SOPHOS

Cybersecurity made simple.

Sophos Mobile

Guía de inicio (Central)

Versión del producto: 9

Contenido

1 Acerca de este documento

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

Las descripciones se aplican al producto Sophos Mobile en Sophos Central.

Para ver otras versiones de este documento, consulte la página web de documentación de Sophos Mobile.

2 Pasos clave

Para empezar a utilizar Sophos Mobile:

1. Opcional: Active sus licencias Mobile Advanced para administrar las apps Sophos Mobile Security, Sophos Secure Workspace y Sophos Secure Email.
2. Configure las opciones personales, los datos de contacto del soporte técnico y las opciones del portal de autoservicio.
3. Cargue un certificado del servicio de notificaciones push de Apple para administrar dispositivos iPhone, iPad y Mac.
4. Opcional: Configure un proxy EAS independiente para filtrar el tráfico de correo electrónico de los dispositivos administrados a un servidor de correo electrónico.
5. Crear políticas de cumplimiento.
6. Cree grupos de dispositivos.
7. Configure los dispositivos.
8. Actualice las opciones del portal de autoservicio.
9. Pruebe la inscripción de dispositivos en el portal de autoservicio.

3 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 Central Admin:

En Sophos Central Admin, haga clic en el nombre de su cuenta (parte superior derecha de la interfaz de usuario), seleccione **Licencias** e introduzca la clave de licencia en el campo **Aplicar código de activación**.

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

4 Configurar las opciones

Configure las siguientes opciones:

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

4.1 Configurar las opciones personales

Puede ajustar el aspecto de Sophos Mobile Admin a sus preferencias personales. Por ejemplo, puede configurar el idioma, la zona horaria o las plataformas de dispositivos que desea visualizar.

Nota
Esta configuración solo afecta a la cuenta de administrador con la que ha iniciado sesión.

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

Opción	Descripción
Zona horaria	La zona horaria en que se mostrarán las fechas.
Sistema de la unidad	El sistema de la unidad (**Métrica** o **Británica**) para los valores de longitud.
Líneas por página en tablas	El máximo de entradas que se visualizarán por página de tabla.
Modo experto	Esta opción de configuración activa funciones adicionales: • La página **Mostrar dispositivo** incluye la ficha **Propiedades personalizadas** con las propiedades personalizadas de los dispositivos. • La página **Mostrar dispositivo** incluye la ficha **Propiedades internas** junto con las propiedades adicionales notificadas por el dispositivo. • Varias páginas de configuración de políticas incluyen la sección **Configuraciones adicionales** para configurar ajustes opcionales.
Plataformas activadas	Las plataformas de dispositivos que desea visualizar. En Sophos Mobile Admin, solo se muestran las páginas y las opciones relevantes para las plataformas seleccionadas.

3. Haga clic en **Guardar**.

4.2 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 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**.

5 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.

5.1 Crear certificado APNs

1. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración de Apple** 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**.

6 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, puede configurar el proxy EAS para bloquear el acceso desde dispositivos específicos.

El proxy EAS 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 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.
- Soporte para autenticación de cliente basada en certificados. Puede seleccionar un certificado de una autoridad de certificación (CA), del cual deben 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 11).
- El proxy EAS recuerda el estado del dispositivo durante 24 horas. Si el servidor de Sophos Mobile está desconectado, por ejemplo durante una actualización, el tráfico de correo electrónico se filtra en función del último estado del dispositivo conocido. Transcurridas 24 horas, se bloquea todo el tráfico de correo.

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.

6.1 Descargar el instalador de proxy EAS

1. Inicie sesión en Sophos Central Admin y vaya a **Mobile**.
2. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración de Sophos** 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.

6.2 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.
- Introduzca la URL del servidor de Sophos Mobile. Consulte Determinar la dirección URL del servidor de Sophos Mobile (página 14).

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 de Sophos Mobile al que se conectará el proxy EAS.

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

   - 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 antes ha seleccionado la opción **Use client certificates for authentication**, 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 relevante y haciendo clic en el enlace **Export config and upload to Sophos Mobile server** de 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. Inicie sesión en Sophos Central Admin y vaya a **Mobile**.
17. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración de Sophos** y, a continuación, haga clic en la ficha **Proxy EAS**.
18. En **Externo**, haga clic en **Subir un archivo**. Cargue el certificado creado por el asistente de configuración.

    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**.

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.

6.3 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. 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 8).

Cargar certificados

10. Inicie sesión en Sophos Central Admin y vaya a **Mobile**.
11. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración de Sophos** 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 **Subir un archivo**. Cargue el certificado creado por el asistente de configuración.

    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.

6.4 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.

Para obtener información sobre la instalación y la configuración del proxy EAS independiente, consulte Proxy EAS independiente (página 7).

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 de Sophos** 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**.

6.5 Determinar la dirección URL del servidor de Sophos Mobile

Necesita la dirección URL del servidor de Sophos Mobile para configurar el proxy EAS independiente. El valor aparece en la configuración del sistema de Sophos Mobile.

1. Inicie sesión en Sophos Central Admin y vaya a **Mobile**.
2. En la barra lateral de menús, en **AJUSTES**, haga clic en **Configuración > Configuración de Sophos** y, a continuación, haga clic en la ficha **Proxy EAS**.

En **Externo**, se muestra la URL del servidor de Sophos Mobile.

7 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.

7.1 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 13). 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.
Establecer estado	Seleccionar el estado de seguridad (**Rojo**, **Amarillos**, **Verde**) que recibe el dispositivo si infringe esta regla. Si el dispositivo infringe más de una regla, obtiene su estado de seguridad de la regla que esté asociada con el peor estado de seguridad. Sophos Mobile informa del estado de seguridad a Sophos Wireless. En función de la configuración de Sophos Wireless, se restringe el acceso a la red. Esta acción está disponible para dispositivos Android e iOS si ha activado la Seguridad Sincronizada. Consulte .
Crear alerta	Activar una alerta. Las alertas se muestran en la página **Alertas** de Sophos Central Admin.
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 Sophos Mobile Ayuda para el administrador. **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.

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

8 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.

8.1 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 Sophos Mobile Ayuda para el administrador.

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

9 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. Para **Android**, puede seleccionar un modo de administración.

   Esta opción afecta a los tipos de política que están disponibles. Recomendamos que utilice el modo **Android para empresas**.
4. 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**.
5. En la página **Contraseñas**, configure los requisitos para la contraseña del dispositivo.
6. 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.
7. 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.
8. 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.
9. 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**.

Si ha optado por el modo **Android para empresas**, debe configurar Android para empresas para su empresa antes de poder inscribir dispositivos. Consulte la Sophos Mobile Ayuda para el administrador.

10 Crear paquete de tareas para dispositivos Android

1. En la barra lateral de menús, en **CONFIGURAR**, haga clic en**Paquetes de tareasAndroid**.
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 15).

   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**.

11 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 15).

   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**.

12 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	El modo propietario (corporativo o personal) de los dispositivos inscritos con esta configuración.
Grupo de dispositivos	El grupo de dispositivos al que se añade el dispositivo.

Opción	Descripción
Paquete de inscripción	Seleccione el paquete de tareas de Android que ha creado.
Términos de uso	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	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.

13 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 una cuenta de usuario de prueba que ha creado en y realice inscripciones de prueba para todas las plataformas que desee administrar con Sophos Mobile.

14 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
   Si lo prefiere, puede iniciar el asistente de varias formas:

   - En la página **Panel de control**, haga clic en el widget **Añadir dispositivo**.
   - En el menú de Sophos Central Admin, haga clic en **Proteger dispositivos > Iniciar asistente de inscripción de dispositivos**.

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.

   Nota
   Puede buscar cadenas parciales, pero solo partiendo del principio de un campo. Por ejemplo, la cadena de búsqueda `ejemplo` coincidirá con *ejemplo de usuario* y *ejemplo@empresa.com* pero no con *usuario@ejemplo.com*.

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. Es la dirección de correo electrónico del usuario asignado al dispositivo según la configuración de la administración de usuarios de Sophos Central.

Opción	Descripción
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.
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.

15 Glosario

perfil de aprovisionamiento ad hoc	Un perfil de aprovisionamiento de distribución que se añade a una app para iOS desarrollada por el usuario. Esto le permite instalar la app en dispositivos designados sin tener que publicarla en el App Store.
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.
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.
aprovisionamiento	El proceso de instalar la app Sophos Mobile Control en un dispositivo.
SMSec	Abreviatura de Sophos Mobile Security.
Sophos Central Admin	La interfaz web que se utiliza para administrar los dispositivos.
Portal de autoservicio de Sophos Central	Interfaz web que permite a los usuarios inscribir sus propios dispositivos y realizar otras tareas sin tener que contactar con soporte.
Cliente de Sophos Mobile	La app Sophos Mobile Control que se instala en los dispositivos administrados por Sophos Mobile.
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.
Team ID	Todas las apps para iOS y macOS están firmadas por un Team ID. El Team ID lo proporciona Apple y es exclusivo de un equipo de desarrollo específico.

16 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/support/contact-support/support-query.aspx.

17 Aviso legal