SOPHOS

Cybersecurity made simple.

Sophos Mobile

Guía de inicio

Versión del producto: 8.6

Contenido

1 Acerca de esta guía

Esta guía explica cómo realizar la configuración inicial de Sophos Mobile paso a paso a fin de administrar sus dispositivos.

Encontrará más información en la Ayuda de administrador de Sophos Mobile.

Esta guía se centra en iOS y Android, las plataformas móviles más comunes. La configuración puede aplicarse de forma similar a los demás sistemas operativos admitidos.

2 Licencias Sophos Mobile

Sophos Mobile ofrece dos tipos de licencia:

- Licencia Mobile Standard
- Licencia Mobile Advanced

La licencia de tipo Mobile Advanced le permite administrar las apps Sophos Mobile Security, Sophos Secure Workspace y Sophos Secure Email.

Para más información sobre cómo administrar Sophos Mobile Security, Sophos Secure Workspace y Sophos Secure Email mediante la consola de Sophos Mobile, consulte la Ayuda de administrador de Sophos Mobile.

Como superadministrador, puede activar las licencias adquiridas en el cliente superadministrador y asignar el número necesario de usuarios con licencia a clientes individuales.

2.1 Licencias de evaluación

Sophos ofrece una evaluación gratuita para Sophos Mobile. Puede registrarse para la evaluación en el sitio web de Sophos: http://www.sophos.com/es-es/products/free-trials/mobile-control.aspx.

La licencia de evaluación le permite administrar hasta cinco usuarios y es válida durante 30 días.

Lo único que necesitará para configurar Sophos Mobile para la evaluación es la dirección de correo electrónico que haya utilizado para registrarse al descargar el instalador.

2.2 Actualizar las licencias de evaluación a licencias completas

Para actualizar las licencias de evaluación a licencias completas, solo tiene que introducir la clave de licencia completa en Sophos Mobile. Para obtener más información, consulte la Ayuda de administrador de Sophos Mobile.

2.3 Actualizar licencias

Para actualizar sus licencias, tiene que activar la nueva clave de licencia en Sophos Mobile. Para más información, consulte la Guía de superadministrador de Sophos Mobile.

3 Pasos clave

Para empezar a utilizar Sophos Mobile:

1. Inicie sesión en Sophos Mobile Admin como superadministrador.
2. Inicie el asistente **Primeros pasos** para realizar la configuración inicial del servidor de Sophos Mobile.

   Nota
   El asistente **Primeros pasos** incluye una opción para solicitar una licencia de evaluación.

3. Compruebe sus licencias.
4. Cree un nuevo cliente para administrar sus dispositivos.
5. Cambie al nuevo cliente.
6. Cree un administrador para el nuevo cliente e inicie sesión en Sophos Mobile Admin como dicho administrador.
7. Configure las opciones personales, las políticas de contraseña para las cuentas de administrador, los datos de contacto del soporte técnico y las opciones del portal de autoservicio.
8. Cargue un certificado del servicio de notificaciones push de Apple para administrar dispositivos iPhone, iPad y Mac.
9. Crear políticas de cumplimiento.
10. Cree grupos de dispositivos.
11. Configure los dispositivos.
12. Actualice la configuración del portal de autoservicio y añada un usuario de prueba del portal de autoservicio.
13. Si usa la administración interna de usuarios: Añada usuarios creándolos o subiendo su lista de usuarios.
14. Si usa la administración externa de usuarios: Configure la conexión a su directorio LDAP.

    Esto se describe en la *Guía de superadministrador de Sophos Mobile*.
15. Pruebe la inscripción de dispositivos en el portal de autoservicio.

4 Iniciar sesión como superadministrador

Debe iniciar sesión en Sophos Mobile Admin utilizando la cuenta de superadministrador que se configuró durante la instalación de Sophos Mobile para realizar algunos pasos de configuración iniciales.

1. Abra la dirección web de Sophos Mobile Admin que ha configurado durante la instalación de Sophos Mobile.
2. En el cuadro de diálogo de inicio de sesión, introduzca el nombre de cliente superadministrador y las credenciales del superadministrador y haga clic en **Iniciar sesión**.

Nota

Cuando se inicia sesión como superadministrador, se accede a una versión especial de Sophos Mobile Admin que está adaptada a las tareas de superadministrador.

Para ver una descripción detallada sobre cómo utilizar Sophos Mobile Admin como superadministrador, consulte la *Guía de superadministrador de Sophos Mobile*.

5 Configurar las opciones de configuración del sistema

Al iniciar sesión en Sophos Mobile Admin por primera vez después de la instalación, el asistente **Primeros pasos** le ayuda a configurar las opciones del sistema.

Debe facilitar la información siguiente:

- La dirección del servidor proxy HTTP (si procede).
- Su clave de licencia para Sophos Mobile.
- Sus certificados SSL/TLS.
- Las credenciales de su servidor SMTP.

Nota
Más tarde puede cambiar todas las opciones en **Configuración > Configuración del sistema**.

1. En la página **Proxy HTTP**, especifique la dirección y el puerto del servidor proxy que va a utilizarse para las conexiones SSL/TLS y HTTP salientes.
2. En la página **Licencia**, introduzca su clave de licencia o solicite una licencia de evaluación:
   - **Clave de licencia Standard**: Especifique su clave de licencia de Mobile y haga clic en **Activar**.
   - **Clave de licencia Advanced**: Especifique su clave de licencia de Mobile Advanced y haga clic en **Activar**. Primero debe introducir una clave de licencia de Mobile.
   - **Solicitar evaluación**: Introduzca la dirección de correo electrónico que ha utilizado para descargar el programa de instalación de Sophos Mobile del sitio web de Sophos.
3. En la página **SSL/TLS**, configure los certificados SSL/TLS utilizados para proteger las conexiones entre el servidor de Sophos Mobile y los clientes.
   a) Haga clic en **Autodescubrir certificado(s)**.
      En la mayoría de los casos, la función autodescubrir detecta los certificados que se están usando.
   b) Si los certificados no se detectan de forma automática, cárguelos de forma manual: haga clic en **Subir un archivo** y seleccione el archivo de certificado codificado CER o DER pertinente.

   Puede configurar hasta cuatro certificados ya que, en función de la arquitectura de su red, es posible que se estén usando distintos certificados para clientes que se conectan desde Internet o desde la Intranet local. El servidor de Sophos Mobile comunicará la lista de certificados a los clientes. Al establecer una conexión SSL o TLS, los clientes solo confiarán en el servidor si el certificado presentado está incluido en la lista (*pineado de certificados*).

   Importante
   Actualice la lista de certificados cuando haya cambiado o renovado certificados SSL. En todo momento debe haber disponible al menos un certificado válido. De lo contrario, los clientes no confiarán en el servidor y no se conectarán al mismo.

4. En la página **SMTP**, configure los datos del servidor SMTP y las credenciales de inicio de sesión. Es necesario configurar la opción de SMTP para permitir el envío de mensajes de correo

electrónico a los nuevos usuarios a fin de proporcionarles sus credenciales de inicio de sesión. También es necesario configurar esta opción para permitir la inscripción por correo electrónico.

Opción	Descripción
Host SMTP	Dirección del servidor SMTP.
Puerto de conexión	El puerto de servidor con el que se establecerá la conexión. **Nota** Los tipos de conexión mostrados (TLS, SSL y sin cifrar) solo muestran usos de puertos estándar. Consulte la documentación del servidor SMTP para obtener instrucciones sobre qué puerto utilizar.
Usuario SMTP	Si lo solicita el servidor SMTP, introduzca el nombre de un usuario que tenga permiso para conectarse.
Contraseña SMTP	Contraseña del usuario SMTP.
Remitente de correo electrónico	Dirección de correo electrónico que aparecerá en el campo *De* de los correos electrónicos de Sophos Mobile.
Nombre del remitente	Nombre del autor que aparecerá en campo *De*. En caso necesario, puede configurar un nombre de remitente (pero no una dirección de correo electrónico) distinto para cada cliente más adelante. Consulte la Ayuda de administrador de Sophos Mobile.
Enviar correos electrónicos de error	Sophos Mobile enviará mensajes de error, por ejemplo, cuando caduque un certificado APNs.
Destinatarios de correo electrónico	Introduzca las direcciones de correo electrónico de los destinatarios que recibirán correos electrónicos de error.

Nota
Sophos Mobile no admite el mecanismo OAUTH para la autenticación SMTP. Los proveedores de correo electrónico que prefieren OAUTH (como Gmail de Google) podrían clasificar los intentos de inicio de sesión desde Sophos Mobile como no seguros.

5. Una vez que haya configurado la información SMTP, haga clic en **Enviar mensaje de prueba** para verificar la configuración de correo electrónico.
6. Haga clic en **Finalizar** para finalizar el asistente **Primeros pasos**.

6 Activar licencias Mobile Advanced

Con las licencias Mobile Advanced, puede utilizar Sophos Mobile para administrar las apps Sophos Mobile Security, Sophos Secure Workspace y Sophos Secure Email.

Si las licencias Mobile Advanced no se han activado durante la configuración inicial de Sophos Mobile, el superadministrador puede activarlas posteriormente desde Sophos Mobile Admin:

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema**.
2. En la ficha **Licencia**, introduzca su clave de licencia en **Clave de licencia Advanced** y haga clic en **Activar**.

Cuando la clave esté activada, se mostrarán los detalles de la licencia.

7 Comprobar sus licencias

Sophos Mobile utiliza una esquema de licencias basado en usuarios. Una licencia de usuario es válida para todos los dispositivos asignados a ese usuario. Los dispositivos que no están asignados a un usuario requieren una licencia para cada uno.

Para comprobar sus licencias disponibles:

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema**.
2. En la página **Configuración del sistema**, haga clic en la ficha **Licencia**.

Aparece la información siguiente:

- **Número máximo de licencias**: Número máximo de usuarios de dispositivo (y dispositivos sin asignar) que pueden administrarse.

  Si el superadministrador no ha establecido una cuota para el cliente, el número de licencias está limitado por el número en general para el servidor de Sophos Mobile.
- **Licencias usadas**: Número de licencias en uso.
- **Válida hasta**: Fecha de vencimiento de la licencia.
- **URL licenciada**: URL del servidor de Sophos Mobile para el que se emite la licencia.

Si tiene cualquier duda o pregunta sobre la información de licencias mostrada, póngase en contacto con su representante de ventas de Sophos.

8 Crear un cliente

Debe haber iniciado sesión en Sophos Mobile Admin como superadministrador para realizar esta tarea.

1. En la barra lateral de menús, en **ADMINISTRAR**, haga clic en **Clientes**.
2. Haga clic en **Crear cliente**.
3. En la página **Editar cliente**, configure las siguientes opciones.

Opción	Descripción
Nombre	Nombre del cliente.
Descripción	Texto para describir la finalidad de la cuenta de cliente.
Número máximo de licencias	Número de usuarios de dispositivos y dispositivos sin asignar que pueden administrarse para el cliente.
Licencias avanzadas	Si se selecciona esta opción, el cliente puede utilizar Sophos Mobile para administrar las apps Sophos Mobile Security, Sophos Secure Workspace y Sophos Secure Email.
Válido hasta	Fecha de vencimiento de las licencias asignadas al cliente. Después de esta fecha, no podrá crear nuevas tareas para dispositivos que estén administrados para el cliente.
Desactivar cuenta	Si se selecciona esta opción, el inicio de sesión en ese cliente está deshabilitado. Como superadministrador, podrá cambiar a la vista del cliente igualmente mediante la lista de clientes en la cabecera de la página. Se puede volver a activar una cuenta desactivada si se desmarca la casilla **Desactivar cuenta**.
Plataformas activadas	Seleccione las plataformas para las que se pueden inscribir dispositivos.
Configuración de privacidad del dispositivo	Seleccione **Permitir a los usuarios localizar dispositivos** para permitir a los usuarios localizar sus dispositivos en caso de robo o extravío. Seleccione **Permitir a los administradores localizar dispositivos** para permitir a los administradores localizar dispositivos. Seleccione **Mostrar apps instaladas** para mostrar las aplicaciones instaladas en los detalles del dispositivo.
Configuración de clonación	Active la casilla **Configuración y paquetes** si desea que todos los perfiles y paquetes creados en la cuenta del superadministrador estén disponibles en la cuenta del cliente.
Directorio de usuario	Seleccione el origen de datos de los usuarios del portal de autoservicio (SSP) que deban ser administrados por Sophos Mobile. Elija de entre estas opciones:

Opción	Descripción
	• **Ninguno. No hay disponibles administradores de LDAP, perfiles específicos de usuario ni SSP**: Esta opción desactiva la creación de cuentas de usuario para el portal de autoservicio y la búsqueda de cuentas para Sophos Mobile Admin desde un directorio LDAP. • **Directorio interno**: Utilice la administración de usuarios internos para Sophos Mobile Admin y el portal de autoservicio. Para obtener más información, consulte la Ayuda de administrador de Sophos Mobile. • **Directorio LDAP externo**: Además de la administración de usuarios internos, puede buscar cuentas para Sophos Mobile Admin y el portal de autoservicio desde un directorio LDAP. Haga clic en **Configurar LDAP externo** para especificar los datos del servidor.

4. Haga clic en **Guardar**.

El cliente se ha creado.

9 Cambiar el cliente

Para finalizar la configuración inicial del cliente que ha creado en la sección anterior, deberá cambiar del cliente superadministrador a ese cliente.

Para cambiar a la vista del nuevo cliente:

1. En la cabecera de la página de la vista de superadministrador, haga clic en el nombre del cliente actual para abrir la lista de clientes disponibles.

   En esta lista, el cliente superadministrador está marcado con un asterisco y aparece al principio.
2. Seleccione el cliente que ha creado en la sección anterior.

La vista cambia a la vista de ese cliente, que es la vista que se ve cuando se inicia sesión con una cuenta de administrador para ese cliente.

10 Crear un administrador para el cliente

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Administradores**.
2. En la página **Mostrar administradores**, haga clic en **Crear administrador**.
3. En la página **Editar administrador**, configure los detalles de la cuenta para el administrador.
   - Cuando **Directorio LDAP externo** está seleccionado como directorio de usuarios para el cliente, puede hacer clic en **Buscar usuario a través de LDAP** para seleccionar una cuenta LDAP existente.
   - Cuando **Directorio interno** o **Ninguno** está seleccionado como directorio de usuarios para el cliente, introduzca los datos relevantes en los campos **Nombre de inicio de sesión**, **Nombre**, **Apellidos**, **Dirección de correo electrónico** y **Contraseña**.

   La contraseña que especifique es una contraseña de un solo uso. En el primer inicio de sesión, se pedirá al administrador que la cambie.
4. En la lista **Rol**, seleccione el rol de usuario **Administrador**.
5. Haga clic en **Guardar** para crear la cuenta de administrador.

Para continuar con la configuración del cliente, cierre la sesión de Sophos Mobile Admin y vuelva a iniciar sesión utilizando las credenciales del administrador que acaba de crear (nombre de cliente, nombre de inicio de sesión y contraseña de un solo uso).

11 Configurar las opciones

Configure las siguientes opciones:

- Configuración personal, por ejemplo, las plataformas que desea administrar
- Políticas de contraseña
- Datos de contacto del soporte técnico
- Opciones del portal de autoservicio

11.1 Configurar las opciones personales

Para utilizar Sophos Mobile Admin de forma más eficiente, puede personalizar la interfaz de usuario de modo que muestre solo las plataformas con las que trabaja.

Nota
Al configurar las plataformas, solo se cambia la vista del usuario que tiene una sesión iniciada en ese momento. No es posible desactivar ninguna función aquí.

Requisitos previos: Ha iniciado sesión en Sophos Mobile Admin como el administrador que ha creado para el nuevo cliente.

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > General** y luego haga clic en la ficha **Personal**.
2. Configure las siguientes opciones:

Opción	Descripción
Idioma	Seleccione el idioma para Sophos Mobile Admin.
Zona horaria	Seleccione la zona horaria en que se mostrarán las fechas.
Sistema de la unidad	Seleccione el sistema de la unidad (**Métrica** o **Británica**) para los valores de longitud.
Líneas por página en tablas	Seleccione el número máximo de líneas de tabla que desea mostrar por página.
Mostrar detalles de dispositivo avanzados	Marque esta casilla para mostrar toda la información disponible sobre el dispositivo. Las fichas **Propiedades personalizadas** y **Propiedades internas** se añaden a la página **Mostrar dispositivo**.
Plataformas activadas	Seleccione las plataformas que desea administrar para el cliente: • **Android** • **Android Things** • **iOS** • **Windows Mobile** (incluye los sistemas operativos Windows Phone 8.1 y Windows 10 Mobile) • **Windows**

Opción	Descripción
	• **Windows IoT** La interfaz de usuario de Sophos Mobile Admin se ajustará en función de las plataformas que seleccione. Solo se mostrarán las vistas y las funciones que sean relevantes para las plataformas seleccionadas. **Nota** La lista de plataformas disponibles depende de las opciones de plataformas de la configuración del superadministrador. Para más información, consulte la Guía de superadministrador de Sophos Mobile.

3. Haga clic en **Guardar**.

11.2 Configurar las políticas de contraseña

Para aplicar contraseñas seguras, configure las políticas de contraseña para los usuarios de Sophos Mobile Admin y el portal de autoservicio.

Nota
Las políticas de contraseña no se aplican a los usuarios de directorios LDAP externos. Para más información acerca de la administración de usuarios externos, consulte la Guía de superadministrador de Sophos Mobile.

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > General** y luego haga clic en la ficha **Políticas de contraseña**.
2. En **Reglas**, puede definir requisitos para las contraseñas, como un número mínimo de caracteres en minúsculas, en mayúsculas o numéricos que debe contener la contraseña para ser válida.
3. En **Configuración**, establezca la siguientes opciones:
   a) **Intervalo de cambio de contraseña (días)**: Introduzca el número de días que deben transcurrir para que caduque una contraseña (entre `1` y `730`) o deje el campo vacío para deshabilitar la caducidad de la contraseña.
   b) **Número de contraseñas anteriores que no deben reutilizarse**: Seleccione un valor entre `1` y `10`, o seleccione `---` para deshabilitar esta restricción.
   c) **Número máximo de intentos de inicio de sesión fallidos**: Seleccione el número de intentos de inicio de sesión fallidos que deben producirse para que se bloquee la cuenta (entre `1` y `10`) o seleccione `---` para permitir un número de intentos de inicio de sesión fallidos ilimitado.
4. Haga clic en **Guardar**.

11.3 Configurar el contacto de TI

Facilite los datos de contacto de su departamento de TI para que los usuarios puedan obtener asistencia ante preguntas o problemas.

La información que introduzca aquí aparecerá en el portal de autoservicio y en los dispositivos de los usuarios.

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > General** y, a continuación, haga clic en la ficha **Contacto de TI**.
2. Introduzca la información de contacto.
3. Haga clic en **Guardar**.

12 Certificados del servicio de notificaciones push de Apple

Para poder usar el protocolo de gestión de dispositivos móviles (MDM) de los dispositivos iOS y macOS, Sophos Mobile debe usar el servicio de notificaciones push de Apple (APNs) para activar los dispositivos.

Sophos Mobile administra los certificados del APNs por cliente. Debe crear y cargar los certificados para cada cliente que utilice.

Los certificados del APNs tienen un plazo de validez de un año.

Para facilitar la renovación de los certificados APNs, el superadministrador puede renovar en un paso los certificados de todos los clientes que utilizan el mismo certificado. Consulte la Ayuda de administrador de Sophos Mobile.

En las siguientes secciones se describen los requisitos que deben cumplirse y los pasos que debe seguir para obtener acceso a los servidores APNs con su propio certificado de cliente.

12.1 Requisitos

Para la comunicación con el servicio de notificaciones push de Apple (APNs), se debe permitir el tráfico TCP de y a los puertos siguientes:

- El servidor de Sophos Mobile necesita conectarse a `gateway.push.apple.com:2195 TCP (17.0.0.0/8)`
- Cada dispositivo iOS con solo acceso Wi-Fi necesita conectarse a `*.push.apple.com:5223 TCP (17.0.0.0/8)`

12.2 Crear certificado APNs

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **APNs**.
2. Haga clic en **Asistente de certificados APNs**.
3. En la página **Modo**, haga clic en **Crear un nuevo certificado APNs**.
4. En la página **CSR**, haga clic en **Descargar la solicitud de firma de certificado**.

   Este paso guarda el archivo de solicitud de firma de certificado `apple.csr` en su ordenador. El archivo de solicitud de firma de certificado es específico del cliente actual.
5. Necesita un ID de Apple. Incluso si ya dispone de un ID, recomendamos que cree uno nuevo para usarlo con Sophos Mobile. En la página **ID de Apple**, haga clic en **Crear ID de Apple en el portal de Apple**.

   Se abre una página web de Apple en la que puede crear un ID de Apple para su empresa.

   Nota
   Guarde las credenciales en un lugar seguro al que puedan acceder sus compañeros. Su empresa necesitará estas credenciales para renovar el certificado cada año.

6. En el asistente, introduzca su nuevo ID de Apple en el campo **ID de Apple**.
7. En la página **Certificado**, haga clic en **Crear certificado en el portal de Apple**.

   Se abre el Portal de certificados push de Apple.
8. Inicie sesión con su ID de Apple y cargue el archivo de solicitud de firma de certificado `apple.csr`.
9. Descargue el archivo de certificado APNs `.pem` y guárdelo en su ordenador.
10. En la página **Cargar**, haga clic en **Cargar certificado** y, a continuación, busque el archivo `.pem` que ha recibido del Portal de certificados push de Apple.
11. Haga clic en **Guardar**.

Sophos Mobile lee el certificado y muestra los detalles del certificado en la ficha **APNs**.

13 Políticas de cumplimiento

Con las políticas de cumplimiento puede:

- Permitir, prohibir o aplicar determinadas funciones en un dispositivo.
- Definir acciones que se ejecutan cuando se infringe una regla de cumplimiento.

Puede crear distintas políticas de cumplimiento y asignarlas a grupos de dispositivos. Esto le permite aplicar distintos niveles de seguridad a sus dispositivos administrados.

Sugerencia
Si tiene previsto administrar dispositivos corporativos y privados, se recomienda que establezca políticas de cumplimiento distintas para al menos estos dos tipos de dispositivos.

13.1 Crear política de cumplimiento

1. En la barra lateral de menús, en **CONFIGURAR**, haga clic en **Políticas de cumplimiento**.
2. En la página **Políticas de cumplimiento**, haga clic en **Crear política de cumplimiento** y, a continuación, seleccione la plantilla en la que se basará la política:
   - **Plantilla predeterminada**: Una selección de reglas de cumplimiento, sin acciones definidas.
   - **Plantilla PCI**, **Plantilla HIPAA**: Acciones y reglas de cumplimiento que se basan en los estándares de seguridad HIPAA y PCI DSS respectivamente.

   La plantilla que elija no limita las opciones de configuración posteriores.
3. Introduzca un nombre y, si lo desea, una descripción para la política de cumplimiento.

Repita los pasos siguientes para todas las plataformas necesarias.

4. Asegúrese de que la casilla **Activar plataforma** de cada ficha esté seleccionada.

   Si no se selecciona esta casilla, no se comprueba si los dispositivos de esa plataforma cumplen las reglas.
5. En **Regla**, configure las reglas de cumplimiento para la plataforma en cuestión.

   Para obtener una descripción de las reglas disponibles para cada tipo de dispositivo, haga clic en **Ayuda** en la cabecera de la página.

   Nota
   Cada regla de cumplimiento tiene fijado un nivel de gravedad (alto, medio, bajo) que está representado por un icono azul. La gravedad le permite valorar la importancia de cada regla y las acciones que debe aplicar si se infringe.

   Nota
   En el caso de los dispositivos en los que Sophos Mobile administra el contenedor de Sophos en lugar de todo el dispositivo, solo es aplicable un subconjunto de las reglas de cumplimiento. En **Resaltar reglas**, seleccione el tipo de administración para resaltar las reglas que son relevantes.

6. En **Si se infringe una regla**, defina las acciones que se aplicarán al infringirse una regla:

Opción	Descripción
Denegar correo electrónico	Prohibir el acceso al correo electrónico. Esta acción solo puede realizarse si el superadministrador ha configurado una conexión al proxy EAS interno o independiente. Consulte Guía de superadministrador de Sophos Mobile. Esta acción solo está disponible para dispositivos Android, iOS, Windows y Windows Mobile.
Bloquear contenedor	Deshabilitar las apps Sophos Secure Workspace y Secure Email. Esto afecta al acceso a documentos, correo electrónico y web administrado por estas apps. Esta acción solo puede realizarse si se ha activado una licencia Mobile Advanced. Esta acción solo está disponible para dispositivos Android e iOS.
Denegar red	Prohibir el acceso a la red. Esta acción solo puede realizarse si el superadministrador ha configurado el control de acceso a la red. Consulte la Guía de superadministrador de Sophos Mobile. Esta acción no está disponible para dispositivos en los que solo Sophos Mobile administre el contenedor de Sophos.
Crear alerta	Cree una alerta. Las alertas se muestran en la página **Alertas**.
Transferir paquete de tareas	Transferir un paquete de tareas específico al dispositivo. Esta acción solo está disponible para dispositivos Android, iOS, macOS y Windows. Se recomienda que establezca esta opción en **Ninguno** por el momento. Para obtener más información, consulte la Ayuda de administrador de Sophos Mobile. **Importante** Si no se usan correctamente, los paquetes de tareas pueden alterar la configuración de los dispositivos o incluso eliminar todo el contenido de los mismos. Para asignar los paquetes de tareas correctos a las reglas de cumplimiento, es necesario tener un conocimiento en profundidad del sistema.

Nota
Cuando un dispositivo en el modo propietario del dispositivo de Android para empresas deja de cumplir las políticas, se desactivan todas las apps.

7. Cuando haya establecido las opciones para todas las plataformas necesarias, haga clic en **Guardar** para guardar la política de cumplimiento con el nombre que haya especificado.

El nuevo conjunto se muestra en la página **Políticas de cumplimiento**.

Para utilizar una política de cumplimiento, esta se asigna a un grupo de dispositivos. Este proceso se describe en la siguiente sección.

14 Grupos de dispositivos

Los grupos de dispositivos se usan para categorizar dispositivos. Le ayudarán a administrarlos de forma eficiente, puesto que se pueden realizar tareas en un grupo en vez de hacerlo en dispositivos individuales.

Un dispositivo siempre pertenece exactamente a un grupo de dispositivos. Se asigna un dispositivo a un grupo de dispositivos cuando se añade a Sophos Mobile.

Sugerencia
Se recomienda que solo agrupe dispositivos con el mismo sistema operativo. Esto facilita el uso de grupos para instalaciones y otras tareas específicas de sistemas operativos.

14.1 Crear grupo de dispositivos

1. En la barra lateral de menús, en **ADMINISTRAR**, haga clic en **Grupos de dispositivos** y luego haga clic en **Crear grupo de dispositivos**.
2. En la página **Editar grupo de dispositivos**, introduzca un nombre y una descripción para el nuevo grupo de dispositivos.
3. En **Políticas de cumplimiento**, seleccione las políticas de cumplimiento que se aplicarán a los dispositivos corporativos y a los personales.
4. Haga clic en **Guardar**.

Nota
La configuración del grupo de dispositivos contiene la opción **Activar la auto inscripción para iOS**. Esta opción le permite inscribir dispositivos iOS con Apple Configurator. Para obtener más información, consulte la Ayuda de administrador de Sophos Mobile.

El nuevo grupo de dispositivos se crea y aparece en la página**Grupos de dispositivos**.

15 Empezar a usar políticas de dispositivo

El asistente **Inicio de políticas** le ayuda a crear políticas de dispositivo básicas para todas las plataformas. Después puede ampliar las políticas.

Nota
En función de la plataforma, las opciones de dispositivo se configuran mediante un perfil de dispositivo (Android, iOS) o una política de dispositivo (macOS, Windows, Windows Mobile). Para simplificar, este apartado utiliza el término *política* tanto para perfiles como para políticas.

1. En el panel de control, haga clic en **Asistente para inicio de políticas** en el widget **Tareas de introducción**.

   Sugerencia
   Si no ve el widget, haga clic en **Añadir widget > Introducción**.

2. En la página **Plataformas**, seleccione las plataformas de dispositivo para las que desea crear una política.

   Seleccione **Android** e **iOS**.
3. En la página **Políticas**, configure las siguientes opciones:

   a) Introduzca un nombre para la política.

   Se crea una política con ese nombre para cada plataforma.

   b) Seleccione las áreas que gestiona la política.

   Si desmarca una casilla, se omitirá la página correspondiente del asistente. Más adelante puede configurar las áreas que omita (y otras opciones).

   Recomendamos seleccionar por lo menos **Requisitos para la contraseña** y **Restricciones**.
4. En la página **Contraseñas**, configure los requisitos para la contraseña del dispositivo.
5. En la página **Restricciones**, configure las restricciones que se aplican a los dispositivos, como desactivar la cámara u otras funciones del dispositivo que podrían suponer un riesgo para la seguridad.

   Al seleccionar **Separar los datos personales de los profesionales en el dispositivo**, se definen las restricciones que evitan el uso compartido de datos corporativos con apps personales (y viceversa), si el sistema operativo del dispositivo lo admite.
6. En la página **Wi-Fi**, configure la conexión con la red Wi-Fi corporativa.

   Si la red Wi-Fi utiliza un tipo de seguridad que no sea **WPA/WPA2 PSK**, se puede cambiar esta opción más tarde.
7. En la página **Correo electrónico**, configure la conexión con el servidor de correo electrónico corporativo de Microsoft Exchange.

   Los marcadores `%_USERNAME_%` y `%_EMAILADDRESS_%` se sustituyen por el nombre y la dirección de correo electrónico del usuario asignado al dispositivo.
8. Haga clic en **Finalizar**.

Para cada plataforma que haya seleccionado, el asistente crea una política.

Para ver la política, haga clic en **Perfiles, políticas** en la barra lateral de menús y, a continuación, haga clic en la plataforma del dispositivo.

Para modificar las áreas que se gestionan, haga clic en el nombre de la política y luego en **Añadir configuración**.

16 Crear paquete de tareas para dispositivos Android

1. En la barra lateral de menús, en **CONFIGURAR**, haga clic en**Paquetes de tareas > Android**.
2. En la página **Paquetes de tareas** haga clic en **Crear paquetes de tareas**.
   Aparece la página **Editar paquete de tareas**.
3. En los campos correspondientes, especifique un nombre y, opcionalmente, una descripción para el nuevo paquete de tareas.

   La versión se incrementa automáticamente cada vez que se guarda el paquete de tareas.
4. Opcional: Seleccione **Seleccionable para acciones de cumplimiento** para transferir el paquete de tareas a un dispositivo cuando infrinja una regla de cumplimiento. Consulte Políticas de cumplimiento (página 18).

   Nota
   Esta opción se desactiva cuando se edita un paquete de tareas existente y el paquete de tareas ya se utiliza como acción de cumplimiento.

5. Haga clic en **Crear tarea**, seleccione **Inscribir** e introduzca el nombre de la tarea. Haga clic en **Aplicar** para crear la tarea.

   El nombre que introduzca aquí se mostrará en el portal de autoservicio mientras se procese la tarea.
6. Haga clic en **Crear tarea** de nuevo y seleccione **Instalar perfil o asignar política**. Dé un nombre descriptivo a la tarea, por ejemplo, `Instalar perfil de políticas de contraseña` y seleccione el perfil que ha creado. Haga clic en **Aplicar** para crear la tarea.
7. Si ha configurado perfiles para las opciones de Exchange, VPN o Wi-Fi, repita este paso para cada perfil.
8. Opcional: Añada más tareas al paquete de tareas.

   Sugerencia
   Puede cambiar el orden de instalación de las tareas por medio de las flechas del lado derecho de la lista de tareas.

9. Una vez que haya añadido todas las tareas necesarias al paquete de tareas, haga clic en **Guardar** en la página **Editar paquete de tareas**.

El paquete de tareas está disponible para transferirse. Se muestra en la página **Paquetes de tareas**.

17 Crear paquete de tareas para dispositivos iOS

1. En la barra lateral de menús, en **CONFIGURAR**, haga clic en **Paquetes de tareas > iOS**.
2. En la página **Paquetes de tareas** haga clic en **Crear paquetes de tareas**.
   Aparece la página **Editar paquete de tareas**.
3. En los campos correspondientes, especifique un nombre y, opcionalmente, una descripción para el nuevo paquete de tareas.

   La versión se incrementa automáticamente cada vez que se guarda el paquete de tareas.
4. Opcional: Seleccione **Seleccionable para acciones de cumplimiento** para transferir el paquete de tareas a un dispositivo cuando infrinja una regla de cumplimiento. Consulte Políticas de cumplimiento (página 18).

   Nota
   Esta opción se desactiva cuando se edita un paquete de tareas existente y el paquete de tareas ya se utiliza como acción de cumplimiento.

5. Opcional: Seleccione **Ignorar errores de instalación de apps** para seguir procesando el paquete de tareas aunque no se pueda instalar una aplicación.

   Esta opción se desactiva cuando el paquete de tareas no tiene una tarea **Instalar app**.
6. Haga clic en **Crear tarea**, seleccione **Inscribir** e introduzca el nombre de la tarea. Haga clic en **Aplicar** para crear la tarea.

   El nombre que introduzca aquí se mostrará en el portal de autoservicio mientras se procese la tarea.
7. Haga clic en **Crear tarea** de nuevo y seleccione **Instalar perfil o asignar política**. Dé un nombre descriptivo a la tarea, por ejemplo, `Instalar perfil de políticas de contraseña` y seleccione el perfil que ha creado. Haga clic en **Aplicar** para crear la tarea.
8. Si ha configurado perfiles para las opciones de Exchange, VPN o Wi-Fi, repita este paso para cada perfil.
9. Opcional: Añada más tareas al paquete de tareas.

   Sugerencia
   Puede cambiar el orden de instalación de las tareas por medio de las flechas del lado derecho de la lista de tareas.

10. Una vez que haya añadido todas las tareas necesarias al paquete de tareas, haga clic en **Guardar** en la página **Editar paquete de tareas**.

El paquete de tareas está disponible para transferirse. Se muestra en la página **Paquetes de tareas**.

18 Configurar las opciones del portal de autoservicio

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Portal de autoservicio**.
2. Haga clic en **Textos de inscripción** y, a continuación, añada un texto de términos de uso y un texto posterior a la inscripción.

   Cuando asigne estos textos a su configuración del portal de autoservicio, se mostrarán antes y después de la inscripción, respectivamente.
3. En la página **Configuraciones del portal de autoservicio**, haga clic en **Añadir** para crear una configuración.
4. Configure las siguientes opciones:

Opción	Descripción
Nombre	El nombre de la configuración. En el portal de autoservicio, los usuarios seleccionan una configuración por este nombre.
Grupos de usuarios	Haga clic en **Añadir** y, a continuación, introduzca un grupo de usuarios. La configuración se aplica a todos los miembros de ese grupo.
Número máximo de dispositivos	La cantidad máxima de dispositivos que un usuario puede inscribir en el portal de autoservicio.
Acciones	Haga clic en **Mostrar** y, a continuación, seleccione las acciones de administración que un usuario puede realizar en el portal de autoservicio.

5. Haga clic en **Añadir > Android**.
6. En el cuadro de diálogo **Configurar opciones de la plataforma**, configure las siguientes opciones:

Opción	Descripción
Mostrar nombre	El nombre de las opciones de configuración de la plataforma. En el portal de autoservicio, los usuarios seleccionan un tipo de inscripción por este nombre.
Descripción	Una descripción de las opciones de configuración de la plataforma. Esta descripción se muestra en el portal de autoservicio junto al nombre.
Propietario	Seleccione esta opción si los dispositivos inscritos con esta configuración se clasifican como dispositivos corporativos o personales.

Opción	Descripción
Grupo de dispositivos	Seleccione el grupo de dispositivos al que se añaden los dispositivos inscritos.
Paquete de inscripción	Seleccione el paquete de tareas de Android que ha creado.
Términos de uso	Seleccione el texto que mostrar en el portal de autoservicio antes de la inscripción. Deje el campo vacío para no mostrar ningún texto. Los usuarios deben estar de acuerdo con el texto para poder proceder con la inscripción.
Texto tras la inscripción	Seleccione el texto que mostrar en el portal de autoservicio después de la inscripción. Deje el campo vacío para no mostrar ningún texto.

7. Haga clic en **Aplicar** para añadir las opciones de la plataforma a la configuración del portal de autoservicio.
8. Haga clic en **Añadir > iOS** y repita los pasos de configuración que ha realizado para Android.
9. En la página **Editar configuración del portal de autoservicio**, haga clic en **Guardar**.

Siempre existe una configuración predeterminada **Default**. Esta configuración tiene la prioridad más baja, de modo que solo se utiliza cuando ninguna otra configuración coincide con un usuario.

19 Crear un usuario de prueba del portal de autoservicio

Para probar el aprovisionamiento a través del portal de autoservicio, cree una cuenta de usuario del portal de autoservicio para usted. Utilizará esta cuenta para iniciar sesión en el portal de autoservicio y probar la inscripción de dispositivos.

Nota
En este procedimiento se presupone que el cliente se ha creado con administración de usuarios interna. Consulte Crear un cliente (página 9). Para más información acerca de la administración de usuarios externos, consulte la *Guía de superadministrador de Sophos Mobile*.

Para crear una cuenta de usuario de prueba para el portal de autoservicio:

1. En la barra lateral de menús, en **ADMINISTRAR**, haga clic en **Usuarios** y luego haga clic en **Crear usuario**.
2. Configure los datos de la cuenta necesarios.

   Asegúrese de que la opción **Enviar correo de registro** esté seleccionada.
3. Haga clic en **Guardar**.

El usuario se añade a la lista de usuarios del portal de autoservicio y se envía un correo electrónico de registro a la dirección de correo electrónico que haya especificado en los datos de la cuenta.

20 Probar la inscripción de dispositivos a través del portal de autoservicio

Se recomienda que pruebe la inscripción de dispositivos a través del portal de autoservicio antes de ampliar el uso del portal de autoservicio a los usuarios.

Inicie sesión en el portal de autoservicio con la cuenta de usuario de prueba que ha creado en Crear un usuario de prueba del portal de autoservicio (página 28) y realice inscripciones de prueba para todas las plataformas que desee administrar con Sophos Mobile.

21 Importar usuarios a Sophos Mobile

Una vez que haya probado la inscripción de dispositivos a través del portal de autoservicio, puede importar su lista de usuarios a Sophos Mobile.

La importación de usuarios solo es relevante para la administración interna de usuarios. Para la administración externa de usuarios, todos los usuarios que están asignados a un determinado grupo LDAP pueden iniciar sesión en el sistema.

Para más información acerca de la administración de usuarios externos, consulte la *Guía de superadministrador de Sophos Mobile*.

Puede añadir nuevos usuarios al portal de autoservicio importando un archivo de valores separados por comas (CSV) con codificación UTF-8 con hasta 500 usuarios.

Nota
Utilice un editor de texto para editar el archivo CSV. Si utiliza Microsoft Excel, es posible que los valores introducidos no se resuelvan correctamente. Asegúrese de guardar el archivo con la extensión `.csv`.

Sugerencia
En la página **Importar usuarios** hay disponible para descargar un archivo de ejemplo con los nombres y el orden de columnas correctos.

Para importar usuarios desde un archivo CSV:

1. En la barra lateral de menús, en **ADMINISTRAR**, haga clic en **Usuarios** y luego haga clic en **Importar usuarios**.
2. En la página **Importar usuarios**, seleccione **Enviar correos de registro**.
3. Haga clic en **Subir un archivo** y busque el archivo CSV que ha preparado.
   Las entradas se leen desde el archivo y se muestran.
4. Si los datos no tienen el formato correcto o no son coherentes, no es posible importar ninguna parte del archivo. En este caso, lea los mensajes de error que se muestran junto a las entradas afectadas, corrija el contenido el archivo CSV como corresponda y vuelva a subirlo.
5. Haga clic en **Finalizar** para crear las cuentas de usuarios.

Los usuarios se importan y se muestran en la página **Usuarios**. Reciben correos electrónicos con sus credenciales de inicio de sesión para el portal de autoservicio.

22 Usar el asistente **Añadir dispositivo**

Puede inscribir dispositivos nuevos fácilmente con el asistente **Añadir dispositivo**. Ofrece un flujo de trabajo que combina las siguientes tareas:

- Añadir un dispositivo nuevo a Sophos Mobile.
- Opcional: Asignar un usuario al dispositivo.
- Inscribir el dispositivo.
- Opcional: Transferir un paquete de tareas al dispositivo.

1. En la barra lateral de menú, en **ADMINISTRAR**, haga clic en **Dispositivos**, y, a continuación, en **Añadir > Asistente añadir dispositivo**.

   Sugerencia
   También puede iniciar el asistente desde la página **Panel de control** haciendo clic en el widget **Añadir dispositivo**.

2. En la página **Usuario**, puede introducir criterios para buscar el usuario al que estará asignado el dispositivo o seleccionar **Omitir asignación de usuario** para inscribir un dispositivo que todavía no estará asignado a ningún usuario.
3. En la página **Selección de usuario**, seleccione el usuario que corresponda de la lista de usuarios que coincida con sus criterios de búsqueda.
4. En la página **Detalles del dispositivo**, configure las siguientes opciones:

Opción	Descripción
Plataforma	Plataforma del dispositivo. Solo se puede seleccionar una plataforma que esté habilitada para el cliente en el que ha iniciado sesión.
Nombre	Nombre único por el cual Sophos Mobile administrará el dispositivo.
Descripción	Descripción opcional del dispositivo.
Número de teléfono	Número de teléfono opcional. Introduzca el número de teléfono con el formato internacional, p. ej., `+491701234567`.
Dirección de correo electrónico	Dirección de correo electrónico a la que se envían las instrucciones de inscripción. Si está configurada la administración de usuarios para el cliente, es la dirección de correo electrónico del usuario asignado al dispositivo. Si no está configurada la administración de usuarios, introduzca una dirección de correo electrónico aquí.
Propietario	Seleccione el tipo de propietario del dispositivo: **Corporativo** o **Personal**.
Grupo de dispositivos	Seleccione el grupo de dispositivos al que estará asignado el dispositivo. Si aún no ha creado ningún grupo de dispositivos,

Opción	Descripción
	puede seleccionar el grupo de dispositivos **Predeterminado**, que siempre está disponible.

5. En la página **Tipo de inscripción**, elija si desea inscribir el dispositivo o solo el contenedor de Sophos.

   Seleccione **Inscribir dispositivo**.
6. Seleccione el paquete de tareas que ha configurado para la plataforma del dispositivo.
7. En la página **Inscripción**, siga las instrucciones para completar el proceso de inscripción.
8. Cuando la inscripción haya finalizado correctamente, haga clic en **Finalizar**.

Nota

- Una vez realizadas todas las selecciones, puede cerrar el asistente sin tener que esperar a que aparezca el botón **Finalizar**. Se crea y procesa una tarea de inscripción en segundo plano.

23 Glosario

cliente	Un cliente representa un área de gestión separada dentro de Sophos Mobile. Se pueden configurar varios clientes y gestionar los dispositivos de cada cliente de forma independiente. Esto también se conoce como *multitenencia*.
dispositivo	El dispositivo que se va a administrar (p. ej., un teléfono inteligente, una tableta o un dispositivo Windows 10).
inscripción	Registro de un dispositivo con Sophos Mobile.
Almacén empresarial de aplicaciones	Un repositorio de apps alojado en el servidor de Sophos Mobile. El administrador puede utilizar Sophos Mobile Admin para añadir apps al almacén empresarial de aplicaciones. Los usuarios pueden usar entonces la app Sophos Mobile Control para instalar esas apps en sus dispositivos.
aprovisionamiento	El proceso de instalar la app Sophos Mobile Control en un dispositivo.
Portal de autoservicio	Interfaz web que permite a los usuarios inscribir sus propios dispositivos y realizar otras tareas sin tener que contactar con soporte.
Licencia Mobile Advanced	La licencia de tipo Mobile Advanced le permite administrar las apps Sophos Mobile Security, Sophos Secure Workspace y Sophos Secure Email mediante Sophos Mobile.
SMSec	Abreviatura de Sophos Mobile Security.
Cliente de Sophos Mobile	La app Sophos Mobile Control que se instala en los dispositivos administrados por Sophos Mobile.
Consola de Sophos Mobile	La interfaz web que se utiliza para administrar los dispositivos.
Sophos Mobile Security	Una app de seguridad para dispositivos Android. Puede administrar esta app con Sophos Mobile, siempre que haya disponible una licencia de tipo Mobile Advanced y esta esté activada.
Sophos Secure Email	Una app para dispositivos Apple iOS y Android que ofrece un contenedor seguro para gestionar su correo electrónico, calendario y contactos. Puede administrar esta app con Sophos Mobile, siempre que haya disponible una licencia de tipo Mobile Advanced y esta esté activada.
Sophos Secure Workspace	Una app para dispositivos iOS y Android que proporciona un espacio de trabajo seguro en el que se pueden explorar, administrar, editar, compartir, cifrar y descifrar documentos de

	distintos proveedores de almacenamiento o distribuidos por su empresa. Puede administrar esta app con Sophos Mobile, siempre que haya disponible una licencia de tipo Mobile Advanced y esta esté activada.
paquete de tareas	Paquete que se crea para agrupar diversas tareas en una transacción. Puede agrupar todas las tareas necesarias para completar la inscripción y la activación de un dispositivo.

24 Soporte técnico

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

- Visitar la comunidad de Sophos en community.sophos.com/ para consultar casos similares.
- Visitar la base de conocimiento de Sophos en www.sophos.com/es-es/support.aspx.
- Descargar la documentación correspondiente desde www.sophos.com/es-es/support/documentation.aspx.
- Abrir un ticket de incidencia con nuestro equipo de soporte en https://secure2.sophos.com/es-es/support/contact-support/support-query.aspx.

25 Aviso legal