SOPHOS

Security made simple.

Sophos for Virtual Environments

Guía de configuración: edición Enterprise Console

Versión: 1.0

Contenido

1 Acerca de esta guía

En esta guía se explica cómo configurar Sophos for Virtual Environments.

En la guía se supone que utiliza Sophos Enterprise Console para gestionar su software de seguridad.

Nota: si usa Sophos Central, consulte la ayuda de Sophos Central Admin en su lugar.

2 Configurar políticas

Sophos for Virtual Environments se configura utilizando políticas de Enterprise Console.

Al incluir su Sophos Security VM en un grupo de Sophos Enterprise Console, se aplican políticas que protegen y actualizan los equipos virtuales invitados.

Recomendamos que utilice la configuración predeterminada, ya que ofrece un equilibrio óptimo entre protección y rendimiento del sistema. No obstante, puede cambiar la configuración en estas políticas:

- Antivirus y HIPS
- Actualización

Las demás políticas de Enterprise Console no son aplicables al Sophos Security VM.

Nota: todos los equipos virtuales invitados protegidos por un Sophos Security VM utilizan las mismas políticas que el Sophos Security VM. Para aplicar una política distinta a algunos equipos virtuales invitados, muévalos a otro Sophos Security VM de otro grupo de Enterprise Console. Después aplique una política diferente a este grupo. Para obtener instrucciones sobre cómo mover equipos virtuales invitados, consulte la *Guía de inicio de Sophos for Virtual Environments: edición Enterprise Console*.

Para ver la lista de todos los equipos virtuales invitados administrados por un Sophos Security VM, consulte Ver equipos virtuales protegidos en la página 11.

2.1 Política antivirus y HIPS

De forma predeterminada, el Sophos Security VM:

- Escanea los archivos cuando se accede a ellos en los equipos virtuales invitados.
- Bloquea el acceso a los archivos infectados.
- Limpia automáticamente las amenazas detectadas.

Las opciones de configuración de la política antivirus y HIPS no son todas aplicables al Sophos Security VM. En esta sección se describe qué opciones de escaneado se aplican y pueden configurarse de forma centralizada.

Para obtener más información sobre la configuración, consulte la ayuda de Sophos Enterprise Console.

Escaneado en acceso

Las opciones del escaneado en acceso son compatibles según se detalla a continuación. El control de comportamiento no es compatible.

Para abrir las páginas de configuración del escaneado en acceso en Enterprise Console:

1. En el panel **Políticas**, haga doble clic en **Antivirus y HIPS**.
2. Haga doble clic en la política que desee modificar.
3. En el cuadro de diálogo **Política antivirus y HIPS**, busque el panel **Escaneado en acceso**. Junto a **Activar el escaneado en acceso**, haga clic en **Configurar**.

   Aparece el cuadro de diálogo **Configuración del escaneado en acceso**.

Opción de escaneado en acceso	¿Aplicable al Sophos Security VM?	Notas
Ficha Escaneado		
Comprobar archivos al leer/cambiar el nombre/escribir	No	Si una o más de las tres opciones (leer, cambiar nombre y escribir) están activadas, el Sophos Security VM escaneará en las tres situaciones. **Importante:** si las tres opciones están desactivadas, el escaneado en acceso queda deshabilitado y su sistema deja de estar protegido.
Detectar adware y aplicaciones potencialmente no deseadas/archivos sospechosos	No	
Permitir el acceso a unidades con sectores de arranque infectados	No	
Escanear dentro de archivos comprimidos (no recomendado)	Sí	
Escanear memoria del sistema	No	.
Ficha Extensiones		
Escanear todos los archivos (no recomendado)	Sí	
Escanear sólo los archivos ejecutables o vulnerables	Sí	
Extensiones adicionales a escanear	Sí	
Escanear archivos sin extensión	Sí	
Excluir tipos de archivo del escaneado	Sí	
Ficha Exclusiones		

Opción de escaneado en acceso	¿Aplicable al Sophos Security VM?	Notas
Ficha Exclusiones de Windows	Sí	Para excluir una carpeta del escaneado debe especificar siempre la ruta completa de la carpeta, incluyendo la letra de la unidad o el nombre del recurso compartido en red, por ejemplo, "C:\Tools\logs\" o "\\Server\Tools\logs\". El Sophos Security VM no puede excluir carpetas solo en función de su nombre. Por ejemplo, "\Tools\logs\" no funcionará. Para más información sobre las exclusiones de Windows, por ejemplo, cómo usar caracteres comodín, consulte la ayuda de Sophos Enterprise Console, sección de configuración de la política antivirus y HIPS.
Ficha Exclusiones de Mac	No	
Ficha Exclusiones de Linux/UNIX	No	
Ficha Limpiar		
Limpieza de virus/programas espía	Sí	Las acciones alternativas que deben aplicarse no tienen efecto si la limpieza falla. El Sophos Security VM denegará siempre el acceso a los elementos infectados.
Limpieza de archivos sospechosos	No	

Para más información sobre la configuración y qué opciones escoger, consulte la ayuda de Enterprise Console.

Escaneado programado

Para configurar o editar un escaneado programado:

- En el cuadro de diálogo **Política antivirus y HIPS**, busque el panel **Escaneado programado**.
- Haga clic en **Añadir** o **Editar**.

También puede especificar tipos de archivo adicionales que quiera incluir o excluir del escaneado haciendo clic en **Extensiones y exclusiones**.

Las opciones del escaneado programado son compatibles según se detalla a continuación.

Opción de escaneado programado	¿Aplicable al Sophos Security VM?	Notas
Añadir/editar > Configuración del escaneado programado		
Escanear		
Discos duros locales	Sí	
Disquetes y unidades extraíbles	Sí	
Unidades de CD-ROM	Sí	
Horario de escaneado	Sí	El Sophos Security VM iniciará el escaneado a la hora y en el día especificados. No obstante, y por defecto, solo escaneará dos equipos virtuales al mismo tiempo para no impactar en el rendimiento del su sistema. Por lo tanto, el escaneado de todos los equipos virtuales puede tardar algo más de tiempo.
Añadir/editar > Configuración del escaneado programado > Configurar > Configuración de escaneado y limpieza		
Ficha Escaneado		
Detectar adware y aplicaciones potencialmente no deseadas/archivos sospechosos/rootkits	No	
Escanear archivos comprimidos	Sí	
Escanear memoria del sistema	No	La memoria del sistema se escaneará de forma predeterminada. Esta opción no puede configurarse.
Ejecutar escaneado con baja prioridad	No	
Ficha Limpiar		
Limpieza de virus/programas espía	Sí	El Sophos Security VM no limpia automáticamente disquetes, unidades de CD ni ubicaciones de red. Las acciones para los elementos infectados no tienen efecto si no se ha ejecutado la limpieza. El Sophos Security VM siempre registrará el evento si la limpieza no se ha ejecutado.

Opción de escaneado programado	¿Aplicable al Sophos Security VM?	Notas
Limpieza de adware y aplicaciones potencialmente no deseadas	No	
Limpieza de archivos sospechosos	No	
Extensiones y exclusiones > Extensiones y exclusiones del escaneado programado		
Ficha Extensiones		
Escanear todos los archivos (no recomendado)	Sí	
Escanear sólo los archivos ejecutables o vulnerables	Sí	
Extensiones adicionales a escanear	Sí	
Escanear archivos sin extensión	Sí	
Excluir tipos de archivo del escaneado	Sí	
Ficha Exclusiones		
Ficha Exclusiones de Windows	Sí	Para excluir una carpeta del escaneado debe especificar siempre la ruta completa de la carpeta, incluyendo la letra de la unidad o el nombre del recurso compartido en red, por ejemplo, "C:\Tools\logs\" o "\\Server\Tools\logs\". El Sophos Security VM no puede excluir carpetas solo en función de su nombre. Por ejemplo, "\Tools\logs\" no funcionará. Para obtener más información sobre las exclusiones de Windows, por ejemplo, cómo utilizar comodines, consulte la ayuda de Enterprise Console.
Ficha Exclusiones de Mac	No	
Ficha Exclusiones de Linux/UNIX	No	

Protección activa de Sophos

La protección activa de Sophos es compatible, exceptuando el envío de archivos.

Protección web

Incompatible.

Autorización

La autorización, así como la detección, de adware y otras aplicaciones potencialmente no deseadas (PUA) no es compatible.

Notificación

Solo es compatible la notificación por correo electrónico.

2.1.1 Extensiones de archivos escaneados

Los archivos con las extensiones siguientes se escanean por defecto.

386 3gr add ani asp aspx asx bat cab chm class cmd com cpl dbx dex dll dmd doc docm	docx dot drv eml exe fas flt fon fot hlp ht? hta html i13 ifs inf ini jar jpeg jpg	Jpz js jse lnk lsp mnl mod mpd mpp mpt mso mui nws o ocx ov? pdf pdr php pif	pl pot pps ppt pptm pptx prc rtf scr sh shb shs src swf sys tif tiff vb? vlx vs?	vxd wbk wma wmf wsf xl? xlsm xlsx xsn zip zipx

Las siguientes extensiones adicionales se escanean por defecto si la opción **Escanear dentro de archivos comprimidos** de la política antivirus y HIPS aplicada al Sophos Security VM está activada.

7z 7zip	lha lzh

??_ a arj bin bz2 gz hqx hxs	rar rpm tar taz tbz tbz2 tgz

Puede añadir extensiones específicas para que sean escaneadas o excluir extensiones del escaneado según se describe en la ayuda de Enterprise Console, sección de configuración de la política antivirus y HIPS.

2.2 Política de actualización

Todas las opciones de configuración de la política de actualización de Enterprise Console son aplicables al Sophos Security VM.

Para obtener más información, consulte la ayuda de Enterprise Console, sección **Actualizar ordenadores** > **Configurar la política de actualización**.

3 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.

4 Escanear equipos virtuales invitados

Sophos for Virtual Environments escanea los archivos en acceso, es decir, cuando se abren y se cierran (si tiene activado el escaneado en acceso en su política).

Un Sophos Security VM también puede realizar un escaneado completo de todos los equipos virtuales invitados que administra. Puede realizar el escaneado de forma inmediata o de forma programada.

El escaneado remoto puede detectar amenazas, pero no limpiarlas.

Note: el Sophos Security VM no puede ejecutar un escaneado si todavía está en el grupo **No asignados** de Enterprise Console. Debe estar en un grupo en el que haya aplicado políticas.

Note: el Sophos Security VM realiza los escaneados por fases para impedir la sobrecarga del hipervisor. De forma predeterminada, se escanean siempre dos equipos virtuales invitados a la vez. Escanear un gran número de equipos virtuales invitados puede tardar bastante tiempo.

Escanear equipos virtuales invitados ahora

Para realizar un escaneado remoto de todos los equipos virtuales invitados de forma inmediata:

1. Vaya a Enterprise Console y localice el Sophos Security VM en la lista de ordenadores.
2. Haga clic con el botón derecho sobre el Sophos Security VM y seleccione **Escaneado remoto**.

   Note: también encontrará este comando en el menú **Acciones**.

Escanear equipos virtuales invitados de forma programada

Para realizar un escaneado remoto de todos los equipos virtuales invitados de forma programada:

1. Vaya a Enterprise Console.
2. Cree un escaneado programado, como se describe en la ayuda de Enterprise Console en la sección sobre la configuración de la política antivirus y HIPS.

Para ver el resultado de los escaneados completados:

En Enterprise Console, en la lista de ordenadores de la parte inferior derecha de la ventana, haga doble clic en el Sophos Security VM para abrir el cuadro de diálogo **Detalles del ordenador**.

5 Información sobre una amenaza

Para obtener información sobre una amenaza y cómo limpiarla:

1. En Enterprise Console, en la lista de ordenadores de la parte inferior derecha de la pantalla, haga doble clic en el Sophos Security VM para abrir el cuadro de diálogo **Detalles del ordenador**.

   En la sección **Historial**, se enumeran los **Elementos detectados**. El nombre de la amenaza se muestra en la columna **Nombre** y el nombre del equipo virtual afectado y el nombre del archivo detectado se muestran en la columna **Detalles**.

2. Haga clic en el nombre de la amenaza.

   Se abrirá el sitio web de Sophos, donde encontrará una descripción del elemento y qué hacer para solucionar el problema.

6 Limpiar una amenaza

6.1 Limpieza automática

El Sophos Security VM puede limpiar automáticamente las amenazas que detecta.

Note: la limpieza automática no está disponible en el caso de CD u otros sistemas de archivos o medios de solo lectura, ni en sistemas de archivos remotos.

¿Qué sucede cuando se produce una limpieza automática?

Cuando se detecta una amenaza y se limpia automáticamente, Enterprise Console:

- Muestra que se ha bloqueado la amenaza (véase la sección "Historial" del cuadro de diálogo **Detalles del ordenador**).
- Muestra una alerta que indica cuál es la amenaza y si se puede limpiar.
- Elimina la alerta si la limpieza se realiza correctamente y la marca como "Imposible limpiar" si la limpieza falla.

A veces puede ser necesario reiniciar un equipo virtual invitado para que se complete la limpieza. En este caso, se muestra la alerta "Es necesario reiniciar" para el Sophos Security VM. Para comprobar a qué equipo virtual invitado corresponde la alerta, haga doble clic en el Sophos Security VM para abrir el cuadro de diálogo **Detalles del ordenador** y ver la descripción de la alerta en la sección **Alertas y errores pendientes**.

6.2 Limpieza manual

Las amenazas pueden limpiarse de forma manual.

Debe borrar la alerta de Enterprise Console una vez que haya eliminado la amenaza.

6.2.1 Limpiar el equipo virtual afectado

Para la limpieza manual, debe restaurar el equipo virtual invitado. Tenga en cuenta que perderá los datos al hacerlo. Utilice uno de estos métodos:

- Revertir el equipo virtual afectado a un estado anterior limpio.
- Eliminar el equipo virtual afectado y volver a crearlo.

Asegúrese de que la imagen de plantilla tenga las herramientas de Sophos necesarias instaladas (consulte la *Guía de inicio de Sophos for Virtual Environments: edición Enterprise Console*).

Independientemente del método usado, ejecute un escaneado completo del equipo virtual posteriormente para asegurarse de que está limpio.

6.2.2 Quitar una alerta en Enterprise Console

Tras limpiar el equipo virtual afectado, quite la alerta en Enterprise Console:

1. En Enterprise Console, en la lista de ordenadores, haga clic con el botón derecho en el Sophos Security VM y seleccione **Resolver alertas y errores**.
2. En el cuadro de diálogo **Resolver alertas y errores**, en la ficha **Alertas**, seleccione la alerta y haga clic en **Quitar**.

La alerta desaparecerá de Enterprise Console.

7 Alertas

En esta sección se describen las alertas que envía el Sophos Security VM cuando se detectan y se limpian amenazas.

Alertas de amenazas

Si el Sophos Security VM detecta alguna amenaza en un equipo virtual invitado, enviará las siguientes alertas:

En Enterprise Console:

- Se muestra una alerta en el panel de control.
- Aparece un icono rojo de alerta en la lista de ordenadores, en la ficha **Estado**, junto al Sophos Security VM en la columna **Alertas y errores**.

Si la amenaza se limpia automáticamente, la alerta relativa a la amenaza se quita de Enterprise Console.

Para saber a qué equipo virtual invitado es aplicable la alerta, haga doble clic en el Sophos Security VM en la lista de ordenadores. En **Detalles del ordenador**, en **Alertas y errores pendientes**, busque la descripción de la alerta. Se muestran los detalles del equipo virtual invitado, seguidos de la ruta de la amenaza, del siguiente modo:

```
NombreEquipo(dirección IP)/C:\amenaza.exe
```

Si el Sophos Security VM detecta una amenaza cuando el usuario intenta acceder a un archivo, también puede aparecer un mensaje en el equipo virtual invitado indicando al usuario que no se puede acceder al archivo. Aunque este depende de la aplicación usada para acceder al archivo.

Alertas después de la limpieza

Si la amenaza se limpia, la alerta se quita de Enterprise Console.

También se informa de la limpieza en Enterprise Console. Para ver el informe, haga doble clic en el Sophos Security VM en la lista de ordenadores para abrir el cuadro de diálogo **Detalles del ordenador** y busque **Historial**.

Si la amenaza se ha eliminado parcialmente, pero es necesario reiniciar el equipo virtual para completar la limpieza, se mostrará la alerta "Requiere reinicio".

8 Registros

En los equipos virtuales, los registros se escriben en el registro de eventos de aplicación de Windows. Encontrará el registro en **Registros de aplicaciones y servicios** > **Sophos** > **SVE**.

En un Sophos Security VM, puede recopilar los registros y recuperarlos desde el directorio de registros compartidos. Para ello:

1. Abra una consola en el Sophos Security VM.
2. Inicie sesión:
   - El nombre de usuario es "sophos".
   - La contraseña es la contraseña de acceso que estableció cuando instaló el Sophos Security VM.
3. Introduzca el siguiente comando:

   ```
   sudo /opt/sophox/logcollector/diagnose
   ```

   Introduzca su contraseña de acceso cuando se le solicite. (Esto puede tardar un minuto en completarse).
4. En el Explorador de Windows, ya puede acceder a los registros recopilados en `\\<SVM-IP-Address>\logs\logs.tgz`. Introduzca sus credenciales cuando se le solicite:
   - El nombre de usuario es "sophos".
   - La contraseña es la contraseña de acceso que estableció cuando instaló el Sophos Security VM.

Para información sobre el registro en Enterprise Console, consulte la ayuda de Enterprise Console.

9 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.

10 Aviso legal

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.