SOPHOS

Cybersecurity made simple.

Sophos Endpoint para Windows

Ayuda

Contenido

1 Acerca de Sophos Endpoint para Windows

Este archivo de ayuda proporciona información sobre Sophos Endpoint para Windows y explica los procedimientos paso a paso.

Copyright © Sophos Limited

2 Sophos Endpoint

Sophos Endpoint se ejecuta en ordenadores y servidores para protegerlos.

Restricción
Es posible que no disponga de todas las funciones descritas aquí. Depende de su licencia.

Sophos Endpoint se configura y administra de forma centralizada desde Sophos Central Admin.

Sin embargo, algunas tareas pueden realizarse desde el ordenador o servidor:

- Comprobar el estado del ordenador.
- Escanear un archivo, ordenador o servidor en busca de amenazas.
- Consultar detalles de eventos en el ordenador o servidor, como las amenazas que se han detectado.
- Limpiar una amenaza.
- Cambiar la configuración de seguridad. Por ejemplo, puede desactivar funciones para solucionar problemas.
- Actualizar.
- Solucionar problemas.

Nota
Para limpiar amenazas o cambiar la configuración, debe utilizar el **inicio de sesión de administrador** e introducir la contraseña de protección contra manipulaciones.

Conceptos relacionados

Estado (página 3)
Puede comprobar el estado de seguridad y escanear su equipo o servidor.

Eventos (página 5)
La página **Eventos** muestra los eventos que tienen lugar en el ordenador o servidor, como las amenazas que se detectan.

Tareas relacionadas

Escanear un archivo (página 9)
Puede escanear archivos individuales.

Escanear el ordenador o servidor (página 9)
Siga estas instrucciones para escanear su ordenador o servidor.

Limpiar una amenaza (página 9)
Siga estas instrucciones para limpiar una amenaza que se haya detectado.

Cambiar la configuración de seguridad (página 9)
Siga estas instrucciones para cambiar la configuración de seguridad.

Actualizar ahora (página 10)
Siga estas instrucciones para actualizar las definiciones de virus.

Solucionar problemas (página 10)
Siga estas instrucciones para solucionar problemas.

Copyright © Sophos Limited

3 Estado

Puede comprobar el estado de seguridad y escanear su equipo o servidor.

Restricción
Es posible que no disponga de todas las funciones descritas aquí. Depende de su licencia.

La página **Estado** le permite:

- Comprobar el estado de seguridad del ordenador o servidor.
- Escanear el ordenador o servidor en busca de amenazas.
- Consultar las funciones instaladas y su estado de seguridad.

Nota
El enlace **Acerca de** en la parte inferior derecha de la página le permite actualizar las definiciones de virus o solucionar problemas con el producto.

Estado de seguridad

Un icono en la parte superior de la página muestra el estado.

Opción de configuración	Descripción
 Verde.	No hay alertas o solo alertas de prioridad baja.
 Rojo.	Hay alertas de prioridad alta.
 Amarillo.	Hay alertas de prioridad media.
 Gris.	Se desconoce el estado.

Debajo, se muestran todas las funciones instaladas con su estado de seguridad individual.

Copyright © Sophos Limited

Escanear el ordenador

Haga clic en **Escanear** para escanear todos los archivos del ordenador o servidor en busca de amenazas.

Tras completarse el escaneado, verá un resumen de los resultados. Si se detectan amenazas, puede ir a la página **Eventos** para ver los detalles.

Copyright © Sophos Limited

4 Eventos

La página **Eventos** muestra los eventos que tienen lugar en el ordenador o servidor, como las amenazas que se detectan.

Restricción
Es posible que no disponga de todas las funciones descritas aquí. Depende de su licencia.

Puede filtrar los eventos, por ejemplo para mostrar solo los que requieran alguna medida, o buscar tipos de eventos específicos.

Lista Eventos

La lista muestra:

- La gravedad. Un icono en el extremo izquierdo de la lista muestra si el evento tiene prioridad alta, prioridad media o es una notificación.
- El origen. Un icono en la parte izquierda de la lista indica la función de Sophos que ha informado del evento.
- La fecha y la hora en que ha tenido lugar el evento.
- Una descripción del evento.
- Un enlace que le permite tomar medidas (si se necesita tomar alguna medida). Este dato solo se muestra si ha iniciado sesión como administrador.

Para ver los detalles de cada evento, haga clic en la flecha de la derecha para expandirlo.

Las medidas que puede tomar son las mismas que las disponibles en Sophos Central Admin. Consulte la lista en la página **Alertas** de la Ayuda de Sophos Central Admin.

Puede filtrar los eventos por los siguientes tipos:

Tipo de evento	Descripción
Programas maliciosos y PUAs	El malware es el término genérico utilizado para englobar programas peligrosos como virus, gusanos, troyanos y programas espía. Las aplicaciones no deseadas (PUA) son programas que no son maliciosos, como marcadores telefónicos, herramientas de administración remota y herramientas de ataque remoto, pero que no se consideran adecuadas en entornos laborales.

Copyright © Sophos Limited

Tipo de evento	Descripción
Amenazas web	Las amenazas web incluyen sitios web maliciosos, sitios web sin clasificar y descargas peligrosas. Algunos sitios web, como sitios para adultos o redes sociales, también se suelen considerar inapropiados en entornos laborales. Estos sitios web pueden bloquearse.
Comportamiento malicioso	El comportamiento malicioso es el comportamiento sospechoso que se detecta en un programa que ya se está ejecutando en el ordenador o servidor. Los programas de ransomware son software malicioso que impide acceder a los archivos hasta que se pague un rescate.
Elementos controlados	Esta categoría incluye: • Aplicaciones que no suponen una amenaza para la seguridad, pero cuyo uso se considera inadecuado en el entorno empresarial. • Periféricos y medios extraíbles. • Descargas peligrosas o sitios web que no son apropiados en el entorno laboral. • Archivos que contienen información confidencial (como datos personales o financieros) que no desea que se filtren.
Tráfico malicioso	El tráfico malicioso es aquel entre ordenadores que indica un posible intento de toma de control del ordenador o servidor (un ataque de "comando y control").
Exploits	Las vulnerabilidades que Sophos puede evitar incluyen el secuestro de aplicaciones y los exploits que se aprovechan de las vulnerabilidades en navegadores, complementos de navegador, aplicaciones Java, aplicaciones multimedia y aplicaciones Microsoft Office.

Copyright © Sophos Limited

5 Configuración

Puede cambiar temporalmente la configuración de seguridad del ordenador o servidor.

Es posible que tenga que hacerlo para solucionar problemas. Por ejemplo, puede desactivar una función para ver si está causando problemas en el ordenador.

Restricción
Es posible que no disponga de todas las funciones descritas aquí. Depende de su licencia.

Restricción
La página **Configuración** solo está disponible si ha introducido la contraseña de protección contra manipulaciones (disponible del administrador de Sophos Central).

Cómo cambiar la configuración

Marque la casilla **Anular política de Sophos Central hasta 4 horas para solucionar problemas**.

Ahora puede realizar cambios en la página. Los cambios anulan temporalmente la política que usted (u otro administrador) haya aplicado desde Sophos Central Admin.

Tras cuatro horas, la configuración vuelve a cambiar automáticamente a la de las políticas impuestas de forma centralizada.

Si lo desea, puede restaurar la configuración antes. No puede usar los controles deslizantes para hacerlo para funciones individuales. En vez de ello, desactive **Anular política de Sophos Central hasta 4 horas para solucionar problemas**.

Deep Learning

El Deep Learning utiliza el aprendizaje automático avanzado para detectar amenazas. Puede identificar malware y aplicaciones no deseadas sin utilizar firmas.

Escaneado en tiempo real

El escaneado en tiempo real escanea elementos cuando los usuarios intentan acceder y bloquea el acceso a menos que estén limpios. Puede seleccionar:

- **Archivos**: Esta opción escanea los archivos locales y (si está seleccionado en la política) los recursos compartidos de red.
- **Internet**: Esta opción escanea los recursos de Internet. Puede escanear descargas en curso, bloquear el acceso a sitios web maliciosos y detectar sitios web de baja reputación.

Controles en usuarios

- La opción **Control de periféricos** le permite controlar el acceso a periféricos y medios extraíbles.

Copyright © Sophos Limited

- La opción **Control de aplicaciones** permite detectar y bloquear aplicaciones que no suponen ningún peligro, pero que no se consideran adecuadas en el entorno empresarial.
- La opción **Control web** le permite protegerse contra descargas peligrosas, controlar los sitios que pueden visitar los usuarios y evitar las fugas de datos.
- La opción **Prevención de fugas de datos** le permite supervisar y restringir las transferencias de archivos que contengan datos confidenciales.
- La opción **Protección contra manipulaciones** le permite restringir los cambios. Si esta opción está activada, un administrador local necesitará la contraseña obligatoria para cambiar la configuración de seguridad o desinstalar Sophos Endpoint.

Protección en tiempo de ejecución

La protección en tiempo de ejecución protege contra amenazas detectando tráfico o comportamientos sospechosos o maliciosos en los ordenadores. Puede seleccionar:

- **Detección de ransomware**: Esta opción protege contra programas maliciosos que restringen el acceso a los archivos y exigen un pago para recuperarlos.
- **Navegación segura**: Esta opción protege los navegadores web contra la explotación por parte de programas maliciosos.
- **Mitigación de vulnerabilidades**: Esta opción protege las aplicaciones más propensas a la explotación por parte de programas maliciosos, como las aplicaciones Java.
- **Protección contra amenazas de la red**: Esto detecta tráfico entre un ordenador y un servidor que indica un posible intento de toma de control del ordenador. Incluye la inspección de paquetes, que escanea las comunicaciones de red, identificando y bloqueando amenazas antes de que puedan perjudicar el sistema operativo o las aplicaciones.

  Nota
  Si desactiva **Protección contra amenazas de la red**, las funciones de EDR, Aislamiento y Obstrucción, también se desactivarán.

- **Detección de comportamiento malicioso**: Esta opción detecta y bloquea comportamientos que se sabe que son maliciosos o que son sospechosos.

Controles del equipo

Puede supervisar el Firewall de Windows (y otros firewalls registrados) en sus ordenadores y servidores.

Copyright © Sophos Limited

6 Cómo...

6.1 Escanear un archivo

Puede escanear archivos individuales.

Para escanear un archivo, haga lo siguiente:

- En el Explorador, haga clic con el botón derecho en el archivo y seleccione **Escanear**.

6.2 Escanear el ordenador o servidor

Siga estas instrucciones para escanear su ordenador o servidor.

Para escanear todos los archivos del ordenador o servidor:

1. Vaya a la página **Estado** o a la página **Detecciones**.
2. Haga clic en **Escanear**.
   Tras completarse el escaneado, verá un resumen de los resultados.
3. Si se detectan amenazas, puede ir a la página **Eventos** para ver los detalles.

6.3 Limpiar una amenaza

Siga estas instrucciones para limpiar una amenaza que se haya detectado.

Para limpiar una amenaza, haga lo siguiente:

1. Haga clic en **Inicio de sesión de administrador** e introduzca la contraseña de protección contra manipulaciones (disponible de su administrador de Sophos Central).
2. Vaya a la página **Eventos** para ver los detalles de la amenaza que se ha detectado.
3. Busque un enlace de acción junto a los detalles de la amenaza.

Las medidas que puede tomar son las mismas que las disponibles en Sophos Central Admin. Consulte la lista en la página **Alertas** de la Ayuda de Sophos Central Admin.

6.4 Cambiar la configuración de seguridad

Siga estas instrucciones para cambiar la configuración de seguridad.

Para cambiar la configuración de seguridad:

1. Haga clic en **Inicio de sesión de administrador** en la parte superior derecha de la interfaz.
2. Introduzca la contraseña de protección contra manipulaciones (disponible de su administrador de Sophos Central).
   En la barra de menús, aparecerá el enlace **Configuración**.
3. Vaya a la página **Configuración**.
4. Marque la casilla **Anular política de Sophos Central hasta 4 horas para solucionar problemas**.
5. Utilice los controles deslizantes de la página para desactivar las funciones de seguridad.

Copyright © Sophos Limited

Tras cuatro horas, la configuración se restaurará automáticamente y volverá a regirse por las políticas impuestas de forma centralizada.

Nota
Si lo desea, puede restaurar la configuración antes. No puede usar los controles deslizantes para hacerlo para funciones individuales. En vez de ello, desmarque la opción **Anular política de Sophos Central hasta 4 horas para solucionar problemas**.

6.5 Actualizar ahora

Siga estas instrucciones para actualizar las definiciones de virus.

Para actualizar, haga lo siguiente:

1. Haga clic en **Acerca de**.
2. Haga clic en **Actualizar ahora**.

6.6 Solucionar problemas

Siga estas instrucciones para solucionar problemas.

Para solucionar problemas, haga lo siguiente:

1. Haga clic en **Acerca de**.
2. Haga clic en **Abrir la herramienta Endpoint Self Help** para recopilar datos sobre el problema o haga clic en el enlace al **Foro de la comunidad**.

6.7 Cifrar su equipo

Siga estas instrucciones para cifrar su ordenador.

Restricción
Device Encryption solo está disponible en estaciones de trabajo.

Device Encryption cifra el disco duro del ordenador utilizando la tecnología de BitLocker de Windows. Su administrador define si debe autenticarse cada vez que accede a su ordenador.

Si no se requiere autenticación, el cifrado del disco duro se iniciará automáticamente tan pronto como reinicie el ordenador después de recibir la política de Sophos Central. No tiene que hacer nada en este caso.

Si necesita autenticarse, haga lo siguiente:

1. Cuando se muestre el cuadro de diálogo **Sophos Device Encryption**, siga las instrucciones. Las instrucciones específicas dependen de su sistema y de la configuración de políticas definida por su administrador.
    - Si la política de Device Encryption requiere un PIN o una contraseña para la autenticación, siga las instrucciones en pantalla para crear un PIN o una contraseña.

Copyright © Sophos Limited

Nota
Tenga cuidado al crear un PIN o una contraseña. El entorno previo al arranque solo admite la distribución de teclado en inglés EE. UU. Si ahora crea un PIN o una contraseña con caracteres especiales, es posible que deba utilizar teclas distintas cuando los introduzca para iniciar sesión más adelante.

- Si la política de Device Encryption requiere una llave USB para la autenticación, debe conectar una memoria USB a su ordenador. El formato de la memoria USB debe ser NTFS, FAT o FAT32.

2. Al hacer clic en **Reiniciar y cifrar**, el ordenador se reinicia y cifra los discos duros. Puede trabajar como de costumbre.

Nota
Puede seleccionar **Más tarde** para cerrar el cuadro de diálogo. Sin embargo, volverá a aparecer la próxima vez que inicie sesión.

Después de que Sophos Central haya cifrado el volumen del sistema, se inicia el cifrado de los volúmenes de datos. Los volúmenes de datos extraíbles, como las memorias USB, no se cifran.

Cuando inicie sesión en el ordenador, es posible que necesite un PIN, una contraseña o una llave USB para desbloquear el volumen del sistema. Los volúmenes de datos se desbloquean automáticamente.

6.8 Acceder a su ordenador si se le olvida la contraseña

Siga estos pasos para obtener acceso a su ordenador.

Si no puede iniciar sesión en su ordenador porque ha olvidado su PIN, contraseña o llave USB, necesitará una clave de recuperación.

Si utiliza Sophos Device Encryption, la clave de recuperación se almacena en Sophos Central. Para obtener su clave de recuperación, escoja una de las opciones siguientes:

- Inicie sesión en el portal de autoservicio de Sophos y siga las instrucciones de la Ayuda.
- Pida al administrador que obtenga la clave de recuperación por usted. Siga este procedimiento si no puede utilizar el portal de autoservicio.

Tareas relacionadas

Usar la recuperación de BitLocker (página 11)
Siga estas instrucciones para recuperar su ordenador.

6.8.1 Usar la recuperación de BitLocker

Siga estas instrucciones para recuperar su ordenador.

Para recuperar su ordenador, haga lo siguiente:

1. Reinicie el ordenador y pulse la tecla Esc en la pantalla de inicio de sesión de **BitLocker**.
2. En la pantalla **Recuperación de BitLocker**, busque el **ID de la clave de recuperación**.

Copyright © Sophos Limited

El **ID de la clave de recuperación** se muestra solo unos instantes. Para volver a verlo, es necesario reiniciar el ordenador.

3. Póngase en contacto con su administrador y proporciónele el **ID de la clave de recuperación**. El administrador debe buscar la clave de recuperación de su ordenador en Sophos Central y darle la clave.
4. En la pantalla **Recuperación de BitLocker**, introduzca la clave de recuperación. Ahora puede iniciar el ordenador.
5. Siga las instrucciones en pantalla para crear una nueva contraseña o PIN de BitLocker cuando se le solicite.

   En ordenadores que ejecuten Windows 7, no verá instrucciones. Tendrá que restablecer su PIN/contraseña manualmente.

Ya puede acceder a su ordenador de nuevo.

Nota
Una clave de recuperación solo puede usarse una vez. Si necesita recuperar su ordenador otra vez más adelante, deberá obtener una nueva clave de recuperación.

Copyright © Sophos Limited

7 ¿Por qué se bloquea una transferencia de archivos?

Es posible que vea un mensaje para informarle que se ha bloqueado una transferencia de archivos (por ejemplo, al copiar, mover o enviar archivos por correo electrónico).

Esto sucede porque su empresa ha configurado una política para evitar que envíe información confidencial de forma involuntaria a usuarios que no deben acceder a ella.

Hay dos tipos de mensaje.

Mensaje	Descripción
Se ha bloqueado la transferencia	Si recibe un mensaje de bloqueo de transferencia de archivos, no puede transferir los archivos. Es posible que el administrador haya incluido algún consejo en el mensaje.
Se puede permitir la transferencia	Si recibe un mensaje de solicitud de transferencia de archivos bloqueada, puede decidir si se van a transferir los archivos. Es posible que el administrador haya incluido algún consejo en el mensaje. Haga clic en **Permitir** para confirmar que es seguro seguir adelante.

Copyright © Sophos Limited

8 Soporte

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/es-es/support/contact-support/support-query.aspx.

Copyright © Sophos Limited

9 Aviso legal

Copyright © 2020 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. Otros productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.