SOPHOS
Security made simple.

Sophos Mobile como servicio

Guía de inicio

Versión del producto: 8.5

Contenido

Acerca de esta guía....1
Pasos clave....2
Cambiar la contraseña....3
Cambiar el nombre de inicio de sesión....4
Activar licencias Mobile Advanced....5
Comprobar sus licencias....6
Configurar las opciones....7
- Configurar las opciones personales....7
- Configurar las políticas de contraseña....8
- Configurar los datos de contacto del soporte técnico....8

Certificados del servicio de notificaciones push de Apple....9
- Requisitos....9
- Crear certificado APNs....9

Proxy EAS independiente....11
- Descargue el instalador de proxy EAS....12
- Instalar el proxy EAS independiente....12
- Configurar el control de acceso al correo electrónico a través de PowerShell....15
- Configurar una conexión al servidor proxy EAS interno....18
- Configurar una conexión al proxy EAS independiente....18

Configurar control de acceso a la red....20
Políticas de cumplimiento....22
- Crear política de cumplimiento....22

Grupos de dispositivos....24
- Crear grupo de dispositivos....24

Empezar a usar políticas de dispositivo....25
Crear paquete de tareas para dispositivos Android....27
Crear paquete de tareas para dispositivos iOS....28
Configurar las opciones del portal de autoservicio....29
Configurar la administración de usuarios....31
Usar la administración de usuarios interna....32
- Crear un usuario de prueba del portal de autoservicio....32
- Probar la inscripción de dispositivos a través del portal de autoservicio....32
- Importar usuarios a Sophos Mobile....32

Usar la administración de usuarios externa....34
- Configurar una conexión de directorio externa....34
- Probar inscripción de dispositivo para usuarios LDAP....36

Usar el asistente **Añadir dispositivo**....37
Glosario....39
Soporte técnico....41
Aviso legal....42

1 Acerca de esta guía

En esta guía se explica cómo configurar Sophos Mobile como servicio para 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 Pasos clave

Para empezar a utilizar Sophos Mobile:

1. Restablezca su contraseña, inicie sesión en Sophos Mobile Admin y cambie su nombre de usuario de administrador.
2. Opcional: Active sus licencias Mobile Advanced para administrar las apps Sophos Mobile Security, Sophos Secure Workspace y Sophos Secure Email.
3. Compruebe sus licencias.
4. 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.
5. Cargue un certificado del servicio de notificaciones push de Apple para administrar dispositivos iOS.
6. Opcional: Configure un proxy EAS independiente para filtrar el tráfico de correo electrónico de los dispositivos administrados a un servidor de correo electrónico.
7. Opcional: Configure la interfaz para sistemas de control de acceso a la red de terceros.
8. Crear políticas de cumplimiento.
9. Cree grupos de dispositivos.
10. Configure los dispositivos.
11. Actualice las opciones del portal de autoservicio.
12. Configure la administración de usuarios.
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.
15. Pruebe la inscripción de dispositivos en el portal de autoservicio.

3 Cambiar la contraseña

Por motivos de seguridad es recomendable que restablezca su contraseña antes de iniciar sesión en Sophos Mobile Admin por primera vez.

1. Abra Sophos Mobile Admin en el navegador web.
2. En el cuadro de diálogo **Iniciar sesión**, haga clic en **¿Ha olvidado la contraseña?**.
3. En el cuadro de diálogo **Restablecer contraseña**, introduzca su información de **Cliente** y **Usuario** recibida en el correo electrónico de activación de su Sophos Mobile como servicio como cuenta de servicio y, a continuación, haga clic en **Restablecer contraseña**.
   Recibirá un mensaje de correo electrónico con un enlace para restablecer la contraseña.
4. Haga clic en el enlace para abrir el cuadro de diálogo **Cambiar contraseña**.
5. Introduzca una contraseña nueva y haga clic en **Cambiar contraseña**.

   A continuación se cambia su contraseña. Recuerde usar esta contraseña la próxima vez que inicie sesión en la consola.

Nota
Recomendamos que modifique las políticas de contraseña para imponer contraseñas más fuertes, p. ej., estableciendo requisitos para el número mínimo de caracteres en minúsculas, mayúsculas o especiales. Consulte Configurar las políticas de contraseña (página 8).

4 Cambiar el nombre de inicio de sesión

Por razones de seguridad recomendamos que cambie su nombre de inicio de sesión la primera vez que inicie sesión en Sophos Mobile Admin.

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Administradores**.
2. Haga clic en su nombre de inicio de sesión.
3. En la página **Editar administrador**, introduzca un valor nuevo en el campo **Nombre de inicio de sesión**.
4. Opcional: Ajuste los valores de los campos restantes:
   - **Nombre**
   - **Apellidos**
   - **Dirección de correo electrónico**
5. Haga clic en **Guardar**.

Los detalles de su cuenta se cambian. Recuerde usar el nuevo nombre de inicio de sesión la próxima vez que inicie sesión en Sophos Mobile Admin.

5 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.

Las licencias de Mobile Advanced se activan en 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.

6 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.
- **Licencias usadas**: Número de licencias en uso.
- **Válida hasta**: Fecha de vencimiento de la licencia.

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

7 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

7.1 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.

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: • **Android** • **Android Things** • **iOS** • **Windows Mobile** (incluye los sistemas operativos Windows Phone 8.1 y Windows 10 Mobile) • **Windows** • **Windows IoT**

Opción	Descripción
	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.

3. Haga clic en **Guardar**.

7.2 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.

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**.

7.3 Configurar los datos de contacto del soporte técnico

Para proporcionar asistencia a los usuarios que tengan preguntas o problemas, puede facilitarles la información de contacto del equipo de soporte técnico.

La información que introduzca aquí aparecerá en la app Sophos Mobile Control y en el portal de autoservicio.

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

8 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.

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

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.

8.1 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)`

8.2 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.
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**.

9 Proxy EAS independiente

Puede configurar un proxy EAS para controlar el acceso de sus dispositivos administrados a un servidor de correo electrónico. El tráfico de correo electrónico de sus dispositivos administrados se enruta a través de ese proxy. Puede bloquear el acceso al correo electrónico para los dispositivos, por ejemplo, un dispositivo que infrinja una regla de cumplimimento.

Los dispositivos deben estar configurados para usar el proxy EAS como servidor de correo electrónico para los correos entrantes y salientes. El proxy EAS solo reenviará el tráfico al servidor de correo electrónico actual si el dispositivo es reconocido por Sophos Mobile y cumple las políticas exigidas. Esto garantiza un nivel de seguridad más alto ya que el servidor de correo electrónico no necesita estar accesible desde Internet y solo los dispositivos autorizados (configurados correctamente, por ejemplo mediante directrices de código de acceso) pueden acceder a él. Además, también es posible configurar el proxy EAS para que bloquee el acceso desde dispositivos específicos.

El proxy EAS independiente se descarga e instala separadamente de Sophos Mobile. Se comunica con el servidor de Sophos Mobile a través de una interfaz web HTTPS.

Nota
Dado que macOS no admite el protocolo ActiveSync, no se puede utilizar el proxy de EAS interno o independiente para filtrar el tráfico de correo electrónico procedente de equipos Mac.

Funciones

- Soporte para múltiples servidores de correo electrónico de Microsoft Exchange o IBM Notes Traveler. Puede configurar una instancia del proxy EAS por servidor de correo electrónico.
- Compatibilidad con equilibrador de carga. Puede configurar instancias de proxy EAS independientes en varios equipos y luego usar un equilibrador de carga para distribuir las solicitudes de los clientes entre ellas.
- Compatibilidad con autenticación de clientes basada en certificados. Puede seleccionar un certificado de una autoridad de certificación (CA) de la cual deban derivarse los certificados de los clientes.
- Soporte para el control de acceso al correo electrónico a través de PowerShell. En este caso, el servicio de proxy EAS se comunica con el servidor de correo electrónico a través de PowerShell para controlar el acceso al correo electrónico de sus dispositivos administrados. El tráfico de correo electrónico se produce directamente desde los dispositivos al servidor de correo electrónico y no se enruta a través de un proxy. Consulte Configurar el control de acceso al correo electrónico a través de PowerShell (página 15).

Nota
Para los dispositivos que no son iOS, las capacidades de filtrado del proxy EAS independiente son limitadas debido a las características específicas del protocolo de IBM Notes Traveler. Los clientes de Traveler con dispositivos que no sean iOS no envían el ID de dispositivo con cada solicitud. Las solicitudes sin un ID de dispositivo se siguen reenviando al servidor de Traveler, aunque el proxy EAS no pueda comprobar que el dispositivo esté autorizado.

9.1 Descargue el instalador de proxy EAS

1. Iniciar sesión en Sophos Mobile Admin.
2. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Proxy EAS**.
3. En **Externo**, haga clic en el enlace para descargar el instalador del proxy EAS.

El archivo del instalador se guarda en su ordenador local.

9.2 Instalar el proxy EAS independiente

Requisitos previos:

- Todos los servidores de correo electrónico necesarios están accesibles. El instalador del proxy EAS no configurará conexiones a los servidores que no estén disponibles.
- Es administrador del ordenador en el que instala el proxy EAS.

Nota
La Guía de distribución del servidor de Sophos Mobile contiene diagramas esquemáticos para la integración del proxy EAS independiente en la infraestructura de su empresa. Recomendamos que lea esta información antes de realizar la instalación y el despliegue del proxy EAS independiente.

1. Ejecute `Sophos Mobile EAS Proxy Setup.exe` para iniciar el **Sophos Mobile EAS Proxy - Setup Wizard**.
2. En la página **Choose Install Location**, elija la carpeta de destino y haga clic en **Install** para iniciar la instalación.
   Una vez que se haya completado la instalación, se iniciará automáticamente el **Sophos Mobile EAS Proxy - Configuration Wizard**, que le guiará durante los pasos de configuración.
3. En el cuadro de diálogo **Sophos Mobile server configuration**, introduzca la URL del servidor SMC al que se conectará el proxy EAS.

   También es recomendable que seleccione **Use SSL for incoming connections (Clients to EAS Proxy)** para asegurar la comunicación entre clientes y el proxy EAS.

   Puede seleccionar **Use client certificates for authentication** si desea que los clientes usen un certificado además de las credenciales del proxy EAS para la autenticación. Esto añade un nivel adicional de seguridad a la conexión.

   Seleccione **Allow all certificates** si su servidor de Sophos Mobile presenta diferentes certificados al proxy EAS, por ejemplo, porque hay varias instancias del servidor detrás de un equilibrador de carga y cada instancia utiliza un certificado distinto. Cuando esta opción está seleccionada, el proxy EAS aceptará cualquier certificado del servidor de Sophos Mobile.

   Importante
   Puesto que la opción **Allow all certificates** reduce el nivel de seguridad de la comunicación con el servidor, es muy recomendable que la seleccione solo si es imprescindible en su entorno de red.

4. Si ha seleccionado **Use SSL for incoming connections (Clients to EAS Proxy)** antes, se mostrará la página **Configure server certificate**. En esta página puede crear o importar un certificado para el acceso seguro (HTTPS) al proxy EAS.

   Nota
   Puede descargar el asistente de certificado SSL de MySophos para solicitar su certificado SSL/TLS para el proxy EAS de Sophos Mobile.

   Para obtener información general sobre cómo descargar el software de Sophos, consulte el artículo 111195 de la base de conocimiento.

   - Si todavía no tiene un certificado de confianza, seleccione **Create self-signed certificate**.
   - Si tiene un certificado de confianza, haga clic en **Import a certificate from a trusted issuer** y seleccione una de las opciones de importación de la lista:
     - **PKCS12 with certificate, private key and certificate chain (intermediate and CA)**
     - **Separate files for certificate, private key, intermediate and CA certificate**
5. En la siguiente página, introduzca la información de certificado pertinente, dependiendo del tipo de certificado que haya seleccionado.

   Nota
   Para un certificado autofirmado, deberá especificar un servidor al que se pueda acceder desde los dispositivos de los clientes.

6. Si ha seleccionado **Use client certificates for authentication**antes, se mostrará la página **SMC client authentication configuration**. En esta página, selecciona un certificado de una autoridad de certificación (CA), del cual deben derivarse los certificados de los clientes.

   Cuando un cliente intenta conectarse, el proxy EAS comprobará si el certificado que el cliente proporciona está derivado de la CA que ha especificado aquí.
7. En la página **EAS Proxy instance setup**, configure una o varias instancias del proxy EAS.
   - **Instance type**: Seleccione **EAS proxy**.
   - **Instance name**: Nombre para identificar la instancia.
   - **Server port**: Puerto del proxy EAS para el tráfico de correo electrónico entrante. Si configura más de una instancia de proxy, cada una de ellas debe usar un puerto diferente.
   - **Require client certificate authentication**: Los clientes de correo electrónico deben autenticarse cuando se conecten al proxy EAS.
   - **ActiveSync server**: Nombre o dirección IP de la instancia del servidor de Exchange ActiveSync con el que se conectará la instancia de proxy.
   - **SSL**: La comunicación entre la instancia de proxy y el servidor de Exchange ActiveSync está protegida mediante SSL o TLS (en función de lo que admita el servidor).
   - **Allow EWS subscription requests from Secure Email**: Seleccione esta opción para permitir que la app Sophos Secure Email en iOS se suscriba a las notificaciones push mediante los servicios Web Exchange (EWS). Las notificaciones push informan al dispositivo cuando hay mensajes para Secure Email.

Nota

— Por defecto, el proxy EAS bloquea todas las solicitudes a la interfaz EWS del servidor de Exchange por motivos de seguridad. Al seleccionar esta casilla, se permitirán las solicitudes de suscripción. El resto de solicitudes seguirán bloqueándose.

— Para obtener información sobre cómo configurar EWS para el servidor de Exchange, consulte el artículo 127137 de la base de conocimiento de Sophos.

- **Enable Traveler client access**: Solo debe seleccionar esta opción si necesita permitir el acceso de los clientes de IBM Notes Traveler en dispositivos que no son iOS.

8. Después de introducir la información de la instancia, haga clic en **Add** para añadir la instancia a la lista **Instances**.

   Para cada instancia de proxy, el instalador crea un certificado que necesitará cargar al servidor de Sophos Mobile. Después de hacer clic en **Add**, se abre una ventana de mensaje en la que se explica cómo cargar el certificado.
9. En la ventana de mensaje, haga clic en **OK**.
   Se abrirá un cuadro de diálogo en el que se muestra la carpeta en la que se ha creado el certificado.

   Nota
   También puede abrir el cuadro de diálogo seleccionando la instancia pertinente y haciendo clic en el enlace **Export config and upload to Sophos Mobile server** en la página **EAS Proxy instance setup**.

10. Tome nota de la carpeta del certificado. Necesitará esta información cuando cargue el certificado en Sophos Mobile.
11. Opcional: Haga clic en **Add** otra vez para configurar más instancias de proxy EAS.
12. Cuando haya configurado todas las instancias de proxy EAS necesarias, haga clic en **Next**.
    Se probarán los puertos de servidor que ha introducido y se configurarán las reglas de tráfico entrante para el firewall de Windows.
13. En la página **Allowed mail user agents**, puede especificar los agentes de usuario de correo (por ejemplo, las aplicaciones cliente de correo electrónico) a los que se permite conectarse al proxy EAS. Cuando un cliente se conecta al proxy EAS utilizando una aplicación de correo electrónico que no está especificada, se rechazará la solicitud.
    - Seleccione **Allow all mail user agents** para no establecer restricciones.
    - Seleccione **Only allow the specified mail user agents** y luego seleccione un agente de usuario de correo de la lista. Haga clic en **Add** para añadir la entrada a la lista de agentes permitidos. Repita este procedimiento para todos los agentes de usuario de correo a los que se permita conectarse al proxy EAS.
14. En la página **Sophos Mobile EAS Proxy - Configuration Wizard finished**, haga clic en **Finish** para cerrar el asistente de configuración y volver al asistente de instalación.
15. En el asistente de instalación, asegúrese de que la casilla **Start Sophos Mobile EAS Proxy server now** esté seleccionada; a continuación, haga clic en **Finish** para completar la configuración e iniciar el proxy EAS de Sophos Mobile por primera vez.

Para finalizar la configuración del proxy EAS, cargue los certificados que se han creado para cada instancia de proxy a Sophos Mobile:

16. Iniciar sesión en Sophos Mobile Admin.
17. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Proxy EAS**.

18. En **Externo**, haga clic en **Cargar un archivo**. Cargue el certificado que ha creado el asistente de instalación para la conexión de PowerShell.

    Si ha configurado más de una instancia, repita este paso para todos los certificados de instancias.
19. Haga clic en **Guardar**.
20. En Windows, abra el cuadro de diálogo **Servicios** y reinicie el servicio **EASProxy**.
21. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Proxy EAS**.
22. En **Externo**, haga clic en **Cargar un archivo**. Cargue el certificado que ha creado el asistente de instalación para la conexión de PowerShell.

    Si ha configurado más de una instancia, repita este paso para todos los certificados de instancias.
23. Haga clic en **Guardar**.
24. En Windows, abra el cuadro de diálogo **Servicios** y reinicie el servicio **EASProxy**.

Con esto finaliza la configuración inicial del proxy EAS independiente.

Nota
Cada día, las entradas del registro del proxy EAS se mueven a un nuevo archivo, usando el patrón de nomenclatura `EASProxy.log.aaaa-mm-dd`. Estos archivos de registro diarios no se eliminan automáticamente y por tanto pueden causar problemas de espacio en el disco con el tiempo. Le recomendamos que configure un proceso para mover los archivos de registro a una ubicación de copia de seguridad.

9.3 Configurar el control de acceso al correo electrónico a través de PowerShell

Puede configurar una conexión de PowerShell a un servidor Exchange u Office 365. Esto significa que el servicio de proxy EAS se comunica con el servidor de correo electrónico a través de PowerShell para controlar el acceso al correo electrónico para sus dispositivos administrados. El tráfico de correo electrónico se enruta directamente desde los dispositivos al servidor de correo electrónico. No se enruta a través de un proxy.

Nota
Dado que macOS no admite el protocolo ActiveSync, no se puede utilizar PowerShell para controlar el acceso al correo electrónico por parte de los equipos Mac.

El entorno de PowerShell tiene estas ventajas:

- Los dispositivos se comunican directamente con el servidor de Exchange.
- No necesita abrir ningún puerto en su servidor para el tráfico de correo electrónico entrante desde sus dispositivos administrados.

Los servidores de correo electrónico admitidos son:

- Exchange Server 2013
- Exchange Server 2016
- Office 365 con un plan Exchange Online

Para configurar PowerShell:

1. Configure PowerShell.

2. Cree una cuenta de servicio en el servidor de Exchange u Office 365. Sophos Mobile utilizará esta cuenta para ejecutar comandos de PowerShell.
3. Configure una o varias instancias de conexión de PowerShell para Exchange u Office 365.
4. Cargue los certificados de instancias a Sophos Mobile.

Configurar PowerShell

1. En el ordenador en el que va a instalar el proxy EAS, abra Windows PowerShell como administrador y escriba:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Nota
Si PowerShell no está disponible, instálelo según se describe en el artículo de Microsoft Instalación de Windows PowerShell (enlace externo).

2. Si desea conectarse a un servidor de Exchange local, abra Windows PowerShell como administrador en ese ordenador y escriba el mismo comando que antes:

```
PS C:\Windows\system32> Set-ExecutionPolicy RemoteSigned
```

Nota
Este paso no es necesario para Office 365.

Crear una cuenta de servicio

3. Inicie sesión en la consola de administración relevante:
   - Para Exchange Server 2013/2016: **Centro de administración de Exchange**
   - Para Office 365: **Centro de administración de Office 365**
4. Cree una cuenta de usuario. Sophos Mobile utilizará esta cuenta como cuenta de servicio para ejecutar comandos de PowerShell.
   - Utilice un nombre de usuario como `smc_powershell` que identifique el propósito de la cuenta.
   - Desactive la opción para hacer que el usuario cambie su contraseña la próxima vez que inicie sesión.
   - Elimine cualquier licencia de Office 365 que se haya asignado automáticamente a la nueva cuenta. Las cuentas de servicio no requieren ninguna licencia.
5. Cree un nuevo grupo de roles y asígnelo a los permisos requeridos.
   - Utilice un nombre de grupo de roles como `smc_powershell`.
   - Añada los roles **Mail Recipients** y **Organization Client Access**.
   - Añada la cuenta de servicio como miembro.

Configurar conexiones de PowerShell

6. Utilice el asistente de instalación como si fuera a configurar un proxy EAS independiente. En la página del asistente **EAS Proxy instance setup**, configure las siguientes opciones:
   - **Instance type**: Seleccione **PowerShell Exchange/Office 365**.
   - **Instance name**: Nombre para identificar la instancia.

- **Exchange server**: Nombre o dirección IP del servidor de Exchange (para la instalación de un servidor de Exchange local) u `outlook.office365.com` (para Office 365). No incluya un prefijo `https://` ni un sufijo `/powershell`. Se añaden automáticamente.
- **Allow all certificates**: El certificado que presenta el servidor de Exchange no es verificado. Utilice esta opción, por ejemplo, si tiene un certificado autofirmado instalado en su servidor de Exchange. Puesto que la opción **Allow all certificates** reduce el nivel de seguridad de la comunicación con el servidor, es muy recomendable que la seleccione solo si es imprescindible en su entorno de red.
- **Allow EWS subscription requests from Secure Email**: Seleccione esta opción para permitir que la app Sophos Secure Email en iOS se suscriba a las notificaciones push mediante los servicios Web Exchange (EWS). Las notificaciones push informan al dispositivo cuando hay mensajes para Secure Email.

  Nota
  - Por defecto, el proxy EAS bloquea todas las solicitudes a la interfaz EWS del servidor de Exchange por motivos de seguridad. Al seleccionar esta casilla, se permitirán las solicitudes de suscripción. El resto de solicitudes seguirán bloqueándose.
  - Para obtener información sobre cómo configurar EWS para el servidor de Exchange, consulte el artículo 127137 de la base de conocimiento de Sophos.

- **Service account**: Nombre de la cuenta de usuario que ha creado en la consola de administración de Exchange u Office 365.
- **Password**: Contraseña de la cuenta de usuario.

7. Haga clic en **Add** para añadir la instancia a la lista **Instances**.
8. Opcional: Repita los pasos anteriores para configurar las conexiones de PowerShell a otros servidores de Exchange u Office 365.
9. Complete el asistente de instalación según se describe en Instalar el proxy EAS independiente (página 12).

Cargar certificados

10. Iniciar sesión en Sophos Mobile Admin.
11. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Proxy EAS**.
12. Opcional: En **General**, seleccione **Restringir a Sophos Secure Email** para limitar el acceso al correo electrónico a la app Sophos Secure Email, disponible para Android e iOS.

    Esto impide que otras aplicaciones de correo electrónico se conecten a su servidor de correo.
13. En **Externo**, haga clic en **Cargar un archivo**. Cargue el certificado que ha creado el asistente de instalación para la conexión de PowerShell.

    Si ha configurado más de una instancia, repita este paso para todos los certificados de instancias.
14. Haga clic en **Guardar**.
15. En Windows, abra el cuadro de diálogo **Servicios** y reinicie el servicio **EASProxy**.

Con esto finaliza la configuración inicial de las conexiones de PowerShell. El tráfico de correo electrónico entre un dispositivo administrado y los servidores de Exchange u Office 365 se bloquea si el dispositivo infringe una regla de cumplimiento. Puede bloquear un dispositivo individual estableciendo el modo de acceso al correo electrónico para ese dispositivo en **Deny**.

Nota
En función de la configuración de su servidor de Exchange, los dispositivos reciben una notificación cuando se bloquea su acceso al correo electrónico.

9.4 Configurar una conexión al servidor proxy EAS interno

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Proxy EAS**.
2. Opcional: En **General**, seleccione **Restringir a Sophos Secure Email** para limitar el acceso al correo electrónico a la app Sophos Secure Email, disponible para Android e iOS.
   Esto impide que otras aplicaciones de correo electrónico se conecten a su servidor de correo.
3. En **Interno**, introduzca la URL del servidor de groupware o Exchange en el campo de texto **URL de servidor de Exchange/groupware**.
4. Seleccione **Usar SSL/TLS** para utilizar una conexión segura.
5. Seleccione **Permitir solicitudes de suscripción EWS de Secure Email** para permitir que la app Sophos Secure Email en iOS se suscriba a las notificaciones push mediante los servicios Web Exchange (EWS). Las notificaciones push informan al dispositivo cuando hay mensajes para Secure Email.

   Nota
   - Por defecto, el proxy EAS bloquea todas las solicitudes a la interfaz EWS del servidor de Exchange por motivos de seguridad. Al seleccionar esta casilla, se permitirán las solicitudes de suscripción. El resto de solicitudes seguirán bloqueándose.
   - Para obtener información sobre cómo configurar EWS para el servidor de Exchange, consulte el artículo 127137 de la base de conocimiento de Sophos.

6. Haga clic en **Comprobar conexión** para probar la conexión.
   Se mostrará un mensaje si se puede acceder al servidor.
7. Haga clic en **Guardar**.

9.5 Configurar una conexión al proxy EAS independiente

Para configurar la conexión entre Sophos Mobile y el proxy EAS independiente, se carga el certificado del servidor proxy EAS a Sophos Mobile. El certificado se generó cuando configuró la instancia de proxy EAS.

Importante
Si el servicio de proxy EAS se inicia antes de que haya cargado el certificado, Sophos Mobile rechaza la conexión al servidor y el servicio no consigue iniciarse.

Para cargar el certificado del proxy EAS independiente:

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Proxy EAS**.
2. Opcional: En **General**, seleccione **Restringir a Sophos Secure Email** para limitar el acceso al correo electrónico a la app Sophos Secure Email, disponible para Android e iOS.

   Esto impide que otras aplicaciones de correo electrónico se conecten a su servidor de correo.
3. En **Externo**, haga clic en **Subir un archivo** y vaya al archivo de certificado.

   Si ha configurado más de una instancia de proxy EAS, repita este paso para todas las instancias.
4. Haga clic en **Guardar**.
5. En Windows, abra el cuadro de diálogo **Servicios** y reinicie el servicio **EASProxy**.

10 Configurar control de acceso a la red

Sophos Mobile incluye una interfaz para sistemas de control de acceso a la red (NAC) de terceros. Mediante la configuración de conexiones a sistemas NAC, se le permite a los mismos obtener una lista de dispositivos y sus estados de cumplimiento. Además, cuando se configura el control de acceso a la red según se describe en esta sección, puede definir posteriormente una política de cumplimiento que deniegue el acceso a la red cuando se infrinjan determinadas reglas de cumplimiento.

Para obtener más información sobre cómo definir políticas de cumplimiento, consulte la Ayuda de administrador de Sophos Mobile.

Para configurar el control de acceso a la red:

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Control de acceso a la red**.
2. Seleccione una de las integraciones NAC disponibles de la lista:

   - **Sophos UTM**

     Esta opción permite la integración de Sophos UTM (para la versión 9.2 y superiores). La integración requiere establecer la URL del servidor de SMC y las credenciales del usuario administrador en la interfaz WebAdmin de Sophos UTM, en **Administración > Sophos Mobile**. Para obtener más detalles, consulte la *Guía de administración de Sophos UTM*.

   - **Cisco ISE**

     Esta opción permite la integración de Cisco ISE. Configure las siguientes opciones:

Nombre de usuario	El nombre de usuario que se debe especificar en Cisco ISE. Este es usado por Cisco ISE para iniciar sesión en Sophos Mobile.
Contraseña	Introduzca una contraseña para iniciar sesión en Sophos Mobile.
Confirmación de contraseña	Repita la contraseña.
Página de redirección para dispositivos bloqueados	Una URL a la que se redireccionan los dispositivos si no se les permite acceder a la red. Recomendamos que use la URL del portal de autoservicio o la de una página de información con un enlace al portal de autoservicio.

     En Cisco ISE, debe configurar las opciones correspondientes de forma que use la URL del servidor Sophos Mobile y las credenciales introducidas aquí al conectarse a la interfaz NAC.

   - **Check Point**

     Esta opción permite la integración de Check Point (para la versión R77.10 y superiores). Configure las siguientes opciones:

Nombre de usuario	El nombre de usuario que se debe especificar en Check Point. Este es usado por Check Point para iniciar sesión en Sophos Mobile.

Contraseña	Introduzca una contraseña para iniciar sesión en Sophos Mobile.
Confirmación de contraseña	Repita la contraseña.

En Check Point Mobile Access Gateway, debe configurar algunas opciones específicas, según se describe en el artículo del Check Point Support Center MDM cooperative enforcement for Mobile clients.

- **Servicio web**

  Esta opción le permite conectar un sistema NAC de terceros a la interfaz del servicio web.

  Sophos Mobile ofrece una interfaz de servicio web RESTful que proporciona direcciones MAC y el estado de acceso a la red de los dispositivos administrados.

  Un sistema NAC de terceros puede conectarse a esa interfaz usando las credenciales de inicio de sesión de una cuenta de administrador de Sophos Mobile.

  Para los detalles de implementación de la interfaz de servicio web consulte la Guía de interfaz de Sophos Mobile Network Access Control.

- **Personalizado**

  Esta opción le permite configurar un acceso basado en certificado a la interfaz NAC.

  Nota
  La opción heredada **Personalizado** ha quedado obsoleta y se eliminará en una próxima versión. Utilice en cambio la opción **Servicio web** para conectar un sistema NAC de terceros a Sophos Mobile.

  Haga clic en **Subir un archivo** y busque el certificado del sistema NAC de terceros. El certificado se carga y se muestra en una tabla.

  Un sistema NAC de terceros que presente el certificado al servidor de Sophos Mobile obtendrá acceso a la interfaz NAC.

3. En la ficha **Control de acceso a la red**, haga clic en **Guardar**.

11 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.

11.1 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 ha configurado una conexión al proxy EAS independiente. Consulte Configurar una conexión al proxy EAS independiente (página 18). 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 ha configurado el control de acceso a la red. Consulte Configurar control de acceso a la red (página 20). 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.

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.

12 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.

12.1 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**.

13 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 **Email**, 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**.

14 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 22).

   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**.

15 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 22).

   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**.

16 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 instalación.

   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. Este nombre aparece en el portal de autoservicio cuando los usuarios deben seleccionar un tipo de inscripción.
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.

17 Configurar la administración de usuarios

Sophos Mobile ofrece dos métodos distintos de administración de cuentas de usuario para Sophos Mobile Admin y el portal de autoservicio:

- La administración de usuarios interna permite crear usuarios añadiéndolos manualmente en Sophos Mobile Admin o importándolos desde un archivo de valores separados por comas (CSV).
- Si usa una administración de usuarios externa, puede conectarse a un directorio LDAP existente y asignar dispositivos a grupos y perfiles basándose en la pertenencia a directorios.

Nota

- No es posible cambiar el método de administración de usuarios una vez asignados los dispositivos a los usuarios.
- Para la administración de usuarios externa, es obligatorio que haya disponible un entorno LDAPS (LDAP sobre SSL/TLS). Sophos Mobile se conecta al servidor LDAP utilizando el puerto LDAPS por defecto 636.

Para seleccionar el método de administración de usuarios:

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Configuración de usuario**.
2. Seleccione el origen de datos de las cuentas de usuario para Sophos Mobile Admin y el portal de autoservicio (SSP):
   - Seleccione **Directorio interno** para usar la administración de usuarios interna.
   - Seleccione **Directorio LDAP externo** para usar la administración externa en lugar de o en combinación con la administración de usuarios interna.
3. Si selecciona **Directorio LDAP externo**, haga clic en **Configurar LDAP externo** para especificar los detalles del servidor. Consulte Configurar una conexión de directorio externa (página 34).
4. Haga clic en **Guardar**.

Nota

Tras guardar la configuración solo estará disponible el método de administración de usuarios seleccionado en la ficha **Configuración de usuario**. Para cambiar su selección posteriormente, seleccione y guarde **Ninguno**. **No hay disponibles administradores de LDAP, perfiles específicos de usuario ni SSP** primero para que todas las opciones vuelvan a estar disponibles.

18 Usar la administración de usuarios interna

18.1 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.

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.

18.2 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 32) y realice inscripciones de prueba para todas las plataformas que desee administrar con Sophos Mobile.

18.3 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.

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.

19 Usar la administración de usuarios externa

19.1 Configurar una conexión de directorio externa

Cuando usa un directorio LDAP externo para la administración de cuentas de usuario para Sophos Mobile Admin y el portal de autoservicio, debe configurar la conexión del directorio de forma que Sophos Mobile pueda recuperar los datos de usuario del servidor LDAP.

Nota
No hay sincronización entre el directorio de LDAP y Sophos Mobile. Sophos Mobile solo accede al directorio de LDAP para buscar información de usuario. Los cambios que se hagan en una cuenta de usuario LDAP no se implementan en la base de datos de Sophos Mobile, y viceversa.

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración del sistema** y, a continuación, haga clic en la ficha **Configuración de usuario**.
2. Seleccione **Directorio LDAP externo**.
3. Haga clic en **Configurar LDAP externo** para especificar los datos del servidor.
4. En la página **Detalles del servidor**, configure las siguientes opciones:
   a) En el campo **Tipo LDAP**, seleccione el tipo de servidor LDAP:
      - **Active Directory**
      - **IBM Domino**
      - **NetIQ eDirectory**
      - **Red Hat Directory Server**
      - **Zimbra**

   b) En el campo **URL principal**, escriba la URL del servidor de directorio primario. Es posible introducir la IP del servidor o el nombre del servidor. Seleccione **SSL/TLS** para proteger la conexión del servidor mediante SSL o TLS (en función de lo que admita el servidor). Para Sophos Mobile como servicio, no se puede deseleccionar **SSL/TLS**.

   c) Opcional: En el campo **URL secundaria**, escriba la URL de un servidor de directorio que se utilice como alternativa si no se puede acceder al servidor primario. Es posible introducir la IP del servidor o el nombre del servidor. Seleccione **SSL/TLS** para proteger la conexión del servidor mediante SSL o TLS (en función de lo que admita el servidor). Para Sophos Mobile como servicio, no se puede deseleccionar **SSL/TLS**.

   d) En el campo **Usuario**, introduzca una cuenta para operaciones de búsqueda en el servidor del directorio. Sophos Mobile utiliza las credenciales de la cuenta cuando se conecta al servidor del directorio.

      Con Active Directory también debe introducir el dominio correspondiente. Los formatos compatibles son:

      - `<dominio>\<nombre de usuario>`
      - `<nombre de usuario>@<dominio>.<código de dominio>`

Nota
Por razones de seguridad, recomendamos que se especifique un usuario que solo tenga permisos de lectura para el servidor del directorio y no permisos de escritura.

e) En el campo **Contraseña**, escriba la contraseña del usuario.

Haga clic en **Siguiente**.

5. En la página **Base de búsqueda**, introduzca el nombre distintivo (DN) del objeto de la base de búsqueda.

   El objeto de base de búsqueda define la ubicación en el directorio externo desde la que se inicia la búsqueda del usuario o grupo de usuarios.

6. En la página **Campos de búsqueda**, defina los campos de directorio que se vayan a usar para resolver las variables *%_USERNAME_%* y *%_EMAILADDRESS_%* en los perfiles y políticas. Escriba los campos requeridos o selecciónelos de las listas **Nombre de usuario** y **Correo electrónico**.

   Nota
   Las listas solo contienen los campos configurados para el usuario conectado en ese momento al directorio LDAP, especificado en el paso 4.d (página 34) anterior. Si, p. ej., no se ha configurado un campo de correo electrónico para ese usuario, es necesario que introduzca manualmente el valor requerido en el campo **Correo electrónico**.

   En el caso de Active Directory, aplican estas asignaciones de campo:

   - **Nombre de usuario**: `sAMAccountName`
   - **Nombre**: `givenName`
   - **Apellidos**: `sn`
   - **Email**: `mail`

7. En la página **Configuración SSP**, especifique los usuarios que pueden iniciar sesión en el portal de autoservicio. Introduzca la información correspondiente en el campo **Grupo del directorio LDAP**, usando una de las opciones siguientes:

   - Si introduce el nombre de un grupo que está definido en el servidor del directorio, todos los miembros de ese grupo pueden iniciar sesión en el portal de autoservicio. Una vez introducido el nombre del grupo, haga clic en **Grupo de prueba** para resolver el nombre de grupo en un nombre distintivo (DN).
   - Si deja el campo vacío, ningún usuario del servidor del directorio podrá iniciar sesión en el portal de autoservicio. Utilice esta opción si quiere permitir la administración externa de usuarios para Sophos Mobile Admin, pero no para el portal de autoservicio.

   Nota
   El grupo especificado aquí no está relacionado con el grupo de usuarios que se define en la ficha **Configuración de grupo** en la página **Portal de autoservicio**. Estas opciones de configuración se usan para definir paquetes de tareas, la pertenencia a grupos de Sophos Mobile y las plataformas de dispositivos disponibles para cada grupo de usuarios.

   Para más información acerca de todas las opciones del grupo de portal de autoservicio, consulte la Ayuda de administrador de Sophos Mobile.

8. Haga clic en **Aplicar**.
9. En la ficha **Configuración de usuario**, haga clic en **Guardar**.

Información relacionada

Cómo conectar un servidor de Sophos Mobile 8.0 con un Azure Active Directory (artículo 128081 de la base de conocimiento de Sophos)

19.2 Probar inscripción de dispositivo para usuarios LDAP

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 sus credenciales LDAP y lleve a cabo pruebas de inscripción en todas las plataformas que desee administrar con Sophos Mobile.

20 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.
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, 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.

   Nota
   En equipos Mac, la inscripción la debe realizar el usuario que será administrado por Sophos Mobile. Para instalar el perfil de inscripción, el usuario debe introducir una contraseña de administrador.

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.

21 Glosario

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.

22 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.

23 Aviso legal