

SOPHOS

Security made simple.

Sophos Enterprise Console

Guía rápida de inicio

Versión: 5.5



Contenido

1	Acerca de esta guía.....	4
2	Productos a instalar.....	5
3	Pasos clave.....	6
4	Descargar el programa de instalación de Enterprise Console.....	7
4.1	Si dispone de licencia de Sophos.....	7
4.2	Si desea evaluar Enterprise Console.....	7
5	Comprobar los requisitos del sistema.....	8
5.1	Hardware y sistema operativo.....	8
5.2	Software de Microsoft.....	8
5.3	Requisitos de puertos.....	9
6	Cuentas necesarias.....	10
6.1	Cuenta de la base de datos.....	10
6.2	Cuenta del gestor de actualización.....	10
7	Preparar la instalación.....	12
8	Instalar Enterprise Console.....	13
9	Mejorar la seguridad de la base de datos.....	14
10	Instalar una consola de administración remota adicional.....	15
11	Descargar el software de seguridad.....	17
12	Crear grupos de ordenadores.....	18
13	Configurar políticas de seguridad.....	19
13.1	Configurar una política de cortafuegos.....	19
14	Buscar ordenadores.....	20
15	Preparar la protección de ordenadores.....	21
15.1	Preparar la eliminación de software de terceros.....	21
15.2	Comprobar que tiene una cuenta que puede utilizar para instalar software.....	21
15.3	Preparar la instalación del software antivirus.....	22
16	Proteger ordenadores.....	23
16.1	Proteger ordenadores Windows de forma automática.....	23
16.2	Proteger los ordenadores Windows o Mac de forma manual.....	24
16.3	Proteger equipos Linux.....	24
17	Comprobar el estado de la red.....	25
18	Solución de problemas.....	26
19	Ayuda para tareas habituales.....	27
20	Soporte técnico.....	28

21 Aviso legal.....29

1 Acerca de esta guía

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

Esta guía le resultará útil si está instalando el software por primera vez.

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

Documentación relacionada

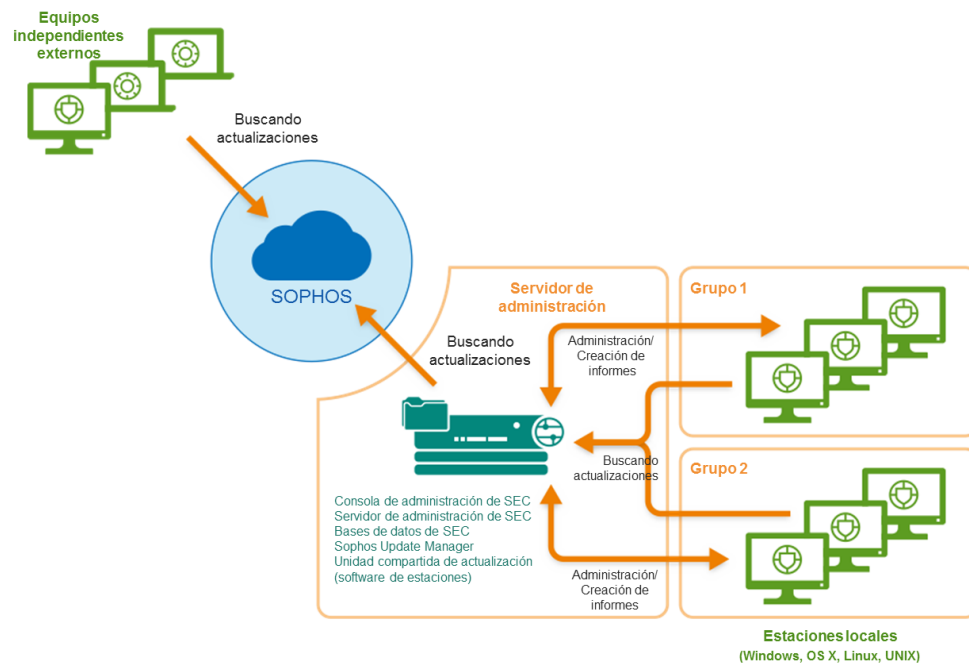
Si cuenta con una red muy grande, tenga en cuenta las opciones de instalación descritas en la *Guía avanzada de inicio de Sophos Enterprise Console*.

La documentación de Sophos se encuentra en <http://www.sophos.com/es-es/support/documentation.aspx>.

2 Productos a instalar

Para proteger los equipos de la red, se instala:

- **Sophos Enterprise Console** en el servidor. Esto le permitirá instalar y administrar el software de seguridad de Sophos.
- El **software de seguridad de Sophos** en las estaciones. Esto le permite proteger los ordenadores contra amenazas y enviar alertas a Enterprise Console.



3 Pasos clave

Los pasos a realizar son:

- Descargar el programa de instalación de Enterprise Console.
- Comprobar los requisitos del sistema.
- Crear las cuentas necesarias.
- Preparar la instalación.
- Instalar Enterprise Console.
- Descargar el software de seguridad.
- Crear grupos de ordenadores.
- Configurar políticas de seguridad.
- Buscar ordenadores.
- Prepare la protección de los ordenadores
- Proteger los ordenadores.
- Comprobar el estado de la red.

4 Descargar el programa de instalación de Enterprise Console

4.1 Si dispone de licencia de Sophos

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.

4.2 Si desea evaluar Enterprise Console

1. Vaya a <http://www.sophos.com/es-es/products/free-trials/endpoint-protection.aspx>.
2. Cumplimente el formulario de registro.

Tras enviar el formulario se le proporcionarán las credenciales de evaluación. También recibirá un email con la información necesaria. Necesitará estos datos al configurar Enterprise Console.

3. Haga clic en **Descargar** para obtener el programa de instalación de Enterprise Console.

5 Comprobar los requisitos del sistema

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

5.1 Hardware y sistema operativo

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

5.2 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.

5.3 Requisitos de puertos

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

6 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**.

6.1 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>.

6.2 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>.

7 Preparar la instalación

Para preparar la instalación:

- Compruebe que cuenta con una conexión a Internet.
- Compruebe que cuenta con los CD-ROM de Windows y de los Service Packs. Puede que los necesite durante la instalación.
- Desactive el Control de cuentas de usuario si se encuentra activado y reinicie el servidor.

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

8 Instalar Enterprise Console

Para instalar Enterprise Console:

1. En el equipo en el que desea instalar Enterprise Console, 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.
2. Localice el programa de instalación de Enterprise Console que descargó antes.
3. Haga doble clic en el programa de instalación.
4. Haga clic en **Instalar**.

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

5. El asistente le guiará en el proceso de instalación. Haga lo siguiente:
 - a) Utilice las opciones predeterminadas si es posible.
 - b) En la página **Selección de componentes**, seleccione todos los componentes.
 - c) En la página **Comprobación de las propiedades del sistema**, revise el resultado y realice las acciones necesarias. Para más información sobre la comprobación de requisitos, consulte <http://www.sophos.com/es-es/support/knowledgebase/113945.aspx>.
 - d) En la página **Detalles de la base de datos**, introduzca los datos de la cuenta creada en [Cuenta de la base de datos](#) en la página 10.
 - e) En la página **Credenciales de Sophos Update Manager**, introduzca los datos de la cuenta creada en [Cuenta del gestor de actualización](#) en la página 10.
6. Puede que tenga que reiniciar el sistema después de realizar la instalación. Haga clic en **Sí** o **Finalizar**.

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.

9 Mejorar 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.

10 Instalar una consola de administración remota 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.

11 Descargar el software de seguridad

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

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

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

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

Al hacer clic en **Siguiente**, se iniciará la descarga del software.

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

Nota: para más información sobre cómo proteger equipos con Windows 8, consulte <http://www.sophos.com/es-es/support/knowledgebase/118261.aspx>.

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

12 Crear grupos de ordenadores

Si utilizó el **Asistente para descargar el 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 19.

Para proteger y administrar ordenadores, debe crear grupos.

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

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

13 Configurar políticas de seguridad

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

- Si desea utilizar Sophos Client Firewall, se recomienda preparar la política del cortafuegos antes de aplicarla.
- Deberá editar las políticas de restricción de aplicaciones, control de dispositivos, parches y control web si desea utilizar estas funciones. Puede hacerlo en cualquier momento.

13.1 Configurar una política de cortafuegos

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

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

1. En , 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 la página **Uso compartido de archivos e impresoras**, seleccione **Permitir el uso compartido de archivos e impresoras**.

14 Buscar 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 [Preparar la protección de ordenadores](#) en la página 21.

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

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

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

15 Preparar la protección de ordenadores

Antes de proteger los ordenadores, debe:

- Preparar la eliminación de software de terceros.
- Comprobar que tiene una cuenta que puede utilizar para instalar software.
- Preparar la instalación del software antivirus.

15.1 Preparar la eliminación de software de terceros

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

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

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

15.2 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 esté instalada.

- 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.

15.3 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), 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.

16 Proteger ordenadores

En esta sección se describe cómo:

- Proteger los ordenadores Windows de forma automática.
- Proteger los ordenadores Windows o Mac de forma manual.
- Proteger los ordenadores Linux (si su licencia lo incluye).

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

16.1 Proteger ordenadores Windows de forma automática

Para proteger ordenadores:

1. Seleccione los ordenadores que desea proteger.
2. Haga clic con el botón derecho y seleccione **Proteger ordenadores**.
Nota: Si los equipos se encuentran en el grupo **No asignados**, arrástrelos a los grupos que desee.
3. Un asistente le guiará durante la instalación del software de seguridad de Sophos. Haga lo siguiente:
 - a) En la página de **bienvenida**, haga clic en **Siguiente**.
 - b) En la página **Tipo de instalación**, deje activada la opción **Software de protección**. Software de «protección» es otro término para software de seguridad.
 - c) En la página **Seleccionar funciones**, puede seleccionar los productos que desee instalar.
La versión actual del cortafuegos (incluida en Endpoint Security and Control 10.2 o anteriores) no se puede instalar en equipos con Windows 8.
 - d) En la página **Resumen de protección**, podrá ver cualquier problema de instalación. Si necesita ayuda, consulte [Solución de problemas](#) en la página 26.
 - e) En la página **Credenciales**, indique la cuenta de Windows que se utilizará para instalar el software en los ordenadores.

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

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

16.2 Proteger los ordenadores Windows o Mac de forma manual

16.2.1 Localizar el programa de instalación

Si cuenta con equipos que Enterprise Console 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.

Para ubicar los programas de instalación:

1. En Enterprise Console, en el menú **Ver**, seleccione **Ubicación de archivos de inicio**.
Se mostrará una lista con las ubicaciones disponibles.
2. Anote la ubicación para cada sistema operativo que desee proteger.

16.2.2 Proteger equipos Windows de forma manual

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

1. En todos los ordenadores que desee proteger, haga doble clic en el programa de instalación `setup.exe` en la ubicación de los archivos de inicio.
2. En el **asistente de instalación**, en la página **Datos de la cuenta de usuario**, introduzca la cuenta de Update Manager, **SophosUpdateMgr**, para acceder a la fuente de actualización. La cuenta se creó en [Cuenta del gestor de actualización](#) en la página 10.

Consejo: También puede utilizar una cuenta con el acceso necesario a la ubicación de los archivos de inicio. Enterprise Console aplicará una política con la cuenta de acceso necesaria.

Nota: Para más información sobre los parámetros de `setup.exe`, consulte <https://www.sophos.com/es-es/support/knowledgebase/12570.aspx>.

16.2.3 Proteger ordenadores Mac de forma manual

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

1. En todos los ordenadores Mac que desee proteger, navegue hasta llegar a los archivos de inicio. 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.
2. Acepte los valores predeterminados. Cuando se le pida, introduzca las credenciales que permitan la instalación.

16.3 Proteger equipos Linux

Para más información sobre cómo proteger ordenadores Linux (si su licencia lo incluye), consulte la *Guía de inicio de Enterprise Console para Linux y UNIX*.

17 Comprobar el estado de la red

Para comprobar el estado de la red desde Enterprise Console:

1. En la barra de menús, haga clic en el icono del **panel de control** (si no está ya a la vista).

El panel de control indica cuántos ordenadores:

- Tienen amenazas detectadas.
- No están actualizados.
- No cumplen las políticas.

18 Solución de problemas

Al ejecutar el **Asistente para proteger ordenadores**, 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 ordenadores Mac de forma manual](#) en la página 24. Para más información sobre otros sistemas operativos (si su licencia lo incluye), consulte la *Guía de inicio de Sophos Enterprise Console para Linux y UNIX*.
- No se puede determinar el sistema operativo. Esto puede ocurrir si, al buscar ordenadores, no introduce su nombre de usuario con el formato dominio\usuario.
- Las reglas con las que se ha configurado el Firewall están bloqueando el acceso necesario para implementar el software de seguridad.

19 Ayuda para tareas habituales

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

Tarea	Documento
Proteger ordenadores independientes	Guía avanzada de inicio de Enterprise Console: <i>Proteger ordenadores independientes</i> en Guía avanzada de inicio de Enterprise Console
Configurar políticas en Enterprise Console	Ayuda de Enterprise Console: Configurar las políticas
Alertas	Ayuda de Enterprise Console: Alertas y errores
Limpiar ordenadores	Ayuda de Enterprise Console: Realizar una limpieza inmediata
Generar informes con Enterprise Console	Ayuda de Enterprise Console: Generar informes

20 Soporte técnico

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

- Visitar el fórum Sophos Community en community.sophos.com/ para consultar casos similares.
- Visitar la base de conocimiento de Sophos en www.sophos.com/es-es/support.aspx.
- Descargar la documentación correspondiente desde 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>.

21 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. Los demás productos y empresas mencionados son marcas 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 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.

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

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (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).

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

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

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

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

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

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

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

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

The 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

Mark Adler madler@alumni.caltech.edu