SOPHOS

Cybersecurity made simple.

Sophos Mobile

Guía de instalación

Versión del producto: 9.6

Contenido

Acerca de esta guía....1
Acerca de Sophos Mobile....2
Licencias Sophos Mobile....3
- Licencias de evaluación....3
- Actualizar las licencias de evaluación a licencias completas....3
- Actualizar licencias....3

Configurar Sophos Mobile....4
- Requisitos previos de instalación....4
- Requisitos del entorno del sistema....5
- Solicitar un certificado SSL/TLS....5
- Instalar y configurar el servidor de Sophos Mobile....6
- Configurar el servidor web de Sophos Mobile....9
- Cambiar el idioma de inicio de sesión de SQL....10

Proxy EAS independiente....11
- Escenarios de uso para el proxy EAS....12
- Descargar el instalador de proxy EAS....13
- Instalar el proxy EAS independiente....13
- Configurar el control de acceso al correo electrónico a través de PowerShell....16
- Bloquear el acceso al correo electrónico para los dispositivos no administrados....19

Equilibrio de carga y alta disponibilidad....21
- Requisitos....21
- Configurar nodos de clúster....22
- Configurar el equilibrio de carga con Sophos UTM....23

Actualizar Sophos Mobile....26
- Actualizar servidor Sophos Mobile....26
- Tareas posteriores a la actualización....26
- Actualizar un clúster de servidores....26
- Actualizar proxy EAS independiente....27

Referencia técnica....28
- Características del servidor de Sophos Mobile....28
- Interfaces web de Sophos Mobile....28

Soporte....30
Aviso legal....31

1 Acerca de esta guía

Esta guía explica cómo instalar y configurar Sophos Mobile 9.6. También describe cómo actualizar una instalación existente de Sophos Mobile.

A no ser que se especifique lo contrario, todos los procedimientos deben realizarse como administrador de Microsoft Windows Server o como un usuario del grupo pertinente.

2 Acerca de Sophos Mobile

Sophos Mobile

Sophos Mobile es la solución EMM para empresas que desean dedicar menos tiempo y esfuerzo a gestionar y proteger dispositivos móviles. Gestione los dispositivos móviles con Sophos Central, nuestra interfaz de administración web unificada y fácil de utilizar, junto con la protección para estaciones de trabajo, redes o servidores de Sophos. Las apps de contenedor seguro y el soporte para la creación de contenedores de sistema operativo móvil en iOS, iPadOS, Android para empresas y Samsung Knox garantizan que los datos de la empresa permanecen separados de la información personal en el dispositivo.

Sophos Mobile ofrece una inmejorable protección de datos, una seguridad integral, opciones flexibles de gestión y una excelente relación calidad-precio. Además, es la mejor manera de permitir el uso de dispositivos móviles para trabajar, al tiempo que se mantiene la productividad de los usuarios, se protegen los datos profesionales y se preservan los datos personales.

Sophos Intercept X for Mobile

Sophos Intercept X for Mobile protege sus dispositivos móviles sin comprometer el rendimiento ni la duración de la batería. Gracias a la tecnología antimalware líder de Sophos, Sophos Intercept X for Mobile ofrece un nivel galardonado de protección antimalware y antivirus, además de detección de aplicaciones no deseadas, asesores de privacidad y seguridad, protección contra pérdidas y robos, protección web y mucho más.

Sophos Secure Workspace

Sophos Secure Workspace es una app de gestión de contenido móvil de contenedor que ofrece una forma segura de proteger, administrar y distribuir documentos empresariales y contenido web. Edite documentos con formato Office sin salir del entorno de contenedor para garantizar que el contenido cifrado permanezca seguro. La tecnología contra la suplantación de identidad protege a los usuarios de enlaces maliciosos en documentos y contenido.

Cuando la app está gestionada por Sophos Mobile, los administradores pueden limitar fácilmente el acceso al contenido en función de las reglas de cumplimiento del dispositivo. Junto con Sophos SafeGuard Encryption, Sophos Secure Workspace proporciona un intercambio fluido de archivos cifrados, almacenados localmente o en la nube, entre usuarios con Windows, Mac, iPhone, iPad y Android.

Sophos Secure Email

Sophos Secure Email es una app de correo electrónico de contenedor completa y segura que le permite aislar el correo electrónico, el calendario y los contactos de la empresa de los datos privados de un dispositivo móvil cuando se administra con Sophos Mobile. Toda la información de la empresa está protegida mediante cifrado AES-256, y se puede revocar fácilmente el acceso en función de las reglas de cumplimiento del dispositivo. Sophos Secure Email también permite al departamento de TI proveer de correo electrónico corporativo a distintos dispositivos y variaciones de SO de forma segura y uniforme.

3 Licencias Sophos Mobile

Sophos Mobile ofrece dos tipos de licencia:

- Licencia Mobile Standard
- Licencia Mobile Advanced

Con una licencia de tipo Mobile Advanced puede administrar Sophos Intercept X for Mobile, Sophos Secure Workspace y Sophos Secure Email.

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

3.1 Licencias de evaluación

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

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

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

3.2 Actualizar las licencias de evaluación a licencias completas

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

3.3 Actualizar licencias

Para actualizar sus licencias, tiene que activar la nueva clave de licencia en Sophos Mobile Admin.

4 Configurar Sophos Mobile

Esta sección describe cómo instalar un servidor de Sophos Mobile nuevo. Para obtener información sobre cómo actualizar una instalación existente, consulte Actualizar Sophos Mobile (página 26).

4.1 Requisitos previos de instalación

Compruebe los siguientes requisitos previos antes de instalar el servidor de Sophos Mobile:

- Ha leído la Sophos Mobile Guía de distribución del servidor. Este documento contiene ejemplos de arquitectura para la integración del servidor de Sophos Mobile en la infraestructura de su empresa, directrices de dimensionamiento y una lista de los protocolos y puertos de red necesarios.
- Ha leído las Sophos Mobile Notas de la edición y ha comprobado que el equipo que aloja el servidor de Sophos Mobile, los dispositivos que desea gestionar y otros componentes relevantes son compatibles con Sophos Mobile.
- Dispone de un certificado SSL/TLS para el servidor de Sophos Mobile.
- En el equipo servidor no hay instalado ningún servidor web de Internet Information Services (IIS) u otra aplicación que utilice los puertos 80 o 443.
- El nombre DNS del equipo servidor se puede resolver a través de Internet.
- Hay uno o más grupos LDAP que contienen los usuarios con permiso para usar el portal de autoservicio, si las cuentas de usuario están almacenadas en un directorio LDAP.

Requisitos previos si se quiere administrar la base de datos de Sophos Mobile con un servidor de base de datos existente:

- Microsoft SQL Server o Microsoft SQL Server Express:
  - Se utiliza la autenticación de Windows o la autenticación de SQL Server.
  - TCP/IP está activado.
  - Está habilitado el servicio de explorador de SQL Server.
  - El idioma de la cuenta que se utiliza para iniciar sesión en SQL es el inglés.
- Microsoft SQL Server Express:
  - Están instaladas las herramientas de administración de SQL.

Tareas relacionadas

Solicitar un certificado SSL/TLS (página 5)
La entrega de productos Sophos incluye el asistente de certificado SSL para solicitar su certificado SSL/TLS para el proxy de EAS de Sophos Mobile.

Información relacionada

Guía de distribución del servidor de Sophos Mobile

Sophos Mobile Notas de la edición

4.2 Requisitos del entorno del sistema

El programa de instalación de Sophos Mobile realiza una serie de pruebas para verificar que su entorno del sistema cumple todos los requisitos necesarios para Sophos Mobile.

Requisitos obligatorios

El programa de instalación de Sophos Mobile solo se inicia si se cumplen los siguientes requisitos:

- Ha iniciado sesión en el equipo con una cuenta de administrador local.
- El sistema operativo del equipo es compatible con Sophos Mobile.
- El equipo tiene al menos un adaptador de red.
- El equipo tiene al menos 4 GB de RAM.
- El servidor web de Microsoft Internet Information Services (IIS) está deshabilitado en el equipo.
- Los puertos 80, 443 y 818 HTTP/S están disponibles en el equipo.
- El equipo puede conectarse a los siguientes servicios web:
  - Servicio de notificaciones push de Apple (APNs)
  - Google Firebase Cloud Messaging (FCM)
  - Google reCAPTCHA
  - Servicios de notificaciones push de Windows (WNS)
  - Servicios de Sophos

Requisitos opcionales

Algunas características de Sophos Mobile solo están disponibles si su equipo puede conectarse a los siguientes servicios web:

- Programa de compras por volumen (VPP) de Apple
- Apple iTunes
- Omisión de bloqueo de activación de Apple
- Programa de inscripción de dispositivos (DEP) de Apple
- Google Android para empresas
- Microsoft Azure
- TeamViewer

4.3 Solicitar un certificado SSL/TLS

La entrega de productos Sophos incluye el asistente de certificado SSL para solicitar su certificado SSL/TLS para el proxy de EAS de Sophos Mobile.

Ejecute el asistente desde la carpeta *%MDM_HOME%*`\tools\Wizard` o descárguelo desde www.sophos.com/mysophos.

Nota
Si utiliza un certificado autofirmado o un certificado que ha emitido su propia autoridad de certificación (CA), se aplican las restricciones siguientes:

- Debe instalar manualmente el certificado autofirmado o su certificado CA en los dispositivos antes de inscribirlos en Sophos Mobile. De no hacerlo, la app Sophos Mobile Control no confiará en su servidor y rechazará la conexión. Los certificados emitidos por una CA de confianza global no requieren esta instalación manual.
- No puede instalar apps de Android a partir de archivos APK alojados en el servidor de Sophos Mobile.
- No puede utilizar el aprovisionamiento automático de Android ni Samsung Knox Mobile Enrollment.
- Si utiliza un certificado autofirmado que no fue creado por el asistente de configuración o el asistente de certificado SSL de Sophos Mobile, consulte el artículo de Apple Requisitos para certificados de confianza en iOS 13 y MacOS 10.15.

Para solicitar su certificado SSL/TLS:

- Ejecute el archivo `Sophos Mobile SSL Certificate Wizard.exe` para iniciar el asistente de certificado SSL.

  El asistente le guiará en el proceso de instalación. Introduzca la información necesaria siguiendo estas instrucciones:

  a) En la página **Upload CSR**, puede hacer clic en el botón **Open CSR** para abrir el archivo CSR si su proveedor de certificados admite la acción de copiar y pegar.

  b) En la página **Import Certificate Files**, introduzca el certificado de CA descargado en la página **Upload CSR**, en el campo **Select CA certificate file**.

  c) En la página **Certificate created**, aparece la ubicación del certificado creado. Deberá hacer referencia a esta ubicación cuando configure Sophos Mobile.

Nota
Se recomienda que cree una copia de seguridad de la carpeta que contiene los archivos de certificados.

Información relacionada
Requisitos para certificados de confianza en iOS 13 y macOS 10.15 (enlace externo)

4.4 Instalar y configurar el servidor de Sophos Mobile

Requisitos previos:

- Si tiene previsto conectar Sophos Mobile a una base de datos existente, asegúrese de que dispone de las credenciales de inicio de sesión para la base de datos antes de iniciar la instalación y de que cuenta con los permisos suficientes para crear nuevos almacenes de datos, cuentas de usuario y registros de datos.
- Si la base de datos no está alojada de manera local, necesita acceso al puerto de conexión del servidor de la base de datos. Los puertos predeterminados son TCP 1433 para Microsoft

SQL Server y TCP 3306 para MySQL. Asimismo, necesita una cuenta de administrador que el servidor de Sophos Mobile puede usar para acceder a la base de datos.

1. Inicie sesión en Windows con una cuenta de usuario que tenga derechos de administrador local.
2. Inicie el instalador de Sophos Mobile.
3. En la página **System Property Checks**, haga clic en **Check** para realizar pruebas para verificar que su entorno de sistema cumple con todos los requisitos necesarios para Sophos Mobile. Consulte Requisitos del entorno del sistema (página 5).

   Puede hacer clic en **Report** para generar un informe de los resultados de las pruebas.
4. En la página **Choose Install Location**, elija la carpeta de destino para el servidor de Sophos Mobile.
5. En la página **Database Type Selection**, seleccione el tipo de base de datos que desea utilizar:
   - **Install and use Microsoft SQL Server Express**: Instala Microsoft SQL Server Express y lo configura para su uso con Sophos Mobile.
   - **Use existing Microsoft SQL Server installation**: utiliza su instalación existente de Microsoft SQL Server y crea una nueva base de datos para Sophos Mobile.
   - **Use existing MySQL installation**: utiliza su instalación existente de MySQL y crea una nueva base de datos para Sophos Mobile.
6. En la página **Database Settings**, introduzca las credenciales de inicio de sesión para la base de datos.

   Nota
   Si ha seleccionado la opción **Use SQL Server Authentication**, deberá asegurarse de que el idioma de inicio de sesión de SQL está establecido en English. Consulte Cambiar el idioma de inicio de sesión de SQL (página 10) para más información.

7. En la página **Database Selection**, haga clic en **Create a new database named** e introduzca un nombre para la base de datos que se va a crear, por ejemplo SMCDB.
8. En la página **Database Configuration**, se muestran mensajes de progreso durante la creación de la base de datos.
   Cuando la base de datos se haya creado y poblado con éxito, haga clic en **Next** para continuar.
9. Si ha seleccionado la autenticación Windows para el acceso a la base de datos, existe una página llamada **Set service credentials** donde se establece la cuenta de Windows con la que se ejecuta el servicio Sophos Mobile.

   Puede utilizar la cuenta del sistema local o una cuenta de usuario. En el segundo caso, introduzca la cuenta de usuario como `<nombre de equipo>\<nombre de usuario>` o como `<dominio>\<nombre de usuario>`.

   El instalador asignará los derechos de acceso a la base de datos a esa cuenta.

Nota
Por razones de seguridad, le recomendamos que ejecute el servicio Sophos Mobile como usuario con permisos de acceso limitados. La cuenta de usuario debe tener las propiedades siguientes:

- La cuenta de usuario es una cuenta local de Windows en el equipo en el que está instalado Sophos Mobile.
- El usuario no es miembro de ningún grupo, ni siquiera del grupo *usuarios*.
- El usuario puede acceder a la base de datos SQL con los derechos de cambio pertinentes. Para una base de datos MS-SQL, esto quiere decir que el usuario debe ser un miembro de los roles *db_datareader* y *db_datawriter*.

10. En la página **Configure super admin account**, configure los detalles de la cuenta del superadministrador.

    El superadministrador es principalmente para la gestión de clientes y no debe usarse para la gestión rutinaria de dispositivos. El superadministrador inicia sesión en el cliente superadministrador y puede, por ejemplo, predefinir ajustes para nuevos clientes e imponer ajustes y configuraciones a clientes existentes. Para más información, consulte Guía de superadministrador de Sophos Mobile.

    Nota
    Para el primer inicio de sesión en Sophos Mobile Admin se necesitan las credenciales del superadministrador. Después de la instalación, es posible añadir superadministradores adicionales en Sophos Mobile Admin.

11. En la página **Configure external server name**, introduzca un nombre de servidor de Sophos Mobile (por ejemplo smc.mycompany.com).

    Nota
    El nombre del servidor debe poder ser resuelto por los dispositivos administrados.

12. En la página **Configure server certificate**, importe un certificado para el acceso seguro (HTTPS) al servidor web.
    - Si tiene un certificado de confianza, haga clic en **Import a certificate from a trusted issuer** y seleccione una opción de la lista desplegable.
    - Si todavía no tiene un certificado de confianza, seleccione **Create self-signed certificate**.

    Nota
    Su producto de Sophos incluye el asistente de certificado SSL que puede usar para solicitar su certificado SSL/TLS para Sophos Mobile. Consulte Solicitar un certificado SSL/TLS (página 5).

13. En la siguiente página, introduzca la información de certificado pertinente, dependiendo del tipo de certificado que haya seleccionado.

Nota
Para un certificado autofirmado, debe especificar un servidor al que se pueda acceder desde los dispositivos administrados.

14. En la página **Server Information**, verifique la información del servidor y a continuación haga clic en **Next** para confirmar el servidor y el proceso de configuración.
15. Una vez finalizada la instalación, aparecerá el cuadro de diálogo **Sophos Mobile Control - Installation finished**. Asegúrese de que la casilla **Start Sophos Mobile server now** esté seleccionada y haga clic en **Finish** para iniciar el servicio Sophos Mobile por primera vez.

Nota
Una vez que el servicio se ha iniciado, puede tardar unos minutos antes de que la interfaz web de Sophos Mobile esté disponible.

Después de la instalación, debe llevar a cabo algunos pasos de configuración inicial:

- Configure el servidor web de Sophos Mobile para que solo acepte las solicitudes que se dirijan a su nombre de dominio. Consulte Configurar el servidor web de Sophos Mobile (página 9).
- Inicie sesión en Sophos Mobile Admin por primera vez para iniciar el asistente **Primeros pasos**. Consulte Guía de inicio de Sophos Mobile.
- Para dispositivos iPhone, iPad y Mac, necesita obtener un certificado del servicio de notificaciones push de Apple. Consulte Guía de inicio de Sophos Mobile.
- También tiene la opción de configurar un proxy EAS independiente para el filtrado de correo electrónico. Consulte Proxy EAS independiente (página 11).

4.5 Configurar el servidor web de Sophos Mobile

Sophos Mobile incluye un componente de servidor web que proporciona el contenido de las aplicaciones web del portal de autoservicio y Sophos Mobile Admin. El servidor web se puede configurar para adaptarlo a su entorno.

Las solicitudes a un servidor web incluyen un campo Host en el encabezado de la solicitud, especificando la aplicación web para procesar la solicitud. Un atacante puede manipular el valor de ese campo Host para provocar comportamientos inesperados.

Después de la instalación, el componente de servidor web de Sophos Mobile no comprueba el valor del campo Host. Le recomendamos configurar el servidor web para que solo acepte las solicitudes que se dirijan a su nombre de dominio.

1. En el equipo en el que ha instalado el servidor de Sophos Mobile, ejecute el script *%MDM_HOME%*`\tools\HostValidationUndertowFilter\addModule.bat`

   Sustituya *%MDM_HOME%* por la carpeta de instalación de Sophos Mobile.
2. Abra el archivo *%MDM_HOME%*`\wildfly\standalone\configuration\smc-config.xml` en un editor de textos y busque esta sección:

```
<filter name="hostheadervalidation" ...>
    <param name="allowedHosts" value="localhost"/>
</filter>
```

3. Después de `localhost`, añada su nombre de dominio para Sophos Mobile Admin y el portal de autoservicio.

Por ejemplo, si su nombre de dominio es `smc.ejemplo.com`, cambie la línea de la siguiente manera:

```
<param name="allowedHosts" value="localhost,smc.ejemplo.com"/>
```

Si el servidor de Sophos Mobile se puede acceder con más de un nombre de dominio, introduzca todos los nombres separados por comas.

4. Guarde el archivo `smc-config.xml`
5. Reinicie el servicio Sophos Mobile.

4.6 Cambiar el idioma de inicio de sesión de SQL

Si ha configurado el servidor de Sophos Mobile para usar la autenticación mediante SQL Server para conectarse a la base de datos, el idioma de inicio de sesión de SQL debe estar establecido en English (inglés). De lo contrario, se producirá un error cuando se inicie el servicio de Sophos Mobile.

Este tema describe cómo cambiar el idioma de inicio de sesión de SQL a English.

1. Detenga el servicio de Sophos Mobile.
2. Abra SQL Server Management Studio en el servidor y seleccione **Seguridad > Inicios de sesión**.
3. En la página **General** de las **Propiedades de inicio de sesión**, establezca el **Idioma predeterminado** en English, y luego haga clic en **Aceptar** para guardar los cambios.
4. Reinicie el servicio Sophos Mobile.

5 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.

Hay dos tipos de proxies EAS:

- El proxy EAS interno que se instala automáticamente con Sophos Mobile. Admite el tráfico entrante de ActiveSync que usa Microsoft Exchange o IBM Notes Traveler para iOS y los dispositivos Samsung Knox.
- Un proxy EAS independiente que se puede descargar e instalar por separado. Se comunica con el servidor de Sophos Mobile a través de una interfaz web HTTPS.

Para obtener una lista de los servidores de correo compatibles con el proxy EAS independiente, consulte las Notas de la edición de Sophos Mobile.

Nota
Por motivos de rendimiento, recomendamos que utilice el servidor proxy EAS independiente en lugar de la versión interna cuando deba gestionarse el tráfico de correo electrónico para más de 500 dispositivos cliente.

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

El proxy EAS independiente tiene características adicionales en comparación con la versión interna:

- Compatibilidad con IBM Notes Traveler para dispositivos no iOS (por ejemplo, Android). El cliente de Traveler para estos dispositivos usa un protocolo (no ActiveSync) que no es compatible con el proxy EAS interno.
- 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 16).
- 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.

5.1 Escenarios de uso para el proxy EAS

Nota
Además de la información proporcionada en esta sección, 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.

Utiliza IBM Notes Traveler (antes IBM Lotus Notes Traveler) para dispositivos que no son iOS

El proxy EAS interno no es apto para este escenario porque solo admite el protocolo ActiveSync, que es el que usa Microsoft Exchange y IBM Notes Traveler para los dispositivos iPhone y iPad. IBM Notes Traveler para dispositivos no iOS (por ejemplo, Android) utiliza un protocolo diferente que admite el proxy EAS independiente.

Para dispositivos no iOS, es necesario contar con un software de cliente de Traveler dedicado. Este software está disponible a través de `<traveler-server>/servlet/traveler` o el sistema de archivos de Traveler. Puede usar las funciones *Instalar app* y *Desinstalar app* de Sophos Mobile para instalar y desinstalar el software de cliente de Traveler. La configuración debe realizarse manualmente.

Desea admitir múltiples servidores de back-end

El proxy EAS independiente permite crear múltiples instancias de sistemas de correo electrónico de back-end. Cada instancia necesita un puerto TCP de entrada. Cada puerto puede conectarse a un back-end diferente. Necesita una URL por instancia de proxy EAS.

Desea configurar el equilibrio de carga para EAS

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.

Para este escenario se requiere un equilibrador de carga existente para HTTP.

Desea usar la autenticación basada en el certificado de cliente

Para este escenario se requiere un PKI existente y la parte pública del certificado de CA debe establecerse en el proxy EAS.

Necesita administrar más de 500 dispositivos

Por motivos de rendimiento, recomendamos que utilice el servidor proxy EAS independiente en lugar de la versión interna cuando deba gestionarse el tráfico de correo electrónico para más de 500 dispositivos cliente.

5.2 Descargar el instalador de proxy EAS

1. Inicie sesión en Sophos Mobile Admin como superadministrador.
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.

5.3 Instalar el proxy EAS independiente

Requisitos previos:

- Ha instalado y configurado Sophos Mobile.
- 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 de Sophos Mobile al que se conectará el proxy EAS.

   Si es necesario, seleccione **Use proxy server** para configurar un servidor proxy que el proxy EAS utilice para conectarse al servidor de Sophos Mobile.

   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.

   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.

   Atención
   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 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.

   Nota
   Su producto de Sophos incluye el asistente de certificado SSL para solicitar su certificado SSL/TLS para el proxy EAS de Sophos Mobile. Para más información, consulte Solicitar un certificado SSL/TLS (página 5).

   - 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 (Sophos Secure Email)**: Permita solicitudes de cliente de correo a la interfaz de Servicios Web Exchange (EWS) del servidor de Exchange.

  Active esta opción solo si está utilizando Sophos Secure Email en dispositivos iPhone y iPad.
- **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 Mobile Admin como superadministrador.
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 durante la 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.

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

Al configurar el proxy EAS independiente en modo PowerShell, se conecta a su servidor de correo de Exchange a través de PowerShell y establece el acceso al correo electrónico en función del estado de cumplimiento del dispositivo.

En el modo PowerShell, el tráfico de correo va directamente desde el servidor de correo de Exchange a los dispositivos sin un proxy. Para ver un esquema del flujo de comunicación, consulte la Sophos Mobile guía de distribución.

Ventajas del modo PowerShell:

- No necesita abrir ningún puerto en su servidor de Sophos Mobile para el tráfico de correo electrónico entrante desde sus dispositivos.
- Puede impedir que los dispositivos que no están inscritos en Sophos Mobile accedan al correo electrónico.

El servidor de correo de Exchange puede ser Exchange Server o Exchange Online, que forma parte de Office 365. Las versiones compatibles son:

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

Restricción
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.

Para configurar el control de acceso al correo electrónico a través de PowerShell, haga lo siguiente.

Información relacionada
Guía de distribución del servidor de Sophos Mobile

Configurar PowerShell

1. Opcional: Si es necesario, instale Windows PowerShell en el equipo en el que va a instalar el proxy EAS.
2. Abra PowerShell como administrador y ejecute el siguiente comando:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

Exchange Server requiere una configuración adicional:

3. Abra el Shell de administración de Exchange.
4. Establezca la política de ejecución de PowerShell:

   ```
   Set-ExecutionPolicy RemoteSigned
   ```

5. Obtenga el nombre del directorio virtual de PowerShell:

   ```
   Get-PowerShellVirtualDirectory -Server <nombre del servidor>
   ```

   <nombre del servidor> es el nombre del equipo en el que está instalado Exchange Server.

   En una instalación estándar, el directorio virtual de PowerShell es `PowerShell(Default Web Site)`.

6. Defina la autenticación básica para el directorio virtual de PowerShell:

   ```
   Set-PowerShellVirtualDirectory -Identity "PowerShell (Default Web Site)"
    -BasicAuthentication $true
   ```

Información relacionada
Instalación de Windows PowerShell (documento de Microsoft)
Abrir el Shell de administración de Exchange (documento de Microsoft)

Crear una cuenta de servicio

Una cuenta de servicio es una cuenta de usuario especial en el servidor de correo de Exchange que Sophos Mobile utiliza para ejecutar comandos de PowerShell.

1. Inicie sesión en la consola de administración relevante:
   - Para Exchange Server: **Centro de administración de Exchange**
   - Para Exchange Online: **Centro de administración de Office 365**
2. Cree una cuenta de usuario.
   - 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.

3. 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 usuario como miembro.

Configurar la conexión de PowerShell

1. Utilice el asistente de configuración como si fuera a configurar un proxy EAS independiente. En la página **EAS Proxy instance setup**, configure las siguientes opciones:
   - **Instance type**: Seleccione **PowerShell Exchange/Office 365**.
   - **Instance name**: Nombre para identificar la instancia.
   - **Exchange server**: En Exchange Server, introduzca el nombre o la dirección IP del servidor.

     Para Exchange Online, escriba `outlook.office365.com` si utiliza el servicio global de Office 365. Para otros servicios, por ejemplo Office 365 Alemania, puede encontrar la dirección en el documento Conexión a Exchange Online PowerShell de Microsoft.

     No escriba el protocolo `https://` ni el sufijo `/powershell-liveid` en el nombre. El asistente de configuración los añade automáticamente.
   - **Allow all certificates**: El proxy EAS no verifica el certificado del servidor. Seleccione esta opción, por ejemplo, si utiliza Exchange Server con un certificado autofirmado.

     Aviso
     Esta opción reduce la seguridad de las conexiones del servidor de correo. Solo seleccione esta opción si lo requiere el entorno de red.

   - **Service account**: Nombre de la cuenta de usuario que ha creado en la consola de administración de Exchange Server o Exchange Online.
   - **Password**: Contraseña de la cuenta de usuario.
2. Haga clic en **Add** para añadir la instancia a la lista **Instances**.
3. Repita los pasos anteriores para configurar las conexiones de PowerShell a otras instancias de Exchange Server.
4. Complete la configuración.
5. Opcional: Si es necesario, configure un servidor proxy que el proxy EAS utilice para conectarse a Exchange Server o Exchange Online. En el equipo en que ha instalado el proxy EAS, abra la línea de comandos con la opción **Ejecutar como administrador** y escriba el siguiente comando:

   ```
   netsh winhttp set proxy <nombre del servidor o IP>:<puerto>
   ```

   Aviso
   Este comando configura un proxy para todo el sistema. Otros programas que se ejecutan en el equipo podrían verse afectados.

Información relacionada

Conexión a Exchange Online PowerShell (documento de Microsoft)

Cargar el certificado de PowerShell

Cargue el certificado de la conexión de PowerShell en Sophos Mobile.

1. Inicie sesión en Sophos Mobile Admin como superadministrador.
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. 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.
4. En **Externo**, haga clic en **Subir un archivo**. Cargue el certificado creado durante la configuración.

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

5.5 Bloquear el acceso al correo electrónico para los dispositivos no administrados

Puede impedir que los dispositivos que no están inscritos en Sophos Mobile accedan al correo electrónico.

Requisito previo: Ha configurado el proxy EAS independiente en modo PowerShell.

En estas instrucciones, Exchange hace referencia a su Exchange Server local o a su plan de Exchange Online incluido en Office 365.

Puede configurar Exchange para poner en cuarentena los dispositivos no administrados. Los usuarios recibirán un mensaje de correo electrónico indicándoles que inscriban el dispositivo en Sophos Mobile. Una vez inscrito el dispositivo, se elimina automáticamente de la cuarentena.

Aviso

Antes de aplicar estas opciones de configuración en un entorno de producción, asegúrese de que los dispositivos están inscritos y pueden sincronizarse con Sophos Mobile. Todos los dispositivos se pondrán en cuarentena de forma predeterminada y solo tendrán acceso al correo electrónico si el servidor de Sophos Mobile los define como conformes.

Además, los dispositivos inscritos se ponen en cuarentena si el proxy EAS no conoce su estado de cumplimiento. Esto puede suceder cuando un dispositivo no se ha sincronizado con Sophos Mobile durante demasiado tiempo o cuando el proxy EAS no puede comunicarse con el servidor de Sophos Mobile.

Para bloquear el acceso al correo electrónico para los dispositivos no administrados:

1. Abra el Shell de administración de Exchange (si tiene Exchange Server) o conéctese a Exchange Online PowerShell.

   Para obtener más información, consulte los enlaces de la información relacionada.

2. Ejecute el siguiente comando (en una línea):

```
Set-ActiveSyncOrganizationSettings -DefaultAccessLevel quarantine
-UserMailInsert "Inscriba su dispositivo en Sophos Mobile."
```

El texto que especifique con `-UserMailInsert` se añade al correo electrónico de notificación que Exchange envía a los usuarios cuando su dispositivo está en cuarentena.

Para obtener más información sobre el control del acceso al correo electrónico en general, consulte el documento de Microsoft Controlling Exchange ActiveSync device access using the Allow/Block/Quarantine list.

Información relacionada

Configurar el proxy EAS independiente en modo PowerShell (página 16)
Al configurar el proxy EAS independiente en modo PowerShell, se conecta a su servidor de correo de Exchange a través de PowerShell y establece el acceso al correo electrónico en función del estado de cumplimiento del dispositivo.

Abrir el Shell de administración de Exchange (documento de Microsoft)

Conexión a Exchange Online PowerShell (documento de Microsoft)

Controlling Exchange ActiveSync device access using the Allow/Block/Quarantine list (documento de Microsoft)

6 Equilibrio de carga y alta disponibilidad

Sophos Mobile permite configurar un entorno de alta disponibilidad. Esto garantiza que el servicio de SMC siga estando accesible externamente y que se sigan pudiendo procesar las tareas, incluso después de un fallo de un nodo de Sophos Mobile. Para lograr esto, es necesario recurrir al equilibrio de carga, que distribuye las sesiones del cliente y del navegador usando DNS Round Robin en los nodos disponibles.

A continuación se describe cómo configurar la organización por clústeres para Sophos Mobile y configurar el equilibrio de carga mediante Sophos UTM.

6.1 Requisitos

- Un servidor de Windows por separado para cada nodo de Sophos Mobile.
- Todos los nodos deben estar en la misma red.
- Un servidor de bases de datos o clúster de Microsoft SQL o MySQL.
- Sophos UTM o proxy inverso Apache (mod_proxy) para el equilibrio de carga. El equilibrador de carga debe admitir cookies de sesión permanentes y certificados de servidor web SSL/TLS oficiales.

Nota
Para obtener información detallada acerca de los requisitos de instalación, consulte las Notas de la edición de Sophos Mobile 9.6.

Arquitectura

Para ver un ejemplo de un clúster de Sophos Mobile de tres nodos, consulte la Guía de distribución del servidor de Sophos Mobile.

Para la comunicación multidifusión entre los nodos de Sophos Mobile individuales, se puede usar una red por separado. La interfaz de red que se usará se puede seleccionar durante la configuración del clúster, según se describe en Configurar el primer nodo (página 22). También puede ser una VLAN.

Nota
Si desea operar un segundo clúster de Sophos Mobile para realizar pruebas, es necesaria una red por separado.

Puertos y protocolos

La siguiente tabla muestra los puertos y protocolos necesarios para la comunicación entre los nodos individuales de un clúster de servidor de Sophos Mobile.

Protocolo	Puertos	Destino
TCP	7600, 8181, 57600	*<Entrante>*
TCP	7600, 8181, 57600	*<Saliente>*
UDP	45700	*<Entrante>*

Certificados de servidor

Cuando configura Sophos Mobile, configura un certificado de servidor web SSL/TLS que permite a la app Sophos Mobile Control establecer una conexión segura al servidor de Sophos Mobile. Recomendamos que utilice un certificado emitido por una autoridad de certificación (CA) de confianza global. En un entorno de clúster con varios nodos de servidor Sophos Mobile tras un equilibrador de carga, esto puede no resultar práctico. Puede ser conveniente utilizar un certificado autofirmado en su lugar.

Tareas relacionadas

Solicitar un certificado SSL/TLS (página 5)
La entrega de productos Sophos incluye el asistente de certificado SSL para solicitar su certificado SSL/TLS para el proxy de EAS de Sophos Mobile.

6.2 Configurar nodos de clúster

Para configurar un entorno organizado en clústeres debe instalar el primer nodo tal y como se describe en Instalar y configurar el servidor de Sophos Mobile (página 6). A continuación, la propia organización por clústeres se activa usando el **Asistente de configuración**.

Para el resto de nodos, debe seleccionarse la base de datos creada durante la instalación del primer nodo y debe activarse la organización por clústeres.

Nota
También es posible configurar un servidor SMC existente para la organización por clústeres y ampliar el entorno añadiendo nodos adicionales.

6.2.1 Configurar el primer nodo

1. Instale Sophos Mobile según se describe en Instalar y configurar el servidor de Sophos Mobile (página 6) y anote el nombre de la base de datos que ha creado. Especifique esta base de datos cuando instale más nodos.
2. Al final de la instalación, deseleccione la opción **Start Sophos Mobile server now** en el cuadro de diálogo **Sophos Mobile - Installation finished**.

Nota
Si el servicio Sophos Mobile ya se ha iniciado, se detendrá y reiniciará automáticamente durante la configuración que se describe a continuación. También puede detener el servicio manualmente desde el menú del icono de Sophos Mobile de la bandeja del sistema.

3. En el servidor, haga clic en **Start**, vaya a **Sophos Mobile** y haga clic en **SMC Configuration Wizard**.
4. Aparecerá la página **Welcome** del Sophos Mobile Configuration Wizard. Haga clic en **Next**.
5. En la página **Database Selection**, seleccione **Skip database configuration** y haga clic en **Next**.
6. En la página **Choose configuration steps**, seleccione **Configure cluster support** y haga clic en **Next**.
7. En la página **Cluster Configuration**, use la lista desplegable de interfaces de red disponibles para seleccionar la interfaz que se usará para la comunicación multidifusión entre el nodo de servidor que está a punto de configurar y el resto de nodos.
8. Haga clic para pasar por las restantes páginas del asistente de configuración. Asegúrese de hacer clic en **Yes** cuando se le pregunte si desea iniciar el servicio SMC.
   La configuración del primer nodo de servidor de SMC ha concluido. Haga clic en **Finish** en el cuadro de diálogo **Sophos Mobile - Configuration Wizard finished**.

6.2.2 Configurar nodos adicionales

1. Inicie la instalación de Sophos Mobile según se describe en Instalar y configurar el servidor de Sophos Mobile (página 6).
2. En la página **Database selection**, seleccione la base de datos que creó cuando instaló el primer nodo y haga clic en **Next**.

   Se abrirá el cuadro de diálogo **Database configuration**. Muestra el progreso del proceso de configuración.
3. En la página **Database configuration**, espere hasta que finalice el proceso de configuración y a continuación haga clic en **Next**.
4. En la página **Choose configuration steps**, seleccione **Configure cluster support** y haga clic en **Next**.
5. En la página **Configure server certificate**, cree un certificado autofirmado como se describe en Instalar y configurar el servidor de Sophos Mobile (página 6) y haga clic en **Next**.
6. En la página **Cluster Configuration**, use la lista desplegable de interfaces de red disponibles para seleccionar la interfaz del nodo de servidor de Sophos Mobile que va a configurar y a continuación haga clic en **Next**.
7. Haga clic para pasar por las restantes páginas del asistente de configuración. En la página **Sophos Mobile - Installation finished**, seleccione **Start Sophos Mobile server now** para iniciar el nodo de clúster que acaba de configurar.
8. Si ha configurado el componente de servidor web de Sophos Mobile en el primer nodo para que solo acepte las solicitudes que se dirijan a su nombre de dominio, repita este procedimiento para el resto de nodos. Consulte Configurar el servidor web de Sophos Mobile (página 9).

Si es necesario, repita este procedimiento para configurar nodos adicionales.

6.3 Configurar el equilibrio de carga con Sophos UTM

En este tema se describe cómo configurar Sophos UTM como un equilibrador de carga para un clúster de nodos de servidor de Sophos Mobile. Para obtener más información acerca de la configuración de Sophos UTM, consulte la documentación de Sophos UTM.

Nota

- Para usar Sophos UTM para la organización en clústeres necesita una licencia de Sophos UTM con una suscripción de **Sophos Webserver Protection**.
- Tal como se describe más adelante en esta sección, debe especificar un certificado para proteger la comunicación entre los dispositivos administrados y el servidor web virtual que ha configurado en Sophos UTM. Para facilitar las cosas, se recomienda usar el mismo certificado que usó para el servidor de Sophos Mobile (consulte Solicitar un certificado SSL/TLS (página 5)). Si usó un certificado autofirmado, debe usar necesariamente ese mismo certificado.

1. Inicie sesión en WebAdmin de Sophos UTM.
2. Desde la sección del menú de WebAdmin **Webserver Protection**, vaya a la pestaña **Cortafuegos de aplicaciones web > Real Webservers**.
3. Haga clic en **New Real Webserver** para crear un nodo de SMC.
4. En el cuadro de diálogo **Add Real Webserver**, introduzca los siguientes valores:
   a) **Name**: Introduzca un nombre descriptivo para el servidor web (por ejemplo `nodo SMC`).
   b) **Host**: Seleccione o añada un host. Seleccione un host haciendo clic en el símbolo de la carpeta situado junto al campo del **Host**. Arrastre un host de la lista de hosts disponibles al campo del **Host**.
      Para obtener información adicional sobre cómo añadir una definición, consulte el tema *Definiciones de red* en la Guía de administración de UTM.
   c) **Type**: Seleccione **Encrypted (HTTPS)**.

   Haga clic en **Save** para guardar la configuración.

   Repita el paso anterior para cada nodo de servidor de Sophos Mobile.
5. Desde la sección del menú WebAdmin **Webserver Protection**, vaya a la pestaña **Certificate Management > Certificates**.
6. Haga clic en **New Certificate** para cargar un certificado de servidor web SSL/TLS.
7. En el cuadro de diálogo **Add Certificate**, introduzca los siguientes valores:
   a) **Name**: Introduzca un nombre descriptivo para el certificado.
   b) **Method**: Seleccione **Upload**.
   c) **File type**: Seleccione **PKCS#12(Cert+CA)**
   d) **Password**: Introduzca la contraseña para su archivo de certificado.
   e) **File**: Haga clic en el icono de la carpeta situado junto a la casilla **File**, seleccione el certificado que desea cargar y haga clic en **Start Upload**.

   Haga clic en **Save** para guardar la configuración. El certificado se añade a la lista **Certificates**.
8. Desde la sección del menú de WebAdmin **Webserver Protection**, vaya a la pestaña **Web Application Firewall > Virtual Webservers**.
9. Haga clic en **New Virtual Webserver** para añadir un servidor web virtual para el clúster.
10. En el cuadro de diálogo **Add Virtual Webserver** que aparece, introduzca los siguientes valores:
    a) **Name**: Introduzca un nombre descriptivo para el servidor web virtual (por ejemplo `clúster SMC`).
    b) En la lista **Interface**, seleccione la interfaz WAN a través de la cual se podrá acceder al clúster desde el exterior.
    c) **Type**: Seleccione **Encrypted (HTTPS) & redirect**.
    d) En la lista **Certificate**, seleccione el certificado del servidor web que ha cargado anteriormente.

e) **Domains** (solo con certificado comodín, que sea un certificado de clave pública que pueda utilizarse con múltiples subdominios): Introduzca los dominios de los que el servidor web es responsable, por ejemplo `tienda.ejemplo.com`, o use el icono **Action** para importar una lista de nombres de dominios.

Los dominios deben introducirse como nombres de dominio completos (FQDN).

Puede usar un asterisco (*) como carácter comodín para el prefijo del dominio, por ejemplo, `*.midominio.com`. Los dominios con caracteres comodines se consideran ajustes alternativos: El servidor web virtual con la entrada de dominio con carácter comodín solo se usa cuando no se ha configurado ningún otro servidor web virtual con un nombre de dominio más específico.

Ejemplo: La solicitud de un cliente a `a.b.c` coincidirá con `a.b.c` antes que `*.b.c` y antes que `*.c`.

f) **Real Webservers**: Seleccione los nodos de SMC que ha creado anteriormente.

Nota
No seleccione un perfil de firewall.

Haga clic en **Save** para guardar la configuración. El servidor se añade a la lista **Virtual Webservers**.

11. Habilitar el servidor web virtual.

    El nuevo servidor web virtual está deshabilitado por defecto. Haga clic en el interruptor de palanca para habilitar el servidor web virtual. El color del interruptor de palanca cambiará de gris (deshabilitado) a verde (habilitado).
12. Vaya a la pestaña **Site Path Routing**.
13. En la lista **Virtual Webservers**, vaya al servidor web virtual que ha añadido y haga clic en **Edit**.
14. En el cuadro de diálogo **Edit Site Path Route**, haga clic en **Advanced** y seleccione **Enable sticky session cookie**.
    Haga clic en **Save** para guardar la configuración.

7 Actualizar Sophos Mobile

Las instalaciones del servidor de Sophos Mobile se pueden actualizar directamente desde las versiones 9 y 9.5 a la versión 9.6.

Las versiones anteriores se deben actualizar antes a Sophos Mobile 9. Para obtener más información, consulte su documentación de Sophos Mobile 9.

7.1 Actualizar servidor Sophos Mobile

Para actualizar su instalación del servidor de Sophos Mobile a la versión 9.6, inicie el programa de instalación de Sophos Mobile 9.6 y siga las instrucciones. El instalador detecta de forma automática si una instalación existente necesita actualizarse.

Se llevará a cabo una comprobación de propiedades del sistema antes de iniciar la actualización. Si se superan todas las comprobaciones, puede proceder con la actualización. La base de datos y los archivos se actualizarán automáticamente sin ninguna interacción por parte del usuario. Una vez completada la actualización, el servicio de Sophos Mobile se iniciará de nuevo.

Nota
Si utilizó la autenticación de Windows durante la instalación inicial de su servidor de Sophos Mobile, la opción **Start Sophos Mobile server now** aparecerá en gris. Debe iniciar el servicio manualmente.

7.2 Tareas posteriores a la actualización

7.2.1 Reconfigurar el servidor web de Sophos Mobile

Si ha configurado el componente de servidor web de Sophos Mobile para que solo acepte las solicitudes que se dirijan a su nombre de dominio, debe repetir este paso después de actualizar Sophos Mobile. Consulte Configurar el servidor web de Sophos Mobile (página 9).

7.3 Actualizar un clúster de servidores

Al actualizar un clúster de servidores de Sophos Mobile, es importante que la versión de todos los nodos sea la misma y que la versión del servidor coincida con la versión de la base de datos. Para ello:

1. Cierre todos los nodos de servidores deteniendo el servicio de Sophos Mobile en los equipos correspondientes.
2. Actualice el primer nodo según se describe en Actualizar servidor Sophos Mobile (página 26).
   Esto también actualiza la base de datos.
3. Inicie el nodo de servidores actualizado y compruebe que la actualización se ha aplicado correctamente.
4. Actualice los nodos de servidores restantes.

Sugerencia
Si está usando el proxy EAS independiente, sus dispositivos administrados pueden acceder a su servidor de correo electrónico incluso con todos los nodos de servidores de Sophos Mobile detenidos. Esto es debido a que el proxy EAS hace una caché del estado del dispositivo de hasta 60 minutos cuando no está conectado al servidor Sophos Mobile.

7.4 Actualizar proxy EAS independiente

Para actualizar el proxy EAS independiente, ejecute el instalador del proxy EAS y siga las instrucciones. El instalador detecta de forma automática si una instalación existente necesita actualizarse.

Si está usando un clúster de nodos de servidores proxy EAS detrás de un equilibrador de cargas, puede actualizar estos nodos de forma independiente entre sí y en cualquier secuencia.

Sugerencia
No detenga todos los nodos de servidores proxy EAS a la vez. De esta forma se asegura que la comunicación por correo electrónico de sus dispositivos administrados no sufra interrupciones durante la actualización.

8 Referencia técnica

8.1 Características del servidor de Sophos Mobile

El componente central del producto Sophos Mobile es el servidor de Sophos Mobile. Sus principales características son:

- El servidor está conectado a Internet.
- El servidor permite configurar un entorno de alta disponibilidad.
- El administrador controla el servidor usando la interfaz web.
- Los usuarios finales pueden registrar sus dispositivos utilizando el portal de autoservicio, o bien obtener un dispositivo del administrador que ya se haya preparado para la inscripción automática.
- Los dispositivos administrados se sincronizan con el servidor mediante HTTPS.
- Puede usar Microsoft SQL Server o una base de datos MySQL existente para almacenar la información del dispositivo y de las aplicaciones. También puede dejar que el instalador de Sophos Mobile cree una nueva base de datos usando Microsoft SQL Server Express.
- La base de datos puede estar alojada en el mismo ordenador o en uno por separado. Esto permite utilizar clústeres de bases de datos.
- El servidor admite configuraciones de múltiples inquilinos para permitir diferentes clientes en el mismo servidor.
- El acceso al correo electrónico es posible a través de un proxy EAS integrado o independiente. Para la variante independiente, se requiere un acceso HTTPS al servidor SMC.

El servidor de Sophos Mobile se ha desarrollado para Java EE (Enterprise Edition). Se instala y se ejecuta en el servidor de aplicaciones WildFly, estándar de la industria y ampliamente probado.

El servidor se puede instalar en entornos virtuales.

8.2 Interfaces web de Sophos Mobile

8.2.1 Interfaz de administración de Sophos Mobile

Sophos Mobile se gestiona a través de una interfaz web que está protegida por un inicio de sesión y un mecanismo de sesiones. Puede implementar políticas de contraseñas. El control de acceso permite diferentes roles de usuario. Estos roles tienen diferentes conjuntos de permisos de acceso. Cada usuario puede asignarse exactamente a un rol.

Para obtener más información, consulte la Ayuda para el administrador de Sophos Mobile.

8.2.2 Interfaz de súper administrador

El superadministrador se usa principalmente para configurar y gestionar clientes para la administración de dispositivos. La primera cuenta de superadministrador se crea durante la

configuración de Sophos Mobile. Consulte Instalar y configurar el servidor de Sophos Mobile (página 6).

Como superadministrador, usted inicia sesión en la cuenta del cliente superadministrador, que también se crea durante la configuración de Sophos Mobile. Para el cliente superadministrador, Sophos Mobile Admin muestra una vista personalizada para las tareas de superadministrador.

8.2.3 Portal de autoservicio

El portal de autoservicio está protegido mediante un inicio de sesión, un mecanismo de sesión y una política de contraseña. La cuenta debe configurarla el administrador de Sophos Mobile y puede asociarse con cualquier inquilino. El portal de autoservicio está diseñado para que los usuarios finales registren sus dispositivos con Sophos Mobile. Los usuarios finales también tienen permiso para realizar tareas para sus dispositivos, como por ejemplo el bloqueo remoto o el borrado remoto. Las tareas que pueden realizar varían en función de la plataforma y la configuración del dispositivo. Como administrador, puede configurar las funciones del portal de autoservicio disponibles para los usuarios finales.

Para más información sobre cómo configurar el portal de autoservicio para usuarios finales, consulte la Ayuda para el administrador de Sophos Mobile.

9 Soporte

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

- Visitar el foro Sophos Community en community.sophos.com/ para consultar casos similares.
- Visitar la base de conocimiento de Sophos en www.sophos.com/es-es/support.aspx.
- 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.

10 Aviso legal