

The Palo Alto Networks logo, featuring a stylized orange and red icon to the left of the word "paloalto" in a lowercase, sans-serif font.

TECHDOCS

Activación e incorporación de Strata Cloud Manager

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2024-2026 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

April 17, 2026

Table of Contents

Active sus licencias de Strata Cloud Manager.....	5
Activar Strata Cloud Manager Essentials.....	6
Activa Strata Cloud Manager Pro.....	9
Migrar de Panorama a Strata Cloud Manager.....	21
Cómo cambia la configuración de la gestión cuando pasa de Panorama a Strata Cloud Manager.....	22
Preparar la migración de sus cortafuegos NGFW a Strata Cloud Manager.....	23
Migrar sus NGFW gestionados por Panorama a Strata Cloud Manager.....	24
Prepárese para migrar a Prisma Access (Managed by Strata Cloud Manager).....	35
Migra su implementación de Prisma Access (Managed by Panorama) a Strata Cloud Manager.....	36
Asociaciones de Dispositivos en Strata Cloud Manager.....	47
Compatibilidad de modelos de dispositivos.....	52
Compatibilidad entre tipos de cortafuegos y licencias.....	57

Active sus licencias de Strata Cloud Manager

Para empezar a usar Strata Cloud Manager, debe activar el nivel de licencia adecuado: Essentials o Pro.

- [Activar Strata Cloud Manager Essentials](#): El nivel gratuito que ofrece gestión de configuración, gestión del ciclo de vida de seguridad de red y también puede proporcionar visibilidad si tiene una licencia de pago de [Strata Logging Service](#).
- [Activa Strata Cloud Manager Pro](#): Este nivel proporciona funciones avanzadas más todas las funciones de Strata Cloud Manager Essentials. Cuando activa Strata Cloud Manager Pro, también incluye acceso a Strata Logging Service, que incluye un año de retención de logs y almacenamiento ilimitado.



Si estaba utilizando Strata Cloud Manager antes de la introducción de estos nuevos niveles de licencia, sus licencias existentes para Prisma Access y AIOps para NGFW Premium siguen siendo compatibles. Puede continuar modificando, ampliando o renovando estas licencias. Además, si está utilizando AIOps para NGFW Free, tiene la opción de actualizar a AIOps para NGFW Premium.

- [Activación de AIOps para NGFW Premium](#)
- [Activar ELA para AIOps para NGFW Premium](#)
- [Activar un contrato de licencia de créditos de Software NGFW](#)
- [Activar su licencia de Prisma Access](#)
- [Licencia ADEM](#)

Activar Strata Cloud Manager Essentials

Strata Cloud Manager Essentials es el nivel gratuito que ofrece configuración y funciones de gestión del ciclo de vida de la seguridad de la red para agilizar las operaciones y proporcionar seguridad básica. Para obtener más información sobre la compatibilidad con modelos de dispositivos, consulte [Compatibilidad con modelos de dispositivos](#).

Puede [activar VM-Series financiados mediante créditos de Software NGFW](#) utilizando el nivel de licencia Strata Cloud Manager Essentials. Si no selecciona una [suscripción en la nube en el perfil de implementación](#), Strata Cloud Manager Essentials se activa automáticamente.

STEP 1 | Inicie sesión en el [hub](#).

STEP 2 | Vaya a la URL de activación de Strata Cloud Manager Essentials: <https://apps.paloaltonetworks.com/activation/scm-essentials>.

STEP 3 | Seleccione la cuenta de servicio de atención al cliente.

STEP 4 | Deberá **Create New (Crear nuevo) inquilino** donde activará Strata Cloud Manager.

STEP 5 | Seleccione una **Region (Región)** donde desee implementar Strata Cloud Manager. Consulte las [Regiones compatibles para Strata Cloud Manager](#).

La compatibilidad de la región varía según si desea gestionar cortafuegos NGFW, Prisma Access o ambos de forma simultánea. Para gestionar ambos, deberá seleccionar una región compatible con los NGFW y Prisma Access.

STEP 6 | Seleccione [Cloud Identity Engine](#) o cree una nueva instancia de CIE para identificar y verificar a todos los usuarios de su infraestructura. También puede omitirlo seleccionando **None (Ninguna)**.

paloalto
Activate Product
Strata Cloud Manager

Select Customer Support Account
This account is used for the registration and support of the products and add-ons that are bundled with this subscription. [Learn more](#)

Customer Support Account: [Edit](#)

Recipient: [Edit](#)

Region: United States - Americas [Edit](#)

Cloud Identity Engine [Done](#)

Create New

CIE instance for this tenant

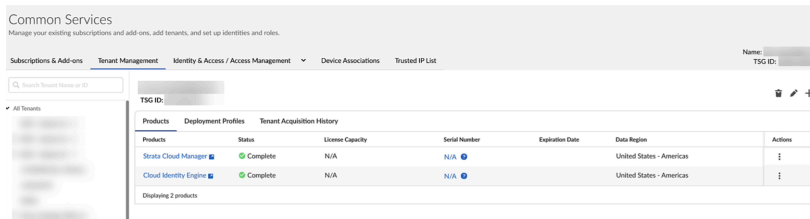
Device Onboarding Steps
You can view the list of devices in the customer support portal. To get the most of the product, follow the onboarding steps below. You can complete these onboarding steps after you finish product activation.

- 1 If you have firewalls: Associate Devices with Tenant**
Go to Settings > Devices Associations to associate devices with the tenant. [Learn more](#)
- 2 If you want to manage configuration in the cloud: Move Devices to Cloud Management**
Move devices to the cloud by following these [steps](#)
- 3 If you want to manage configuration in Panorama**
Please follow the Panorama documentation to configure the devices in Panorama [steps](#)
- 4 Enable Telemetry**
Device telemetry collects data about your device and shares it with Palo Alto Networks by uploading the data to Strata Logging Service. Enable telemetry on the device by following these [steps](#)

STEP 7 | Aceptar las **Terms and Conditions (Condiciones)** y **Activate (Activar)**.

STEP 8 | Espere a que Strata Cloud Manager se inicialice y a que el Estado se muestre Completo.

Si ha creado una nueva instancia de Cloud Identity Engine, espere a que su estado se muestre como Completo.

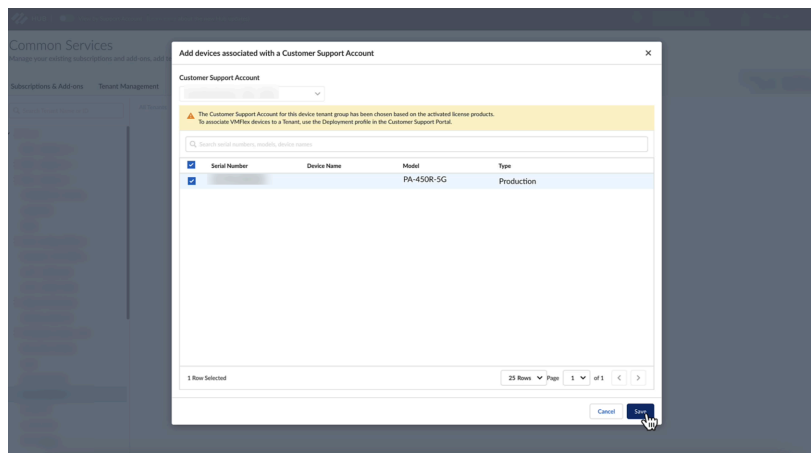


STEP 9 | Asocie los NGFW, Panorama o ambos a un inquilino que contenga su Strata Cloud Manager.



Asegúrese de asociar individualmente todos los cortafuegos gestionados por Panorama al inquilino.

1. Seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **Añadir dispositivos.**

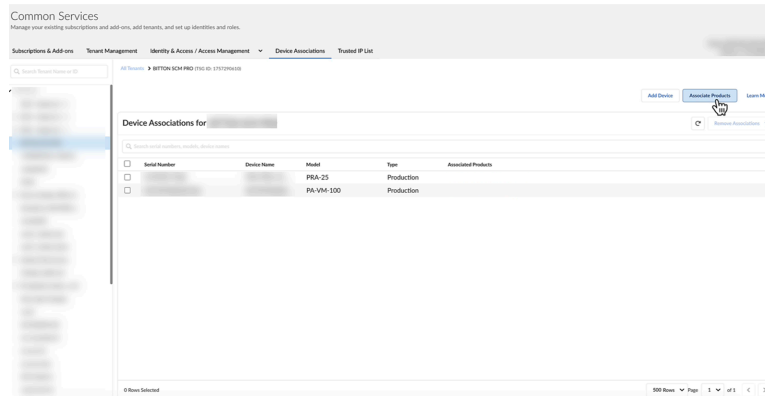


3. Seleccione uno o más cortafuegos o dispositivos Panorama y **Save (Guardar)**.

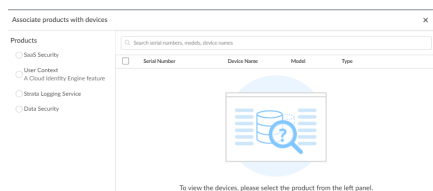
STEP 10 | Si tiene [Strata Logging Service](#), puede [asociarlo a dispositivos](#). De lo contrario, puedes omitirlo.

Después de activar Strata Cloud Manager Essentials, puede especificar los cortafuegos o dispositivos Panorama que desea utilizar con Strata Logging Service.

1. Seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **Asociar productos.**




3. En la columna Selección de productos, seleccione **Strata Logging Service**.



4. Seleccione dispositivos y **Save (Guardar)**.

STEP 11 | [Habilitar la telemetría en los dispositivos](#). Strata Cloud Manager evalúa el estado de los dispositivos en su implementación mediante el análisis de los datos de telemetría que sus dispositivos PAN-OS envían a Strata Logging Service. Para enviar estos datos, debe tener habilitada la telemetría de dispositivos en sus dispositivos.

 *A partir de PAN-OS 12.1.2, 11.1.11, 11.2.8, 10.2.17 y versiones posteriores, la [función de habilitación automática de la telemetría](#) configura la telemetría para que esté habilitada de forma predeterminada en sus dispositivos. Al incorporar un nuevo dispositivo (Panorama o cortafuegos), la telemetría se habilita automáticamente con ajustes controlados de forma central a través de Strata Cloud Manager o el Hub.*

STEP 12 | Inicie sesión en Strata Cloud Manager haciendo clic en su icono en el hub.

Activa Strata Cloud Manager Pro

Strata Cloud Manager Pro proporciona funciones avanzadas más allá de la licencia Essentials. A diferencia de la versión Essentials, esta incluye Strata Logging Service y proporciona un año de retención de logs. Para obtener más información sobre la compatibilidad con modelos de dispositivos, consulte [Compatibilidad con modelos de dispositivos](#).

Cuando su licencia Strata Cloud Manager Pro caduca, la instancia Strata Cloud Manager volverá al nivel de licencia Strata Cloud Manager Essentials. Cuando la licencia caduca para otras suscripciones, algunas siguen funcionando con una capacidad limitada y otras dejan de funcionar por completo. Consulte [qué sucede cuando cada suscripción caduca](#).

- [NGFW](#)
- [Prisma Access](#)
- [VM-Series con créditos de Software NGFW](#)
- [ELA](#)
- [ESA Pro](#)

Activar Strata Cloud Manager Pro para NGFW

Esta tarea muestra cómo activar Strata Cloud Manager Pro para NGFW. Para obtener más información sobre la compatibilidad con modelos de dispositivos, consulte [Compatibilidad con modelos de dispositivos](#).

Estos son los requisitos previos para NGFW:

- **Requisitos previos para la puesta en marcha de la gestión en la nube:** antes de incorporar su NGFW a Strata Cloud Manager, compruebe que se cumplen todas las condiciones para que el dispositivo esté listo. Esto incluye configuración de red, compatibilidad de software y requisitos de licencia. Completar estos pasos garantiza que su cortafuegos se pueda gestionar correctamente con Strata Cloud Manager.
- **Puertos TCP y FQDN para la gestión en la nube:** para permitir una comunicación fluida entre el NGFW y Strata Cloud Manager, configure puertos TCP específicos y nombres de dominio completos (FQDN).

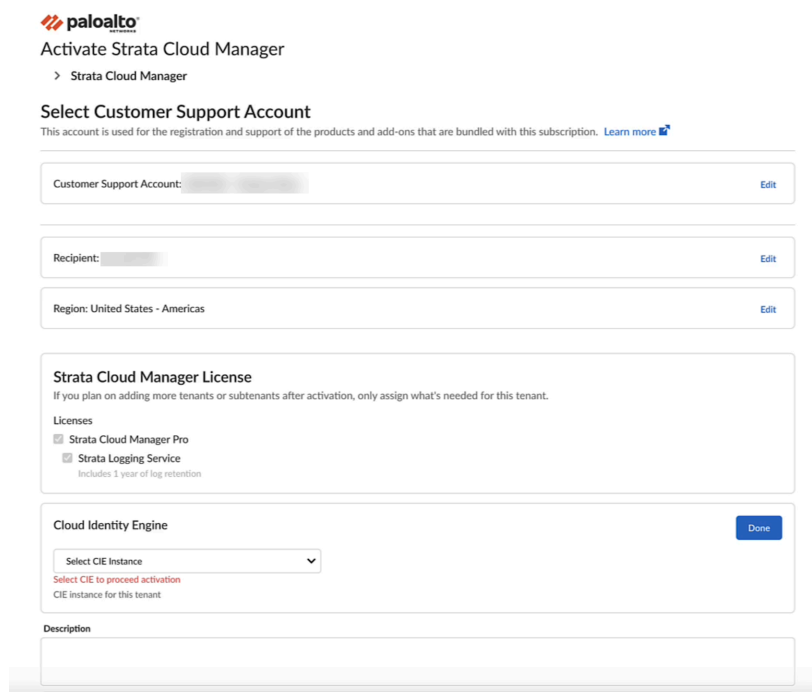
STEP 1 | Después de recibir un correo electrónico de Palo Alto Networks que identifique la licencia de Strata Cloud Manager Pro que está activando, haga clic en el enlace del correo electrónico para iniciar el proceso de activación.

STEP 2 | Elija la cuenta de servicio de atención al cliente que desea utilizar.

STEP 3 | Deberá **Select Tenant (Seleccionar inquilino)** donde activará Strata Cloud Manager Pro. Si no tiene un inquilino existente, seleccione **inquilino, Create New (Crear nuevo)**.

STEP 4 | Seleccione una **Region (Región)** donde desee implementar Strata Cloud Manager. Consulte las [Regiones compatibles para Strata Cloud Manager](#).

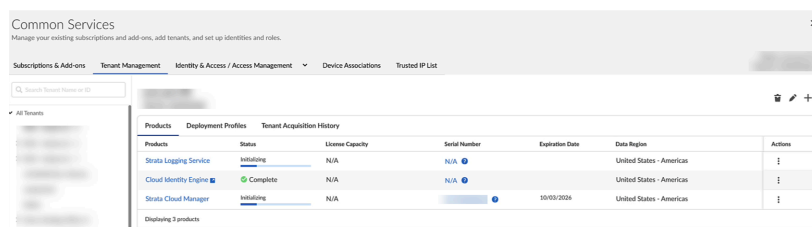
Strata Cloud Manager Pro incluye [Strata Logging Service](#) con un año de retención de logs.




STEP 5 | Seleccione [Cloud Identity Engine](#) o cree una nueva instancia de CIE para identificar y verificar a todos los usuarios de su infraestructura.

STEP 6 | Aceptar las **Terms and Conditions (Condiciones)** y **Activate (Activar)**.

STEP 7 | Espere a que Strata Cloud Manager, Cloud Identity Engine y Strata Logging Service se inicialicen y a que el estado se muestre completo.



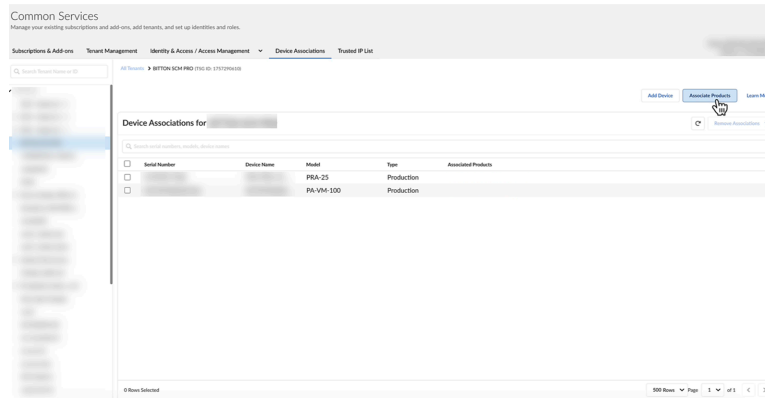
STEP 8 | [Asocie los NGFW, Panorama o ambos](#) a un inquilino que contenga su Strata Cloud Manager.

 **Asegúrese de asociar individualmente todos los cortafuegos gestionados por Panorama al inquilino.**

1. Seleccione **Common Services (Servicios comunes)** > **Device Associations (Asociaciones de dispositivos)**.
2. **Añadir dispositivos.**
3. Seleccione uno o más cortafuegos o dispositivos Panorama y **Save (Guardar)**.

STEP 9 | Asociar productos con dispositivos. Después de activar Strata Cloud Manager Pro, debe especificar los cortafuegos o dispositivos Panorama que desea usar con él.

1. Seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **Asociar productos.**



3. En la columna Selección de productos, seleccione **Strata Cloud Manager**.
4. Seleccione dispositivos y **Save (Guardar)**.

STEP 10 | Habilitar la telemetría en los dispositivos. Strata Cloud Manager evalúa el estado de los dispositivos en su implementación mediante el análisis de los datos de telemetría que sus dispositivos PAN-OS envían a Strata Logging Service. Para enviar estos datos, debe tener habilitada la telemetría de dispositivos en sus dispositivos.



A partir de PAN-OS 12.1.2, 11.1.11, 11.2.8, 10.2.17 y versiones posteriores, la **función de habilitación automática de la telemetría** configura la telemetría para que esté habilitada de forma predeterminada en sus dispositivos. Al incorporar un nuevo dispositivo (Panorama o cortafuegos), la telemetría se habilita automáticamente con ajustes controlados de forma central a través de Strata Cloud Manager o el Hub.

STEP 11 | Inicie sesión en Strata Cloud Manager haciendo clic en su icono en el hub.

Activar Strata Cloud Manager Pro para Prisma Access

Todos los **tipos de licencia de Prisma Access** incluyen acceso a Strata Cloud Manager, y todas las implementaciones de Prisma Access pueden aprovechar Strata Cloud Manager para características de visibilidad, como el Centro de control y Activity Insights, y supervisión de **Autonomous DEM**.

Además, puede optar por usar Strata Cloud Manager para la **Gestión de configuración de Prisma Access**; su otra opción es usar Panorama para la gestión de configuración. En ambos casos, se le guiará para activar Strata Cloud Manager Pro durante la activación de su licencia de Prisma Access:

- **Activa Prisma Access, con la gestión de configuración de Strata Cloud Manager**
- **Active Prisma Access, con gestión de configuración de Panorama**

Activar Strata Cloud Manager Pro para VM-Series mediante créditos de Software NGFW

Puede gestionar cortafuegos VM-Series financiados mediante créditos de Software NGFW usando Strata Cloud Manager, lo que permite un acceso sin problemas a funciones avanzadas de administración y supervisión mediante la activación de Strata Cloud Manager Pro.

Strata Cloud Manager admite la gestión de cortafuegos VM-Series independientes e implementaciones VM-Series gestionadas por Panorama, ofreciendo una solución integral para supervisar múltiples entornos:

- [Activar Strata Cloud Manager Pro para VM-Series](#)
- [Activar Strata Cloud Manager Pro para modelos VM-Series gestionado por Panorama](#)

Activar Strata Cloud Manager Pro con el acuerdo de licencia de la empresa

Esta tarea muestra cómo activar el Acuerdo de licencia empresarial (ELA) para Strata Cloud Manager. El complemento para ELA es un modelo de consumo para que las grandes empresas asignen suscripciones de forma masiva a los activos comprados a Palo Alto Networks.

Estos son los requisitos previos para NGFW:

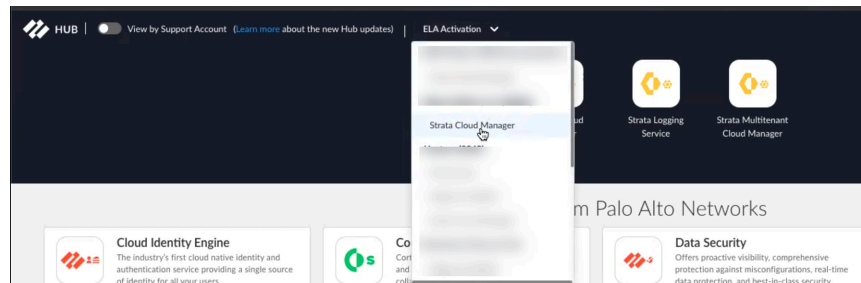
- **Requisitos previos para la puesta en marcha de la gestión en la nube:** antes de incorporar su NGFW a Strata Cloud Manager, compruebe que se cumplen todas las condiciones para que el dispositivo esté listo. Esto incluye configuración de red, compatibilidad de software y requisitos de licencia. Completar estos pasos garantiza que su cortafuegos se pueda gestionar correctamente con Strata Cloud Manager.
- **Puertos TCP y FQDN para la gestión en la nube:** para permitir una comunicación fluida entre el NGFW y Strata Cloud Manager, configure puertos TCP específicos y nombres de dominio completos (FQDN).



*Puede activar varios inquilinos Strata Cloud Manager Pro utilizando la misma licencia para dispositivos que pertenecen a las mismas cuentas de soporte. Para ello, diríjase a la Gestión de inquilinos para [crear nuevos inquilinos](#). Luego, vaya a **Suscripciones y complementos**, busque su suscripción, haga clic en **Activate Cloud Tenant (Activar Cloud Tenant)** que le redirigirá a la página de activación. Elija el mismo TSG en la página de activación que utilizó inicialmente.*

STEP 1 | Utilice uno de los siguientes métodos de activación.

- Inicie sesión en el [hub](#) y seleccione **ELA Activation (Activación de ELA) > Strata Cloud Manager**.



- Inicie sesión en el Portal de atención al cliente y active desde **License Management (Gestión de licencias) > Licenses (Licencias)** y, a continuación, haga clic en **ELA-Ngfw Activation (Activación de ELA-Ngfw)**.

STEP 2 | Elija la cuenta de servicio de atención al cliente que desea utilizar.

STEP 3 | Deberá **Select Tenant (Seleccionar inquilino)** donde activará Strata Cloud Manager Pro. Si no tiene un inquilino existente, seleccione **inquilino, Create New (Crear nuevo)**.

STEP 4 | Seleccione una **Region (Región)** donde desee implementar Strata Cloud Manager. Consulte las [Regiones compatibles para Strata Cloud Manager](#).

Strata Cloud Manager Pro incluye [Strata Logging Service](#) con un año de retención de logs.

A screenshot of the 'Activate Strata Cloud Manager' configuration page in the Palo Alto Networks HUB. The page title is 'Activate Strata Cloud Manager' with a breadcrumb 'Strata Cloud Manager'. It features a 'Customer Support Account' dropdown menu, a 'Recipient: SCM ELA demo 1' field with an 'Edit' link, and a 'Region: United States - Americas' field with an 'Edit' link. Below these is a 'Strata Cloud Manager License' section with a note: 'If you plan on adding more tenants or subtenants after activation, only assign what's needed for this tenant.' Under 'Licenses', there are two checked items: 'Strata Cloud Manager Pro' and 'Strata Logging Service' (which includes a note 'Includes 1 year of log retention'). At the bottom, there is a 'Cloud Identity Engine' section with a 'Select CIE Instance' dropdown menu and a 'Done' button.

STEP 5 | Seleccione [Cloud Identity Engine](#) o cree una nueva instancia de CIE para identificar y verificar a todos los usuarios de su infraestructura.

STEP 6 | Aceptar las **Terms and Conditions (Condiciones)** y **Activate (Activar)**.

STEP 7 | Espere a que Strata Cloud Manager y Strata Logging Service se inicialicen y a que el Estado de activación de ambos aparezca como Completado.

STEP 8 | **Asocie los NGFW, Panorama o ambos** a un inquilino que contenga su Strata Cloud Manager.



Asegúrese de asociar individualmente todos los cortafuegos gestionados por Panorama al inquilino.

1. Seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **Añadir dispositivos.**
3. Seleccione uno o más cortafuegos o dispositivos Panorama y **Save (Guardar)**.

STEP 9 | **Asociar productos** con dispositivos. Después de activar Strata Cloud Manager Pro, debe especificar los cortafuegos o dispositivos Panorama que desea usar con él.

1. Inicia sesión en el hub y seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **Asociar productos.**
3. En la columna Selección de productos con licencia, seleccione **Strata Cloud Manager**.
4. Seleccione dispositivos y **Save (Guardar)**.

STEP 10 | **Habilitar la telemetría en los dispositivos.** Strata Cloud Manager evalúa el estado de los dispositivos en su implementación mediante el análisis de los datos de telemetría que sus dispositivos PAN-OS envían a Strata Logging Service. Para enviar estos datos, debe tener habilitada la telemetría de dispositivos en sus dispositivos.



*A partir de PAN-OS 12.1.2, 11.1.11, 11.2.8, 10.2.17 y versiones posteriores, la **función de habilitación automática de la telemetría** configura la telemetría para que esté habilitada de forma predeterminada en sus dispositivos. Al incorporar un nuevo dispositivo (Panorama o cortafuegos), la telemetría se habilita automáticamente con ajustes controlados de forma central a través de Strata Cloud Manager o el Hub.*

STEP 11 | Inicie sesión en Strata Cloud Manager haciendo clic en su icono en el hub.

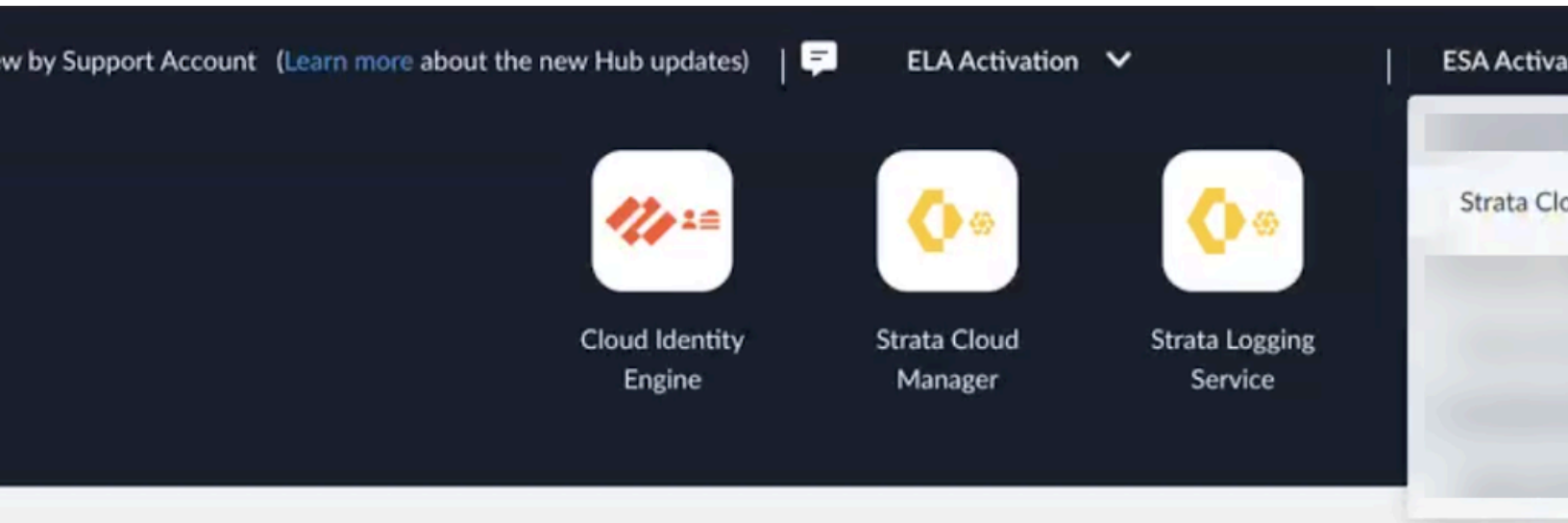
Activar Strata Cloud Manager Pro con el Acuerdo de asistencia para empresas

El Acuerdo de asistencia para empresas (ESA) Pro de Palo Alto Networks incluye Strata Cloud Manager Pro para NGFW. ESA Pro proporciona una solución optimizada para una experiencia de asistencia coherente en todos sus activos existentes y compras anticipadas. Este programa de empresas permite a las organizaciones maximizar los ahorros y beneficios a medida que se amplían, por lo que es una opción ideal para clientes con implementaciones de cortafuegos grandes y en expansión.

Esta tarea muestra cómo activar ESA Pro para Strata Cloud Manager. Puede iniciar el proceso de activación de ESA Pro desde el hub o portal de atención al cliente como se describe a continuación.

STEP 1 | Utilice uno de los siguientes métodos de activación:

- Inicia sesión en el [hub](#) y seleccione **ESA Activation (Activación de ESA) > Strata Cloud Manager**.



- Inicie sesión en el portal de atención al cliente. En el panel lateral izquierdo, vaya a **License Management (Gestión de licencias)** y, a continuación, en **Licenses (Licencias)**, seleccione **Activate Enterprise Agreement (Activar acuerdo de empresas)**.

▼ Set as Default Feedback ex. Where can I find m

ion Details EA Contract Details

nt Activate SCM ELA-ADNSR Activation

Account Name	Auth Code	License Description	Expiration Date	Licenses (Used / Total)
ELA				
ESA				

STEP 2 | Elija la cuenta de servicio de atención al cliente que desea utilizar.

STEP 3 | Cree un **New (Nuevo)** inquilino donde activará la instancia Strata Cloud Manager.

Strata Cloud Manager

Manager

Manager Pro for NGFW

Account ⓘ

Support Account

Recipient

where the product will be activated. [Learn more about tenants](#)

STEP 4 | Seleccione una **Region (Región)** donde desee implementar Strata Cloud Manager. Consulte las [Regiones compatibles para Strata Cloud Manager](#).

Una licencia Strata Cloud Manager Pro incluye [Strata Logging Service](#) con un año de retención de logs.

Manager License

For more tenants or subtenants after activation, only assign what's needed for this tenant.

Manager Pro

g Service

f log retention

STEP 5 | Seleccione [Cloud Identity Engine](#) o cree una nueva instancia de CIE para identificar y verificar a todos los usuarios de su infraestructura.

STEP 6 | **Agree to the Terms and Conditions (Aceptar las condiciones)** y **Activate (Activar)**.

STEP 7 | Espere a que Strata Cloud Manager y Strata Logging Service se inicialicen y a que el Estado de activación de ambos aparezca como **Completado**.

STEP 8 | [Asocie los NGFW, Panorama o ambos](#) a un inquilino que contenga su Strata Cloud Manager.



Asegúrese de asociar individualmente todos los cortafuegos gestionados por Panorama al inquilino.

1. Seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **Añadir dispositivos.**
3. Seleccione uno o más cortafuegos o dispositivos Panorama y **Save (Guardar)**.

STEP 9 | [Asociar productos](#) con dispositivos. Después de activar Strata Cloud Manager Pro, debe especificar los cortafuegos o dispositivos Panorama que desea usar con él.

1. Inicia sesión en el hub y seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **Asociar productos.**
3. En la columna Selección de productos con licencia, seleccione **Strata Cloud Manager**.
4. Seleccione dispositivos y **Save (Guardar)**.

STEP 10 | Habilitar la telemetría en los dispositivos. Strata Cloud Manager evalúa el estado de los dispositivos en su implementación mediante el análisis de los datos de telemetría que sus dispositivos PAN-OS envían a Strata Logging Service. Para enviar estos datos, debe tener habilitada la telemetría de dispositivos en sus dispositivos.



A partir de PAN-OS 12.1.2, 11.1.11, 11.2.8, 10.2.17 y versiones posteriores, la función de habilitación automática de la telemetría configura la telemetría para que esté habilitada de forma predeterminada en sus dispositivos. Al incorporar un nuevo dispositivo (Panorama o cortafuegos), la telemetría se habilita automáticamente con ajustes controlados de forma central a través de Strata Cloud Manager o el Hub.

STEP 11 | Inicie sesión en Strata Cloud Manager haciendo clic en su icono en el [hub](#).

Migrar de Panorama a Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> • NGFW (Managed by Panorama) • Prisma Access (Managed by Panorama) 	<p>Migración de cortafuegos NGFW:</p> <ul style="list-style-type: none"> ❑ Strata Cloud Manager Essentials o Pro ❑ Asegúrese de que sus NGFW cumplan con los requisitos previos para la gestión en la nube <p>Migración de Prisma Access:</p> <ul style="list-style-type: none"> ❑ Prisma Access ❑ Para comenzar la migración de Prisma Access (gestionado por Panorama) a Prisma Access (gestionado por Strata Cloud Manager), comuníquese con su equipo de cuentas de Palo Alto Networks

La migración de Panorama a Strata Cloud Manager ya está disponible para las implementaciones de Prisma Access y NGFW, lo que le permite disfrutar de los beneficios de la gestión en la nube y la gestión de configuración compartida en el entorno de la nube. El proceso de migración aborda consideraciones como la preservación de la configuración y la continuidad de la política.

Para las implementaciones de NGFW, puede seguir este flujo de trabajo para revisar la compatibilidad de la configuración, incluso si aún no está listo para migrar. Puede decidir recortar o aceptar cualquier característica que no sea compatible o que sea parcialmente compatible con la gestión de configuración de Strata Cloud Manager. Durante la migración, Strata Cloud Manager convierte las jerarquías de grupos de dispositivos de Panorama en estructuras de carpetas correspondientes de Strata Cloud Manager, y convierte las plantillas de Panorama y las pilas de plantillas en fragmentos reutilizables.

Para las implementaciones de Prisma Access, las migraciones se centran en preservar su infraestructura de acceso remoto, configuraciones de usuarios móviles y conectividad sitio a sitio mientras se transfiere la supervisión de la gestión a Strata Cloud Manager.

- [Migración de cortafuegos de nueva generación](#)
- [Migración de Prisma Access](#)

Migrar de Panorama a Strata Cloud Manager (NGFW)

Puede migrar las configuraciones de NGFW existentes de Panorama a Strata Cloud Manager para la gestión de la configuración basada en la nube.

Durante la migración, Strata Cloud Manager:

- Copia y traduce políticas de seguridad, configuraciones de red y objetos compatibles.
- Mantiene la topología de red existente e implementaciones de NGFW.
- Destaca las áreas que son parcialmente compatibles o no compatibles.

Póngase en contacto con su equipo de cuentas de Palo Alto Networks para habilitar el flujo de trabajo de migración.

Gestionar sus NGFW usando [Strata Cloud Manager en lugar de Panorama puede ofrecerle beneficios tales como](#) la gestión unificada para Prisma Access y cortafuegos NGFW, escalabilidad nativa de la nube de su red y visibilidad mejorada.

Strata Cloud Manager le guía a través de la migración de sus configuraciones con estos pasos clave:

- Cargar configuraciones existentes: importe sus configuraciones Panorama actuales.
- Ejecutar evaluación de compatibilidad: identifique características o configuraciones no compatibles que necesitan atención.
- Realizar la validación y prepararse para la implementación: complete las comprobaciones finales antes de la migración.
- Control de la migración: los dispositivos y grupos de dispositivos se pueden migrar por fases, lo que le permite migrar dispositivos no críticos o ir sitio por sitio.

Revise los resultados en cada paso, realice los ajustes necesarios y verifique que sus configuraciones sean totalmente compatibles con Strata Cloud Manager antes de completar la migración.

Cómo cambia la configuración de la gestión cuando pasa de Panorama a Strata Cloud Manager

La gestión de la configuración de Panorama se basa en:

- Grupos de dispositivos: organice cortafuegos en grupos jerárquicos para la gestión de políticas de seguridad (reglas de seguridad, políticas NAT, filtros de aplicaciones).
- Plantillas y pilas de plantillas: defina la configuración de la red y dispositivos (interfaces, zonas, enrutamiento, ajustes del sistema).
- Herencia: los grupos de dispositivos heredan las políticas de los grupos principales; las pilas de plantillas superponen múltiples plantillas con capacidad de anulación.

La gestión de la configuración de Strata Cloud Manager se basa en:

- Carpetas: contenedores jerárquicos que contienen tanto políticas de seguridad COMO configuraciones de red.

- Fragmentos: bloques de configuración reutilizables que se pueden adjuntar a carpetas a cualquier nivel.
- Contenedores: carpetas de configuración específicos del dispositivo para requisitos de cortafuegos únicos.

Durante la migración, Strata Cloud Manager convierte su configuración basada en Panorama y la compila en carpetas y fragmentos:

Panorama	Strata Cloud Manager
Grupos de dispositivos	Carpetas
Plantillas y pilas de plantillas	Fragmentos
DG compartido	Carpeta Todos los cortafuegos
Objetos compartidos	Carpeta global como fragmento adjunto
Políticas en grupos de dispositivos	Políticas en Carpeta(s) asignada(s)
Objetos (direcciones, EDL, etc.)	Objetos en Carpeta(s) asignada(s)

Diferencia clave entre Panorama y Strata Cloud Manager a tener en cuenta:

- Strata Cloud Manager Folders contienen configuraciones tanto de red como de seguridad, mientras Panorama separa estas entre Plantillas y Grupos de dispositivos
- Las carpetas de Strata Cloud Manager proporcionan una herencia más flexible con anulaciones basadas en fragmentos frente a las anulaciones de grupo de nivel inferior que se ven en Panorama
- Strata Cloud Manager Snippets proporciona un enfoque de configuración más directo y listo para usar en comparación con las plantillas y pilas de plantillas de Panorama que se heredan en la pila.

Después de la migración, usted gestiona las configuraciones a través del modelo de carpetas y fragmentos. El orden de los adjuntos de fragmentos determina la precedencia de configuración, proporcionando un control granular sobre cómo se combinan varias fuentes de configuración. También puede crear contenedores específicos de dispositivo para NGFW que requieran configuraciones únicas fuera del modelo de herencia de carpetas.



Recursos adicionales

Más información sobre [Grupos de dispositivos](#) y [Plantillas](#).

Más información sobre [Fragmentos](#) y [Carpetas](#)

Preparar la migración de sus cortafuegos NGFW a Strata Cloud Manager

Antes de comenzar la migración, asegúrese de tener listos los siguientes elementos:

- Requisitos mínimos de software: PAN-OS 10.2.3 o posterior.

- [Exportar archivo de configuración de Panorama](#): Exporte la configuración en ejecución completa de su instancia de Panorama de origen en formato XML
- [Clave maestra de Panorama](#): Obtenga la clave maestra utilizada para el cifrado en su configuración de Panorama (si no utiliza la clave predeterminada)
- [Inquilino de Strata Cloud Manager](#): Compruebe que su inquilino de Strata Cloud Manager está implementado, tiene la licencia adecuada y está operativo
- [Configuración de NGFW](#): Recopile los últimos archivos de configuración enviados (archivos de asistencia técnica) de los NGFW que planea validar después de la migración
- [Topología de red](#): Revise las jerarquías de su grupo de dispositivos actual, las relaciones de plantillas y las asignaciones de NGFW
- [Copia de seguridad de la configuración](#): Cree copias de seguridad completas de sus configuraciones de Panorama y NGFW actuales como medida de seguridad
- [Acceso administrativo](#): Asegúrese de tener acceso a la función de superusuario tanto en Panorama como en Strata Cloud Manager.
- Planificación de la migración: Identifique qué grupos de dispositivos, plantillas y NGFW desea migrar en su fase inicial
- [Matriz de compatibilidad](#): comprenda qué características pueden no admitirse en Strata Cloud Manager y planifique los ajustes de configuración necesarios

Migrar sus NGFW gestionados por Panorama a Strata Cloud Manager

Migre sus configuraciones de NGFW de Panorama a Strata Cloud Manager:

STEP 1 | Prepare su Panorama para la migración.

1. Inicie sesión en el Panorama que gestiona sus NGFW con una cuenta administrativa que tiene asignado la función de [Superusuario](#).
2. **(Opcional)** Si has configurado una Clave maestra personalizada para Panorama, haga una nota de ello.
Si su implementación utiliza la clave maestra predeterminada, este paso no es necesario.
3. Asegúrese de que su configuración actual de Panorama esté actualizada y de que haya confirmado y enviado todos sus cambios a Panorama, para ello, vaya a **Commit (Confirmar) > Commit & Push (Confirmar y enviar)** y **Preview Changes (Vista previa de cambios)**.
4. **(Opcional)** Verifique las diferencias entre la configuración en ejecución y la configuración candidata y determine si desea aplicar esos cambios. Para confirmar y enviar los cambios,

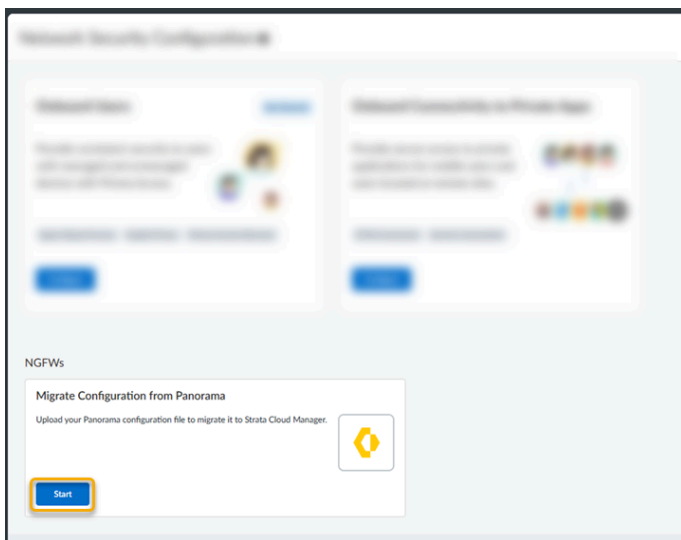
deberá **Edit Selections (Editar las selecciones)** y seleccionar los NGFW que desea enviar en el **Push Scope (Ámbito de envío)**.

5. **(Opcional) Commit and Push (Confirmar y enviar)** sus cambios.
6. Vaya a **Panorama > Setup (Configuración) > Operations (Operaciones)** y **Export (Exportar)** la instantánea de configuración de Panorama con nombre.

El archivo .xml es necesario para cargarlo en Strata Cloud Manager durante el proceso de migración. No cargue un archivo de asistencia técnica ni ningún otro archivo excepto un archivo de configuración .xml.

7. Seleccione el archivo de configuración **running-config.xml** y luego haga clic en **OK (Aceptar)**.

STEP 2 | Inicie sesión en Strata Cloud Manager como administrador con un rol de Superusuario y vaya a **Configuration (Configuración) > Onboarding (Incorporación)**.



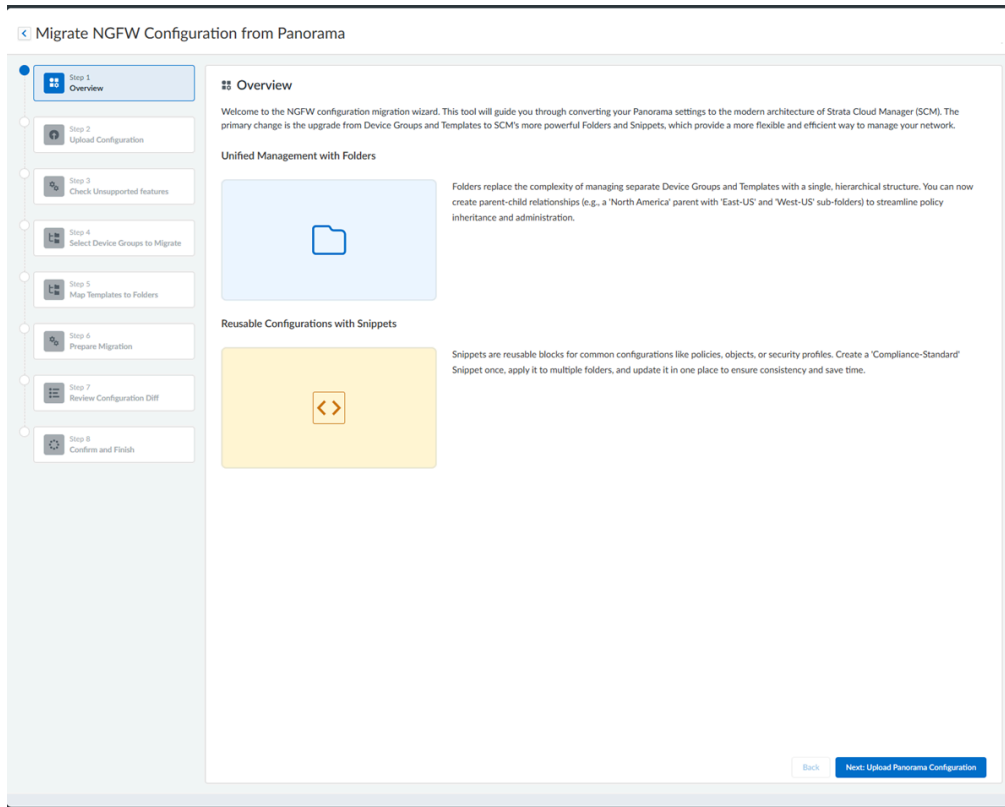
El programa de migración detecta que tiene una implementación gestionado por Panorama.

1. Confirme que el inquilino es correcto.
2. (Opcional) [Cree una instantánea con nombre](#) de su configuración en ejecución en caso de que sea necesario un retroceso.



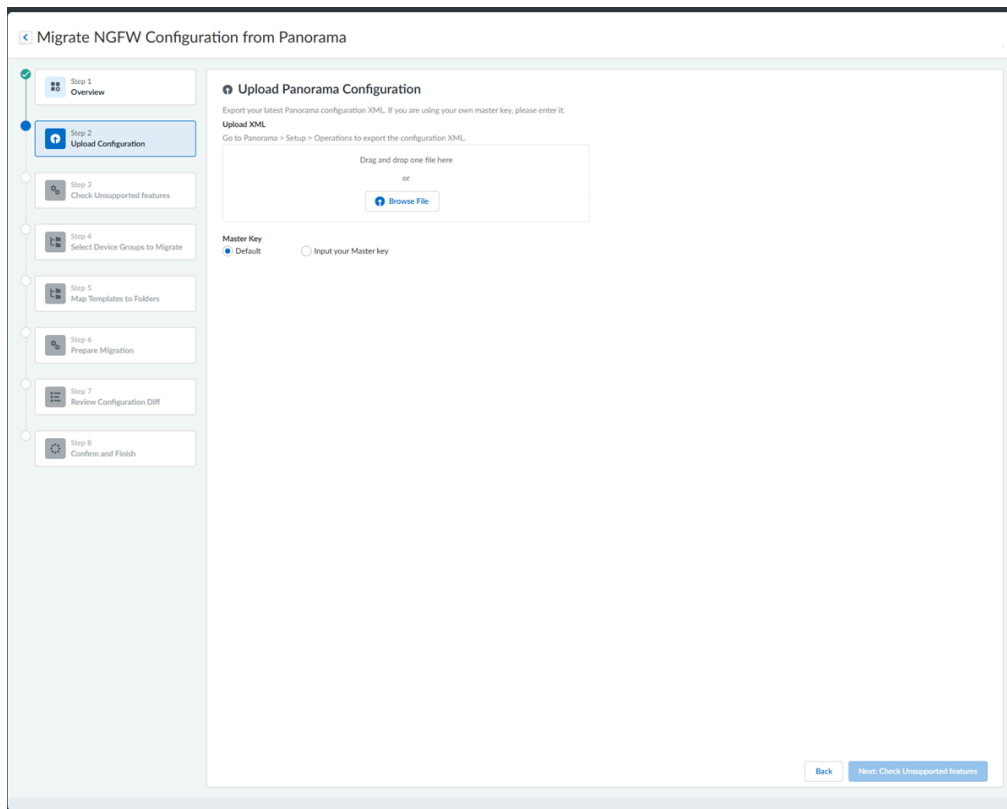
No se debe intentar la migración durante una ventana de actualización de Strata Cloud Manager. Consulte su calendario de actualizaciones para ver si tiene una próxima actualización.

STEP 3 | Lea la **Overview (Descripción general)** de la migración.



1. Revise los componentes básicos de la gestión de Strata Cloud Manager: **Folders (Carpetas)** y **Snippets (Fragmentos)**.
2. Haga clic en **Next (Siguiente): Cargar configuración de Panorama**.

STEP 4 | Cargar la configuración de Panorama.



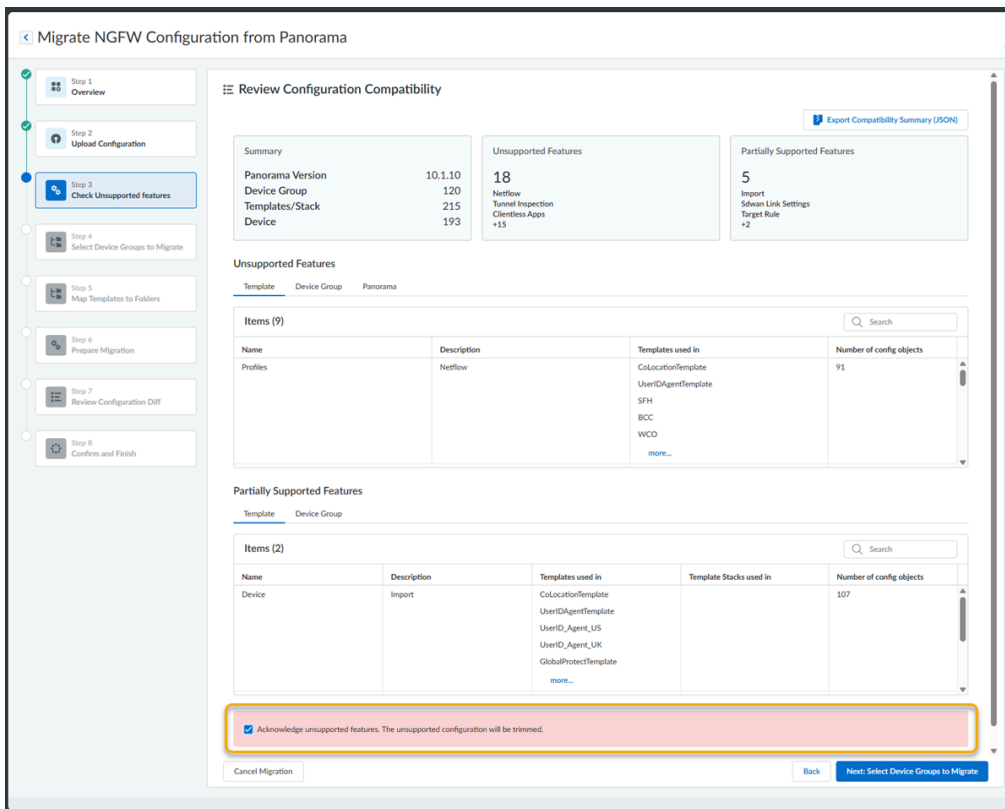
1. Seleccione el archivo de configuración Panorama *.xml* que descargó en un paso anterior arrastrándolo y soltándolo desde su explorador de archivos o seleccionando **Choose File (Seleccionar archivo)**.
2. **(opcional)** Introduzca su **Master Key (Clave maestra)**, o si no creó una clave maestra personalizada, utilice la **Default (Predeterminada)**.

Master Key
 Default Input your Master key

Master Key *

3. Haga clic en **Next (Siguiente):** Revise la compatibilidad de la migración.

STEP 5 | Revise la configuración compatible.



1. **(Opcional)** Puede **Export Compatibility Summary (Exportar resumen de compatibilidad)** y revisar la compatibilidad de configuración de su organización antes de continuar y

permitir que Strata Cloud Manager recorte cualquier configuración no compatible o parcialmente compatible.

El recorte de las características no compatibles y parcialmente compatibles evita la migración de características que no se pueden implementar de forma segura en Strata Cloud Manager.

Este proceso solo afectará a la configuración escalonada de Strata Cloud Manager. Las configuraciones en Panorama no se verán afectadas.

Para cada área marcada, deberá planificar reconstruir, reemplazar o diferir esas configuraciones.

Review Configuration Compatibility

Export Compatibility Summary (JSON)

Summary	
Panorama Version	10.1.10
Device Group	120
Templates/Stack	215
Device	193

Unsupported Features
18
Netflow
Tunnel Inspection
Clientless Apps
+15

Partially Supported Features
5
Import
Sdwan Link Settings
Target Rule
+2

2. Revise las **Unsupported Features (Características no compatibles)** que se recortarán de su configuración durante la migración.

Estas características se recortarán de sus configuraciones y no se ejecutarán en Strata Cloud Manager durante el proceso de migración de configuración.

3. Revise las **Partially Supported Features (Características parcialmente compatibles)** y determine una ruta de resolución.

Identifique qué es exactamente lo que va a faltar en la configuración.

Puede aceptar las características parcialmente compatibles y crear un plan de recuperación después de la migración o volver a su configuración Panorama y limpiar estas áreas antes de comenzar el proceso de migración de nuevo.

4. **Acknowledge (Reconocer)** las características no compatibles y parcialmente compatibles.
5. Haga clic en **Next (Siguiendo): Seleccione Grupos de dispositivos para migrar.**

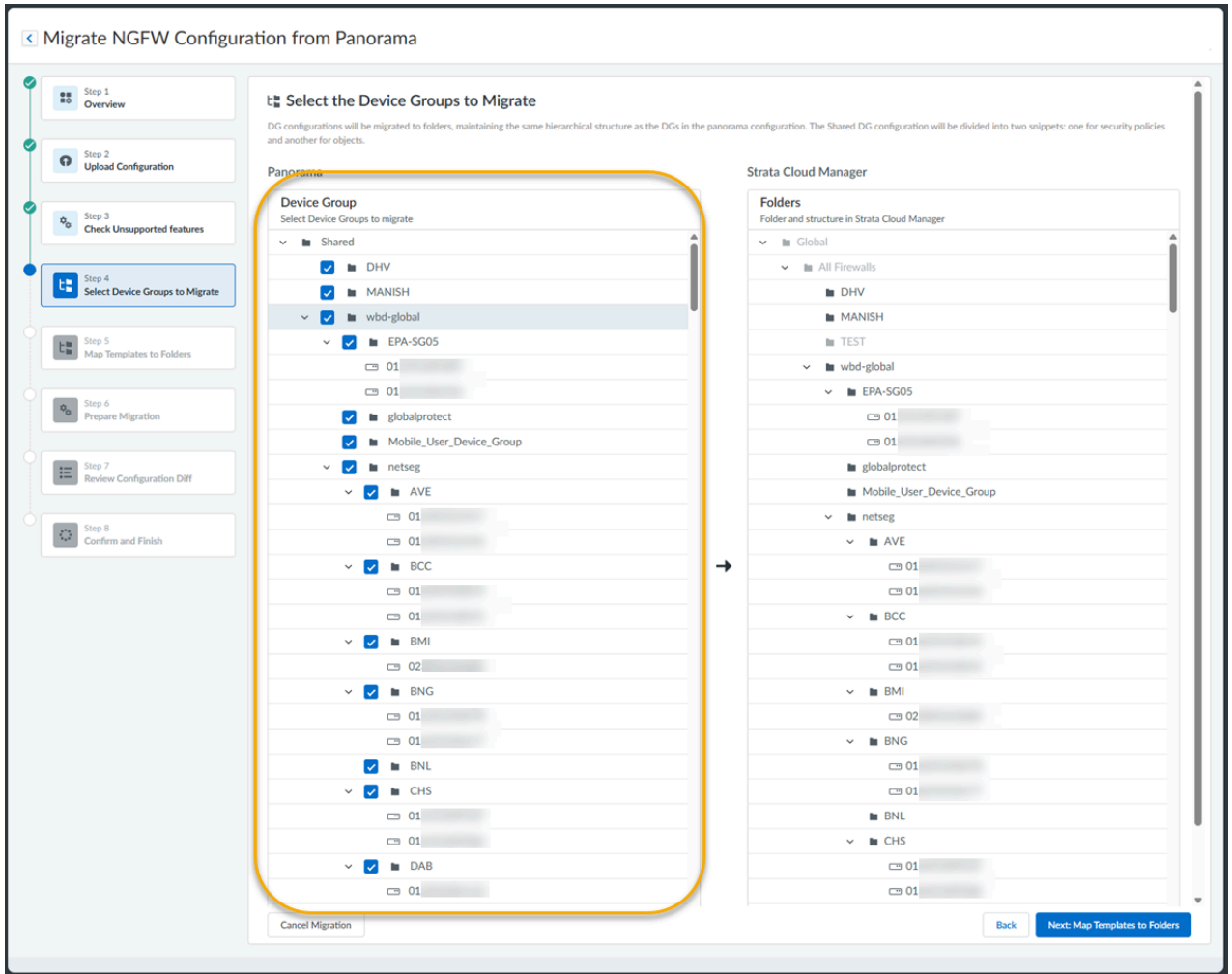


Para aquellos que solo buscan comparar configuraciones compatibles, o si se decide que se necesita más planificación, puede finalizar el proceso de migración aquí.

STEP 6 | Seleccione los **Devices (Dispositivos)** o **Device Groups (Grupos de dispositivos)** que desea migrar.



Si va a migrar cortafuegos NGFW desde Panorama por primera vez, se recomienda migrar primero solo dispositivos o grupos de dispositivos no críticos para probar cómo se migrarán sus configuraciones a Strata Cloud Manager.



Durante la migración:

- Los objetos se importan a un fragmento y se adjuntan a la carpeta Global.
- Las políticas se importan en la(s) carpeta(s) migrada(s) por el flujo de trabajo.
- Los Grupos de dispositivos compartidos se asignan automáticamente a la carpeta Todos los cortafuegos.

1. Haga clic en **Next (Siguiete): Asigne plantillas a Carpetas.**

STEP 7 | Asigne Templates (Plantillas) a sus Folders (Carpetas) recién configuradas.

Migrate NGFW Configuration from Panorama

Step 1 Overview

Step 2 Upload Configuration

Step 3 Review Configuration Compatibility

Step 4 Select Device Groups to Migrate

Step 5 Map Templates to Folders

Step 6 Prepare Migration

Step 7 Review Configuration Diff

Step 8 Confirm and Finish

Map Templates to Folders

Auto Template Mapping
This option automatically associates the template and template stack configuration, after being migrated to snippets, to the respective folders.

Manual Template Mapping
This option enables administrators to manually associate template and template stack configurations with folders after migration to snippets.

Rule: You must assign every Template and Template Stack to a folder. They will be imported into SCM as Snippets.

Recommendation: We recommend assigning commonly used configurations to a shared folder (like "All Firewalls") for more efficient management later.


Shared

- US
 - 11111
 - 22222
- US-West
 - 33333
- California
 - 44444

Templates/Template Stacks used in 44444

Name	SHARED		SCOPED (44444)	
	Referenced Template Stack / Total	Referenced NGFW / Total	Referenced Template Stack / Total	Referenced NGFW / Total
Template Stacks (1)				
ts4	N/A	1/4	N/A	1/1
Templates (3)				
tpl-Common	4/4	4/4	1/1	1/1
tpl-US-West	2/4	2/4	1/1	1/1
tpl-VM	2/4	2/4	1/1	1/1

Durante la migración, las **Templates (Plantillas)** se configuran en **Snippets (Fragmentos)** equivalentes.

 Si dos o más grupos de dispositivos reutilizan la misma plantilla, elévela a una carpeta superior. Si solo un sitio lo requiere, manténgalo en el nivel del sitio.

1. Seleccione un **Device Group (Grupo de dispositivos)** para revelar las **Templates/ Template Stacks (Plantillas/Pilas de plantillas)** utilizadas por ese grupo de dispositivos.

Activación e incorporación de Strata Cloud Manager

31

©2026 Palo Alto Networks, Inc.

AVE-STACK

Associate the migrated snippets to either the folder or the device, depending how they are applied within the Panorama configuration.

Name	Attached Snippets
▼ All Firewalls	0
▼ <input checked="" type="checkbox"/> wbd-global	1
▼ <input type="checkbox"/> netseg	0
▼ <input type="checkbox"/> AVE	0
<input type="checkbox"/> 01 [redacted]	0
<input type="checkbox"/> 01 [redacted]	0
▼ <input type="checkbox"/> BCC	0
<input type="checkbox"/> 01 [redacted]	0
<input type="checkbox"/> 01 [redacted]	0
▼ <input type="checkbox"/> BMI	0
<input type="checkbox"/> 02 [redacted]	0

Referenced Template Stack Referenced NGFW

Referenced NGFWs (2)

Name
01 [redacted]
01 [redacted]

* Required Field

2. Deberá **Edit (Editar)** la asignación para asignar cada **Template/Template Stack (Plantilla/ Pila de plantillas)** a una **Folder (Carpeta)**.
3. Eleve plantillas a las que se hace referencia en varios lugares a carpetas superiores.
 Por ejemplo, si tiene configuraciones de plantilla globales, asignarlas a la carpeta Todos los cortafuegos establece esas configuraciones como verdaderas para todos los NGFW.
4. Después de asignar más de un Fragmento a una Carpeta, ajuste el orden.
5. Deberá **Move Up (Subir)** o **Move Down (Bajar)** para finalizar el pedido.
6. **Update (Actualizar)** el orden.
7. **Save (Guardar)** el nuevo orden.

Antes de pasar al siguiente paso, asegúrese de lo siguiente:

- No quedan plantillas ni pilas de plantillas sin asignar.
- Cualquier plantilla a la que hayan hecho referencia múltiples grupos de dispositivos se ha elevado a las carpetas adecuadas.

8. Haga clic en **Next (Siguiente): Preparar Migración**.

El proceso de migración empieza.

Espera a que se completen todos los pasos.



Si hay algún problema con la migración, vuelva a los pasos anteriores para evaluar y hacer cambios. Si los problemas persisten, póngase en contacto con la asistencia de Palo Alto Networks.

STEP 8 | Prepárese para migrar.

1. **Cargue la configuración en Strata Cloud Manager** para preparar la migración.

1. El flujo de trabajo de migración:

- Traduce dispositivos y grupos de dispositivos, y plantillas y pilas de plantillas a carpetas y fragmentos utilizando el orden de asignaciones y fragmentos definido por usted.
 - Crea una instantánea de Strata Cloud Manager para permitir la reversión de los cambios por etapas.
 - Comprueba conflictos en las configuraciones existentes de Strata Cloud Manager (choques de nombres, referencias que faltan, límites de 31 caracteres, alcance de RBAC).
 - Crea la configuración por etapas que estará en Strata Cloud Manager después de la carga.
2. deberá **Load Results (Cargar resultados)** y revisar qué objetos, políticas o fragmentos se crearon, actualizaron u omitieron.
 3. Revise los **Validation Results (Resultados de validación)** para detectar errores, advertencias y mensajes informativos después de la migración.
 4. Haga clic en **Next (Siguiente): Revisar diferencias de configuración**.
Esto aplica la configuración recién generada a Strata Cloud Manager.

STEP 9 | Revisar las diferencias de configuración.

1. En el árbol de carpetas de la izquierda, expanda a la carpeta y seleccione un número de serie de NGFW para validar
2. Deberá **Browse File (Examinar archivo)** y seleccionar el TSF para el número de serie seleccionado.

La carga del TSF para el NGFW elegido le permitirá validar correctamente todas las configuraciones admitidas, parcialmente admitidas y no admitidas.

Asegúrese de buscar cualquier cosa que se haya creado, modificado o eliminado. Las configuraciones que se están recortando no deben ser una sorpresa.



Debido a las convenciones de nombres en Strata Cloud Manager, algunos nombres largos se comprimirán cuando sea necesario.

3. Revise los paneles de diferencias de configuración.
 1. Paneles verdes: Creado o añadido. Están presentes en Strata Cloud Manager, pero no en el dispositivo original.
 2. Paneles rojos: Borrado o recortado. Puede que no sea compatible con Strata Cloud Manager, pero están en el dispositivo.
 3. Paneles amarillos: Modificado.



La vista de diferencias puede ser muy extensa, está limitada a un solo NGFW a la vez y se calcula a partir del último XML enviado desde el TSF.

4. Verifique las diferencias para los dispositivos representativos de cada patrón o tipo de sitio.
5. **(Opcional) Export (Exportar)** los diferentes resultados.
6. **(Opcional) Regenerate Diffs (Regenerar diferencias)** si se ha realizado alguna corrección.
7. Haga clic en **Next (Siguiete): Confirmar y finalizar**.

STEP 10 | Debe **Confirm (Confirmar)** y finalizar sus migraciones de NGFW a Strata Cloud Manager.

Ahora que su migración se ha completado, revise la [documentación](#) disponible para Strata Cloud Manager.

1. Asegúrese de que se aceptan los resultados de los pasos 8 y 9.
2. proceda a **Confirm (Confirmar)** la migración.
Esto marca oficialmente la migración como completa.
3. **(Opcional)** Para revertir la configuración a su estado anterior a la migración en cualquier momento, seleccione **Revert (Revertir)**. Esto inicia un flujo de trabajo de retroceso, restaurando Strata Cloud Manager a una instantánea tomada antes de que se cargara la migración.
4. **(Opcional)** Para cancelar la migración en cualquier momento, seleccione **Cancel Migration (Cancelar migración)**. Esto cancela el proceso de migración y limpia cualquier cambio temporal.

Migrar de Panorama a Strata Cloud Manager (Prisma Access)

Si tiene una implementación de Prisma Access existente para la cual la configuración es gestionada por Panorama y desea migrar a Strata Cloud Manager para la gestión de la configuración, Palo Alto Networks ofrece un flujo de trabajo en el producto que le permite migrar su configuración existente de Prisma Access a Strata Cloud Manager.



Para habilitar el flujo de trabajo de migración, debe ponerse en contacto con su equipo de cuenta de Palo Alto Networks.

Gestionar su configuración de Prisma Access utilizando Strata Cloud Manager en lugar de Panorama puede ofrecerte beneficios como:

- [Evaluaciones continuas de prácticas recomendadas](#)
- Configuraciones predeterminadas seguras
- Optimización de configuración basada en aprendizaje automático (ML)
- Flujos de trabajo de seguridad web optimizados
- Un resumen visual interactivo ([Centro de control](#)) que le ayuda a evaluar la salud, la seguridad y la eficiencia de la red.
- [Flujos de trabajo](#) intuitivos para tareas complejas
- [Gestión de las API](#) simples y seguras
- La arquitectura nativa de la nube proporciona escalabilidad, resiliencia y alcance global.
- No hay hardware que gestionar ni software que mantener

Prepárese para migrar a Prisma Access (Managed by Strata Cloud Manager)

Antes de comenzar su migración, debe estar al tanto de los requisitos mínimos de software y de los tipos de implementaciones de Prisma Access (Managed by Panorama) que puede migrar.

- **Cuándo migrar:** no realice su actualización durante una actualización del plano de datos o de la infraestructura. Verifique sus [preferencias de actualización](#) para ver si tiene una próxima actualización del plano de datos.
- **Migración unidireccional de Panorama a Prisma Access (Managed by Strata Cloud Manager):** solo puede migrar de un Prisma Access (Managed by Panorama) a una implementación de Prisma Access (Managed by Strata Cloud Manager). Después de migrar a Strata Cloud Manager, no puede volver a gestionar su implementación de Prisma Access utilizando Panorama.
- **Versión mínima de Panorama:** se requiere una versión mínima de Panorama de 10.0.
- **Función de administrador requerido:** debe haber iniciado sesión como superusuario en Strata Cloud Manager para comenzar la migración.
- **Requisitos de licencia:** se requiere una licencia de Prisma Access válida.

- **Cloud Identity Engine:** debe haber [integrado el componente Directory Sync](#) de Cloud Identity Engine con el inquilino de Prisma Access (Managed by Panorama) actual antes de migrar.
- **Funcionalidades no soportadas:** el programa de migración no soporta las siguientes funcionalidades de Prisma Access:
 - [Filtrado de datos](#) (como alternativa, utilice [Enterprise DLP](#))
 - Implementaciones de [FedRAMP](#)
 - [IoT Security](#)
 - Implementaciones [Multiinquilino](#)
 - [Proxy SSH](#)
 - Autenticación independiente para portales y gateways de GlobalProtect
- **Migraciones de Prisma SD-WAN y Prisma Access:** si migra una implementación de Prisma Access y una de [Prisma SD-WAN](#), Prisma Access y Prisma SD-WAN deben compartir el mismo ID de grupo de servicios de inquilino ([TSG ID](#)).
- **Config Diff Issues (Problemas de diferencia de configuración):** cuando ejecute la diferencia de configuración durante la migración, ignore cualquier diferencia que muestre los siguientes nombres de objeto porque no afectan a su configuración:
 - Clientless-vpn crypto-settings
 - Hip-profiles rename
 - Mobile-user-redundancy
 - Exclude-video-traffic

Migra su implementación de Prisma Access (Managed by Panorama) a Strata Cloud Manager

Para migrar su Prisma Access (Managed by Panorama) a una implementación de Prisma Access (Managed by Strata Cloud Manager), complete los siguientes pasos.

A un alto nivel, usted:

1. Asegúrese de haber enviado correctamente la última configuración a Prisma Access, haber guardado la última configuración y haber exportado un archivo de configuración .xml desde el Panorama que gestiona Prisma Access.
2. Inicie el programa de migración desde Strata Cloud Manager.
3. Verifique las diferencias de configuración (difs) entre la configuración de Panorama y la configuración migrada de Strata Cloud Manager.
4. Resuelve las diferencias y completa la migración.

STEP 1 | Prepare su Panorama para la migración.

1. Inicie sesión en el Panorama que gestiona Prisma Access con una cuenta administrativa que tiene asignado la función de superusuario.
2. **(Opcional)** Si has configurado una **Clave Maestra** personalizada para su Panorama y para Prisma Access, haga una nota de ello.
Si su implementación utiliza la clave maestra predeterminada, este paso no es necesario.
3. Asegúrese de que su configuración actual de Panorama esté actualizada y de que haya confirmado y enviado todos sus cambios a Panorama y a Prisma Access yendo a **Commit (Confirmar) > Commit & Push (Confirmar y enviar) y Preview Changes (Vista previa de cambios)**.
4. **(Opcional)** Verifique las diferencias entre la configuración en ejecución y la configuración candidata y determine si desea aplicar esos cambios. Si desea confirmar y enviar los

cambios, deberá **Edit Selections (Editar las selecciones)** y seleccionar los componentes de Prisma Access que desea enviar en el **Push Scope (Ámbito de envío)**.

The screenshot shows the 'Panorama Local Config Audit' window with a comparison between 'Running Configuration' and 'Candidate Configuration'. A legend indicates 'Added' (green), 'Modified' (yellow), and 'Deleted' (red). The 'Candidate Configuration' section shows a new entry for 'adobe-express' highlighted in green. Below this is the 'Push Scope Selection' dialog, which has tabs for 'Device Groups', 'Templates', 'Collector Groups', 'WildFire Appliances and Clusters', 'Firewall Clusters', and 'Prisma Access'. Under the 'Prisma Access' tab, several items are checked: Remote Networks, Mobile Users, Service Setup, Explicit Proxy, and Colo Connect. 'OK' and 'Cancel' buttons are at the bottom right.

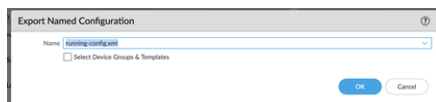
5. **(Opcional) Commit and Push (Confirmar y enviar) sus cambios.**

The screenshot shows the 'Commit and Push' dialog box. It contains a message: 'Doing a commit will overwrite the Panorama running configuration with the commit scope. Show config size'. There are two radio buttons: 'Commit And Push All Changes' (selected) and 'Commit And Push Changes Made By: [1] admin'. Below is a table with columns: COMMIT SCOPE, LOCATION TYPE, OBJECT TYPE, ENTITIES, and ADMINS. The first row shows 'shared-object' with 'Shared' location type. Below the table are buttons for 'Preview Changes', 'Change Summary', and 'Validate Commit'. Another table with columns: PUSH SCOPE, LOCATION TYPE, OBJECT TYPE, ENTITIES, and ADMINS. The first row shows 'Remote_Network_Device_Group' with 'Prisma Access' location type. Below this table are checkboxes for 'Edit Selections' (checked), 'No Default Selections', 'Validate Device Group Push', and 'Validate Template Push'. A note states: 'Note: By default, devices that are associated with the entities in the commit scope are selected, however you may customize the selection.' There is a text field 'Enter a description'. At the bottom are 'Schedule', 'Commit And Push' (highlighted in yellow), and 'Cancel' buttons.

6. Vaya a **Panorama > Setup (Configuración) > Operations (Operaciones)** y **Export named Panorama configuration snapshot (Exportar instantánea de configuración de Panorama con nombre)**.

Este archivo .xml es necesario para cargar a Strata Cloud Manager durante el proceso de migración. **No suba un archivo de asistencia técnica ni ningún otro archivo excepto un archivo de configuración .xml.**

7. Seleccione el archivo de configuración **running-config.xml** y luego **OK (Aceptar)**.

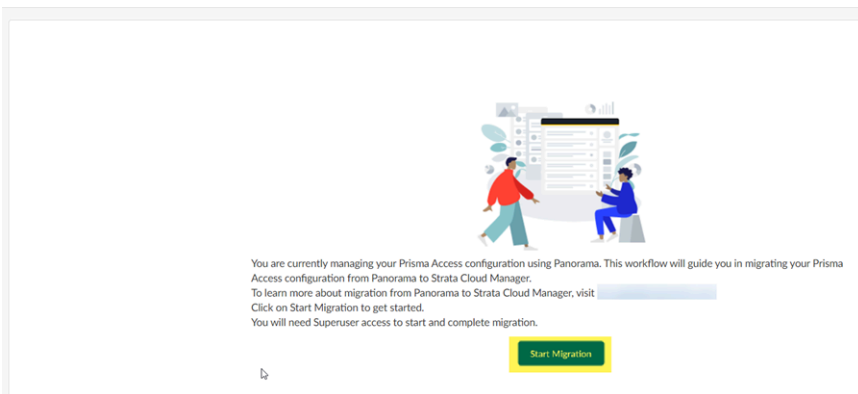


- STEP 2 |** Inicie sesión en Strata Cloud Manager como administrador con una **función de Superusuario** y vaya a **Manage (Gestionar) > Configuration (Configuración) > NGFW and Prisma Access (NGFW y Prisma Access) Configuration (Configuración) > NGFW and Prisma Access (NGFW y Prisma Access)**.

El programa de migración detecta que tiene una implementación gestionado por Panorama.

- STEP 3 |** Iniciar la migración.

Migrate to Strata Cloud Manager



- STEP 4 |** El programa de migración le pide que se asegure de que su configuración esté actualizada y le muestra el último usuario que la actualizó. Después de haber verificado que esta configuración tiene los últimos cambios, seleccione **Confirmed they are up to date (Confirmado que están actualizados)** y haga clic en **Next (Siguiete)**.

Migrate to Strata Cloud Manager

1 - Check latest configuration

Before beginning this migration, please push the latest configuration to all Strata Access device groups. If the latest version is not reflected, the migration may not be confirmed correctly.

Latest Configuration Status			
Device	Last date the configuration was pushed	Pushed By	Job ID
Remote Networks	2024/07/08 15:10:36	admin	7664
Mobile Users	2024/07/08 15:10:38	admin	7665
Mobile Users Explicit Proxy	2024/06/28 11:23:34	admin	4589
Service Connections	2024/07/08 15:10:39	admin	7666

Confirmed they are up to date

STEP 5 | Seleccione el archivo de configuración Panorama .xml que descargó en un paso anterior arrastrándolo y soltándolo o **Choose File (Seleccione el archivo)**.

STEP 6 | Introduzca su **Master Key (Clave maestra)**, o si no creó una **clave maestra** personalizada, pida a Strata Cloud Manager usar la **predeterminada** y haga clic en **Next (Siguiente)**.

The screenshot shows the '2 - Upload Panorama Configuration' step of the migration wizard. At the top, a progress bar indicates the current step (2) and previous steps (1: Check latest configuration, 3: Preparation, 4: Final Confirmation, 5: Migration). The main content area includes instructions to export the latest Panorama configuration XML and a file upload interface. The file '2153.xml' (160 KB) is shown as uploaded. Below the upload section, there are radio buttons for 'Master Key' selection: 'Default' (selected) and 'Input your Master key'. At the bottom right, there are 'Cancel Migration' and 'Next' buttons.

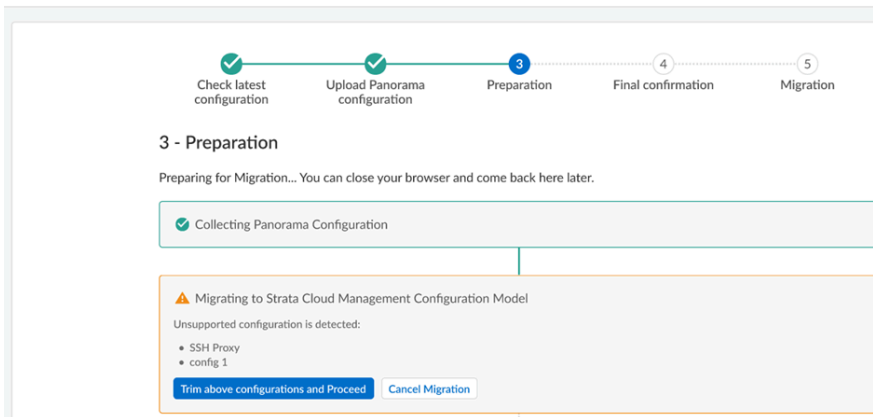
El programa de migración comienza.

The screenshot shows the '3 - Preparation' step of the migration wizard. The progress bar at the top shows steps 1 and 2 as completed, and step 3 as the current step. The main content area displays a list of preparation tasks: 'Collecting Panorama Configuration' (checked), 'Migrating to Strata Cloud Management Configuration Model' (checked), 'Onboarding Strata Cloud Manager Configuration Service (Takes up to 5 minutes)' (loading), 'Loading and Validating Migrated Configuration (Takes up to 5 minutes)' (not started), and 'Generate Push Configuration Changes for Preview' (not started). At the bottom right, there are 'Cancel Migration' and 'Next' buttons.

Espere a que se completen todos los pasos.

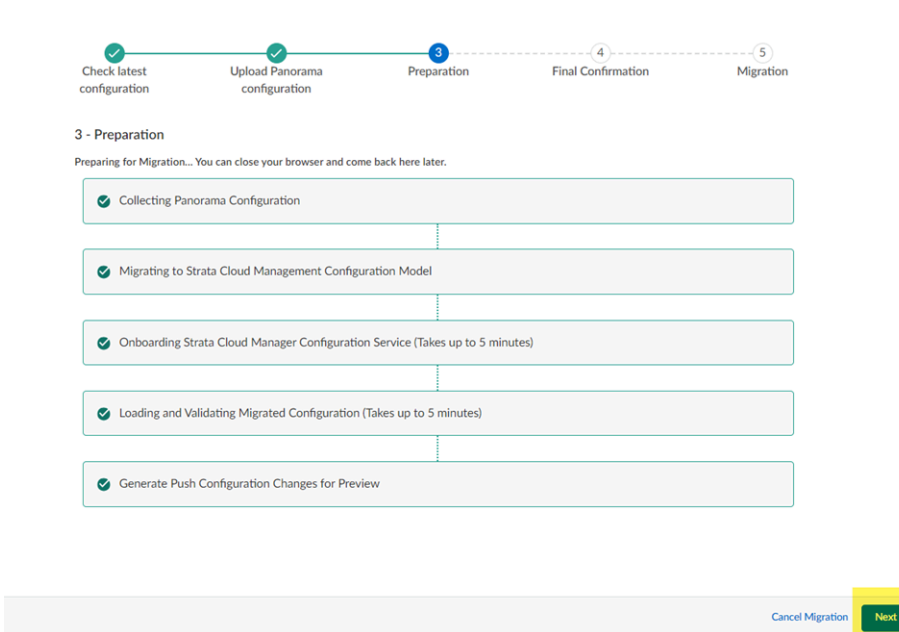
STEP 7 | Si, durante la migración, el programa indica que encontró una **configuración no compatible**, puede **recortar las configuraciones anteriores y continuar** o **cancelar la migración**.

Migrate to Strata Cloud Manager



Algunas configuraciones no compatibles (como una configuración de varios inquilinos) cancelan la migración y el programa de migración no puede resolver el problema; en este caso, opte por **Cancel Migration (Cancelar Migración)**.

STEP 8 | Después de que se complete la migración, haga clic en **Next (Siguiete)**.



STEP 9 | Si el programa de migración realizó cambios, revíselos en la pantalla de confirmación final.

El programa de migración podría hacer cambios en su configuración para tener en cuenta las diferencias en el Panorama y la configuración de Strata Cloud Manager o para corregir funcionalidades no soportadas. Si se requieren cambios, el programa de migración muestra

esos cambios en una vista de diferencias con las nuevas líneas en verde y las líneas eliminadas en rojo.



Ignore cualquier diferencia que muestre los siguientes nombres de objeto; estos no afectan su configuración:

- Clientless-vpn crypto-settings
- Renombrar perfiles hip
- Redundancia de usuario móvil
- Excluir tráfico de vídeo

4 - Final Confirmation

There are differences in the configurations. If everything is OK, click the Complete Migration button.

Cloud Service Plugin Policies and Objects

Prisma Access Mobile Users Mobile Users Explicit Proxy Remote Networks Service Connections

Items (3)

Object Name	Config Diff Type	Object Type	Acknowledge
Backbone Routing	Modified	backbone-routing	<input type="checkbox"/>
Traffic Steering	Deleted	traffic-steering	<input type="checkbox"/>
Cloud_services	Deleted	cloud_services	<input type="checkbox"/>

Backbone Routing	
1 {	1 {
2 - "backbone-routing": "no-asymmetric-routing"	2 + "backbone-routing": "asymmetric-routing-only"
3 }	3 }

STEP 10 | (Opcional) Realizar cambios en las diferencias.

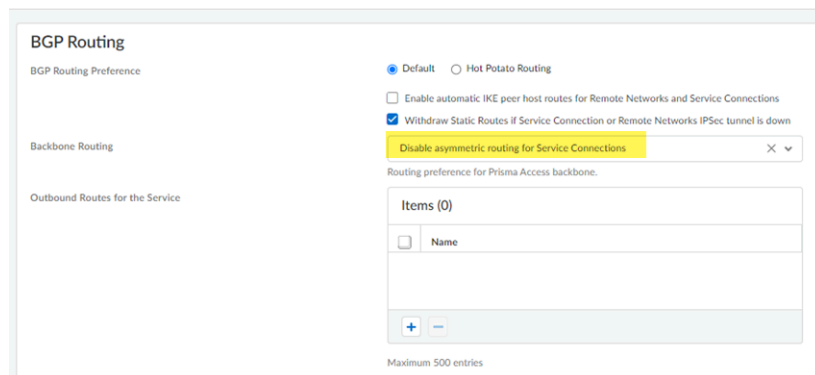
Cualquier cambio que realice no se guardará en su configuración hasta que complete la migración y envíe sus cambios a Strata Cloud Manager.

1. Navegue a la zona en la configuración de Prisma Access donde encontró las diferencias y haga cambios en la configuración.

Para el ejemplo en el paso anterior, el programa de migración realizó un cambio en el enrutamiento de la red troncal (de **no-asymmetric-routing (no-enrutamiento-asimétrico)** a **asymmetric-routing-only (enrutamiento-asimétrico-sólo)**). Para cambiar esta configuración de vuelta a su configuración original, vaya a **Workflows (Flujos de trabajo) > Prisma Access Setup Configuración de Prisma Access > Service Connections (Conexiones de servicio) > Advanced Settings (Configuración avanzada) Configuration (Configuración) > NGFW and (NGFW y) Prisma Access > Configuration Scope (Alcance de la configuración) > Prisma Access > Service Connections (Conexiones de servicio) > Advanced Settings (Configuración avanzada)** y cambie la configuración del **Backbone**

Routing (Enrutamiento de la red troncal) a Disable Asymmetric Routing for Service Connections (Deshabilitar enrutamiento asimétrico para conexiones de servicio).

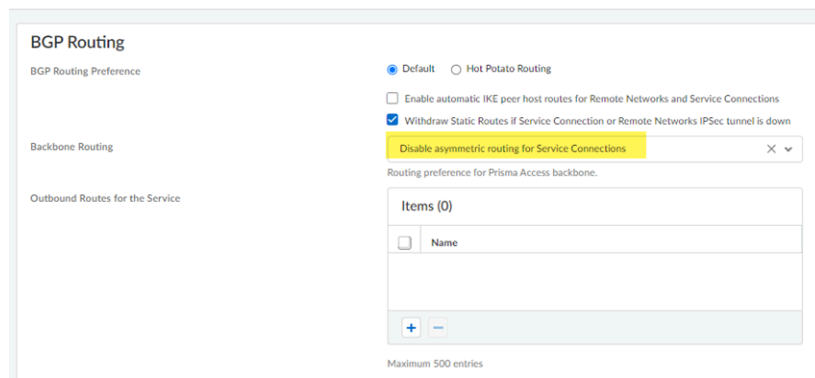
Advanced Settings



2. (Opcional) Para hacer un seguimiento de sus cambios, **reconózclos** a medida que los complete.

Si bien no es obligatorio, puede ser útil reconocer cada cambio a medida que los realice, para que pueda hacer un seguimiento de ellos.

Advanced Settings



3. Continúe revisando los cambios, realice las modificaciones y confírmelos.

STEP 11 | (Opcional) Si ha realizado algún cambio en la configuración, deberá **Regenerate Diffs (Regenerar las diferencias)** para ver las diferencias actualizadas.

The screenshot shows the 'Service Connections' tab in the Strata Cloud Manager interface. It displays a table with two items that have been deleted:

Object Name	Config Diff Type	Object Type	Acknowledge
Onboarding	Deleted	onboarding	<input type="checkbox"/>
Remote Networks	Deleted	remote-networks	<input type="checkbox"/>

Below the table, the configuration for 'Onboarding' is shown in a code editor:

```

1 - {
2   - "entry": {
3     - "@name": "VPN_Sivesa_Nogales",
4     - "ecmp-load-balancing": "disabled",
5     - "ipsec-tunnel": "VPN_Sivesa_Nogales",
6     - "license-type": "FWAAS-5Mbps",
7     - "protocol": {
8       - "bgp": {
9         - "enable": "yes",
10        - "local-ip-address": "192.168.196.189",
11        - "peer-as": "65010",
12        - "peer-ip-address": "192.168.15.21"
13      - }
14    - },
15    - "region": "mexico-central",
16    - "secondary-van-enabled": "no",
17    - "subnets": {
18      - "member": "192.72.208.0/28"
19    - }
20  - }
21 - }
    
```

At the bottom of the interface, there are three buttons: 'Cancel Migration', 'Regenerate Diffs' (highlighted in yellow), and 'Complete Migration'.

STEP 12 | Completar migración:

Si bien no es obligatorio, también puede **Acknowledge (Reconocer)** sus cambios.

Después de Complete Migration (Completar la migración), no puede volver a una implementación gestionada por Panorama y su implementación utiliza permanentemente Strata Cloud Manager para su gestión.

The screenshot shows the '4 - Final Confirmation' step in the Strata Cloud Manager interface. It displays a table with three items that have been updated:

Object Name	Config Diff Type	Object Type	Acknowledge
Internal Dns List	Deleted	internal-dns-list	<input checked="" type="checkbox"/>
Onboarding	Deleted	onboarding	<input checked="" type="checkbox"/>
Service Connection	Created	service-connection	<input checked="" type="checkbox"/>

Below the table, the configuration for 'Service Connection' is shown in a code editor:

```

1 + {
2 +   + "app-blocks-bgp-advertise": "no",
3 +   + "connector-application-blocks": {
4 +     + "member": "10.1.0.0/16"
5 +   + }
6 + }
7 + }
    
```

At the bottom of the interface, there are three buttons: 'Cancel Migration', 'Regenerate Diffs', and 'Complete Migration' (highlighted in yellow).

STEP 13 | (Opcional) Seleccione Go to Configuration Page (Ir a la página de configuración) para ver su configuración migrada.

Migrate to Strata Cloud Manager

5 - Migration
Migration is completed.

Congratulations!
Your migration is completed successfully.
Your Prisma Access deployment is now fully managed through Cloud Management.
The config diff for this migration can be found on the [Config Version Snapshots](#) page.

[Go to Configuration Page](#)

Su implementación migrada se muestra.

Configuration Scope: **Global** | **Overview** | Security Services | Network Policies | Identity Services | Objects

Overview

Folder Name Global (Tenant Name)	Variables 20	Prisma Access Sync Status GlobalProtect: Out of Sync Explicit Proxy: In sync Remote Networks: In sync Service Connections: Out of Sync	Firewall Sync Status In sync (250) Out of Sync (50)
Prisma Access Mobile Users: 1500/2000 Users Remote Networks: 29 Sites Service Connections: 5 Connections	Labels JP, Taiwan	Firewall Connectivity Status In sync (278) Out of Sync (22)	
Firewalls 300			

Config Snippets

- 1 APAC Local Configurations
- 2 Dropbox Snippet
- 3 VPN config Snippet
- 4 GP Snippet
- 6 Root (Inherited)

Support

[Create tech support files](#)

General Information

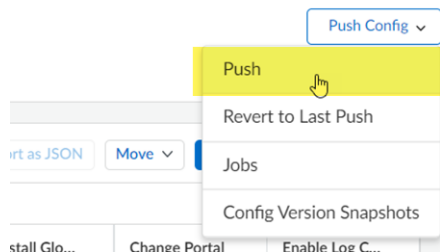
Cloud Management ID	TOSHI-HOME-PA820
Cloud Management Tenant Name	Linux Mails - Prisma Access
Cloud Management Region	us-central1

License

Prisma Access	Prisma Access Enterprise
Edition	Prisma Access Enterprise
Prisma Access Enterprise	2000 Mobile Users & 2000 Net (Mbps)
Expiry Date	15 July 2023 (Expires in 60 days)

STEP 14 | Push Config (Enviar configuración) > Push (Enviar) para aplicar los cambios de configuración migrados.

Esta operación de Envío garantiza que su migración se ha completado con éxito y que Prisma Access ha aplicado todos los cambios a su configuración migrada.



STEP 15 | Tome nota de cualquier mensaje que reciba durante la operación de Envío y, si ve algún problema, realice los cambios necesarios en su configuración.

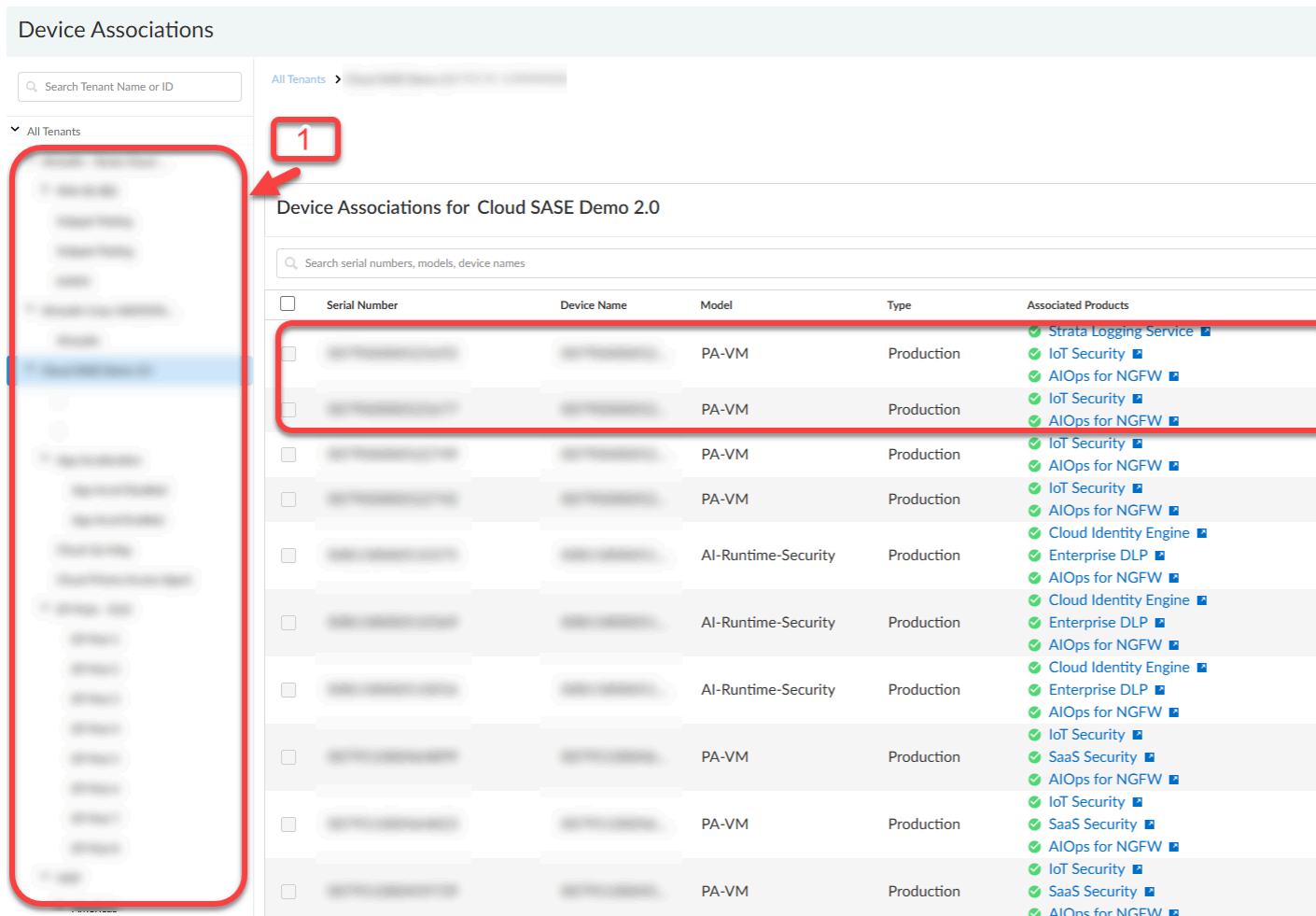
Asociaciones de Dispositivos en Strata Cloud Manager

¿Dónde puedo usar esto?	¿Qué necesito?
<ul style="list-style-type: none"> • Cortafuegos NGFW, incluidos los financiados mediante créditos de Software NGFW 	<p>Uno de estos:</p> <ul style="list-style-type: none"> ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro <p>Si comenzó a usar Strata Cloud Manager antes de que se introdujeran estos niveles de licencia, sus licencias siguen siendo compatibles.</p>

Parte de Strata Cloud Manager y Servicios comunes, **Device Associations** proporciona una vista de gestión centralizada de todos los dispositivos en su implementación. Le permite organizar dispositivos en [grupos de servicios de inquilinos \(TSG\)](#) (contenedores lógicos para organizar dispositivos) y facilita la asociación de productos compatibles con sus dispositivos.

Puede usar Device Associations con los siguientes productos:

- ❑ [Strata Cloud Manager](#)
- ❑ [AIOps for NGFW](#)
- ❑ [IoT Security](#) (Acuerdo de licencia empresarial)
- ❑ [Next-Generation CASB for Prisma Access and NGFW \(CASB-X\)](#)
- ❑ [SaaS Security Inline](#)
- ❑ [Strata Logging Service](#)



1. En **Device Associations (Asociaciones de dispositivos)** [**Settings (Ajustes)** > **Device Associations (Asociaciones de Dispositivos)**], puede ver una lista de todos los **grupos de servicios de inquilinos (TSG)** asociados con su cuenta de soporte al cliente.
 2. Seleccione un Grupo de servicios de inquilino (TSG) para ver cualquier cortafuegos o dispositivo Panorama asociado con él. Si no ve ninguno, puede **Add Devices (Añadir dispositivos)** desde su cuenta de servicio de asistencia al cliente.
 3. Deberá **Add Device (Añadir dispositivo)** siempre que necesite asociar nuevos dispositivos con su TSG.
 4. Después de haber añadido un cortafuegos o dispositivo Panorama, puede **Associate Products (Asociar productos)** para comenzar a usar el dispositivo con los productos que ha activado. La aplicación debe ser compatible con el modelo de hardware de su dispositivo, de lo contrario, el dispositivo no aparecerá durante la asociación de la aplicación.
- [Asociar dispositivos](#)
 - [Asociar Productos](#)
 - [Eliminar asociaciones](#)

Asociaciones de dispositivos (Asociar dispositivos con un inquilino)

Antes de comenzar a utilizar un cortafuegos o un dispositivo Panorama con productos con licencia que haya activado, primero debe asociarlo con el [inquilino](#) en el que haya activado un [producto compatible](#).

STEP 1 | Navegue hasta **Device Associations** usando el hub o Strata Cloud Manager.

1. **(Opcional)** Inicie sesión en el [hub](#) usando sus credenciales de Palo Alto Networks CSP y seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **(Opcional)** Inicie sesión en Strata Cloud Manager y seleccione **Settings (Configuración) > Device Associations (Asociaciones de dispositivos)**.

STEP 2 | Añada el cortafuegos o el dispositivo Panorama a su inquilino.

1. Seleccione **Add Device (Añadir dispositivo)**.

Su **Customer Support Account (Cuenta de servicio de atención al cliente)** se selecciona automáticamente en función de los productos activados en el inquilino en el que se encuentre. Si no ha activado ningún [producto compatible con Device Associations](#), **Add Device (Añadir dispositivo)** aparecerá atenuado.

2. Seleccione uno o más cortafuegos o dispositivos Panorama.
Puede usar un número de serie para buscar un dispositivo específico.
3. **Save (Guardar)**.

STEP 3 | Continúe asociando productos con dispositivos.

Asociaciones de dispositivos (Asociar dispositivos con un producto)

Después de activar la licencia para un [producto compatible](#), use **Device Associations (Asociaciones de dispositivos)** para especificar los cortafuegos o dispositivos Panorama que desea usar con el producto.

STEP 1 | Active su licencia de producto.

La forma de hacerlo depende de la licencia que active. Consulte la documentación específica del producto para obtener más detalles. También puede ver la compatibilidad de la licencia con Strata Cloud Manager aquí.

STEP 2 | Navegue hasta **Device Associations** usando el hub o Strata Cloud Manager.

1. **(Opcional)** Inicie sesión en el [hub](#) usando sus credenciales de Palo Alto Networks CSP y seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **(Opcional)** Inicie sesión en Strata Cloud Manager y seleccione **Settings (Configuración) > Device Associations (Asociaciones de dispositivos)**.

STEP 3 | Asocie productos con cortafuegos o dispositivos Panorama.

1. Seleccione **Associate Products (Asociar productos)**.
2. En la columna Selección de productos, seleccione el producto que desea asociar.
3. Si corresponde, seleccione el tipo de licencia.
Algunos productos tienen licencias para términos de validez y modelos de dispositivo específicos. Solo los dispositivos [compatibles con el tipo de licencia](#) seleccionado aparecerán para la asociación.
4. Seleccionar dispositivos.
5. **Save (Guardar)** o **Apply Licenses (Aplicar licencias)**.

STEP 4 | Verifique que la asociación se realizó correctamente.

Si la asociación falló, copie el ID de error y siga [los pasos para abrir un caso de asistencia técnica](#). Al abrir el caso de asistencia técnica, asegúrese de incluir el ID de error, el número de serie del dispositivo, el ID de TSG y el nombre del producto que falló en la asociación.

STEP 5 | Vuelva a la documentación del producto que está asociando para obtener más pasos de incorporación.

Asociaciones de dispositivos (Eliminar asociaciones de dispositivos)

Es posible que desee eliminar asociaciones de dispositivos si, por ejemplo, va a retirar o devolver un cortafuegos o un dispositivo Panorama, o si desea asociarlo a otro [Grupo de servicio para inquilinos \(TSG\)](#).

Si está intentando [convertir una licencia de prueba a producción](#), convierta la licencia en lugar de desasociarla.

STEP 1 | Navegue hasta **Device Associations** usando el hub o Strata Cloud Manager.

1. **(Opcional)** Inicie sesión en el [hub](#) usando sus credenciales de Palo Alto Networks CSP y seleccione **Common Services (Servicios comunes) > Device Associations (Asociaciones de dispositivos)**.
2. **(Opcional)** Inicie sesión en Strata Cloud Manager y seleccione **Settings (Configuración) > Device Associations (Asociaciones de dispositivos)**.

STEP 2 | Eliminar las asociaciones de productos.

Si desea eliminar un cortafuegos o dispositivo Panorama de su TSG, primero debe eliminar cualquier producto asociado.

1. Seleccione los cortafuegos o dispositivos Panorama cuyos productos desea desvincular.
2. Seleccione **Remove Associations (Eliminar asociaciones) > Remove product association (Eliminar asociación de productos)**.
3. Seleccione los productos que desea eliminar y luego **Remove Associations (Eliminar asociaciones)**.

STEP 3 | Eliminar una asociación de inquilinos.



Puede eliminar asociaciones de inquilinos solo de dispositivos que no tengan asociaciones de aplicaciones. Si el dispositivo está asociado con una aplicación, elimine la asociación de la aplicación antes de continuar.

1. Seleccione los cortafuegos o dispositivos Panorama que desea eliminar de su inquilino.
2. Seleccione **Remove Associations (Eliminar asociaciones) > Remove tenant association (Eliminar asociación de inquilinos)**.
3. Confirme que desea proceder y **Remove (Eliminar)**.

STEP 4 | Si va a eliminar un cortafuegos o un dispositivo Panorama para añadirlo a un nuevo SGT, [asócielo al nuevo SGT](#).

Compatibilidad de modelos de dispositivos

Estos son los modelos de dispositivos que puede asociar a diferentes aplicaciones.

- [AIOps for NGFW o Strata Cloud Manager](#)
- [CASB-X](#)
- [IoT Security](#)
- [SaaS Security](#)

AIOps for NGFW o Strata Cloud Manager

Límite de frecuencia de la	Modelos
Dispositivos virtuales Panorama	<ul style="list-style-type: none"> • PRA-25 • PRA-100 • PRA-1000
VM-SERIES	<ul style="list-style-type: none"> • VM-200 • VM-300 • VM-500 • VM-600 • VM-700
200	<ul style="list-style-type: none"> • 220
400	<ul style="list-style-type: none"> • 410 • 410R • 440 • 445 • 450 • 450R • 460
800	<ul style="list-style-type: none"> • 820 • 850
3000	<ul style="list-style-type: none"> • 3220 • 3250 • 3260 • 3410 • 3420

Límite de frecuencia de la	Modelos
	<ul style="list-style-type: none"> • 3430 • 3440
5000	<ul style="list-style-type: none"> • 5220 • 5250 • 5260 • 5280 • 5410 • 5420 • 5430 • 5445 • 5450
7000	<ul style="list-style-type: none"> • 7050 • 7080

CASB-X

Límite de frecuencia de la	Modelos
200	<ul style="list-style-type: none"> • 220
400	<ul style="list-style-type: none"> • 400 • 410 • 415 • 440 • 445 • 450 • 450R • 460
800	<ul style="list-style-type: none"> • 820 • 850
1000	<ul style="list-style-type: none"> • 1410 • 1420
3000	<ul style="list-style-type: none"> • 3200 • 3220

Límite de frecuencia de la	Modelos
	<ul style="list-style-type: none"> • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
5000	<ul style="list-style-type: none"> • 5220 • 5250 • 5260 • 5280 • 5400 • 5420 • 5430 • 5440 • 5445 • 5450
7000	<ul style="list-style-type: none"> • 7050 • 7080

IoT Security

Esta tabla contiene solo los modelos de dispositivos que puede asociar con IoT Security en Device Associations. La tabla no contiene información sobre las [funciones disponibles con diferentes modelos de dispositivos y combinaciones de versiones de PAN-OS](#) de IoT Security.

Límite de frecuencia de la	Modelos
VM-SERIES	<ul style="list-style-type: none"> • VM-100 • VM-300 • VM-500 • VM-700
200	<ul style="list-style-type: none"> • 200 • 220 • 220R
400	<ul style="list-style-type: none"> • 410

Límite de frecuencia de la	Modelos
	<ul style="list-style-type: none"> • 410R • 440 • 450 • 450R • 460
500	<ul style="list-style-type: none"> • 500
800	<ul style="list-style-type: none"> • 820 • 850
3000	<ul style="list-style-type: none"> • 3020 • 3050 • 3060 • 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
7000	<ul style="list-style-type: none"> • 7050 • 7080

SaaS Security

Esta tabla contiene solo los modelos de dispositivos que puede asociar con SaaS Security en Device Associations. La tabla no contiene información sobre las [funciones disponibles con diferentes modelos de dispositivos y combinaciones de versiones de PAN-OS](#) de SaaS Security.

Límite de frecuencia de la	Modelos
200	<ul style="list-style-type: none"> • 220 • 220R
400	<ul style="list-style-type: none"> • 410 • 410R • 440 • 440R

Límite de frecuencia de la	Modelos
	<ul style="list-style-type: none"> • 450 • 450R • 460 • 460R
800	<ul style="list-style-type: none"> • 820 • 850
3000	<ul style="list-style-type: none"> • 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
5000	<ul style="list-style-type: none"> • 5220 • 5250 • 5260 • 5280 • 5410 • 5420 • 5430 • 5450
7000	<ul style="list-style-type: none"> • 7050 • 7080

Compatibilidad entre tipos de cortafuegos y licencias

Algunas suscripciones de productos tienen diferentes tipos de licencia, lo que las hace compatibles con solo tipos específicos de cortafuegos y dispositivos. Cuando [asocia productos con dispositivos](#) y selecciona la licencia de producto, solo aparecerán los dispositivos que correspondan al tipo de licencia. Sin embargo, algunos tipos de licencia, como Eval, Trial y Acuerdo de licencia empresarial (ELA) son compatibles con cualquier modelo de cortafuegos.

Un tipo de cortafuegos se define por el SKU del cortafuegos. Para ver el SKU de un cortafuegos, inicie sesión en su cuenta del Portal de atención al cliente, seleccione **Assets (Activos) > Devices (Dispositivos)** y compruebe el número de serie de su cortafuegos en la columna Nombre del modelo. Este es el SKU, que indica el tipo de cortafuegos de la siguiente manera:

- Un SKU de producción termina con el nombre del modelo de cortafuegos; por ejemplo, PAN-PA-410
- Un SKU de evaluación termina con -E60, que significa *Eval + 60 días*; por ejemplo, PAN-PA-410-E60
- Un SKU de laboratorio termina con -LAB; por ejemplo, PAN-PA-410-LAB

Consulte a continuación los cortafuegos y las combinaciones de tipos de licencia que admite su aplicación.

- [#unique_38](#)
- [AIOps for NGFW](#)
- [IoT Security](#)
- [SaaS Security Inline](#)

AIOps for NGFW

Tipos de licencia de AIOps for NGFW	Tipos cortafuegos			
	NFR	LAB	PROD	EVAL
PRUEBA	No	Sí	Sí	Sí
EVAL	No	Sí	Sí	Sí
NFR	Sí	No	No	No
LAB	No	Sí	No	No
PROD	No	No	Sí	No

IoT Security

Tipos de licencia de IoT Security	Tipos cortafuegos			
	NFR	LAB	PROD	EVAL
PRUEBA	No	Sí	Sí	Sí
EVAL	No	Sí	Sí	Sí
NFR	Sí	No	No	No
LAB	No	Sí	No	No
PROD	No	No	Sí	No

SaaS Security Inline

Tipos de licencia de SaaS Security Inline	Tipos cortafuegos			
	NFR	LAB	PROD	EVAL
PRUEBA	No	Sí	Sí	Sí
EVAL	No	Sí	Sí	Sí
NFR	Sí	No	No	No
LAB	No	Sí	No	No
PROD	No	No	Sí	No