment\\_guide/es-es/index.html](https://docs.sophos.com/esg/enterprise-console/tools/deployment_guide/es-es/index.html)), en particular la sección de preparación de equipos informáticos para la implementación.

Le recomendamos que disponga de un firewall activo en los ordenadores que esté protegiendo.

**Nota:** Una vez que haya protegido con éxito los ordenadores y aparezcan como administrados en Enterprise Console, considere la posibilidad de deshabilitar aquellas excepciones en el firewall que hayan sido específicamente añadidas para permitir la implementación remota en los ordenadores.

# 13 Proteger ordenadores

## 13.1 Proteger ordenadores Windows de forma automática

En esta sección se describe cómo utilizar Enterprise Console para proteger ordenadores Windows de forma automática.

Si lo desea, puede utilizar sus propias herramientas o scripts para instalar la protección en ordenadores Windows. Para más información, consulte [www.sophos.com/es-es/support/knowledgebase/114191.aspx](http://www.sophos.com/es-es/support/knowledgebase/114191.aspx).

**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. Escoja una de las siguientes opciones:
  - Si los ordenadores que desea proteger ya están en un grupo, selecciónelos, haga clic con el botón derecho y seleccione **Proteger ordenadores**.
  - 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:

- a) En el cuadro de diálogo **Seleccionar funciones**, seleccione las funciones adicionales que desea instalar.
- b) En la página **Resumen de protección**, podrá ver cualquier problema de instalación. Si necesita ayuda, consulte [Solución de problemas](#) en la página 39.
- c) 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 comprobar la lista de equipos. En la columna **En acceso**, **Activo** quiere decir que el escaneo en acceso está activado.

### 13.1.1 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 la instalación de forma manual. Consulte [Proteger los ordenadores Windows o Mac de forma manual](#) en la página 40. 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.

- Las reglas con las que se ha configurado el Firewall están bloqueando el acceso necesario para implementar el software de seguridad.
- 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.

## 13.2 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. Esta carpeta se conoce como la ubicación de los archivos de inicio.

Debe disponer de derechos de administrador en los equipos que desea proteger.

Para proteger los ordenadores Windows o Mac de forma manual:

1. En Enterprise Console, en el menú **Ver**, seleccione **Ubicación de archivos de inicio**.

Se mostrará una lista con las ubicaciones disponibles. Anote la ubicación para cada sistema operativo que desee proteger.

2. En todos los ordenadores que desee proteger, acceda a la ubicación de los archivos de inicio y haga lo siguiente:
  - En Windows, localice el archivo `setup.exe` y haga doble clic.
  - Para Mac, copie el archivo instalador `Sophos Installer.app` y el directorio `Sophos Installer Components` en la ubicación que desee (por ejemplo, el escritorio) y haga doble clic.

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

- En Windows, en la página **Datos de la cuenta de usuario**, escriba la información de la cuenta que seleccionó para Update Manager. Esto lo hizo cuando instaló Enterprise Console, en [Cuenta del gestor de actualización](#) en la página 11.

**Consejo:** Si no está seguro de qué cuenta utilizar, puede seleccionar una cuenta con privilegios limitados que tenga acceso a la ubicación correspondiente. Enterprise Console aplicará una política con la cuenta de acceso necesaria.

## 13.3 Proteger equipos Linux y UNIX

Para más información sobre cómo proteger ordenadores Linux y UNIX, consulte la *Guía de inicio de Enterprise Console para Linux y UNIX*.

## 14 Comprobar el estado de la red

Para comprobar el estado de la red desde Enterprise Console:

1. Vea 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.

## 15 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 dos planteamientos posibles:

- El usuario puede descargar el software desde [www.sophos.com/es-es/support/downloads/standalone-installers/esc-for-windows-2000-up.aspx](http://www.sophos.com/es-es/support/downloads/standalone-installers/esc-for-windows-2000-up.aspx). Instalarlo y configurarlo para que se actualice desde Sophos.
- Puede ofrecer el software y las actualizaciones posteriores en su propio sitio web. El usuario puede descargar el software desde dicho sitio web, instalarlo y configurarlo para actualizarse desde el sitio web. Para más información sobre cómo ofrecer las actualizaciones de Sophos en su sitio web, consulte [www.sophos.com/es-es/support/knowledgebase/38238.aspx](http://www.sophos.com/es-es/support/knowledgebase/38238.aspx).

### 15.1 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*.
- 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.

## 16 Soporte técnico

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

- Visitar el fórum Sophos Community en [community.sophos.com/](https://community.sophos.com/) para consultar casos similares.
- Visitar la base de conocimiento de Sophos en [www.sophos.com/es-es/support.aspx](https://www.sophos.com/es-es/support.aspx).
- Descargar la documentación correspondiente desde [www.sophos.com/es-es/support/documentation.aspx](https://www.sophos.com/es-es/support/documentation.aspx).
- Abrir un ticket de incidencia con nuestro equipo de soporte en <https://secure2.sophos.com/support/contact-support/support-query.aspx>.

## 17 Aviso legal

Copyright © 2009–2017 Sophos Limited. Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, mecánico, grabación, fotocopia o cualquier otro sin la correspondiente licencia del producto, bajo dichos términos, o sin la previa autorización escrita por parte del propietario.

Sophos, Sophos Anti-Virus y SafeGuard son marcas registradas de Sophos Limited, Sophos Group y Utimaco Safeware AG, según corresponda. Todos los demás nombres de productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by [Douglas C. Schmidt](#) and his [research group](#) at [Washington University](#), [University of California, Irvine](#), and [Vanderbilt University](#), Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available 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 any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

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 misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way 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](#) know so we can promote your project in the [DOC software success stories](#).

The [ACE](#), [TAO](#), [CIAO](#), [DAnCE](#), and [CoSMIC](#) web sites are maintained by the [DOC Group](#) at the [Institute for Software Integrated Systems](#) (ISIS) and the [Center for Distributed Object Computing](#) of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, 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. 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.

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](#) 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. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, 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. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let [me](#) know.

[Douglas C. 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>

## Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Common Public License

The Sophos software that is referenced 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 <https://www.sophos.com/en-us/support/contact-support.aspx>. 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.

## Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## Microsoft Public License (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

### 1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

## 2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

## 3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

A copy of the MS-PL terms can be found at <https://opensource.org/licenses/MS-PL>.

## OpenSSL Cryptography and SSL/TLS 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 © 1998–2016 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 ([eay@cryptsoft.com](mailto:eay@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 ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)) All rights reserved.

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto:eay@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](mailto: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](mailto: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 license 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 license [including the GNU Public License.]

## WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

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

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

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "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 COPYRIGHT HOLDER 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.

## Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: <https://sourceforge.net/projects/wtl/files/>

## zlib data compression library

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly [jloup@gzip.org](mailto:jloup@gzip.org)

Mark Adler [madler@alumni.caltech.edu](mailto:madler@alumni.caltech.edu)