SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

Guía de administrador

Contenido

1 Acerca de Sophos Central Device Encryption

Sophos Central Device Encryption le permite gestionar el Cifrado de unidad BitLocker en estaciones Windows y el cifrado FileVault en equipos Mac a través de Sophos Central.

El cifrado de discos duros garantiza la seguridad de los datos, incluso en caso de pérdida o robo de un dispositivo.

En esta guía se describe cómo configurar y utilizar Device Encryption. También explica cómo recuperar la clave de recuperación mediante el portal de autoservicio. Para obtener información detallada sobre la configuración de directivas, las alertas y la recuperación mediante Sophos Central, consulte la Sophos CentralAyuda.

Información relacionada

Ayuda de Sophos Central

2 Administrar el Cifrado de unidad BitLocker

En esta sección se describen los requisitos previos para usar el Cifrado de unidad BitLocker en las estaciones Windows de su red, los distintos modos de autenticación que hay disponibles y cómo interactúan con la configuración de directiva de grupo de BitLocker.

2.1 Migrar a Sophos Central Device Encryption

Si ya utiliza SafeGuard Enterprise con el Cifrado de unidad BitLocker o Sophos Full Disk Encryption, en esta sección se describe cómo migrar a Sophos Central Device Encryption.

Abarca:

- SafeGuard Enterprise y BitLocker
- SafeGuard Enterprise y Sophos Full Disk Encryption
- Para obtener información sobre la migración de equipos Mac, consulte Migrar a Sophos Central Device Encryption (Mac).

Tareas relacionadas

Migrar a Sophos Central Device Encryption (Mac) (página 14)
Si quiere utilizar Sophos Central para administrar equipos Mac que ya estén cifrados con FileVault, les debe aplicar una política de Sophos Central Device Encryption.

2.1.1 Migrar de SafeGuard Enterprise BitLocker

Siga estos pasos para migrar.

Nota
Si utiliza BitLocker con la versión 6.x o 7.x de SafeGuard Enterprise, le recomendamos que primero actualice a la versión más reciente de SafeGuard Enterprise.

Si utiliza la versión 6.x o 7.x de SafeGuard Enterprise, debe descifrar el disco del sistema siguiendo los pasos descritos en la Ayuda de administrador de SafeGuard Enterprise antes de migrar a Sophos Central Device Encryption.

Para migrar de un cliente de BitLocker con SafeGuard Enterprise (versión 8.0 o posterior) a Sophos Central Device Encryption:

1. Vaya a **Panel de control > Desinstalar un programa** y haga clic con el botón derecho en **Sophos SafeGuard Client**.
2. Seleccione **Cambiar** del menú contextual.
   Se abrirá el asistente de configuración Sophos SafeGuard Client Setup.
3. Desinstale el componente BitLocker.

Nota
Desinstalar el componente BitLocker no conlleva el descifrado de sus volúmenes o archivos.

4. Instale el software de Sophos Central Device Encryption.
5. Asegúrese de que haya una política de Sophos Central Device Encryption asignada a una estación de trabajo y que esté activada.

Ahora ya puede administrar BitLocker mediante Sophos Central. No es necesario volver a cifrar. Cuando haya aplicado una política de Sophos Central Device Encryption a la estación, la clave de recuperación se renovará y enviará a Sophos Central. La funcionalidad del cifrado de archivos no varía.

Información relacionada
Ayuda de administrador de SafeGuard Enterprise

2.1.2 Migrar desde SafeGuard Enterprise Full Disk Encryption

Siga estos pasos para migrar.

Para migrar desde SafeGuard Enterprise Full Disk Encryption:

1. Desinstale el software del cliente Sophos SafeGuard.
   Los volúmenes cifrados se descifrarán automáticamente. Los archivos cifrados seguirán estando cifrados.
2. Instale el software de Sophos Central Device Encryption.
3. Asegúrese de que haya una política de Sophos Central Device Encryption asignada a una estación de trabajo y que esté activada.
4. Vuelva a instalar el módulo necesario de SafeGuard Enterprise File Encryption (Synchronized Encryption o cifrado de archivos basado en la ubicación).

Ahora ya puede administrar BitLocker mediante Sophos Central. Cuando haya aplicado una política de Sophos Central Device Encryption a la estación, el cifrado se iniciará en segundo plano y la clave de recuperación se renovará y enviará a Sophos Central.

2.2 Preparar el cifrado de dispositivos

De forma predeterminada, la mayoría de unidades del sistema están preparadas para BitLocker. De no ser así, Sophos Central Device Encryption ejecuta automáticamente la herramienta de línea de comandos necesaria de Microsoft `BdeHdCfg.exe` para preparar la unidad.

Esto significa que en la unidad del sistema se crea una partición de BitLocker aparte.

Durante la configuración de Sophos Central Device Encryption, un mensaje informará al usuario de que debe reiniciarse el equipo para preparar la unidad del sistema. El usuario puede optar por reiniciar el equipo inmediatamente o aplazar la operación. El cifrado de dispositivos solo puede iniciarse cuando el equipo se haya reiniciado y la unidad del sistema se haya preparado correctamente.

La versión de .NET Framework requerida por Device Encryption se instala en las estaciones de trabajo automáticamente.

2.3 Cifrado de dispositivos paso a paso

Siga estos pasos para cifrar dispositivos.

Antes de que los usuarios puedan empezar:

- El software del agente de Sophos Central debe estar instalado en las estaciones.
- Debe haber configurada una directiva de cifrado de dispositivos en Sophos Central.
- Los usuarios deben iniciar sesión en sus estaciones de forma interactiva y conectarse y sincronizarse con Sophos Central. Tenga en cuenta que no se admite el inicio de sesión remoto.
- El sistema operativo debe ser compatible con el Cifrado de unidad BitLocker. Para obtener más información, consulte Preparar el cifrado de dispositivos y Sistemas compatibles con Device Encryption.

Las instrucciones siguientes le indican lo que verán los usuarios y lo que deben hacer:

1. Si el hardware de seguridad TPM aún no está activado, se desencadena una acción del BIOS para activarlo. Esto requiere reiniciar el equipo. El usuario puede optar por reiniciar el equipo inmediatamente o aplazar la operación.
   Durante el reinicio, se pedirá al usuario que active el TPM. Si no se puede activar el TPM o el usuario no responde, se mostrará un mensaje.
2. Si el TPM está activo pero no es propio, el software del agente de Sophos Central genera y define la información de propiedad del TPM de forma automática. Si se produce un error, se envía una alerta a Sophos Central.
3. Si faltan las claves de aprobación del TPM, el software del agente de Sophos Central las crea automáticamente. Si se produce un error, se envía una alerta a Sophos Central.
4. Si la política de Device Encryption no especifica **Requerir autenticación de inicio**, el cifrado del disco duro se inicia automáticamente. Los usuarios no tienen que hacer nada en este caso. Puede ir al paso 8.
5. Si la política de Device Encryption sí que especifica **Requerir autenticación de inicio**, el usuario verá el cuadro de diálogo **Sophos Device Encryption**.
   - Si la política de Device Encryption requiere un PIN o una contraseña para la autenticación, los usuarios deben seguir las instrucciones en pantalla para definir un PIN o una contraseña. Si se utiliza TPM+PIN, la clave de cifrado para el disco del sistema se almacenará en el TPM.

     Nota
     Los usuarios deben tener cuidado a la hora de definir una contraseña. El entorno previo al arranque solo admite la distribución de teclado en inglés EE. UU. Si ahora establecen un PIN o una contraseña con caracteres especiales, es posible que deban utilizar teclas distintas cuando los introduzcan para iniciar sesión más adelante.

   - Si la política de Device Encryption requiere una llave USB para la autenticación, los usuarios deben conectar una memoria USB a su ordenador. El formato de la memoria USB debe ser NTFS, FAT o FAT32.
6. Cuando el usuario hace clic en **Reiniciar y cifrar**, el equipo se reinicia y comprueba que Device Encryption funcione.
   El usuario puede seleccionar **Más tarde** para cerrar el cuadro de diálogo. Sin embargo, volverá a aparecer la próxima vez que el usuario inicie sesión o cuando usted cambie la política de Device Encryption.

7. Si el usuario no puede introducir la contraseña o el PIN correcto, puede pulsar la tecla `Esc`. El sistema arranca normalmente ya que el cifrado no se ha aplicado todavía. Se pedirá al usuario que vuelva a introducir la contraseña o el PIN después de iniciar sesión.
8. Puede ver los usuarios que aún no han activado el cifrado. Esto significa que aún no han reiniciado el ordenador o que no todavía no han seguido las instrucciones en pantalla. Consulte **Informes** en Sophos Central.
9. Si la prueba previa al arranque es satisfactoria, el software del agente de Sophos Central inicia el cifrado de los discos fijos. El cifrado tiene lugar en un segundo plano, lo que permite al usuario trabajar con normalidad.
   Si la prueba de hardware da error, el sistema se reiniciará y no se aplicará el cifrado. Se enviará un evento a Sophos Central para notificarle.
10. Después de que el agente de Sophos Central haya cifrado el volumen del sistema, se inicia el cifrado de los volúmenes de datos (si se especifica en la política). La protección para estos volúmenes se almacena en el volumen del sistema, de modo que los volúmenes de datos están disponibles automáticamente después del inicio. Esto quiere decir que cuando un usuario inicia sesión en su equipo, se puede acceder a los volúmenes de datos sin más interacción por parte del usuario. Los volúmenes de datos extraíbles, como las unidades de memoria USB, no se cifran.

Puede encontrar dos archivos de registro, `CDE.log` y `CDE_trace.xml`, en `%ProgramData%\Sophos\Sophos Data Protection\Logs` en la estación de trabajo.

Conceptos relacionados

Preparar el cifrado de dispositivos (página 3)
De forma predeterminada, la mayoría de unidades del sistema están preparadas para BitLocker. De no ser así, Sophos Central Device Encryption ejecuta automáticamente la herramienta de línea de comandos necesaria de Microsoft `BdeHdCfg.exe` para preparar la unidad.

Sistemas compatibles con Device Encryption (página 5)
La tabla siguiente muestra los tipos de protección que se admiten en cada plataforma. El tipo de protección que se aplica depende de la versión de Windows utilizada y de si el hardware de seguridad TPM está disponible.

TPM + PIN (página 7)
El modo TPM + PIN utiliza el hardware de seguridad TPM del ordenador y un PIN como autenticación.

2.4 Sistemas compatibles con Device Encryption

La tabla siguiente muestra los tipos de protección que se admiten en cada plataforma. El tipo de protección que se aplica depende de la versión de Windows utilizada y de si el hardware de seguridad TPM está disponible.

El número entre paréntesis describe la prioridad del tipo de protección concreto.

(*) Cuando la opción **Requerir autenticación de inicio** está activada, no es posible la instalación de la protección Solo TPM y, por ello, TPM + PIN es la primera prioridad.

	Win 7 sin TPM	Win 7 con TPM	Win 8.1 sin TPM	Win 8.1 con TPM	Win 10 sin TPM	Win 10 con TPM
Solo TPM	-	compatible (1*)	-	compatible (1*)	-	compatible (1*)
TPM + PIN	-	compatible (2)	-	compatible (2)	-	compatible (2)

	Win 7 sin TPM	Win 7 con TPM	Win 8.1 sin TPM	Win 8.1 con TPM	Win 10 sin TPM	Win 10 con TPM
Frase de acceso	-	-	compatible (1)	compatible (3)	compatible (1)	compatible (3)
Llave USB	compatible (1)	compatible (3)	-	-	-	-

Es posible que tenga que configurar TPM en la estación de trabajo cuando esté utilizando Central Device Encryption.

Si utiliza TPM 2.0 o posterior, debe formatear el disco duro como GPT y el BIOS debe estar en modo UEFI.

Si utiliza TPM 1.2, debe activar TPM en el BIOS/UEFI y debe estar listo para su uso. Puede comprobarlo mediante `TPM.MSC`.

Le recomendamos que actualice sus equipos a la última versión de BIOS/UEFI antes de instalar Central Device Encryption.

Cuando el modo FIPS de Windows está activado, el cifrado de BitLocker solo es compatible en sistemas con Windows 8.1 o Windows 10. Para obtener información detallada sobre BitLocker en modo FIPS en Windows 7, consulte Una contraseña de recuperación compatible con FIPS no se puede guardar en AD DS para BitLocker en Windows 7 o Windows Server 2008 R2.

Con Sophos Central Device Encryption, puede utilizar discos duros cifrados. Para obtener más información, consulte Unidad de disco duro cifrada.

Central Device Encryption admite BitLocker provisionado previamente.

Información relacionada

Una contraseña de recuperación compatible con FIPS no se puede guardar en AD DS para BitLocker en Windows 7 o Windows Server 2008 R2

Unidad de disco duro cifrada

2.5 Modos de autenticación del cifrado de dispositivos

Puede utilizar el control deslizante **Requerir autenticación de inicio** en la configuración del cifrado de dispositivos para controlar si los usuarios deben autenticarse al iniciar sesión en su equipo.

El modo de autenticación instalado en los equipos depende del sistema, la configuración de directiva de grupo de BitLocker y la directiva de cifrado de dispositivos configurada. En función de la compatibilidad del sistema de cifrado de dispositivos, se instalará uno de los siguientes métodos de autenticación en las estaciones:

- TPM + PIN
- Frase de acceso
- Solo TPM
- Llave USB

En las estaciones que ya están cifradas con BitLocker, un mensaje informará a los usuarios de los pasos necesarios.

Al activar la opción **Requerir autenticación de inicio**, se solicita a los usuarios que definan un PIN / frase de acceso / llave USB y hagan clic en **Aplicar**. Tendrán que usar ese PIN / frase de acceso / llave USB cada vez que inicien el equipo. Al desactivar la opción **Requerir autenticación de inicio**, el modo Solo TPM se aplica de forma automática y no se requiere una autenticación adicional. Se informará a los usuarios de que su equipo desbloqueará el dispositivo automáticamente cuando se inicie.

Sophos Device Encryption puede configurar automáticamente el objeto de directiva de grupo (GPO) de modo que se permitan todos los métodos de autenticación, siempre que la opción de configuración correspondiente esté definida como **no configurado**. Al configurar la opción de configuración de forma manual, el software no sobrescribe estas definiciones. Para más información, consulte Configuración de directiva de grupo de BitLocker.

Los usuarios pueden decidir aplazar la instalación de los modos de autenticación. En tal caso, no se lleva a cabo el cifrado. Cuando un usuario vuelva a iniciar sesión en Windows o cuando el administrador despliegue una nueva directiva de cifrado, el sistema pedirá al usuario que reinicie el equipo. Tras el reinicio, se instala el modo de autenticación y se inicia Device Encryption. A partir de entonces, los usuarios no podrán descifrar sus dispositivos.

Conceptos relacionados

Sistemas compatibles con Device Encryption (página 5)
La tabla siguiente muestra los tipos de protección que se admiten en cada plataforma. El tipo de protección que se aplica depende de la versión de Windows utilizada y de si el hardware de seguridad TPM está disponible.

Configuración de directiva de grupo de BitLocker (página 9)
Sophos Central define automáticamente algunas opciones de configuración de directiva de grupo, de modo que los administradores no tienen que preparar los equipos para el cifrado de dispositivos.

2.5.1 TPM + PIN

El modo TPM + PIN utiliza el hardware de seguridad TPM del ordenador y un PIN como autenticación.

El usuario debe introducir ese PIN en el entorno previo al arranque de Windows cada vez que se inicie el equipo.

TPM + PIN requiere un TPM preparado y la configuración de los GPO del sistema debe permitir el modo TPM + PIN.

Si se cumplen todas las condiciones, se mostrará el cuadro de diálogo de configuración de TPM + PIN y se pedirá al usuario que defina un PIN. El usuario puede hacer clic en **Reiniciar y cifrar** para reiniciar el equipo inmediatamente e iniciar el cifrado.

Si la opción de los GPO **Permitir los PIN mejorados para el inicio** está activada, el PIN puede incluir números, letras y caracteres especiales. De lo contrario, solo se permiten números.

Los PIN para BitLocker tienen una longitud de entre 4 y 20 caracteres. Puede definir una longitud mínima superior mediante una directiva de grupo. El software del agente de Sophos Central define la directiva de grupo para permitir los PIN mejorados. El cuadro de diálogo indica al usuario los caracteres que se pueden introducir y la longitud mínima/máxima que se permite.

Nota
Todos los usuarios de un equipo Windows concreto tienen que usar el mismo PIN para desbloquear el disco del sistema. Después, inician sesión en el sistema operativo con sus credenciales individuales. Los equipos Windows no admiten el inicio de sesión único.

2.5.2 Frase de acceso

Para la autenticación en estaciones de trabajo sin el hardware de seguridad TPM, puede utilizarse una frase de acceso.

El usuario debe introducir esa frase de acceso en el entorno previo al arranque de Windows cada vez que se inicie el equipo.

La protección con frases de acceso requiere Windows 8.0 o posterior y la configuración de los GPO del sistema debe permitir el modo de frase de acceso.

Si se cumplen todas las condiciones, se mostrará el cuadro de diálogo de configuración de frase de acceso y se pedirá al usuario que defina una frase de acceso con una longitud de 8-100 caracteres. El usuario puede hacer clic en **Reiniciar y cifrar** para reiniciar el equipo inmediatamente e iniciar el cifrado.

2.5.3 Solo TPM

El modo Solo TPM utiliza el hardware de seguridad TPM sin autenticación de PIN.

Esto significa que el usuario puede iniciar el equipo sin que se le pida un PIN en el entorno previo al arranque de Windows.

El modo Solo TPM requiere un TPM preparado y que la opción de configuración de directiva **Requerir autenticación de inicio** del cifrado de dispositivos esté desactivada. Además, la configuración de los GPO del sistema deben permitir la protección Solo TPM.

Si se cumplen todas las condiciones, se mostrará el cuadro de diálogo de instalación de la protección Solo TPM. El usuario puede hacer clic en **Reiniciar y cifrar** para reiniciar el equipo inmediatamente e iniciar el cifrado.

2.5.4 Llave USB

El modo Llave USB utiliza una clave almacenada en una memoria USB para la autenticación.

La memoria USB debe conectarse al ordenador en cada inicio.

La protección Llave USB se utiliza en estaciones Windows 7 si no hay ningún TPM disponible o si está desactivado a través de los GPO.

El formato de la memoria USB debe ser NTFS, FAT o FAT32. El formato exFAT no es compatible. Además, la memoria USB debe ser editable.

Si se cumplen todas las condiciones, se mostrará el cuadro de diálogo de instalación de llave USB y se pedirá al usuario que seleccione una memoria USB conectada que se utilizará para almacenar la clave.

El usuario puede hacer clic en **Reiniciar y cifrar** para reiniciar el equipo inmediatamente e iniciar el cifrado.

2.6 Configuración de directiva de grupo de BitLocker

Sophos Central define automáticamente algunas opciones de configuración de directiva de grupo, de modo que los administradores no tienen que preparar los equipos para el cifrado de dispositivos.

Si los administradores ya han establecido las opciones de configuración, los valores configurados no se sobrescribirán.

En el **Editor de directivas de grupo local**, en **Configuración del equipo > Plantillas administrativas > Componentes de Windows > Cifrado de unidad BitLocker > Unidades del sistema operativo**, verá las directivas siguientes:

Directiva	Opción de configuración	Valor establecido por Sophos Central	Comentario
Permitir desbloqueo de la red al iniciar		Activado	Puede permitir que un desbloqueo de red de BitLocker preconfigurado siga operativo después de habilitar Central Device Encryption.
Requerir autenticación adicional al iniciar	Permitir BitLocker sin un TPM compatible	Seleccionado	Esto está configurado para Windows 8 si no hay ningún TPM disponible para permitir el uso de una contraseña al iniciar para desbloquear el disco del sistema.
Requerir autenticación adicional al iniciar	Configurar PIN de inicio del TPM	Permitir PIN de inicio con TPM	Si la opción de configuración de directiva **Requerir autenticación de inicio** de Device Encryption está activada y el sistema tiene un TPM, esta opción de configuración de directiva de grupo permitirá la protección de la unidad del sistema por parte de TPM, además de pedir un PIN al usuario.
Permitir los PIN mejorados para el inicio	n/d	Activado	Esto está configurado para permitir el uso de PIN alfanuméricos para proteger la unidad del sistema con TPM. Si no se puede configurar, solo se permiten dígitos.
Configurar la dirección URL y el mensaje de recuperación previo al arranque	Selecciona una opción para el mensaje de recuperación previo al arranque	Usar la dirección URL y el mensaje de recuperación predeterminado	Se establece para utilizar la URL y el mensaje predeterminado de Sophos.

Directiva	Opción de configuración	Valor establecido por Sophos Central	Comentario
Configurar la dirección URL y el mensaje de recuperación previo al arranque	Opción de mensaje de recuperación personalizado	¿No tiene su clave de recuperación? Póngase en contacto con el servicio de asistencia técnica o visite el portal de autoservicio: `https://sophos.com/ssp`	
Configurar la dirección URL y el mensaje de recuperación previo al arranque	Opción de dirección URL de recuperación personalizada		
Configurar el uso de cifrado basado en hardware para unidades de datos fijas	n/a	Desactivado	Se establece para imponer el cifrado basado en software. Sin embargo, si la configuración de una directiva de grupo de BitLocker existente requiere cifrado basado en hardware, esa configuración de directiva no se anula.
Configurar el uso de cifrado basado en hardware para unidades de sistema operativo	n/a	Desactivado	Se establece para imponer el cifrado basado en software. Sin embargo, si la configuración de una directiva de grupo de BitLocker existente requiere cifrado basado en hardware, esa configuración de directiva no se anula.

- Algoritmo de cifrado que se utiliza: de forma predeterminada, Sophos Central Device Encryption usa AES-256. Existe una opción de configuración de directiva de grupo que puede utilizarse para seleccionar AES-128.
- Requisitos de PIN/contraseña: hay opciones de configuración de directiva de grupo que pueden utilizarse para definir una longitud mínima del PIN o de la contraseña o requerir contraseñas complejas.
- Cifrar todos los datos o solo el espacio utilizado: si la directiva de grupo para volúmenes de arranque y/o volúmenes de datos está configurada para requerir el cifrado completo de datos, anula cualquier directiva de Sophos Central que permita cifrar solo el espacio utilizado.

Algunas opciones de configuración de directiva de grupo pueden entrar en conflicto con Sophos Central, de modo que el cifrado no puede activarse. En tal caso, se envía un evento a Sophos Central.

- Se requiere una tarjeta inteligente: si una directiva de grupo requiere que se utilice una tarjeta inteligente para BitLocker, no es compatible con Sophos Central y se genera un evento de error.
- Cifrar todos los datos o solo el espacio utilizado: si la directiva de grupo para volúmenes de arranque y/o volúmenes de datos está configurada para cifrar solo el espacio utilizado pero la directiva de Sophos Central requiere el cifrado completo, se genera un evento de error.

Si quiere cifrar tabletas (como la MS Surface Pro) y utilizar la autenticación de inicio, debe activar la siguiente configuración de directiva de grupo:

Habilitar el uso de autenticación BitLocker que requiera entrada de teclado de prearranque en pizarras

Para más información, consulte el artículo 125772 de la base de conocimiento.

Para obtener información más general sobre la configuración de directiva de grupo de BitLocker y TPM, consulte Configuración de directiva de grupo de BitLocker y Configuración de directiva de grupo de los servicios del Módulo de plataforma segura.

Conceptos relacionados

Método de cifrado y generación de informes (página 11)
Los volúmenes pueden cifrarse con cifrado basado en software o en hardware.

Información relacionada

Configuración de directiva de grupo de BitLocker
Configuración de directiva de grupo de TPM
Artículo 125772 de la base de conocimiento

2.7 Limitaciones

Discos dinámicos

BitLocker no admite los discos dinámicos. Las estaciones enviarán un evento a Sophos Central para notificarle que se ha producido un error en el cifrado. Esto se da porque no se puede cifrar un volumen de sistema en un disco dinámico. Los volúmenes de datos en discos dinámicos simplemente se omiten.

Remote desktop (escritorio remoto)

Al utilizar una estación Windows mediante Remote Desktop que tenga instalado el software del agente de Sophos Central, no se mostrarán cuadros de diálogo y el cifrado de dispositivos NO se impondrá si se despliega una política de cifrado. Activar el cifrado generaría una secuencia de reinicio para comprobar la compatibilidad del hardware. El usuario debe poder introducir el PIN o frase de acceso en el entorno previo al arranque y esto no se puede realizar mediante Remote Desktop.

2.8 Método de cifrado y generación de informes

Los volúmenes pueden cifrarse con cifrado basado en software o en hardware.

Device Encryption siempre utiliza el cifrado basado en software para nuevos volúmenes, aunque la unidad admita el cifrado basado en hardware.

Si una unidad ya está cifrada con el cifrado basado en hardware, no se cambia.

Si la configuración de una directiva de grupo de BitLocker requiere cifrado basado en hardware, no se cambia.

En la página **Ordenadores**, puede filtrar los equipos según su estado de cifrado, por ejemplo, el método de cifrado o los equipos que no están cifrados.

La página de detalles de un equipo muestra el método de cifrado y el algoritmo utilizados para un volumen.

Para equipos Windows, también puede ver **Cifrado desde**. La información mostrada depende del dispositivo.

- Para los equipos ya cifrados con Sophos Central Device Encryption, muestra la fecha y la hora en que el ordenador se actualizó a la versión 2.1 de Sophos Central Device Encryption.
- Para los equipos cifrados con otro producto de cifrado, muestra la fecha y la hora en que se instaló Sophos Central Device Encryption.
- Para los equipos nuevos cifrados con Sophos Central Encryption 2.1 (o posterior), muestra la fecha y la hora del cifrado.

El informe **Estado de cifrado** muestra el estado de cifrado de los equipos.

Puede ver qué equipos están cifrados, qué tipos de volumen están cifrados y qué equipos cumplen con las políticas de cifrado. También puede averiguar cómo se autentican sus equipos y cómo se cifran.

Conceptos relacionados

Configuración de directiva de grupo de BitLocker (página 9)
Sophos Central define automáticamente algunas opciones de configuración de directiva de grupo, de modo que los administradores no tienen que preparar los equipos para el cifrado de dispositivos.

Ordenadores
Resumen de ordenador

2.9 Acerca del descifrado

Generalmente no es necesario descifrar. Si necesita excluir del cifrado una estación que ya se había cifrado, puede hacerlo eliminando todos sus usuarios de la política y, después, desactivando el cifrado.

En Windows Explorer (en la estación de trabajo), haga clic con el botón derecho en el disco del sistema y seleccione **Administrar BitLocker**. En el cuadro de diálogo **Cifrado de unidad BitLocker**, haga clic en **Desactivar BitLocker**. Solamente puede realizar esta operación un administrador de Windows.

Si hay una directiva de cifrado aplicada y un usuario con privilegios administrativos intenta descifrar su disco duro de forma manual, Sophos Central anula el comando del usuario y el disco permanecerá cifrado.

2.10 Recuperar estaciones de trabajo Windows

Si los usuarios olvidan su contraseña o PIN de BitLocker, pueden recuperar el acceso a sus ordenadores de dos formas.

- Los usuarios pueden ir al portal de autoservicio de Sophos; consulte Recuperar la clave de recuperación a través del portal de autoservicio. Los usuarios de Windows 10 reciben instrucciones en la pantalla **Recuperación de BitLocker**.
- Puede ayudarles a acceder a su equipo. Las instrucciones siguientes le indican lo que verán los usuarios y lo que deben hacer. Deben:

1. Reiniciar el ordenador y pulsar la tecla **Esc** en la pantalla de inicio de sesión de **BitLocker**.
2. En la pantalla **Recuperación de BitLocker**, buscar el **ID de la clave de recuperación**.
3. Ponerse en contacto con el administrador y comunicarle el ID de la clave de recuperación. Usted puede facilitarles la clave de recuperación. Para obtener ayuda sobre cómo recuperar una clave para un usuario, consulte la Ayuda de Sophos Central.
4. El usuario debe introducir la clave de recuperación y, a continuación, seguir las instrucciones en pantalla para crear un nuevo PIN o contraseña.

   En ordenadores que ejecuten Windows 7, los usuarios no verán instrucciones. Tendrán que restablecer su PIN/contraseña manualmente.

Los usuarios podrán acceder a sus ordenadores de nuevo. Normalmente, los volúmenes de datos se desbloquean automáticamente tan pronto como el usuario puede acceder al volumen de arranque. Si no es así, puede obtener una clave de recuperación para el volumen de datos en Sophos Central de la misma manera que para los volúmenes de arranque.

Tareas relacionadas

Recuperar la clave de recuperación a través del portal de autoservicio (página 22)
Si los usuarios no pueden iniciar sesión en su equipo (han olvidado su PIN de BitLocker, su contraseña de macOS, etc.), pueden utilizar el portal de autoservicio de Sophos para recuperar la clave de recuperación.

Información relacionada

Portal de autoservicio

Ayuda de Sophos Central

3 Administrar el cifrado FileVault

Sophos Central Device Encryption para Mac gestiona la funcionalidad del cifrado de disco completo FileVault en equipos Macs.

Los usuarios solo necesitan su contraseña de inicio de sesión de macOS para cifrar y acceder a sus datos.

3.1 Migrar a Sophos Central Device Encryption (Mac)

Si quiere utilizar Sophos Central para administrar equipos Mac que ya estén cifrados con FileVault, les debe aplicar una política de Sophos Central Device Encryption.

Nota
Si utiliza FileVault con SafeGuard Enterprise, primero debe desinstalar el software de **Sophos SafeGuard Device Encryption**.

Antes de que los usuarios puedan empezar:

- Debe instalar el software del agente de Sophos Central en las estaciones de trabajo.
- Debe configurar y activar una política de Device Encryption en Sophos Central.
- Los usuarios deben iniciar sesión en sus estaciones de trabajo. Deben estar conectados y sincronizados con Sophos Central. Tenga en cuenta que no se admite el inicio de sesión remoto.

Estas instrucciones le indican lo que ven los usuarios y lo que deben hacer:

1. Cuando los usuarios inician sesión o cuando aplica una política de Sophos Central Device Encryption mientras los usuarios están conectados, se les informará de que se ha configurado Device Encryption para proteger sus equipos.
2. Para activar Sophos Central Device Encryption, los usuarios deben especificar su contraseña de inicio de sesión y hacer clic en **Crear clave**.
   Una nueva clave de recuperación se crea y almacena a nivel central con fines de recuperación. Si hay otros discos internos sin cifrar, también se cifrarán. No es necesaria otra contraseña de disco para ellos.
3. Si hay discos internos que ya están cifrados con una contraseña de disco, los usuarios deben introducir esta contraseña y hacer clic en **Continuar**.
   Ahora, la contraseña de disco la administra Sophos Central. El disco se desbloquea de forma automática durante el arranque.

Ahora, Sophos Central Device Encryption administra la estación.

3.2 Cifrado de dispositivos paso a paso (Mac)

Siga estos pasos para cifrar equipos Mac.

Antes de que los usuarios puedan empezar:

- Debe instalar el software del agente de Sophos Central en las estaciones de trabajo.

- Debe configurar y activar una política de Device Encryption en Sophos Central.
- Los usuarios deben iniciar sesión en sus estaciones de trabajo. Deben estar conectados y sincronizados con Sophos Central. Tenga en cuenta que no se admite el inicio de sesión remoto.

Estas instrucciones le indican lo que ven los usuarios y lo que deben hacer.

1. Introducir su contraseña de inicio de sesión tras iniciar su Mac.

   Esto activa Sophos Device Encryption.
2. Hacer clic en **Cifrar** para iniciar el cifrado del disco de sistema o en **Posponer** para iniciar el proceso en otro momento.

   Cuando los usuarios introducen su contraseña de inicio de sesión y hacen clic en **Cifrar**, la clave de recuperación se almacena localmente en el llavero y en Sophos Central.

   Todos los usuarios existentes de una estación de trabajo se añaden automáticamente a FileVault.

   En las estaciones de trabajo que ejecutan macOS 10.12 o anterior, cada usuario debe iniciar sesión por separado para añadirse a FileVault.

Cuando el disco del sistema está cifrado, los volúmenes de datos internos se cifran de forma automática. Los discos cifrados se desbloquean automáticamente cuando se inicia el ordenador.

Los usuarios recibirán notificaciones sobre el estado del cifrado en los discos individuales.

3.2.1 Añadir nuevos usuarios de FileVault

Si los usuarios no se añaden a FileVault automáticamente, estas instrucciones le indican lo que ven los nuevos usuarios y lo que deben hacer.

Deben:

1. Introducir su contraseña y hacer clic en **Continuar**.
   Normalmente, los usuarios pueden usar su contraseña de inicio de sesión de macOS para acceder a su equipo Mac y utilizar FileVault.
2. Si todavía no hay ninguna clave de recuperación guardada en Sophos Central, los usuarios nuevos deben seleccionar un usuario de FileVault existente para autorizar esta tarea.
3. A continuación, el usuario de FileVault existente debe introducir su contraseña de inicio de sesión y hacer clic en **Continuar**.

Ahora, los usuarios nuevos pueden usar su contraseña de inicio de sesión de macOS para acceder a su equipo Mac y utilizar FileVault.

3.3 Recuperar estaciones de trabajo Mac

Siga estos pasos para recuperar equipos Mac.

Si los usuarios olvidan su contraseña de inicio de sesión, pueden recuperar el acceso a sus ordenadores de varias formas.

- Si el usuario ha sido la última persona en iniciar sesión en el ordenador, puede utilizar el portal de autoservicio de Sophos. Consulte Recuperar la clave de recuperación a través del portal de autoservicio.
- Los usuarios pueden iniciar su equipo con un disco de inicio Mac externo y después usar comandos en Terminal para desbloquear el disco.

- Los usuarios pueden iniciar su equipo en modo de disco de destino y después usar comandos en Terminal para desbloquear el disco.
- Los usuarios pueden iniciar su equipo con Recuperación de macOS y después usar comandos en Terminal para desbloquear el disco.

  Para obtener información sobre cómo trabajar con comandos en Terminal, consulte Desbloquear volúmenes HFS+ con comandos en Terminal y Desbloquear volúmenes APFS con comandos en Terminal.

Puede ayudar a los usuarios a recuperar el acceso. Las instrucciones siguientes le indican lo que verán los usuarios y lo que deben hacer. Deben:

1. Encender la estación de trabajo y esperar hasta que aparezca el **ID de la clave de recuperación**. El ID de la clave de recuperación se mostrará solamente durante unos minutos. Para volverlo a visualizar, los usuarios deben reiniciar el equipo.
2. Ponerse en contacto con el administrador y comunicarle el ID de la clave de recuperación. Usted puede facilitarles la clave de recuperación. Para obtener ayuda sobre cómo recuperar una clave para un usuario, consulte la Ayuda de Sophos Central.
3. Hacer clic en el icono de signo de interrogación en el campo **Contraseña**. Se mostrará un mensaje.
4. Hacer clic en el icono de flecha junto al mensaje para cambiar al campo de la clave de recuperación.
5. Introducir la clave de recuperación.

   Para los usuarios importados de Active Directory, es necesario realizar los siguientes pasos adicionales:

   - Restablezca la contraseña existente en Active Directory. A continuación, genere una contraseña preliminar y désela al usuario.
   - Indique al usuario que haga clic en **Cancelar** en el cuadro de diálogo **Restablecer contraseña** e introduzca la contraseña preliminar en su lugar.
6. Siga las instrucciones en pantalla para crear una contraseña nueva.
7. Si se les solicita, hacer clic en **Crear un nuevo llavero**.

Los usuarios podrán acceder de nuevo al volumen de arranque de su equipo.

En las estaciones de trabajo que ejecutan macOS 10.12 o anterior, se creará una nueva clave de recuperación y se almacenará en Sophos Central. Una clave de recuperación solo puede usarse una vez. Si necesita volver a recuperar un ordenador más adelante, debe obtener una nueva clave de recuperación.

En las estaciones de trabajo que ejecutan macOS 10.13 y Apple File System (APFS), no se crea ninguna clave de recuperación nueva. La clave de recuperación existente sigue siendo válida.

Tareas relacionadas

Recuperar la clave de recuperación a través del portal de autoservicio (página 22)
Si los usuarios no pueden iniciar sesión en su equipo (han olvidado su PIN de BitLocker, su contraseña de macOS, etc.), pueden utilizar el portal de autoservicio de Sophos para recuperar la clave de recuperación.

Desbloquear volúmenes HFS+ con comandos en Terminal (página 17)
Puede utilizar comandos de Terminal para desbloquear volúmenes cifrados. Los comandos de esta sección se aplican en estaciones de trabajo que ejecutan macOS 10.12 o anterior con volúmenes formateados con HFS+.

Desbloquear volúmenes APFS con comandos en Terminal (página 17)
Puede utilizar comandos de Terminal para desbloquear volúmenes cifrados. Los comandos de esta sección se aplican en estaciones de trabajo que ejecutan macOS 10.13 y Apple File System (APFS).

Información relacionada

Recuperación de macOS

Cómo seleccionar un disco de inicio diferente

Ayuda de Sophos Central

3.3.1 Desbloquear volúmenes HFS+ con comandos en Terminal

Puede utilizar comandos de Terminal para desbloquear volúmenes cifrados. Los comandos de esta sección se aplican en estaciones de trabajo que ejecutan macOS 10.12 o anterior con volúmenes formateados con HFS+.

Las instrucciones siguientes le indican lo que verán los usuarios y lo que deben hacer. Deben:

1. Abrir la aplicación **Terminal** y ejecutar `diskutil corestorage list`.
   Aparecerá una lista con todos los volúmenes conectados.
2. Buscar el nombre del volumen (`LV Name`) que quieran recuperar y tomar nota de la identificación del `Logical Volume`.
3. Ponerse en contacto con el administrador y pedirle la clave de recuperación usando la identificación del `Logical Volume` como ID de la clave de recuperación.
   Usted les facilita la clave de recuperación. Para obtener ayuda sobre cómo recuperar una clave para un usuario, consulte la Ayuda de Sophos Central.
4. Introducir la clave de recuperación en el cuadro de diálogo de la contraseña de disco para desbloquear el disco.
   Otra opción es que los usuarios utilicen el comando `diskutil corestorage unlockVolume` y especifiquen la clave de recuperación en la aplicación **Terminal** para desbloquear el disco.

Ahora se puede acceder al disco en Finder.

Información relacionada

Ayuda de Sophos Central

3.3.2 Desbloquear volúmenes APFS con comandos en Terminal

Puede utilizar comandos de Terminal para desbloquear volúmenes cifrados. Los comandos de esta sección se aplican en estaciones de trabajo que ejecutan macOS 10.13 y Apple File System (APFS).

Las instrucciones siguientes le indican lo que verán los usuarios y lo que deben hacer. Deben:

1. Abrir la aplicación **Terminal** y ejecutar `diskutil apfs list`.
   Aparecerá una lista con todos los volúmenes conectados.
2. Buscar el nombre del volumen que quieran recuperar y tomar nota de la identificación del volumen, por ejemplo, `Volume disk1s1`.
3. Ponerse en contacto con el administrador y pedirle la clave de recuperación usando la identificación del volumen como ID de la clave de recuperación.
   Usted les facilita la clave de recuperación. Para obtener ayuda sobre cómo recuperar una clave para un usuario, consulte la Ayuda de Sophos Central.
4. Introducir la clave de recuperación en el cuadro de diálogo de la contraseña de disco para desbloquear el sistema.
   Otra opción es que los usuarios utilicen el comando `diskutil apfs unlockVolume` y especifiquen la clave de recuperación en la aplicación **Terminal** para desbloquear el disco.

Ahora se puede acceder al disco en Finder.

Información relacionada
Ayuda de Sophos Central

3.3.3 Error: No se ha podido almacenar la clave de recuperación

En raras ocasiones, es posible que el sistema no pueda almacenar la clave de recuperación a nivel local (en el llavero) o en Sophos Central.

Esto quiere decir que el equipo no es recuperable si los usuarios olvidan su contraseña. Para mitigar este riesgo, se muestra un mensaje de error con la clave de recuperación y se solicita al usuario que haga una copia de la clave.

El sistema intentará almacenar la clave de recuperación en Sophos Central repetidas veces. Tan pronto como lo consiga, se notificará a los usuarios de que Sophos Central administra una nueva clave de recuperación y de que pueden destruir la copia de la clave de recuperación.

3.4 Estado del cifrado de dispositivos (Mac)

Los usuarios pueden acceder a información sobre el estado del cifrado mediante la aplicación **Sophos Device Encryption**. Está instalada en el directorio `Applications` y puede iniciarse a través del Finder, Launchpad o Spotlight.

La aplicación **Sophos Device Encryption** proporciona la información siguiente:

- Estado de la política: La primera línea indica a los usuarios si su estación está gestionada por Sophos Device Encryption o no.
- Estado del usuario: La segunda línea indica a los usuarios lo que pueden hacer y lo que no.
- Estado del disco: Aparece una lista con todos los discos internos. Si el nombre del disco es de color gris, el disco no está montado. Un icono junto al nombre del disco indica su estado. Existen los estados siguientes:
  - Verde: El disco está totalmente cifrado y la clave de recuperación está almacenada de forma centralizada.
  - Amarillo: El disco está totalmente cifrado pero la clave de recuperación no está almacenada en Sophos Central. Esto puede ocurrir cuando no se puede acceder a Sophos Central. Si no se requiere el cifrado del disco, es posible que ni siquiera exista la clave de recuperación. Generalmente, esto suele ocurrir cuando el disco no lo administra Sophos Central Device Encryption y ha sido cifrado con herramientas del sistema operativo.
  - Amarillo + signo de exclamación: El disco está totalmente cifrado, existe una política que requiere que el disco esté cifrado pero no hay ninguna clave de recuperación.
  - Rojo: El disco no está cifrado pero hay activa una política que requiere que el disco esté cifrado.
  - Gris: El disco no está cifrado y la política no requiere cifrado o no existe ninguna política.
  - Barra de estado + **Cifrando**: El disco se está cifrando en este momento.
  - Barra de estado + **Descifrando**: El disco se está descifrando en este momento.

Nota
Si un usuario con privilegios administrativos en un equipo Mac intenta descifrar su disco duro de forma manual mientras se aplique una política de cifrado, Sophos Central no puede anular el comando del usuario y el disco se descifrará. Cuando ha finalizado el descifrado, se pide al usuario su contraseña para activar FileVault y el disco se cifrará de nuevo.

- Estado de recuperación: En la parte inferior de la ventana, se informa a los usuarios si las claves de recuperación están disponibles para sus discos.

También se puede acceder a información sobre el estado del cifrado de dispositivos mediante la herramienta de línea de comandos. La herramienta está instalada en `/usr/local/bin/seadmin`. Existen los comandos siguientes:

- `help`: Muestra una lista de comandos disponibles.
- `status`: Muestra la última sincronización del software de cifrado y el intervalo de sincronización.
- `--device-encryption`: Muestra la política de cifrado actual y el cifrado y el estado de recuperación de todos los discos internos.

4 Proteger archivos con contraseña para compartirlos de forma segura

Puede activar esta opción en una directiva de **cifrado de dispositivos**.

Nota
La función solo está disponible en Central Device Encryption 2.0 o posterior. Esta opción solo está disponible para Windows.

Puede proteger archivos de hasta 50 MB.

Activar menú contextual con clic derecho: Si activa esta opción, se añade una opción **Crear archivo protegido con contraseña** al menú contextual. Los usuarios pueden adjuntar archivos protegidos con contraseña a los correos electrónicos cuando envían datos confidenciales a destinatarios de fuera de su red corporativa. Los archivos se envuelven en un nuevo archivo HTML con contenido cifrado.

Los destinatarios pueden abrir el archivo haciendo doble clic en él e introduciendo la contraseña. Pueden enviar de vuelta el archivo recibido y protegerlo con la misma contraseña o con una nueva, o pueden crear un nuevo archivo protegido con contraseña.

Activar complemento de Outlook: Esta opción añade cifrado de archivos adjuntos de correo electrónico a Outlook. Los usuarios pueden proteger los archivos adjuntos seleccionando **Proteger archivos adjuntos** en la cinta de Outlook. Todos los archivos adjuntos desprotegidos se envuelven en un nuevo adjunto HTML con contenido cifrado y se envía el correo electrónico.

Preguntar siempre qué hacer con los archivos adjuntos: Si activa esta opción, los usuarios deben elegir cómo enviar archivos adjuntos siempre que el mensaje contenga uno. Pueden enviarlos protegidos con contraseña o sin proteger.

Puede introducir dominios excluidos para los que la opción **Preguntar siempre qué hacer con los archivos adjuntos** no se aplicará, por ejemplo, el dominio de su empresa. Si los destinatarios pertenecen a un dominio de este tipo, no se pregunta a los remitentes cómo quieren gestionar los archivos adjuntos.

Introduzca solo los nombres de dominio completos y sepárelos por comas.

Información relacionada
Política de cifrado de dispositivos

5 Solicitar a los usuarios que cambien su contraseña/PIN

Hay dos formas de pedir a los usuarios que cambien su contraseña.

Nota
Esta opción solo está disponible para Windows.

- Utilice la opción **Requerir contraseña/PIN de autenticación nuevo a los usuarios** de la directiva de cifrado.

  Esta opción está desactivada por defecto. Obliga a cambiar la contraseña o el PIN de BitLocker tras un tiempo especificado. Un evento se registra cuando los usuarios cambian su contraseña o PIN.

  Nota
  La función solo está disponible en Central Device Encryption 2.0 o posterior.

- Utilice la opción **Activar cambio de contraseña/PIN** de la ficha **Resumen** de la página de detalles de un equipo.

  Esta opción requiere que los usuarios cambien inmediatamente su contraseña o PIN de BitLocker. Se visualiza un mensaje cuando la solicitud se ha enviado correctamente.

En la estación de trabajo, el sistema pide a los usuarios que establezcan una nueva contraseña o PIN de BitLocker. Si los usuarios cierran el cuadro de diálogo sin introducir una nueva contraseña o PIN, el cuadro de diálogo se vuelve a mostrar al cabo de 30 segundos. El cuadro de diálogo deja de mostrarse cuando introducen uno. Después de que los usuarios hayan cerrado el cuadro de diálogo cinco veces sin cambiar la contraseña o el PIN, se registra una alerta.

Información relacionada
Política de cifrado de dispositivos
Resumen de ordenador

6 Recuperar la clave de recuperación a través del portal de autoservicio

Si los usuarios no pueden iniciar sesión en su equipo (han olvidado su PIN de BitLocker, su contraseña de macOS, etc.), pueden utilizar el portal de autoservicio de Sophos para recuperar la clave de recuperación.

Con la clave de recuperación, pueden volver a obtener acceso a su ordenador.

Para permitir que los usuarios recuperen el acceso a sus equipos en el portal de autoservicio, vaya a **Sophos Central > Personas > Usuarios**, seleccione uno o varios usuarios y haga clic en el botón **Enlace de configuración de correo electrónico**. En el siguiente cuadro de diálogo, seleccione **Correo electrónico de bienvenida/configuración de Sophos Central Self Service** para enviar un enlace de activación a los usuarios. Cuando los usuarios sigan las instrucciones del correo, pueden utilizar el portal de autoservicio de Sophos para recuperar el acceso a su equipo.

Las instrucciones siguientes le indican lo que verán los usuarios y lo que deben hacer. Deben:

1. Iniciar sesión en el portal de autoservicio de Sophos utilizando otro equipo.
2. Ir a la página **Device Encryption**.
   Se muestra una lista de todos los equipos en los que el usuario fue la última persona en iniciar sesión. Si mientras tanto otra persona ha iniciado sesión en un equipo, el usuario no podrá recuperar el acceso a ese equipo a través del portal de autoservicio.
3. Seleccionar un equipo de la lista y hacer clic en el botón **Recuperar** en la columna **CLAVE DE RECUPERACIÓN**.
   Se abrirá un cuadro de diálogo con la clave de recuperación.
4. Iniciar su equipo y dirigirse a la página de recuperación.
   - Windows: Pulse la tecla **Esc** para cambiar a la pantalla **Recuperación de BitLocker**.
   - Mac: Hacer clic en el icono de signo de interrogación en el campo **Contraseña** para cambiar a la página de recuperación de FileVault.
5. Introducir la clave de recuperación.

Los usuarios podrán acceder a sus ordenadores de nuevo.

Información relacionada

Portal de autoservicio

7 Más información

Windows

- Preguntas frecuentes: artículo 124819 de la base de conocimiento
- Preguntas frecuentes sobre BitLocker
- Configuración de directiva de grupo de BitLocker
- Aspectos básicos sobre TPM
- Configuración de directiva de grupo de TPM
- Descripción técnica de administración de módulos de plataforma segura (TPM)

Mac

- Preguntas frecuentes: artículo 125982 de la base de conocimiento
- Configuración de FileVault: Utilizar FileVault para cifrar el disco de arranque del Mac
- Claves de recuperación de FileVault: Establecer una clave de recuperación de FileVault para los ordenadores de su institución
- Restablecimiento de contraseña: Cambiar o restablecer la contraseña de una cuenta de usuario de macOS

Información relacionada

Preguntas frecuentes sobre BitLocker
Configuración de directiva de grupo de BitLocker
Configuración de directiva de grupo de TPM
Aspectos básicos sobre TPM
Descripción técnica de administración de módulos de plataforma segura (TPM)
Utilizar FileVault para cifrar el disco de arranque del Mac
Establecer una clave de recuperación de FileVault para los ordenadores de su institución
Cambiar o restablecer la contraseña de una cuenta de usuario de macOS
Artículo 124819 de la base de conocimiento
Artículo 125982 de la base de conocimiento

8 Navegadores de Internet compatibles

Actualmente, son compatibles los siguientes navegadores:

- Microsoft Internet Explorer 11 y Microsoft Edge.
- Google Chrome.
- Mozilla Firefox.
- Apple Safari (sólo Mac).

Le recomendamos que instale o se actualice a una versión compatible de las que aparecen en la lista anterior y que utilice siempre una versión actualizada. Nuestro objetivo es ofrecer compatibilidad para la última versión y la versión anterior de Google Chrome, Mozilla Firefox y Apple Safari. Si se detecta un navegador no compatible, se le redirigirá a https://central.sophos.com/unsupported.

Nota
Sophos Central Admin no es compatible con los dispositivos móviles.

9 Obtener más ayuda

Para obtener ayuda del soporte técnico de Sophos:

1. Haga clic en **Ayuda** en la parte superior derecha de la interfaz de usuario y seleccione **Crear solicitud de soporte**.
2. Complete el formulario. Sea lo más preciso posible para que el soporte técnico pueda ayudarle de forma efectiva.
3. Si lo prefiere, seleccione la opción para permitir que el soporte técnico acceda directamente a su sesión de Sophos Central para poder prestarle una ayuda mejor.
4. Haga clic en **Enviar**.

Sophos se pondrá en contacto con usted dentro de las 24 horas siguientes.

Nota
Si ha seleccionado la opción para permitir que el soporte técnico acceda a su sesión de Sophos Central, esta función se activa al hacer clic en **Enviar**. La asistencia remota se desactivará automáticamente después de 72 horas. Para desactivarla antes, haga clic en el nombre de su cuenta (parte superior derecha de la interfaz de usuario), seleccione **Datos de la cuenta** y haga clic en la ficha **Soporte de Sophos**.

Enviar comentarios

Para enviar comentarios o sugerencias al soporte técnico de Sophos:

1. Haga clic en **Ayuda** en la parte superior derecha de la interfaz de usuario y seleccione **Dar opinión**.
2. Complete el formulario.
3. Haga clic en **Enviar**.

Ayuda adicional

También puede encontrar soporte técnico en los siguientes recursos:

- 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.

10 Aviso legal