SOPHOS

Cybersecurity made simple.

Sophos Connect

Ayuda

Contenido

(2020/05/26)

1 Acerca de Sophos Connect

Sophos Connect es un cliente VPN que se puede instalar en equipos Windows y Mac. Permite conectarse a redes que se encuentran detrás de XG desde una ubicación remota, por ejemplo, la red de su empresa El administrador de firewall configurará los detalles de conexión en el dispositivo XG y le proporcionará el paquete de instalación y los archivos de configuración de conexión.

Esta guía ofrece información sobre cómo utilizar Sophos Connect:

- Para obtener instrucciones sobre cómo instalar y desinstalar Sophos Connect, consulte Instalar Sophos Connect (página 1).
- Para obtener instrucciones sobre la importación de archivos de conexión y la gestión de conexiones, consulte Conexiones (página 2).
- Para obtener información sobre eventos y sobre cómo solucionar errores de eventos, consulte Eventos (página 11).
- Para solucionar problemas que no aparecen en la sección Eventos, consulte Solución de problemas generales (página 18).

1.1 Instalar Sophos Connect

Instalar Sophos Connect en Windows

- Abra el instalador.
- Acepte el acuerdo de licencia y haga clic en **Instalar**.
- Al completarse la instalación, haga clic en **Finalizar**. Puede optar por iniciar Sophos Connect después de salir.

Instalar Sophos Connect en Mac

- Abra el instalador.
- Seleccione el destino de la instalación. Asegúrese de que tiene suficiente espacio libre en el destino que ha elegido, por ejemplo, la unidad del sistema.
- Haga clic en **Instalar**.
- Al completarse la instalación, haga clic en **Finalizar**.

1.2 Desinstalar Sophos Connect

Desinstalar Sophos Connect de Windows

- Vaya a **Panel de control** y en **Programas**, haga clic en **Desinstalar un programa**.
- Haga clic con el botón derecho en Sophos Connect y seleccione **Desinstalar**.

Desinstalar Sophos Connect de Mac

- Abra Terminal.
- Aumente los permisos al directorio raíz y ejecute el script de desinstalación desde la ubicación en la que está instalado Sophos Connect:

  ```
  sudo /Library/Sophos Connect/uninstall.sh
  ```

Obtendrá el siguiente mensaje si la desinstalación se ha realizado correctamente:

```
Sophos Connect has been uninstalled
```

1.3 Conexiones

Puede importar conexiones, establecer conexiones y ver y editar conexiones.

Sophos Connect admite VPN SSL y VPN IPsec.

1.3.1 Importar conexiones

El cliente de Sophos Connect puede conectarse XG Firewall mediante conexiones VPN SSL o IPsec. Puede importar conexiones al cliente de Sophos Connect.

Introducción

Para la versión 2.0 del cliente de Sophos Connect, puede importar conexiones VPN SSL e IPsec. Si utiliza una versión anterior del cliente de Sophos Connect, solo puede importar conexiones IPsec.

En esta página se explica cómo hacer lo siguiente:

- Importe una conexión IPsec utilizando un archivo proporcionado por el administrador.
- Importe una conexión SSL utilizando un archivo proporcionado por el administrador.
- Importe una conexión SSL descargando un archivo del portal de usuario.

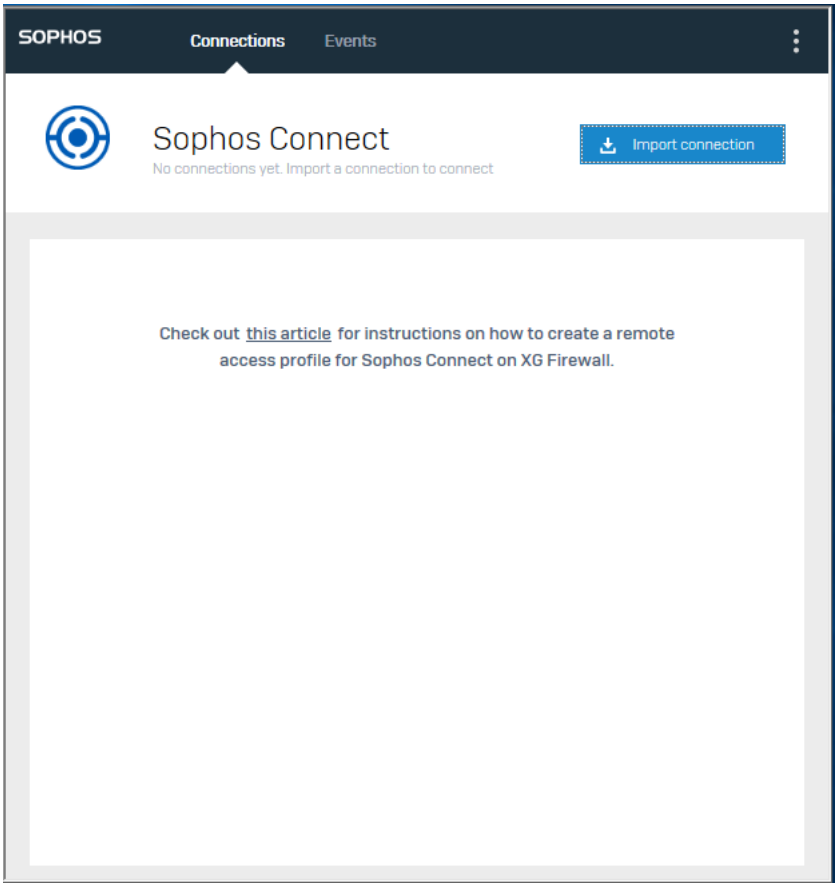
Importar una conexión IPsec

Se le ha proporcionado un archivo de conexión. Tiene la extensión `tgb`, por ejemplo, `Conexión_empresa.tgb`.

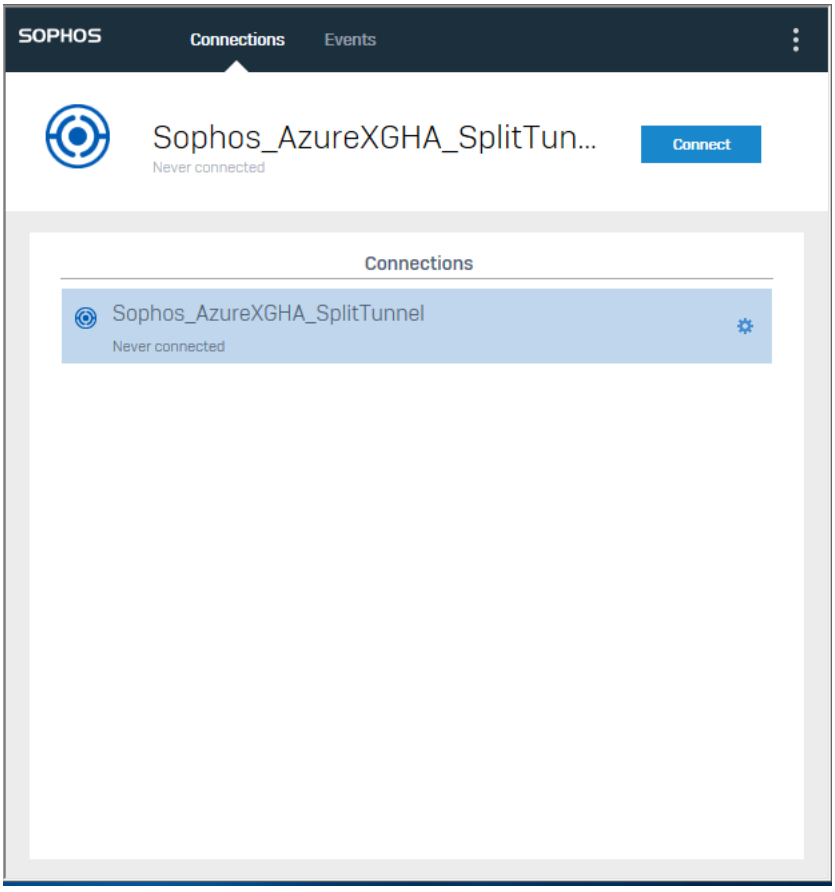
Para importar una conexión:

1. En la página **Conexiones**, haga clic en **Importar conexión**.

   Si hay conexiones existentes, haga clic en el botón de menú y elija **Importar conexión** en el menú desplegable.



2. Busque el archivo `.tgb` y haga doble clic en él.
   La conexión se mostrará en **Conexiones**.



Ahora puede establecer la conexión.

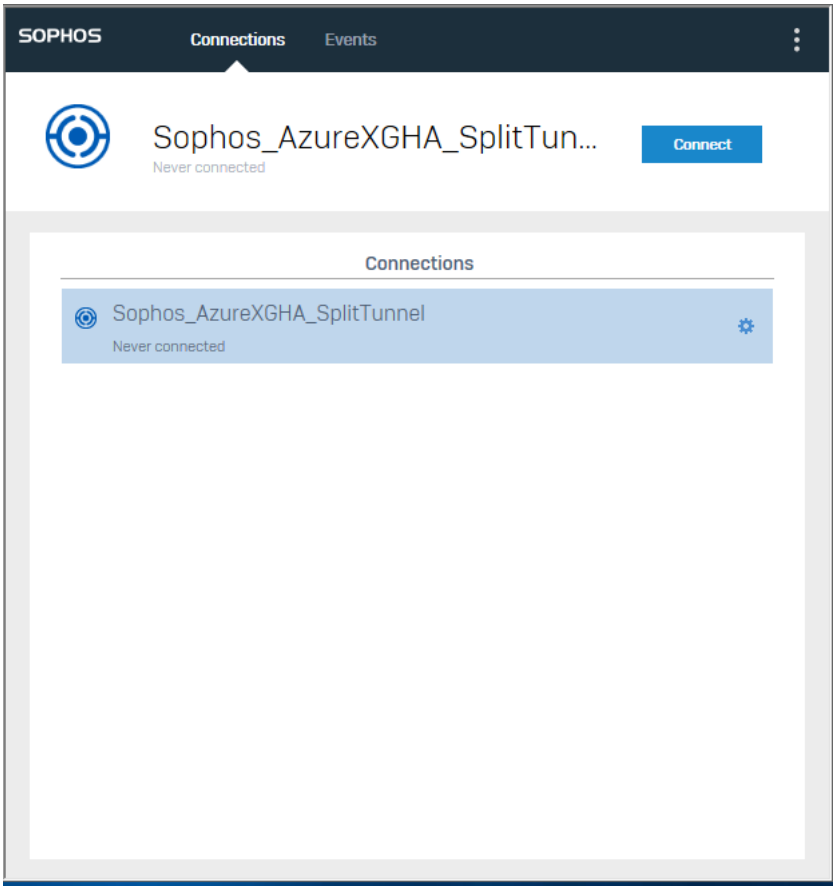
Nota
Puede importar varias conexiones.

Importar una conexión SSL

Se le ha proporcionado un archivo de conexión. Tiene la extensión `pro`, por ejemplo `Company_connection.pro`.

Para importar una conexión:

Busque el archivo `.pro` y haga doble clic en él.
La conexión se importará automáticamente y Sophos Connect se abrirá. La conexión se mostrará en **Conexiones**.



Ahora puede establecer la conexión.

Nota
Puede importar varias conexiones.

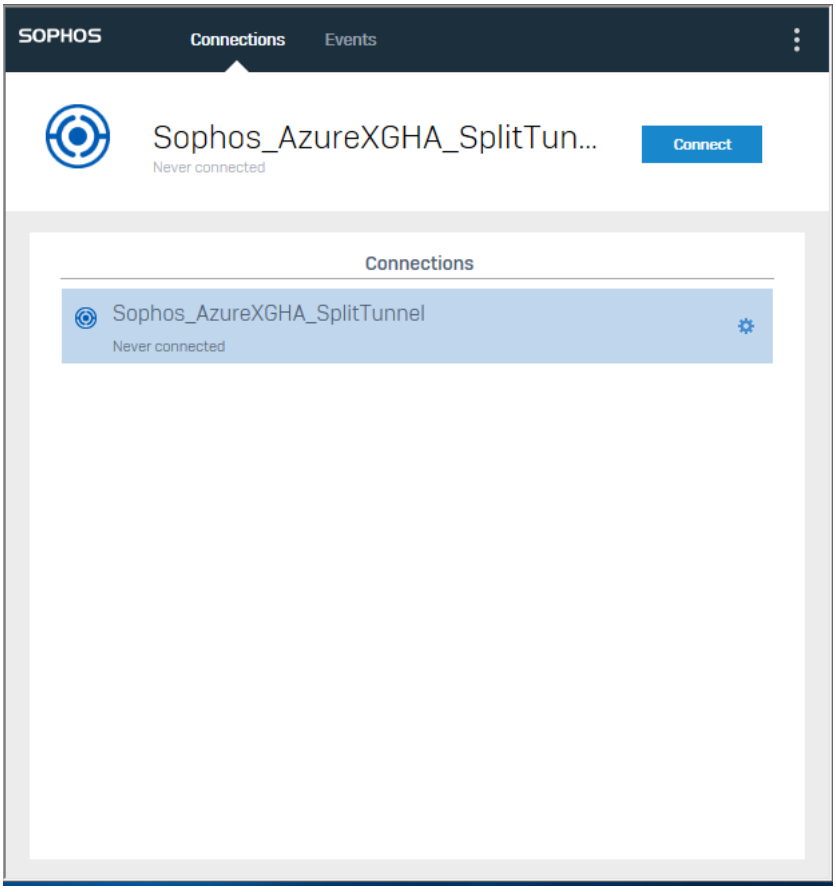
Importar una conexión SSL desde el portal de usuario

Para importar una conexión:

1. Inicie sesión en el portal de usuario.
2. Vaya a **VPN SSL** y haga clic en **Descargar configuración para otros SO** .
3. Abra el cliente de Sophos Connect.
4. En la página **Conexiones**, haga clic en **Importar conexión**.

   Si hay conexiones existentes, haga clic en el botón de menú y elija **Importar conexión** en el menú desplegable.
5. Busque el archivo `.ovpn` y ábralo.

La conexión se mostrará en **Conexiones**.



Ahora puede establecer la conexión.

Nota
Puede importar varias conexiones.

1.3.2 Conectar

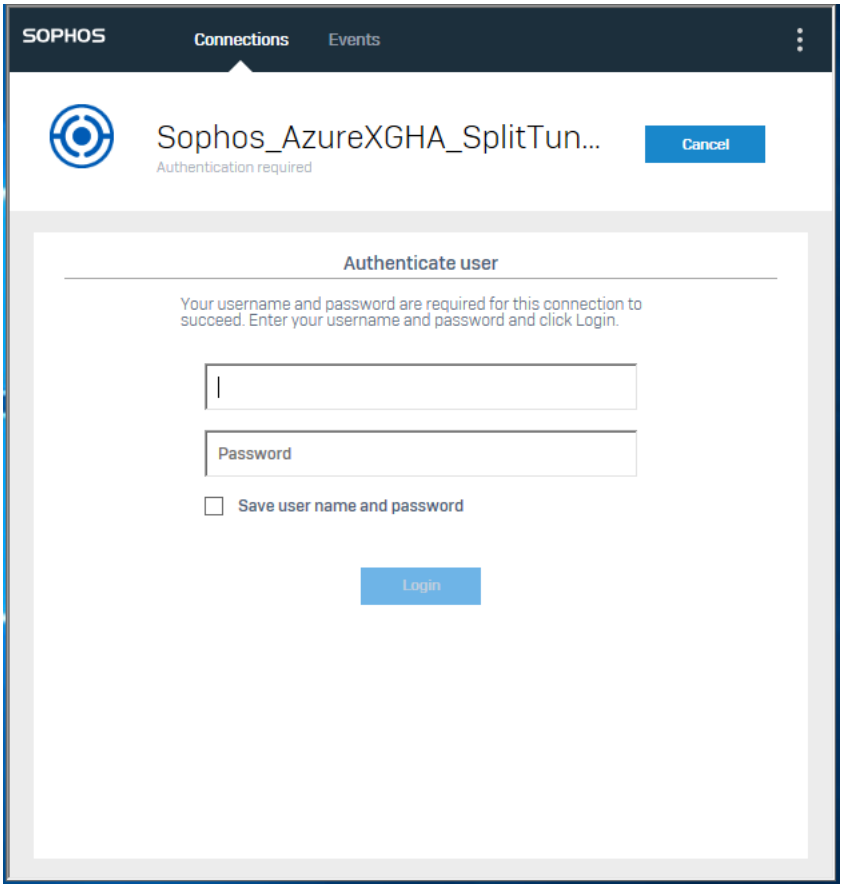
Asegúrese de que haya al menos una conexión importada disponible y de que se le hayan otorgado las credenciales necesarias.

Para establecer una conexión:

1. En la página **Conexiones**, seleccione una conexión.
2. Haga doble clic en ella.

   También puede hacer clic en **Conectar**.

   Aparecerá la pantalla de inicio de sesión.



3. Introduzca su nombre de usuario y contraseña y haga clic en **Iniciar sesión**.

   Es posible que el administrador haya configurado la autenticación de dos factores.

   - Si el administrador ha configurado OTP, además de introducir su nombre de usuario y contraseña, debe introducir su código de acceso OTP de 6 dígitos.
   - Si el administrador ha configurado la autenticación DUO, es posible que reciba uno o dos mensajes de DUO durante el proceso de conexión.

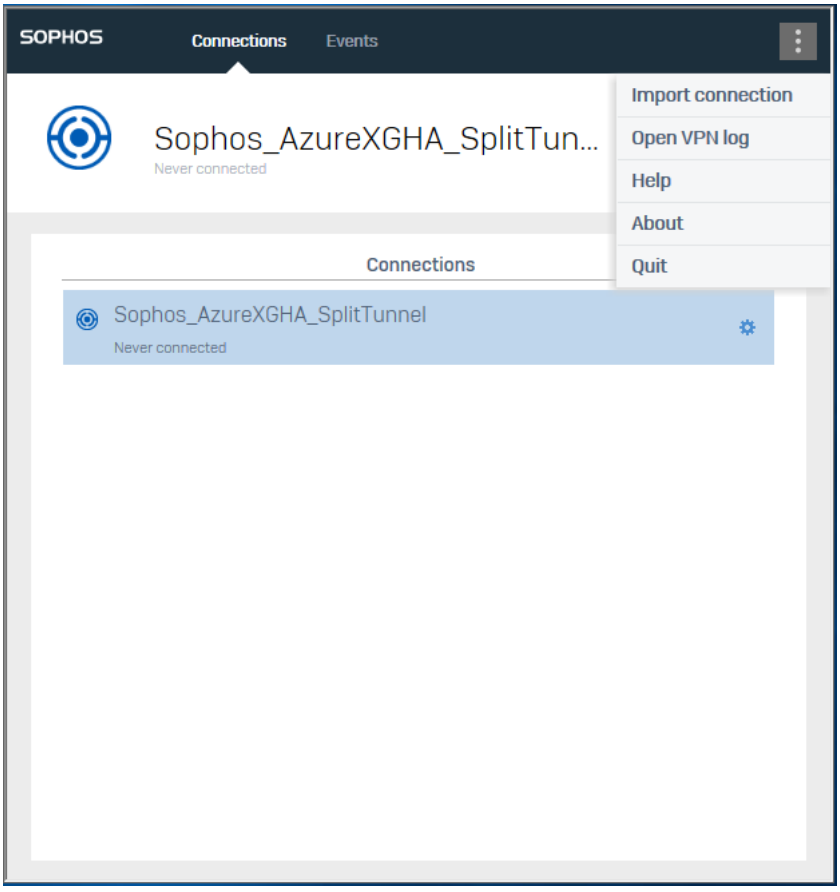
   Nota

   Si ha importado la conexión mediante un archivo de aprovisionamiento, recibirá una advertencia de que no se puede verificar el certificado del servidor. Puede hacer clic en **Aceptar** para continuar. Si no desea ver el mensaje, póngase en contacto con el administrador.

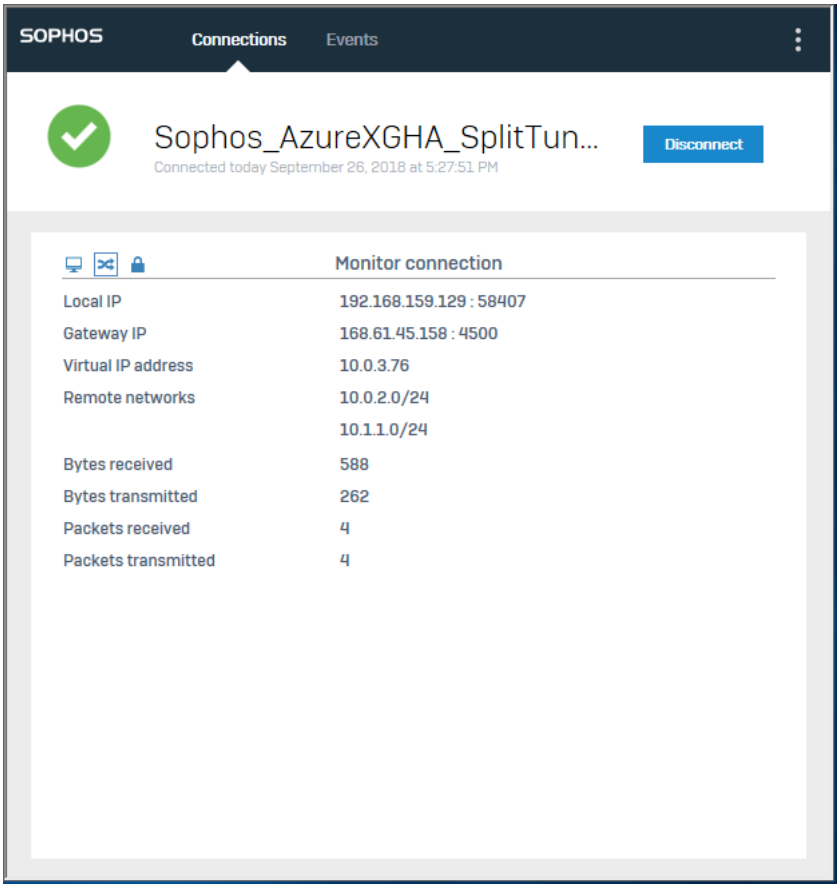
   Sophos Connect intentará establecer la conexión y autenticarle.

   Nota

   Si tiene problemas de conexión, eche un vistazo a la página **Eventos** y póngase en contacto con su departamento de TI. También puede revisar los registros de VPN haciendo clic en el icono del menú y seleccionándolos.



Se establece la conexión con el servidor remoto.



Si la conexión se realiza correctamente, verá este icono en la barra de tareas:

En cambio, si la conexión no se realiza correctamente, verá este icono en la barra de tareas:

Nota
Si ha cambiado el nombre de la conexión, el nombre original proporcionado por el administrador del firewall seguirá apareciendo en los detalles de la conexión. Para obtener instrucciones sobre cómo cambiarle de nombre, consulte Opciones de conexión (página 9).

1.3.3 Opciones de conexión

Puede realizar varios cambios en las conexiones de Sophos Connect haciendo clic en el icono de configuración que aparece al lado derecho de la conexión.

1. **Conexión automática** trata de establecer una conexión cuando se inicia Sophos Connect.
2. **Eliminar** elimina la conexión. Si desea volver a habilitar esa conexión, deberá importarla de nuevo.
3. **Cambiar nombre** le da la opción de cambiar el nombre de la conexión.
4. **Borrar credenciales** borra las credenciales almacenadas anteriormente.
5. **Actualizar política** (solo disponible si la conexión se ha creado con un archivo de aprovisionamiento). Esta opción le permite extraer la política más reciente del firewall XG a petición.

Sugerencia
Si la conexión falla después de múltiples intentos, inicie una actualización de políticas y pruebe a conectarse de nuevo.

1.4 Eventos

Consulte las acciones de Sophos Connect y los resultados de dichas acciones. Esto incluye los errores provocados por las acciones de los usuarios, así como los errores de negociación IKE. Para solucionar los problemas relacionados con los eventos, consulte Solución de problemas con eventos (página 12).

- Si necesita mensajes de error detallados para solucionar un problema, haga clic en **Abrir registro de VPN**.
- Para eliminar eventos de la lista, haga clic en **Borrar eventos**.

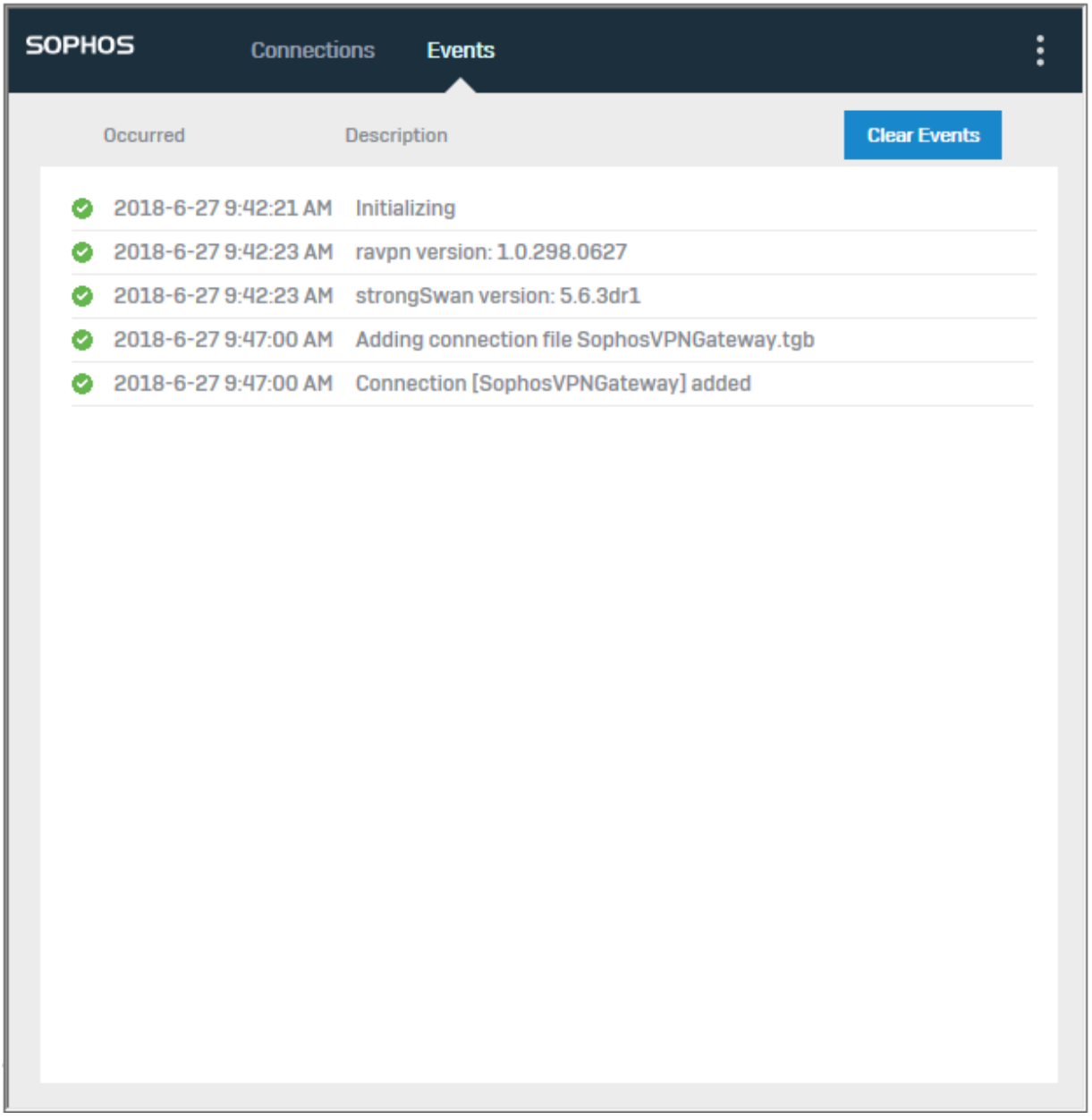


Figura 1: Eventos

1.4.1 Solución de problemas con eventos

Si tiene problemas al conectarse, haga clic en **Eventos**, mire la marca de tiempo de cuando se ha intentado establecer la conexión y localice el error correspondiente.

En esta sección verá los mensajes de error, las posibles causas de los errores e información sobre cómo proceder. Si tiene algún problema que no aparece a continuación, consulte el tema Solución de problemas generales.

Si necesita más ayuda, póngase en contacto con el soporte técnico de Sophos.

Sin conexión a la red.

Causa: El adaptador de red (Ethernet o Wi-Fi) no tiene dirección IP.

Qué hacer: Compruebe que dispone de una dirección IP válida y que su conexión de red existente funciona.

Error en la resolución DNS

Causa: El cliente no puede resolver el nombre de host de la puerta de enlace.

Qué hacer: Compruebe si hay un servidor DNS asignado a la interfaz de red. Ejecute `nslookup` desde el símbolo del sistema (Windows) o desde Terminal (Mac) para un host público, por ejemplo, www.sophos.com, y verifique que se resuelve en una dirección IP. Si no se resuelve, póngase en contacto con su proveedor de servicio de Internet.

Puertos UDP 500/4500 bloqueados

Causa: El firewall o router bloquea los puertos UDP 500 y 4500.

Qué hacer: Compruebe la configuración local del firewall o router y autorice el tráfico en esos puertos. Si no tiene acceso al firewall o router, por ejemplo, si se encuentra en un hotel, conéctese a través de su punto de acceso móvil y vuelva a conectarse.

No hay respuesta de la puerta de enlace: <FQDN o IP de puerta de enlace especificado en la conexión>

Causa: La puerta de enlace no responde a los mensajes de negociación IKE. Esto puede deberse a que:

- La puerta de enlace remota (firewall o router) se ha apagado.
- La dirección WAN de la puerta de enlace remota no está conectada directamente a Internet.

Qué hacer: Póngase en contacto con el administrador del firewall para que el problema se investigue más a fondo.

Se ha recibido la notificación NO_PROPOSAL_CHOSEN de la puerta de enlace

Causa: La puerta de enlace remota ha respondido a las negociaciones IKE de Sophos Connect con esta notificación de error. Esto puede deberse a que:

- La política de Sophos Connect no está definida ni activada en el firewall.
- El administrador del firewall ha cambiado las propuestas de IKE de fase 1 utilizadas para la política de Sophos Connect en el firewall y la nueva configuración no se ha exportado ni se ha cargado en el cliente.

Qué hacer: Póngase en contacto con el administrador del firewall para que el problema se investigue más a fondo.

El servidor esperaba el <valor de ID esperado> del ID remoto pero obtuvo el <valor de ID real>

Causa: El tipo o valor del ID local configurado en la política de Sophos Connect en el firewall es diferente del valor utilizado para esta conexión. Esto puede deberse a que el administrador del firewall ha cambiado el ID local en el firewall y el nuevo archivo de configuración no se ha importado a Sophos Connect.

Qué hacer: Póngase en contacto con el administrador del firewall para que el problema se investigue más a fondo.

Posible error de coincidencia de clave previamente compartida <nombre de conexión>

Causa: La clave previamente compartida en el firewall no coincide con la utilizada para esta conexión. Esto puede deberse a que el administrador del firewall la ha cambiado en el firewall y el nuevo archivo de configuración no se ha cargado en Sophos Connect.

Qué hacer: Póngase en contacto con el administrador del firewall para que el problema se investigue más a fondo.

No se ha podido autenticar al usuario <nombre de usuario introducido>

Causa: El nombre de usuario o la contraseña no coinciden.

Qué hacer: Vuelva a intentarlo para ver si se debe a un error del usuario al introducir la información. Si lo intenta varias veces y obtiene el mismo error, es posible que la contraseña haya cambiado o se haya desactivado en el firewall. En tal caso, póngase en contacto con el administrador del firewall para que el problema se investigue más a fondo.

Un error al añadir la ruta [red/máscara] ha impedido que finalice la fase 2

Nota
Los pasos que se indican a continuación son solo para Windows.

Causa: Una vez establecida la SA de fase 2, falla el comando `route add` a la red remota. Esto puede deberse a que el servicio strongSwan se ha bloqueado mientras el túnel estaba activo.

Qué hacer: Desactive y active el adaptador TAP. Abra la línea de comandos como administrador y escriba los siguientes comandos:

```
net stop scvpn
net start scvpn
```

No se han podido añadir los datos de conexión. Ya existe una conexión con el nombre <nombre de conexión>

Causa: Ya se ha importado una conexión con ese nombre.

Qué hacer: Elimine la conexión existente de Sophos Connect. Asegúrese de que realmente desea eliminar la conexión existente antes de hacerlo. De lo contrario, póngase en contacto con el administrador para que el problema se investigue más a fondo.

El servicio no está disponible

Nota
Los pasos que se indican a continuación son solo para Windows.

Causa: El servicio Sophos Connect (scvpn) no está funcionando.

Qué hacer: Abra la línea de comandos como administrador y escriba el siguiente comando:

```
net start scvpn
```

No se ha podido cargar la información de conexión en strongSwan

Nota
Los pasos que se indican a continuación son solo para Windows.

Causa: El servicio strongSwan no está funcionando (Nombre del servicio: charon-svc.exe).

Qué hacer: Abra la línea de comandos como administrador y escriba el siguiente comando:

```
net start strongswan
```

SA desactivada o eliminada por la puerta de enlace

Causa: La puerta de enlace ha enviado una solicitud de eliminación IKE y luego el túnel ha sido borrado. Esto puede deberse a que:

- El administrador del firewall ha cambiado la política en el firewall. Esto envía una solicitud de eliminación IKE a todas las SA activas en el firewall.
- El administrador del firewall ha eliminado manualmente todas las conexiones IPsec para este usuario en el firewall.

Qué hacer: Vuelva a establecer la conexión. Si sigue sin funcionar, póngase en contacto con el administrador para que el problema se investigue más a fondo.

Error en la resolución DNS de la puerta de enlace: <nombre de puerta de enlace:puerto>

Causa: Este error se debe a un nombre de host no válido.

Qué hacer:

- Si la conexión se ha añadido mediante un archivo de aprovisionamiento, verifique el nombre de host proporcionado.
- Si la conexión se ha añadido importando un archivo `ovpn`, compruebe la configuración de VPN SSL en XG Firewall.

No se puede verificar el certificado del servidor: <nombre de puerta de enlace> ¿Desea continuar?

Causa: El cliente de Sophos Connect importa la configuración de VPN SSL conectándose al portal de usuario de XG Firewall utilizando las propiedades del archivo de aprovisionamiento. El portal de usuario utiliza un certificado autofirmado que el cliente Sophos Connect no puede verificar.

Qué hacer: Acepte la advertencia de seguridad para conectarse y descargue el archivo de configuración `ovpn` desde el portal de usuario. Para evitar que el mensaje aparezca en el futuro, utilice una de estas opciones:

- Emita un nuevo certificado para XG Firewall firmado por una CA pública. En XG Firewall, importe el certificado y, a continuación, seleccione el certificado en **Configuración de administración** para iniciar sesión en la consola de administración web.
- Inserte el certificado de CA predeterminado desde XG Firewall en el almacén de confianza de los equipos remotos.

No se ha podido conectar con el servidor de no confianza: <puerta de enlace>

Causa: Ha cancelado el mensaje de advertencia del certificado y la conexión ha finalizado.

Qué hacer: Acepte la advertencia de seguridad para conectarse y descargue la política VPN SSL de XG Firewall. Para evitar que el mensaje aparezca mientras se descarga la política VPN SSL, utilice una de estas opciones:

- Emita un nuevo certificado para XG Firewall firmado por una CA pública. En XG Firewall, importe el certificado y, a continuación, seleccione el certificado en **Configuración de administración** para iniciar sesión en la consola de administración web.
- Inserte el certificado de CA predeterminado de XG Firewall en el almacén de confianza de los equipos remotos.

El archivo de importación contiene una conexión duplicada: <nombre de conexión>

Causa: La conexión importada de un archivo de aprovisionamiento tiene un nombre para mostrar duplicado.

Qué hacer: Compruebe el atributo `display_name` en el archivo de aprovisionamiento y cambie cualquier nombre duplicado.

No se puede conectar con la puerta de enlace de la política: <nombre de puerta de enlace>

Causa: El archivo de aprovisionamiento no está configurado correctamente. Esto puede ocurrir por cualquiera de las siguientes razones:

1. Nombre de host o dirección IP de puerta de enlace no válidos.
2. Puerto no válido o puerto saliente bloqueado.
3. No se puede acceder a la puerta de enlace de políticas porque está desactivada.

Qué hacer:

Compruebe lo siguiente en el archivo de aprovisionamiento:

1. Asegúrese de que el valor asignado al atributo `gateway` es correcto.
2. Asegúrese de que el valor asignado al atributo `user_portal_port` coincide con la configuración del puerto HTTPS del portal de usuario en XG Firewall.
3. Si el archivo de aprovisionamiento está configurado correctamente, póngase en contacto con el administrador para que el problema se investigue más a fondo.

No hay ninguna política VPN SSL definida para este usuario: <nombre de usuario>

Causa: La política VPN SSL (acceso remoto) en XG Firewall no contiene ningún miembro de la política.

Qué hacer: Póngase en contacto con el administrador.

Error de coincidencia de compresión. Se volverá a intentar la conexión.

Causa: Se descarga por primera vez una política VPN SSL desde XG Firewall y se establece el túnel VPN SSL con ella.

Qué hacer: El error se resuelve en función cómo esté configurada la conexión:

- Con un archivo de aprovisionamiento: Sophos Connect intenta conectarse de nuevo automáticamente.
- Con un archivo `ovpn`: Vuelva a conectarse manualmente.

Error de coincidencia de política. Se descargará la política y se volverá a intentar la conexión.

Causa: El cliente de Sophos Connect ha intentado establecer una conexión VPN SSL con una política existente que ha guardado para esta conexión.

El administrador ha cambiado la configuración de VPN SSL en XG Firewall después de que Sophos Connect estableciera y guardara una conexión VPN SSL.

Qué hacer: La conexión se ha creado mediante un archivo de aprovisionamiento. Sophos Connect descargará automáticamente la nueva política y volverá a establecer el túnel VPN SSL.

Nota
Si el administrador cambia la política VPN SSL en XG Firewall mientras el túnel está conectado y es una VPN SSL a través de TCP, el cliente de Sophos Connect detectará y descargará la nueva política inmediatamente. Si se trata de un túnel VPN SSL a través de UDP, debe esperar a que el temporizador de inactividad elimine el túnel. Sophos Connect descargará la nueva política para restablecer el túnel.

Error de coincidencia de política. Importe una nueva política para esta conexión.

Causa: El cliente de Sophos Connect ha intentado establecer una conexión VPN SSL con una política existente que ha guardado para esta conexión.

El administrador ha cambiado la configuración de VPN SSL en XG Firewall después de que Sophos Connect estableciera y guardara una conexión VPN SSL.

Qué hacer: La conexión se ha creado importando un archivo ovpn. El usuario debe descargar e importar un nuevo archivo ovpn desde el portal de usuario de XG Firewall para restablecer el túnel VPN SSL.

Nota
Si el administrador cambia la política VPN SSL en XG Firewall mientras el túnel está conectado y es una VPN SSL a través de un túnel TCP, el cliente de Sophos Connect detectará y desconectará el túnel con un error. Si se trata de un túnel VPN SSL a través de UDP, debe esperar a que el temporizador de inactividad elimine el túnel. El usuario debe descargar e importar un nuevo archivo ovpn desde el portal de usuario de XG Firewall para restablecer el túnel VPN SSL correctamente.

Se ha agotado el tiempo de espera para la respuesta del servidor.

Causa: La política VPN SSL no está configurada correctamente en XG Firewall. Los posibles motivos del error son los siguientes:

1. Se ha configurado Anular nombre de host, pero no se resuelve en la dirección IP pública correcta o válida.
2. Se ha configurado DDNS, pero no se resuelve en la dirección IP pública correcta o válida.
3. Tanto **Anular nombre de host** como DDNS no están configurados y el puerto WAN no tiene una dirección IP pública.

Qué hacer: Si ha utilizado un archivo de aprovisionamiento para importar la conexión, actualice el menú de configuración de la conexión de políticas (en el cliente de Sophos Connect). Si ha utilizado un archivo ovpn para crear la conexión, exporte un nuevo archivo ovpn desde el portal de usuario y vuelva a importarlo en el cliente de Sophos Connect.

1.5 Solución de problemas generales

Este tema trata la resolución de problemas que no aparecen en la página de eventos.

Si necesita más ayuda, póngase en contacto con el soporte técnico de Sophos.

El tráfico deja de pasar por el túnel VPN

Causa: Si ejecuta una versión de firmware anterior a la 17.5, es posible que el cliente haya recibido una nueva IP virtual después de la regeneración de clave de la fase 1.

Qué hacer: Tendrá que desconectarse y volver a conectarse. La solución permanente es actualizarse a la versión 17.5.

El panel de control de Sophos Connect no se abre

Causa: Si el panel de control de Sophos Connect no se abre o no responde al hacer clic en el icono de la bandeja, significa que la interfaz gráfica de Sophos Connect se ha atascado en un bucle infinito y no puede responder a la entrada externa.

Qué hacer (Windows): Abra el administrador de tareas y seleccione la pestaña Detalles. Localice scgui.exe y, a continuación, haga clic con el botón derecho para finalizar la tarea. Reinicie la aplicación desde el acceso directo del escritorio.

Qué hacer (Mac): Abra el Monitor de actividad y localice el proceso de Sophos Connect. Abra el proceso y seleccione Forzar salida. Reinicie la aplicación desde LaunchPad.

La navegación web deja de funcionar cuando se desconecta el túnel

Nota
Esto es más común en Mac.

Causa: Cuando se desconecta una conexión de tunelizar todo, los servidores DNS no se restauran desde los adaptadores de red físicos. Esto significa que los servidores DNS internos que se utilizaron cuando se conectó a través de la VPN siguen utilizándose. Como el túnel ya no existe, la resolución de nombres no funcionará.

Qué hacer: Desconéctese de la red local y vuelva a conectarse.

La interfaz gráfica de Sophos Connect muestra "Servicio no disponible"

Nota
Esto es más común en Mac.

Causa: Cuando se inicia una desconexión de túnel, el daemon del servicio IPsec strongSwan se atasca en un bucle infinito. Esto dará lugar a que la interfaz gráfica no obtenga una respuesta para la desconexión y, en última instancia, agote el tiempo de espera y muestre el error como "Servicio no disponible".

Qué hacer (Mac):

1. Abra el Monitor de actividad y finalice el proceso de la interfaz gráfica de Sophos Connect.
2. Abra el Terminal y ejecute los siguientes comandos:

   ```
   sudo /bin/launchctl unload -w /Library/LaunchDaemons/
   com.sophos.connect.scvpn.plist
   ```

   ```
   sudo /bin/launchctl load -w /Library/LaunchDaemons/
   com.sophos.connect.scvpn.plist
   ```
3. Abra Sophos Connect y compruebe que se ha resuelto el error "Servicio no disponible".

Qué hacer (Windows):

1. Abra `cmd` como administrador y ejecute los siguientes comandos:

   ```
   net stop scvpn
   ```

   ```
   net start scvpn
   ```

2. Abra Sophos Connect y compruebe que se ha resuelto el error "Servicio no disponible".

Sophos Connect no puede establecer un túnel

Causa: Probablemente haya instalado primero el cliente de Sophos Connect y luego el cliente VPN SSL de Sophos.

Qué hacer: Desinstale ambos clientes y vuelva a instalar el cliente VPN SSL de Sophos y, a continuación, el cliente de Sophos Connect.

Nota
Deben instalarse en ese orden.

Se ha recibido un restablecimiento de conexión desde la puerta de enlace: <nombre de puerta de enlace>

Este mensaje se registra en el archivo `scvpn.log` (en la carpeta de instalación).

Causa: La configuración de VPN SSL se cambia en XG Firewall, un usuario se desconecta manualmente o se reinicia XG Firewall. Si la conexión utiliza VPN SSL a través de TCP, XG Firewall enviará una solicitud de restablecimiento de conexión. Si la conexión utiliza VPN SSL a través de UDP, dependiendo del período de tiempo de espera de inactividad, la conexión puede volver a conectarse automáticamente.

Qué hacer: Importe un nuevo archivo de configuración en el cliente de Sophos Connect y vuelva a conectarse. Si el administrador no le ha enviado el archivo, vaya al portal de usuario y descárguelo. De lo contrario, vaya al portal de usuario para descargar el archivo `ovpn`.

La conexión VPN SSL tiene elementos de menú de conexión automática y actualización de políticas atenuados.

Causa: Si la conexión VPN SSL se crea importando un archivo `ovpn`, estas opciones no estarán disponibles.

Qué hacer: Para activar estas opciones, debe crear una conexión mediante un archivo de aprovisionamiento. Añada estas opciones al archivo de aprovisionamiento. **Activar política** estará disponible después de conectarse por primera vez. Para activar **Conexión automática**, debe definir un valor `auto_connect_host` al que solo se pueda acceder en la red interna.

Ejemplo de un archivo de aprovisionamiento con los requisitos mínimos para activar la conexión automática:

```
[
 {
  "display_name": "<Introducir nombre de conexión>",
  "gateway": "<Introducir nombre de host o IP de la puerta de enlace>",
"auto_connect_host":" <Introducir nombre de host o IP del recurso de red
 interno>"
}
]
```

Error de VPN SSL

Causa: Error generado por el servicio OpenVPN.

Qué hacer: Vuelva a establecer la conexión. Si esto no funciona, reinicie el dispositivo e inténtelo de nuevo.

El puerto de administración no está disponible

Causa: Sophos Connect no puede reclamar el puerto TCP 25340, que es necesario para comunicarse con OpenVPN.

Qué hacer: Compruebe si se está ejecutando otra aplicación en el dispositivo que utiliza este puerto. Si es posible, salga de la aplicación. Si no soluciona este problema, Sophos Connect 2.0 no se puede ejecutar en el dispositivo. Si ninguna otra aplicación está utilizando este puerto, puede tratarse de una situación temporal. El restablecimiento de la conexión debería resolver el problema.

No se ha podido crear el archivo temporal

Causa: Sophos Connect utiliza un archivo temporal para pasar los atributos de conexión al servicio OpenVPN. Sophos Connect no ha podido crear el archivo en este dispositivo.

Qué hacer: Reinicie el dispositivo.

El servicio OpenVPN no está disponible

Causa: Es posible que el servicio OpenVPN no se haya iniciado.

Qué hacer: Si el tipo de inicio del servicio OpenVPN está establecido en **desactivado**, cámbielo a **manual** y reinicie el servicio Sophos Connect.

No se ha podido escribir en la canalización

Causa: Error generado por el cliente de Sophos Connect.

Qué hacer: Vuelva a establecer la conexión. Si esto no funciona, reinicie el dispositivo e inténtelo de nuevo.

2 Acerca de Sophos Connect Admin

En Sophos Connect Admin, puede importar archivos de configuración (`.tgb`) y establecer varias opciones para la configuración de VPN.

Nota
Para obtener información sobre cómo configurar y exportar un archivo .tgb en XG, consulte la sección Cliente de Sophos Connect de la guía de ayuda de XG: Cliente de Sophos Connect.

Los procesos de instalación y desinstalación de Sophos Connect Admin son los mismos que los de Sophos Connect. Consulte Instalación en la guía de ayuda de Sophos Connect para obtener más información.

2.1 Edición de archivos de configuración

Puede editar los archivos de configuración (`.tgb`) en Sophos Connect Admin, que le proporciona opciones de configuración VPN más granulares.

Abra el archivo `.tgb` que ha exportado desde XG en Sophos Admin. Puede:

- Active **Tunelizar todo** para enviar todo el tráfico a través de la conexión VPN.
- Active **Enviar Security Heartbeat** para permitir que Sophos Endpoint envíe un latido a XG. Esto solo funcionará si el usuario tiene instalado el cliente de Sophos Endpoint en su equipo.
- Active **Permitir guardar contraseña** para permitir a los usuarios guardar su nombre de usuario y contraseña en su equipo. Las credenciales de usuario se almacenan de forma segura mediante servicios de llavero.
- Active **Solicitar 2FA** si ha configurado la autenticación de dos factores para los usuarios de VPN en XG.
- Active **Túnel de conexión automática** para activar automáticamente la conexión después de que el usuario inicie sesión en Sophos Connect en su equipo. Sophos Connect no iniciará automáticamente la conexión si el usuario ya está conectado a la red corporativa.

  La conexión automática requiere un parámetro de configuración adicional: **Host de supervisión/sufijo DNS**, que se puede utilizar para determinar si el sistema local del usuario está dentro o fuera de la red corporativa. Utilice uno de los valores siguientes:

  — Una dirección IP.

  — Un nombre de dominio completo (FQDN). El nombre de host solo se debe resolver cuando se utiliza el servidor DNS interno.

  — Un sufijo DNS.

  Nota
  Si configura una dirección IP o FQDN, debe permitirse ICMP en este host.

- Añada, modifique y elimine **redes** a las que el usuario puede conectarse. Añadir redes específicas a la lista permite los túneles divididos, ya que el usuario accederá a los recursos de esas redes a través de la conexión VPN, pero accederá a los recursos de Internet directamente a través de su puerta de enlace remota.

Nota
Si elimina todas las redes, se activará el modo **Tunelizar todo**, lo que significa que todo el tráfico se dirigirá a través de la conexión VPN.

- Cambie el **Nombre de conexión** y el **Host de destino**.

  Si opta por **Borrar** la configuración, tendrá que importar el archivo `.tbg` de nuevo.

  Si decide **Guardar** la configuración, se guardará como un archivo `.scx`.

  Nota
  Puede importar archivos `.scx` y volver a editarlos.

Una vez guardado el archivo de configuración, puede enviarlo al usuario, quien lo importará a Sophos Connect. Para obtener más información, consulte Sophos Connect.

3 Aviso legal