SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

Ayuda (Android)

Versión del producto: 9.6

Contenido

Accesibilidad....1
Acerca de Sophos Intercept X for Mobile....2
Panel de control....3
Seguridad de dispositivos....4
    Asesor de actualizaciones....4
Filtrado web....5
Comprobador de enlaces....7
Seguridad Wi-Fi....8
Seguridad de apps....10
Authenticator....11
    Acerca de las contraseñas de un solo uso....11
    Añadir una cuenta a partir de un código QR....12
    Añadir una cuenta manualmente....12
Cofre de contraseñas....14
    Crear una entrada en el Cofre de contraseñas....14
    Generar contraseñas....15
    Usar datos de contraseña para iniciar sesión....15
    Administrar entradas del cofre de contraseñas....15
    Buscar entradas en el cofre de contraseñas....16
    Realizar copia de seguridad de Cofre de contraseñas....16
Escáner de códigos QR....17
Protección de apps....18
Gestor de privacidad....19
Gestor de privacidad (Android 5)....21
Gestión corporativa....22
    Resolver infracciones de cumplimiento....22
    Obtener asistencia....22
Configuración....24
Crear una copia de seguridad y restaurar....26
Registro....27
Aviso legal....28

1 Accesibilidad

Sophos Intercept X for Mobile cumple con las Directrices de accesibilidad para el contenido web (WCAG) 2.1 Nivel AA. Puede encontrar más información sobre estas directrices en la información relacionada.

Le recomendamos utilizar Sophos Intercept X for Mobile con TalkBack, el lector de pantalla de Google incluido en los dispositivos Android. Puede encontrar un enlace para utilizar TalkBack en la información relacionada. Si necesita más ayuda con TalkBack, puede ponerse en contacto con el servicio de asistencia técnica de Google.

Si desea utilizar productos de tecnología de asistencia con nuestro software, le recomendamos que esté familiarizado con el funcionamiento del producto elegido y los comandos de teclado disponibles.

Limitación conocida

Debido a una limitación del sistema operativo Android, los usuarios de lectores de pantalla solo pueden utilizar encabezados para navegar si tienen Android 9 o posterior.

Información relacionada

Directrices de accesibilidad para el contenido web

Ayuda de accesibilidad de Android: Empezar a utilizar TalkBack en Android

Copyright © Sophos Limited

2 Acerca de Sophos Intercept X for Mobile

Sophos Intercept X for Mobile protege su dispositivo Android y su privacidad sin que esto afecte al rendimiento ni a la duración de la batería. Con la información actualizada al minuto de SophosLabs, las apps se escanean automáticamente en busca de malware mientras se instalan, a fin de protegerle de fugas de datos y costes inesperados.

Copyright © Sophos Limited

3 Panel de control

El panel de control de Sophos Intercept X for Mobile le ofrece una visión general del estado de seguridad del dispositivo.

Las funciones tienen colores diferentes en función de su estado:

- Verde: No se han detectado problemas
- Rojo: Se han encontrado problemas
- Azul: Función activada
- Gris: La función está desactivada o no está configurada

Copyright © Sophos Limited

4 Seguridad de dispositivos

Al igual que todos los sistemas operativos, Android le permite configurar opciones que hacen que el dispositivo sea menos seguro. Sophos Intercept X for Mobile comprueba estas opciones relacionadas con la seguridad y ofrece recomendaciones para que el dispositivo sea más seguro.

Nota
Cuando Sophos Mobile administra Sophos Intercept X for Mobile, las opciones del sistema relacionadas con la seguridad las configura su empresa.

Las opciones que aparecen en **Seguridad de dispositivos** tienen colores diferentes en función de su estado:

- Verde (Seguro): La opción garantiza la máxima seguridad posible del dispositivo.
- Rojo (No seguro): La opción puede provocar problemas de seguridad. Siga las recomendaciones para cambiarla.
- Amarillo (Desconocido): Los dispositivos Android tienen opciones de configuración diferentes en función del modelo de dispositivo y de la versión de Android. Si Sophos Intercept X for Mobile no se puede determinar si la opción no es segura, aparece de color amarillo. Considere la posibilidad de cambiarla.
- Gris (Desactivado): La comprobación está desactivada. La opción no se tiene en cuenta a la hora de determinar el estado de seguridad del dispositivo.

Toque una opción para cambiarla o para obtener más información sobre cómo afecta a la seguridad del dispositivo.

4.1 Asesor de actualizaciones

El Asesor de actualizaciones muestra información sobre su versión de Android y comprueba si hay disponibles versiones más recientes.

El Asesor de actualizaciones utiliza las estadísticas de instalación de Sophos para averiguar si hay una versión más reciente de Android disponible para su dispositivo.

Para abrir el Asesor de actualizaciones, seleccione **Última versión de Android** en la página **Seguridad de dispositivos**.

Le recomendamos que instale las actualizaciones automáticamente. Si el dispositivo tiene una opción de configuración opcional para ello, toque **Comprobar configuración** y active las actualizaciones automáticas en la app **Configuración** del dispositivo.

Copyright © Sophos Limited

5 Filtrado web

El Filtrado web se utiliza para especificar tipos de sitios web sobre los que desea recibir advertencias antes de abrirlos. Esto le protege contra la navegación en sitios con contenido malicioso, no deseado o ilegal.

Configurar el Filtrado web

En el panel de control, el filtrado web está disponible en **Seguridad de red**.

- En la página **Filtrado web**, actívelo.
- Para activar el filtrado de sitios web maliciosos, toque **Contenido malicioso** y seleccione **Avisar** o **Bloquear**.
- Para activar el filtrado de sitios web de una determinada categoría, toque en categoría y seleccione **Avisar** o **Bloquear**.
- **Lista de permisos:** Puede anular de forma permanente el aviso para determinadas páginas maliciosas o páginas que estén englobadas dentro de una categoría. Esto resulta útil cuando una de las páginas que visita frecuentemente está englobada dentro de una de las categorías que activan una advertencia o que están bloqueadas. Seleccione **Permitir siempre acceder a esta página** en el cuadro de diálogo de aviso **Filtrado web**. Para filtrar estas páginas de nuevo, toque en **Vaciar lista de páginas permitidas**.

Sugerencia
Para probar el filtrado de sitios web, Sophos ha creado el sitio sophostest.com con páginas de ejemplo para cada categoría. Aunque algunas de estas páginas están clasificadas como potencialmente ofensivas o peligrosas, el contenido en sí de la página es inocuo en todos los casos.

Navegadores de Internet compatibles

El filtrado web le protege cuando utiliza una de las apps que aparecen en **Navegadores protegidos**.

Navegadores compatibles:

- Google Chrome
- Firefox
- Navegador web de Android
- Microsoft Edge

En **Navegadores protegidos (no probados)**, se indican las apps que pueden funcionar pero que no se han probado.

Copyright © Sophos Limited

Sugerencia
Si un navegador web compatible está instalado en el dispositivo pero no aparece en la lista de **Navegadores protegidos**, compruebe que Sophos Accessibility Service esté activado (en la configuración del sistema en **Accesibilidad**).

Copyright © Sophos Limited

6 Comprobador de enlaces

El Comprobador de enlaces se utiliza para revisar los enlaces de un correo electrónico o un documento a fin de detectar contenido malicioso o inadecuado.

El Comprobador de enlaces procesa todos los enlaces que toca en apps distintas de los navegadores. El Filtrado web se utiliza para comprobar los enlaces de las páginas web. Consulte Filtrado web (página 5).

En el panel de control, el Comprobador de enlaces está disponible en **Seguridad de red**.

Para configurar el Comprobador de enlaces:

1. En la página **Comprobador de enlaces**, actívelo.
2. Seleccione la app de navegador normal para abrir enlaces web.
3. La primera vez que toque un enlace después de activar el Comprobador de enlaces, Android le pedirá que seleccione una app para abrir el enlace. Seleccione **Comprobador de enlaces de Sophos**.

Al tocar un enlace, se envía al Comprobador de enlaces para determinar si incluye contenido malicioso o inadecuado en función de la clasificación proporcionada por SophosLabs. Posteriormente, el enlace se abre en el navegador.

Nota

El Comprobador de enlaces no puede revisar enlaces en aquellas apps que los abren internamente en lugar de enviarlos a la app de navegador. Si la app le permite elegir cómo abrir los enlaces web, utilice el navegador para que el Comprobador de enlaces pueda procesarlos.

En Gmail, por ejemplo, la opción se llama **Abrir enlaces web en Gmail**. Desactive esta opción para que el Comprobador de enlaces revise los enlaces de sus mensajes de correo electrónico.

Copyright © Sophos Limited

7 Seguridad Wi-Fi

Seguridad Wi-Fi se utiliza para revisar su conexión Wi-Fi a fin de detectar amenazas basadas en red.

Nota
Si Sophos Intercept X for Mobile está inscrito en Sophos Mobile, esta función la administra la empresa.

En el panel de control, la seguridad Wi-Fi está disponible en **Seguridad de red**.

Tipos de problemas

Sophos Intercept X for Mobile detecta los siguientes problemas:

Suplantación ARP	La suplantación ARP consiste en que un atacante envía mensajes ARP (Protocolo de resolución de direcciones) maliciosos a su ordenador de forma que parece que la dirección MAC del atacante está asociada a la dirección IP de su puerta de enlace de red. Esto le permite acceder a la red privada del usuario, robar datos confidenciales y lanzar ataques adicionales como ataques de denegación de servicio o de tipo «Man in the middle».
Portal cautivo	Un portal cautivo es una forma que tienen las redes Wi-Fi públicas de solicitar autenticación antes de otorgar acceso a la red. Dado que todo el tráfico se redirecciona al portal cautivo, es posible que reciba avisos adicionales.
Manipulación de contenido	La manipulación de contenido consiste en que un atacante manipula el contenido de un sitio web para forzarle a realizar acciones dañinas. Esto le permite hacer cosas como omitir la autenticación o borrar datos.
Interceptación de SSL	La interceptación de SSL es cuando un atacante utiliza un certificado de servidor falso para interceptar la conexión segura entre el equipo del usuario y un sitio web. El atacante puede descifrar datos sensibles mientras hace creer al usuario que la conexión sigue siendo segura.
Decapado de SSL	El decapado de SSL es cuando un atacante degrada la conexión a un sitio web de HTTPS seguro a HTTP no seguro. El atacante puede redireccionar todo el tráfico entre el equipo del usuario y el sitio web a través de su propio servidor proxy. Esto le permite descifrar datos confidenciales mientras le hace creer que sigue conectado mediante HTTPS.

Copyright © Sophos Limited

Ejecutar comprobaciones

- Para comprobar la red Wi-Fi a la que está conectado, toque **Comprobar Wi-Fi**.
- Para realizar comprobaciones de red automáticamente en segundo plano, active **Comprobación en segundo plano**. Esta opción ejecuta una comprobación cada vez que el dispositivo se conecta a una red Wi-Fi.

Copyright © Sophos Limited

8 Seguridad de apps

Puede buscar apps o archivos maliciosos en su dispositivo.

Sophos Intercept X for Mobile escanea el dispositivo en busca de malware e informa acerca de cualquier app potencialmente no deseada o maliciosa que encuentra. El escáner emplea un servicio online para comprobar las apps utilizando los datos de amenazas más recientes en la base de datos de SophosLabs en la nube, así como un completo motor de escaneado integrado para una mejor detección tanto si el dispositivo está online como si se encuentra sin conexión. Los datos antivirus se actualizan permanentemente por SophosLabs, que analiza amenazas Android las 24 horas del día.

Realizar escaneados

Sophos Intercept X for Mobile escanea las apps cuando se instalan. Además, puede configurar escaneados programados y ejecutar escaneados manuales.

Para configurar escaneados programados:

En la configuración de la app, seleccione **Escaneados programados** y, a continuación, seleccione un intervalo de escaneado en **Intervalo de escaneado programado**. También puede configurar qué partes del dispositivo se escanean y qué tipos de apps se notifican.

Para ejecutar un escaneado manual:

En la página **Seguridad de apps**, seleccione **Mostrar detalles del escaneado** y, a continuación, **Iniciar**.

Ver los resultados de escaneado

En la página **Seguridad de apps**, se muestra un resumen de los resultados del escaneado en **Problemas de seguridad de apps**.

Para ver los problemas individuales, seleccione **Mostrar detalles del escaneado**.

Para ver todavía más detalles sobre un problema, seleccione una app que aparezca en **Amenazas y apps no deseadas** para abrir su página **Datos del objeto**. En esa página, puede hacer lo siguiente:

- Ver cómo se instaló la app y los permisos que solicitó.
- Ver la descripción de una amenaza.
- Abrir una página web con información detallada sobre amenazas en el navegador.
- Desinstalar la app.
- Permitir la app.

Referencia relacionada

Configuración (página 24)

Copyright © Sophos Limited

9 Authenticator

Authenticator se utiliza para generar contraseñas de un solo uso (o códigos de verificación) para iniciar sesión en sus cuentas que utilizan la autenticación multifactor.

Consulte a su proveedor de cuenta si se admite la autenticación multifactor y cómo habilitarla para su cuenta.

Authenticator admite contraseñas de un solo uso **basadas en tiempo** y **basadas en contador**. Consulte Acerca de las contraseñas de un solo uso (página 11).

Para iniciar Authenticator, mantenga pulsado el icono de Sophos y, a continuación, toque **Authenticator**.

Funciones:

- Para las contraseñas **basadas en tiempo,** Authenticator muestra la contraseña de un solo uso válida en ese momento junto con un icono animado que ilustra el tiempo que queda para que el código caduque y se calcule el siguiente código.
- Para las contraseñas **basadas en contador**, toque **Actualizar** junto al elemento de cuenta para generar una nueva contraseña de un solo uso. Para impedir que pueda generar varios códigos seguidos de forma accidental, se aplica una latencia de varios segundos después de crearse un código hasta que pueda generarse el siguiente.
- Para copiar la contraseña de un solo uso actual para una cuenta en el portapapeles, mantenga pulsado el elemento de cuenta y luego toque **Copiar**.
- Para editar los detalles de la cuenta, mantenga pulsado el elemento de cuenta y luego toque **Editar**. Por motivos de seguridad, no se puede mostrar ni editar la clave secreta.
- Para eliminar una cuenta, mantenga pulsado el elemento de cuenta y luego toque **Eliminar**.

Aviso
Al eliminar una entrada de Authenticator, perderá la capacidad de generar contraseñas de un solo uso para esa cuenta. Esto no desactiva la autenticación multifactor. Si elimina la entrada de Authenticator, es posible que no pueda iniciar sesión en su cuenta.

Antes de eliminar la entrada, asegúrese de que dispone de un mecanismo alternativo para generar contraseñas de un solo uso, o bien un mecanismo alternativo para iniciar sesión en su cuenta sin la autenticación multifactor.

9.1 Acerca de las contraseñas de un solo uso

Las contraseñas de un solo uso (también llamadas códigos de verificación) están formadas por una serie de dígitos. Se calculan a partir de estos parámetros:

- Una clave secreta compartida que solo su proveedor de cuenta y usted conocen.
- Los valores de configuración específicos de su proveedor de cuenta.
- Un contador consecutivo.

Al utilizar una contraseña de un solo uso para autenticarse, su proveedor de cuenta espera una contraseña que se calcula a partir de un determinado valor del contador. Como Authenticator utiliza

Copyright © Sophos Limited

las mismas reglas que su proveedor de cuenta para determinar el valor del contador actual, el proveedor aceptará su contraseña de un solo uso.

Authenticator admite contraseñas de un solo uso **basadas en tiempo** y **basadas en contador**. Estos tipos se diferencian por la forma en que se determina el valor del contador actual:

- **Contraseñas de un solo uso basadas en tiempo** (TOTP, según RFC 6238): El valor del contador se incrementa de forma continua en función de la hora actual. El siguiente valor de la serie de códigos de verificación se genera cuando ha transcurrido un período de tiempo definido.
- **Contraseñas de un solo uso basadas en contador** (HOTP, según RFC 4226): El valor del contador se incrementa a demanda. El siguiente valor de la serie de códigos de verificación se genera cuando usted lo solicita.

9.2 Añadir una cuenta a partir de un código QR

Utilice este procedimiento si ha habilitado la autenticación multifactor para una cuenta y su proveedor de cuenta le ha proporcionado un código QR con los datos de configuración.

1. Toque **+** y luego **Escanear código QR**.
2. Escanee el código QR con el dispositivo.

Una vez que la app haya leído los detalles de configuración del código QR, creará una nueva cuenta de Authenticator.

9.3 Añadir una cuenta manualmente

Utilice este procedimiento si ha habilitado la autenticación multifactor para una cuenta y su proveedor de cuenta le ha proporcionado una lista con los datos de configuración.

1. Toque **+** y luego **Añadir manualmente**.
2. En el campo **Nombre**, escriba un nombre para la nueva cuenta de Authenticator.
3. En el campo **Clave**, escriba la clave secreta que le haya indicado su proveedor de cuenta. La clave es específica de su cuenta y constituye la base de cálculo para las contraseñas de un solo uso.
4. En el campo **Tipo**, seleccione el tipo de cálculo que le haya indicado su proveedor de cuenta.
5. Si su proveedor de cuenta ha especificado otros datos de configuración, toque **Avanzadas** para mostrar campos de entrada adicionales.

Atención
Rellene únicamente la información que le haya indicado su proveedor de cuenta.

- En el campo **Emisor**, introduzca una cadena que especifique el proveedor al que está asociada la cuenta.
- En el campo **Período de tiempo**, introduzca el período de validez en segundos. Solo está disponible para las contraseñas de un solo uso basadas en tiempo.
- En el campo **Contador**, introduzca el valor inicial del contador. Solo está disponible para las contraseñas de un solo uso basadas en contador.
- En el campo **Longitud de código**, seleccione el número de dígitos de las contraseñas de un solo uso.

Copyright © Sophos Limited

- En el campo **Algoritmo hash**, seleccione el algoritmo hash para el cálculo de las contraseñas de un solo uso.

6. Opcional: En el campo **Color de fondo**, seleccione un color para la entrada de cuenta a fin de identificarla fácilmente en la lista de cuentas.
7. Cuando haya terminado, toque **Aceptar** ✓.

Así se configurará una nueva cuenta de Authenticator.

Copyright © Sophos Limited

10 Cofre de contraseñas

El Cofre de contraseñas se utiliza para guardar todos los datos de su cuenta en un solo sitio protegido por una contraseña maestra.

Para iniciar el Cofre de contraseñas, mantenga pulsado el icono de Sophos y, a continuación, toque **Cofre de contraseñas**.

Tiene las opciones siguientes:

- Cree un nuevo archivo de Cofre de contraseñas.
- Importe un archivo KDBX de KeePass existente. Cuando edite entradas de contraseña, solo se cambiará la copia local.

Activar Autorrellenar contraseñas

En iOS 12 y posterior, se puede utilizar el Cofre de contraseñas para autorrellenar contraseñas.

Para activar la opción **Autorrellenar contraseñas** en el Cofre de contraseñas:

1. Vaya a la app **Ajustes** y desplácese hacia abajo hasta **Contraseñas y cuentas**.
2. Toque **Autorrellenar contraseñas** y active la opción **Autorrellenar contraseñas**.
3. Seleccione **Intercept X** en **Permitir relleno desde:**.

Ahora puede acceder al Cofre de contraseñas con solo tocar **Contraseñas** en la barra QuickType situada sobre el teclado cuando se le pida que introduzca las credenciales.

10.1 Crear una entrada en el Cofre de contraseñas

Para añadir una entrada o grupo de entradas en un archivo de Cofre de contraseñas:

1. En Cofre de contraseñas, toque **+**.
2. Seleccione el tipo de entrada que quiere crear:
   - **Añadir entrada de cuenta** crea una entrada con campos predefinidos adecuados para cuentas web y elementos similares.
   - **Añadir entrada de tarjeta de crédito** crea una entrada con campos predefinidos adecuados para tarjetas de crédito y elementos similares.
   - **Añadir grupo** crea una carpeta en el Cofre de contraseñas para organizar sus entradas.
3. Introduzca sus datos en los campos de la entrada.
4. Opcional: Toque **Añadir campo** para añadir un campo personalizado a la entrada.

   Si activa **Protegido** para un campo personalizado, debe tocar el botón del ojo situado junto al campo para ver el valor. Además, los campos protegidos no aparecen en los resultados de búsqueda.
5. Toque el icono **Disco** para guardar la entrada.

Los datos de contraseña permiten iniciar sesión fácilmente en una página web o una app. Consulte Usar datos de contraseña para iniciar sesión (página 15).

Copyright © Sophos Limited

10.2 Generar contraseñas

1. Abra la entrada de Cofre de contraseñas para la que quiere generar una contraseña.
2. Toque **Editar** para cambiar al modo de edición.
3. Toque en **+** junto al campo de contraseña para abrir el generador de contraseñas.
4. Defina la longitud de la contraseña y el tipo de caracteres que deban incluirse en la contraseña.
5. Toque **Generar contraseña** para generar una contraseña basada en las opciones que ha definido.
6. Si está de acuerdo con la contraseña generada, cierre el generador de contraseñas. La contraseña se actualiza con el valor generado.
7. Guarde la entrada.

10.3 Usar datos de contraseña para iniciar sesión

- Para copiar el valor de un campo al portapapeles, toque en el campo correspondiente.
- Para mostrar el valor de los campos protegidos, toque el icono **Ojo** junto al campo protegido.
- Para abrir una URL en el navegador web, tóquela. Para copiar la URL al portapapeles, toque y mantenga pulsada la URL.

Sugerencia
Cada vez que se abre una entrada de Cofre de contraseñas, se añade una notificación al área de notificaciones de Android. Los valores del nombre de usuario y la contraseña se pueden copiar al portapapeles desde esta notificación.

10.4 Administrar entradas del cofre de contraseñas

1. Toque y mantenga pulsada una entrada para cambiar al modo de selección.
2. Opcional: Seleccione las entradas adicionales para las que desee realizar la misma acción.
3. Toque un icono para realizar la acción correspondiente:
   - **Editar**: Editar el contenido de la entrada. Opción solo disponible cuando solo hay seleccionada una entrada.
   - **Cortar**: Mover las entradas seleccionadas a otro grupo en el archivo de Cofre de contraseñas.
   - **Copiar**: Copiar las entradas seleccionadas a otro grupo en el archivo de Cofre de contraseñas.
   - **Eliminar**: Mover las entradas seleccionadas al grupo especial **Papelera de reciclaje**.
     Para eliminar entradas de forma permanente, utilice **Eliminar** en las entradas en el grupo **Papelera de reciclaje**.
   - Para pegar una entrada que haya cortado o copiado, navegue hasta la nueva ubicación y, a continuación, toque **Portapapeles**.

Copyright © Sophos Limited

10.5 Buscar entradas en el cofre de contraseñas

En Cofre de contraseñas, puede buscar nombres de entradas y grupos, y valores de campos de entrada.

Nota
No puede buscar campos de contraseña o campos que haya configurado con la opción **Protegido**.

1. En Cofre de contraseñas, toque **Buscar** para cambiar al modo de búsqueda.
2. Introduzca una cadena de búsqueda. La lista de resultados se actualiza según va escribiendo.

10.6 Realizar copia de seguridad de Cofre de contraseñas

Es importante que haga copias de seguridad del archivo de Cofre de contraseñas de forma periódica. Si pierde el archivo de Cofre de contraseñas porque lo elimina sin querer o pierde su dispositivo, por ejemplo, no podrá acceder a sus datos de contraseña a menos que tenga una copia de seguridad reciente.

1. En Cofre de contraseñas, toque **Más** y luego **Exportar**.
2. Seleccione la app a la que desea exportar el archivo de Cofre de contraseñas.
   Se compartirá una copia del archivo de Cofre de contraseñas con la app que haya seleccionado.

Nota
Le recomendamos que anote la ubicación de la copia de seguridad y que guarde la nota en un lugar seguro.

Copyright © Sophos Limited

11 Escáner de códigos QR

El Escáner de códigos QR se utiliza para escanear códigos QR y luego procesar la información asociada.

Para iniciar el Escáner de códigos QR, mantenga pulsado el icono de Sophos y, a continuación, toque **Escáner de códigos QR**.

Direcciones web

Al escanear un código QR, se comprueba la URL asociada por si incluye contenido malicioso o inadecuado en función de la clasificación proporcionada por SophosLabs.

- Cuando se indique que la URL es segura, toque **Abrir** para abrirla en el navegador web.

Contactos

Escanee el código QR y después:

- Toque **Añadir contacto** para crear una entrada en sus contactos con la información de tarjeta de presentación asociada.
- Toque **Mostrar en mapa** para mostrar la ubicación asociada en la aplicación de mapas (Google Maps de forma predeterminada).
- Toque **Marcar número** para hacer una llamada telefónica al número asociado. Si el código QR contiene más de un número de teléfono, se utilizan en este orden:
  1. Número de teléfono móvil
  2. Número de teléfono del trabajo
  3. Número de teléfono de casa
- Toque **Enviar correo electrónico** para enviar un nuevo mensaje de correo electrónico a la dirección asociada. Si el código QR contiene más de una dirección de correo electrónico, se añaden todas al campo **Para**.

Additional information
Sophos Intercept X for Mobile puede leer la información de tarjetas de visita en los formatos vCard 2.1 y 3.0.

Configuraciones Wi-Fi

Escanee el código QR y luego toque **Conectarse a la red** para conectarse a la red Wi-Fi configurada en el código QR.

Nota
Verá un aviso si intenta conectarse a una red no segura, por ejemplo, una red sin protección WPA o WPA2.

Copyright © Sophos Limited

12 Protección de apps

Protección de apps se utiliza para configurar una lista de apps que solo se pueden abrir una vez que lo haya autorizado usted mismo. Esto resulta útil cuando, p. ej., deja su dispositivo a otra persona y no quiere que use determinadas apps.

Nota
Cuando Sophos Mobile administra Sophos Intercept X for Mobile, la protección de apps no está disponible. El acceso a las apps está administrado por su empresa.

1. En el menú de la app, seleccione **Protección de apps**.
2. En **Configuración base**, active Protección de apps.
3. La app Intercept X debe ser Administrador del dispositivo de Android. Si no ha activado todavía esta función, se le conducirá a la página de **Configuración** correspondiente de Android. Toque en **Activar**.
4. Seleccione un tipo de autenticación para **Protección de apps**.

   Puede elegir entre **Patrón**, **PIN**, **Contraseña** y **Huella digital** (si su dispositivo cuenta con un sensor de huella digital).

   Nota
   Cuando Sophos Mobile administra Sophos Intercept X for Mobile, el administrador puede desactivar la autenticación de huella dactilar.

5. Algunos administradores de tareas pueden desactivar la **Protección de apps** finalizando su proceso. Para la protección de administradores de tareas debe instalar la app Sophos Security & Antivirus Guard. Un mensaje en **Configuración base** lo indica. Toque el mensaje para abrir en Google Play la aplicación y, a continuación, instálela.
6. Toque **Período de gracia** y seleccione el tiempo durante el cual se recuerda la contraseña al cerrar una app y volver a abrirla.
7. **Configuración de protección** enumera las apps que se pueden usar para desinstalar o desactivar la protección de apps. También puede proteger Google Play y otros instaladores para impedir la instalación sin control de apps en el dispositivo.
8. Deslice a la izquierda. Aparece la lista de **Selección de apps**. Podrá:
   - Seleccionar apps de la lista **No protegida** para protegerlas. Las apps se muestran en la lista **Protegida**.
   - Desactivar apps de la lista **Protegida** para quitar la protección. Las apps se muestran en la lista **No protegida**.

Sophos Security & Antivirus Guard supervisa los procesos de la **Protección de apps** y los reinicia en caso necesario.

Nota
Si no ha instalado Sophos Security & Antivirus Guard y sale de la configuración de **Protección de apps**, se le volverá a solicitar que lo instale. Es muy recomendable instalarlo.

Copyright © Sophos Limited

13 Gestor de privacidad

El Gestor de privacidad muestra información sobre los permisos que tienen las apps instaladas en su dispositivo.

Nota
En esta sección se describe el Gestor de privacidad para Android 6 o posterior. Para el Gestor de privacidad para Android 5, consulte Gestor de privacidad (Android 5) (página 21).

Gestión de permisos de Android

Los permisos son un mecanismo de seguridad central en Android que otorgan determinados derechos a una app. Con la versión 6, Android ha cambiado la forma en que solicitan permisos las apps:

- Las apps creadas para Android 6 o posterior le solicitan que conceda un permiso *en el momento de la ejecución*, es decir, cuando accede a una función de la app que necesita un permiso que aún no ha concedido.
- Las apps creadas para Android 5 o anterior (conocidas como *apps heredadas*) solicitan todos los permisos *en el momento de la instalación*. Cuando una app heredada se instala en Android 6 o posterior, puede denegar permisos individuales. No obstante, como la app no está diseñada para esta funcionalidad, es posible que deje de funcionar.

Qué puede ver en el Gestor de privacidad

El Gestor de privacidad le muestra el estado de los permisos clasificados por Google como *peligrosos* porque afectan a su privacidad o al funcionamiento de otras apps:

- **Permiso de calendario** **Calendario**
- **Permiso de cámara** **Cámara**
- **Permiso de contactos** **Contactos**
- **Permiso de ubicación** **Ubicación**
- **Permiso de micrófono** **Micrófono**
- **Permiso de teléfono** **Teléfono**
- **Permiso de sensores corporales** **Sensores corporales**
- **Permiso de SMS** **SMS**
- **Permiso de almacenamiento** **Almacenamiento**

Los permisos pueden tener uno de los siguientes estados:

- **Otorgado** Solicitado y concedido
- **Denegado** Solicitado y denegado

Copyright © Sophos Limited

Nota
Para las apps heredadas, los permisos siempre se muestran como "Solicitado y concedido", aunque se haya desactivado el permiso en la configuración de la app.

Qué puede hacer en el Gestor de privacidad

- Para ver información detallada de todos los permisos que ha solicitado una app (incluidos los permisos que no son peligrosos), toque el icono de la app.
- Para conceder o denegar un permiso, toque el icono de la app y luego toque **Cambiar permisos** para abrir la página **Información de la aplicación** de la app. Desde aquí, toque **Permisos**.
- Para mostrar el historial de cambios que ha hecho en los permisos, toque **Historial de cambios de permisos** en la barra de título.
- Para configurar lo que ve en el Gestor de privacidad, toque **Filtrar**. Puede excluir determinados permisos o apps de cierto tipo, como apps del sistema o apps heredadas.
- Para cambiar el orden de las apps, toque **Ordenar** y seleccione cómo se ordenarán las apps.

Copyright © Sophos Limited

14 Gestor de privacidad (Android 5)

El Gestor de privacidad muestra información sobre los permisos que tienen las apps instaladas en su dispositivo.

Nota
En esta sección se describe el Gestor de privacidad para Android 5. Para obtener información sobre el Gestor de privacidad para Android 6 o posterior, consulte Gestor de privacidad (página 19).

Existen tres filtros de permisos:

- **Apps que pueden ocasionar costes**

  Algunas apps pueden ocasionar costes adicionales. Dependiendo de los permisos y las solicitudes de la app, la app puede llamar a números de teléfono de tarifas especiales, cambiar el estado de la red de su teléfono (lo que puede ocasionar costes en roaming) o enviar mensajes de texto sin su confirmación.

- **Apps que pueden dañar su privacidad**

  Su teléfono inteligente o tableta contienen información privada. Las apps con determinados permisos pueden leer su lista de contactos. No puede controlar qué es lo que la app va a hacer con esta información debido a los permisos otorgados. En combinación con determinados permisos de conectividad, una app podría enviar fácilmente toda la información de sus contactos a un tercero sin que sea necesaria ninguna confirmación por su parte. Este tipo de apps puede dañar su privacidad.

- **Apps que pueden acceder a Internet**

  Actualmente, la mayoría de las apps disponibles necesitan permiso para conectarse a Internet. En combinación con otros permisos, esto puede representar un gran problema de seguridad. La información que se envía a y recibe desde Internet no se puede controlar. Compruebe si la app necesita acceder a Internet y si la app es de confianza.

Gestor de privacidad enumera todas las apps que hay instaladas en el dispositivo. En la parte inferior de la pantalla, se muestran los iconos de los tres filtros del Gestor de privacidad. Toque un icono para activar o desactivar el filtro correspondiente.

Los filtros se pueden combinar de forma que se seleccionan todas las apps con permisos relacionados con los filtros activos en ese momento.

Las apps seleccionadas se clasifican en función de la correspondencia de los permisos de la app con los filtros seleccionados:

- Apps en rojo: Los permisos que la app solicita indican un riesgo alto para el filtro seleccionado.
- Apps en amarillo: Los permisos que la app solicita indican un riesgo normal para el filtro seleccionado.
- Apps en blanco: Los permisos que la app solicita indican un riesgo bajo para el filtro seleccionado.

Toque una entrada de la lista para mostrar información detallada sobre la app. La pantalla muestra qué permisos tiene la app y para que se pueden usar los permisos.

Si desea desinstalar la app de su dispositivo, toque **Desinstalar**.

Copyright © Sophos Limited

15 Gestión corporativa

En un entorno corporativo, Sophos Mobile puede administrar Sophos Intercept X for Mobile. Esto permite a su empresa supervisar el estado de cumplimiento del dispositivo.

Para inscribir Sophos Intercept X for Mobile en Sophos Mobile, siga las instrucciones que le haya proporcionado su empresa.

Cuando Sophos Mobile administra Sophos Intercept X for Mobile, se aplican las siguientes diferencias:

- La configuración de la app es definida de forma centralizada por su empresa.
- Su empresa puede activar escaneados para determinar el estado de seguridad de su dispositivo.
- Si su dispositivo infringe la política de cumplimiento de su empresa, es posible que se le restrinja el acceso a la red u otras funciones. Puede ver el estado de cumplimiento en el panel de control de la app. Consulte Resolver infracciones de cumplimiento (página 22).

Nota
Como alternativa, su empresa puede gestionar su dispositivo, o un área de trabajo de su dispositivo, con la app Sophos Mobile Control. Así la empresa tiene aún más control para, por ejemplo, instalar o desinstalar apps o desactivar funciones del dispositivo. En este caso, puede ver el estado de cumplimiento de su dispositivo y ponerse en contacto con el departamento de TI a través de la app Sophos Mobile Control. Para obtener más información, consulte la Ayuda de usuario de Sophos Mobile.

15.1 Resolver infracciones de cumplimiento

Cuando Sophos Mobile administra Sophos Intercept X for Mobile, el panel de control muestra el estado de cumplimiento en función de la política de su empresa.

Para ver y resolver infracciones de cumplimiento:

1. En el panel de control, toque **Gestión corporativa**.
   Cuando hay infracciones de cumplimiento, la casilla tiene un icono rojo.
2. Toque la infracción de cumplimiento y siga las instrucciones indicadas para resolverla.

Nota
Cuando un dispositivo infringe reglas de cumplimiento, es posible que se le restrinja el acceso a la red u otras funciones.

15.2 Obtener asistencia

Cuando Sophos Mobile administra Sophos Intercept X for Mobile, puede mostrar información sobre cómo ponerse en contacto con el departamento de TI y cualquier otra información proporcionada.

En el panel de control, toque **Gestión corporativa**.

Los datos de contacto se muestran en **Contacto de TI** e **Información adicional**.

Copyright © Sophos Limited

Sugerencia
Puede tocar los campos **Correo electrónico**, **Teléfono** o **Móvil** para escribir un mensaje de correo electrónico o llamar al departamento de TI.

Copyright © Sophos Limited

16 Configuración

Opción de configuración	Descripción
Escaneados programados	Realice escaneados automáticos periódicos.
Intervalo de escaneado programado	Frecuencia de los escaneados programados. Si selecciona **Diariamente mientras se carga**, se realizará un escaneado cuando el dispositivo haya estado conectado a una fuente de alimentación durante más de 30 minutos.
Administrar apps permitidas	Toque esta opción para mostrar la lista de apps permitidas. Estas apps no se muestran en los resultados del escaneado. Puede quitar apps de esta lista. Las apps que quite se volverán a mostrar en la lista **Amenazas y apps no deseadas**.
Quitar valores por defecto	Toque esta opción para dejar de utilizar Intercept X como app predeterminada para abrir enlaces admitidos.
Escanear apps de sistema	Seleccione esta opción para incluir apps del sistema Android en el escaneado. Las apps del sistema no se escanean por defecto, ya que están protegidas por Android y no pueden ser eliminadas por el usuario.
Escanear almacenamiento	Seleccione esta opción para incluir las tarjetas SD y los dispositivos de almacenamiento USB en el escaneado.
Detectar apps no deseadas	Seleccione esta opción para activar la detección de aplicaciones no deseadas (PUA). Las aplicaciones no deseadas aunque no son maliciosas, normalmente se consideran inapropiadas en redes corporativas. Las principales clases de apps no deseadas son programas publicitarios, marcadores telefónicos, monitores de sistema, herramientas de administración remota y herramientas usadas por hackers. En cualquier caso, ciertas apps que pueden entrar en la categoría de apps no deseadas pueden ser consideradas útiles por algunos usuarios.
Reputación de app	Seleccione esta opción para activar la detección de apps de baja reputación. Las apps con una baja reputación son las que tienen una baja reputación según los datos de Sophos Live Protection.

Copyright © Sophos Limited

Opción de configuración	Descripción
Notificación de escaneado	Seleccione esta opción para activar las notificaciones de escaneado de apps limpias. Si no se selecciona esta opción, solo se reciben notificaciones de malware, aplicaciones no deseadas y apps de baja reputación. Sophos Intercept X for Mobile escanea las apps durante la instalación en el dispositivo Android o cuando se ejecutan desde la tarjeta SD o los dispositivos de almacenamiento USB. Encontrará las notificaciones en el Panel de notificaciones.
Supervisar almacenamiento	Seleccione esta opción para escanear todas las apps y los archivos nuevos que se descargan o se copian en la tarjeta SD o los dispositivos de almacenamiento USB. Todo los nuevos dispositivos de almacenamiento conectados se escanean automáticamente.
Versión	La versión del motor antivirus y los datos antivirus.
Última actualización	La fecha en la que se han recuperado los datos antivirus de Sophos. Toque la opción para comprobar si hay actualizaciones.
Modo de actualización	Esta configuración define la conexión de datos que utiliza Sophos Intercept X for Mobile para descargar las actualizaciones de datos de detección de virus.
Enviar registro por correo electrónico	Toque esta opción para enviar un correo electrónico con el archivo de registro de la aplicación adjunto. La dirección de correo electrónico de soporte de Sophos se inserta por defecto.
Seguimiento de datos para ayudar a mejorar la facilidad de uso	Permita que Sophos recopile datos de uso anónimos para mejorar la aplicación.
Desinstalar Sophos Intercept X for Mobile	Toque para desinstalar la app Intercept X y la app Security & Antivirus Guard asociada, si está instalada.

Copyright © Sophos Limited

17 Crear una copia de seguridad y restaurar

Puede realizar una copia de seguridad de la configuración de la app, por ejemplo, para utilizarla en otro dispositivo.

Puede crear una copia de seguridad de los siguientes elementos:

- Configuración
- Escáner
- Filtrado web
- Protección de apps
- Authenticator

Cuando Sophos Mobile gestiona Sophos Intercept X for Mobile, solo puede realizar una copia de seguridad de las cuentas de Authenticator.

Realizar una copia de seguridad de la configuración

1. En el menú de la app, seleccione **Copia de seguridad y restaurar**.
2. Toque **Realizar copia de seguridad**.
3. Seleccione las opciones que desea exportar.
4. Toque **Realizar copia de seguridad**.
5. Introduzca las credenciales de su dispositivo y pulse **Siguiente**.
6. Seleccione la ubicación para crear la copia de seguridad.

   Sugerencia
   Guarde la copia de seguridad en la nube para que pueda utilizarla en otros dispositivos.

7. Introduzca el nombre del archivo y toque **Guardar**.
8. Especifique una contraseña para la copia de seguridad, confírmela y toque **Aceptar**.

Restaurar la configuración

1. En la página **Copia de seguridad y restaurar**, toque **Restaurar**.
2. Vaya a la ubicación donde ha guardado el archivo y toque la copia de seguridad.
3. Especifique la contraseña para la copia de seguridad y toque **Aceptar**.
4. Seleccione las opciones que desea restaurar.
5. Toque **Restaurar**.

Copyright © Sophos Limited

18 Registro

Sophos Intercept X for Mobile deja constancia de las operaciones importantes en un registro propio. Este es adicional al registro de Android. No se obtiene información directa sobre los resultados de las operaciones en segundo plano que realiza la app, como los escaneados de malware al instalar otras apps. El registro proporciona un informe detallado sobre estas acciones. Da detalles sobre cuándo se han realizado estas acciones y los resultados correspondientes.

- Para mostrar el registro, toque **Menú** ☰ y luego **Registro**.
- Para borrar el registro, toque **Eliminar** 🗑 en la barra de título.

Copyright © Sophos Limited

19 Aviso legal

Copyright © 2020 Sophos Limited. Todos los derechos reservados. Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, mecánico, grabación, fotocopia o cualquier otro sin la correspondiente licencia del producto, bajo dichos términos, o sin la previa autorización escrita por parte del propietario.

Sophos, Sophos Anti-Virus y SafeGuard son marcas registradas de Sophos Limited, Sophos Group y Utimaco Safeware AG, según corresponda. Otros productos y empresas mencionados son marcas comerciales o registradas de sus respectivos propietarios.