

SOPHOS

Security made simple.

Sophos for Virtual Environments

Guía de inicio: edición Enterprise Console



Contenido

Acerca de esta guía.....	1
Acerca de Sophos for Virtual Environments.....	2
Pasos clave para la instalación.....	5
Comprobar los requisitos del sistema.....	6
Requisitos de VMware.....	6
Requisitos de Microsoft Hyper-V.....	7
Requisitos de los equipos virtuales invitados.....	7
Requisitos de red.....	8
Requisitos de administración de Sophos.....	8
Desinstalar otros productos antivirus.....	10
Configurar el software de administración de Sophos.....	11
Instalar Enterprise Console.....	11
Crear una unidad compartida de actualización de Sophos.....	12
Comprobar el acceso a la unidad compartida de actualización de Sophos.....	12
Instalar el Sophos Security VM.....	14
Comprobar que dispone de las contraseñas necesarias.....	14
Comprobar que los sistemas están sincronizados.....	14
Comprobar los requisitos del programa de instalación.....	14
Descargar el programa de instalación de Sophos Security VM.....	15
Instalar el Sophos Security VM.....	15
Comprobar que el Sophos Security VM está instalado.....	18
Usar Enterprise Console para aplicar políticas.....	18
Instalar Sophos Guest VM Agent.....	20
Comprobar que los equipos virtuales invitados están protegidos.....	21
Comprobar la configuración de protección.....	21
Probar el escaneado en tiempo real.....	21
Solución de problemas del escaneado en acceso.....	22
Ver equipos virtuales protegidos.....	23
Mantener el Sophos Security VM.....	24
Desinstalar Sophos Security VM.....	25
Desinstalar Sophos Guest VM Agent.....	26
Migrar a Sophos for Virtual Environments.....	27
Apéndice: Añadir procesadores al Sophos Security VM.....	29
Soporte técnico.....	30
Aviso legal.....	31

1 Acerca de esta guía

En esta guía se explica cómo:

- Utilizar Sophos for Virtual Environments para proporcionar una protección centralizada contra amenazas para equipos virtuales en un entorno VMware ESXi o un entorno Microsoft Hyper-V.
- Utilizar Sophos Enterprise Console para administrar Sophos for Virtual Environments.

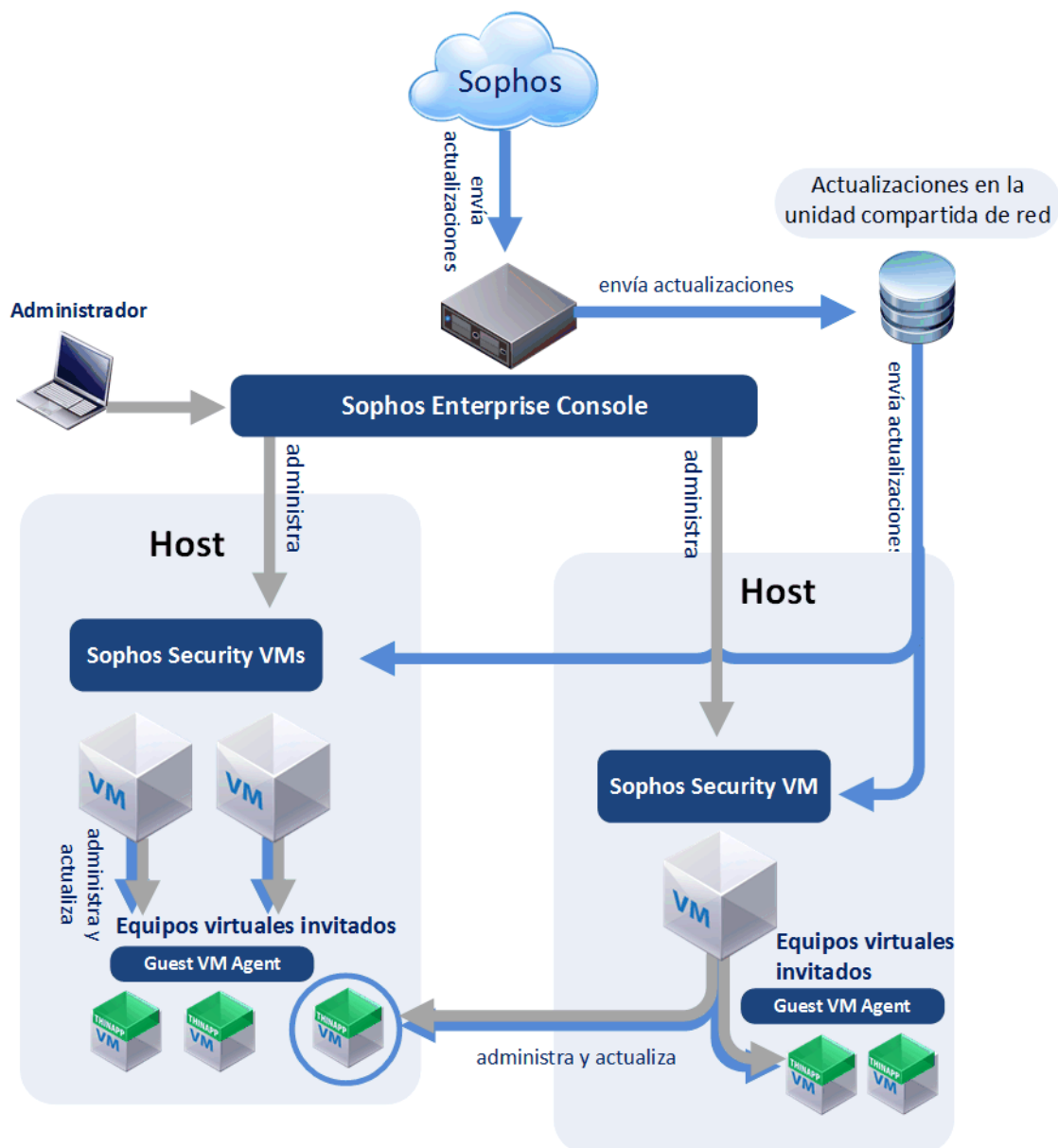
Si está migrando a Sophos for Virtual Environments, consulte [Migrar a Sophos for Virtual Environments](#) (página 27).

Si desea utilizar Sophos Central en lugar de Enterprise Console, consulte la *Guía de inicio de Sophos for Virtual Environments: edición Sophos Central*.

2 Acerca de Sophos for Virtual Environments

Sophos for Virtual Environments es un sistema de seguridad para la protección de equipos virtuales. El funcionamiento es el siguiente:

- Se realiza una o varias instalaciones de Sophos Security VM en el host de cada hipervisor. Entonces el Sophos Security VM puede detectar y bloquear amenazas en equipos virtuales invitados conectados a él.
- Se debe instalar Sophos Guest VM Agent en cada equipo virtual invitado.
- Se utiliza Sophos Enterprise Console en otro ordenador para administrar los Sophos Security VM y mantenerlos actualizados.



¿En qué entornos se puede utilizar Sophos?

Sophos for Virtual Environments puede proteger equipos virtuales en un entorno VMware ESXi o un entorno Microsoft Hyper-V.

¿Qué equipos virtuales invitados se pueden proteger?

El Sophos Security VM puede proteger equipos virtuales invitados que ejecutan sistemas operativos Windows. Para conocer las versiones compatibles, consulte [Requisitos de los equipos virtuales invitados](#) (página 7).

El Sophos Security VM puede proteger equipos virtuales invitados que se encuentran en otro host.

¿Cómo funciona el escaneado?

Cuando un equipo virtual invitado intenta acceder a un archivo:

- Sophos Guest VM Agent en ejecución en el equipo virtual notifica al Sophos Security VM.
- El Sophos Security VM escanea el archivo.
- Si el Sophos Security VM detecta alguna amenaza, se bloquea el acceso al archivo y el Sophos Security VM envía una alerta a Enterprise Console.

El Sophos Security VM también puede realizar un escaneado completo de los equipos virtuales invitados. Puede ejecutar este escaneado inmediatamente o programarlo.

El escáner de archivos utiliza el almacenamiento inteligente en caché para conservar los resultados de escaneados anteriores. Esto ayuda a mejorar el rendimiento general cuando hay demasiados equipos virtuales conectados o cuando se accede al mismo archivo repetidamente.

¿Pueden moverse los equipos virtuales invitados entre Sophos Security VM?

Puede permitir a los equipos virtuales invitados moverse entre Sophos Security VM con fines de protección.

Así los equipos virtuales invitados se mantienen protegidos si no pueden conectarse a su Sophos Security VM actual. Esto también reparte la carga de trabajo entre Sophos Security VM.

Los equipos virtuales invitados clonados desde una única plantilla también pueden migrar entre Sophos Security VM. Al crear la plantilla, se pueden enumerar todos los Sophos Security VM disponibles, de modo que los clones puedan conectarse a cualquiera de ellos. Consulte el [artículo 127955 de la base de conocimiento](#).

Puede configurar la migración de equipos virtuales invitados durante la instalación.

¿Cómo se administra el Sophos Security VM?

Enterprise Console muestra el estado del Sophos Security VM, incluido si está actualizado y si ha detectado alguna amenaza.

Enterprise Console permite configurar el escaneado mediante políticas.

¿Qué hacer ante una amenaza?

El Sophos Security VM ofrece la posibilidad de limpiar las amenazas automáticamente. Consulte la *Guía de configuración de Sophos for Virtual Environments: edición Enterprise Console*.

¿Cómo se actualiza el Sophos Security VM?

Enterprise Console mantiene el Sophos Security VM actualizado.

Enterprise Console descarga los datos de las amenazas más recientes, las actualizaciones de mantenimiento y las nuevas versiones del producto desde Sophos y los copia en una unidad compartida de red. El Sophos Security VM obtiene e instala las actualizaciones automáticamente.

La fecha en que se obtiene una actualización de mantenimiento puede depender de si se suscribe o no a las versiones [Recommended](#) o [Preview](#).

¿Cómo se actualiza Sophos Guest VM Agent?

Sophos Guest VM Agent se actualiza automáticamente.

El agente no escanea archivos, de modo que no necesita identidades de amenazas actualizadas. Sin embargo, sí que recibe actualizaciones cuando mejoramos el producto.

El Sophos Security VM obtiene estas actualizaciones de producto y las aplica a los equipos virtuales invitados.

Las actualizaciones se distribuyen de forma escalonada para minimizar la carga en el Sophos Security VM y el host del hipervisor subyacente.

3 Pasos clave para la instalación

Los pasos de instalación que se describen en las siguientes secciones son:

- Comprobar los requisitos del sistema.
- Desinstalar otros productos antivirus.
- Configurar el software de administración de Sophos (Enterprise Console).
- Instalar el Sophos Security VM y aplicar políticas.
- Instalar Sophos Guest VM Agent en los equipos virtuales invitados.
- Comprobar que los equipos virtuales invitados están protegidos.

4 Comprobar los requisitos del sistema

En esta sección se describen los requisitos del sistema necesarios y cómo comprobar que los cumple.

También se explica toda la información (como los datos de los ordenadores) que debe reunir ahora para tenerla a mano cuando vaya a instalar los Sophos Security VM.

Se cubren los requisitos tanto para entornos VMware ESXi como para entornos Microsoft Hyper-V.

4.1 Requisitos de VMware

En esta sección se indica el software que necesita en un entorno VMware.

4.1.1 Host VMware ESXi

Instale los siguientes componentes en todos los hosts que vayan a ejecutar un Sophos Security VM:

- Host VMware ESXi 5.5, 6.0 o 6.5.

Nota

Se recomienda que [configure el host de modo que reciba actualizaciones de VMware](#).

Requisitos de hardware

El host VMware ESXi debe ser capaz de asignar los recursos siguientes para cada Sophos Security VM:

- 2 procesadores.
- 20 Gb de espacio en disco.
- 4 Gb de RAM.

Notas

No se debe imponer ningún límite de recursos de los procesadores en el Sophos Security VM.

Se asignan 2 procesadores de forma predeterminada. Si necesita proteger una gran cantidad de equipos virtuales invitados, puede configurar más procesadores después de instalar el Sophos Security VM. En esta guía se explica cómo hacerlo.

El Sophos Security VM reserva memoria. Los sistemas de alta disponibilidad y equilibrio de cargas eligen de forma automática según las reservas de recursos para los equipos virtuales del entorno VMware. No elimine la reserva de memoria del Sophos Security VM.

4.1.2 VMware vCenter y vSphere

Es necesario el software de vCenter y vSphere siguiente.

Software	Versión	Notas
vCenter	Versión 5.5, 6.0, 6.5	También necesitará: La dirección de red. Una cuenta de administrador.
vSphere Client	Versión 5.5, 6.0, 6.5	

4.1.3 Herramientas de VMware

Recomendamos utilizar herramientas de VMware en los equipos virtuales invitados ya que pueden mejorar el rendimiento.

4.2 Requisitos de Microsoft Hyper-V

En esta sección se indica el software que necesita en un entorno Microsoft Hyper-V.

El sistema Microsoft Hyper-V debe ser uno de los siguientes:

- Hyper-V en Windows Server 2012 (Core, completo)
- Hyper-V en Windows Server 2012 R2 (Core, completo)
- Hyper-V en Windows Server 2016 (Core, Server con Experiencia de escritorio)

Componentes de integración de Microsoft Hyper-V

Los componentes de integración de Microsoft Hyper-V se instalarán automáticamente si la actualización de Windows está activada y funciona correctamente. Sin estas herramientas, el rendimiento de su equipo virtual podría verse reducido.

Directrices sobre antivirus para Microsoft Hyper-V

Microsoft publica directrices sobre cómo proteger su servidor Hyper-V de la forma más efectiva. Consulte [Microsoft KBA 3105657](#).

4.3 Requisitos de los equipos virtuales invitados

Los equipos virtuales invitados deben utilizar uno de los sistemas operativos indicados aquí.

Sistema operativo	Service Packs	Comentarios
Windows 10 (32 y 64 bits). El artículo de la base de conocimiento 125679 incluye una lista con todas las versiones compatibles.		Los contenedores de Windows y Hyper-V no son compatibles.
Windows 8.1 (32 y 64 bits)	---	
Windows 7 (32 y 64 bits).	SP1+	

Sistema operativo	Service Packs	Comentarios
Windows Server 2016 (64 bits). El artículo de la base de conocimiento 125679 incluye una lista con todas las versiones compatibles.		Los contenedores de Windows y Hyper-V no son compatibles.
Windows Server 2012 R2 (64 bits)	---	
Windows Server 2012 (64 bits)	---	
Windows Server 2008 R2 (64 bits)	---	

4.4 Requisitos de red

Los requisitos de infraestructura son los siguientes:

- El Sophos Security VM y los equipos virtuales invitados deben compartir una conexión de red. Lo ideal es que sea una red de área local (LAN) de alta velocidad sin limitación de tráfico de red.
- El tráfico de red entre el Sophos Security VM y los equipos virtuales invitados no debe estar bloqueado por firewalls ni controladores de acceso a la red.

4.4.1 Requisitos de redes NAT

Si tiene un equipo virtual invitado dentro de una red NAT (traducción de direcciones de red), puede protegerlo con un Sophos Security VM dentro o fuera de esa red.

Durante la instalación, debe configurar el Sophos Security VM con lo siguiente:

- Una dirección IP principal fuera de la red NAT (esta dirección debe poder comunicarse con la consola de administración)
- Una dirección IP secundaria dentro de la red NAT.

4.4.2 Subredes

Puede configurar el Sophos Security VM con hasta cinco direcciones IP. Cada dirección IP debe encontrarse en una subred diferente.

4.5 Requisitos de administración de Sophos

Necesitará el siguiente software de Sophos para poder instalar y utilizar el Sophos Security VM. Si no tiene este software, siga las instrucciones de la sección [Configurar el software de administración de Sophos](#) (página 11).

Software	Versión	Notas
Sophos Enterprise Console	Versión 5.4 o posterior.	Recomendamos la versión 5.5.

Software	Versión	Notas
Unidad compartida de red para Sophos for Virtual Environments	Sin versión mínima.	Es necesario configurar una unidad compartida de red en la que Enterprise Console pueda poner las actualizaciones más recientes a disposición del Sophos Security VM. En esta guía se explica cómo hacerlo.

5 Desinstalar otros productos antivirus

Debe desinstalar todos los productos antivirus, incluidos los productos de Sophos, que ya estén instalados en sus equipos virtuales invitados.

Debe deshabilitar Windows Defender en las plataformas de servidor donde no esté presente el centro de seguridad. Se recomienda que lo haga mediante una política de grupo.

No puede utilizar Sophos for Virtual Environments para proteger equipos virtuales invitados que ejecutan otros productos antivirus. Si intenta hacerlo, es posible que el rendimiento se vea afectado o que se produzca un interbloqueo del sistema en que el equipo virtual invitado deja de responder.

Esta limitación también es aplicable a equipos virtuales con productos de servidor o puerta de enlace de Sophos que incluyan o requieran componentes antivirus.

Para más información, vea el [artículo 125679 en la base de conocimiento](#).

6 Configurar el software de administración de Sophos

Antes de instalar los Sophos Security VM, debe:

- Instalar Sophos Enterprise Console (si no dispone ya de una instalación). Se utiliza para descargar actualizaciones del software de protección y administrar los equipos virtuales que protege.
- Crear una unidad compartida de red para Sophos for Virtual Environments. Esta unidad compartida se utiliza para mantener actualizados los Sophos Security VM.

En las secciones siguientes se describe cómo hacerlo.

Si ya utiliza Enterprise Console

Aviso

Si ya utiliza Enterprise Console para administrar otros productos de Sophos y desea añadir Sophos for Virtual Environments, es posible que sus credenciales de cliente no le permitan configurar la unidad compartida de red de Sophos. Si esto ocurre, compruebe que su licencia incluye este producto. Puede enviar las consultas relativas a las licencias a customercare@sophos.com

6.1 Instalar Enterprise Console

Si ya tiene Enterprise Console instalado, vaya a [Crear una unidad compartida de actualización de Sophos](#) (página 12).

Debe instalar Enterprise Console en un equipo Windows que se encuentre en la misma red que el Sophos Security VM

Siga las instrucciones que aparecen en la [Guía rápida de inicio de Enterprise Console](#). Cuando tenga que seleccionar las plataformas que desea proteger, incluya **Sophos for Virtual Environments**. Se creará la unidad compartida de red de Sophos for Virtual Environments.

Atención

Esto proporciona la versión recomendada (Recommended). Si desea la versión de avance (Preview), que le da acceso a funciones nuevas, [Crear una unidad compartida de actualización de Sophos](#) (página 12).

Nota

Tanto si tiene la versión Recommended como la versión Preview, debe utilizar la misma versión al instalar los Sophos Security VM con posterioridad.

Después de la instalación, consulte [Comprobar el acceso a la unidad compartida de actualización de Sophos](#) (página 12).

6.2 Crear una unidad compartida de actualización de Sophos

Si acaba de realizar una nueva instalación de Enterprise Console y se ha suscrito a Sophos for Virtual Environments, puede saltarse esta sección.

1. En Enterprise Console, en el menú **Ver**, seleccione **Gestores de actualización**.
2. Cree una "suscripción" a Sophos for Virtual Environments:
 - a) En la vista **Gestores de actualización**, haga clic en **Añadir** en la parte superior del panel de suscripciones.
 - b) En el cuadro de diálogo **Suscripción de software**, indique un nombre en el cuadro **Suscripción**.
 - c) En la lista de plataformas, seleccione **Sophos for Virtual Environments**.

Nota

Si no ve esta opción en la lista, significa que necesita actualizar las credenciales de cliente. Póngase en contacto con el soporte técnico de Sophos.

- d) En el cuadro de versión, seleccione **Recommended** o **Preview**.

Nota

Preview proporciona acceso anticipado a funciones nuevas. Lea más información acerca de [Recommended y Preview](#).

Nota

Debe utilizar la misma versión al instalar los Sophos Security VM con posterioridad.

3. Configure el gestor de actualización para que utilice esta suscripción:
 - 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 la suscripción nueva aparece en la lista **Suscrito**.
 - c) Haga clic en **Aceptar**.

Continúe en la siguiente sección.

6.3 Comprobar el acceso a la unidad compartida de actualización de Sophos

Debe localizar la unidad compartida de actualización de Sophos y asegurarse de que se pueda acceder a ella utilizando credenciales válidas o una cuenta de invitado.

Nota

A menos que se haya especificado de otro modo, a la unidad compartida de actualización de Sophos se accede con la cuenta de usuario establecida durante la instalación de Enterprise Console, donde aparece como la cuenta de "Update Manager", y que suele utilizarse con el nombre de usuario SophosUpdateMgr.

1. En Enterprise Console, en el menú **Ver**, seleccione **Ubicación de archivos de inicio**. Se mostrará una lista con las ubicaciones disponibles.
2. Busque la ubicación de Sophos for Virtual Environments y anótela. Necesitará esta información cuando instale los Sophos Security VM.
Necesitará el nombre completo de dominio de esta ubicación.
3. Si la unidad compartida está en Windows Server 2008 o 2012, puede que necesite cambiar la configuración del Firewall de Windows de forma temporal en el servidor para permitir el acceso del programa de instalación de Sophos Security VM.
Las siguientes reglas de entrada deben estar activadas (opción predeterminada):
 - Uso compartido de archivos e impresoras (NB-Datagram-In)
 - Uso compartido de archivos e impresoras (NB-Name-In)
 - Uso compartido de archivos e impresoras (NB-Session-In)
 Puede volver a desactivarlas después de instalar los Sophos Security VM.

Notas:

Si dispone de un instalación personalizada de Enterprise Console o si ha creado alguna otra unidad compartida de red para actualizar el Sophos Security VM, tenga en cuenta que:

- Si se requieren credenciales, deben almacenarse en los Sophos Security VM tras la instalación, por lo que se recomienda que utilice credenciales de solo lectura.
- Si la unidad compartida de red está en un ordenador distinto de Enterprise Console (o el gestor de actualización de Enterprise Console), asegúrese de que también se pueda acceder a ella usando una cuenta con acceso de escritura.

7 Instalar el Sophos Security VM

Puede instalar uno o más Sophos Security VM en cada host en el que desee proteger equipos virtuales invitados.

Los pasos necesarios para la instalación, que se describen en las secciones siguientes, son:

- Comprobar que dispone de las contraseñas necesarias.
- Comprobar que los sistemas están sincronizados.
- Comprobar los requisitos del programa de instalación.
- Descargar el programa de instalación.
- Instalar el Sophos Security VM.
- Comprobar que el Sophos Security VM esté instalado.
- Usar Enterprise Console para aplicar políticas al Sophos Security VM.

7.1 Comprobar que dispone de las contraseñas necesarias

Al ejecutar el programa de instalación de Sophos Security VM, es necesario introducir ciertas contraseñas. Asegúrese de que dispone de las contraseñas para las siguientes cuentas:

- La cuenta utilizada para acceder a la unidad compartida de red de Sophos for Virtual Environments (o "carpeta de actualización de Sophos").
- Si se encuentra en un entorno MVware, la cuenta de administrador de vCenter.

7.2 Comprobar que los sistemas están sincronizados

Asegúrese de que la hora esté sincronizada en el servidor de Enterprise Console, en el host en el que instala el Sophos Security VM y en los equipos virtuales invitados.

Puede utilizar la sincronización NTP (protocolo de tiempo de redes) para cada host.

Aviso

Si la hora no está sincronizada, podrá instalar el Sophos Security VM pero no podrá administrarlo desde Enterprise Console.

7.3 Comprobar los requisitos del programa de instalación

Compruebe que el ordenador y la cuenta de usuario que va a utilizar cumplan los requisitos.

- El programa de instalación debe encontrarse en un ordenador Windows que tenga acceso a su servidor VMware vCenter o Microsoft Hyper-V a través de la red.
- La instalación del Sophos Security VM debe realizarse en la red local. Actualmente el programa de instalación no admite el uso de un proxy.
- El programa de instalación no puede utilizarse en un ordenador con Windows XP o Windows Server 2003.
- Si utiliza Microsoft Hyper-V, debe ejecutar el programa de instalación como usuario con derechos para crear y controlar equipos virtuales en el servidor Hyper-V. Esto puede ser una cuenta de usuario local en el servidor Hyper-V o un usuario de dominio.

El ordenador donde se guarda el programa de instalación se utiliza solo para la instalación. No se usa para la administración ni la protección de su Sophos Security VM ni de equipos virtuales invitados tras la instalación.

7.4 Descargar el programa de instalación de Sophos Security VM.

Descargue el programa de instalación de Sophos Security VM desde el sitio web de Sophos (si todavía no lo ha hecho).

Se asume que dispone de una cuenta de MySophos y que tiene su licencia asociada a dicha cuenta. Si necesita ayuda, consulte www.sophos.com/es-es/support/knowledgebase/111195.aspx.

Notas:

- Puede descargar el programa de instalación de Sophos Security VM desde cualquier ordenador y después copiarlo al ordenador donde desea utilizarlo.
- Las instrucciones de instalación de las secciones siguientes le indicarán en qué ordenador u ordenadores debe utilizar el programa de instalación.

Para descargar el programa de instalación:

1. Vaya a www.sophos.com/es-es/support/downloads/.
2. Introduzca su nombre de usuario y la contraseña de MySophos.
3. Si ve una página web que muestra sus licencias, seleccione una.
4. En **Programas de instalación independientes**, haga clic en **Sophos for Virtual Environments**.
5. En la página web **Sophos for Virtual Environments**, busque el programa de instalación del hipervisor que esté utilizando (Hyper-V o ESXi).
6. Decida si desea la versión **Recommended** o **Preview**.
7. Descargue el programa de instalación.

Después de instalar el Sophos Security VM, podrá obtener Sophos Guest VM Agent desde una unidad compartida pública del Sophos Security VM.

7.5 Instalar el Sophos Security VM

Antes de empezar, asegúrese de realizar lo siguiente:

- [Descargar el programa de instalación de Sophos Security VM](#). (página 15)
- [Comprobar los requisitos del programa de instalación](#) (página 14)

Algunos pasos de la instalación son aplicables solo a VMware ESXi o solo a Microsoft Hyper-V. Esto se indica al principio del paso.

1. Hacer doble clic en el programa de instalación para ejecutarlo.
2. Aceptar el acuerdo de licencia.
3. En la página de bienvenida, haga clic en **Next** para extraer los archivos de instalación a una carpeta en el equipo.
4. Compruebe los requisitos previos para la instalación en **Prerequisites for installation**.
5. Este paso solo es para VMware ESXi:
En **VMware vCenter credentials**, introduzca los detalles y un nombre para el Sophos Security VM.

Nota

Introduzca el nombre de usuario del administrador en el formato utilizado al iniciar sesión en vCenter con vSphere Client (con o sin el prefijo del dominio, según proceda, y con las mismas mayúsculas y minúsculas).

6. En **ESXi host** o **Hyper-V host name**, especifique el host en el que desea instalar el Sophos Security VM.
7. En **Management console**, seleccione **Use Sophos Enterprise Console**.
8. En **Sophos update folder details**, introduzca los detalles de la unidad compartida de red de Sophos for Virtual Environments que creó anteriormente.
 - a) Introduzca la ubicación. Utilice una ruta UNC incluyendo el nombre completo del dominio o una dirección web (si la unidad compartida está en un servidor web).
Por ejemplo:
`\\<nombre del servidor.nombre del dominio>\sophosupdate\CIDs\Sxxx\SVE`
Sugerencia: Para comprobar la ubicación, vaya a Enterprise Console. En el menú **Ver**, haga clic en **Ubicación de archivos de inicio** y busque la unidad compartida de Sophos for Virtual Environments.
 - b) Complete el nombre de usuario y la contraseña. Esta cuenta se configura durante la instalación de Enterprise Console, donde aparece como la cuenta de "Update Manager", y suele utilizarse con el nombre de usuario SophosUpdateMgr.
Tenga en cuenta que:
 - Si es una cuenta de dominio, debe incluir el nombre del dominio.
 - Las credenciales se almacenan de forma segura en el Sophos Security VM.
9. Cree una contraseña de acceso en Password for access to your Sophos Security VM.
Esta contraseña es necesaria para ver los equipos virtuales invitados protegidos. También la necesita para recopilar registros para la resolución de problemas.
10. Cree una contraseña de acceso en **Password for access to Guest VM Agent installer** para el programa de instalación del agente de equipo virtual de Sophos.
Necesitará esta contraseña más adelante para instalar el software del agente en los equipos virtuales invitados.
11. En **Timezone**, seleccione la zona horaria que utilizará el Sophos Security VM para programar los escaneados.
12. Este paso solo es para VMware ESXi:
En **Datastore for the Security VM**, seleccione el tipo de almacén de datos en el que desea instalar el Sophos Security VM.

Nota

El Sophos Security VM protege los equipos virtuales invitados incluso si sus plantillas se guardan en distintos almacenes de datos.

13. En **IP settings for the Sophos Security VM**, introduzca la configuración de IP para todas las redes en las que desea proteger equipos virtuales invitados. Un Sophos Security VM puede proteger los equipos virtuales de varias redes.
 - a) En **Select virtual LAN (ESXi)** o **Select vSwitch (Hyper-V)**, seleccione de entre las opciones disponibles.
 - b) Introduzca la dirección IPv4 estática en **Static IPv4 address**. Solo puede utilizar direcciones estáticas.
 - c) Introduzca una máscara de subred en **Subnet mask**.
 - d) Introduzca el sufijo del dominio en **Domain suffix**.
 - e) Seleccione **Make Primary** si esta es la red que debe tener acceso a la consola de administración de Sophos. Solo puede tener una red principal.
Puede utilizar el botón "+" que aparece sobre los campos para añadir otra red. El botón "-" sirve para eliminar una red. Los botones "<" y ">" le permiten desplazarse por las opciones de configuración de las distintas redes.
14. En **Gateway and DNS server details for the primary network card**, introduzca los datos que permitirán al Sophos Security VM comunicarse con la consola de administración y descargar las actualizaciones.

Nota

Puede introducir un servidor DNS o, si lo desea, dos.

15. En **Guest VM migration**, puede permitir a los equipos virtuales invitados moverse entre Sophos Security VM.
Si no activa la migración, salte al paso 18.
16. En **Guest VM migration: Security VM certificate**, especifique los datos de un paquete de certificados.
Para obtener ayuda con la creación de certificados, consulte el [artículo 127562 de la base de conocimiento](#).
17. En **Guest VM migration: Available Security VMs**, especifique las direcciones IPv4 de los Sophos Security VM disponibles para proteger los equipos virtuales invitados.
Se recomienda utilizar Sophos Security VM con las mismas políticas de seguridad para garantizar uniformidad en la limpieza y generación de informes.
Para obtener más información sobre la migración de equipos virtuales invitados clonados desde una plantilla, consulte el [artículo 127955 de la base de conocimiento](#).
18. Este paso solo es para Hyper-V:
En **Disk image location**, especifique una ubicación para la imagen de disco del Sophos Security VM. Puede ser una unidad compartida de red o una carpeta local en el host.
19. En la página **Summary of installation**, haga clic en **Install**.
20. En la página **Finished**, verá si la instalación de los Sophos Security VM se ha realizado correctamente. Si se ha producido algún error, consulte el registro para más información.
Sugerencia: Puede hacer clic en **Start Over** para ejecutar otra instalación o intentarlo de nuevo.
En Hyper-V, esta opción solo se muestra si se ha producido un error con la instalación.

Siga las instrucciones de las dos secciones siguientes para:

- Comprobar que puede ver el Sophos Security VM en Enterprise Console.
- Usar Enterprise Console para aplicar políticas al Sophos Security VM.

A continuación, debe [Instalar Sophos Guest VM Agent](#) (página 20).

Aviso

No "suspenda" el Sophos Security VM. Si lo hace, más tarde no se podrán reanudar las comunicaciones con el software de administración.

7.6 Comprobar que el Sophos Security VM está instalado

En esta sección se explica cómo comprobar si el Sophos Security VM está instalado y si dispone de los recursos que necesita.

Comprobar que puede ver el Sophos Security VM

Cuando se haya instalado el Sophos Security VM, vaya a Enterprise Console.

Debería ver que el Sophos Security VM está registrado e incluido en el grupo de ordenadores **No asignados**.

Si cambia el nombre de un Sophos Security VM después de la instalación, seguirá apareciendo en Enterprise Console con el mismo nombre asignado durante la instalación.

Comprobar si necesita configurar recursos

Normalmente, no es necesario configurar recursos para el Sophos Security VM. Tenga en cuenta que:

- Si el Sophos Security VM protege un gran número de equipos virtuales invitados, debe asegurarse de que tenga suficiente capacidad de procesamiento para el escaneado. Consulte [Apéndice: Añadir procesadores al Sophos Security VM](#) (página 29).
- El programa de instalación reserva memoria para el Sophos Security VM. En un entorno VMware, los sistemas de alta disponibilidad y equilibrio de cargas eligen de forma automática según las reservas de recursos para los equipos virtuales y podrían hacer elecciones diferentes una vez instalado el Sophos Security VM. No elimine la reserva de memoria del Sophos Security VM.

Ya está listo para utilizar Enterprise Console para aplicar políticas al Sophos Security VM.

7.7 Usar Enterprise Console para aplicar políticas

1. En Sophos Enterprise Console, cree una política de actualización y una políticas antivirus y HIPS. Haga clic con el botón derecho en cada política y seleccione **Restaurar la política predeterminada**.
2. Haga doble clic en la política de actualización nueva para abrirla.
3. En el cuadro de diálogo **Política de actualización**:
 - a) Haga clic en la ficha **Suscripción** y seleccione la suscripción para Sophos for Virtual Environments.

- b) Haga clic en la ficha **Servidor primario** y asegúrese de que la ubicación de la carpeta de actualización incluye el nombre de dominio completo. Guarde la política.
4. Cree un nuevo grupo de ordenadores para incluir el Sophos Security VM.
5. Aplique las nuevas políticas al nuevo grupo.
6. Arrastre el Sophos Security VM del grupo **No asignados** al nuevo grupo.

Ahora puede proceder a [Instalar Sophos Guest VM Agent](#) (página 20) en los equipos virtuales invitados.

Para obtener consejos generales sobre las tareas de mantenimiento y posteriores a la instalación, consulte [Mantener el Sophos Security VM](#) (página 24).

8 Instalar Sophos Guest VM Agent

Sophos Guest VM Agent debe ejecutarse en todos los equipos virtuales invitados que desee proteger.

Compruebe en qué sistemas operativos puede instalar Sophos Guest VM Agent. Consulte [Requisitos de los equipos virtuales invitados](#) (página 7).

1. En el equipo virtual invitado, desplácese hasta el host en que esté instalado el Sophos Security VM. Debe utilizar la dirección IP.
2. En la unidad compartida **Pública**, busque el programa de instalación **SVE-Guest-Installer.exe**
3. Haga doble clic en el programa de instalación para ejecutarlo o transfíralo al equipo virtual invitado y ejecútelo. Siga las instrucciones en pantalla. Alternativamente puede:
 - Usar la línea de comandos. Puede optar por instalarlo con (IU limitada) o sin (sin IU) una barra de progreso para indicar el estado de la instalación. En los comandos se distingue entre mayúsculas y minúsculas. Introduzca la opción que corresponda:

IU limitada: `SVE-Guest-Installer.exe SVMIPAddress=<IP Address of SVM> /install /passive`

Sin IU: `SVE-Guest-Installer.exe SVMIPAddress=<IP Address of SVM> /install /quiet`
 - Utilice la implementación de política de grupo. Para más información, consulte este artículo de Microsoft: <http://support.microsoft.com/kb/816102>

Recomendamos que haga una instantánea del equipo virtual invitado antes de instalar el agente. Esto le permitirá revertir el equipo virtual invitado de forma segura posteriormente en caso de que sea necesario.

9 Comprobar que los equipos virtuales invitados están protegidos

En esta sección se explica cómo puede comprobar si sus equipos virtuales invitados están protegidos. Puede:

- Comprobar la configuración de protección en un equipo virtual invitado.
- Probar el escaneado en tiempo real en un equipo virtual invitado.
- Solucionar problemas del escaneado en tiempo real.

9.1 Comprobar la configuración de protección

Para comprobar si un equipo virtual invitado está protegido:

1. Vaya al equipo virtual invitado y busque **Seguridad y mantenimiento** desde el menú Inicio. Si no encuentra esta opción, busque **Centro de actividades**.

Atención

Si no encuentra ninguna de estas dos opciones, significa que el equipo virtual invitado no ofrece el Centro de seguridad de Windows. Debe comprobar si el equipo virtual invitado está protegido siguiendo los pasos que se indican en [Probar el escaneado en tiempo real](#) (página 21).

2. Haga clic en la flecha desplegable junto a **Seguridad**. Debería ver que Sophos for Virtual Environments está habilitado.

Nota

Si no lo está, consulte .

9.2 Probar el escaneado en tiempo real

El escaneado en tiempo real es el principal método de protección contra amenazas. Al abrir, escribir, mover o cambiar de nombre un archivo, el Sophos Security VM escanea el archivo y concede acceso al mismo solo si no supone una amenaza. Al ejecutar un programa, el Sophos Security VM escanea el archivo ejecutable y cualquier otro archivo que cargue.

Importante

Asegúrese de que Sophos Endpoint para Windows *no* esté instalado en ninguno de los equipos virtuales invitados que están protegidos con un Sophos Security VM.

Para comprobar que el equipo virtual de seguridad realiza el escaneado en acceso de archivos:

1. Visite eicar.org/86-0-Intended-use.html. Copie el texto de prueba EICAR en un archivo nuevo. Asigne un nombre al archivo con la extensión .com y guárdelo en uno de los equipos virtuales invitados.
2. Pruebe a acceder al archivo desde el equipo virtual invitado.
3. Iniciar sesión en Sophos Central.
 - Si tiene la limpieza automática activada, vaya a la página **Servidores** y haga clic en el Sophos Security VM para abrir la página de detalles. En su ficha **Eventos**, debe ver que se ha detectado y limpiado EICAR.
 - Si no tiene activada la limpieza automática, busque en la página **Alertas**. Debería ver una alerta en el Sophos Security VM. Se ha detectado EICAR, pero no se ha limpiado.

Si no se ha detectado EICAR, consulte . Si no se limpia EICAR, simplemente elimínelo.

9.3 Solución de problemas del escaneado en acceso

Si el escaneado en acceso no funciona:

1. Asegúrese de que el Sophos Security VM esté en un grupo cuya política antivirus especifique que el escaneado en acceso debe estar activado:
 - a) En Enterprise Console, en el panel **Grupos**, haga clic con el botón derecho en el grupo que contiene el Sophos Security VM y seleccione **Ver/editar políticas del grupo**. Compruebe qué política antivirus y HIPS usan.
 - b) En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
 - c) Haga doble clic en la política que usa el grupo que contiene el Sophos Security VM.
 - d) En el panel **Escaneado en acceso**, asegúrese de que la opción **Activar el escaneado en acceso** se encuentra activada. Haga clic en **Aceptar**.
 - e) En la lista de ordenadores, haga clic con el botón derecho en el Sophos Security VM y seleccione **Cumplir con**. Seleccione **Política antivirus y HIPS del grupo**.
 - f) Compruebe que el Sophos Security VM cumpla con la política.
2. Asegúrese de que el equipo virtual invitado esté protegido. Vaya al host del Sophos Security VM y consulte el archivo de registro. Consulte [Ver equipos virtuales protegidos](#) (página 23).
3. Asegúrese de que el Centro de seguridad de Windows muestre el equipo virtual invitado como protegido por Sophos for Virtual Environments.
4. Compruebe que no haya reinicios pendientes solicitados por las actualizaciones de Microsoft, ya que pueden impedir que se complete la instalación de Sophos Guest VM Agent.
5. Compruebe que no haya otros productos antivirus instalados. En las plataformas de servidor en que no está presente el centro de seguridad, compruebe que Windows Defender no esté activo. Recuerde que no puede utilizar Sophos for Virtual Environments para proteger equipos virtuales invitados que ejecutan otros productos antivirus.
6. Si el problema persiste, póngase en contacto con soporte técnico de Sophos.

10 Ver equipos virtuales protegidos

Puede ver todos los equipos virtuales invitados que están protegidos por un Sophos Security VM.

1. Desplácese hasta el Sophos Security VM. Debe utilizar el Explorador de Windows y la dirección IP.
2. Haga doble clic en la unidad compartida **Registros**.
3. Cuando se le solicite, introduzca sus credenciales:
 - El nombre de usuario es "sophos".
 - La contraseña es la contraseña de acceso que estableció cuando instaló el Sophos Security VM.
4. Abra ProtectedGVMs.log para ver los equipos virtuales invitados protegidos.

Nota: El archivo ProtectedGVMs.log solo aparece cuando el Sophos Security VM empieza a proteger los equipos virtuales invitados.

11 Mantener el Sophos Security VM

Esta sección ofrece consejos sobre las tareas de mantenimiento y posteriores a la instalación.

- Debe encender el Sophos Security VM de forma manual cada vez que retire el host del modo de mantenimiento o espera. Enciéndalo antes que los equipos virtuales invitados para que estén protegidos de forma inmediata.
- No "suspenda" el equipo virtual de seguridad. Si lo hace, más tarde no se podrán reanudar las comunicaciones con el software de administración.
- Verifique que el Sophos Security VM esté recibiendo actualizaciones de seguridad de Sophos. Para hacerlo, revise su estado de actualización en Enterprise Console.
- Copias de seguridad. Recomendamos que el Sophos Security VM se excluya de las tareas periódicas de copia de seguridad, ya que esto puede afectar al rendimiento. Si necesita recuperarse el Sophos Security VM debido a fallos en la infraestructura, le recomendamos que vuelva a desplegar el Sophos Security VM.

12 Desinstalar Sophos Security VM

Para desinstalar un Sophos Security VM, debe eliminarlo.

Antes de comenzar, asegúrese de que los equipos virtuales invitados vayan a seguir protegidos. Vaya al Sophos Security VM y siga los pasos de [Ver equipos virtuales protegidos](#) (página 23). A continuación, mueva los equipos virtuales invitados a otro Sophos Security VM con una configuración de políticas similar.

Para mover los equipos virtuales invitados:

1. Desinstale Sophos Guest VM Agent. Consulte [Desinstalar Sophos Guest VM Agent](#) (página 26).
2. Vuelva a instalar Sophos Guest VM Agent con la dirección IP del nuevo Sophos Security VM. Consulte [Instalar Sophos Guest VM Agent](#) (página 20).

Una vez que haya movido los equipos virtuales invitados, puede eliminar el Sophos Security VM. Para ello:

1. Vaya a su hipervisor.
2. Apague el Sophos Security VM.
3. Elimine el equipo virtual.

13 Desinstalar Sophos Guest VM Agent

Puede desinstalar Sophos Guest VM Agent desde el Panel de control.

1. En el equipo virtual invitado, abra el **Panel de control**.
2. Haga clic en **Programas y características**.
3. Seleccione estas funciones y haga clic en **Desinstalar**:
 - Sophos for Virtual Environments
 - Sophos Guest VM Scanning Service
 - Sophos Virus Removal Tool

14 Migrar a Sophos for Virtual Environments

¿Desde qué productos puedo realizar la migración?

Puede migrar a Sophos for Virtual Environments desde estos productos.

- Sophos Anti-Virus para vShield en un entorno VMWare ESXi
- Sophos Anti-Virus ejecutado localmente en cada equipo virtual invitado en un entorno VMware ESXi o un entorno Microsoft Hyper-V
- Sophos for Virtual Environments en un entorno VMware ESXi o Microsoft Hyper-V gestionado por Sophos Enterprise Console
- Productos antivirus de otros proveedores en un entorno VMware ESXi o un entorno Microsoft Hyper-V

Nota

Sophos for Virtual Environments protege equipos virtuales invitados en un host VMware ESXi incluso cuando se ejecuta en un entorno NSX. Sin embargo, Sophos for Virtual Environments no se integra con NSX Manager. No debe instalar ningún software antivirus para ejecutarse en NSX, ya que esto afectaría al rendimiento y provocaría interbloqueos.

Nota

Sophos for Virtual Environments utiliza un Sophos Security VM para ofrecer un escaneo de amenazas centralizado. Cuando lo haya instalado, los equipos virtuales invitados ya no necesitarán actualizaciones de datos de amenazas.

¿Cómo realizo la migración?

Siga los pasos que incluimos a continuación. Encontrará más información sobre cada paso en esta guía.

Nota

Si está migrando desde un software antivirus de terceros, tenga en cuenta lo siguiente:

- Sophos for Virtual Environments requiere conectividad de red entre el Sophos Security VM y los equipos virtuales invitados.
- Sophos for Virtual Environments admite tecnologías de equilibrio de cargas de equipos virtuales dinámico como vMotion y Live Migration, pero el rendimiento es mejor si se mantiene la conectividad de red de alta velocidad entre el Sophos Security VM y los equipos virtuales invitados.

Para migrar:

1. Instale un Sophos Security VM.

Nota

Este nuevo Sophos Security VM puede estar en el mismo host que un Sophos Security VM existente que ejecute SAV para vShield.

2. Vaya a la consola de administración y verifique que el Sophos Security VM se esté actualizando correctamente.
3. Apague el Sophos Security VM anterior o desinstale el software antivirus anterior.

Atención

Sus equipos virtuales invitados quedarán desprotegidos; asegúrese de garantizar su seguridad.

4. Instale el nuevo agente ligero Sophos Guest VM Agent.
5. Verifique, como se describe en esta guía, que todos los equipos virtuales invitados estén ahora protegidos.

15 Apéndice: Añadir procesadores al Sophos Security VM

Si tiene una muchos equipos virtuales invitados en un host, asegúrese de que el Sophos Security VM dispone de capacidad de procesamiento suficiente para escanear los archivos que utilizan al iniciarse.

Para ello, añada más procesadores al Sophos Security VM. Puede hacerlo en cualquier momento.

Nota

Si añade procesadores después de incluir el Sophos Security VM en un grupo de ordenadores en Enterprise Console, debe esperar hasta que el Sophos Security VM cumpla la política de grupo.

En función del tipo de carga, añadir procesadores también puede mejorar el rendimiento general del sistema.

Añadir procesadores en VMware ESXi

Añada procesadores del siguiente modo:

1. Apague el Sophos Security VM.
2. En vSphere Client, seleccione el Sophos Security VM.
3. Seleccione **Edit Settings > Hardware > CPUs**. A continuación, especifique el número de procesadores o CPU.

Añadir procesadores en Microsoft Hyper-V

Añada procesadores del siguiente modo:

1. Haga clic en Inicio, seleccione Herramientas administrativas y haga clic en Administrador de Hyper-V.
2. En el panel de resultados, en Máquinas virtuales, seleccione el Sophos Security VM.
3. En el panel Acción, debajo del nombre del equipo virtual, haga clic en Configuración.
4. Haga clic en Procesador y especifique el número de procesadores.

16 Soporte técnico

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

- Visitar el foro 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>.

17 Aviso legal

Copyright © 2018 Sophos Limited. Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, almacenada en un sistema de recuperación ni transmitida de ninguna forma ni por ningún medio, sea éste electrónico, mecánico, por fotocopia, por grabación o cualquier otro, a menos que disponga de una licencia válida, en cuyo caso puede reproducirse según los términos del acuerdo de licencia, o con 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.

Licencias de terceros

Para las licencias de terceros aplicables a su uso de este producto, consulte la siguiente carpeta del Sophos Security VM: `/usr/share/doc`.

Algunos programas de software se ofrecen al usuario bajo licencias de público general (GPL) o licencias similares de software gratuito que, entre otros derechos, permiten copiar, modificar y redistribuir ciertos programas o partes de los mismos, y tener acceso al código fuente. Las licencias de dichos programas, que se distribuyen al usuario en formato binario ejecutable, exigen que el código fuente esté disponible. Para cualquiera de tales programas que se distribuya junto con el producto de Sophos, se puede obtener el código fuente siguiendo las instrucciones que se incluyen en el [artículo de la base de conocimiento 124427](#).