paloalto TECHDOCS

Prisma Access Browser Activación e incorporación

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

July 15, 2024

Table of Contents

Activar el nuevo Prisma Access Browser con el paquete de licencia de Prisma Access Enterprise

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager • Panorama	• Enlace de activación para su producto • Strata Logging Service (SLS) es necesario para la activación • Cloud Identity Engine (CIE) está incluida y se gestiona durante la activación • Cuenta del Portal de atención al cliente

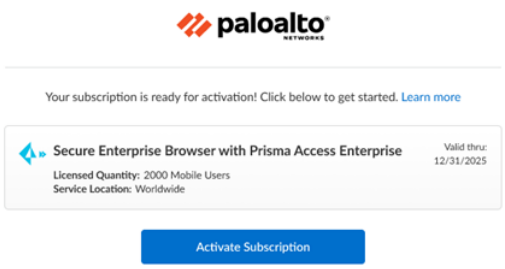
Consulte los requisitos previos antes de comenzar esta tarea.

- Nube
- Panorama

Licencia de paquete de Prisma Access Browser gestionado en la nube

Después de recibir un correo electrónico de Palo Alto Networks que identifique la licencia que está activando, utilice el enlace de activación para comenzar el proceso de activación.

STEP 1 | Seleccione **Activate Subscription (Activar suscripción)** en su correo electrónico.



STEP 2 | Siga las instrucciones para activar una licencia de Prisma Access, asignar una licencia de Prisma Access y planificar conexiones de servicio.

STEP 3 | Continúe a Asignar licencias de Prisma Access Secure Enterprise Browser y complementos. Los **Products (Productos)** o **Add-ons (Complementos)** están habilitados de forma predeterminada según su contrato.

STEP 4 | Seleccione el **Navegador de empresa seguro con Prisma Access Enterprise**.

Esto es similar a asignar licencias de PA para usuarios móviles. Podrá asignar y activar parcialmente licencias de Prisma Access Browser en varios inquilinos de Prisma Access. Por ejemplo:

- Puede comprar 5.000 unidades de Prisma Access Browser Enterprise para usuarios móviles.
- Puede asignar:
  - 1,000 a un inquilino de PoC (esta es la cantidad mínima requerida)
  - 3.000 a un inquilino de producción
  - Dejar 1.000 unidades sin activar para su uso posterior

STEP 5 | Vaya a la Guía de administración de Prisma Access Browser para gestionar su Prisma Access Browser.

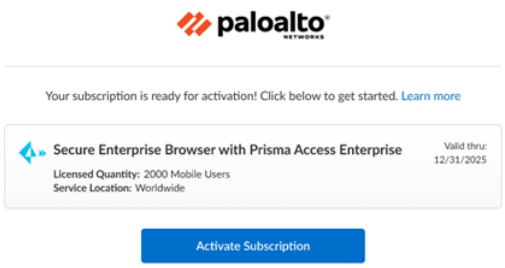
STEP 6 | (Opcional) Asigne roles para que sus administradores puedan gestionar Prisma Access Browser.

Paquete de licencias de Prisma Access Browser gestionado por Panorama

Después de recibir un correo electrónico de Palo Alto Networks que identifique la licencia que está activando, utilice el enlace de activación para comenzar el proceso de activación.

No disponible para Panorama de varios inquilinos.

STEP 1 | Seleccione **Activate Subscription (Activar suscripción)** en su correo electrónico.



STEP 2 | Siga las instrucciones para activar una licencia de Prisma Access (gestionada por Panorama).

STEP 3 | Continúe habilitando los complementos disponibles. Los **Products (Productos)** o **Add-ons (Complementos)** están habilitados de forma predeterminada según su contrato.

STEP 4 | Seleccione la opción **Secure Enterprise Browser with Prisma Access Enterprise (Navegador de empresa seguro con Prisma Access Enterprise**.

STEP 5 | En Panorama, vaya a la **pestaña de Prisma Access Browser** en**Panorama tab (Pestaña Panorama)** > **Cloud Services Plugin (Complemento de servicios en la nube)**.

Esto inicia una nueva pestaña con una versión reducida de Strata Cloud Manager que tiene solo la vistas específicas de Prisma Access Browser.

STEP 6 | Vaya a la Guía de administración de Prisma Access Browser para gestionar su Prisma Access Browser.

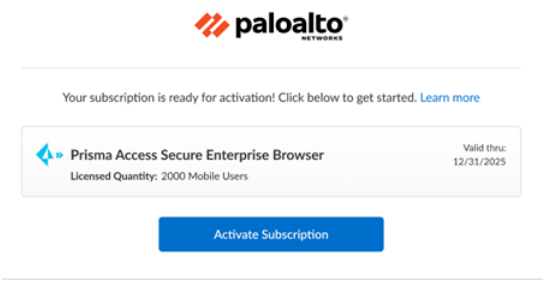
STEP 7 | (Opcional) Asigne roles para que sus administradores puedan gestionar Prisma Access Browser.

Activar licencia de Prisma Access Browser independiente

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	• Enlace de activación para su producto • Cloud Identity Engine (CIE) está incluida y se gestiona durante la activación • Cuenta del Portal de atención al cliente

Consulte los requisitos previos *antes de comenzar esta tarea.*

Después de recibir un correo electrónico de Palo Alto Networks que identifique la licencia que está activando, utilice el enlace de activación para comenzar el proceso de activación.



STEP 1 | Inicie sesión con su dirección de correo electrónico.

- Si tiene una cuenta de Atención al cliente de Palo Alto Networks, introduzca la dirección de correo electrónico que utilizó cuando se registró para esa cuenta y seleccione **Next (Siguiente)**.
- Si no tiene una cuenta de Atención al cliente de Palo Alto Networks, entonces deberá **Create a New Account (Crear una nueva cuenta)** > **Password (Contraseña)** > **Next (Siguiente)**.

El servicio utiliza esta dirección de correo electrónico para la cuenta de usuario asignada al inquilino que utiliza para esta licencia. Este inquilino, y cualquier otro creado por esta dirección de correo electrónico, tendrá el rol de `Superusuario`.

STEP 2 | Si solo tiene una cuenta del Portal de atención al cliente asociada con su nombre de usuario, la **Customer Support Account (Cuenta de atención al cliente)** se completa previamente.

Si tiene más de una cuenta del Portal de atención al cliente, entonces se puede esperar otros comportamientos.

STEP 3 | Asigne el producto al **Recipient (Destinatario)** de su elección.

El nombre proporcionado coincide con su cuenta del Portal de atención al cliente para mayor comodidad. Puede usar el nombre proporcionado o cambiarlo.

STEP 4 | Elija la **Region (Región)** de ingestión de datos donde desea implementar su producto.

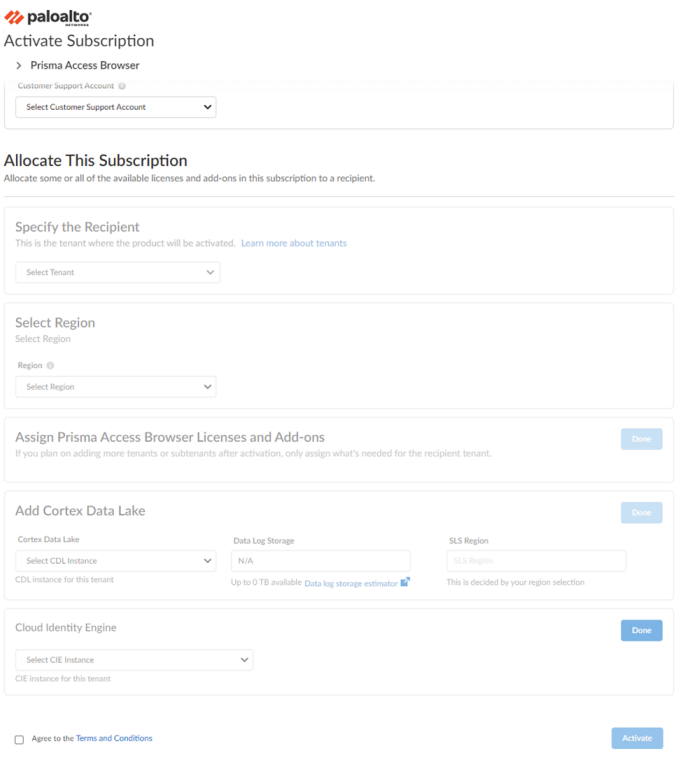
STEP 5 | Asigne las licencias y complementos de Prisma Access Secure Enterprise Browser

1. Seleccione **Prisma Access Secure Enterprise Browser**:
2. Esto es similar a asignar licencias de PA para usuarios móviles. Podrá asignar y activar parcialmente licencias de Prisma Access Browser en varios inquilinos de Prisma Access. Por ejemplo:
   - Puede comprar 1.000 unidades de Prisma Access Browser independiente
   - Puede asignar:
     - 200 a un inquilino de PoC (esta es la cantidad mínima requerida)
     - 600 a un inquilino de producción
     - Dejar 200 unidades sin activar para su uso posterior

STEP 6 | Añada Strata Logging Service (anteriormente conocido como Cortex Data Lake) para almacenar datos de inquilinos, como configuración, logs de telemetría, logs del sistema y estadísticas. Puede seleccionar una instancia existente o crear una nueva instancia.

STEP 7 | Seleccione Cloud Identity Engine o cree una nueva instancia de CIE para identificar y verificar a todos los usuarios de su infraestructura.

STEP 8 | Deberá **Agree to the terms and conditions (Aceptar las condiciones)** y **Activate (Activar)**.



STEP 9 | Vaya a la Guía de administración de Prisma Access Browser para gestionar su Prisma Access Browser.

STEP 10 | (Opcional) Asigne roles para que sus administradores puedan gestionar Prisma Access Browser.

Incorpore Prisma Access Browser en Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	❑ Licencia de paquete de Prisma Access con Prisma Access Browser ❑ Superusuario o rol de Prisma Access Browser

Consulte los requisitos previos antes de comenzar esta tarea.

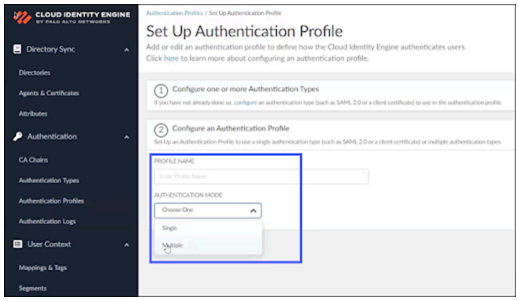
Completar las tareas previas a la incorporación

Antes de incorporar Prisma Access Browser, hay un par de tareas que debe realizar antes de poder continuar.

STEP 1 | Defina las entidades de Cloud Identity Engine. Esto se puede configurar utilizando el Cloud Identity Engine que seleccionó durante el proceso de activación.

STEP 2 | Necesita el perfil de autenticación y los grupos de usuarios que forman parte de su proceso de incorporación. Estos se configuran en Cloud Identity Engine. Para obtener más información, consulte Perfil de autenticación y Grupos de usuarios.

*Solo puede tener un perfil de autenticación. Si utiliza más de un proveedor de identidad (IdP), puede configurar varios IdP por perfil. Esto se puede hacer si en **Authentication Mode (Modo de autenticación)** selecciona **Multiple (Múltiples)** cuando configura el Perfil de autenticación.*

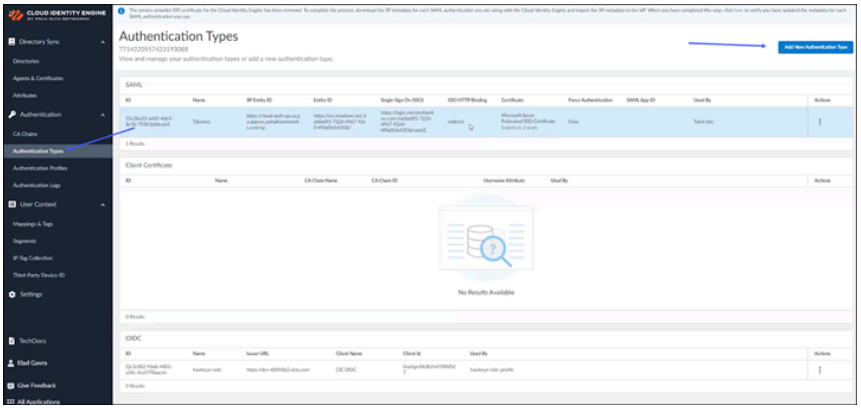


Añadir configuración de IdP

Puede utilizar su proveedor de IdP SAML actual para gestionar un único conjunto de credenciales de inicio de sesión en su red. La configuración de IdP es un componente de Cloud Identity Engine y puede gestionarlo dentro de esa herramienta.

STEP 1 | En Cloud Identity Engine, seleccione **Authentication Type (Tipo de autenticación)**.

STEP 2 | Haga clic en **Add New Authentication Type (Añadir nuevo tipo de autenticación)**.



Cuando utiliza la información del proveedor de IdP para completar sus grupos de usuarios, debe asegurarse de introducir correctamente una dirección de correo electrónico válida. La UPN no es suficiente.

STEP 3 | En Configurar tipo de autenticación, haga clic en **Setup (Configurar)**SAML 2.0.

STEP 4 | Para continuar configurando su autenticador SAML, consulte Configurar un tipo de autenticación SAML 2.0 en Cloud Identity Engine.

STEP 5 | (Opcional) Utilice la integración de Google Workspace.

Incorporar Prisma Access Browser

Después de realizar los pasos previos a la incorporación, puede incorporar Prisma Access Browser en Strata Cloud Manager.

Necesita activar y configurar Prisma Access Browser en Strata Cloud Manager antes de poder añadir usuarios. En general, este es un procedimiento único que solo necesita realizar una vez después de la activación, sin embargo, puede volver a realizar estas tareas en cualquier momento que necesite modificarlas.

Hay un asistente que puede utilizar para este proceso y puede modificar la configuración global en cualquier momento. El asistente proporciona instrucciones detalladas sobre cómo completar cada paso de la integración.

Los controles que vea dependerá de su licencia de Prisma Access Browser; no toda la funcionalidad de incorporación en Strata Cloud Manager está disponible para todas las licencias.

Desde Strata Cloud Manager, seleccione **Workflows (Flujos de trabajo)** > **Setup (Configuración de) Prisma Access** > **Prisma Access Browser.**

Paso 1 - Usuarios

Defina el método de autenticación de usuarios y los grupos de usuarios incorporados.

STEP 1 | En la lista desplegable, seleccione el **CIE profile that will be used for User Authentication (Perfil CIE que se utilizará para la autenticación del usuario)**.

STEP 2 | En la lista desplegable Grupos de usuarios, seleccione los **User groups (Grupos de usuarios)** que podrán acceder a Prisma Access Browser.

STEP 3 | **Next (Siguiente): Integration (Integración de) Prisma Access**.

Paso 2 - Integración de Prisma Access

STEP 1 | Habilite la conectividad externa a Prisma Access.

1. Seleccione **Go to Explicit Proxy settings (Ir a la configuración de proxy explícito)**.
2. Esto le lleva a **Workflows (Flujos de trabajo)** > **Setup (Configuración de)Prisma Access** > **Explicit Proxy (Proxy explícito)** .
3. Habilitar Prisma Access Browser.
4. **Done (Hecho)**.

STEP 2 | Permitir Prisma Access Browser en la Política de seguridad de Prisma Access.

1. Seleccione **Manage (Gestionar > Prisma Access > Security policy (Política de seguridad)**.
2. Esto le lleva a **Manage (Gestionar)** > **Prisma Access** > **Security policy (Política de seguridad).**
3. Añada una regla que permita el tráfico web en su política de seguridad.
4. Envíe la configuración para aceptar la regla.
5. **Done (Hecho)**.

STEP 3 | Crear una conexión de servicio.

1. Seleccione **Create a service connection (Crear una conexión de servicio)**.
2. Esto te lleva a **Workflows (Flujos de trabajo)** > **Setup (Configuración de) Prisma Access** > **Service Connections (Conexiones de servicio)** y **Add Service Connection (Añadir conexión de servicio)**.
3. **Done (Hecho)**.
4. **Siguiente: Enrutamiento.**

Paso 3 - Enrutamiento

El control de enrutamiento le permite gestionar la forma en que Prisma Access Browser gestiona el tráfico de la red. Este rol establece la configuración predeterminada para Prisma Access Browser. Si necesita ajustar la granularidad del control para una regla específica, consulte Controles de personalización del navegador para flujos de tráfico .

STEP 1 | Elija una de las siguientes opciones:

- **Only route private application traffic through Prisma Access (Enrutar únicamente el tráfico de aplicaciones privadas a través de Prisma Access)**.
- **Route all traffic through (Enrutar todo el tráfico a través de) Prisma Access**.

STEP 2 | (Opcional) Asegúrese de que el tráfico de Prisma Access Browser fluye de manera óptima cuando el navegador detecta que se está ejecutando dentro de la red interna. Esta identificación se basa en establecer una conexión con un host que sólo está disponible dentro de la red interna.

- Introduzca el FQDN a resolver.
- Introduzca la dirección IP prevista.

STEP 3 | **Next (Siguiente): Enforce SSO applications (Aplicar aplicaciones SSO)**.

Paso 4: Aplicar aplicaciones SSO

Es importante que la única forma en que sus usuarios puedan autenticarse en aplicaciones habilitadas para SSO sea mediante el uso de Prisma Access Browser. Esto garantizará que los actores externos no tengan acceso a sus aplicaciones empresariales. Para seleccionar su IdP:

STEP 1 | En Elegir y configurar sus proveedores de identidad, seleccione el IdP disponible. Las opciones son las siguientes:

- Okta
- Directorio activo de Microsoft Azure
- PingID
- OneLogin
- Acceso a VMware Workspace ONE

STEP 2 | Al configurar sus ajustes locales, asegúrese de tomar nota de las direcciones IP de salida.

STEP 3 | **Siguiente: Descargar y distribuir.**

Paso 5 - Descargar y distribuir

Puedes descargar los archivos de instalación de Prisma Access Browser para probarlos en su propio dispositivo antes de enviarlos a sus usuarios. Una vez que esté satisfecho con sus pruebas, puede descargar el instalador correspondiente para que lo distribuya su aplicación de gestión de dispositivos móviles (MDM).

También puede enviar a sus usuarios el enlace de descarga para que puedan descargar el Prisma Access Browser por su cuenta. Este es un enlace único solo para usuarios de macOS y Windows.

STEP 1 | Seleccione una de las opciones disponibles:

- Escritorio:
  - macOS
  - Windows
- Móvil:
  - iOS
  - Android

También puede enviar a sus usuarios el enlace de descarga para que puedan descargar el Prisma Access Browser por su cuenta. Este es un enlace único solo para usuarios de macOS y Windows.

Si envía a sus usuarios el enlace de descarga, recuérdeles que solo pueden iniciar sesión con el correo electrónico configurado en el servicio IdP.

STEP 2 | **Next (Siguiente): Browser Policy (Política del navegador)**.

Paso 6 - Política del navegador

Ahora puede comenzar a explorar y configurar el Motor de políticas de Prisma Access Browser para crear un entorno de usuario seguro y protegido.

STEP 1 | Seleccione **Browser Policy (Política del navegador)**.

STEP 2 | Esto le lleva a **Manage (Gestionar)** > **Configuration (Configuración)** > **Rules (Reglas)** > **Policy (Política)** > **Browser (Navegador de) Prisma Access**.

STEP 3 | Gestionar las Reglas de la política de Prisma Access Browser.

Incorporar nuevos usuarios

El flujo de trabajo de incorporación es una serie configurable de ventanas que se muestran cuando un nuevo usuario final comienza a utilizar el navegador.

En función de las necesidades y requisitos de TI, puede seleccionar hasta ocho páginas individuales que permiten a los usuarios finales personalizar el navegador con sus imágenes y marcadores, y obtener información básica sobre el navegador: una especie de guía de "inicio rápido".

El control de personalización del Asistente de incorporación configura el flujo de trabajo de incorporación. Puede seleccionar qué ventanas se mostrarán en su red.

Esto se configura en **Manage (Gestionar)** > **Configuration (Configuración)** > **Browser (Navegador de) Prisma Access** > **Policy (Política)** > **Profiles (Perfiles)** cuando crea o modifica un perfil de **Browser Customization (Personalización del navegador)** y selecciona **Onboarding Wizard (Asistente de incorporación)**. Para obtener detalles de configuración, consulte Controles de personalización del navegador para el Asistente de incorporación.

Asignar roles de Prisma Access Browser

¿Dónde puedo usar esto?	¿Qué necesito?
• Strata Cloud Manager	❑ Prisma Access con licencia de paquete de Prisma Access Browser o licencia independiente de Prisma Access Browser ❑ Rol: Superusuario Multiinquilino o Superusuario con acceso al Portal de atención al cliente

Puede crear y gestionar el control de acceso basado en roles para diferentes tipos de administradores de Prisma Access Browser. Esto permite al administrador principal de una organización grande designar administradores adicionales con permisos relevantes para sus funciones específicas, incluida la visibilidad y el acceso.

Después de activar su licencia, puede gestionar el acceso de los usuarios administradores y asignar uno de los siguientes roles específicos para Prisma Access Browser:

Funciones de empresa	Permisos	Aplicaciones compatibles
Acceso al navegador de PA y administrador de datos	Acceso de lectura y escritura para establecer y administrar políticas de acceso y datos, definir aplicaciones personalizadas o privadas, gestionar solicitudes de los usuarios finales relacionadas con las políticas y el permiso de solo lectura para aspectos relacionados con el inventario (usuarios, dispositivos, extensiones), y para cualquier aspecto de visibilidad (paneles, eventos de usuario final) dentro de las secciones de gestión de Prisma Access Browser	• Prisma Access Browser
Administrador de personalización de navegador de PA	Acceso de lectura y escritura para establecer y gestionar políticas de personalización del navegador. Permiso de solo lectura para los aspectos de inventario (usuarios, dispositivos, aplicaciones, extensiones) y para cualquier aspecto de visibilidad (paneles, eventos de usuario final) dentro de las secciones de gestión de Prisma Access Browser.	• Prisma Access Browser
Administrador de solicitud de	Acceso de lectura y escritura para gestionar las solicitudes de los usuarios finales relacionadas con las políticas y permisos de solo lectura para los aspectos de visibilidad (paneles, eventos de usuario final)	• Prisma Access Browser

Funciones de empresa	Permisos	Aplicaciones compatibles
permisos de PA Browser	dentro de las secciones de gestión de Prisma Access Browser.	
Administrador de PA Browser	Acceso de lectura y escritura para establecer y gestionar políticas de seguridad del navegador, y permiso de solo lectura para los aspectos relacionados con el inventario (usuarios, dispositivos, aplicaciones, extensiones), y para cualquier aspecto de visibilidad (paneles, eventos de usuario final) dentro de las secciones de gestión de Prisma Access Browser.	• Prisma Access Browser
Administrador del dispositivo y de la postura de seguridad de PA Browser	Acceso de lectura y escritura para establecer y gestionar políticas de seguridad del navegador, gestionar grupos de postura de dispositivos y establecer reglas de inicio de sesión. También proporciona permiso de solo lectura para inventariar aspectos como usuarios, aplicaciones, extensiones; y cualquier aspecto de visibilidad (paneles, eventos de usuario final) dentro de las secciones de gestión del Prisma Access Browser.	• Prisma Access Browser
Análisis de Ver solo del PA Browser	Acceso de lectura a cualquier aspecto de visibilidad dentro de las secciones de gestión de Prisma Access Browser, incluidos los paneles, los eventos detallados del usuario final y los aspectos relacionados con el inventario (usuarios, dispositivos, aplicaciones y extensiones).	• Prisma Access Browser

