paloalto TECHDOCS

Guía del usuario de la aplicación de GlobalProtect

Version 6.3

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

October 24, 2024

Table of Contents

Aplicación de GlobalProtect para Windows

GlobalProtect™ es una aplicación que se ejecuta en su endpoint (ordenador de escritorio, portátil, tableta o teléfono inteligente) para protegerlo mediante el uso de las mismas políticas de seguridad que protegen los recursos sensibles de su red corporativa. GlobalProtect™ protege su tráfico de centro de datos, nube privada, nube pública e Internet, y le permite acceder a los recursos de su empresa desde cualquier parte del mundo.

Los siguientes temas describen cómo instalar y utilizar la aplicación de GlobalProtect para Windows:

Descargar e instalar la aplicación GlobalProtect para Windows

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints Windows	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Antes de conectarse a la red de GlobalProtect, debe descargar e instalar la aplicación de GlobalProtect en su endpoint Windows. Para asegurarle de que obtiene la aplicación correcta para la implementación de GlobalProtect o Prisma Access de su organización, debe descargar la aplicación directamente desde un portal de GlobalProtect dentro de su organización. Por esta razón, no hay un enlace de descarga directa de la aplicación de GP disponible en el sitio web de Palo Alto Networks.

Antes de que pueda descargar e instalar la aplicación GP, debe obtener la dirección IP o el nombre de dominio completo (FQDN) del portal de GlobalProtect de su administrador de GP. Además, su administrador debe verificar qué información de nombre de usuario y contraseña puede usar para conectarse al portal y a las puertas de enlace. En la mayoría de los casos, el nombre de usuario y la contraseña son el mismo nombre de usuario y contraseña que usa para conectarse a su red corporativa. Después de recopilar la información requerida, siga los siguientes pasos para descargar e instalar la aplicación:

Para ejecutar la aplicación de GlobalProtect 5.0 y versiones posteriores, los endpoints Windows requieren los componentes redistribuibles de Visual C++ 12.0.3 para Visual Studio 2013. Si aún no ha instalado ningún paquete redistribuible en su endpoint, la aplicación de GlobalProtect instala Visual C++ Redistributables 12.0.3 automáticamente. Si ya has instalado Visual C++ Redistributables 12.0.2 o una versión anterior, debe desinstalar los paquetes redistribuibles existentes de su endpoint o actualizar a Visual C++ Redistributables 12.0.3 antes de instalar la aplicación de GlobalProtect.

STEP 1 | Inicie sesión en el portal de GlobalProtect.

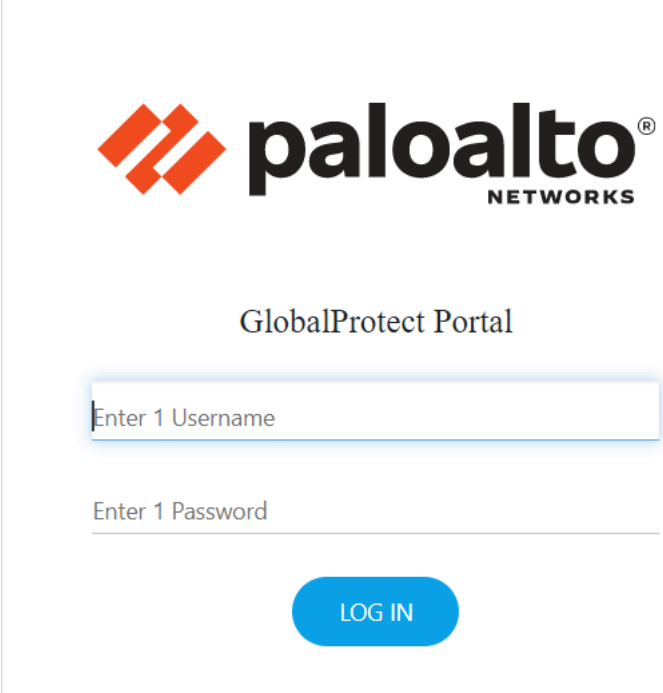
1. Inicie un navegador web y vaya a la siguiente URL:

   `https://<portal IP address or FQDN>`

   Ejemplo: **`HTTP://gp.acme.com`**

   Si está ejecutando GlobalProtect 6.3 o posterior y ha preimplementado la función de portal inteligente, GlobalProtect le redirige automáticamente al portal de Prisma Access apropiado según la ubicación de su país. Los portales definidos en el mapa del país del portal están disponibles en el menú desplegable. Para obtener más información, consulte Configurar el portal inteligente.
2. En la página de inicio de sesión del portal, introduzca su nombre de usuario en **Name (Nombre)** (nombre de usuario) y **Password (Contraseña)** y, a continuación, haga clic

en **LOG IN (Iniciar sesión)**. En la mayoría de los casos, puede usar el mismo nombre de usuario y contraseña que usa para conectarte a su red corporativa.



STEP 2 | Vaya a la página de descarga de la aplicación.

En la mayoría de las instancias, la página de descarga de la aplicación aparece inmediatamente después de que inicia sesión en el portal. Use esta página para descargar el paquete de software de la aplicación más reciente.

Si su administrador del sistema ha habilitado el acceso VPN sin cliente de GlobalProtect, se abre una página de aplicaciones (en lugar de la página de descarga de la aplicación) cuando inicia sesión en el portal. Seleccione **GlobalProtect Agent (Agente de GlobalProtect)** para abrir la página de descarga.

STEP 3 | Descargue la aplicación.

1. Para comenzar la descarga, haga clic en el enlace de software que corresponde al sistema operativo que ejecuta su ordenador. Si no está seguro de si el sistema operativo es de 32 bits o de 64 bits, pregunte a su administrador del sistema antes de continuar.
2. Abra el archivo de instalación del software.
3. Cuando se le solicite, proceda a **Run (Ejecutar)** el software.
4. Cuando se le solicite nuevamente, debe **Run (Ejecutar)** el Asistente de configuración de GlobalProtect.

STEP 4 | Complete la configuración de la aplicación de GlobalProtect.

1. En el Asistente de configuración de GlobalProtect, haga clic en **Next (Siguiente)**.
2. Haga clic en **Next (Siguiente)** para aceptar la carpeta de instalación por defecto (C:\Program Files\Palo Alto Networks\GlobalProtect) y luego haga clic en **Next (Siguiente)** dos veces.

   *Aunque puede **Browse (Examinar)** para seleccionar una ubicación diferente en la que instalar la aplicación de GlobalProtect, la práctica recomendada es instalarla en la ubicación predeterminada. La ubicación de instalación predeterminada es de solo lectura para usuarios sin privilegios y, por lo tanto, instalar en esta ubicación protege contra el acceso malicioso a la aplicación.*
3. Una vez completada la instalación, haga clic en **Close (Cerrar)** para cerrar el asistente.

Usar Conectar antes del inicio de sesión

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints Windows	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Los métodos de conexión previa al inicio de sesión y de inicio de sesión previo y bajo demanda no son compatibles simultáneamente con Connect Before Logon (Conectar antes de iniciar sesión).

Conectar antes del inicio de sesión no es compatible con las configuraciones de puertas de enlace internas.

Para simplificar el proceso de inicio de sesión y mejorar su experiencia, GlobalProtect ofrece Connect Before Logon (Conectar antes del inicio de sesión) para permitirle establecer la conexión VPN a la red corporativa antes de iniciar sesión en el endpoint Windows 10 mediante una tarjeta inteligente, un servicio de autenticación como LDAP, RADIUS o Security Assertion Markup Language (SAML), autenticación basada en nombre de usuario y contraseña o autenticación con contraseña de un solo uso (OTP). Los administradores pueden beneficiarse de la habilitación de Conectar antes del inicio de sesión cuando incorporan nuevos usuarios de GlobalProtect en el endpoint que no está configurado con un perfil o cuenta local para el usuario. Conectar antes del inicio de sesión está deshabilitado de forma predeterminada. Cuando el administrador habilita Conectar antes del inicio de sesión, puede iniciar el proveedor de credenciales de la aplicación de GlobalProtect y conectarse a la red corporativa antes de iniciar sesión en Windows endpoint. Después de que Conectar antes del inicio de sesión establezca una conexión VPN, puede usar la pantalla de inicio de sesión de Windows para iniciar sesión en el endpoint Windows. GlobalProtect puede actuar como proveedor de credenciales de proveedor de acceso previo al inicio de sesión (PLAP) para proporcionar acceso a su organización antes de iniciar sesión en Windows.

Debido a que Conectar antes del inicio de sesión le pide que se autentique dos veces en el portal y la puerta de enlace al iniciar sesión en el endpoint Windows por primera vez, la cookie Anular autenticación no funciona como se esperaba.

Para usar Conectar antes del inicio de sesión, el administrador debe implementar la configuración en el registro de Windows y elegir el método de autenticación:

- Conectar antes del inicio de sesión mediante autenticación con tarjeta inteligente
- Conectar antes del inicio de sesión mediante autenticación SAML)
- Conectar antes del inicio de sesión mediante autenticación basada en nombre de usuario y contraseña

Conectar antes del inicio de sesión mediante autenticación con tarjeta inteligente

Conectar antes del inicio de sesión es compatible con la autenticación con tarjeta inteligente El administrador debe importar el certificado CA raíz que emitió los certificados contenidos en la

tarjeta inteligente en el portal y la puerta de enlace. El administrador puede aplicar el perfil del certificado y esa CA raíz a su portal o configuración de puerta de enlace para habilitar el uso de la tarjeta inteligente en el proceso de autenticación. Puede autenticarse en GlobalProtect antes de iniciar sesión en el endpoint Windows con una tarjeta inteligente. Cuando se le solicite, inserte su tarjeta inteligente para verificar que la autenticación de la tarjeta inteligente sea correcta. Si la autenticación de la tarjeta inteligente es correcta, GlobalProtect se conectará al portal o puerta de enlace especificado en la configuración.

STEP 1 | Antes de poder usar Conectar antes del inicio de sesión, el administrador debe haber completado las siguientes tareas:

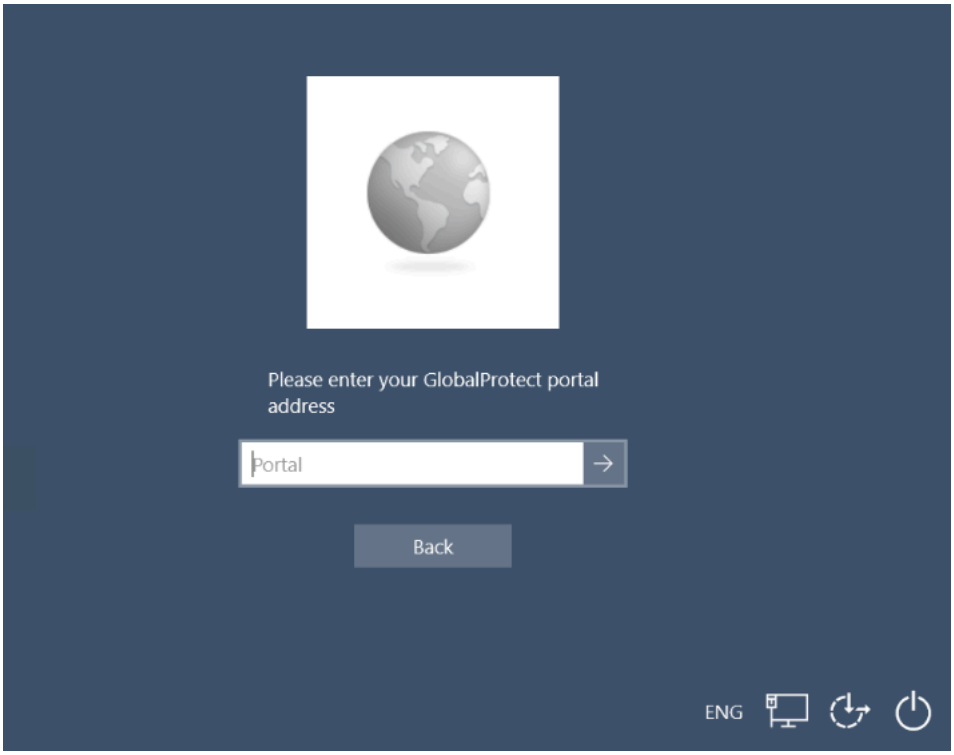
1. Implementar la configuración de Conectar antes del inicio de sesión en el registro de Windows.
2. Configurar la tarjeta inteligente para la autenticación de dos factores.
3. Asignar el perfil del certificado al portal de GlobalProtect.
4. Configurar la puerta de enlace para autenticar a los usuarios finales en una tarjeta inteligente.

STEP 2 | Inicie sesión en el endpoint de Windows utilizando Conectar antes del inicio de sesión.

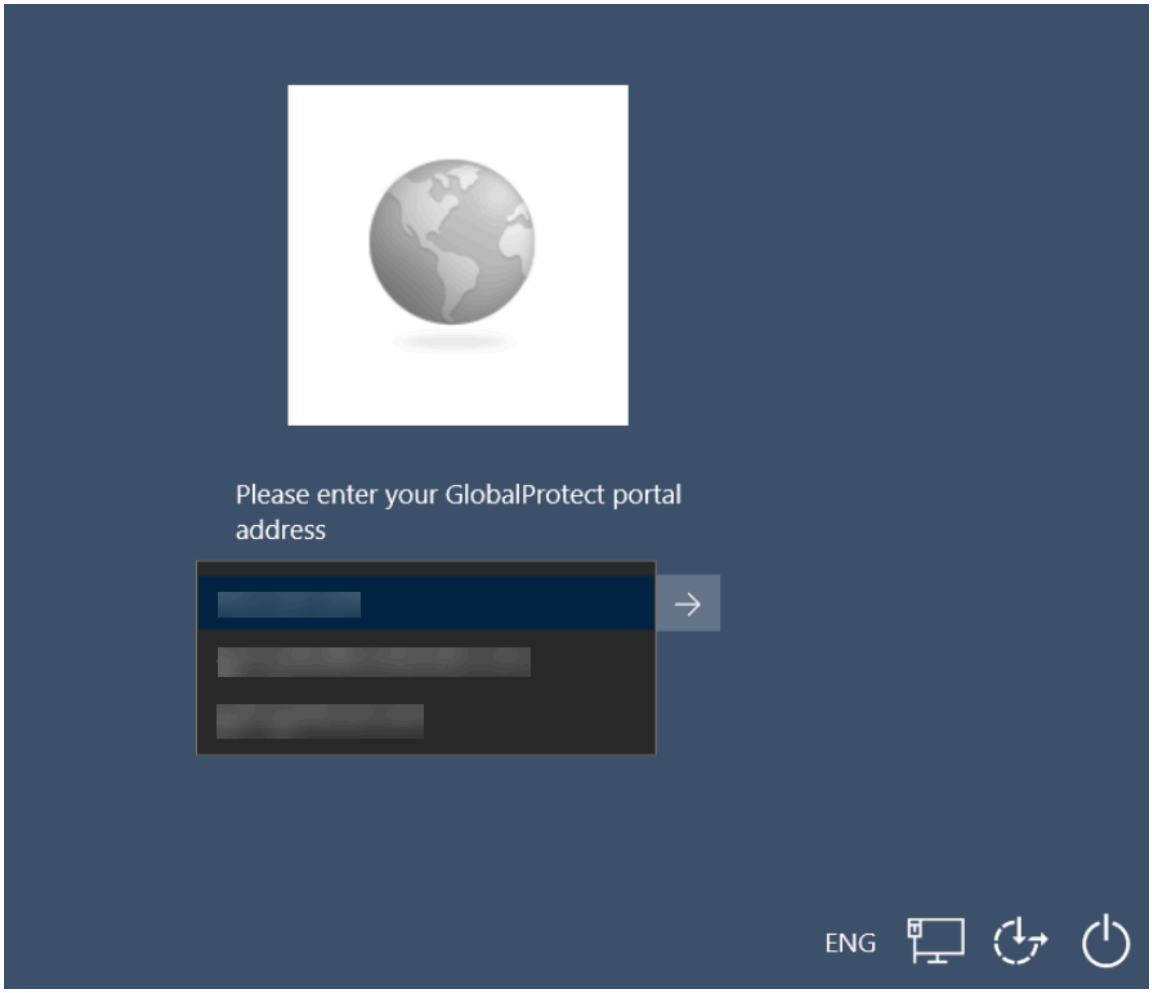
1. Haga clic en el botón **Network Sign-In (Inicio de sesión en red)** () en la esquina inferior derecha de la pantalla de inicio de sesión de Windows.

   Si la conexión VPN se realiza correctamente, aparece el botón **Disconnect (Desconectar)** () junto al botón **Network Sign-In (Iniciar sesión en red)** de la pantalla de inicio de sesión de Windows. Si aún no ha iniciado sesión en su endpoint dentro del período de tiempo configurado, se cerrará la sesión de la VPN. Esto hace que el túnel VPN se desconecte.

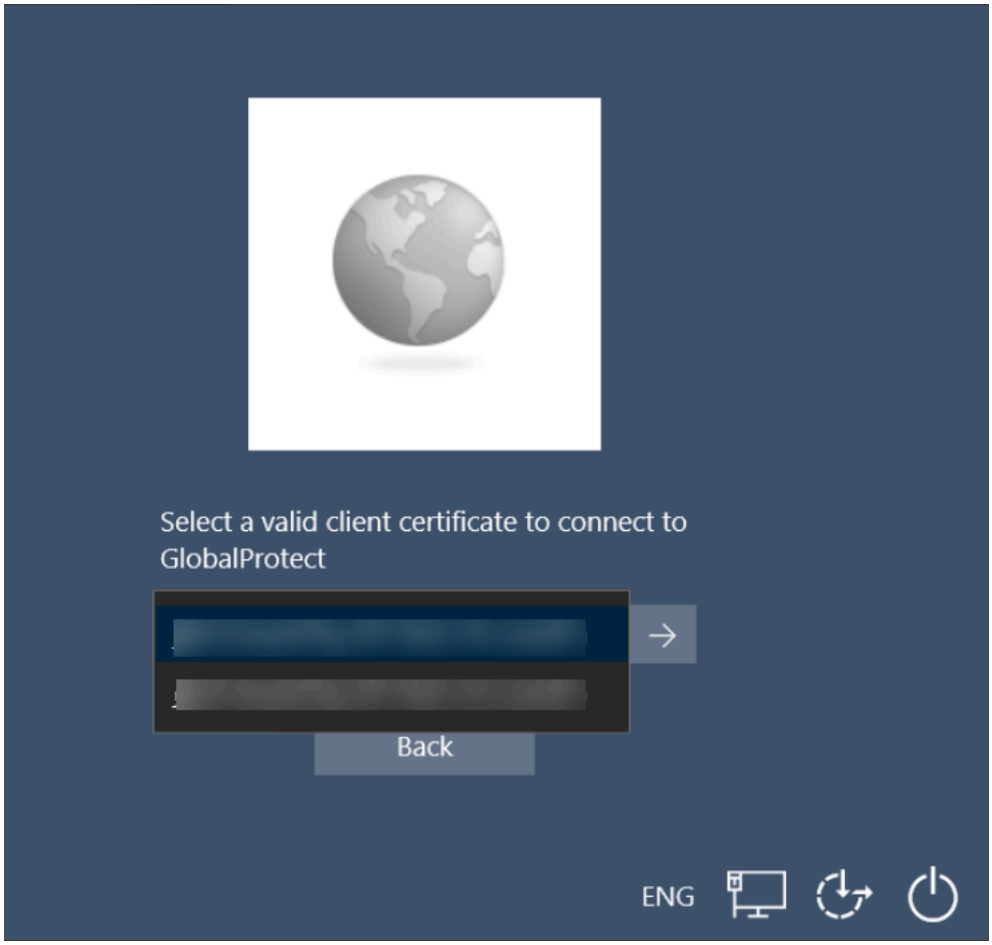
2. (Opcional) Si está iniciando sesión en el endpoint por primera vez y el administrador no ha predefinido los portales, introduzca el FQDN o dirección IP del portal de GlobalProtect y seleccione **Submit (Enviar)**.



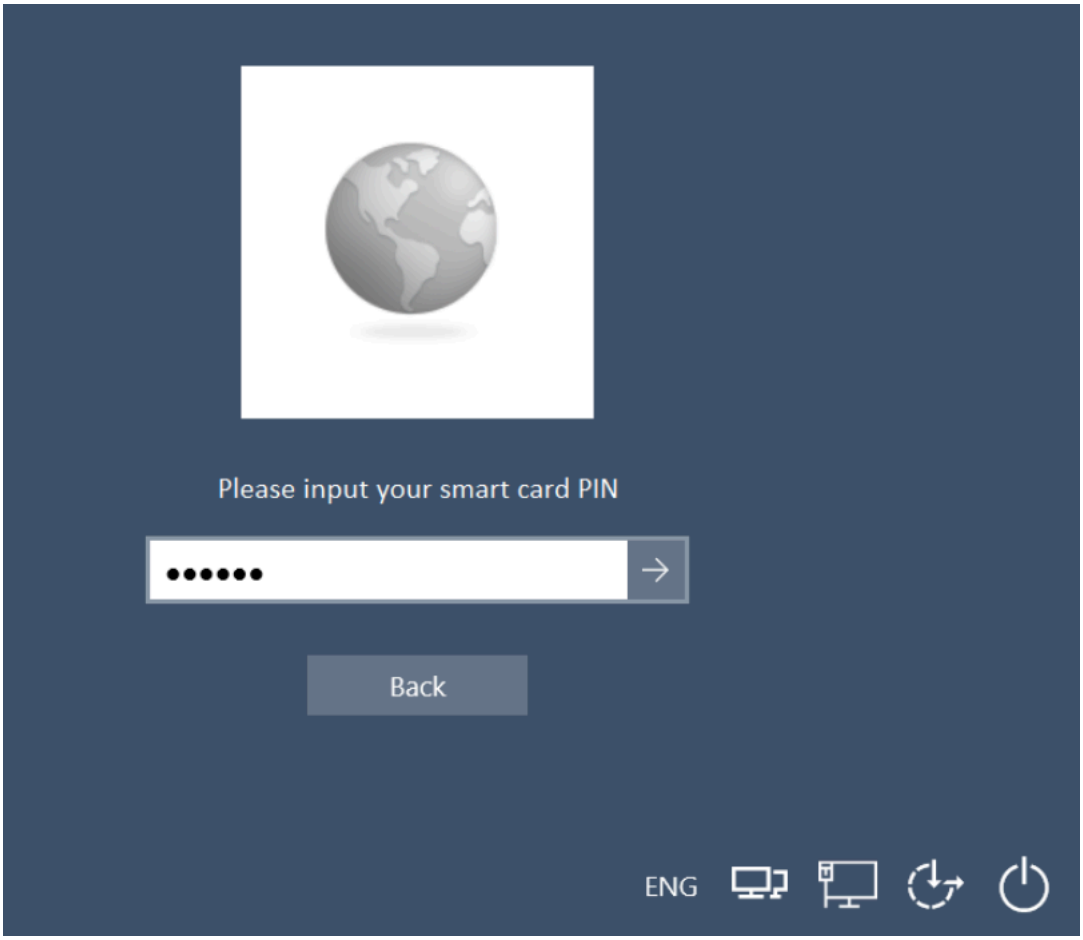
3. (Opcional) Si inicia sesión en el endpoint por primera vez y el administrador ha predefinido los portales, seleccione un portal en el menú desplegable **Portal** y haga clic en la flecha para enviar.



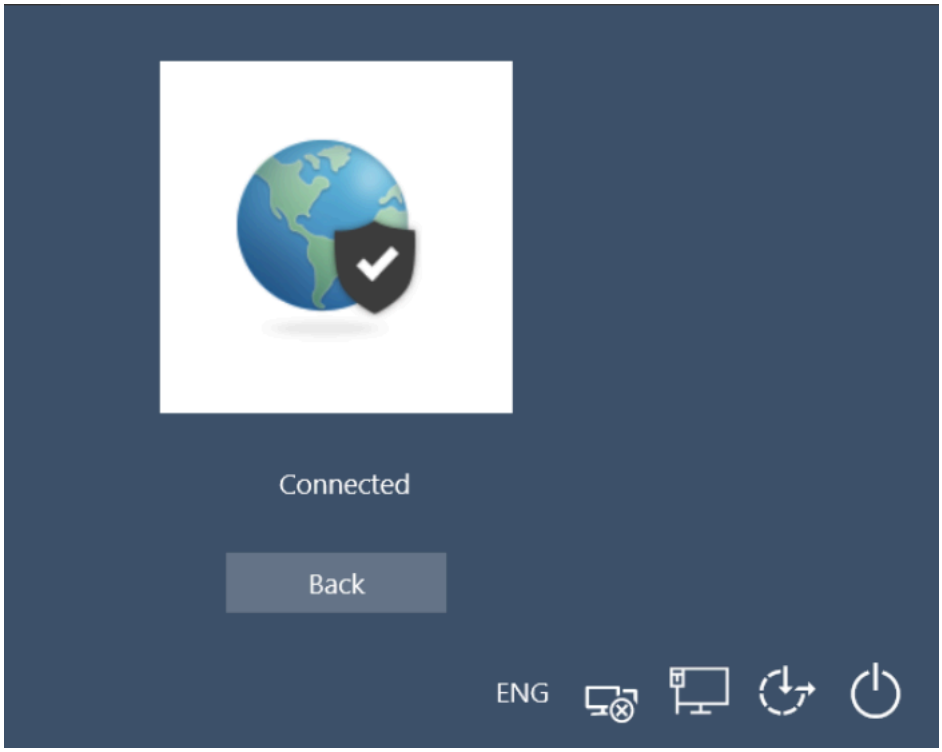
4. Seleccione el certificado cliente de una lista de certificados válidos en el endpoint para autenticarse con el portal o puerta de enlace y haga clic en la flecha para enviar.



5. Introduzca el número de identificación personal (PIN) de la tarjeta inteligente y haga clic en la flecha para enviar.



6. Si la autenticación se realiza correctamente, el estado de la conexión se muestra como **Connected (Conectado)** tras una conexión VPN correcta. Haga clic en **Back (Atrás)** para mostrar la pantalla de inicio de sesión de Windows.



STEP 3 | Compruebe que está conectado a la puerta de enlace de GlobalProtect.

1. Inicie sesión en el endpoint Windows de nuevo. Haga clic en el botón **Network Sign-In (Inicio de sesión en red)** ( ) en la esquina inferior derecha de la pantalla de inicio de sesión de Windows.
2. Se abre el panel de estado. De forma predeterminada, se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**.

Conectar antes del inicio de sesión mediante autenticación SAML)

Conectar antes del inicio de sesión admite autenticación SAML para el inicio de sesión de usuario. Puede autenticarse en GlobalProtect antes de iniciar sesión en el endpoint Windows utilizando los proveedores de identidad SAML (IdP) configurados, como OneLogin u Okta. Si la autenticación SAML se realiza correctamente, GlobalProtect se conectará al portal o puerta de enlace especificados en la configuración.

El método de autenticación Conectar antes del inicio de sesión con SAML es compatible con todas las versiones de GlobalProtect cuando se utiliza la vista web incrustada anterior (oew). Sin embargo, los errores de pantalla en blanco y JavaScript pueden mostrarse intermitentemente al cargar ciertas URL del IdP externo en el modo Conectar antes de iniciar sesión. Este problema surge del hecho de que la vista web incrustada anterior utiliza el navegador IE heredado, que ha quedado obsoleto en Windows 11. La alternativa basada en el navegador Edge WebView2 no es compatible con el método Conectar antes del inicio de sesión. GlobalProtect continuará utilizando la vista web incrustada antigua (oew) basada en IE heredada con la limitación anterior.

STEP 1 | Antes de poder usar Conectar antes del inicio de sesión, el administrador debe haber completado las siguientes tareas:

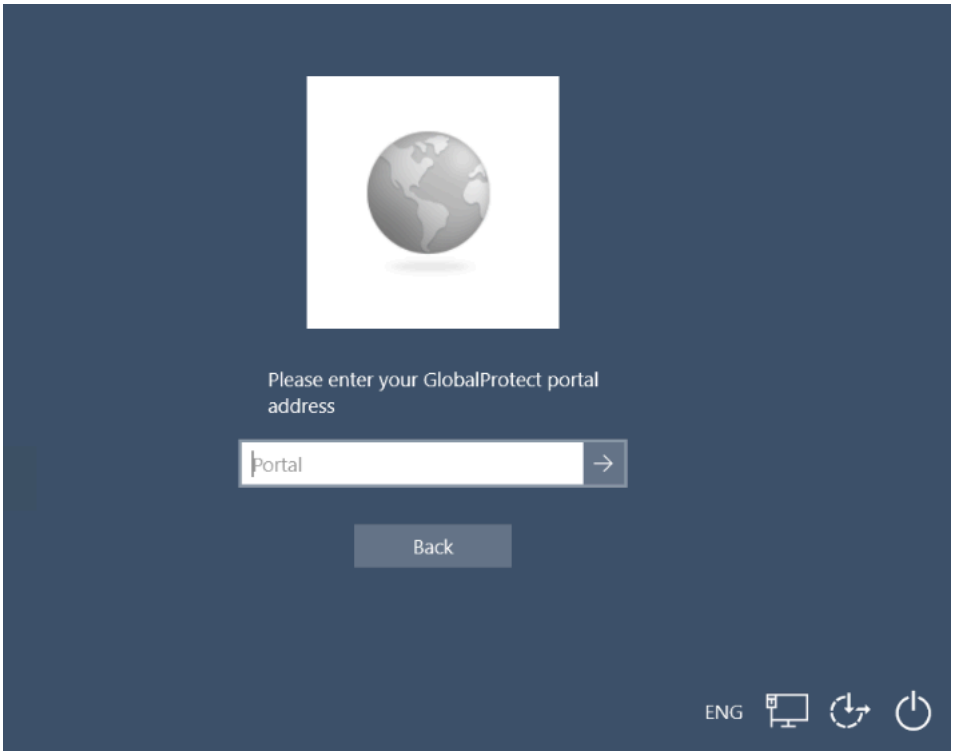
1. Implementar la configuración de Conectar antes del inicio de sesión en el registro de Windows
2. Configurar la autenticación SAML para autenticar usuarios finales.
   - Crear un perfil de servidor con la configuración del servicio de autenticación SAML.
   - Cree un perfil de autenticación que haga referencia al perfil de servicio.
3. Especifique la autenticación SAML para la puerta de enlace de GlobalProtect.
4. Especifique una autenticación SAML para el cliente (consulte Definir las configuraciones de autenticación del cliente de GlobalProtect).

STEP 2 | Inicie sesión en el endpoint de Windows utilizando Conectar antes del inicio de sesión.

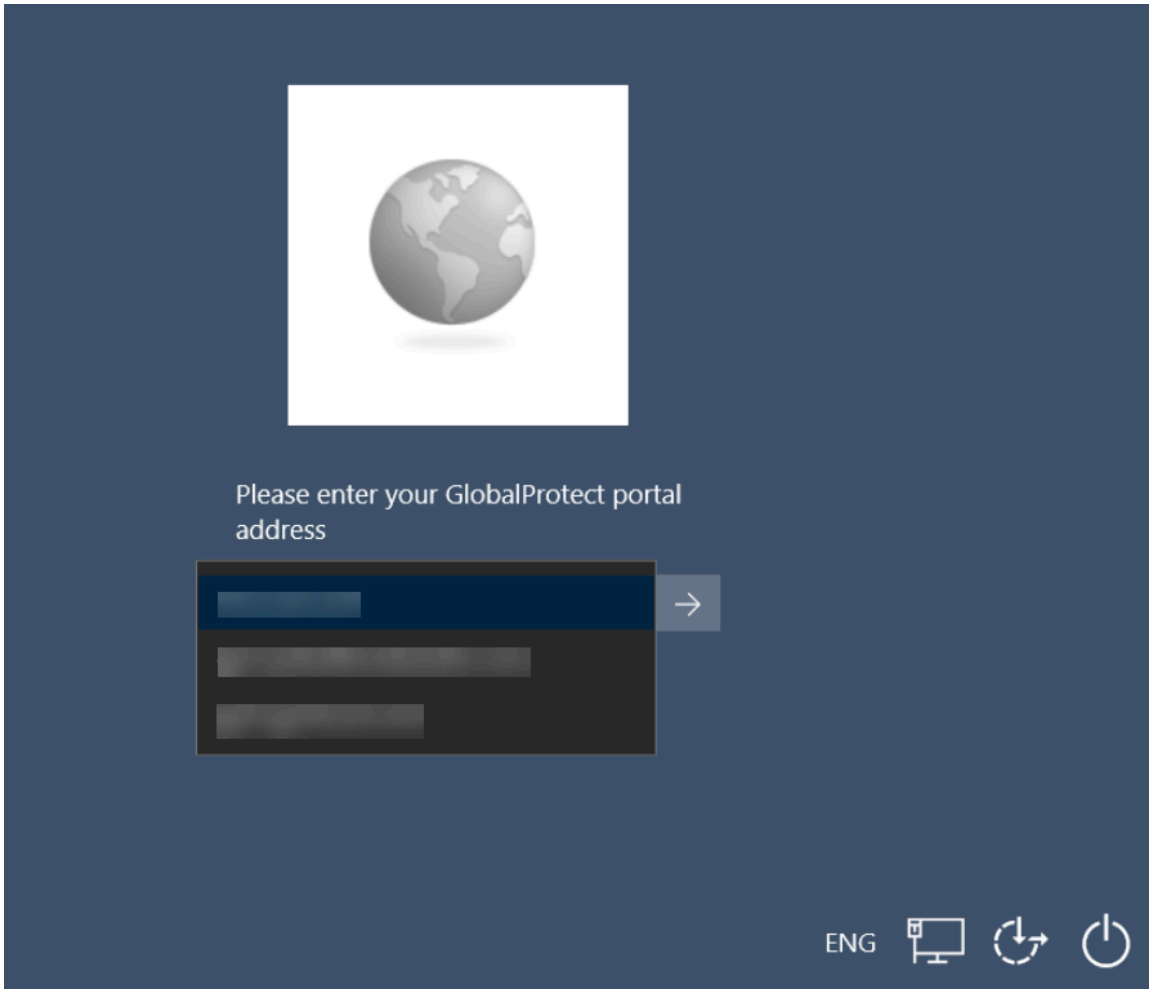
1. Haga clic en el botón **Network Sign-In (Inicio de sesión en red)** () en la esquina inferior derecha de la pantalla de inicio de sesión de Windows.

   Si la conexión VPN se realiza correctamente, aparece el botón **Disconnect (Desconectar)** () junto al botón **Network Sign-In (Iniciar sesión en red)** de la pantalla de inicio de sesión de Windows. Si aún no ha iniciado sesión en su endpoint dentro del período de tiempo configurado, se cerrará la sesión de la VPN. Esto hace que el túnel VPN se desconecte.

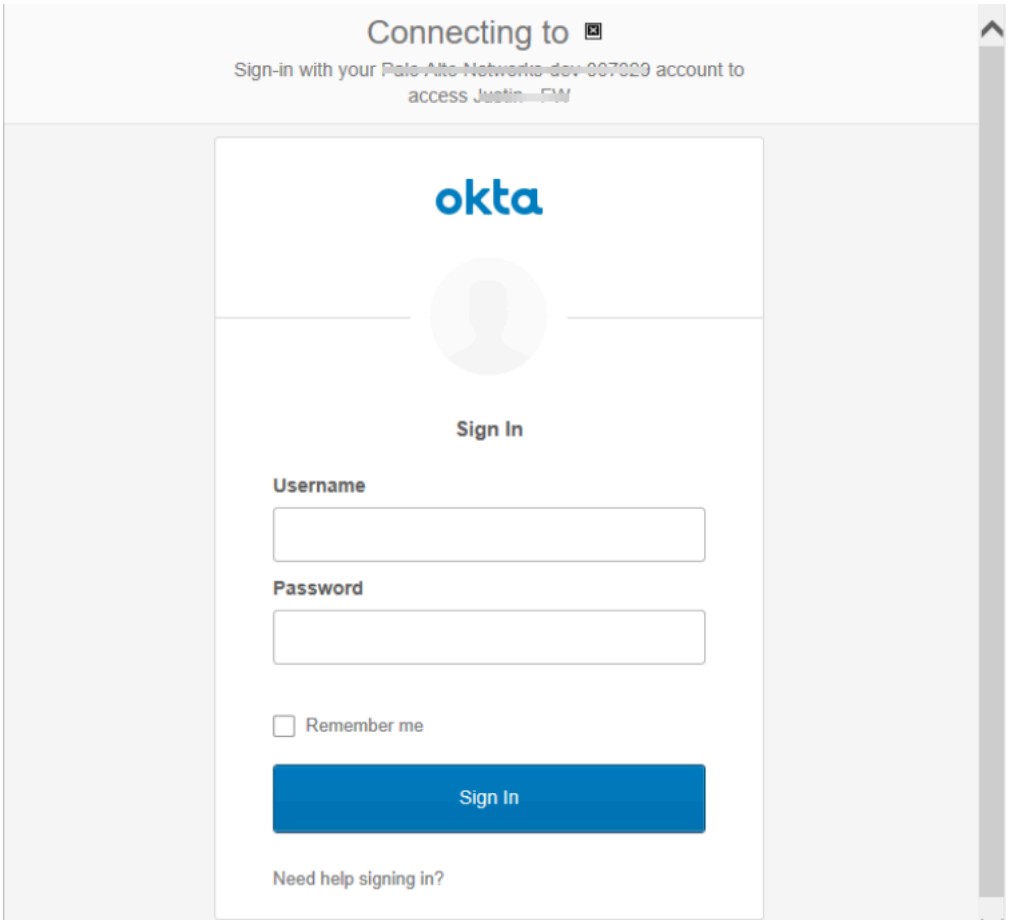
2. (Opcional) Si está iniciando sesión en el endpoint por primera vez y el administrador no ha predefinido los portales, introduzca el FQDN o dirección IP del portal de GlobalProtect y haga clic en la flecha para enviar.



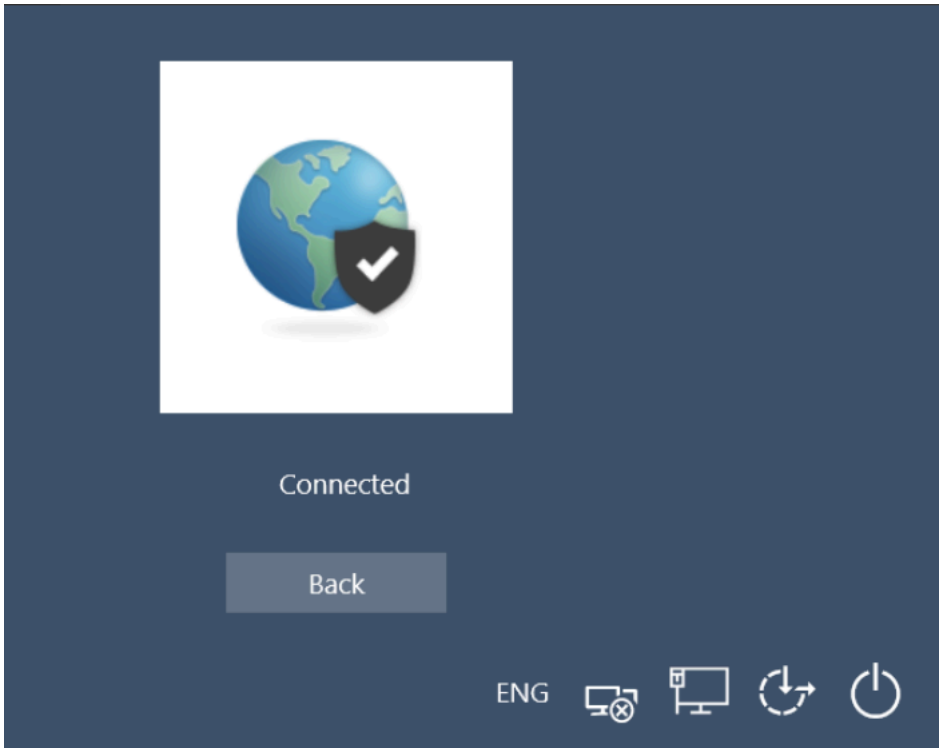
3. (Opcional) Si inicia sesión en el endpoint por primera vez y el administrador ha predefinido los portales, seleccione un portal en el menú desplegable **Portal** y haga clic en la flecha para enviar.



4. Introduzca el nombre de usuario y la contraseña para autenticarse en el IdP y, a continuación, haga clic en **Sign In (Iniciar sesión)**.



5. Si la autenticación se realiza correctamente, el estado de la conexión se muestra como **Connected (Conectado)** tras una conexión VPN correcta. Haga clic en **Back (Atrás)** para mostrar la pantalla de inicio de sesión de Windows.



STEP 3 | Compruebe que está conectado a la puerta de enlace de GlobalProtect.

1. Inicie sesión en el endpoint Windows de nuevo. Haga clic en el botón **Network Sign-In (Inicio de sesión en red)** ( ) en la esquina inferior derecha de la pantalla de inicio de sesión de Windows.
2. Se abre el panel de estado. De forma predeterminada, se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**.

Conectar antes del inicio de sesión mediante autenticación basada en nombre de usuario y contraseña

Conectar antes del inicio de sesión admite autenticación basada en nombre de usuario y contraseña para inicio de sesión de usuario mediante un servicio de autenticación como LDAP, RADIUS u OTP. Puede autenticarse en GlobalProtect antes de iniciar sesión en el endpoint Windows utilizando el nombre de usuario y contraseña. Si la autenticación basada en nombre de usuario y contraseña se realiza correctamente, GlobalProtect se conectará al portal o puerta de enlace especificados en la configuración.

STEP 1 | Antes de poder usar Conectar antes del inicio de sesión, el administrador debe haber completado las siguientes tareas:

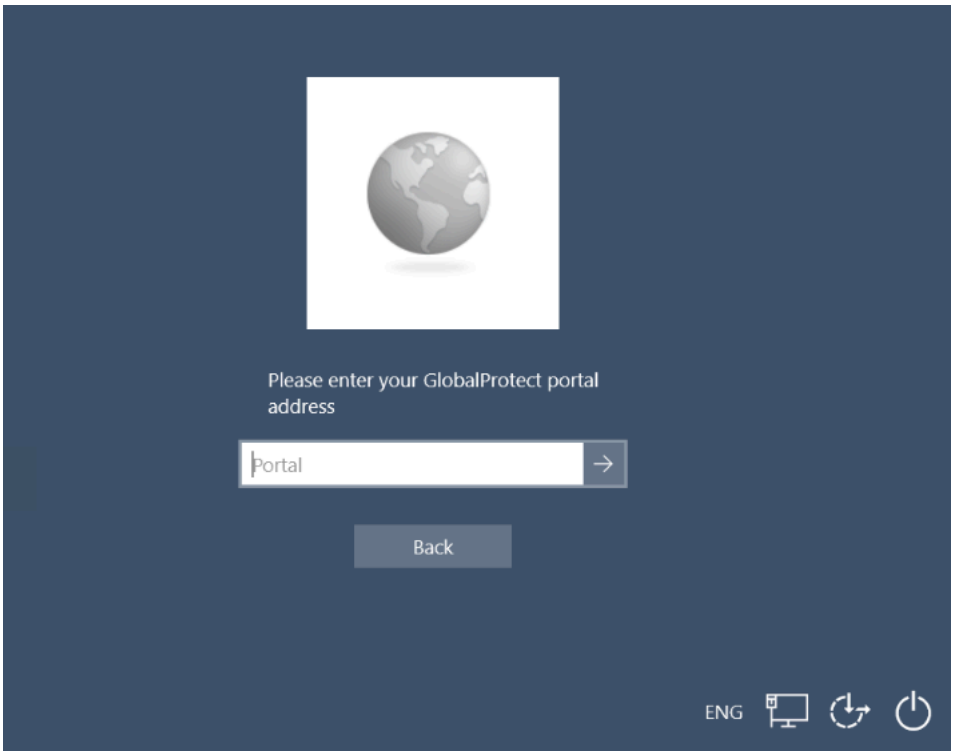
1. Implementar la configuración de Conectar antes del inicio de sesión en el registro de Windows
2. Configurar el acceso al portal de GlobalProtect para autenticar a los usuarios finales en el portal utilizando sus credenciales.
3. Configurar una puerta de enlace de GlobalProtect para autenticar a los usuarios finales en la puerta de enlace utilizando sus credenciales.

Conectar antes del inicio de sesión no admite un mensaje de autenticación personalizado.

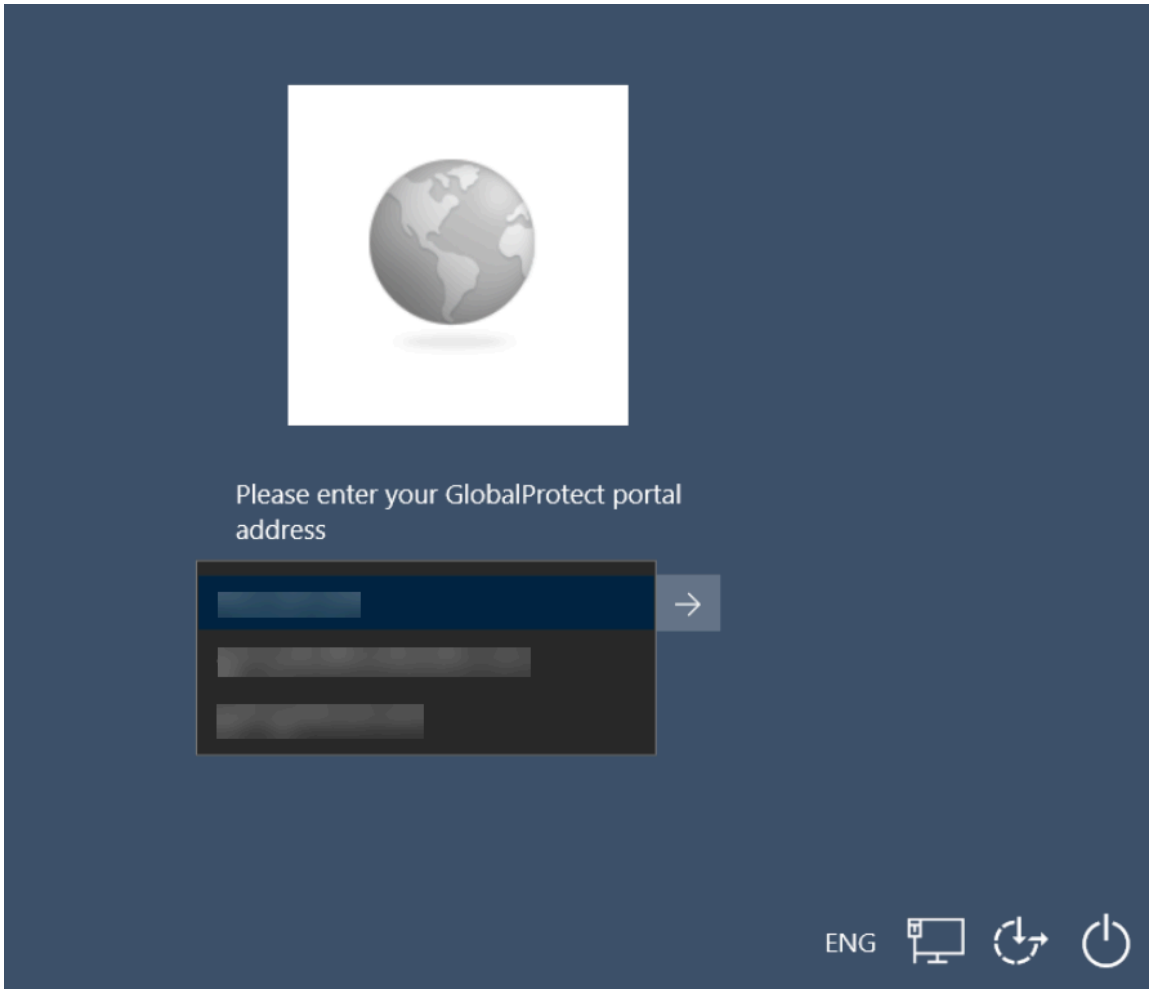
STEP 2 | Inicie sesión en el endpoint de Windows utilizando Conectar antes del inicio de sesión.

1. Haga clic en el botón **Network Sign-In (Inicio de sesión en red)** ( ) en la esquina inferior derecha de la pantalla de inicio de sesión de Windows.

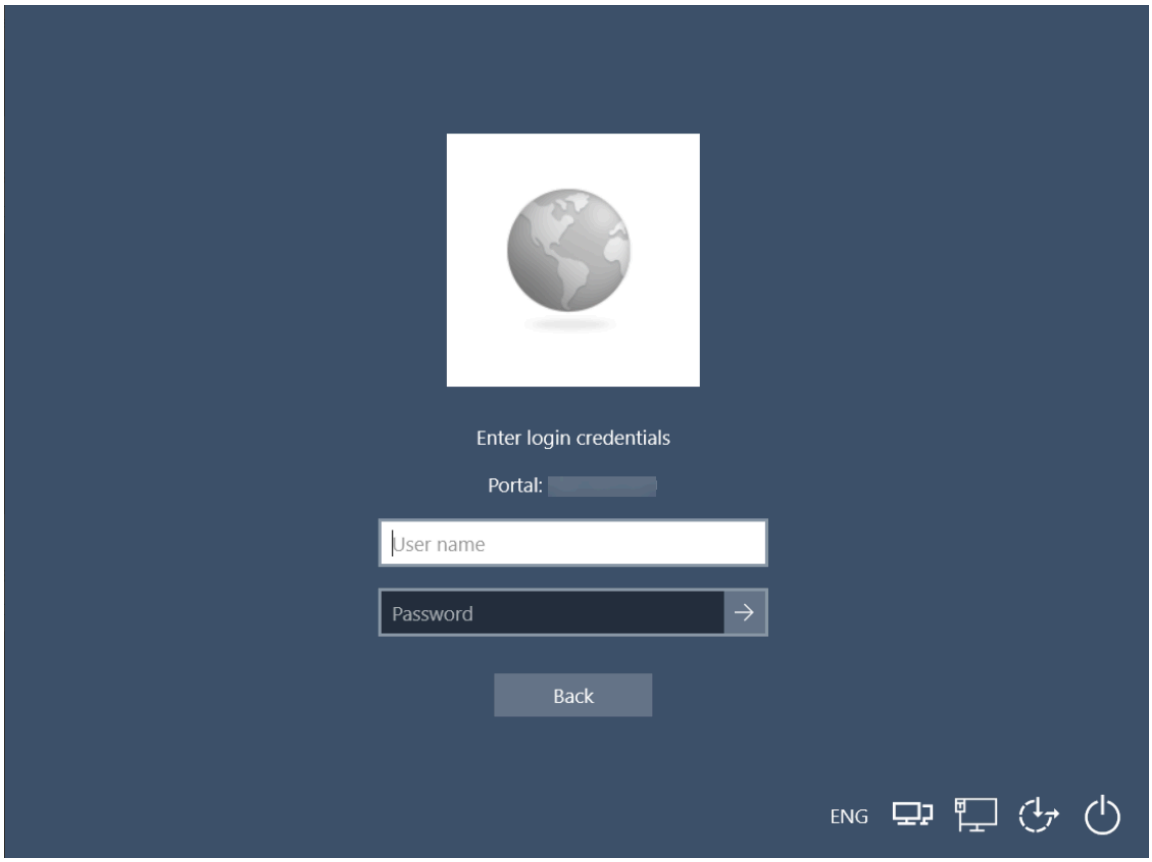
   Si la conexión VPN se realiza correctamente, aparece el botón **Disconnect (Desconectar)** ( ) junto al botón **Network Sign-In (Iniciar sesión en red)** de la pantalla de inicio de sesión de Windows. Si aún no ha iniciado sesión en su endpoint dentro del período de tiempo configurado, se cerrará la sesión de la VPN. Esto hace que el túnel VPN se desconecte.
2. (Opcional) Si está iniciando sesión en el endpoint por primera vez y el administrador no ha predefinido los portales, introduzca el FQDN o dirección IP del portal de GlobalProtect y haga clic en la flecha para enviar.



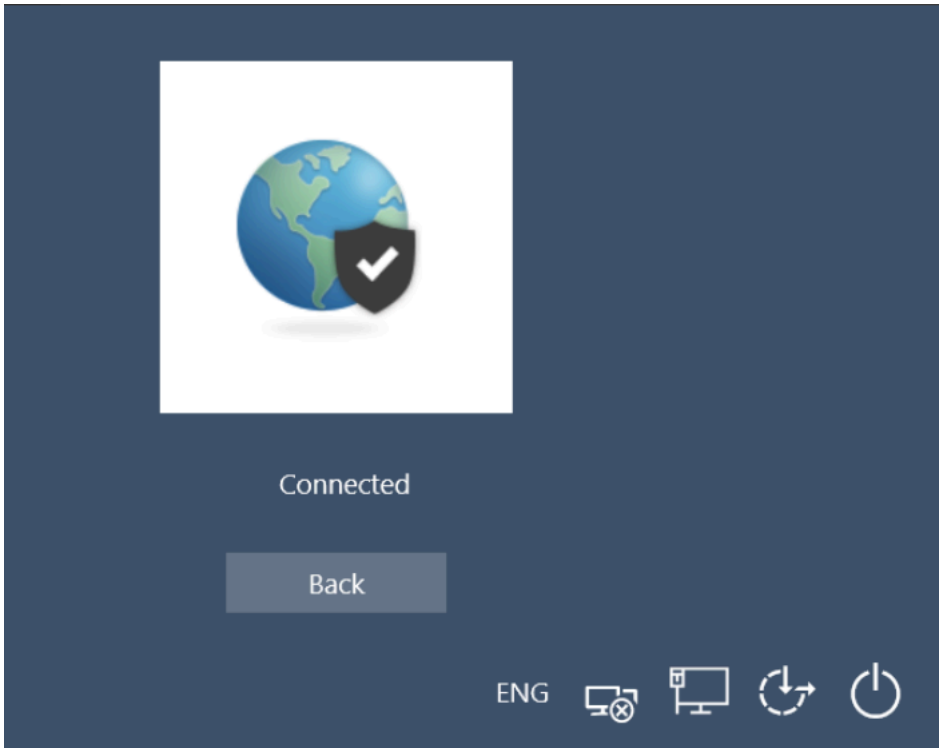
3. (Opcional) Si inicia sesión en el endpoint por primera vez y el administrador ha predefinido los portales, seleccione un portal en el menú desplegable **Portal** y haga clic en la flecha para enviar.



4. Introduzca el nombre de usuario y la contraseña, y haga clic en la flecha para enviar.



5. Si la autenticación se realiza correctamente, el estado de la conexión se muestra como **Connected (Conectado)** tras una conexión VPN correcta. Haga clic en **Back (Atrás)** para mostrar la pantalla de inicio de sesión de Windows.



STEP 3 | Compruebe que está conectado a la puerta de enlace de GlobalProtect.

1. Inicie sesión en el endpoint Windows de nuevo. Haga clic en el botón **Network Sign-In (Inicio de sesión en red)** ( ) en la esquina inferior derecha de la pantalla de inicio de sesión de Windows.
2. Se abre el panel de estado. De forma predeterminada, se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**.

Utilizar el inicio de sesión único para la autenticación mediante tarjeta inteligente

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints Windows	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si su administrador ha configurado el portal de GlobalProtect para permitirle autenticar mediante el inicio de sesión único (SSO) a través de la autenticación con tarjeta inteligente, puede conectar sin volver a introducir el número de identificación personal (PIN) de su tarjeta inteligente en la aplicación de GlobalProtect para una experiencia de SSO unificada. Puede aprovechar el mismo PIN de tarjeta inteligente para GlobalProtect con su endpoint Windows. Puede beneficiarse del uso del SSO para la autenticación de tarjetas inteligentes reduciendo el número de veces que debe introducir el PIN de su tarjeta inteligente cuando inicia sesión. Después de iniciar sesión correctamente en el endpoint de Windows, la aplicación de GlobalProtect adquiere y recuerda el PIN de su tarjeta inteligente para autenticarse con el portal y la puerta de enlace de GlobalProtect.

Su administrador puede definir el tipo de política de almacenamiento en caché del PIN para Windows que está asociada con el PIN del proveedor de la tarjeta inteligente. El PIN se almacena en caché solo si se permite desde el proveedor de la tarjeta inteligente. GlobalProtect borra el PIN de la caché si cierra sesión manualmente de la aplicación de GlobalProtect, cierra sesión en Windows o cambia el PIN.

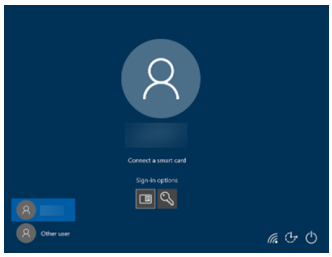
STEP 1 | Antes de poder utilizar el SSO para la autenticación de tarjetas inteligentes, el administrador debe haber completado las siguientes tareas:

1. Establezca el ajuste previo a la implementación en los endpoints de Windows para usar SSO para la autenticación de tarjetas inteligentes.

   Su administrador debe establecer el ajuste previo a la implementación en su endpoint Windows antes de habilitar el SSO para el PIN de la tarjeta inteligente. GlobalProtect recupera esta entrada solo una vez, cuando se inicializa la aplicación GlobalProtect.
2. Configurar la tarjeta inteligente para la autenticación de dos factores.
3. Asignar el perfil del certificado al portal de GlobalProtect.
4. Configurar la puerta de enlace para que pueda autenticarse con una tarjeta inteligente.
5. Habilite la aplicación de GlobalProtect para usar SSO para PIN de tarjeta inteligente en el portal de GlobalProtect, de modo que pueda vincular el mismo PIN de tarjeta inteligente para GlobalProtect con su endpoint Windows.

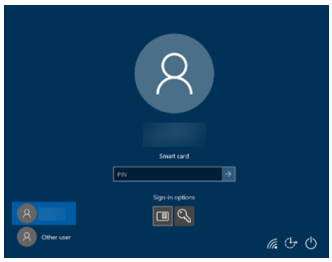
STEP 2 | Inicie sesión en el endpoint Windows con el PIN de la tarjeta inteligente.

1. Haga clic en **Sign-in options (Opciones de inicio de sesión)** y, a continuación, haga clic en el botón **smart card (tarjeta inteligente)** ( ).
2. Cuando se le solicite, inserte la tarjeta inteligente para verificar que la autenticación de la tarjeta inteligente sea correcta.



3. Introduzca el PIN de la tarjeta inteligente y haga clic en la flecha para enviar.

   Si la autenticación de la tarjeta inteligente se realiza correctamente, puede conectarse al portal o puerta de enlace especificados en la configuración sin tener que volver a introducir el PIN de su tarjeta inteligente.

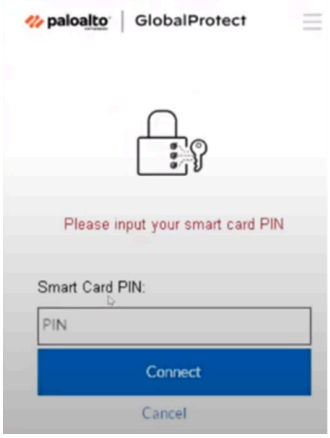


STEP 3 | (Opcional) Inicie sesión en GlobalProtect con el mismo PIN de tarjeta inteligente.

Puede aprovechar el mismo PIN de tarjeta inteligente que utilizó para iniciar sesión en su endpoint Windows.

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. Haga clic en el menú de tres barras para abrir el panel de **Settings (Configuración)**.
3. En el panel **Settings (Configuración)**, deberá **Sign Out (Cerrar sesión)** para borrar las credenciales de usuario guardadas de la aplicación de GlobalProtect.
4. Vuelva a conectarse a GlobalProtect con el mismo PIN de tarjeta inteligente.

   La aplicación GlobalProtect muestra un error de PIN de tarjeta inteligente si el PIN no es válido.



Usar la aplicación de GlobalProtect para Windows

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints Windows	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Este capítulo se aplica a su caso únicamente si su configuración requiere que introduzca sus credenciales de acceso de GlobalProtect después de haber iniciado sesión en su endpoint (el inicio de sesión único o 'single sign-on' está desactivado).

Por lo general, recomendamos que las organizaciones permitan que sus usuarios de GlobalProtect inicien sesión de manera transparente después de instalar la aplicación. Después de iniciar sesión en un endpoint con inicio de sesión GlobalProtect transparente, la aplicación de GlobalProtect inicia y se conecta automáticamente a la red corporativa sin intervención adicional del usuario.

Si su configuración requiere que introduzca sus credenciales de GlobalProtect, siga los pasos aplicables a continuación.

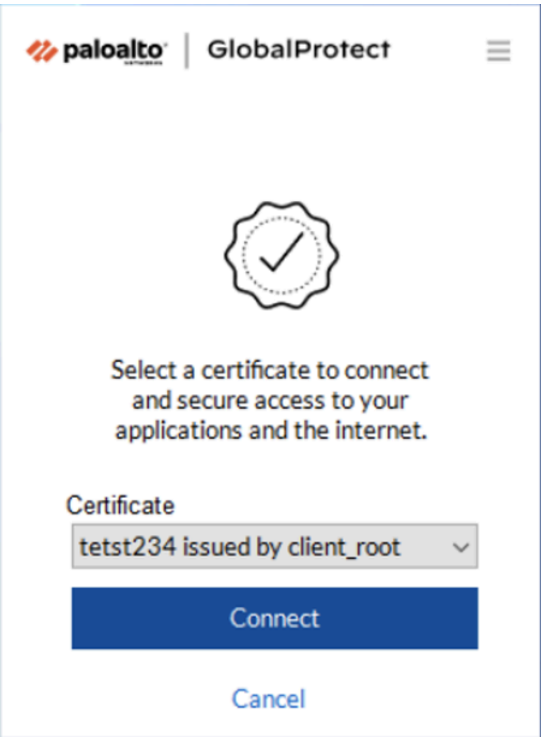
STEP 1 | Inicie sesión en GlobalProtect.

Si esta iniciando sesión en el endpoint por primera vez, la aplicación de GlobalProtect muestra una página de bienvenida tras el inicio de sesión correcto. Haga clic en **Get Started (Comenzar)**.

1. (Opcional) Si su administrador configura GlobalProtect con el método de conexión **On-Demand (Bajo demanda)** y está iniciando sesión en GlobalProtect por primera vez,

seleccione el certificado cliente de una lista de certificados válidos del menú desplegable **Certificate (Certificado)** para autenticarse con el portal o la puerta de enlace.

2. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.



3. (Opcional) Revise las condiciones de servicio de su empresa antes de conectarse a GlobalProtect si su administrador requiere que vea una página para acceder a recursos internos.

   Si no acepta las condiciones de uso, no podrá conectarse a GlobalProtect.

   Opcionalmente, si hace clic en **Cancel (Cancelar)**, debe introducir la dirección IP (o dominio) del portal de GlobalProtect y, a continuación, hacer clic en **Connect (Conectar)** para iniciar la conexión.

4. Introduzca la dirección IP o el dominio del portal que proporcionó su administrador de GlobalProtect y, a continuación, haga clic en **Connect (Conectar)**.

5. (Opcional) De manera predeterminada, usted se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, seleccione la puerta de enlace desde el menú desplegable **Change Gateway (Cambiar puerta de enlace)** (solo para puertas de enlace externas).

   Esta opción solo está disponible si su administrador habilita la selección manual de la puerta de enlace.

6. (Opcional) Dependiendo del modo de conexión, haga clic en **Connect (Conectarse)** para iniciar la conexión.
7. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** y haga clic en **Sign In (Iniciar sesión)**.

   Si su administrador le ha permitido usar información biométrica (huella digital) para iniciar sesión, primero debe iniciar sesión con un nombre de usuario y contraseña dos veces (una para guardarla y otra para autenticarse); luego puede usar información biométrica para iniciar sesión.

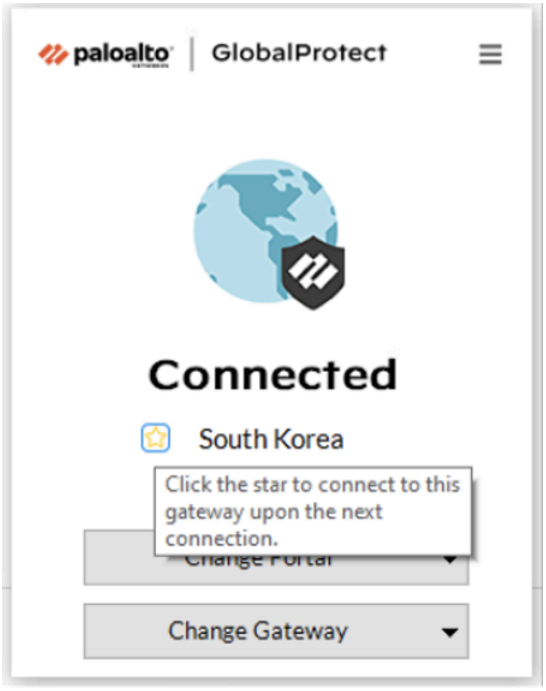
   Si la autenticación se realiza correctamente, usted está conectado a su red corporativa y el panel de estado muestra el estado **Connected (Conectado)** o **Connected - Internal (Conectado: interno)**. Si su administrador configura una página de bienvenida de GlobalProtect, esta se muestra después de un inicio de sesión correcto.

STEP 2 | Conéctese a la puerta de enlace o portal de GlobalProtect.

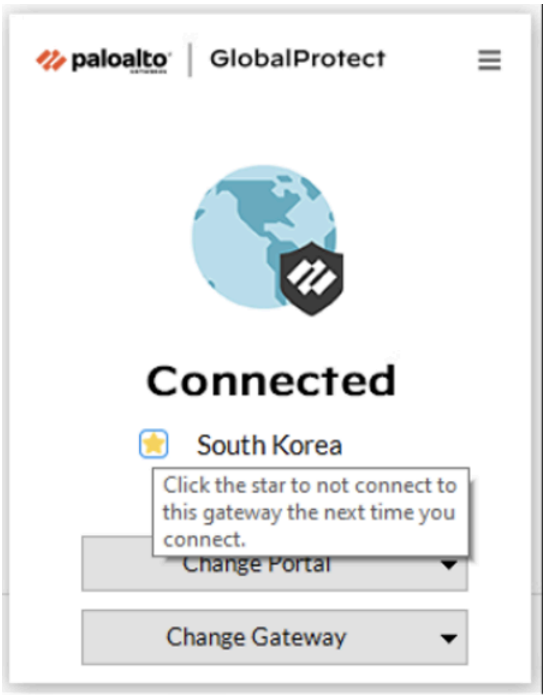
Puede determinar si está conectado marcando el icono de la bandeja del sistema de GlobalProtect. Si no está conectado, el icono está atenuado () y ***Not Connected (No conectado)*** *aparece cuando pasa el cursor sobre el icono.*

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. (Opcional) Si inicia sesión en la aplicación de GlobalProtect por primera vez, introduzca la dirección IP o el dominio del portal de GlobalProtect y, a continuación, haga clic en **Connect (Conectar)**.
3. (Opcional) Si se guardan varios portales en su aplicación, selecciona un portal en el menú desplegable **Change Portal (Cambiar portal)**. De forma predeterminada, el portal conectado más recientemente está preseleccionado en el menú desplegable **Change Portal (Cambiar portal)**.
4. (Opcional) De manera predeterminada, usted se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, haga clic en el menú desplegable **Change Gateway (Cambiar puerta de enlace)** y, a continuación, utilice una de las siguientes opciones:
   - Seleccione una puerta de enlace manualmente (solo puertas de enlace externas). Esta opción solo está disponible si su administrador habilita la selección manual de la puerta de enlace.

- Asigne y conéctese automáticamente a una puerta de enlace preferida:
  1. Para designar una puerta de enlace preferida, haga clic en el icono de estrella ( ). La próxima vez que se conecte, se conectará automáticamente a su puerta de enlace preferida designada.



Si más tarde decide que ya no desea esta puerta de enlace como su puerta de enlace preferida, puede borrar el icono de estrella. La próxima vez que se conecte, se conectará automáticamente a la mejor puerta de enlace disponible.



2. De forma predeterminada, se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)** que se identifica mediante una marca de verificación en el menú desplegable **Change Gateway (Cambiar puerta de enlace)**. Si establece la puerta de enlace preferida, una estrella aparecerá junto a la puerta de enlace destacada en el menú desplegable **Change Gateway (Cambiar puerta de enlace)**.

   Si su administrador configuró puertas de enlace externas manuales en la configuración del agente del portal, puede elegir una puerta de enlace específica utilizando el campo de búsqueda de puerta de enlace.

5. (Opcional) Dependiendo del modo de conexión, haga clic en **Connect (Conectarse)** para iniciar la conexión.
6. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** y luego haga clic en **Connect (Conectar)**.

   Si su administrador le ha permitido usar información biométrica (huella digital) para iniciar sesión, primero debe iniciar sesión con un nombre de usuario y contraseña dos veces (una para guardarla y otra para autenticarse); luego puede usar información biométrica para iniciar sesión.

Cuando la aplicación se conecta en modo externo, el icono de la bandeja del sistema de GlobalProtect muestra un escudo () y **Connected (Conectado)** aparece cuando pasa el cursor sobre el icono. Cuando la aplicación se conecta en modo interno, el icono de la bandeja del sistema de GlobalProtect muestra una casa () y la**Internal Network (Red interna)** aparece cuando pasa el cursor sobre el icono.

STEP 3 | Abra la aplicación GlobalProtect.

Haga clic en el icono de la bandeja del sistema de GlobalProtect para iniciar la interfaz de la aplicación.

Aparece una notificación si su administrador configuró el portal para instalar el agente de endpoint Autonomous DEM (ADEM) durante la instalación de la aplicación de GlobalProtect y le permitió habilitar las pruebas o no le permitió habilitar las pruebas. Si su administrador ya ha instalado el agente de endpoint ADEM y más tarde ha configurado el portal para desinstalar el agente de endpoint ADEM, aparecerá una notificación en el próximo inicio de sesión.

STEP 4 | Vea información sobre sus servicios de red.

Después de iniciar la aplicación, haga clic en el menú de tres barras en el panel de estado para abrir el menú de configuración. Seleccione **Settings (Configuración)** para abrir el panel **GlobalProtect Settings (Configuración de GlobalProtect)** y, a continuación, seleccione una de las siguientes configuraciones para ver y modificar la aplicación de GlobalProtect:

- **Connections (Conexiones)**: la pestaña **Connections (Conexiones)** muestra los portales asociados con la cuenta de GlobalProtect. Puede añadir, editar o eliminar portales desde esta pestaña. Esta pestaña también muestra la puerta de enlace a la que está conectado. Puede ver las estadísticas de conexión de la puerta de enlace (por ejemplo, la dirección IP de la puerta de enlace, la ubicación y el tiempo de actividad de la sesión VPN) cuando su

administrador establece **Enable Advanced View (Habilitar vista avanzada)** en **Yes (Sí)** en la configuración del agente del portal de GlobalProtect.

La pestaña **Connections (Conexiones)** también muestra el temporizador de cuenta regresiva para el inicio de sesión.

La pestaña **Connections (Conexiones)** muestra los detalles del proxy si la funcionalidad Conectividad mediante proxy explícito en GlobalProtect for Always-On Internet Security (Conectividad de proxy explícito en GlobalProtect para seguridad de Internet siempre activa) está habilitada para la aplicación a través de Prisma Access.

Modo proxy:

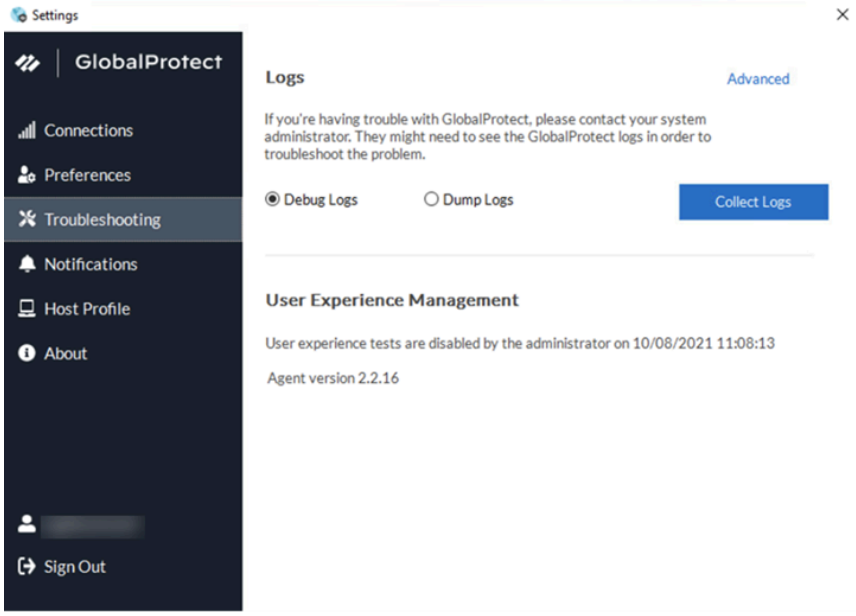
- **Preferences (Preferencias)**: la pestaña **Preferences (Preferencias)** ahora está disponible solo si su administrador configura al menos una de las siguientes opciones:
  - **Enable Biometric Sign-in (Habilitar inicio de sesión biométrico)**: puede optar por utilizar información biométrica (huella digital) para iniciar sesión. Esta opción está disponible solo si su administrador configura **Save User Credentials (Guardar credenciales de usuario)** en **Only with User Fingerprint (Solo con huellas digitales de usuario)** en la configuración del agente de GlobalProtect. Debe proporcionar una huella que coincida con una plantilla de huella fiable en el endpoint para usar una contraseña guardada para la autenticación en el portal y las puertas de enlace de GlobalProtect.
  - **Do not display a welcome page upon each successful connection (No mostrar una página de bienvenida en cada conexión correcta)**: puede elegir mostrar una página de bienvenida tras el inicio de sesión correcto. Esta opción solo está disponible si su administrador establece la **Welcome Page (Página de bienvenida)** en **factory-default** en la configuración del agente del portal de GlobalProtect.
  - **Connect with SSL (Conectar con SSL)**: puede elegir usar SSL o quedarse con IPSec. Esta opción solo está disponible si su administrador establece **Connect with SSL Only (Conectar solo con SSL)** en **User can Change (El usuario puede cambiar)** en la configuración del agente del portal de GlobalProtect.
  - **Always run diagnostic tests and include logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**: puede optar por habilitar la aplicación de GlobalProtect para que ejecute pruebas de diagnóstico e incluya logs de diagnóstico. Esta opción solo está disponible si su administrador habilita la recopilación de logs de la aplicación de GlobalProtect para la resolución de problemas en el portal de GlobalProtect.

- **Troubleshooting (Resolución de problemas)**: la pestaña **Troubleshooting (Resolución de problemas)** le permite **Collect Logs (Recopilar logs)** y establecer el nivel de creación de logs

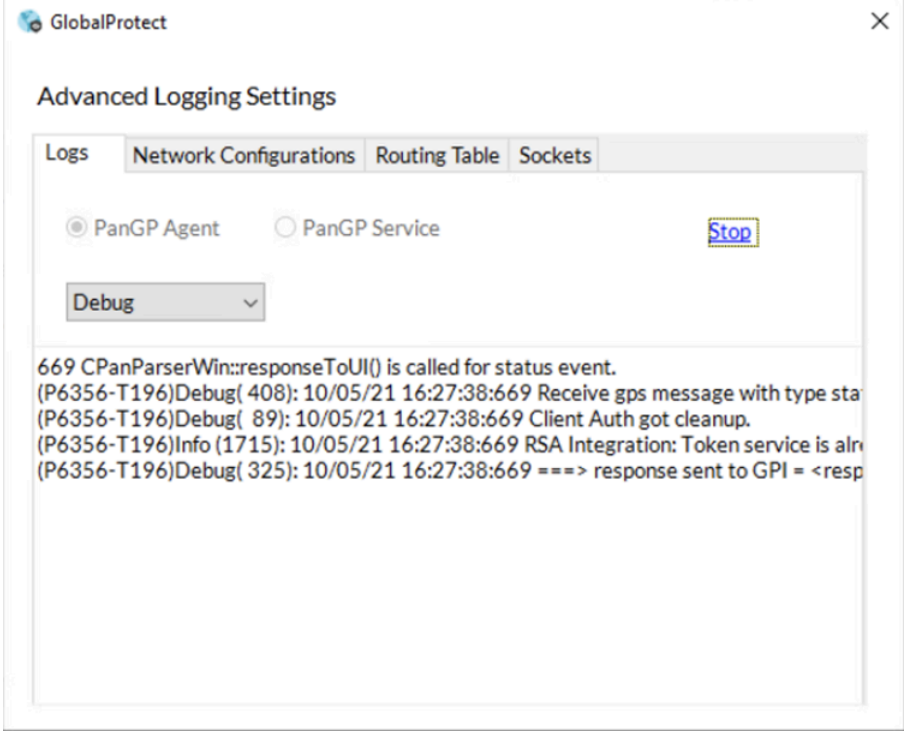
en **Debug Logs (Depurar logs)** o **Dump Logs (Volcar logs)** y opcionalmente **Enable User Experience Tests (Habilitar pruebas de experiencia de usuario)**.

A fin de que la aplicación de GlobalProtect envíe logs de solución de problemas, logs de diagnóstico o ambos a Strata Logging Service para un mayor análisis, debe configurar el portal de GlobalProtect para habilitar la recopilación de logs de la aplicación de GlobalProtect para la solución de problemas. Además, puede configurar las URL de destino basadas en HTTPS que pueden contener direcciones IP o nombres de dominio completos de los servidores/recursos web que desea sondear y determinar ciertos problemas, como la latencia o el rendimiento de la red, en el endpoint del usuario final.

Puede hacer clic en **Advanced (Avanzado)** para ver información detallada sobre su endpoint.



La ventana **Advanced Logging Settings (Configuración de creación de logs avanzada)**: muestra información sobre la configuración de red, la configuración de ruta, las conexiones activas y los logs.



Cuando GlobalProtect está conectado, puede verificar que el agente de endpoint de Autonomous DEM (ADEM) puede realizar pruebas de experiencia de usuario si la casilla de verificación **Enable user experience tests (Habilitar pruebas de experiencia de usuario)** se ve en la aplicación de GlobalProtect. O puede verificar que se muestre un mensaje si su administrador instaló el agente de endpoint ADEM durante la instalación de la aplicación GlobalProtect, pero no le permite habilitar o deshabilitar las pruebas de experiencia del usuario desde la aplicación GlobalProtect. De forma predeterminada, las alertas heartbeat aún se reenvían a ADEM incluso cuando GlobalProtect está deshabilitado o desconectado.

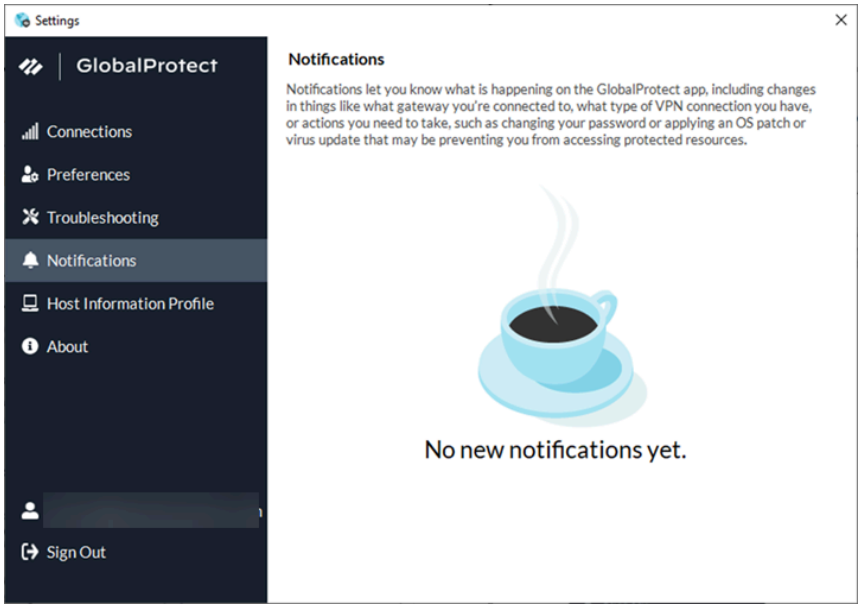
Si su administrador configuró el portal para instalar el agente de endpoint de Autonomous DEM durante la instalación de la aplicación de GlobalProtect y le permitió habilitar las pruebas, seleccione la casilla de verificación **Enable user experience tests (Habilitar pruebas de experiencia de usuario)** en la aplicación de GlobalProtect. Esta casilla de verificación no aparece si su administrador no le permite habilitar o deshabilitar las pruebas de experiencia del usuario desde la aplicación GlobalProtect. En su lugar, se muestra un mensaje que confirma que la aplicación está habilitada para ejecutar pruebas de experiencia de usuario.

Si no selecciona la casilla de verificación **Enable user experience tests (Habilitar pruebas de experiencia de usuario)**, las alertas de heartbeat continúan reenviándose a ADEM.

- **Notifications (Notificaciones)**: la pestaña **Notifications (Notificaciones)** muestra la información detallada sobre notificaciones específicas activadas en la aplicación de GlobalProtect. Puede configurar notificaciones de usuario final sobre el vencimiento

de las sesiones de la aplicación de GlobalProtect en la puerta de enlace y programar la visualización de estas notificaciones personalizadas en la aplicación.

También se le notificará si no hay nuevas notificaciones activadas en la aplicación GlobalProtect.

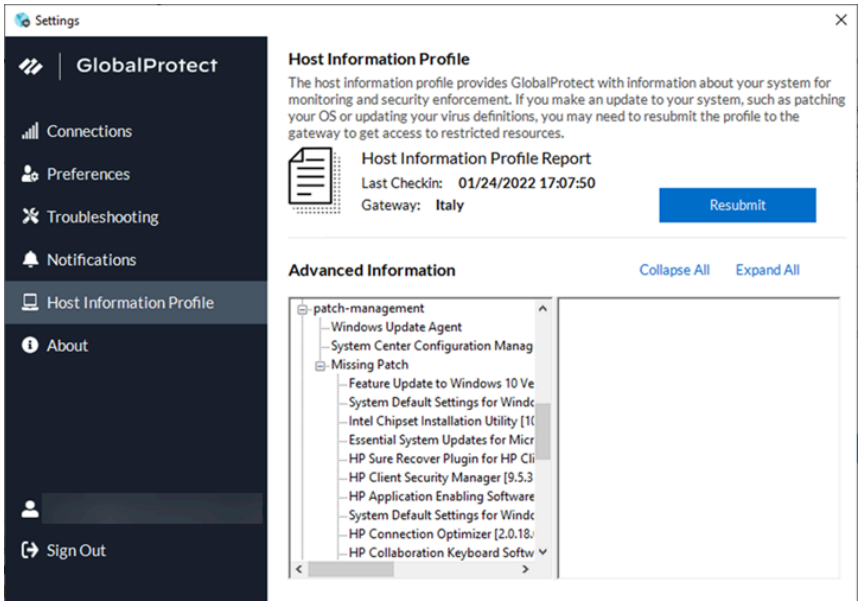


A partir de la versión 6.2.3 de la aplicación GlobalProtect, los mensajes de tiempo de espera de inactividad y sesión se suprimen para el método de conexión siempre activa.

A partir de la versión 6.2 de la aplicación de GlobalProtect, puede ampliar la duración de la sesión de inicio de sesión de la aplicación de GlobalProtect antes de que caduque para evitar el cierre abrupto de la sesión de la aplicación. La notificación de vencimiento de la duración del inicio de sesión le informa por adelantado cuando las sesiones de la aplicación están a punto de caducar y ofrece la opción de ampliar la duración de la sesión de usuario para que no se cierre la sesión abruptamente. La aplicación mostrará la notificación de vencimiento con la opción de ampliar la sesión de usuario si su administrador ha configurado los ajustes de notificación para ampliar la sesión.

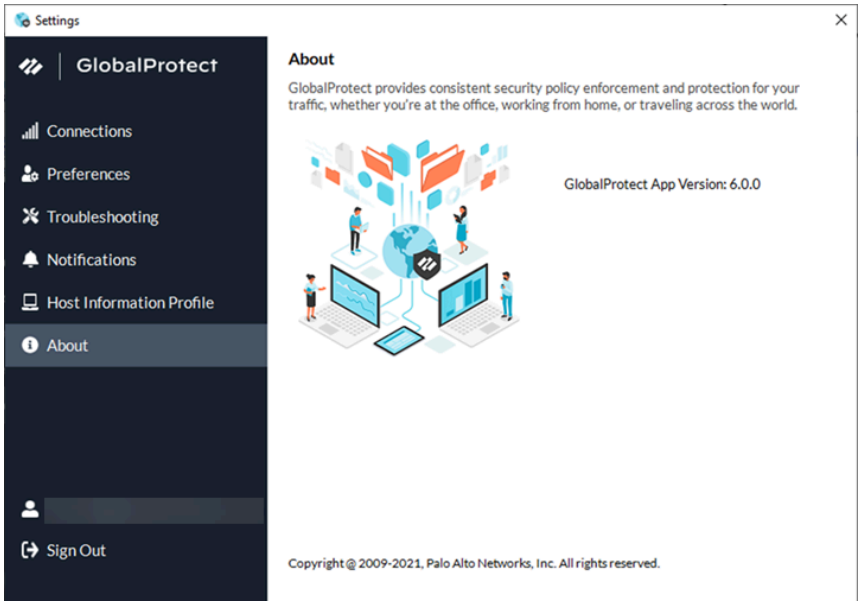
- **Host Information Profile (Perfil de información de host)**: la pestaña **Host Information Profile (Perfil de información de host)** muestra los datos de endpoint que utiliza GlobalProtect para supervisar y aplicar políticas a través del Host Information Profile (Perfil

de información de host). Puede **Resubmit (Volver a enviar)** manualmente datos HIP a la puerta de enlace.



Si su administrador configuró varias puertas de enlace internas en modo sin túnel y detección de host interno, puede hacer clic en **More Details (Más detalles)** para supervisar el envío de informes del perfil de información de host (Host Information Profile, HIP) para cada puerta de enlace desde una ubicación central para ayudarle a solucionar rápidamente problemas relacionados con HIP.

- **About (Acerca de)**: la pestaña **About (Acerca de)** muestra la versión de GlobalProtect instalada actualmente en el endpoint y le permite **Check for Updates (Buscar actualizaciones)**.



STEP 5 | (Opcional) Inicie sesión con una contraseña nueva.

*Si el administrador de GlobalProtect configura el agente del portal de GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, las credenciales se guardarán automáticamente en la aplicación de GlobalProtect. Si su contraseña de acceso a la red corporativa cambia, debe iniciar sesión en GlobalProtect con su nueva contraseña.*

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. Haga clic en el menú de tres barras para abrir el menú de configuración.
3. Seleccione **Settings (Ajustes)** para abrir el panel **GlobalProtect Settings (Ajustes de GlobalProtect)**.
4. En el panel **GlobalProtect Settings (Configuración de GlobalProtect)**, proceda a **Sign Out (Cerrar sesión)** para borrar las credenciales de usuario guardadas de la aplicación de GlobalProtect.
5. Después de borrar sus credenciales de usuario, puede volver a conectarse a GlobalProtect con su nuevo nombre de usuario y contraseña.

STEP 6 | (Opcional) Desconéctese de GlobalProtect.

Si su administrador configura GlobalProtect con el método de conexión **On-Demand (Bajo demanda)**, puede desconectarse de GlobalProtect haciendo clic en **Disconnect (Desconectar)** en el panel de estado.

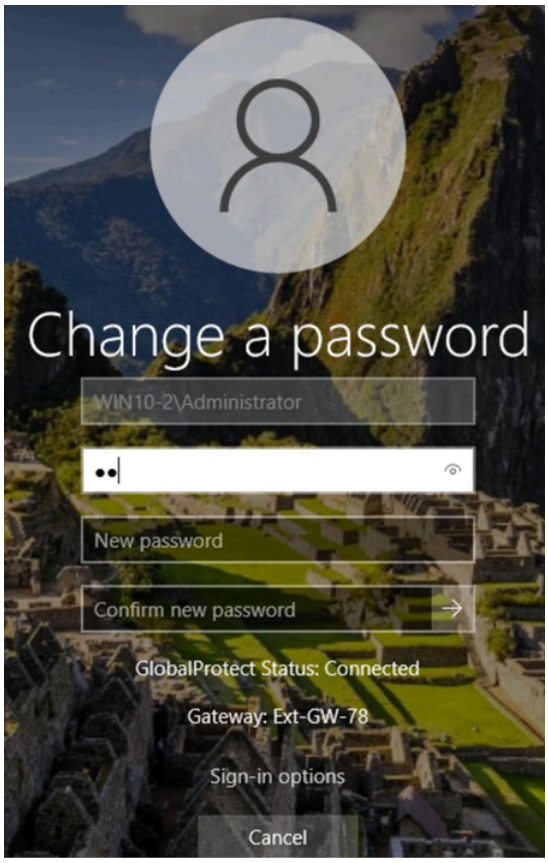
Mostrar contraseña en la pantalla de inicio de sesión de Windows para GlobalProtect

Al iniciar sesión en su escritorio de Windows 10 o Windows 11 o al cambiar su contraseña, puede hacer clic en el icono **Reveal Password (Mostrar contraseña)** para mostrar la contraseña mientras escribe. La contraseña se muestra en texto sin formato. Esta función ayuda a prevenir errores de escritura y reduce el riesgo de bloqueos de cuenta al permitirte confirmar su contraseña visualmente.

Esta función está disponible en GlobalProtect™ 6.3.3 y versiones posteriores, y se puede habilitar a través de una clave de registro. Para detalles sobre la clave de registro, consulte las Opciones de visualización de la aplicación.

La pantalla de inicio de sesión de Windows muestra el estado de conexión de GlobalProtect y la puerta de enlace, además del icono de mostrar contraseña en el campo de contraseña.

El cuadro de diálogo Cambiar contraseña muestra su nombre de usuario, nombre de dominio, estado de conexión de GlobalProtect y puerta de enlace, además del icono Mostrar contraseña en el campo de contraseña.



Informar de un problema desde la aplicación de GlobalProtect para Windows

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints Windows	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si experimenta un comportamiento inusual, como un rendimiento de red deficiente o si no se establece la conexión con el portal y la puerta de enlace, puede informar de la incidencia directamente a Strata Logging Service para que su administrador pueda acceder a ella Ya no es necesario recopilar y enviar manualmente los logs de aplicaciones de GlobalProtect por correo electrónico o almacenarlos en una unidad de nube.

*Para mostrar la opción **Report an Issue (Informar de un problema)** en la aplicación de GlobalProtect, su administrador debe habilitar la recopilación de logs de la aplicación de GlobalProtect para la resolución de problemas en el portal de GlobalProtect.*

STEP 1 | Conéctese a la puerta de enlace o portal de GlobalProtect.

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. (Opcional) Si inicia sesión en la aplicación de GlobalProtect por primera vez, introduzca el FQDN o la dirección IP del portal de GlobalProtect y luego haga clic en **Connect (Conectar)**.
3. (Opcional) Si se guardan varios portales en su aplicación, seleccione un portal en el menú desplegable **Portal**. De manera predeterminada, el portal conectado más recientemente está preseleccionado del menú desplegable **Portal**.
4. (Opcional) De manera predeterminada, usted se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, haga clic en el menú desplegable del gateway.

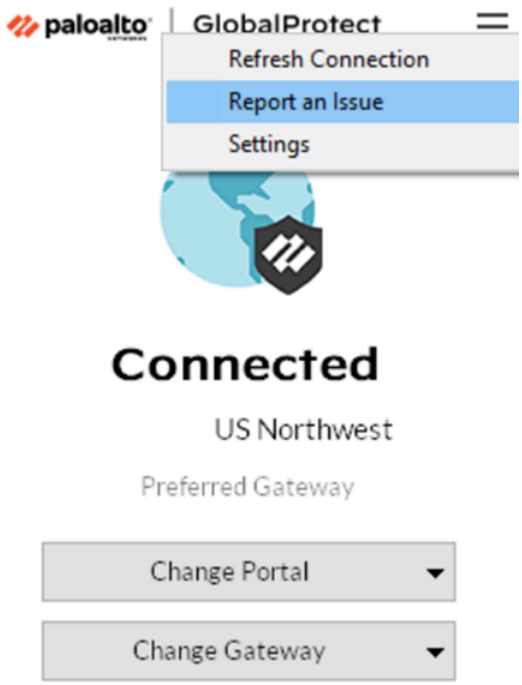
STEP 2 | Abra la aplicación GlobalProtect.

Haga clic en el icono de la bandeja del sistema de GlobalProtect para iniciar la interfaz de la aplicación.

STEP 3 | Informe de un problema desde la aplicación de GlobalProtect desde su endpoint.

Después de iniciar la aplicación, haga clic en el menú de tres barras del panel de estado para informar de un problema a su administrador.

1. Seleccione **Report an Issue (Informar de un problema)**.



2. Habilite la aplicación de GlobalProtect para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico. Los logs de diagnóstico y resolución de problemas se recopilan y envían a Strata Logging Service como un informe de resolución de problemas compacto.

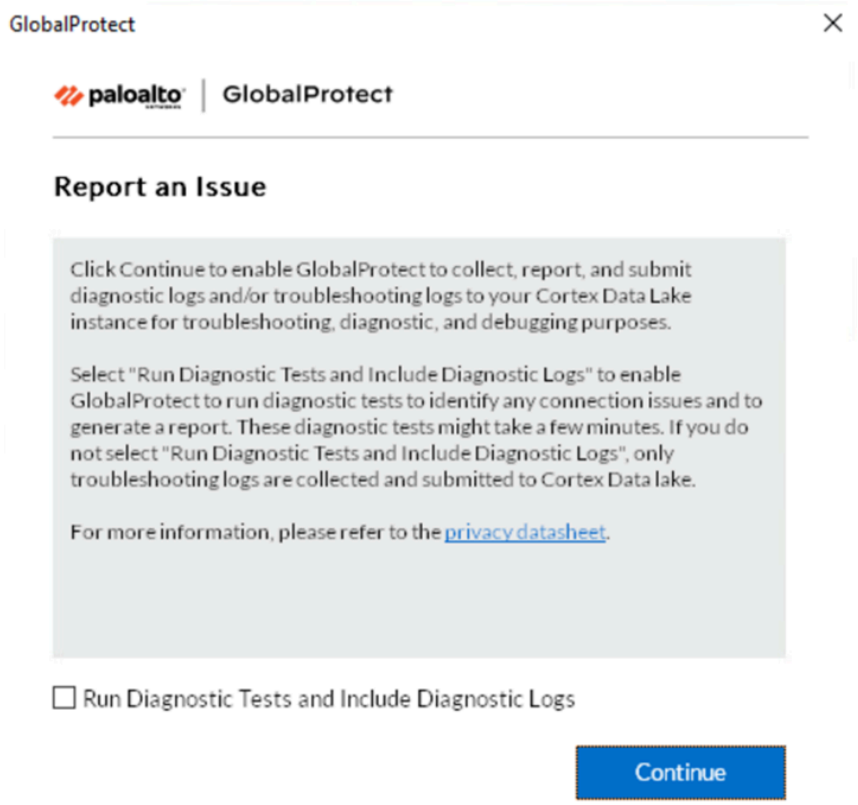
   Después de que las pruebas de diagnóstico se completen correctamente, los archivos de log de depuración de GlobalProtect se cargan en Strata Logging Service desde su endpoint.

   *Si no habilita la aplicación para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico, solo se recopilan logs de resolución de problemas y se envían a Strata Logging Service como un informe de resolución de problemas compacto. La aplicación de GlobalProtect comprueba los archivos de informe (pan_gp.trb.log o pan_gp_trbl.log) que se generan automáticamente en formato `.json`. Aparece un mensaje de notificación si no se encontraron problemas en los logs de resolución de problemas. Haga clic en **Retry (Reintentar)** para verificar si existen los archivos pan_gp.trb*.log.*

3. Seleccione la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**
4. Haga clic en **Continue (Continuar)** para permitir que la aplicación cree un registro de resolución de problemas y envíe el informe a la instancia de Strata Logging Service de su administrador.

   Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging

Service de su administrador junto con los archivos pan_gp.trb*.log. La aplicación de GlobalProtect puede ejecutar pruebas de diagnóstico con túnel o sin túnel. Por ejemplo, es posible que desee introducir sus credenciales de inicio de sesión de GlobalProtect antes de que la aplicación conecte y ejecute pruebas de diagnóstico a través del túnel.



Aparecerá un mensaje que confirma que la aplicación está ejecutando pruebas de diagnóstico solo si ha seleccionado la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**.

5. Haga clic en **Close (Cerrar)** para confirmar que la aplicación envió correctamente el informe a Strata Logging Service. Este mensaje de confirmación muestra la fecha y hora en que se procesó y envió el informe.

Desconectar la aplicación de GlobalProtect para Windows

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints Windows	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si su administrador configura el método de conexión GlobalProtect como **Always On (Siempre activado)**, puede desconectar la aplicación de GlobalProtect si tiene un buen motivo. Por ejemplo, es posible que desee desconectar la aplicación si la red privada virtual (VPN) de GlobalProtect no funciona en un hotel y el fallo de la VPN le impide conectarse a Internet. Después de desconectar la aplicación de GlobalProtect, puede conectarse a Internet mediante una comunicación no segura (sin VPN).

El método, el tiempo y el número de veces que puede desconectar la aplicación de GlobalProtect depende de cómo configure el administrador su servicio de GlobalProtect (PanGPS). Esta configuración puede evitar que desconecte la aplicación completamente o Permitirle desconectar la aplicación solo después de responder correctamente a una pregunta.

Si su configuración incluye una pregunta (desafío), la aplicación de GlobalProtect le solicita una de las siguientes opciones:

- Motivo por el que desea desconectar la aplicación
- Responder a una o más razones como **velocidad Internet lenta** o **aplicación no funciona** (si es necesario)
- Código de acceso
- Número de ticket de incidencia

Si el desafío requiere un código de acceso o un número de ticket, le recomendamos que se ponga en contacto con un administrador GlobalProtect o con una persona del servicio de asistencia por teléfono.

Los administradores suelen proporcionar contraseñas por adelantado, ya sea por correo electrónico (para los nuevos usuarios de GlobalProtect) o publicadas en el sitio web de su organización. En respuesta a un corte o problema del sistema, los administradores también pueden proporcionar códigos de acceso por teléfono.

Antes de obtener un número de ticket válido, su endpoint muestra un número de solicitud de ticket que debe comunicar a su administrador GlobalProtect o la persona del servicio de asistencia por teléfono. Si se aprueba su solicitud de desconexión, recibirá un número de ticket válido que puede usar para desconectar GlobalProtect.

Los siguientes pasos describen cómo desconectar la aplicación y superar una pregunta:

STEP 1 | Desconecte la aplicación de GlobalProtect.

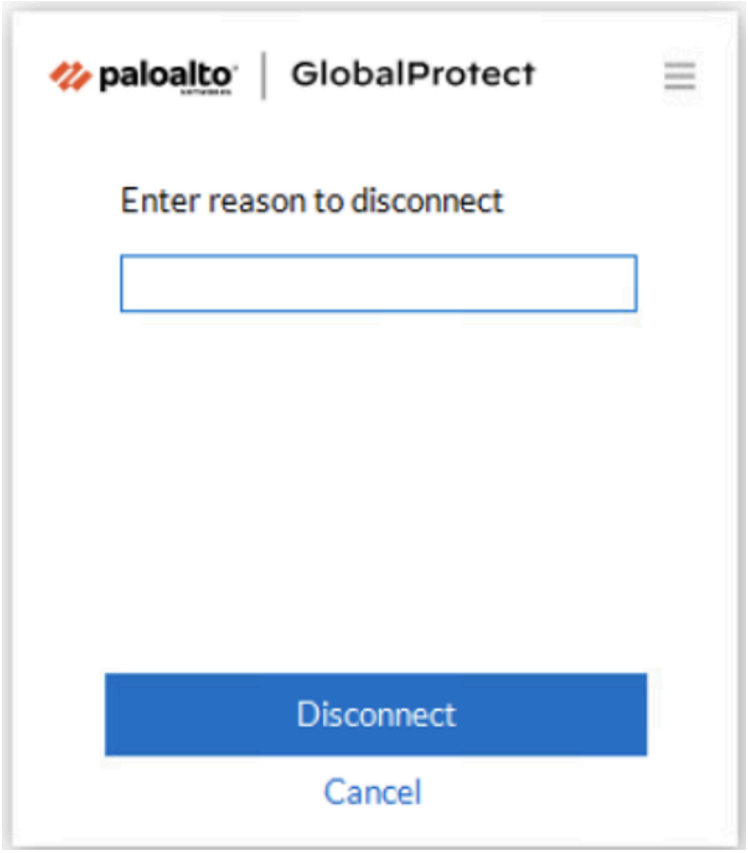
1. Inicie la aplicación de GlobalProtect haciendo clic en el icono de la bandeja del sistema de GlobalProtect. Se abre el panel de estado.
2. Haga clic en el menú de tres barras para abrir el menú de configuración.
3. Seleccione **Disconnect (Desconectar)**.

*La opción **Disconnect (Desconectar)** solo es visible si la configuración del agente de GlobalProtect le permite desconectar la aplicación. Si la configuración le permite desconectar la aplicación de GlobalProtect sin que tenga que responder a una pregunta (desafío), la aplicación de GlobalProtect se cierra sin que sea necesario realizar ninguna otra acción.*

STEP 2 | Responder a una o más preguntas, si es necesario.

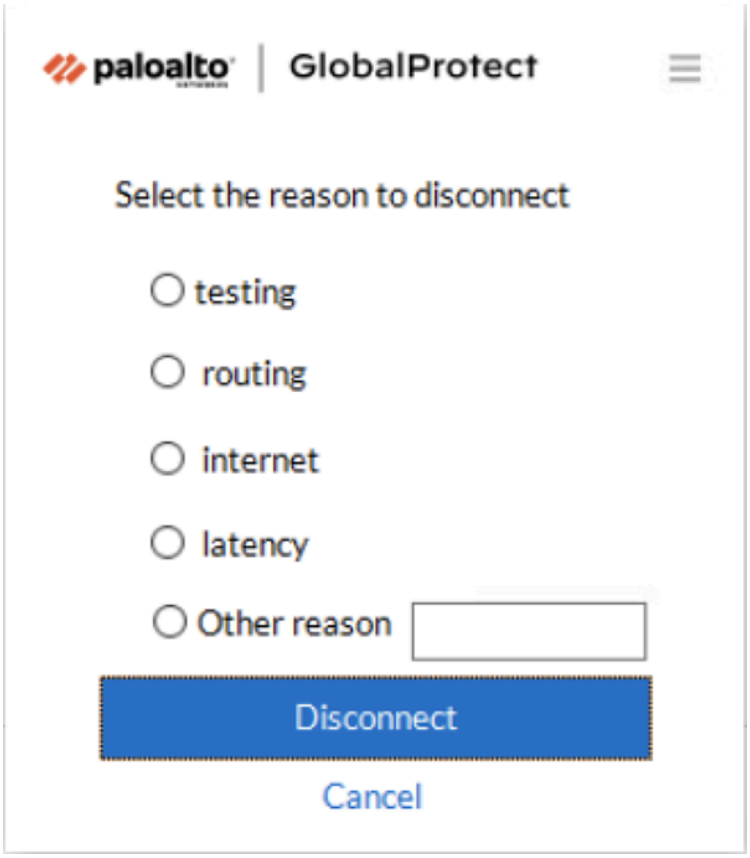
Si se le solicita, proporcione la siguiente información:

- **Tell us the issue to disconnect (Indique el motivo de la desconexión)**: su motivo para desconectar la aplicación de GlobalProtect.



- **Select the reason to disconnect (Seleccione el motivo de la desconexión)**: si su configuración requiere que responda a una o más razones o introduzca otra razón, la

aplicación de GlobalProtect muestra las razones tan pronto como seleccione **Disconnect (Desconectarse)**.



- **Passcode (Contraseña)**: código de acceso que suele proporcionar el administrador con antelación, en función de un problema o evento conocido que requiere que deshabilite la aplicación.
- **Ticket (Ticket de incidencia)**: si su configuración requiere que proporcione un número de ticket, la aplicación de GlobalProtect muestra un número de solicitud hexadecimal de ticket de ocho caracteres tan pronto como seleccione **Disconnect (Desconectar)**. Para desconectar la aplicación con un número de ticket, póngase en contacto con su administrador o con la persona del servicio de asistencia por teléfono y proporcione el número de solicitud. Después de aprobar su solicitud, su administrador o la persona del servicio de asistencia por teléfono le proporcionará un número de ticket hexadecimal de ocho caracteres. Introduzca el número de ticket en el campo **Ticket (Ticket de incidencia)** y, a continuación, haga clic en **OK (Aceptar)**.

Desinstalar la aplicación de GlobalProtect para Windows

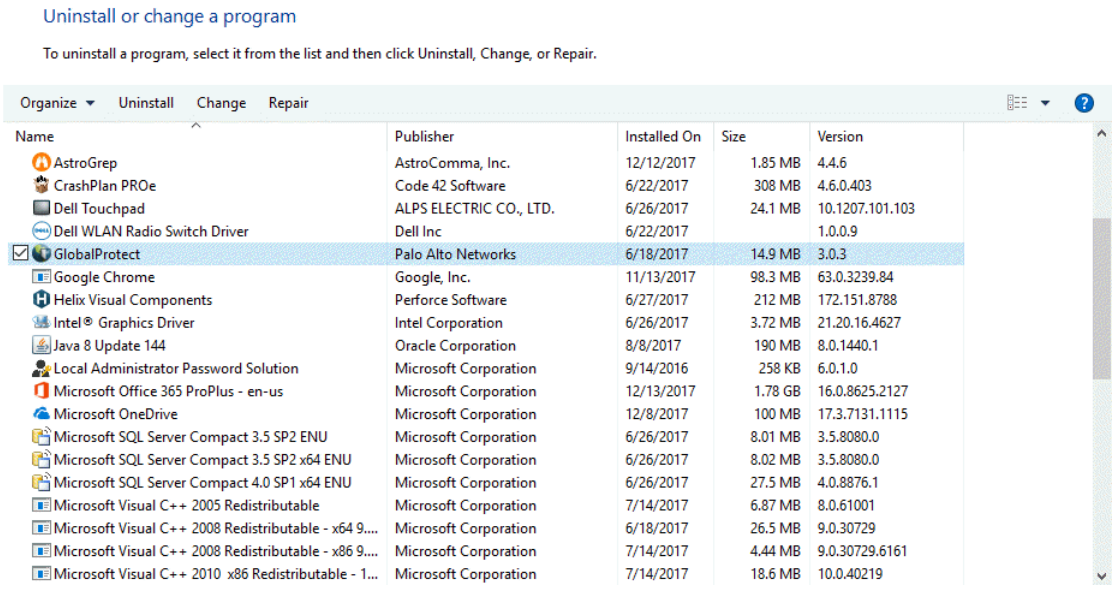
¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints Windows	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Siga los siguientes pasos para desinstalar la aplicación de GlobalProtect de su endpoint Windows . Tenga en cuenta que al desinstalar la aplicación, ya no tiene acceso VPN a su red corporativa y su endpoint no estará protegido por las políticas de seguridad de su empresa.

Solo los usuarios con privilegios de administrador pueden desinstalar la aplicación de GlobalProtect de los endpoints de Windows.

STEP 1 | Seleccione **Start (Iniciar)** > **Control Panel (Panel de control)** > **Programs (Programas)** > **Programs and Features (Programas y características)**.

STEP 2 | Seleccione **GlobalProtect** de la lista y, a continuación, haga clic en **Uninstall (Desinstalar)**.



STEP 3 | Cuando se le solicite continuar con la desinstalación, haga clic en **Yes (Sí)**.

Solucionar un conflicto de Microsoft Installer

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints Windows	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si procede a **Enforce GlobalProtect for Network Access (Aplicar GlobalProtect para el acceso a la red)** en una configuración de agente de portal de GlobalProtect y actualiza un endpoint Windows a una versión más reciente de la aplicación de GlobalProtect, la instalación puede fallar y la configuración de aplicación puede bloquear todo el tráfico.

Este problema se debe a una limitación del sistema operativo que se produce cuando varias instancias del instalador de Microsoft (`msiexec.exe`) se ejecutan simultáneamente en un endpoint Windows. Debe utilizar el procedimiento siguiente para resolver el conflicto del instalador de Microsoft:

STEP 1 | Reinicie el endpoint.

STEP 2 | Detenga todos los instaladores de terceros que se ejecutan en segundo plano.

1. Pulse **Ctrl+Alt+Delete (Ctrl+Alt+Supr)** y, a continuación, haga clic en **Task Manager (Administrador de tareas).**
2. En el **Task Manager (Administrador de tareas)**, localice todos los programas `msiexec` de terceros que se estén ejecutando actualmente (por ejemplo, **`msiexec línea de comandos - Google Search`**).
3. Seleccione el instalador externo y, a continuación, haga clic en **End Task (Finalizar tarea)** para detener el instalador.

STEP 3 | Restaure la versión existente de GlobalProtect y, a continuación, actualice a la versión más reciente de la aplicación.

1. (Opcional) Si es necesario, vuelva a instalar la versión existente (antigua) de GlobalProtect para repararla. Este paso es necesario si la actualización sigue fallando.
2. Permita que la actualización proceda según lo esperado.

Aplicación de GlobalProtect para macOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints macOS:	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

GlobalProtect™ es una aplicación que se ejecuta en su endpoint (ordenador de escritorio, portátil, tableta o teléfono inteligente) para protegerlo mediante el uso de las mismas políticas de seguridad que protegen los recursos sensibles de su red corporativa. GlobalProtect™ protege su tráfico de intranet, nube privada, nube pública e Internet, y le permite acceder a los recursos de su empresa desde cualquier parte del mundo.

Los siguientes temas describen cómo instalar y utilizar la aplicación de GlobalProtect para macOS:

- Descargar e instalar la aplicación GlobalProtect para macOS
- Usar la aplicación de GlobalProtect para macOS
- Informar de un problema desde la aplicación de GlobalProtect para macOS
- Deshabilitar la aplicación de GlobalProtect para macOS
- Desinstalar la aplicación de GlobalProtect para macOS
- Eliminar la extensión del kernel de GlobalProtect Enforcer
- Habilite la aplicación de GlobalProtect para macOS para usar certificados de cliente para la autenticación

Descargar e instalar la aplicación GlobalProtect para macOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints macOS:	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Antes de conectarse a la red GlobalProtect, debe descargar e instalar la aplicación de GlobalProtect en su endpoint macOS. Para asegurarle de que obtiene la aplicación correcta para la implementación de GlobalProtect o Prisma Access de su organización, debe descargar la aplicación directamente desde un portal de GlobalProtect dentro de su organización. Por esta razón, no hay un enlace de descarga directa de la aplicación de GP disponible en el sitio web de Palo Alto Networks.

Antes de descargar e instalar la aplicación de GlobalProtect, debe obtener la dirección IP o FQDN del portal de GlobalProtect de su administrador. Además, su administrador debe verificar qué nombre de usuario y contraseña puede usar para conectarse al portal y las puertas de enlace. Este es normalmente el mismo nombre de usuario y contraseña que utiliza para conectarse a su red corporativa.

Cuando instale la aplicación de GlobalProtect por primera vez en un dispositivo macOS con macOS Catalina 10.15.4, macOS Big Sur 11 o posterior, o actualice a la aplicación de GlobalProtect 5.1.4, debe habilitar las extensiones del sistema que se utilizan para funciones específicas de GlobalProtect. Si su administrador ha configurado túnel dividido en la puerta de enlace de GlobalProtect en función del nombre de dominio de destino y el nombre del proceso de aplicación o ha impuesto conexiones de GlobalProtect para el acceso a la red en el portal de GlobalProtect (consulte Personalización de GlobalProtect), el mensaje de notificación **Bloqueado de extensión del sistema** se mostrará en la aplicación de GlobalProtect durante la instalación. El mensaje solicita a los usuarios que habiliten y permitan que las extensiones del sistema en macOS que están bloqueadas se carguen para usar el túnel dividido y hacer cumplir las características de GlobalProtect para el acceso a la red.

Siga estas directrices cuando utilice extensiones del sistema:

- *Solo los usuarios con privilegios de administrador pueden habilitar las extensiones del sistema en la aplicación de GlobalProtect para endpoints macOS.*
- *Debido a la mejora de seguridad en macOS Catalina 10.15 y macOS Big Sur 11 para garantizar que sus datos estén protegidos mientras usa aplicaciones de terceros, GlobalProtect debe solicitar su permiso antes de intentar acceder a los archivos y carpetas almacenados en sus carpetas de Documentos, Escritorio y Descargas, además de unidades de red. Si su administrador ha habilitado las comprobaciones HIP, aparecerán nuevas ventanas emergentes de permisos en su endpoint con macOS cuando GlobalProtect solicite acceso a determinados archivos y carpetas almacenados en su sistema de archivos.*
- *La aplicación de GlobalProtect 5.1.4 que se ejecuta en macOS Catalina 10.15.4, macOS Big Sur 11 o posterior no utiliza extensiones del núcleo y utilizará extensiones del sistema.*
- *La aplicación de GlobalProtect 5.1.4 que se ejecuta en macOS Catalina 10.15.4, macOS Big Sur 11 o versiones posteriores no utilizará las extensiones del núcleo (**com.paloaltonetworks.kext.pangpd**) y, en su lugar, utilizará cualquiera de las* interfaces untu *disponibles proporcionadas por macOS como adaptador virtual.*
- *Si va a actualizar desde una versión anterior a la aplicación de GlobalProtect 5.1.4 que se ejecuta en macOS Catalina 10.15.4, macOS Big Sur 11 o posterior, ya no son necesarias las extensiones del núcleo. Tras la actualización, aparece el mensaje de notificación **Extensión del sistema bloqueada** en la aplicación GlobalProtect, solicitando a los usuarios que habiliten y permitan las extensiones del sistema en macOS que no se pudieron cargar por estar bloqueadas. De forma predeterminada, la aplicación no instalará extensiones del sistema y se aplican los mismos ajustes predeterminados.*

Después de recopilar la información requerida, siga los siguientes pasos para descargar e instalar la aplicación:

STEP 1 | Inicie sesión en el portal de GlobalProtect.

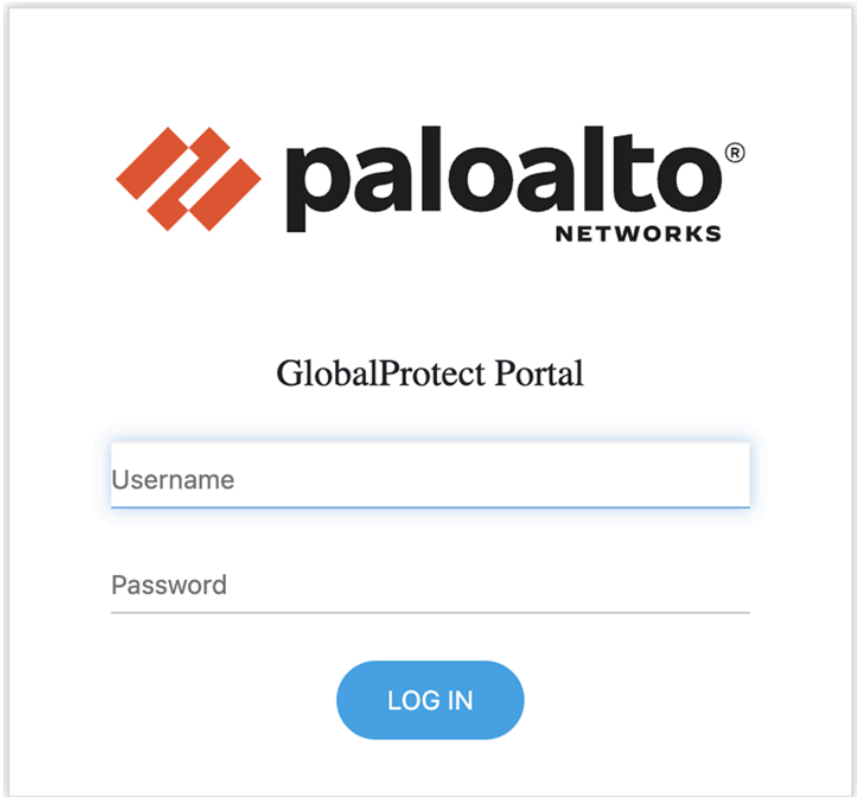
1. Inicie un navegador web y vaya a la siguiente URL:

   `https://<portal IP address or FQDN>`

   Ejemplo: **`HTTP://gp.acme.com`**

   Si está ejecutando GlobalProtect 6.3 o posterior y ha preimplementado la función de portal inteligente, GlobalProtect le redirige automáticamente al portal de Prisma Access apropiado según la ubicación de su país. Los portales definidos en el mapa del país del portal están disponibles en el menú desplegable. Para obtener más información, consulte Configurar el portal inteligente.

2. En la página de inicio de sesión del portal, introduzca su nombre de usuario en **Name (Nombre)** y la contraseña en **Password (Contraseña)** y, a continuación, haga clic en **LOG IN (Iniciar sesión)**. En la mayoría de los casos, puede usar el mismo nombre de usuario y contraseña que usa para conectarte a su red corporativa.



STEP 2 | Vaya a la página de descarga de la aplicación.

En la mayoría de las instancias, las páginas de descarga de la aplicación aparece inmediatamente después de que inicia sesión en el portal. Use esta página para descargar el paquete de software de la aplicación más reciente.

Si su administrador del sistema ha habilitado el acceso VPN sin cliente de GlobalProtect, se abre una página de aplicaciones (en lugar de la página de descarga de la aplicación) cuando

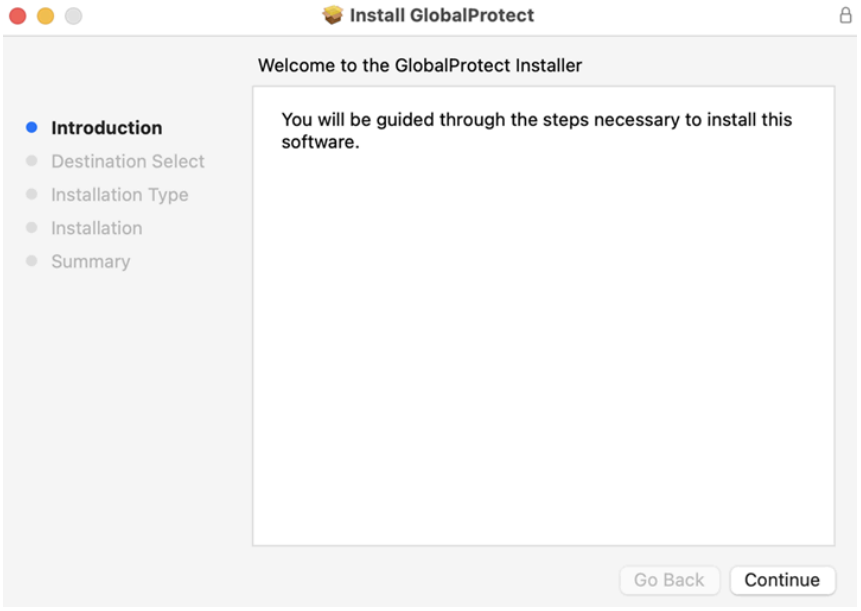
inicia sesión en el portal. Seleccione **GlobalProtect Agent (Agente de GlobalProtect)** para abrir la página de descarga.

STEP 3 | Descargue la aplicación.

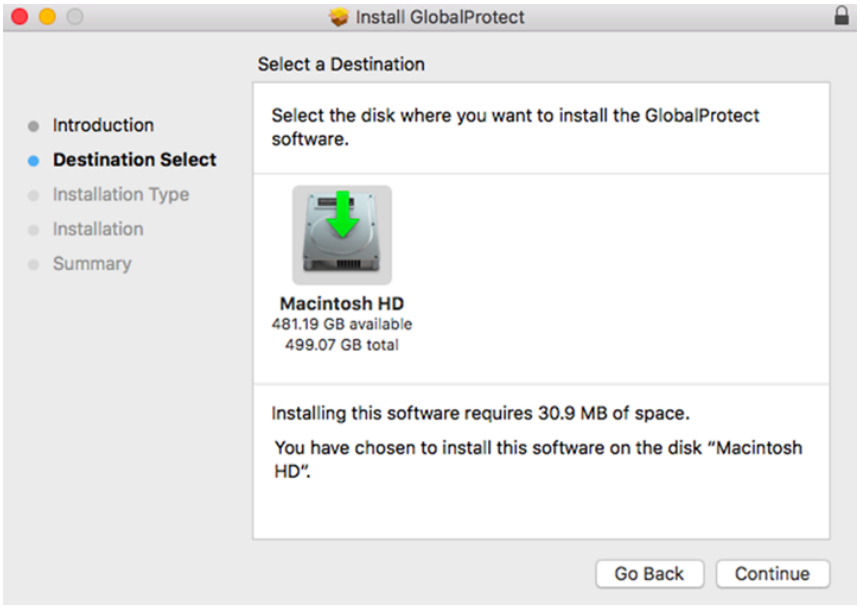
1. Haga clic en **Download Mac 32/64 bit GlobalProtect agent (Descargar agente de GlobalProtect MAC 32/64 bits)**.

2. Cuando se le solicite, proceda a **Run (Ejecutar)** el software.
3. Cuando se le solicite de nuevo, deberá**Run (Ejecutar)** el instalador de GlobalProtect.

STEP 4 | Complete la configuración de la aplicación de GlobalProtect con el Instalador de GlobalProtect.



1. Desde el Instalador de GlobalProtect, haga clic en **Continue (Continuar)**.
2. En la pantalla **Destination Select (Seleccionar destino)**, seleccione la carpeta de instalación de la aplicación de GlobalProtect y, a continuación, haga clic en **Continue (Continuar)**.

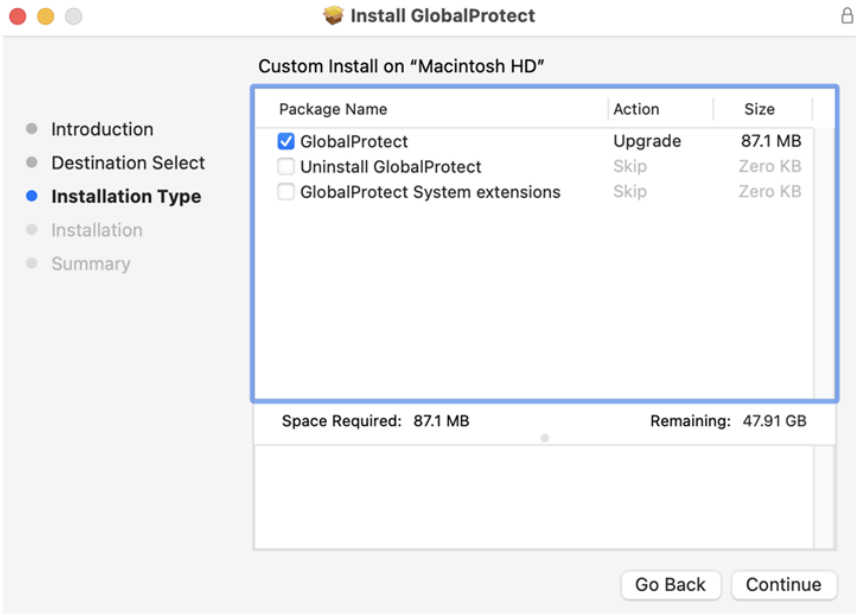


3. En la pantalla **Installation Type (Tipo de instalación)**, seleccione la casilla de verificación Paquete de instalación de **GlobalProtect**.

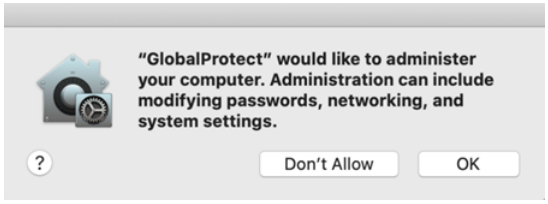
   Si el administrador del sistema ha configurado el túnel dividido en la puerta de enlace o ha impuesto conexiones GlobalProtect para el acceso a la red en el portal, active la

casilla de verificación **GlobalProtect System extensions (Extensiones del sistema de GlobalProtect)** (desactivada de forma predeterminada).

Haga clic en **Continue (Continuar)**.

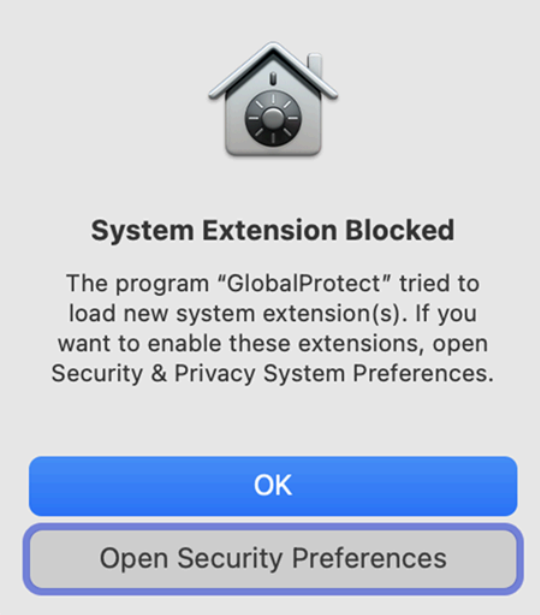


4. Haga clic en **Install (Instalar)** para confirmar que desea instalar GlobalProtect.
5. Cuando se le solicite, introduzca su **User Name (Nombre de usuario)** y **Password (Contraseña)**y, a continuación, haga clic en **Install Software (Instalar software)** para comenzar la instalación.
6. Después de que la instalación se haya completado, haga clic en **Close (Cerrar)** para cerrar el asistente de instalación.
7. Si su administrador ha configurado el portal para instalar el agente de endpoint Autonomous DEM (ADEM) durante la instalación de la aplicación de GlobalProtect por primera vez, seleccione **OK (Aceptar)** en el siguiente mensaje emergente para que no vuelva a aparecer:



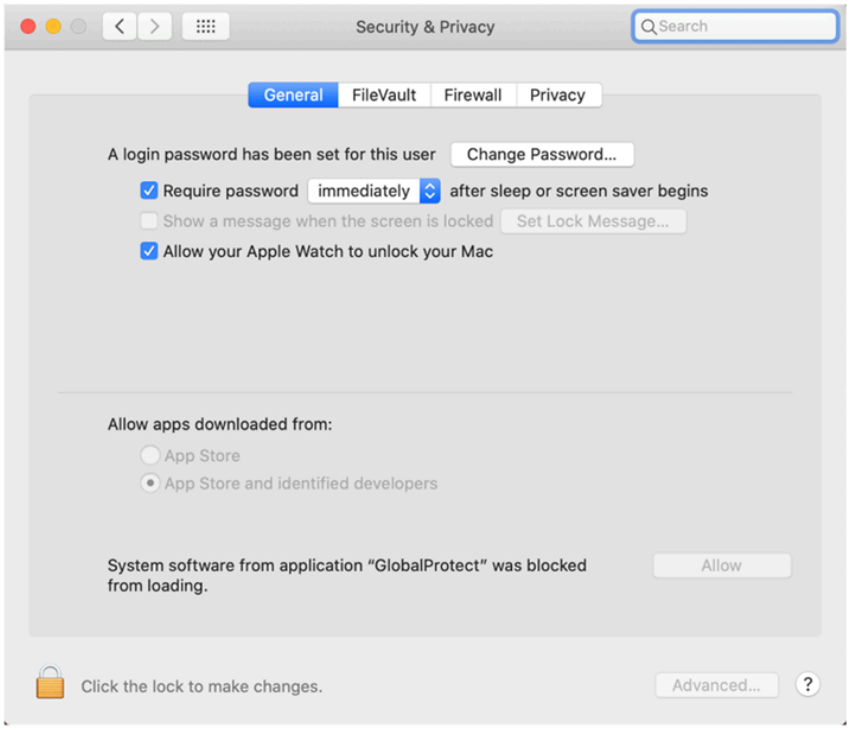
8. Si habilitó las **GlobalProtect System Extensions (Extensiones del sistema de GlobalProtect)**, seleccione **Open Security Preferences (Abrir preferencias de seguridad)** para habilitar las extensiones del sistema en macOS que se bloquearon para que no se

cargaran desde la siguiente notificación de **System Extension Blocked (Extensión del sistema bloqueado)**:



Si su administrador ha suprimido esta notificación mediante el sistema de gestión de dispositivos móviles (MDM) compatible, Jamf Pro, puede cargar automáticamente las extensiones del sistema sin recibir esta notificación.

9. En el cuadro de diálogo **Security & Privacy (Seguridad y privacidad)**, haga clic en el icono del **padlock (candado)** para realizar cambios y, a continuación, seleccione **App Store and identified developers (App Store y desarrolladores identificados)** en el área **Allow apps downloaded (Permitir descargas de aplicaciones)**. Haga clic en **Allow (Permitir)**.



Usar la aplicación de GlobalProtect para macOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints macOS:	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Este tema solo se aplica a usted si su configuración requiere que introduzca sus credenciales de inicio de sesión de GlobalProtect después de haber iniciado sesión en su endpoint (el inicio de sesión único está deshabilitado).

Por lo general, recomendamos que las organizaciones permitan que sus usuarios de GlobalProtect inicien sesión de manera transparente después de instalar la aplicación. Después de iniciar sesión en un endpoint con inicio de sesión GlobalProtect transparente, la aplicación de GlobalProtect inicia y se conecta automáticamente a la red corporativa sin intervención adicional del usuario.

Una vez completada la instalación, aparece el mensaje de notificación **Extensión del sistema bloqueado**, que solicita a los usuarios que habiliten las extensiones del sistema en macOS que se bloquearon para que no se carguen. Si no se selecciona la opción **GlobalProtect System Extensions (Extensiones del sistema de GlobalProtect)** durante la instalación, este mensaje de notificación aparece una vez que los usuarios se conectan a la puerta de enlace. Esta notificación aparece si su administrador ha configurado túnel dividido en la puerta de enlace GlobalProtect, ha aplicado conexiones de GlobalProtect para el acceso a la red en el portal GlobalProtect (consulte Personalización de la aplicación de GlobalProtect) o ambas. Ambas funciones requieren que los usuarios habiliten las extensiones del sistema.

Si su configuración requiere que introduzca sus credenciales de GlobalProtect, siga los pasos aplicables a continuación.

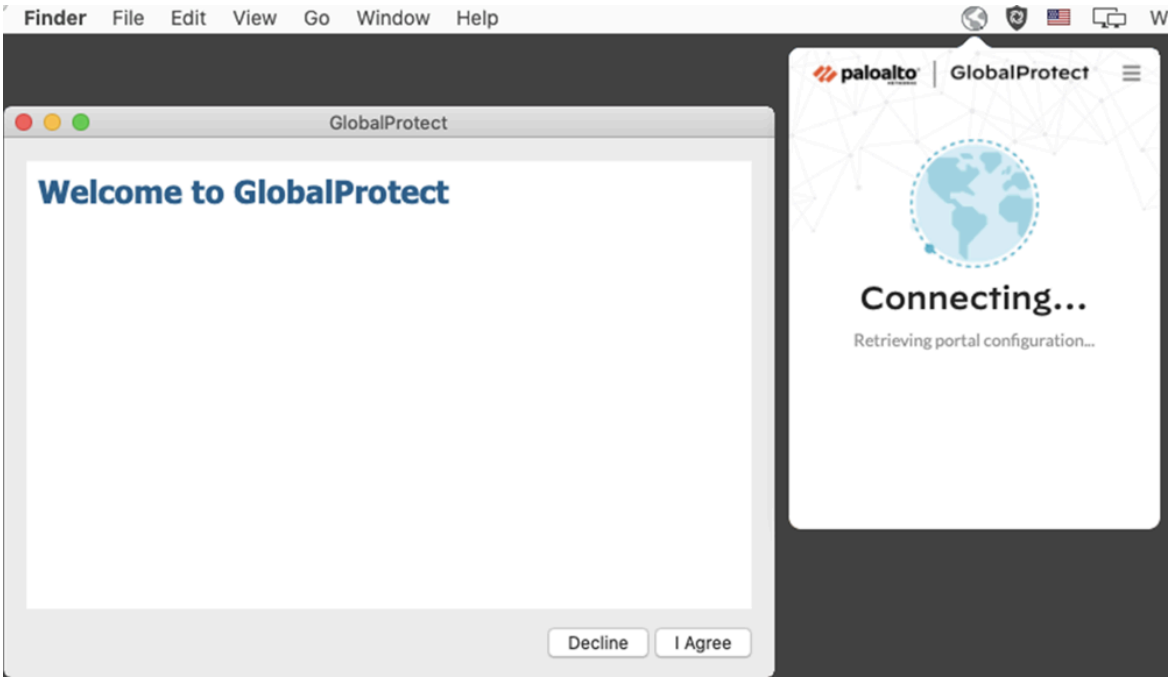
STEP 1 | Inicie sesión en GlobalProtect.

Si esta iniciando sesión en el endpoint por primera vez, la aplicación de GlobalProtect muestra una página de bienvenida tras el inicio de sesión correcto. Haga clic en **Get Started (Comenzar)**.

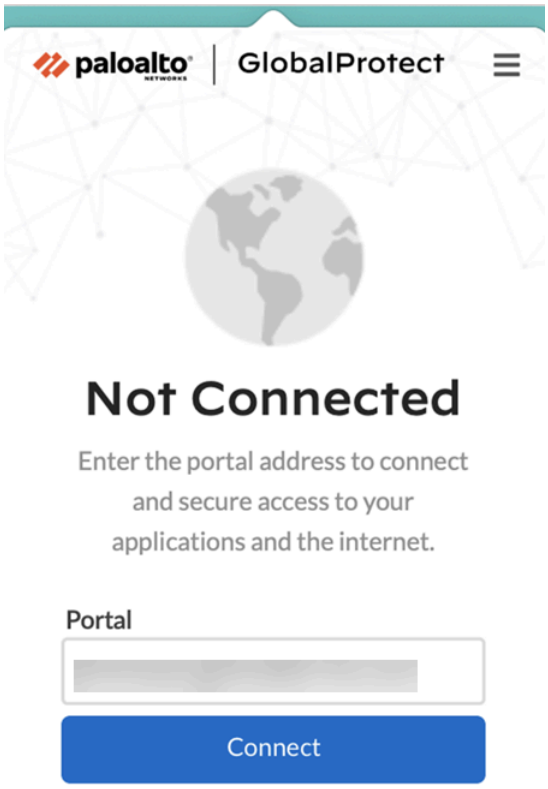
1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. (Opcional) Revise las condiciones de servicio de su empresa antes de conectarse a GlobalProtect si su administrador requiere que vea una página para acceder a recursos internos.

   Si no acepta las condiciones de uso, no podrá conectarse a GlobalProtect.

   Opcionalmente, si hace clic en **Cancel (Cancelar)**, debe introducir la dirección IP (o dominio) del portal de GlobalProtect y, a continuación, hacer clic en **Connect (Conectar)** para iniciar la conexión.



3. Introduzca la dirección IP o el dominio del portal que proporcionó su administrador de GlobalProtect y, a continuación, haga clic en **Connect (Conectar)**.



STEP 2 | Conéctese a la puerta de enlace o portal de GlobalProtect.

Puede determinar si está conectado consultando el icono de la bandeja del sistema de GlobalProtect. Si no está conectado, el icono está atenuado () y ***Not Connected (No conectado)*** *aparece cuando pasa el cursor sobre el icono.*

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. (Opcional) Si inicia sesión en la aplicación de GlobalProtect por primera vez, introduzca el FQDN o la dirección IP del portal de GlobalProtect y luego haga clic en **Connect (Conectar)**.
3. (Opcional) Si se guardan varios portales en su aplicación, selecciona un portal en el menú desplegable **Change Portal (Cambiar portal)**. De forma predeterminada, el portal conectado más recientemente está preseleccionado en el menú desplegable **Change Portal (Cambiar portal)**.
4. (Opcional) De manera predeterminada, usted se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, haga clic en el menú desplegable **Change Gateway (Cambiar puerta de enlace)** y, a continuación, utilice una de las siguientes opciones:
   - Seleccione una puerta de enlace manualmente (solo puertas de enlace externas). Esta opción solo está disponible si su administrador habilita la selección manual de la puerta de enlace.

- Asigne y conéctese automáticamente a una puerta de enlace preferida:

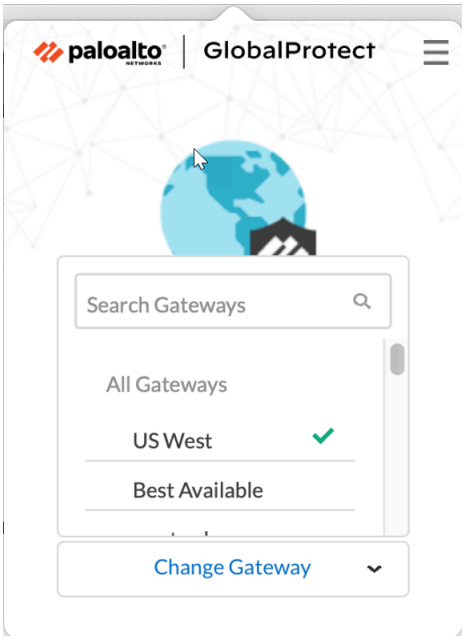
  1. Para designar una puerta de enlace como preferida, haga clic en el icono de estrella ( ). La próxima vez que se conecte, se conectará automáticamente a esta puerta de enlace preferida.

     Si luego decide que ya no desea la puerta de enlace como su puerta de enlace preferida, sencillamente borre el icono de estrella para eliminar esta puerta de enlace como conexión preferida.

  2. De forma predeterminada, se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)** que se identifica mediante una marca de verificación en el menú desplegable **Change Gateway (Cambiar puerta de enlace)**. Si establece

la puerta de enlace preferida, una estrella aparecerá junto a la puerta de enlace destacada en el menú desplegable **Change Gateway (Cambiar puerta de enlace)**.

Si su administrador configuró puertas de enlace externas manuales en la configuración del agente del portal, puede elegir una puerta de enlace específica utilizando el campo de búsqueda de puerta de enlace.



5. (Opcional) Dependiendo del modo de conexión, haga clic en **Connect (Conectarse)** para iniciar la conexión.
6. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** y haga clic en **Sign In (Iniciar sesión)**.

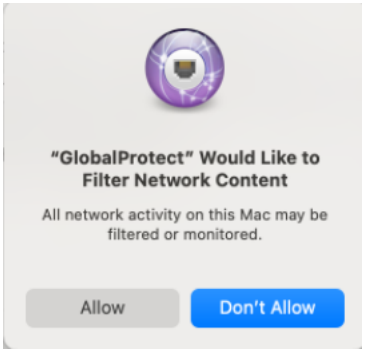
   Si su administrador le ha permitido usar información biométrica (huella digital) para iniciar sesión, primero debe iniciar sesión con un nombre de usuario y contraseña dos veces (una para guardarla y otra para autenticarse); luego puede usar información biométrica para iniciar sesión.

   Si el administrador del sistema ha habilitado las **GlobalProtect System Extensions (Extensiones del sistema de GlobalProtect)**, debe habilitar las extensiones del sistema en

macOS que se bloquearon para que no se carguen y usar las funciones de túnel dividido y Aplicar GlobalProtect para el acceso de red.

Los usuarios no necesitan privilegios de administrador para permitir las dos solicitudes emergentes ***Network Extensions Configuration (Configuración de extensiones de red)****. Su administrador puede suprimir estas solicitudes de mensajes utilizando el sistema de gestión de dispositivos móviles (MDM), como Jamf Pro, para cargar automáticamente las extensiones de red sin recibir estas solicitudes. Consulte el artículo de la base de conocimientos en https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8 para obtener información sobre cómo habilitar las extensiones de red y del sistema con Jamf Pro.*

1. (macOS Catalina 10.15.4 o posterior y macOS Big Sur 11 o posterior únicamente) Si el administrador del sistema configuró el túnel dividido basado en dominios y aplicaciones en la puerta de enlace de GlobalProtect o habilitó la función Aplicar conexiones de GlobalProtect para el acceso de red, seleccione **Allow (Permitir)** en la siguiente ventana emergente:



   Si selecciona **Don't Allow (No permitir)**, la función de túnel dividido no se puede utilizar en la aplicación de GlobalProtect, la función Aplicar conexiones de GlobalProtect para el acceso de red no funcionará y las conexiones de GlobalProtect para el acceso de red no se podrán aplicar. Este mensaje emergente aparecerá la próxima vez que se conecte al portal o puerta de enlace, o hasta que seleccione **Allow (Permitir)**.

Cuando la aplicación se conecta en modo externo, el icono de la bandeja del sistema de GlobalProtect muestra un escudo ( ) y **Connected (Conectado)** aparece cuando pasa el cursor sobre el icono. Cuando la aplicación se conecta en modo interno, el icono de la bandeja del sistema de GlobalProtect muestra una casa ( ) y la**Internal Network (Red interna)** aparece cuando pasa el cursor sobre el icono.

STEP 3 | Abra la aplicación GlobalProtect.

Haga clic en el icono de la bandeja del sistema de GlobalProtect para iniciar la interfaz de la aplicación.

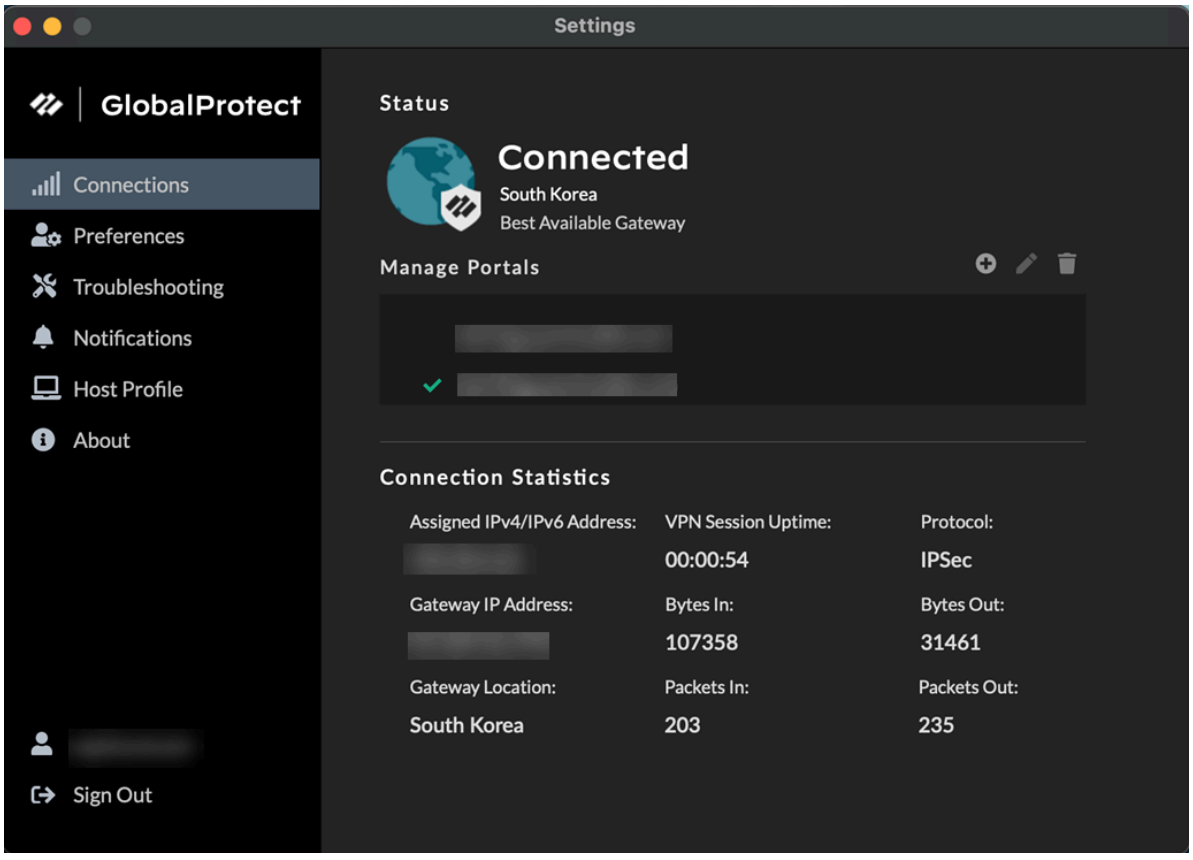
Aparece una notificación si su administrador configuró el portal para instalar el agente de endpoint Autonomous DEM (ADEM) durante la instalación de la aplicación de GlobalProtect y le permitió habilitar las pruebas o no le permitió habilitar las pruebas. Si su administrador ya ha

instalado el agente de endpoint ADEM y más tarde ha configurado el portal para desinstalar el agente de endpoint ADEM, aparecerá una notificación en el próximo inicio de sesión.

STEP 4 | Vea información sobre sus servicios de red.

Después de iniciar la aplicación, haga clic en el menú de tres barras en el panel de estado para abrir el menú de configuración. Seleccione **Settings (Configuración)** para abrir el panel **GlobalProtect Settings (Configuración de GlobalProtect)** y, a continuación, seleccione una de las siguientes configuraciones para ver y modificar la aplicación de GlobalProtect:

- **Connections (Conexiones)**: la pestaña **Connections (Conexiones)** muestra los portales asociados con la cuenta de GlobalProtect. Puede añadir, editar o eliminar portales desde esta pestaña. Esta pestaña también muestra la puerta de enlace a la que está conectado. Puede ver las estadísticas de conexión de la puerta de enlace (por ejemplo, la dirección IP de la puerta de enlace, la ubicación y el tiempo de actividad de la sesión VPN) cuando su administrador establece **Enable Advanced View (Habilitar vista avanzada)** en **Yes (Sí)** en la configuración del agente del portal de GlobalProtect. Seleccione la pestaña **Connections (Conexiones)** para ver el temporizador de la cuenta regresiva para la duración del inicio de sesión.



La pestaña **Connections (Conexiones)** muestra los detalles del proxy si la funcionalidad Conectividad mediante proxy explícito en GlobalProtect for Always-On Internet Security (Conectividad de proxy explícito en GlobalProtect para seguridad de Internet siempre activa) está habilitada para la aplicación a través de Prisma Access.

Modo proxy:

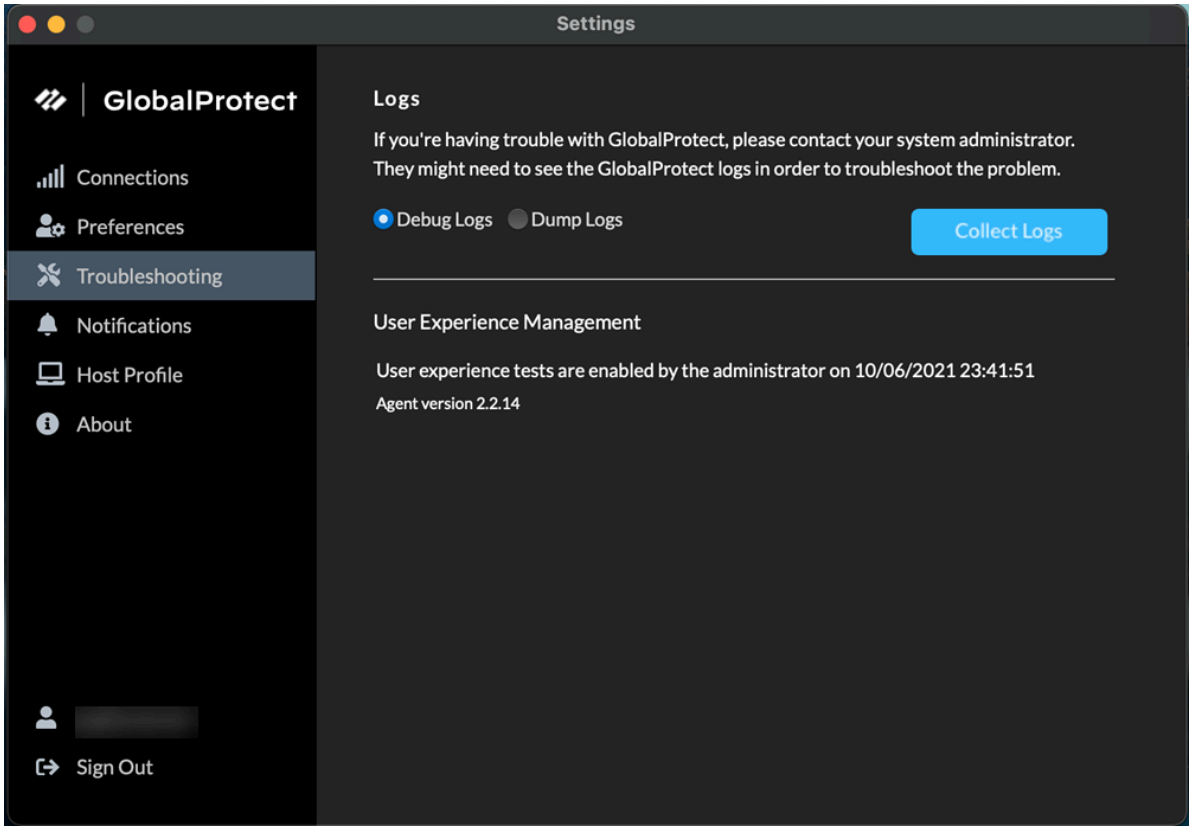
- **Preferences (Preferencias)**: la pestaña **Preferences (Preferencias)** ahora está disponible solo si su administrador configura al menos una de las siguientes opciones:
  - **Enable Biometric Sign-in (Habilitar inicio de sesión biométrico)**: puede optar por utilizar información biométrica (huella digital) para iniciar sesión. Esta opción está disponible solo si su administrador configura **Save User Credentials (Guardar credenciales de usuario)** en **Only with User Fingerprint (Solo con huellas digitales de usuario)** en la configuración del agente de GlobalProtect. Debe proporcionar una huella que coincida con una plantilla de huella fiable en el endpoint para usar una contraseña guardada para la autenticación en el portal y las puertas de enlace de GlobalProtect.
  - **Do not display a welcome page upon each successful connection (No mostrar una página de bienvenida en cada conexión correcta)**: puede elegir mostrar una página de bienvenida tras el inicio de sesión correcto. Esta opción solo está disponible si su administrador establece la **Welcome Page (Página de bienvenida)** en **factory-default** en la configuración del agente del portal de GlobalProtect.
  - **Connect with SSL (Conectar con SSL)**: puede elegir usar SSL o quedarse con IPSec. Esta opción solo está disponible si su administrador establece **Connect with SSL Only (Conectar solo con SSL)** en **User can Change (El usuario puede cambiar)** en la configuración del agente del portal de GlobalProtect.
  - **Always run diagnostic tests and include logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**: puede optar por habilitar la aplicación de GlobalProtect para que ejecute pruebas de diagnóstico e incluya logs de diagnóstico. Esta opción solo está disponible si su administrador habilita la recopilación de logs de la aplicación de GlobalProtect para la resolución de problemas en el portal de GlobalProtect.

- **Troubleshooting (Resolución de problemas)**: la pestaña **Troubleshooting (Resolución de problemas)** le permite **Collect Logs (Recopilar logs)** y establecer el nivel de creación de logs

en **Debug Logs (Depurar logs)** o **Dump Logs (Volcar logs)** y opcionalmente **Enable User Experience Tests (Habilitar pruebas de experiencia de usuario)**.

A fin de que la aplicación de GlobalProtect envíe logs de solución de problemas, logs de diagnóstico o ambos a Strata Logging Service para un mayor análisis, debe configurar el portal de GlobalProtect para habilitar la recopilación de logs de la aplicación de GlobalProtect para la solución de problemas. Además, puede configurar las URL de destino basadas en HTTPS que pueden contener direcciones IP o nombres de dominio completos de los servidores/recursos web que desea sondear y determinar ciertos problemas, como la latencia o el rendimiento de la red, en el endpoint del usuario final.

Puede hacer clic en **Advanced (Avanzado)** para ver información detallada sobre su endpoint.



La ventana **Advanced Logging Settings (Configuración de creación de logs avanzada)**: muestra información sobre la configuración de red, la configuración de ruta, las conexiones activas y los logs.

Cuando GlobalProtect esté conectado, verifique que el agente de endpoint ADEM pueda realizar pruebas de experiencia del usuario si la casilla de verificación **Enable user experience tests (Habilitar pruebas de experiencia de usuario)** se muestra en la aplicación de GlobalProtect. O puede verificar que se muestre un mensaje si su administrador instaló el agente de endpoint ADEM durante la instalación de la aplicación GlobalProtect, pero no le permite habilitar o deshabilitar las pruebas de experiencia del usuario desde la aplicación

GlobalProtect. De forma predeterminada, las alertas heartbeat aún se reenvían a ADEM incluso cuando GlobalProtect está deshabilitado o desconectado.

Si su administrador configuró el portal para instalar el agente de endpoint de Autonomous DEM durante la instalación de la aplicación de GlobalProtect y le permitió habilitar las pruebas, seleccione la casilla de verificación **Enable user experience tests (Habilitar pruebas de experiencia de usuario)** en la aplicación de GlobalProtect. Esta casilla de verificación no aparece si su administrador no le permite habilitar o deshabilitar las pruebas de experiencia del usuario desde la aplicación GlobalProtect. En su lugar, se muestra un mensaje que confirma que la aplicación está habilitada para ejecutar pruebas de experiencia de usuario.

Si no selecciona la casilla de verificación **Enable user experience tests (Habilitar pruebas de experiencia de usuario)**, las alertas de heartbeat continúan reenviándose a ADEM.

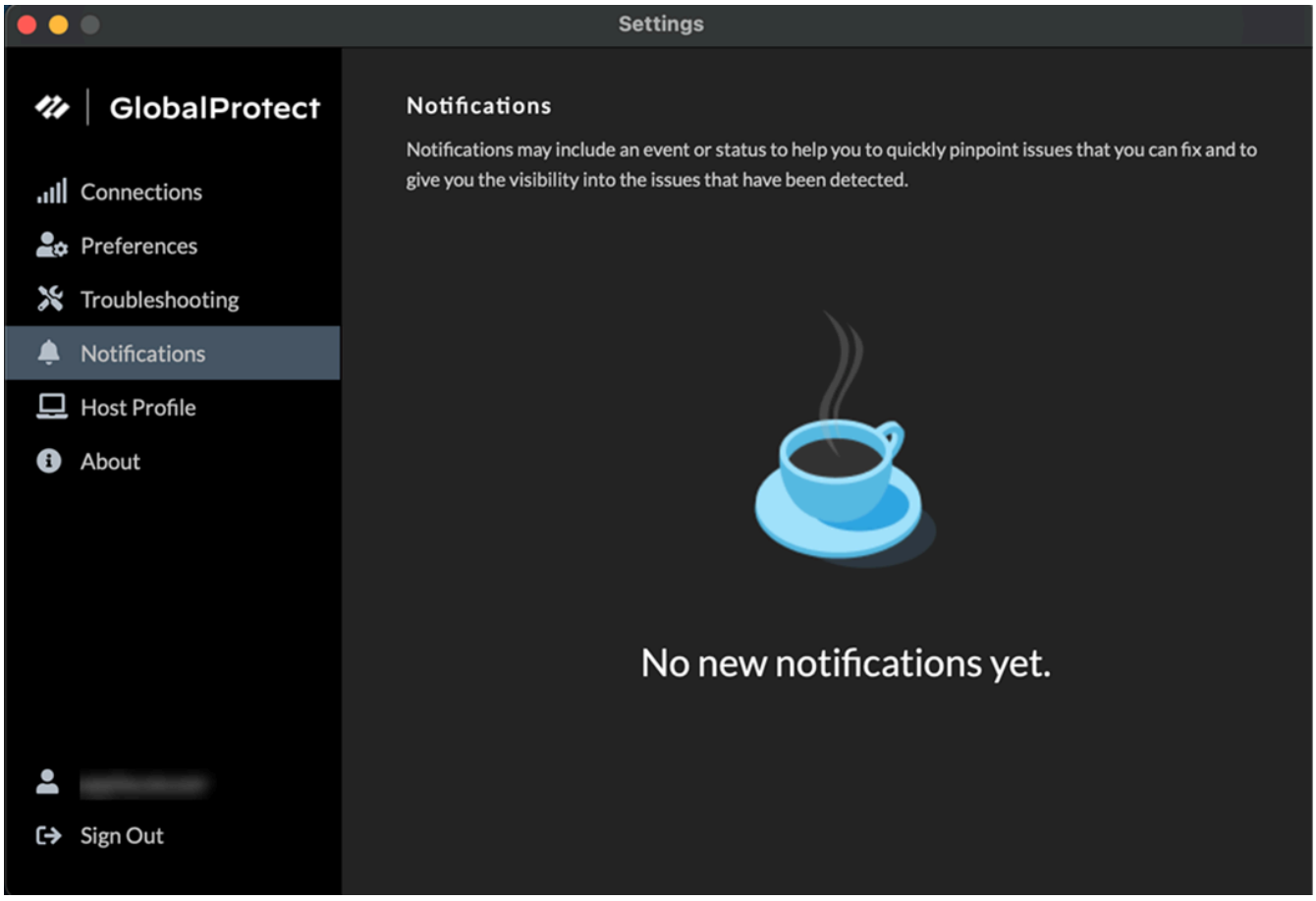
- **Notifications (Notificaciones)**: la pestaña **Notifications (Notificaciones)** muestra la información detallada sobre notificaciones específicas activadas en la aplicación de GlobalProtect. Puede configurar notificaciones de usuario final sobre el vencimiento de las sesiones de la aplicación de GlobalProtect en la puerta de enlace y programar la visualización de estas notificaciones personalizadas en la aplicación.

A partir de la versión 6.2.3 de la aplicación GlobalProtect, los mensajes de tiempo de espera de inactividad y sesión se suprimen para el método de conexión siempre activa.

A partir de la versión 6.2 de la aplicación de GlobalProtect, puede ampliar la duración de la sesión de inicio de sesión de la aplicación de GlobalProtect antes de que caduque para evitar el cierre abrupto de la sesión de la aplicación. La notificación de vencimiento de la duración del inicio de sesión le informa por adelantado cuando las sesiones de la aplicación están a punto de caducar y ofrece la opción de ampliar la duración de la sesión de usuario para que no se cierre la sesión abruptamente. La aplicación mostrará la notificación

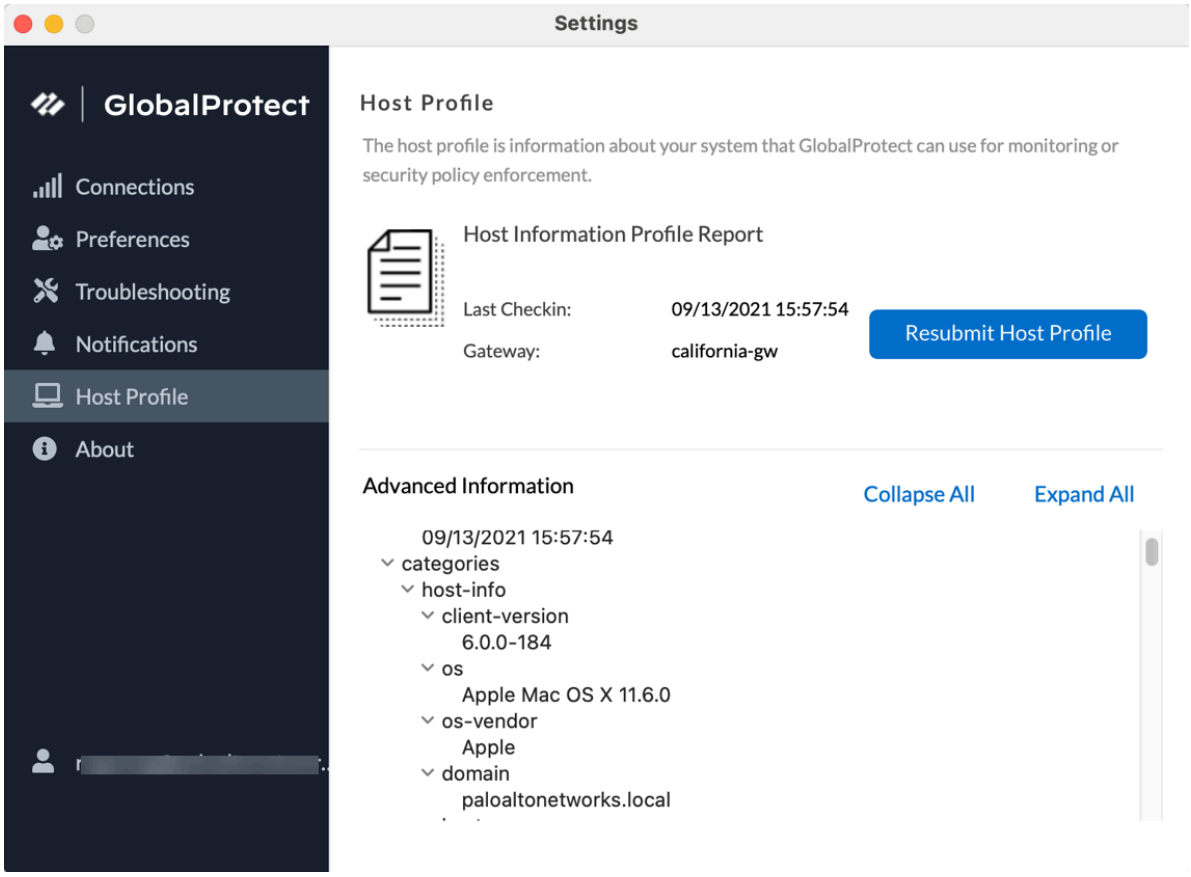
de vencimiento con la opción de ampliar la sesión de usuario si su administrador ha configurado los ajustes de notificación para ampliar la sesión.

También se le notificará si no hay nuevas notificaciones activadas en la aplicación GlobalProtect.



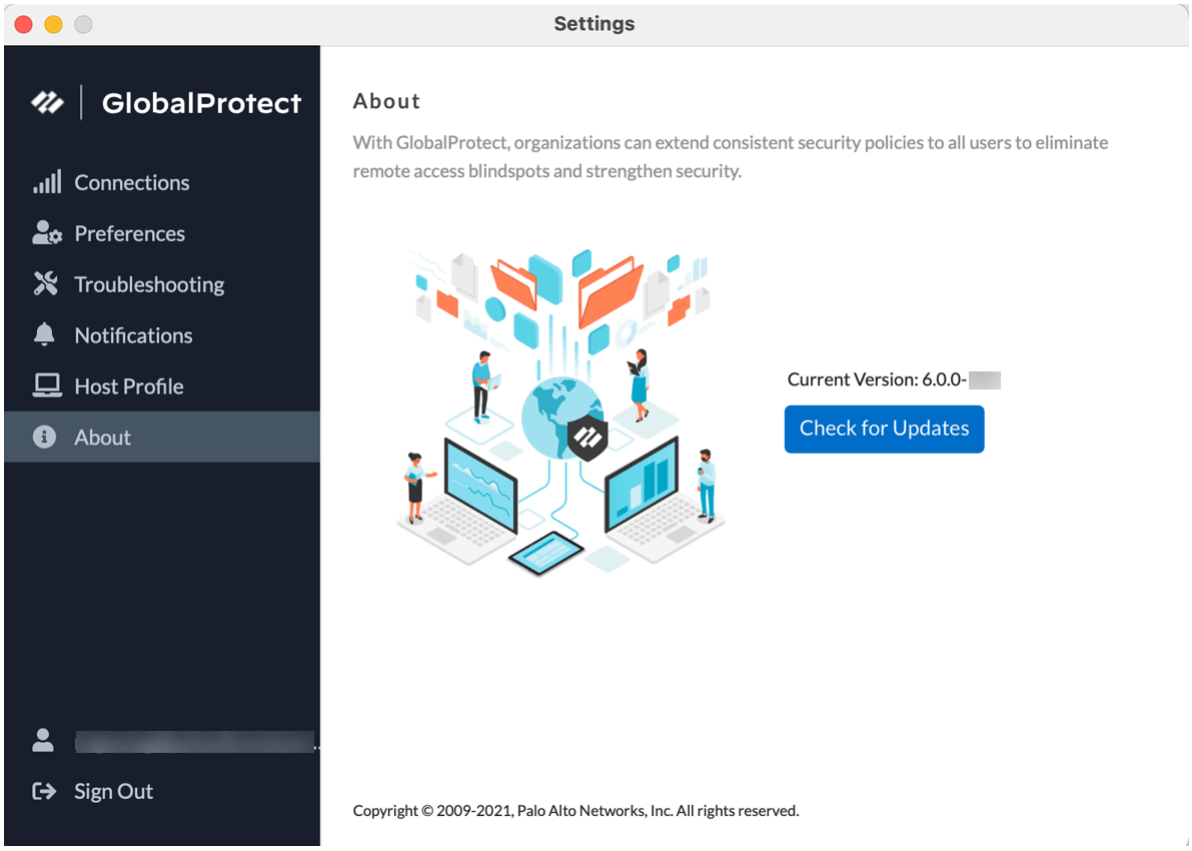
- **Host Profile (Perfil de host)**: la pestaña **Host Profile (Perfil de host)** muestra los datos de endpoint que utiliza GlobalProtect para supervisar y aplicar políticas a través del Host

Information Profile (Perfil de información de host). Puede **Resubmit Host Profile (Reenviar perfil de host)** para reenviar manualmente los datos de HIP a la puerta de enlace.



Si su administrador configuró varias puertas de enlace internas en modo sin túnel y detección de host interno, puede hacer clic en **More Details (Más detalles)** para supervisar el envío de informes del perfil de información de host (Host Information Profile, HIP) para cada puerta de enlace desde una ubicación central para ayudarle a solucionar rápidamente problemas relacionados con HIP.

- **About (Acerca de)**: la pestaña **About (Acerca de)** muestra la versión de GlobalProtect instalada actualmente en el endpoint y permite a los usuarios finales **Check for Updates (Buscar actualizaciones)**.



STEP 5 | (Opcional) Inicie sesión con una contraseña nueva.

*Si el administrador de GlobalProtect configura el agente del portal de GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, las credenciales se guardarán automáticamente en la aplicación de GlobalProtect. Si su contraseña de acceso a la red corporativa cambia, debe iniciar sesión en GlobalProtect con su nueva contraseña.*

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. Haga clic en el menú de tres barras para abrir el menú de configuración.
3. Seleccione **Settings (Ajustes)** para abrir el panel **GlobalProtect Settings (Ajustes de GlobalProtect)**.
4. En el panel **GlobalProtect Settings (Configuración de GlobalProtect)**, proceda a **Sign Out (Cerrar sesión)** para borrar las credenciales de usuario guardadas de la aplicación de GlobalProtect.
5. Después de borrar sus credenciales de usuario, puede volver a conectarse a GlobalProtect con su nuevo nombre de usuario y contraseña.

STEP 6 | (Opcional) Desconéctese de GlobalProtect.

Si su administrador configura GlobalProtect con el método de conexión **On-Demand (Bajo demanda)**, puede desconectarse de GlobalProtect haciendo clic en **Disconnect (Desconectar)** en el panel de estado.

Informar de un problema desde la aplicación de GlobalProtect para macOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints macOS:	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si experimenta un comportamiento inusual, como un rendimiento de red deficiente o si no se establece la conexión con el portal y la puerta de enlace, puede informar de la incidencia directamente a Strata Logging Service para que su administrador pueda acceder a ella Ya no es necesario recopilar y enviar manualmente los logs de aplicaciones de GlobalProtect por correo electrónico o almacenarlos en una unidad de nube.

*Para mostrar la opción **Report an Issue (Informar de un problema)** en la aplicación de GlobalProtect, su administrador debe habilitar la recopilación de logs de la aplicación de GlobalProtect para la resolución de problemas en el portal de GlobalProtect.*

STEP 1 | Conéctese a la puerta de enlace o portal de GlobalProtect.

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. (Opcional) Si inicia sesión en la aplicación de GlobalProtect por primera vez, introduzca el FQDN o la dirección IP del portal de GlobalProtect y luego haga clic en **Connect (Conectar)**.
3. (Opcional) Si se guardan varios portales en su aplicación, seleccione un portal en el menú desplegable **Portal**. De manera predeterminada, el portal conectado más recientemente está preseleccionado del menú desplegable **Portal**.
4. (Opcional) De manera predeterminada, usted se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, haga clic en el menú desplegable del gateway.

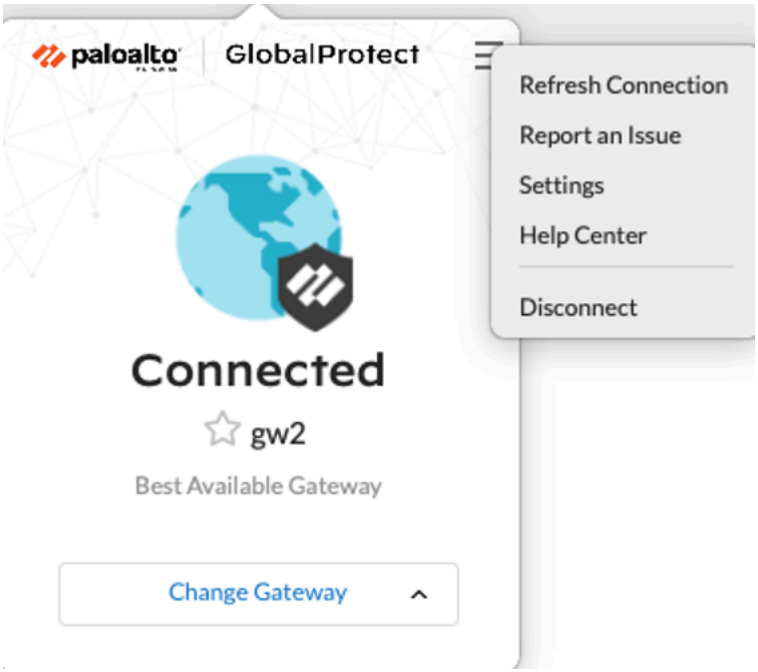
STEP 2 | Abra la aplicación GlobalProtect.

Haga clic en el icono de la bandeja del sistema de GlobalProtect para iniciar la interfaz de la aplicación.

STEP 3 | Informe de un problema desde la aplicación de GlobalProtect desde su endpoint.

Después de iniciar la aplicación, haga clic en el menú de tres barras del panel de estado para informar de un problema a su administrador.

1. Seleccione **Report an Issue (Informar de un problema)**.



2. Habilite la aplicación de GlobalProtect para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico. Los logs de diagnóstico y resolución de problemas se recopilan y envían a Strata Logging Service como un informe de resolución de problemas compacto.

   Después de que las pruebas de diagnóstico se completen correctamente, los archivos de log de depuración de GlobalProtect se cargan en Strata Logging Service desde su endpoint.

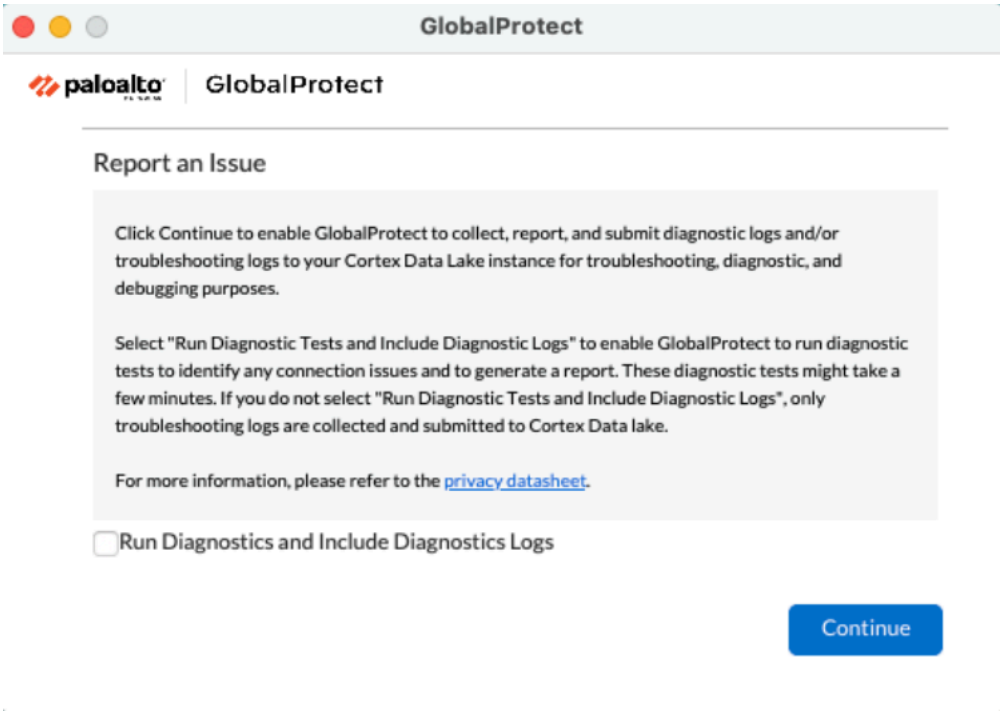
   *Si no habilita la aplicación para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico, solo se recopilan logs de resolución de problemas y se envían a Strata Logging Service como un informe de resolución de problemas compacto. La aplicación de GlobalProtect comprueba los archivos de informe (pan_gp.trb.log o pan_gp_trbl.log) que se generan automáticamente en formato `.json`. Aparece un mensaje de notificación si no se encontraron problemas en los logs de resolución de problemas. Haga clic en **Retry (Reintentar)** para verificar si existen los archivos pan_gp.trb*.log.*

3. Seleccione la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**
4. Haga clic en **Continue (Continuar)** para permitir que la aplicación cree un registro de resolución de problemas y envíe el informe a la instancia de Strata Logging Service de su administrador.

   Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging Service de su administrador junto con los archivos pan_gp.trb*.log.

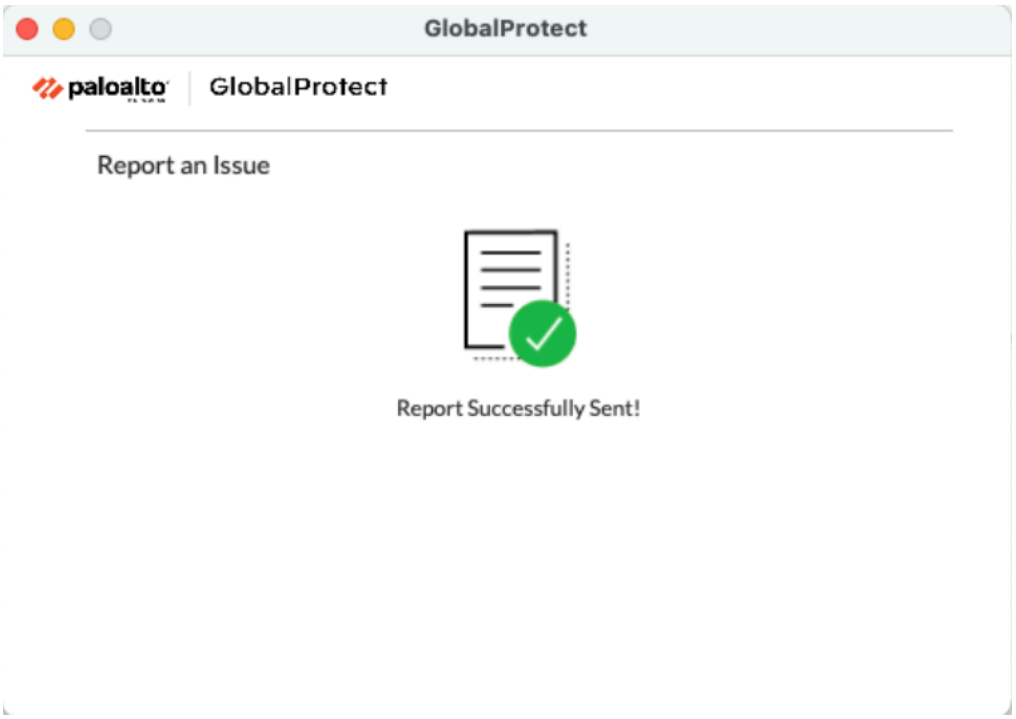
Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging Service de su administrador junto con los archivos pan_gp.trb*.log. La aplicación de GlobalProtect puede ejecutar pruebas de diagnóstico con túnel o sin túnel. Por ejemplo,

es posible que desee introducir sus credenciales de inicio de sesión de GlobalProtect antes de que la aplicación conecte y ejecute pruebas de diagnóstico a través del túnel.



Aparecerá un mensaje que confirma que la aplicación está ejecutando pruebas de diagnóstico solo si ha seleccionado la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**.

5. Haga clic en **Close (Cerrar)** para confirmar que la aplicación envió correctamente el informe a Strata Logging Service. Este mensaje de confirmación muestra la fecha y hora en que se procesó y envió el informe.



Desconectar la aplicación de GlobalProtect para macOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints macOS:	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si el administrador configura el método de conexión de GlobalProtect como **Always On (Siempre activado)**, puede desconectar la aplicación de GlobalProtect. Por ejemplo, es posible que desee desconectar la aplicación si la red privada virtual (VPN) de GlobalProtect no funciona en un hotel y el fallo de la VPN le impide conectarse a Internet. Después de desconectar la aplicación de GlobalProtect, puede conectarse a Internet mediante una comunicación no segura (sin VPN).

El método, el tiempo y el número de veces que puede desconectar la aplicación de GlobalProtect depende de cómo configure el administrador su servicio de GlobalProtect (PanGPS). Esta configuración puede evitar que desconecte la aplicación completamente o Permitirle desconectar la aplicación solo después de responder correctamente a una pregunta.

Si su configuración incluye una pregunta (desafío), la aplicación de GlobalProtect solicita una de las siguientes opciones:

- Motivo por el que desea desconectar la aplicación
- Responder a una o más razones como **velocidad Internet lenta** o **aplicación no funciona** (si es necesario)
- Código de acceso
- Número de ticket de incidencia

Si el desafío implica un código de acceso o un número de ticket, le recomendamos que se ponga en contacto con un administrador de GlobalProtect o una persona del servicio de asistencia por teléfono.

Los administradores suelen proporcionar contraseñas por adelantado, ya sea por correo electrónico (para los nuevos usuarios de GlobalProtect) o publicadas en el sitio web de su organización. En respuesta a un corte o problema del sistema, los administradores también pueden proporcionar códigos de acceso por teléfono.

Antes de obtener un número de ticket válido, su endpoint muestra un número de solicitud de ticket que debe comunicar a su administrador GlobalProtect o a una persona del servicio de asistencia por teléfono. Si se aprueba su solicitud de desconexión, recibirá un número de ticket válido que puede usar para desconectar GlobalProtect.

Los siguientes pasos describen cómo desconectar la aplicación y superar una pregunta:

STEP 1 | Desconecte la aplicación de GlobalProtect.

1. Inicie la aplicación de GlobalProtect haciendo clic en el icono de la bandeja del sistema de GlobalProtect. Se abre el panel de estado.
2. Haga clic en el menú de tres barras para abrir el menú de configuración.
3. Seleccione **Disconnect (Desconectar)**.

*La opción **Disconnect (Desconectar)** solo es visible si la configuración del agente de GlobalProtect le permite desconectar la aplicación. Si la configuración le permite desconectar la aplicación de GlobalProtect sin que tenga que responder a una pregunta (desafío), la aplicación de GlobalProtect se cierra sin que sea necesario realizar ninguna otra acción.*

STEP 2 | Responder a una o más preguntas, si es necesario.

Si se le solicita, proporcione la siguiente información:

- **Tell us the issue to disconnect (Indique el motivo de la desconexión)**: su motivo para desconectar la aplicación de GlobalProtect.
- **Select the reason to disconnect (Seleccione el motivo de la desconexión)**: si su configuración requiere que responda a una o más razones o introduzca otra razón, la aplicación de GlobalProtect muestra las razones tan pronto como seleccione **Disconnect (Desconectarse)**.
- **Passcode (Contraseña)**: código de acceso que suele proporcionar el administrador con antelación, en función de un problema o evento conocido que requiere que desconecte la aplicación.
- **Ticket (Ticket de incidencia)**: si su configuración requiere que proporcione un número de ticket, la aplicación de GlobalProtect muestra un número de solicitud hexadecimal de ticket de ocho caracteres tan pronto como seleccione **Disconnect (Desconectar)**. Para desconectar la aplicación con un número de ticket, póngase en contacto con su administrador o con la persona del servicio de asistencia por teléfono y proporcione el número de solicitud. Después de aprobar su solicitud, su administrador o la persona del servicio de asistencia por teléfono le proporcionará un número de ticket hexadecimal de ocho caracteres. Introduzca el número de ticket en el campo **Ticket (Ticket de incidencia)** y, a continuación, haga clic en **OK (Aceptar)**.

Desinstalar la aplicación de GlobalProtect para macOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints macOS:	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Siga los siguientes pasos para desinstalar la aplicación de GlobalProtect de su endpoint macOS . Tenga en cuenta que al desinstalar la aplicación, ya no tiene acceso VPN a su red corporativa y su endpoint no estará protegido por las políticas de seguridad de su empresa.

Solo los usuarios con privilegios de administrador pueden desinstalar la aplicación de GlobalProtect de los endpoints de macOS.

En los endpoints macOS, puede usar el programa de instalación de macOS (en este caso, el Instalador GlobalProtect) para desinstalar un programa. Para desinstalar la aplicación de GlobalProtect de su endpoint, instale el paquete de software de GlobalProtect e inicie el instalador de GlobalProtect. El Instalador de GlobalProtect le pide que seleccione el paquete **Uninstall GlobalProtect (Desinstalar GlobalProtect)**. Si el administrador habilitó las extensiones del sistema en la aplicación de GlobalProtect para su endpoint macOS durante la instalación de la aplicación de GlobalProtect, la aplicación de GlobalProtect también le solicitará que elimine las extensiones del sistema durante la desinstalación de GlobalProtect. Después de instalar correctamente el paquete **Uninstall GlobalProtect (Desinstalar GlobalProtect)**, la aplicación de GlobalProtect se elimina del endpoint.

Si ya no tiene el instalador de GlobalProtect en su endpoint macOS, puede desinstalar GlobalProtect ejecutando el siguiente comando desde la línea de comandos:

```
sudo /Applications/GlobalProtect.app/Contents/Resources/
uninstall_gp.sh
```

STEP 1 | Inicie sesión en el portal de GlobalProtect.

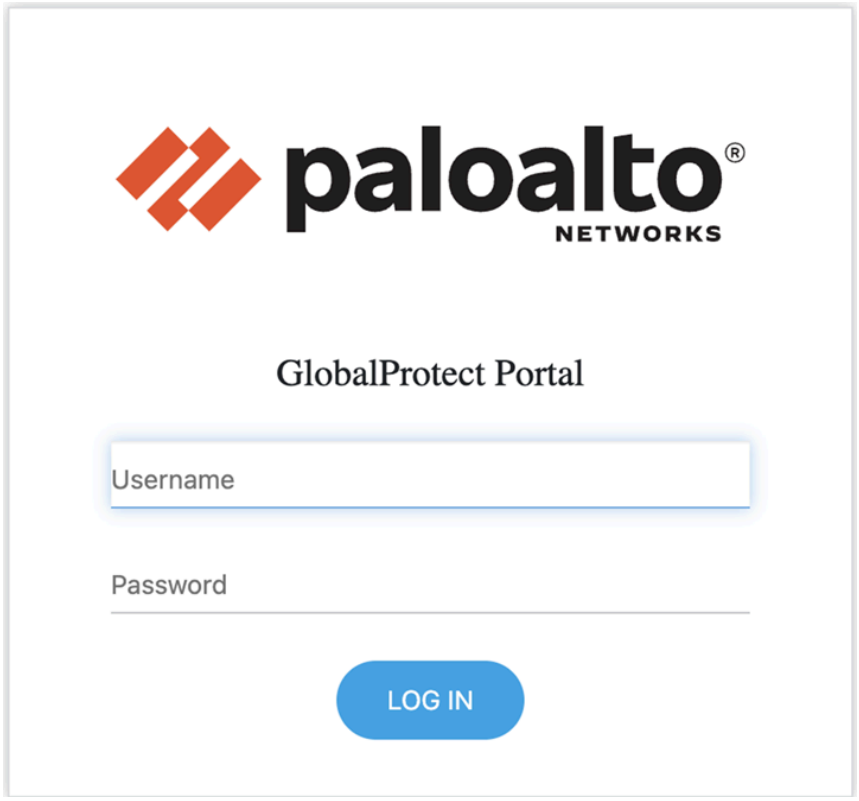
1. Inicie su navegador web y vaya a la siguiente URL:

   `https://<portal address or name>`

   Ejemplo: **`HTTP://gp.acme.com`**

2. En la página de inicio de sesión del portal, introduzca su nombre de usuario en **Name (Nombre)** (nombre de usuario) y **Password (Contraseña)** y, a continuación, haga clic

en **LOG IN (Iniciar sesión)**. En la mayoría de los casos, puede usar el mismo nombre de usuario y contraseña que usa para conectarte a su red corporativa.



STEP 2 | Vaya a la página de descarga de la aplicación.

En la mayoría de las instancias, la página de descarga de la aplicación aparece inmediatamente después de que inicia sesión en el portal.

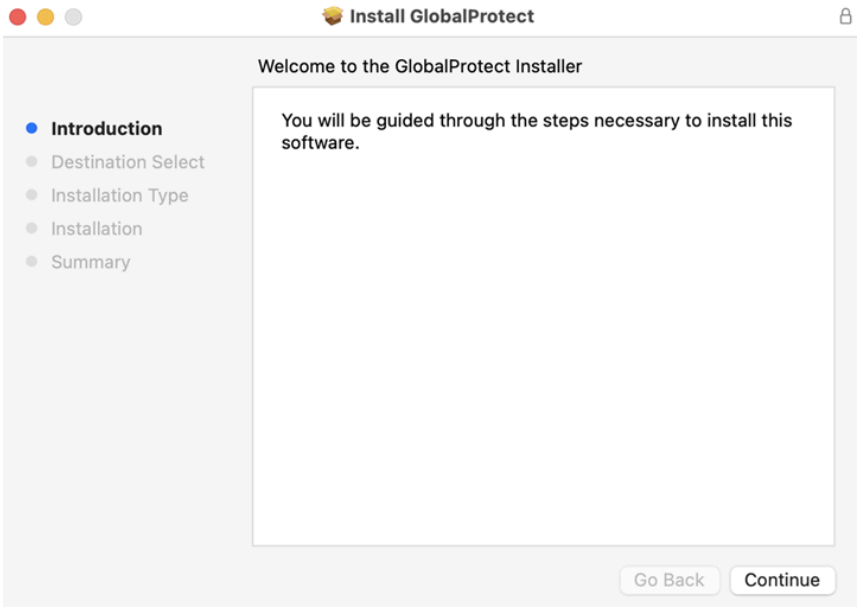
*Si el administrador del sistema ha habilitado el acceso VPN sin cliente de GlobalProtect, la página de la aplicación se abre después de iniciar sesión en el portal (en lugar de la página de descarga de la aplicación). Seleccione **GlobalProtect Agent (Agente de GlobalProtect)** para abrir la página de descarga.*

STEP 3 | Descargue la aplicación.

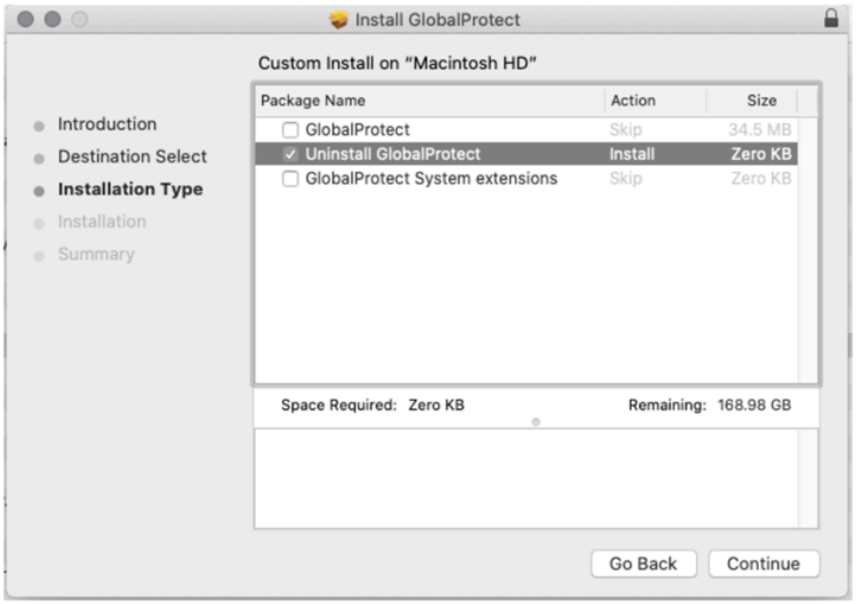
1. Haga clic en **Download Mac 32/64 bit GlobalProtect agent (Descargar agente de GlobalProtect MAC 32/64 bits)**.
2. Cuando se le solicite, proceda a **Run (Ejecutar)** el software.
3. Cuando se le solicite de nuevo, deberá**Run (Ejecutar)** el instalador de GlobalProtect.

STEP 4 | Desinstalar GlobalProtect.

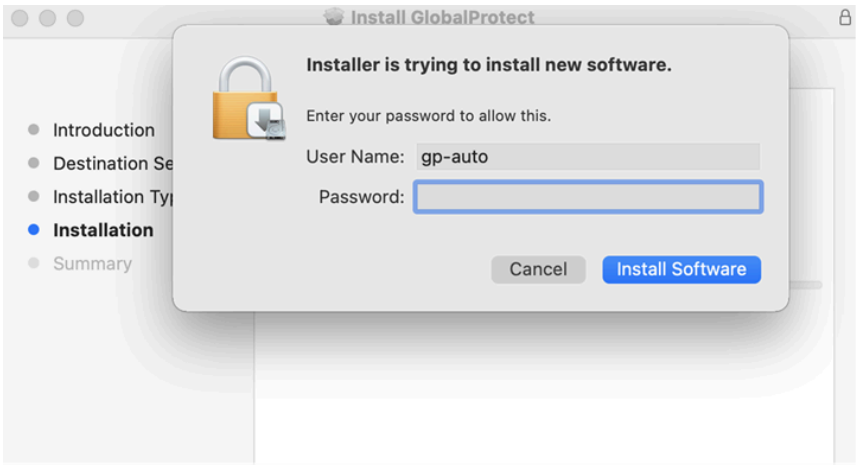
1. Desde el Instalador de GlobalProtect, haga clic en **Continue (Continuar)**.



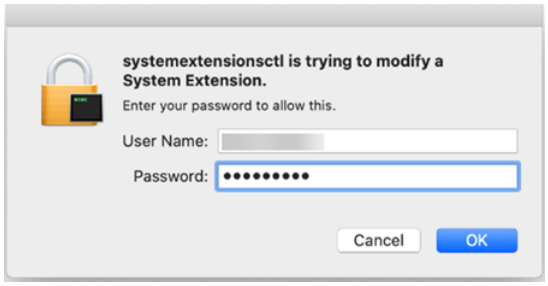
2. En la pantalla **Destination Select (Seleccionar destino)**, haga clic en **Continue (Continuar)**.
3. En la pantalla **Installation Type (Tipo de instalación)**, seleccione la casilla de verificación **Uninstall GlobalProtect (Desinstalar GlobalProtect)** y, a continuación, haga clic en **Continue (Continuar)**.



4. Haga clic en **Install (Instalar)** para confirmar que desea eliminar la aplicación de GlobalProtect.
5. Cuando se le solicite, introduzca su **User Name (Nombre de usuario)** y **Password (Contraseña)**y, a continuación, haga clic en **Install Software (Instalar software)** para desinstalar GlobalProtect.

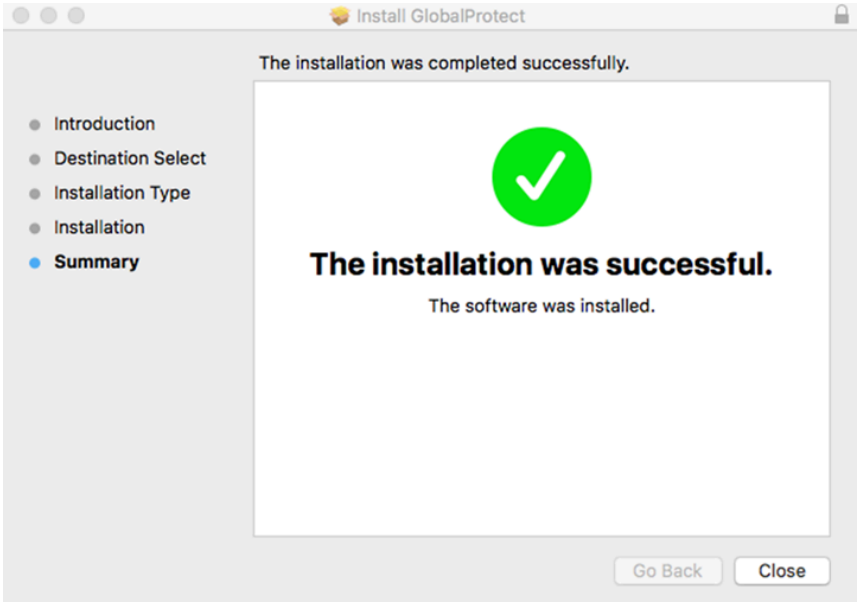


6. Si el administrador del sistema ha habilitado las extensiones del sistema macOS durante la instalación de la aplicación de GlobalProtect 5.1.4 que ejecuta macOS Catalina 10.15.4 o posterior, aparecerá el mensaje emergente para que desinstale las extensiones del sistema. Cuando se le solicite, introduzca su **User Name (Nombre de usuario)** y **Password (Contraseña)** y, a continuación, haga clic en **OK (Aceptar)** para eliminar las extensiones del sistema.



STEP 5 | Confirme que la aplicación de GlobalProtect ya no está instalada.

Aparece un mensaje que confirma que el paquete **Uninstall GlobalProtect (Desinstalar GlobalProtect)** se instaló correctamente. Esta confirmación indica que la aplicación de GlobalProtect se ha eliminado de su endpoint.



Eliminar la extensión del kernel de GlobalProtect Enforcer

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints macOS:	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Cuando desinstale la aplicación de GlobalProtect para macOS y luego instale una nueva instancia de la aplicación, puede encontrar problemas de conexión si la extensión del kernel de GlobalProtect enforcer no se actualiza correctamente. Una extensión del núcleo (`kext`) es un complemento para el sistema operativo macOS que gestiona aplicaciones. Si no puede conectarte a GlobalProtect después de instalar una nueva instancia de la aplicación, utilice los siguientes procedimientos para localizar y eliminar la extensión del kernel de GlobalProtect enforcer.

STEP 1 | Desinstalar la aplicación de GlobalProtect para Mac.

STEP 2 | Determina si la extensión del kernel de GlobalProtect enforcer existe en el endpoint.

En el endpoint macOS, abra la aplicación de **Terminal** en la carpeta **Applications (Aplicaciones)** > **Utilities (Utilidades)** y luego introduzca el siguiente comando:

```
kextstat | grep gplock
```

STEP 3 | Si la extensión existe, descargue el enforcer.

Introduzca el siguiente comando en la aplicación de **Terminal** para descargar el enforcer:

```
sudo kextunload -b com.paloaltonetworks.GlobalProtect.gplock
```

STEP 4 | Evite que el enforcer se recargue después de un reinicio.

Introduzca el siguiente comando en la aplicación de **Terminal** para eliminar el enforcer del disco duro de macOS:

```
sudo rm -r "/System/Library/Extensions/gplock*.kext"
```

STEP 5 | Descargar e instalar la aplicación GlobalProtect para Mac.

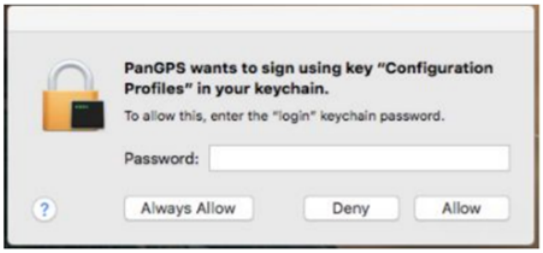
Habilite la aplicación de GlobalProtect para macOS para usar certificados de cliente para la autenticación

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo para endpoints macOS:	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Cuando la aplicación de GlobalProtect se instala en los endpoints macOS por primera vez y la autenticación con certificado de cliente está habilitada en el portal o puerta de enlace, aparece el aviso emergente del Llavero, solicitando a los usuarios que introduzcan su contraseña para que GlobalProtect pueda acceder y utilizar los certificados de cliente del llavero de inicio de sesión. El aviso emergente del llavero también puede aparecer cuando se instala un nuevo certificado porque el certificado anterior ha caducado.

Debe usar el siguiente procedimiento para habilitar la aplicación de GlobalProtect para macOS para usar certificados de cliente para la autenticación:

STEP 1 | Introduzca su contraseña para permitir el acceso al llavero de inicio de sesión con el endpoint macOS en el siguiente aviso emergente del llavero:



STEP 2 | Seleccione **Always Allow (Permitir siempre)** para permitir que GlobalProtect establezca el túnel VPN. El aviso emergente del llavero no aparece hasta que el certificado de cliente ha caducado. Este aviso emergente puede aparecer nuevamente cuando se renueva el certificado de cliente.

*Si selecciona **Allow (Permitir)**, el aviso emergente del llavero aparecerá cada vez que los usuarios se conecten a GlobalProtect. Si selecciona **Deny (Denegar)**, GlobalProtect no puede establecer un túnel VPN y aparecerá el aviso emergente del llavero. GlobalProtect puede establecer un túnel VPN solo después de que permita el acceso al llavero de inicio de sesión.*

Aplicación de GlobalProtect para iOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Sólo endpoints con iOS	☐ Versión 6.1 o posterior de la aplicación GlobalProtect.

GlobalProtect™ es una aplicación que se ejecuta en su endpoint (ordenador de escritorio, portátil, tableta o teléfono inteligente) para protegerlo mediante el uso de las mismas políticas de seguridad que protegen los recursos sensibles de su red corporativa. GlobalProtect™ protege su tráfico de intranet, nube privada, nube pública e Internet, y le permite acceder a los recursos de su empresa desde cualquier parte del mundo.

Descargar e instalar la aplicación GlobalProtect para iOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Sólo endpoints con iOS	❑ Versión 6.1 o posterior de la aplicación GlobalProtect.

Antes de poder conectar su endpoint con iOS a la red GlobalProtect, debe descargar e instalar la aplicación. Si su endpoint con iOS es gestionado por un sistema de gestión de dispositivos móviles (MDM), es posible que su administrador haya enviado automáticamente la aplicación de GlobalProtect a su endpoint y configurado los ajustes de la VPN. Si aún no tiene la aplicación de GlobalProtect en su endpoint con iOS, puede descargarla desde la aplicación Store.

Antes de descargar la aplicación, debe obtener la dirección IP o FQDN del portal de GlobalProtect de su administrador. Además, su administrador debe verificar qué nombre de usuario y contraseña puede usar para conectarse al portal y las puertas de enlace. Este es normalmente el mismo nombre de usuario y contraseña que utiliza para conectarse a su red corporativa. Si su administrador le ha permitido usar información biométrica (huella dactilar o, solo para dispositivos macOS X, Face ID) para iniciar sesión, primero debe iniciar sesión con un nombre de usuario y contraseña dos veces (una para guardarla y otra para autenticarse). A continuación, puede usar información biométrica para iniciar sesión.

Después de recopilar la información requerida, puede descargar e instalar la aplicación de la siguiente manera:

STEP 1 | Inicie el App Store.

STEP 2 | **Busque `GlobalProtect`**.

STEP 3 | En los resultados de búsqueda, seleccione **GlobalProtect™**.

STEP 4 | En la página de producto de la aplicación de GlobalProtect, toque **GET (OBTENER)**.

STEP 5 | Seleccione **Install (Instalar)** la aplicación.

STEP 6 | Cuando se le solicite, deberá**Sign In (iniciar sesión)** con el ID de Apple.

Usar la aplicación de GlobalProtect para iOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Sólo endpoints con iOS	❑ Versión 6.1 o posterior de la aplicación GlobalProtect.

Este tema solo se aplica a usted si su configuración requiere que introduzca sus credenciales de inicio de sesión GlobalProtect después de haber iniciado sesión en su endpoint (el inicio de sesión único está deshabilitado).

Por lo general, recomendamos que las organizaciones permitan que sus usuarios de GlobalProtect inicien sesión de manera transparente después de instalar la aplicación. Después de iniciar sesión en un endpoint con inicio de sesión GlobalProtect transparente, la aplicación de GlobalProtect inicia y se conecta automáticamente a la red corporativa sin intervención adicional del usuario.

Si su configuración requiere que introduzca sus credenciales de GlobalProtect, siga los pasos aplicables a continuación.

STEP 1 | Conéctese a la puerta de enlace o portal de GlobalProtect.

Utilice uno de los siguientes flujos de trabajo para conectarse al portal de GlobalProtect o a la puerta de enlace:

- Experiencia de primera conexión:
  1. Inicie la aplicación de GlobalProtect.
  2. (Opcional) Si no ha habilitado las notificaciones de GlobalProtect en su endpoint, aparecerá un cuadro de diálogo de permiso de notificación. **Allow (Permitir)** que GlobalProtect le envíe notificaciones.

     Si elije **Don”t Allow (No permitir)** que GlobalProtect le envíe notificaciones, aparecerá un recordatorio la próxima vez que inicie la aplicación. Pulse el enlace **Settings -> GlobalProtect** (Configuración -> GlobalProtect) para ir a la pantalla de permisos de

notificación, donde puede habilitar las notificaciones. Si aún no desea habilitar las notificaciones, elija **Skip (Omitir)** esta pantalla.

3. Introduzca la dirección del portal de GlobalProtect.

4. (Opcional) Dependiendo del modo de conexión, toque **Connect (Conectarse)** para iniciar la conexión.
5. Cuando aparezca el mensaje `“GlobalProtect” desea añadir configuraciones VPN`, siga estos pasos para añadir las configuraciones VPN a su endpoint:
   1. Debe **Allow (Permitir)** que GlobalProtect añada configuraciones VPN a su endpoint. Este ajuste permite a GlobalProtect filtrar y supervisar la actividad de red en el endpoint cuando está usando la VPN.

   2. Introduzca su contraseña de iPhone o iPad para confirmar que desea añadir configuraciones VPN a su endpoint.

6. (Opcional) Si su endpoint no puede verificar la identidad del portal de GlobalProtect utilizando el certificado del servidor del portal, aparecerá el mensaje `No es posible verificar la identidad del servidor`. Si confía en el certificado, toque **Continue (Continuar)** para continuar con la conexión.
7. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** y luego en **SIGN IN (Iniciar sesión)**.

   Si su administrador le ha permitido usar información biométrica (huella dactilar o, solo para dispositivos iOS X, face ID) para iniciar sesión, primero debe iniciar sesión con un

nombre de usuario y contraseña dos veces (una para guardarla y otra para autenticarse). A continuación, puede usar información biométrica para iniciar sesión.

8. (Opcional) Si utiliza autenticación multifactor, introduzca el **Code (Código)** de verificación de GlobalProtect que se envía a su endpoint después de iniciar sesión y, a continuación, toque **Continue (Continuar)**.
9. (Opcional) Si el administrador configura la aplicación de GlobalProtect para que muestre un mensaje de bienvenida, el mensaje de bienvenida aparecerá tras una conexión correcta. Cierre el mensaje de bienvenida para ir a la pantalla de inicio.
10. (Opcional) Si hay notificaciones en su aplicación, el cuadro de diálogo Notificaciones aparecerá al conectarse correctamente. Cierre el cuadro de diálogo Notificaciones para pasar a la pantalla de inicio.
11. Cuando aparezca la pantalla de inicio, compruebe que su conexión se ha establecido correctamente. Si la conexión se realiza correctamente, la pantalla de inicio muestra el estado **CONNECTED (CONECTADO)**.
12. (Opcional) De manera predeterminada, el endpoint se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, toque el menú desplegable de la puerta de enlace en la parte inferior de la pantalla de inicio y, a continuación, utilice una de las siguientes opciones:
    - Seleccione una puerta de enlace manualmente (solo puertas de enlace externas). Si su administrador configura más de 10 puertas de enlace externas manuales en la configuración del agente del portal, también puede localizar una puerta de enlace específica mediante la opción de búsqueda de puertas de enlace.
    - Asigne y conéctese automáticamente a una puerta de enlace preferida tocando el icono More Options (Más opciones) ( ) para la puerta de enlace que desea establecer como la puerta de enlace preferida y, a continuación, **Set As Preferred (Establecer como preferida)**. De forma alternativa, puede pulsar durante un tiempo (mantener pulsada) la puerta de enlace y luego **Set As Preferred (Establecer como preferida)**.

      Para eliminar la asignación de puerta de enlace preferida, toque el icono More Options (Más opciones) ( ) para la puerta de enlace preferida y, a continuación, **Remove Preferred (Eliminar preferida)**. De forma alternativa, puede pulsar durante

un tiempo (mantener pulsada) la puerta de enlace y luego **Remove Preferred (Eliminar preferida)**.

- Experiencia de conexión bajo demanda (VPN de acceso remoto):

  Cuando el administrador de GlobalProtect configura GlobalProtect con el método de conexión **On-Demand (Bajo demanda)**, debe iniciar la aplicación de GlobalProtect para iniciar la conexión manualmente. Una vez iniciada la conexión, puede **TAP TO CONNECT (TOCAR PARA CONECTAR)** para establecer la conexión a GlobalProtect. Si su administrador habilita GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, la conexión se establece sin requerir más interacción del usuario. Si su administrador no habilita GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, debe iniciar sesión para establecer la conexión.

- Experiencia de conexión Always On (Siempre activado)

  Cuando el administrador de GlobalProtect configura GlobalProtect con el método de conexión **Always On (Siempre activado)**, la conexión se inicia automáticamente. Dependiendo de si su administrador configura la aplicación de GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, puede establecer la conexión de GlobalProtect sin iniciar la aplicación. Si su administrador habilita GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, la conexión se establece automáticamente sin requerir ninguna interacción del usuario. Si su administrador no habilita GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, debe iniciar sesión a través de la aplicación para establecer la conexión.
- (Opcional) Si su administrador ha configurado GlobalProtect con el método de conexión **Always On (Siempre activado)**, la conexión se inicia automáticamente. La pantalla de inicio muestra el estado **CONNECTED (CONECTADO)**.

  Con el método de conexión **Always On (Siempre activado)**, la pantalla de inicio muestra el estado **CONNECTED (CONECTADO)** con un mensaje de desconexión para evitar que se desconecte cuando intente tocar el icono **Connect (Conectar)**.

STEP 2 | Consulte información sobre su conexión a GlobalProtect.

Después de establecer la conexión de GlobalProtect, inicie la aplicación de GlobalProtect. Haga clic en el icono de configuración para abrir el menú de ajustes. En el menú de configuración,

toque **SETTINGS (Configuración)** para ver información sobre su conexión, incluida la dirección del **Portal** y el **Status (Estado)** de la conexión.

- Si desea conectarse a otro portal de GlobalProtect, pulse la dirección del **Portal**. Cuando se le solicite, introduzca una nueva dirección de portal y, a continuación, toque **CONNECT (CONECTAR)**.
- Si está conectado a una puerta de enlace externa, toque el **Status (Estado)** de la conexión para ver detalles adicionales sobre su conexión (incluido el SSID de red y la dirección IP/FQDN).

STEP 3 | (Opcional) Cambie la contraseña guardada.

Si el administrador de GlobalProtect configura el agente del portal de GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, las credenciales se guardarán automáticamente en la aplicación de GlobalProtect. Cuando su contraseña caduque o un administrador RADIUS o AD requiera un cambio de contraseña en el próximo inicio de sesión, puede actualizar su contraseña en la aplicación. Esta función solo se habilita cuando se autentica con un servidor RADIUS utilizando el Protocolo de autenticación extensible protegido con el protocolo de autenticación por desafío mutuo de Microsoft versión 2 (PEAP-MSCHAPv2).

1. Inicie la aplicación de GlobalProtect.
2. Desde la pantalla de inicio, **TAP TO CONNECT (TOCAR PARA CONECTAR)**.
3. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** *anteriores* y haga clic en **SIGN IN (Iniciar sesión)**.
4. Cuando la aplicación de GlobalProtect le indica que debe `Actualizar la contraseña`, introduzca su **Current Password (Contraseña actual)** seguida de su **New Password (Nueva contraseña)**.
5. Deberá **Retype Password (Volver a escribir la contraseña)** para confirmar su nueva contraseña.
6. Ahora deberá **SIGN IN (Iniciar sesión)** para volver a conectarte a GlobalProtect con su nueva contraseña.

STEP 4 | (Opcional) Desconéctese de GlobalProtect.

Si su administrador configura GlobalProtect con el método de conexión **On-Demand (Bajo demanda)**, puede **TAP TO DISCONNECT (TOCAR PARA DESCONECTARSE)** de la pantalla de inicio.

Informar de un problema desde la aplicación de GlobalProtect para iOS

¿Dónde puedo usar esto?	¿Qué necesito?
• Sólo endpoints con iOS	❑ Versión 6.1 o posterior de la aplicación GlobalProtect.

Si experimenta un comportamiento inusual, como un rendimiento de red deficiente o si no se establece la conexión con el portal y la puerta de enlace, puede informar de la incidencia directamente a Strata Logging Service para que su administrador pueda acceder a ella Ya no es necesario recopilar y enviar manualmente los logs de aplicaciones de GlobalProtect por correo electrónico o almacenarlos en una unidad de nube.

*Para mostrar la opción **Report an Issue (Informar de un problema)** en la aplicación de GlobalProtect, su administrador debe habilitar la recopilación de logs de la aplicación de GlobalProtect para la resolución de problemas en el portal de GlobalProtect.*

STEP 1 | Conéctese a la puerta de enlace o portal de GlobalProtect.

1. Inicie la aplicación de GlobalProtect.
2. Introduzca la dirección del portal de GlobalProtect.
3. (Opcional) Dependiendo del modo de conexión, toque **Connect (Conectarse)** para iniciar la conexión.
4. Debe **Allow (Permitir)** que GlobalProtect añada configuraciones VPN a su endpoint. Este ajuste permite a GlobalProtect filtrar y supervisar la actividad de red en el endpoint cuando está usando la VPN.
5. Introduzca su contraseña de iPhone o iPad para confirmar que desea añadir configuraciones VPN a su endpoint.
6. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** y luego en **SIGN IN (Iniciar sesión)**.
7. Cuando aparezca la pantalla de inicio, compruebe que su conexión se ha establecido correctamente. Si la conexión es correcta, la pantalla de inicio muestra el estado **CONNECTED (CONECTADO)**.
8. (Opcional) De manera predeterminada, el endpoint se conecta automáticamente a la puerta de enlace Mejor disponible, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, toque el menú desplegable Puerta de enlace en la parte inferior de la pantalla de inicio y, a continuación, seleccione una puerta de enlace de la lista (solo puertas de enlace externas).

STEP 2 | Consulte información sobre su conexión a GlobalProtect.

Después de establecer la conexión de GlobalProtect, inicie la aplicación de GlobalProtect. Haga clic en el icono de configuración para abrir el menú de ajustes. En el menú de configuración,

toque **SETTINGS (Configuración)** para ver información sobre su conexión, incluida la dirección del **Portal** y el **Status (Estado)** de la conexión.

STEP 3 | Informe un problema de la aplicación de GlobalProtect desde el endpoint del usuario final.

Después de iniciar la aplicación, toque en **HELP (Ayuda)** para informar de un problema desde su endpoint.

1. Toque **Report an Issue (Informar de un problema)**.

2. Habilite la aplicación de GlobalProtect para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico. Los logs de diagnóstico y resolución de problemas se recopilan y envían a Strata Logging Service como un informe de resolución de problemas compacto.

   Después de que las pruebas de diagnóstico se completen correctamente, los archivos de log de depuración de GlobalProtect se cargan en Strata Logging Service desde su endpoint.

   *Si no habilita la aplicación para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico, solo se recopilan logs de resolución de problemas y se envían a Strata Logging Service como un informe de resolución de problemas compacto. La aplicación de GlobalProtect comprueba los archivos de informe (pan_gp.trb.log o pan_gp_trbl.log) que se generan automáticamente en formato `.json`. Aparece un mensaje de notificación si no se encontraron problemas en los logs de resolución de problemas. Haga clic en **Retry (Reintentar)** para verificar si existen los archivos pan_gp.trb*.log.*

3. Seleccione la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**
4. Pulse **CONTINUE (CONTINUAR)** para permitir que la aplicación cree un log de resolución de problemas y envíe el informe a la instancia de Strata Logging Service de su administrador.

   Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging Service de su administrador junto con los archivos pan_gp.trb*.log.

   Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging Service de su administrador junto con los archivos pan_gp.trb*.log. La aplicación de GlobalProtect puede ejecutar pruebas de diagnóstico con túnel o sin túnel. Por ejemplo,

es posible que desee introducir sus credenciales de inicio de sesión de GlobalProtect antes de que la aplicación conecte y ejecute pruebas de diagnóstico a través del túnel.

Aparecerá un mensaje que confirma que la aplicación está ejecutando pruebas de diagnóstico solo si ha seleccionado la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**.

Aparece un mensaje que confirma que la aplicación está enviando el informe a Strata Logging Service.

5. Pulse **DONE (HECHO)** para confirmar que la aplicación envió correctamente el informe a Strata Logging Service.

Desinstalar la aplicación de GlobalProtect para iOS.

¿Dónde puedo usar esto?	¿Qué necesito?
• Sólo endpoints con iOS	❑ Versión 6.1 o posterior de la aplicación GlobalProtect.

Siga los siguientes pasos para desinstalar la aplicación de GlobalProtect de su endpoint con iOS . Tenga en cuenta que al desinstalar la aplicación, ya no tiene acceso VPN a su red corporativa y su endpoint no estará protegido por las políticas de seguridad de su empresa.

STEP 1 | Mantenga pulsado el icono de la aplicación GlobalProtect hasta que el icono se mueva.

STEP 2 | Pulse la **X** en la esquina superior izquierda del icono.

STEP 3 | Cuando se le solicite, elija **Delete (Eliminar)** GlobalProtect.

STEP 4 | Pulse **Done (Listo)** o pulse el botón de inicio para volver a la pantalla de inicio.

Aplicación de GlobalProtect para Android

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints con Android	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

GlobalProtect™ es una aplicación que se ejecuta en su endpoint (ordenador de escritorio, portátil, tableta o teléfono inteligente) para protegerlo mediante el uso de las mismas políticas de seguridad que protegen los recursos sensibles de su red corporativa. GlobalProtect™ protege su tráfico de intranet, nube privada, nube pública e Internet, y le permite acceder a los recursos de su empresa desde cualquier parte del mundo.

Los siguientes temas describen cómo instalar y utilizar la aplicación de GlobalProtect para Android:

- Descargar e instalar la aplicación de GlobalProtect para Android
- Descargar e instalar la aplicación de GlobalProtect para Android en Chromebooks
- Utilice la aplicación de GlobalProtect para Android
- Informar de un problema desde la aplicación de GlobalProtect para Android
- Desconectar la aplicación de GlobalProtect para Android
- Desinstalar la aplicación de GlobalProtect para Android
- Desinstalar la aplicación de GlobalProtect para Android de Chromebooks

Descargar e instalar la aplicación de GlobalProtect para Android

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints con Android	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Antes de poder conectar su endpoint Android a la red GlobalProtect, debe descargar e instalar la aplicación. Si su endpoint con Android está gestionado por un sistema de gestión de dispositivos móviles (MDM), es posible que su administrador haya enviado automáticamente la aplicación de GlobalProtect a su endpoint y configurado los ajustes de VPN. Si aún no tiene la aplicación de GlobalProtect en su endpoint con Android, puede descargarla desde Google Play.

Antes de descargar la aplicación, debe obtener la dirección IP o FQDN del portal de GlobalProtect de su administrador. Además, su administrador debe verificar qué nombre de usuario y contraseña puede usar para conectarse al portal y las puertas de enlace. Este es normalmente el mismo nombre de usuario y contraseña que utiliza para conectarse a su red corporativa.

Después de recopilar la información requerida, puede descargar e instalar la aplicación de la siguiente manera:

STEP 1 | Inicie Google Play.

STEP 2 | **Busque `GlobalProtect`.**

STEP 3 | En los resultados de búsqueda, seleccione **GlobalProtect**.

STEP 4 | En la página del producto de la aplicación de GlobalProtect, toque **Install (Instalar)**.

STEP 5 | Cuando se le solicite, revise y seleccione **Accept (Aceptar)** la información para la que GlobalProtect necesita acceso.

Descargar e instalar la aplicación de GlobalProtect para Android en Chromebooks

¿Dónde puedo usar esto?	¿Qué necesito?
• Sólo endpoints con Android (Chromebooks)	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Para usar la aplicación de GlobalProtect para Android en un Chromebook, debe descargar e instalar la aplicación. Si su Chromebook está gestionado por Workspace ONE o la consola de gestión de Google, es posible que su administrador haya enviado automáticamente la aplicación de GlobalProtect a su endpoint y configurado los ajustes de la VPN. Si aún no tiene la aplicación de GlobalProtect para Android en su Chromebook, puede descargarla desde Google Play Store.

Antes de descargar la aplicación, debe obtener la dirección IP o FQDN del portal de GlobalProtect de su administrador. Además, su administrador debe verificar qué nombre de usuario y contraseña puede usar para conectarse al portal y las puertas de enlace. Este es normalmente el mismo nombre de usuario y contraseña que utiliza para conectarse a su red corporativa.

Después de recopilar la información requerida, puede descargar e instalar la aplicación de la siguiente manera:

La aplicación de GlobalProtect para Android solo se admite en algunos Chromebooks. Si estaba usando la versión 4.1.x de la aplicación de GlobalProtect para Chrome OS, la aplicación ya no está disponible. Considere la posibilidad de actualizar a un sistema Chrome OS que admita aplicaciones de Android y utilice la aplicación de GlobalProtect para Android.

STEP 1 | Habilite la aplicación Google Play Store en su Chromebook.

1. (Opcional) Si su Chromebook está ejecutando Chrome OS versión 52 o anterior, actualice su sistema operativo Chromebook.
2. Desde su Chromebook, haga clic en la foto de su cuenta en la esquina inferior derecha de la pantalla.
3. Seleccione **Settings**.
4. En el área Google Play Store, seleccione **Enable Google Play Store on your Chromebook (Habilitar Google Play Store en su Chromebook)**.

   Si esta opción no está disponible, su Chromebook no admite aplicaciones Android.
5. Cuando se le solicite, haga clic en **Get Started (Comenzar)** para iniciar Google Play Store.
6. Deberá **Agree (Aceptar)** las condiciones de servicio.
7. En la página de bienvenida, deberá **SIGN IN (Iniciar sesión)** en Google Play Store.
8. Deberá **Accept (Aceptar)** las condiciones de servicio de Google Play.

STEP 2 | Descargue e instale la aplicación de GlobalProtect para endpoints con Android en su Chromebook.

1. Abra la aplicación Google Play Store.
2. Busque la **`aplicación de GlobalProtect`**.
3. Haga clic en el icono de la aplicación de GlobalProtect.
4. Haga clic en **INSTALL (Instalar)** y, a continuación, siga las instrucciones que aparecen en pantalla para completar la instalación de la aplicación.

Utilice la aplicación de GlobalProtect para Android

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints con Android	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Este tema solo se aplica a usted si su configuración requiere que introduzca sus credenciales de inicio de sesión GlobalProtect después de haber iniciado sesión en su endpoint (el inicio de sesión único está deshabilitado).

Por lo general, recomendamos que las organizaciones permitan que sus usuarios de GlobalProtect inicien sesión de manera transparente después de instalar la aplicación. Después de iniciar sesión en un endpoint con inicio de sesión GlobalProtect transparente, la aplicación de GlobalProtect inicia y se conecta automáticamente a la red corporativa sin intervención adicional del usuario.

Si su configuración requiere que introduzca sus credenciales de GlobalProtect, siga los pasos aplicables a continuación.

STEP 1 | Conéctese a la puerta de enlace o portal de GlobalProtect.

Utilice uno de los siguientes flujos de trabajo para conectarse al portal de GlobalProtect o a la puerta de enlace:

- Experiencia de primera conexión:
  1. Inicie la aplicación de GlobalProtect.
  2. Introduzca la dirección del portal de GlobalProtect.
  3. (Opcional) Dependiendo del modo de conexión, toque **Connect (Conectarse)** para iniciar la conexión.
  4. (Opcional) Si su endpoint no puede verificar la identidad del portal de GlobalProtect utilizando el certificado del servidor del portal, aparecerá el mensaje `No es posible`

`verificar la identidad del servidor`. Si confía en el certificado, toque **Continue (Continuar)** para continuar con la conexión.

5. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** y luego en **SIGN IN (Iniciar sesión)**.

   Si su administrador le ha permitido utilizar la información biométrica (huella digital) para iniciar sesión, primero debe iniciar sesión con un nombre de usuario y contraseña; a continuación, puede utilizar la información biométrica para iniciar sesión.

6. Cuando aparezca el mensaje de `Connection request (Solicitud de conexión)`, toque **OK (Aceptar)** para permitir que GlobalProtect configure una conexión VPN en su endpoint.

7. (Opcional) Si utiliza autenticación multifactor, introduzca el **Code (Código)** de verificación de GlobalProtect que se envía a su endpoint después de iniciar sesión y, a continuación, toque **Continue (Continuar)**.
8. (Opcional) Si el administrador configura la aplicación de GlobalProtect para que muestre un mensaje de bienvenida, el mensaje de bienvenida aparecerá tras una conexión correcta. Pulse fuera del mensaje de bienvenida para ir a la pantalla de inicio.

9. (Opcional) Si hay notificaciones en su aplicación, el cuadro de diálogo Notificaciones aparecerá al conectarse correctamente. Cierre el cuadro de diálogo Notificaciones para pasar a la pantalla de inicio.

10. Cuando aparezca la pantalla de inicio, compruebe que su conexión se ha establecido correctamente. Si la conexión se realiza correctamente, la pantalla de inicio muestra el estado **CONNECTED (CONECTADO)**.

11. (Opcional) Si su administrador ha configurado GlobalProtect con el método de conexión **Always On (Siempre activado)**, la conexión se inicia automáticamente. La pantalla de inicio muestra el estado **CONNECTED (CONECTADO)**.

    Con el método de conexión **Always On (Siempre activado)**, la pantalla de inicio muestra el estado **CONNECTED (CONECTADO)** con un mensaje de desconexión para evitar que se desconecte cuando intente tocar el icono **Connect (Conectar)**.

12. (Opcional) De manera predeterminada, el endpoint se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, toque el menú desplegable Puerta de

enlace en la parte inferior de la pantalla de inicio y, a continuación, seleccione una puerta de enlace de la lista (solo puertas de enlace externas).

- Experiencia de conexión bajo demanda (VPN de acceso remoto):

  Cuando su administrador de GlobalProtect configura GlobalProtect con el método de conexión **On-Demand (Bajo demanda)**, debe iniciar la aplicación de GlobalProtect para iniciar la conexión manualmente. Una vez iniciada la conexión, puede **TAP TO CONNECT (TOCAR PARA CONECTAR)** para establecer la conexión a GlobalProtect. Si su administrador habilita GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, la conexión se establece sin requerir más interacción del usuario. Si su administrador no habilita GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, debe iniciar sesión para establecer la conexión.

- Experiencia de conexión Always On (Siempre activado):

  Cuando el administrador de GlobalProtect configura GlobalProtect con el método de conexión **Always On (Siempre activado)**, la conexión se inicia automáticamente. Dependiendo de si su administrador configura la aplicación de GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, puede establecer la conexión de GlobalProtect sin iniciar la aplicación. Si su administrador habilita GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, la conexión se establece automáticamente sin requerir ninguna interacción del usuario. Si su administrador no habilita GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, debe iniciar sesión a través de la aplicación para establecer la conexión.

STEP 2 | Consulte información sobre su conexión a GlobalProtect.

Después de establecer la conexión de GlobalProtect, inicie la aplicación de GlobalProtect. Haga clic en el icono de configuración para abrir el menú de ajustes. En el menú de configuración, toque **SETTINGS (Configuración)** para ver información sobre su conexión, incluida la dirección del **Portal** y el **Status (Estado)** de la conexión.

- Si desea conectarse a otro portal de GlobalProtect, pulse la dirección del **Portal**. Cuando se le solicite, introduzca una nueva dirección de portal y, a continuación, toque **CONNECT (CONECTAR)**.

- Si está conectado a una puerta de enlace externa, toque el **Status (Estado)** de la conexión para ver detalles adicionales sobre su conexión (incluido el SSID de red y la dirección IP/FQDN).

STEP 3 | (Opcional) Cambie la contraseña guardada.

Si el administrador de GlobalProtect configura el agente del portal de GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, las credenciales se guardarán automáticamente en la aplicación de GlobalProtect. Cuando su contraseña caduque o un administrador RADIUS o AD requiera un cambio de contraseña en el próximo inicio de

sesión, puede actualizar su contraseña en la aplicación. Esta función solo se habilita cuando se autentica con un servidor RADIUS utilizando el Protocolo de autenticación extensible protegido con el protocolo de autenticación por desafío mutuo de Microsoft versión 2 (PEAP-MSCHAPv2).

1. Inicie la aplicación de GlobalProtect.
2. Desde la pantalla de inicio, **TAP TO CONNECT (TOCAR PARA CONECTAR)**.
3. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** *anteriores* y haga clic en **SIGN IN (Iniciar sesión)**.
4. Cuando la aplicación de GlobalProtect le indica que debe `Actualizar la contraseña`, introduzca su **Current Password (Contraseña actual)** seguida de su **New Password (Nueva contraseña)**.
5. Deberá **Retype Password (Volver a escribir la contraseña)** para confirmar su nueva contraseña.
6. Ahora deberá **SIGN IN (Iniciar sesión)** para volver a conectarte a GlobalProtect con su nueva contraseña.

STEP 4 | (Opcional) Desconéctese de GlobalProtect.

Si su administrador configura GlobalProtect con el método de conexión **On-Demand (Bajo demanda)**, puede **TAP TO DISCONNECT (TOCAR PARA DESCONECTARSE)** de la pantalla de inicio.

Informar de un problema desde la aplicación de GlobalProtect para Android

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints con Android	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si experimenta un comportamiento inusual, como un rendimiento de red deficiente o si no se establece la conexión con el portal y la puerta de enlace, puede informar de la incidencia directamente a Strata Logging Service para que su administrador pueda acceder a ella Ya no es necesario recopilar y enviar manualmente los logs de aplicaciones de GlobalProtect por correo electrónico o almacenarlos en una unidad de nube.

*Para mostrar la opción **Report an Issue (Informar de un problema)** en la aplicación de GlobalProtect, su administrador debe habilitar la recopilación de logs de la aplicación de GlobalProtect para la resolución de problemas en el portal de GlobalProtect.*

STEP 1 | Conéctese a la puerta de enlace o portal de GlobalProtect.

1. Inicie la aplicación de GlobalProtect.
2. Introduzca la dirección del portal de GlobalProtect.
3. (Opcional) Dependiendo del modo de conexión, toque **Connect (Conectarse)** para iniciar la conexión.
4. (Opcional) Si se le solicita, introduzca su **Username (Nombre de usuario)** y **Password (Contraseña)** y luego en **SIGN IN (Iniciar sesión)**.
5. Cuando aparezca el mensaje de **Connection request (Solicitud de conexión)**, toque **OK (Aceptar)** para permitir que GlobalProtect configure una conexión VPN en su endpoint.
6. Cuando aparezca la pantalla de inicio, compruebe que su conexión se ha establecido correctamente. Si la conexión es correcta, la pantalla de inicio muestra el estado **CONNECTED (CONECTADO)**.
7. (Opcional) De manera predeterminada, el endpoint se conecta automáticamente a la puerta de enlace Mejor disponible, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, toque el menú desplegable Puerta de enlace en la parte inferior de la pantalla de inicio y, a continuación, seleccione una puerta de enlace de la lista (solo puertas de enlace externas).

STEP 2 | Consulte información sobre su conexión a GlobalProtect.

Después de establecer la conexión de GlobalProtect, inicie la aplicación de GlobalProtect. Haga clic en el icono de configuración para abrir el menú de ajustes. En el menú de configuración, toque **SETTINGS (Configuración)** para ver información sobre su conexión, incluida la dirección del **Portal** y el **Connection Status (Estado de la conexión)**.

STEP 3 | Informe un problema de la aplicación de GlobalProtect desde el endpoint del usuario final.

Después de iniciar la aplicación, toque en **HELP (Ayuda)** para informar de un problema desde su endpoint.

1. Toque **Report an Issue (Informar de un problema)**.

2. Habilite la aplicación de GlobalProtect para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico. Los logs de diagnóstico y resolución de problemas se recopilan y envían a Strata Logging Service como un informe de resolución de problemas compacto.

   Después de que las pruebas de diagnóstico se completen correctamente, los archivos de log de depuración de GlobalProtect se cargan en Strata Logging Service desde su endpoint.

   *Si no habilita la aplicación para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico, solo se recopilan logs de resolución de problemas y se envían a Strata Logging Service como un informe de resolución de problemas compacto. La aplicación de GlobalProtect comprueba los archivos de informe (pan_gp.trb.log o pan_gp_trbl.log) que se generan automáticamente en formato `.json`. Aparece un mensaje de notificación si no se encontraron problemas en los logs de resolución de problemas. Haga clic en **Retry (Reintentar)** para verificar si existen los archivos pan_gp.trb*.log.*

3. Seleccione la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**
4. Pulse **CONTINUE (CONTINUAR)** para permitir que la aplicación cree un log de resolución de problemas y envíe el informe a la instancia de Strata Logging Service de su administrador.

   Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging Service de su administrador junto con los archivos pan_gp.trb*.log.

   Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging Service de su administrador junto con los archivos pan_gp.trb*.log. La aplicación de GlobalProtect puede ejecutar pruebas de diagnóstico con túnel o sin túnel. Por ejemplo,

es posible que desee introducir sus credenciales de inicio de sesión de GlobalProtect antes de que la aplicación conecte y ejecute pruebas de diagnóstico a través del túnel.

Aparecerá un mensaje que confirma que la aplicación está ejecutando pruebas de diagnóstico solo si ha seleccionado la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**.

Aparece un mensaje que confirma que la aplicación está enviando el informe a Strata Logging Service.

5. Pulse **DONE (HECHO)** para confirmar que la aplicación envió correctamente el informe a Strata Logging Service.

Desconectar la aplicación de GlobalProtect para Android

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints con Android	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si el administrador configura el método de conexión de GlobalProtect como **Always On (Siempre activado)**, puede desconectar la aplicación de GlobalProtect. Por ejemplo, es posible que desee desconectar la aplicación si la red privada virtual (VPN) de GlobalProtect no funciona en un hotel y el fallo de la VPN le impide conectarse a Internet. Después de desconectar la aplicación de GlobalProtect, puede conectarse a Internet mediante una comunicación no segura (sin VPN).

El método, el tiempo y el número de veces que puede desconectar la aplicación de GlobalProtect depende de cómo configure el administrador su servicio de GlobalProtect (PanGPS). Esta configuración puede evitar que desconecte la aplicación completamente o Permitirle desconectar la aplicación solo después de responder correctamente a una pregunta.

Si su configuración incluye una pregunta (desafío), la aplicación de GlobalProtect solicita una de las siguientes opciones:

- Motivo por el que desea desconectar la aplicación
- Código de acceso

Si la pregunta implica un código de acceso, le recomendamos que se ponga en contacto con un administrador de GlobalProtect o con una persona del servicio de asistencia por teléfono. Los administradores suelen proporcionar contraseñas por adelantado, ya sea por correo electrónico (para los nuevos usuarios de GlobalProtect) o publicadas en el sitio web de su organización. En respuesta a un corte o problema del sistema, los administradores también pueden proporcionar códigos de acceso por teléfono.

Los siguientes pasos describen cómo desconectar la aplicación y superar una pregunta:

STEP 1 | Desconecte la aplicación de GlobalProtect.

1. Inicie la aplicación de GlobalProtect.
2. Haga clic en el icono de configuración para abrir el menú de ajustes.
3. En el menú de configuración, toque **DISCONNECT (DESCONECTAR)**.

*La opción **Disconnect (Desconectar)** solo es visible si la configuración del agente de GlobalProtect le permite desconectar la aplicación. Si la configuración le permite desconectar la aplicación de GlobalProtect sin que tenga que responder a una pregunta (desafío), la aplicación de GlobalProtect se cierra sin que sea necesario realizar ninguna otra acción.*

STEP 2 | Responder a una o más preguntas, si es necesario.

Si se le solicita, proporcione la siguiente información:

- **Reason (Motivo)**: su motivo para desconectar la aplicación de GlobalProtect.

- **Passcode (Contraseña)**: código de acceso que suele proporcionar el administrador con antelación, en función de un problema o evento conocido que requiere que desconecte la aplicación.

Desinstalar la aplicación de GlobalProtect para Android

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints con Android	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Siga los siguientes pasos para desinstalar la aplicación de GlobalProtect de su endpoint con Android . Tenga en cuenta que al desinstalar la aplicación, ya no tiene acceso VPN a su red corporativa y su endpoint no estará protegido por las políticas de seguridad de su empresa.

STEP 1 | Inicie la aplicación de configuración.

STEP 2 | Pulse **Apps & notifications (Aplicaciones y notificaciones)**.

STEP 3 | Pulse **GlobalProtect**.

STEP 4 | Pulse **Uninstall (Desinstalar)**.

Desinstalar la aplicación de GlobalProtect para Android de Chromebooks

¿Dónde puedo usar esto?	¿Qué necesito?
• Sólo endpoints con Android (Chromebooks)	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Siga los siguientes pasos para desinstalar la aplicación de GlobalProtect para Android de su Chromebook . Tenga en cuenta que al desinstalar la aplicación, ya no tiene acceso VPN a su red corporativa y su endpoint no estará protegido por las políticas de seguridad de su empresa.

STEP 1 | Abra la aplicación Google Play Store.

STEP 2 | Haga clic en el botón de menú () junto a la barra de búsqueda de Google Play.

STEP 3 | Seleccione **Apps & games (Aplicaciones y juegos)** > **My apps & games (Mis aplicaciones y juegos)**.

STEP 4 | Seleccione **INSTALLED (INSTALADO)**.

STEP 5 | En el área En este dispositivo, seleccione **GlobalProtect**.

STEP 6 | Haga clic en **UNINSTALL (DESINSTALAR)**.

Aplicación de GlobalProtect para Linux

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints de Linux	☐ Versión 6.3 o posterior de la aplicación de GlobalProtect.

GlobalProtect™ es un programa que se ejecuta en su endpoint (ordenador de escritorio, portátil o servidor) para protegerlo mediante el uso de las mismas políticas de seguridad que protegen los recursos confidenciales de su red corporativa. GlobalProtect™ protege su tráfico de intranet, nube privada, nube pública e Internet, y le permite acceder a los recursos de su empresa desde cualquier parte del mundo.

Las siguientes secciones proporcionan instrucciones para instalar y usar la aplicación de GlobalProtect para Linux:

- Descargar e instalar la aplicación GlobalProtect para Linux
- Usar la aplicación de GlobalProtect para Linux
- Informar de un problema desde la aplicación de GlobalProtect para Linux
- Deshabilitar la aplicación de GlobalProtect para Linux
- Desinstalar la aplicación de GlobalProtect para Linux

Descargar e instalar la aplicación GlobalProtect para Linux

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints de Linux	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

GlobalProtect le ofrece dos métodos diferentes para instalar la aplicación de GlobalProtect en su dispositivo Linux: una versión de instalación basada en GUI y una versión CLI. Si utiliza un sistema operativo Linux compatible con una interfaz gráfica, puede instalar la versión de interfaz gráfica de usuario de GlobalProtect; de lo contrario, descargue e instale la versión CLI de la aplicación de GlobalProtect.

- Descargar e instalar la versión GUI de GlobalProtect para Linux
- Descargar e instalar la versión de CLI de GlobalProtect para Linux

Descargar e instalar la versión GUI de GlobalProtect para Linux

Si su dispositivo Linux admite una interfaz gráfica de usuario, complete estos pasos para instalar la versión de interfaz gráfica de usuario de GlobalProtect para Linux.

STEP 1 | Descargue la aplicación de GlobalProtect para Linux.

1. Inicie sesión en el Portal de atención al cliente. Después de introducir su nombre de usuario y credenciales de contraseña, se autentica y se inicia sesión en el sitio de asistencia.
2. Seleccione **Updates (Actualizaciones)** > **Software Updates (Actualizaciones de software)**.
3. Filtre por agente de GlobalProtect para Linux, y descargue el archivo TGZ asociado.
4. Extraiga los archivos del paquete.

```
user@linuxhost:~$ tar -xvf ~/pkgs/PanGPLinux-6.0.0.tgz
 ./ ./GlobalProtect_deb-6.0.0.0-62.deb ./
GlobalProtect_deb_arm-6.0.0.0-62.deb ./
GlobalProtect_rpm-6.0.0.0-62.rpm ./
GlobalProtect_rpm_arm-6.0.0.0-62.rpm ./
GlobalProtect_tar-6.0.0.0-62.tgz ./
GlobalProtect_tar_arm-6.0.0.0-62.tgz ./
GlobalProtect_UI_deb-6.0.0.0-62.deb ./
GlobalProtect_UI_rpm-6.0.0.0-62.rpm /
GlobalProtect_UI_tar-6.0.0.0-62.tgz ./manifest ./relinfo ./
gp_install.sh ./gp_uninstall.sh
```

Verá varios paquetes de instalación para las versiones del sistema operativo compatibles: DEB para Debian y Ubuntu y RPM para CentOS y Red Hat. El paquete para la versión GUI se indica con un prefijo GlobalProtect_UI.

STEP 2 | (Opcional) Si su endpoint Linux debe utilizar una configuración manual del servidor proxy, configure la configuración de proxy.

La aplicación de GlobalProtect para Linux admite solo una configuración básica de servidor proxy, pero no admite el uso de archivos de configuración automática de proxy (PAC) y autenticación de proxy.

La aplicación de GlobalProtect para Linux obtiene la configuración del proxy a partir de las variables de entorno `HTTP_PROXY`, `HTTPS_PROXY` y `NO_PROXY` en el archivo `/etc/environment`. Si luego cambia la configuración proxy del sistema, compruebe que el terminal desde el que se ejecuta GlobalProtect utiliza las variables de entorno proxy. Si no ve los nuevos ajustes, cierre sesión y vuelva a iniciar sesión para que los nuevos ajustes surtan efecto.

Si ha configurado la variable HTTP_PROXY o la variable HTTPS_PROXY, asegúrese de que el portal de GlobalProtect coincida con los ajustes configurados para la variable NO_PROXY.

1. Para establecer su proxy en su endpoint Linux, edite la variable de entorno `HTTP_PROXY` o la variable de entorno `HTTPS_PROXY` (por ejemplo, `HTTPS_PROXY="HTTPS://yourproxy.local:8080"`).
2. Para configurar las direcciones IP o los nombres de dominio que desea excluir del proxy, edite la variable de entorno `NO_PROXY` (por ejemplo, `NO_PROXY="www.gpqa.com"`).

   Utilice comas para separar varias direcciones IP o nombres de dominio. A partir de la aplicación de GlobalProtect 5.1.6, puede utilizar el carácter comodín (*) para las direcciones IP o los nombres de dominio (por ejemplo, `NO_PROXY="*.domain.com"`).

STEP 3 | Instale la versión de interfaz gráfica de la aplicación de GlobalProtect para Linux.

Para instalar el paquete de distribución de IU de la aplicación de GlobalProtect, utilice el comando **`$ ./gp_install.sh`**:

```
$ ./gp_install.sh --help Usage: $ sudo ./gp_install [--cli-only |
 --arm | --help] --cli-only: CLI Only --arm: ARM no options: UI
```

Una vez finalizada la instalación, la aplicación de GlobalProtect se inicia automáticamente.

STEP 4 | Cierre sesión en el sistema operativo Linux o en la sesión SSH según el método de instalación utilizado y vuelva a iniciar sesión.

Este paso es necesario para garantizar que cualquier actualización de paquete nuevo durante la instalación se aplique a la aplicación de GlobalProtect.

STEP 5 | Especifique la dirección de su portal e introduzca sus credenciales cuando se le solicite que comience el proceso de conexión.

STEP 6 | (Opcional) Para importar un certificado, complete los siguientes pasos.

Cuando desee implementar previamente un certificado cliente en un endpoint para la autenticación basada en certificados, puede copiar el certificado en el endpoint e importarlo para su uso por la aplicación de GlobalProtect. Utilice el comando **`globalprotect import-`**

certificate --location <*location*> para importar el certificado en el endpoint. Cuando se le solicite, debe proporcionar la contraseña del certificado.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12 Please input passcode:
 Import certificate is successful.
```

Descargar e instalar la versión de CLI de GlobalProtect para Linux

Si su dispositivo Linux no admite una interfaz gráfica de usuario, instale la aplicación de GlobalProtect para Linux siguiendo estos pasos. La aplicación de GlobalProtect para Linux admite los paquetes de instalación DEB, RPM y TAR.

STEP 1 | Descargue la aplicación de GlobalProtect para Linux.

1. Obtenga el paquete de aplicaciones de su administrador de TI y, a continuación, copie el archivo TGZ en el endpoint Linux.

   Por ejemplo, si descargó el paquete en un endpoint macOS, puede abrir un terminal y, a continuación, copiar el archivo:

   ```
   macUser@mac:~$ scp ~/Downloads/PanGPLinux-6.0.0.tgz
    linuxUser@linuxHost: <DestinationFolder>
   ```

   donde ***<DestinationFolder>*** es una ubicación como `~/pkgs/` donde desea almacenar el archivo TGZ.

2. Desde el endpoint Linux, descomprima el paquete.

   ```
   user@linuxhost:~$ tar -xvf ~/pkgs/PanGPLinux-6.0.0.tgz
   ```

   Después de descomprimir el paquete, verá los paquetes de instalación (DEB para Ubuntu y RPM para CentOS y Red Hat) y los scripts para instalar y desinstalar los paquetes.

STEP 2 | (Opcional) Si su endpoint Linux debe utilizar una configuración manual del servidor proxy, configure la configuración de proxy.

La aplicación de GlobalProtect para Linux admite solo una configuración básica de servidor proxy, pero no admite el uso de archivos de configuración automática de proxy (PAC) y autenticación de proxy.

La aplicación de GlobalProtect para Linux obtiene la configuración del proxy a partir de las variables de entorno `HTTP_PROXY`, `HTTPS_PROXY` y `NO_PROXY` en el archivo `/etc/environment`. Si luego cambia la configuración proxy del sistema, compruebe que el terminal

desde el que se ejecuta GlobalProtect utiliza las variables de entorno proxy. Si no ve los nuevos ajustes, cierre sesión y vuelva a iniciar sesión para que los nuevos ajustes surtan efecto.

Si ha configurado la variable HTTP_PROXY o la variable HTTPS_PROXY, asegúrese de que el portal de GlobalProtect coincida con los ajustes configurados para la variable NO_PROXY.

1. Para establecer su proxy en su endpoint Linux, edite la variable de entorno HTTP_PROXY o la variable de entorno HTTPS_PROXY (por ejemplo, HTTPS_PROXY="HTTPS://yourproxy.local:8080").
2. Para configurar las direcciones IP o los nombres de dominio que desea excluir del proxy, edite la variable de entorno NO_PROXY (por ejemplo, NO_PROXY="www.gpqa.com").

   Utilice comas para separar varias direcciones IP o nombres de dominio. A partir de la aplicación de GlobalProtect 5.1.6, puede utilizar el carácter comodín (*) para las direcciones IP o los nombres de dominio (por ejemplo, NO_PROXY="*.domain.com").

STEP 3 | Instale el paquete de la aplicación usando el comando **CLI Only**:

```
$ ./gp_install.sh --help Usage: $ sudo ./gp_install [--cli-only |
 --arm | --help] --cli-only: CLI Only --arm: ARM no options: UI
```

STEP 4 | (Opcional) Cambiar los modos de la CLI.

Puede ejecutar comandos en línea de comandos o en modo de solicitud. El modo de línea de comandos requiere que especifique el comando GlobalProtect completo. El modo de solicitud requiere que especifique solo el comando (sin el nombre de la aplicación) y muestra una salida más detallada que el modo de línea de comandos.

1. Para cambiar al modo prompt, introduzca **globalprotect** sin ningún argumento.

   ```
   user@linuxhost:~$ globalprotect >>
   ```

2. Para salir del modo prompt, introduzca **quit**.

   ```
   >> quit user@linuxhost:~$
   ```

STEP 5 | Vea la ayuda para la aplicación de GlobalProtect para Linux.

Modo de prompt:

```
>> help Usage: only the following commands are supported: collect-
log -- collect log information connect -- connect to server
 disconnect -- disconnect disable -- disable connection import-
certificate -- import client certificate file quit -- quit from
 prompt mode rediscover-network -- network rediscovery remove-user
 -- clear credential resubmit-hip -- resubmit hip information set-
log -- set debug level show -- show information
```


Modo de línea de comandos:

```
user@linuxhost:~$ globalprotect help Usage: only the following
 commands are supported: collect-log -- collect log information
 connect -- connect to server disconnect -- disconnect disable --
 disable connection import-certificate -- import client certificate
 file quit -- quit from prompt mode rediscover-network -- network
 rediscovery remove-user -- clear credential resubmit-hip --
 resubmit hip information set-log -- set debug level show -- show
 information
```

STEP 6 | Utilice la versión de CLI de la aplicación de GlobalProtect para Linux.

Usar la aplicación de GlobalProtect para Linux

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints de Linux	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

GlobalProtect admite dos versiones de la aplicación de GlobalProtect para Linux: Una versión si su dispositivo Linux admite una interfaz gráfica de usuario y una versión CLI si su dispositivo Linux no admite una interfaz gráfica de usuario.

- Usar la versión de interfaz gráfica de la aplicación de GlobalProtect para Linux
- Utilice la versión de CLI de la aplicación de GlobalProtect para Linux

Usar la versión de interfaz gráfica de la aplicación de GlobalProtect para Linux

Para usar la versión de interfaz gráfica de la aplicación de GlobalProtect para Linux, complete estos pasos.

STEP 1 | En la ventana de GlobalProtect, introduzca el FQDN o dirección IP del portal de GlobalProtect, y luego haga clic en **Connect (Conectar)**.

Después de descargar e instalar la versión GUI de la aplicación de GlobalProtect para Linux, la aplicación de GlobalProtect se inicia automáticamente.

1. (Opcional) Si se guardan varios portales en su aplicación, seleccione un portal en el menú desplegable **Portal**. De manera predeterminada, el portal conectado más recientemente está preseleccionado del menú desplegable **Portal**.

2. Introduzca el **Username (Nombre de usuario)** y la **Password (Contraseña)** para el portal y haga clic en **Sign In (Iniciar sesión)**.

   En la mayoría de los casos, puede usar el mismo nombre de usuario y contraseña que usa para conectarte a su red corporativa. Después de iniciar sesión, el portal de GlobalProtect muestra el estado como **Connected (Conectado)**.

3. (Opcional) De manera predeterminada, usted se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles.

Para conectarse a una puerta de enlace diferente, haga clic en el menú desplegable de puerta de enlace y, a continuación, utilice una de las siguientes opciones:

- Seleccione una puerta de enlace manualmente (solo puertas de enlace externas).

  Esta opción solo está disponible si su administrador habilita la selección manual de la puerta de enlace.

- Asigne y conéctese automáticamente a una puerta de enlace preferida:

  1. En el menú de la parte superior derecha del panel de estado de la aplicación, seleccione **Preferred Gateway (Puerta de enlace preferida)** para abrir GlobalProtect: Cuadro de diálogo de Puerta de enlace preferida
  2. En la lista de puertas de enlace disponibles, seleccione la puerta de enlace que desea establecer como puerta de enlace preferida y, a continuación, seleccione **Set as Preferred (Establecer como preferida)**.
  3. Ahora debe **Close (Cerrar)** el diálogo.

  Si ya no desea conectarse a la puerta de enlace automáticamente, también puede eliminar la asignación de puerta de enlace preferida:

  1. En el menú de la parte superior derecha del panel de estado de la aplicación, seleccione **Preferred Gateway (Puerta de enlace preferida)** para abrir GlobalProtect: Cuadro de diálogo de Puerta de enlace preferida
  2. En la lista de puertas de enlace disponibles, seleccione la puerta de enlace preferida y, a continuación, seleccione **Remove Preferred (Eliminar preferida)**.
  3. Ahora debe **Close (Cerrar)** el diálogo.

STEP 2 | Abra la aplicación GlobalProtect.

Haga clic en el icono de la bandeja del sistema de GlobalProtect para iniciar la interfaz de la aplicación.

STEP 3 | Vea información sobre sus servicios de red.

Después de iniciar la aplicación, seleccione el menú ( ) en la parte superior derecha del panel de la aplicación, seleccione **Settings (Configuración)** para abrir el panel **Configuración**

de GlobalProtect y, a continuación, seleccione una de las pestañas siguientes para ver información sobre su conexión de red:

- **General**: muestra el nombre de usuario y los portales asociados a la cuenta de GlobalProtect. También puede añadir, eliminar o modificar los portales desde esta pestaña.

- **Connection (Conexión)**: muestra las puertas de enlace configuradas para la aplicación de GlobalProtect y brinda la siguiente información sobre cada puerta de enlace:
  - Gateway name (Nombre de la puerta de enlace)
  - Tunnel status (Estado del túnel)
  - Authentication status (Estado de autenticación)
  - Connection type (Tipo de conexión)
  - Gateway IP address or FQDN (Dirección IP o FQDN de la puerta de enlace) (solo disponible en el modo externo)

  *En el modo interno, la pestaña **Connection (Conexión)** muestra la lista completa de puertas de enlace disponibles. En el modo externo, la pestaña **Connection (Conexión)** muestra la puerta de enlace a la que se conecta y los detalles adicionales sobre la puerta de enlace (como la dirección IP, la ubicación y el tiempo activo de la puerta de enlace).*

- **Troubleshooting (Resolución de problemas)**: le permite **Collect Logs (Recopilar logs)** y establecer el **Logging Level (Nivel de registro)**.

  A fin de que la aplicación de GlobalProtect envíe logs de solución de problemas, logs de diagnóstico o ambos a Strata Logging Service para un mayor análisis, debe configurar el portal de GlobalProtect para habilitar la recopilación de logs de la aplicación de GlobalProtect para la solución de problemas. Además, puede configurar las URL de destino basadas en HTTPS que pueden contener direcciones IP o nombres de dominio completos de los servidores/recursos web que desea sondear y determinar ciertos problemas, como la latencia o el rendimiento de la red, en el endpoint del usuario final.

STEP 4 | (Opcional) Inicie sesión con una contraseña nueva.

*Si el administrador de GlobalProtect configura el agente del portal de GlobalProtect para **Save User Credentials (Guardar credenciales de usuario)**, las credenciales se guardarán automáticamente en la aplicación de GlobalProtect. Si su contraseña de acceso a la red corporativa cambia, debe iniciar sesión en GlobalProtect con su nueva contraseña.*

1. Haga clic en el icono de la bandeja del sistema para iniciar la aplicación de GlobalProtect. Se abre el panel de estado.
2. Seleccione el menú ( ) en la parte superior derecha del panel de la aplicación y, a continuación, seleccione **Settings (Configuración)** para abrir el panel **GlobalProtect Settings (Configuración de GlobalProtect)**.
3. En la pestaña **General** del panel **GlobalProtect Settings (Configuración de GlobalProtect)**, elija **Sign Out (Cerrar sesión)** para borrar las credenciales de usuario guardadas de la aplicación de GlobalProtect.
4. Después de borrar sus credenciales de usuario, puede volver a conectarse a GlobalProtect con su nuevo nombre de usuario y contraseña.

STEP 5 | (Opcional) Desconéctese de GlobalProtect.

Si su administrador configura GlobalProtect con el método de conexión **On-Demand (Bajo demanda)**, puede desconectarse de GlobalProtect haciendo clic en **Disconnect (Desconectar)** en el panel de estado.

Utilice la versión de CLI de la aplicación de GlobalProtect para Linux

Con la interfaz de línea de comandos (CLI) de la aplicación de GlobalProtect™ para Linux, puede realizar tareas comunes a la aplicación de GlobalProtect Los siguientes ejemplos muestran el resultado en modo de línea de comandos. Para ejecutar el mismo comando en modo prompt, introdúzcalo sin el prefijo **`globalprotect`** (para obtener más información, consulte Descargar e instalar la aplicación de GlobalProtect para Linux).

- Conectarse a un portal de GlobalProtect:

  Utilice el comando **`globalprotect connect --portal <gp-portal>`** donde ***<gp-portal>*** es la dirección IP o FQDN de su portal de GlobalProtect.

  Por ejemplo:

```
user@linuxhost:~$ globalprotect connect --portal
 myportal.example.com Retrieving configuration... Disconnected
 myportal.example.com - portal:local:Enter login credentials
 username:user1 Password: Retrieving configuration... Discovering
 network... Connecting... Connected
```

  Cuando utiliza la autenticación basada en certificados, la primera vez que se conecta sin un certificado CA raíz, la aplicación de GlobalProtect y el portal de GlobalProtect intercambian certificados. La aplicación de GlobalProtect muestra un error de certificado, que debe

reconocer antes de autenticar. Cuando se conecte a continuación, no se le solicitará el mensaje de error del certificado.

```
user@linuxhost:~$ globalprotect connect
 --portal myportal.example.com Retrieving
 configuration...
 Disconnected There is a problem with the security certificate,
 so the identity of 10.3.188.61 cannot be verified.
 Póngase en contacto con el servicio de asistencia para
 que su organización corrija el problema. Advertencia: The
 communication with 10.3.188.61 may have been compromised.
 We recommend that you do not continue with this connection.
 Error details:Do you want to continue(y/n)?y Retrieving
 configuration...
  Disconnected 10.3.188.61 - portal:local:Enter login
 credentials username:user1 Password: Retrieving
 configuration...
 Discovering network... Connecting... Connected
```

*También puede especificar un nombre de usuario en el comando utilizando la opción **--nombre de usuario <username>**. La aplicación de GlobalProtect le pide que se autentique y, si especificó la opción nombre de usuario, confirme su nombre de usuario.*

- Importar un certificado.

  Cuando desee implementar previamente un certificado cliente en un endpoint para la autenticación basada en certificados, puede copiar el certificado en el endpoint e importarlo para su uso por la aplicación de GlobalProtect. Utilice el comando **globalprotect import-certificate --location <location>** para importar el certificado en el endpoint. Cuando se le solicite, debe proporcionar la contraseña del certificado.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12 Please input passcode:
 Import certificate is successful.
```

- Conectarse a una puerta de enlace:
  1. (Opcional) Visualice las puertas de enlace manuales a las que puede conectarse mediante el comando **globalprotect show --manual-gateway**.
  2. Conectarse a una puerta de enlace mediante el comando **globalprotect connect --gateway <gp-gateway>** donde **<gp-gateway>** es la dirección IP o FQDN de la puerta de enlace de GlobalProtect.
  3. Vea detalles sobre su conexión usando el comando **globalprotect show --details**.

```
user@linuxhost:~$ globalprotect show --manual-gateway Name Address
 ------------------------------ gw1 192.168.1.180 gw2 192.168.1.181
 user@linuxhost:~$ globalprotect connect --gateway 192.168.1.180
```



```
 Retrieving configuration... Discovering network... Connecting...
 Connected
```

- Verificar el estado de su conexión GlobalProtect y ver los detalles sobre ella:

  Utilice el comando **globalprotect show --status** para verificar el estado de su conexión.

  Utilice el comando **globalprotect show --details** para ver los detalles de su conexión.

```
user@linuxhost:~$ globalprotect show --status GlobalProtect status:
 Connected user@linuxhost:~$ globalprotect show --details Assigned
 IP address: 192.168.1.132 Gateway IP address: 192.168.1.180
 Protocol: IPSec Uptime(sec): 231
```

- Volver a descubrir la red:

  Utilice el comando **globalprotect rediscover-network** para desconectarse y volver a conectarse de GlobalProtect.

```
user@linuxhost:~$ globalprotect rediscover-network Disconnecting...
 Retrieving configuration... Retrieving configuration...
 Discovering network... Connecting... Connecting... Connected
 GlobalProtect status: Connected
```

- Borrar las credenciales para el usuario actual:

  Utilice el comando **globalprotect remove-user** para borrar las credenciales utilizadas para autenticarse con el portal y las puertas de enlace. Después de confirmar que la aplicación de GlobalProtect debe eliminar sus credenciales, la aplicación de GlobalProtect desconecta el túnel y luego requiere que introduzca sus credenciales la próxima vez que se conecte.

```
user@linuxhost:~$ globalprotect remove-user Credential will be
 cleared and current tunnel will be terminated. Do you want to
 continue(y/n)?y Clear is done successfully. user@linuxhost:~
$ globalprotect connect --portal 192.168.1.179 Retrieving
 configuration... Disconnected 192.168.1.179 - portal:local:Enter
 login credentials username:user1 Password: Retrieving
 configuration... Discovering network... Connecting... Connected
```

- Volver a enviar la información del host a la puerta de enlace.

  Utilice el comando **globalprotect show --host-state** para ver la información actual del host sobre su endpoint. Utilice el comando **globalprotect resubmit-HIP** para volver a enviar información sobre el endpoint a la puerta de enlace. Esto es útil en los casos en que la política de seguridad basada en HIP impide que los usuarios accedan a los recursos porque

permite al usuario solucionar el problema de cumplimiento en el endpoint y, a continuación, volver a enviar el HIP.

```
user@linuxhost:~$ globalprotect show --host-state generate-time:
 09/28/2017 11:24:07 categories host-info client-version: 4.1.0
 os: Linux Ubuntu 16.04.3 LTS os-vendor: Linux domain: host-
name: linuxhost host-id: 4C4C4544-0034-4D10-804C-**********
 network-interface enp0s31f6 description: enp0s31f6 mac-address:
 D4:81:D7:D4:5A:A5 wlp2s0 description: wlp2s0 mac-address:
 14:AB:C5:DE:D1:0E user@linuxhost:~$ globalprotect resubmit-hip
 Resubmit is successful.
```

- Ver cualquier notificación de GlobalProtect.

  Utilice el comando **`globalprotect show --notification`** para ver las notificaciones.

- Ver el icono de bandeja del sistema GlobalProtect.

  Utilice el comando **`globalprotect launch-ui`** para mostrar el icono de la bandeja del sistema en su escritorio. Puede abrir la aplicación GlobalProtect haciendo clic en el icono de la bandeja del sistema.

- Ver la página de bienvenida.

  Utilice el comando **`globalprotect show --welcome-page`**. La aplicación de GlobalProtect muestra la página de bienvenida en un navegador si existe una página de bienvenida o muestra una notificación si la página de bienvenida no existe.

- Ver errores.

  Utilice el comando **`globalprotect show --error`** para ver los errores notificados por la aplicación.

```
user@linuxhost:~$ globalprotect show --error Error: Cannot connect
 to GlobalProtect Portal
```

- Recopilar logs.

  La aplicación almacena los archivos de logs PanGPA y PanGPI en el directorio `/home/<user>/.Globalprotect`. Utilice el comando **`globalProtect collect-logs`** para permitir que la aplicación de GlobalProtect para Linux empaquete estos logs y otra información útil. A continuación, puede utilizar los logs para solucionar problemas o reenviarlos a un ingeniero de soporte para un análisis experto.

```
user@linuxhost:~$ globalprotect collect-log Start collecting...
 collecting network info... collecting machine info... copying
 files... generating final result file... The support file is saved
 to /home/user/.GlobalProtect/Collect.tgz
```


- Muestra la versión de la aplicación de GlobalProtect para Linux.

```
user@linuxhost:~$ globalprotect show --version GlobalProtect:
 6.0.0-23 Copyright(c) 2009-2021 Palo Alto Networks, Inc.
```


Informar de un problema desde la aplicación de GlobalProtect para Linux

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints de Linux	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si experimenta un comportamiento inusual, como un rendimiento de red deficiente o si no se establece la conexión con el portal y la puerta de enlace, puede informar de la incidencia directamente a Strata Logging Service para que su administrador pueda acceder a ella Ya no es necesario recopilar y enviar manualmente los logs de aplicaciones de GlobalProtect por correo electrónico o almacenarlos en una unidad de nube.

Solo puede informar de un problema a su administrador utilizando la versión de interfaz gráfica de usuario de la aplicación de GlobalProtect para Linux.

*Para mostrar la opción **Report an Issue (Informar de un problema)** en la aplicación de GlobalProtect, su administrador debe habilitar la recopilación de logs de la aplicación de GlobalProtect para la resolución de problemas en el portal de GlobalProtect.*

STEP 1 | Conéctese a la puerta de enlace o portal de GlobalProtect.

1. En la ventana de GlobalProtect, introduzca el FQDN o la dirección IP del portal de GlobalProtect y, a continuación, haga clic en **Connect (Conectar)**.

   Después de descargar e instalar la versión GUI de la aplicación de GlobalProtect para Linux, la aplicación de GlobalProtect se inicia automáticamente.
2. (Opcional) Si se guardan varios portales en su aplicación, seleccione un portal en el menú desplegable **Portal** desplegable. De manera predeterminada, el portal conectado más recientemente está preseleccionado del menú desplegable **Portal**.
3. Introduzca el **Username (Nombre de usuario)** y la **Password (Contraseña)** para el portal y haga clic en **Sign In (Iniciar sesión)**.

   En la mayoría de los casos, puede usar el mismo nombre de usuario y contraseña que usa para conectarte a su red corporativa. Después de iniciar sesión, el portal de GlobalProtect muestra el estado como **Connected (Conectado)**.
4. (Opcional) De manera predeterminada, usted se conecta automáticamente a la puerta de enlace **Best Available (Mejor disponible)**, en función de la configuración que el administrador define y los tiempos de respuesta de las puertas de enlace disponibles. Para conectarse a una puerta de enlace diferente, haga clic en el menú desplegable del gateway.

STEP 2 | Abra la aplicación GlobalProtect.

Haga clic en el icono de la bandeja del sistema de GlobalProtect para iniciar la interfaz de la aplicación.

STEP 3 | Informe de un problema desde la aplicación de GlobalProtect desde su endpoint.

Después de iniciar la aplicación, seleccione el menú ( ) en la parte superior derecha del panel de la aplicación para informar de un problema a su administrador.

1. Seleccione **Report an Issue (Informar de un problema)**.

2. Habilite la aplicación de GlobalProtect para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico. Los logs de diagnóstico y resolución de problemas se recopilan y envían a Strata Logging Service como un informe de resolución de problemas compacto.

   Después de que las pruebas de diagnóstico se completen correctamente, los archivos de log de depuración de GlobalProtect se cargan en Strata Logging Service desde su endpoint.

   Si no habilita la aplicación para ejecutar pruebas de diagnóstico e incluir logs de diagnóstico, solo se recopilan logs de resolución de problemas y se envían a Strata Logging Service como un informe de resolución de problemas compacto. La aplicación de GlobalProtect comprueba los archivos de informe (pan_gp.trb.log o pan_gp_trbl.log) que se generan automáticamente en formato `.json`*. Aparece un mensaje de notificación si no se encontraron problemas en los logs de resolución de problemas. Haga clic en* ***Retry (Reintentar)*** *para verificar si existen los archivos pan_gp.trb*.log.*

3. Seleccione la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**
4. Haga clic en **Continue (Continuar)** para permitir que la aplicación cree un registro de resolución de problemas y envíe el informe a la instancia de Strata Logging Service de su administrador.

   Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging Service de su administrador junto con los archivos pan_gp.trb*.log.

   Los resultados de las pruebas de diagnóstico de extremo a extremo se almacenan en el archivo pan_gp_diag.log en formato `.json` y se envían a la instancia de Strata Logging Service de su administrador junto con los archivos pan_gp.trb*.log. La aplicación de GlobalProtect puede ejecutar pruebas de diagnóstico con túnel o sin túnel. Por ejemplo,

es posible que desee introducir sus credenciales de inicio de sesión de GlobalProtect antes de que la aplicación conecte y ejecute pruebas de diagnóstico a través del túnel.

Aparecerá un mensaje que confirma que la aplicación está ejecutando pruebas de diagnóstico solo si ha seleccionado la casilla de verificación **Run Diagnostic Tests and Include Diagnostic Logs (Ejecutar siempre las pruebas de diagnóstico e incluir los logs)**.

Aparece un mensaje que confirma que la aplicación está enviando el informe a Strata Logging Service.

5. Haga clic en **Close (Cerrar)** para confirmar que la aplicación envió correctamente el informe a Strata Logging Service. Este mensaje de confirmación muestra la fecha y hora en que se procesó y envió el informe.

Desconectar la aplicación de GlobalProtect para Linux

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints de Linux	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Si el administrador configura el método de conexión de GlobalProtect como **Always On (Siempre activado)**, puede desconectar la aplicación de GlobalProtect. Por ejemplo, es posible que desee desconectar la aplicación si la red privada virtual (VPN) de GlobalProtect no funciona en un hotel y el fallo de la VPN le impide conectarse a Internet. Después de desconectar la aplicación de GlobalProtect, puede conectarse a Internet mediante una comunicación no segura (sin VPN).

El método, el tiempo y el número de veces que puede desconectar la aplicación de GlobalProtect depende de cómo configure el administrador su servicio de GlobalProtect. Esta configuración puede evitar que desconecte la aplicación completamente o Permitirle desconectar la aplicación solo después de responder correctamente a una pregunta.

Si su configuración incluye una pregunta (desafío), la aplicación de GlobalProtect solicita una de las siguientes opciones:

- Motivo por el que desea desconectar la aplicación
- Código de acceso

Si la pregunta implica un código de acceso, le recomendamos que se ponga en contacto con un administrador de GlobalProtect o con una persona del servicio de asistencia por teléfono. Los administradores suelen proporcionar contraseñas por adelantado, ya sea por correo electrónico (para los nuevos usuarios de GlobalProtect) o publicadas en el sitio web de su organización. En respuesta a un corte o problema del sistema, los administradores también pueden proporcionar códigos de acceso por teléfono.

GlobalProtect admite dos versiones de la aplicación de GlobalProtect para Linux: Una versión si su dispositivo Linux admite una interfaz gráfica de usuario y una versión CLI si su dispositivo Linux no admite una interfaz gráfica de usuario.

- Desconectar la aplicación de GlobalProtect para Linux mediante la versión de la interfaz gráfica de usuario
- Desconectar la aplicación de GlobalProtect para Linux mediante la versión CLI

Desconectar la aplicación de GlobalProtect para Linux mediante la versión de la interfaz gráfica de usuario

(Disponible solo en modo siempre activado) Para desconectar la aplicación de GlobalProtect para Linux utilizando la versión de interfaz gráfica de usuario, complete estos pasos.

STEP 1 | Desconecte la aplicación de GlobalProtect.

1. Inicie la aplicación de GlobalProtect haciendo clic en el icono de la bandeja del sistema de GlobalProtect. Se abre el panel de estado.
2. Seleccione el menú ( ) en la parte superior derecha del panel de la aplicación para abrir el menú de configuración.
3. Seleccione **Disconnect (Desconectar)**.

   *La opción **Disconnect (Desconectar)** solo es visible si la configuración del agente de GlobalProtect le permite desconectar la aplicación. Si la configuración le permite desconectar la aplicación de GlobalProtect sin que tenga que responder a una pregunta (desafío), la aplicación de GlobalProtect se cierra sin que sea necesario realizar ninguna otra acción.*

STEP 2 | Responder a una o más preguntas, si es necesario.

Si se le solicita, proporcione la siguiente información:

- **Reason (Motivo)**: su motivo para desconectar la aplicación de GlobalProtect.
- **Passcode (Contraseña)**: código de acceso que suele proporcionar el administrador con antelación, en función de un problema o evento conocido que requiere que desconecte la aplicación.

Desconectar la aplicación de GlobalProtect para Linux mediante la versión CLI

Para desconectar la aplicación de GlobalProtect para Linux mediante la versión CLI, complete estos pasos.

- (Disponible solo en modo a petición) Desconectarse de GlobalProtect:

  Utilice el comando **`globalprotect disconnect`** para desconectarse de GlobalProtect.

```
user@linuxhost:~$ globalprotect disconnect GlobalProtect status:
 Desconectado
```


- (Disponible solo en modo siempre activado) Desconectar GlobalProtect:

  Utilice el comando **`globalprotect disconnect`** para desconectar y deshabilitar la aplicación de GlobalProtect. Si su configuración lo requiere, también debe especificar un motivo o un código de acceso cuando se le solicite.

  ```
  user@linuxhost:~$ globalprotect disconnect
  ```

  ```
  user@linuxhost:~$ globalprotect disconnect Please enter reason for
   disconnecting: This is my reason for disconnecting
  ```

  ```
  user@linuxhost:~$ globalprotect disconnect Please enter passcode
   for disconnecting: ITp@ssw0rd
  ```


Desinstalar la aplicación de GlobalProtect para Linux

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo endpoints de Linux	❑ Versión 6.3 o posterior de la aplicación de GlobalProtect.

Puede desinstalar la aplicación de GlobalProtect para Linux mediante el siguiente comando:

```
$ ./gp_uninstall.sh --help Usage: $ sudo ./gp_uninstall [--cli-only |
 --arm | --help] --cli-only: CLI Only --arm: ARM no options: UI
```


GlobalProtect para dispositivos IoT

¿Dónde puedo usar esto?	¿Qué necesito?
• Solo dispositivos IoT	☐ Versión 6.1 o posterior de la aplicación GlobalProtect.

GlobalProtect™ es una aplicación que se ejecuta en su endpoint (ordenador de escritorio, portátil o servidor, o dispositivo IoT) para protegerlo mediante el uso de las mismas políticas de seguridad que protegen los recursos sensibles de su red corporativa. Para los dispositivos IoT, GlobalProtect™ asegura el tráfico hacia y desde el dispositivo a cualquier origen o destino en cualquier lugar de Internet o dentro de su red corporativa.

Puede instalar GlobalProtect en dispositivos IoT integrados en los siguientes sistemas operativos:

- IoT en Android
- IoT en Raspbian
- IoT en Ubuntu
- IoT en Windows:

