paloalto
TECHDOCS

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

April 16, 2026

Table of Contents

Licencias AI Access Security 5

¿Qué incluye una licencia AI Access Security? 6

Requisitos previos de configuración de AI Access Security 11

Activar la licencia de AI Access Security 15

Convertir una licencia de evaluación de AI Access Security a otra de Producción 29

Renovar una licencia AI Access Security 31

Licencias AI Access Security

Revise las licencias de AI Access Security disponibles para comenzar a adoptar y controlar de forma segura aplicaciones de IA generativa (GenAI) en su red.

- **Licencia de AI Access Security**

  La licencia AI Access Security es una licencia independiente. Incluye los siguientes tres tipos de licencia:

  - **AI Access Security EVAL**: licencia de evaluación para AI Access Security. Si tiene activa la licencia EVAL, debe convertir la licencia de evaluación en una licencia de producción una vez finalizado el período de evaluación para continuar controlando de forma segura el acceso a las aplicaciones GenAI y adoptarlas de forma segura.
  - **AI Access Security LAB**: licencia de AI Access Security específica para sus entornos de laboratorio. Esta licencia no está destinada a un entorno de producción.
  - **AI Access Security**: licencia de producción para AI Access Security.
- **CASB-PA y CASB-X**

  AI Access Security se incluye de forma predeterminada con las licencias CASB-PA y CASB-X. No se requiere medidas adicionales para activar AI Access Security. Puede comenzar a usar AI Access Security para adoptar aplicaciones GenAI de forma segura después de activar cualquiera de estas licencias.
- **Prisma Browser** **Licencia independiente**

  AI Access Security se incluye de forma predeterminada con la licencia independiente de Prisma Browser. No se requiere medidas adicionales para activar AI Access Security. Puede comenzar a usar AI Access Security para adoptar aplicaciones GenAI de forma segura después de activar esta licencia.

¿Qué incluye una licencia AI Access Security?

Qué se incluye con AI Access Security depende de si otras licencias están activas en el inquilino.

La funcionalidad de AI Access Security incluida depende de la versión de PAN-OS o plano de datos que se esté ejecutando actualmente en el inquilino de NGFW o Prisma Access. Consulte los requisitos previos de configuración para obtener más información sobre qué funcionalidad se incluye.

- **AI Access Security sólo**

  Esto se aplica a l NGFW o Prisma Access gestionado por Panorama o Strata Cloud Manager cuando solo la licencia de AI Access Security está activa.

Versión de plano de datos o PAN-OS	NGFW y Prisma Access (gestionado por Panorama o Strata Cloud Manager)
11.2.2-h1 y posteriores Prisma Access 5.1 Innovation y posteriores	• Visibilidad de más de 2.250 aplicaciones GenAI entregadas a través de actualizaciones de contenido dinámico y App-ID Cloud Engine (ACE). • Definir reglas de políticas para controlar el acceso a las aplicaciones GenAI y a las aplicaciones no GenAI. • Inspección de Enterprise DLP y representación de veredictos solo para aplicaciones GenAI compatibles. Las coincidencias de tráfico que contengan datos confidenciales no se reenvían a Enterprise DLP para la inspección y representación de veredictos en aplicaciones no GenAI. • Acceder a Strata Cloud Manager Command Center para obtener visibilidad de GenAI. • Acceda al panel de Activity Insights de AI Access Security para ver los datos detallados de uso de aplicaciones GenAI, los usuarios y los casos de uso de GenAI más comunes que se producen en su red. • Etiquete aplicaciones GenAI en Strata Cloud Manager para reflejar si la aplicación está aprobada dentro de su organización y para la aplicación de políticas basadas en etiquetas. AI Access Security no sincroniza etiquetas de aplicaciones GenAI con Panorama. • Generar informes solo para las aplicaciones GenAI descubiertas. • Vea las aplicaciones GenAI en el diccionario de aplicaciones para obtener más información sobre aplicaciones, proveedores, cumplimiento y características de riesgo específicos de GenAI que subyacen a esas aplicaciones SaaS. • Vea las aplicaciones GenAI instaladas como aplicaciones / complementos conectados de terceros en 7 aplicaciones del mercado SaaS.

Versión de plano de datos o PAN-OS	NGFW y Prisma Access (gestionado por Panorama o Strata Cloud Manager)
	• Visibilidad y control de los datos en reposo que residen en la aplicación ChatGPT Enterprise.

- **Licencias AI Access Security y Enterprise DLP**

  Esto se aplica a NGFW o Prisma Access gestionado por Panorama o Strata Cloud Manager cuando las licencias AI Access Security y Enterprise DLP están activas.

Versión de plano de datos o PAN-OS	NGFW y Prisma Access (gestionado por Panorama o Strata Cloud Manager)
11.2.2-h1 y posteriores Prisma Access 5.1 Innovation y posteriores	• Visibilidad de más de 2.250 aplicaciones GenAI entregadas a través de actualizaciones de contenido dinámico y App-ID Cloud Engine (ACE). • Definir reglas de políticas para controlar el acceso a las aplicaciones GenAI y a las aplicaciones no GenAI. • Inspección de Enterprise DLP y emisión de veredictos para aplicaciones GenAI y no GenAI compatibles. • Acceder a Strata Cloud Manager Command Center para obtener visibilidad de GenAI. • Acceda al panel de Activity Insights de AI Access Security para ver los datos detallados de uso de aplicaciones GenAI, los usuarios y los casos de uso de GenAI más comunes que se producen en su red. • Etiquete aplicaciones GenAI en Strata Cloud Manager para reflejar si la aplicación está aprobada dentro de su organización y para la aplicación de políticas basadas en etiquetas. AI Access Security no sincroniza etiquetas de aplicaciones GenAI con Panorama. • Generar informes solo para las aplicaciones GenAI descubiertas. • Vea las aplicaciones GenAI en el diccionario de aplicaciones para obtener más información sobre aplicaciones, proveedores, cumplimiento y características de riesgo específicos de GenAI que subyacen a esas aplicaciones SaaS. • Vea las aplicaciones GenAI instaladas como aplicaciones / complementos conectados de terceros en 7 aplicaciones del mercado SaaS. • Visibilidad y control de los datos en reposo que residen en la aplicación ChatGPT Enterprise.

- **Licencias CASB-PA y CASB-X**

  Esto se aplica a NGFW o Prisma Access gestionada por Strata Cloud Manager cuando las licencias CASB-PA o CASB-X están activas.

Versión de plano de datos o PAN-OS	CASB-PA y CASB-X

10.2
11.1
Prisma Access 5.0 Preferred e Innovation
Prisma Access 5.1 Preferred y posterior
	• Visibilidad de más de 2.250 aplicaciones GenAI entregadas a través de actualizaciones de contenido dinámico y App-ID Cloud Engine (ACE).
	• Definir reglas de políticas para controlar el acceso a las aplicaciones GenAI y a las aplicaciones no GenAI.
	• Inspección de Enterprise DLP y emisión de veredictos para aplicaciones GenAI y no GenAI compatibles.
	• Acceder a Strata Cloud Manager Command Center para obtener visibilidad de GenAI.
	• Acceda al panel de Activity Insights de AI Access Security para ver los datos detallados de uso de aplicaciones GenAI, los usuarios y los casos de uso de GenAI más comunes que se producen en su red.
	• Vea lo siguiente para todas las aplicaciones SaaS Inline, incluidas las aplicaciones GenAI:
	  • Paneles
	  • Usuarios
	  • Diccionario de aplicaciones
	  • Aplicaciones
	  • Informes
	  • Recomendaciones de políticas
	• Ver todos los complementos de terceros (SSPM), incluidos los complementos GenAI.
	• Ver detalles de activos de todas las aplicaciones SaaS autorizadas (datos en reposo), incluidas las aplicaciones GenAI.

11.2.2-h1 y posteriores Prisma Access 5.1 Innovation y posteriores	• Visibilidad de más de 2.250 aplicaciones GenAI entregadas a través de actualizaciones de contenido dinámico y App-ID Cloud Engine (ACE). • Definir reglas de políticas para controlar el acceso a las aplicaciones GenAI y a las aplicaciones no GenAI. • Inspección de Enterprise DLP y emisión de veredictos para aplicaciones GenAI y no GenAI compatibles. • Acceder a Strata Cloud Manager Command Center para obtener visibilidad de GenAI.

Versión de plano de datos o PAN-OS	CASB-PA y CASB-X

	• Acceda al panel de Activity Insights de AI Access Security para ver los datos detallados de uso de aplicaciones GenAI, los usuarios y los casos de uso de GenAI más comunes que se producen en su red.
	• Etiquete aplicaciones GenAI en Strata Cloud Manager para reflejar si la aplicación está aprobada dentro de su organización y para la aplicación de políticas basadas en etiquetas.
	AI Access Security no sincroniza etiquetas de aplicaciones GenAI con Panorama.
	• Vea lo siguiente para todas las aplicaciones SaaS Inline, incluidas las aplicaciones GenAI:
	  • Paneles
	  • Usuarios
	  • Diccionario de aplicaciones
	  • Aplicaciones
	  • Informes
	  • Recomendaciones de políticas
	• Ver todos los complementos de terceros (SSPM), incluidos los complementos GenAI.
	• Ver detalles de activos de todas las aplicaciones SaaS autorizadas (datos en reposo), incluidas las aplicaciones GenAI.

Requisitos previos de configuración de AI Access Security

Revisar los requisitos previos para usar AI Access Security. Los requisitos previos describen las versiones mínimas de planos de datos PAN-OS y Prisma Access, y los servicios adicionales necesarios para utilizar AI Access Security.

Revise las diferentes combinaciones de licencias de AI Access Security y versiones de PAN-OS para obtener más información sobre la funcionalidad que AI Access Security admite.

- **NGFW y Prisma Access (gestionado por Panorama)**

  Consulte los requisitos previos de la **licencia de AI Access Security** cuando gestione su configuración de AI Access Security desde Panorama y solo tenga activa la licencia de AI Access Security.

  Consulte los requisitos previos de licencias **CASB PA y CASB-X** cuando gestione su configuración de AI Access Security desde Panorama y tenga una licencia CASB PA o CASB-X activa.

Requisito previo	Licencia de AI Access Security	Licencias CASB-PA y CASB-X
PAN-OS o plano de datos	PAN-OS 11.2.2-h1	• PAN-OS 10.2.3 y Prisma Access 5.0 Preferred e Innovation • PAN-OS 11.1.0 y Prisma Access 5.1 Preferred • PAN-OS 11.2.2-h1 y Prisma Access 5.1 Innovation Revise las Notas de versión de Prisma Access para obtener los detalles mínimos requeridos de la versión de Prisma Access.
Data Filtering	Complemento de Enterprise DLP 5.0.4 o posterior	Revise la matriz de compatibilidad para la versión del complemento de Enterprise DLP compatible con su versión de PAN-OS.

Requisito previo	Licencia de AI Access Security	Licencias CASB-PA y CASB-X
	AI Access Security incluye Enterprise DLP cuando activa las licencias CASB-PA, AI Access Security y CASB-X.	
Gestión	Strata Cloud Manager Essentials o Strata Cloud Manager Pro Obtenga más información sobre lo que incluye cada licencia.	n/c
Complemento de servicios en la nube	Complemento de servicios en la nube 5.1	
Registro de logs	Strata Logging Service	

- **NGFW y Prisma Access (gestionado por Strata Cloud Manager)**

  Consulte los requisitos previos de la **licencia de AI Access Security** cuando gestione su configuración de AI Access Security desde Strata Cloud Manager y solo tenga activa la licencia de AI Access Security.

  Consulte los requisitos previos de las licencias **CASB PA y CASB-X** cuando gestione su configuración de AI Access Security desde Strata Cloud Manager y tenga una licencia CASB PA o CASB-X activada.

Requisito previo	Licencia de AI Access Security	Licencias CASB-PA y CASB-X
PAN-OS o plano de datos	PAN-OS 11.2.2-h1	• PAN-OS 10.2.3 y Prisma Access 5.0 Preferred e Innovation • PAN-OS 11.1.0 y Prisma Access 5.1 Preferred • PAN-OS 11.2.2-h1 y Prisma Access 5.1 Innovation Revise las Notas de versión de Prisma Access para obtener los detalles mínimos requeridos de la versión de Prisma Access.
Data Filtering	AI Access Security incluye Enterprise DLP cuando activa las licencias CASB-PA, AI Access Security y CASB-X.	

Requisito previo	Licencia de AI Access Security	Licencias CASB-PA y CASB-X
Gestión	Strata Cloud Manager Essentials o Strata Cloud Manager Pro Obtenga más información sobre lo que incluye cada licencia.	n/c
Registro de logs	Strata Logging Service	

Activar la licencia de AI Access Security

Active su licencia AI Access Security para permitir que su organización adopte de forma segura aplicaciones de IA generativa (GenAI) para el uso por parte de sus empleados. La activación de AI Access Security se realiza mediante un enlace mágico proporcionado por Palo Alto Networks después de la compra de la licencia AI Access Security. Estos procedimientos asumen que ya tiene todos los códigos de autenticación de licencia y enlaces mágicos necesarios para la activación.

Después de comprar su licencia de AI Access Security, debe activar la licencia mediante un enlace mágico que se le envía a través de Palo Alto Networks. La AI Access Security se incluye cuando activa una licencia CASB-PA o CASB-X. No se requiere ninguna otra acción para activar la AI Access Security después de activar una licencia CASB-PA o CASB-X.

- Nuevas implementaciones
- Implementaciones existentes

Activar la Licencia AI Access Security (Nuevas Implementaciones)

STEP 1 | Instalar y realizar la configuración inicial para su NGFW.

Esto incluye activar todas las licencias de asistencia requeridas.

STEP 2 | Configurar la gestión para su NGFW o inquilino de Prisma Access.

- **NGFW (Managed by Panorama)**
  1. Configurar Panorama.
     - **Dispositivo M-Series**: Configure el dispositivo M-Series en modo Solo Gestión o Modo Panorama.
     - **Panorama Dispositivo Virtual**: Instalar el dispositivo virtual Panorama en su hipervisor preferido en modo Solo Gestión o modo Panorama
  2. Implementar Strata Logging Service.
  3. Registrar Panorama.
  4. Activar la licencia de asistencia Panorama.
  5. Activar la licencia de gestión del dispositivo Panorama (Dispositivo M-Series o Panorama Dispositivo Virtual).
  6. Añadir sus cortafuegos gestionados a la gestión de Panorama.
  7. Actualizar Panorama a la versión mínima de PAN-OS compatible con AI Access Security.
  8. Actualizar su NGFW a la versión mínima de PAN-OS compatible con AI Access Security.
- **NGFW (Managed by Strata Cloud Manager)**
  1. Implementar Strata Logging Service.

     Strata Cloud Manager requiere Strata Logging Service para el registro.
  2. Activar la licencia Strata Cloud Manager Essentials o Strata Cloud Manager Pro.
  3. Incorporar su NGFW a Strata Cloud Manager.
  4. Instalar las últimas actualizaciones de contenido dinámico y actualizar su NGFW a la versión mínima de PAN-OS compatible con AI Access Security.
- **Prisma Access (Managed by Panorama)**
  1. Configurar Panorama.
     - **Dispositivo M-Series**: Configure el dispositivo M-Series en modo Solo Gestión o Modo Panorama.
     - **Panorama Dispositivo Virtual**: Instalar el dispositivo virtual Panorama en su hipervisor preferido en modo Solo Gestión o modo Panorama
  2. Implementar Strata Logging Service.
  3. Registrar Panorama.
  4. Activar la licencia de asistencia Panorama.
  5. Activar la licencia de gestión del dispositivo Panorama (Dispositivo M-Series o Panorama Dispositivo Virtual).
  6. Actualizar Panorama a la versión mínima de PAN-OS compatible con AI Access Security.
  7. Instalar el complemento de servicios en la nube en Panorama.
  8. Configurar Panorama Managed Prisma Access
- **Prisma Access (Managed by Strata Cloud Manager)**
  1. Implementar Strata Logging Service.

Strata Cloud Manager requiere Strata Logging Service para el registro.

2. Activar la licencia de Prisma Access on Strata Cloud Manager.
3. Configurar Prisma Access

STEP 3 | Configurar Enterprise Data Loss Prevention (E-DLP).

- **NGFW (Managed by Panorama)**
  1. Instalar el complemento de Enterprise DLP en Panorama.
  2. Habilitar Enterprise DLP para NGFW.
  3. Editar el contenido en la nube, filtrado de datos y configuraciones de fragmentos de Enterprise DLP según sea necesario.
- **NGFW (Managed by Strata Cloud Manager)**
  1. Habilitar Enterprise DLP para NGFW.
  2. Edita el filtrado de datos y la configuración de fragmentos de Enterprise DLP según sea necesario.
- **Prisma Access (Managed by Panorama)**
  1. Instalar el complemento de Enterprise DLP en Panorama.
  2. Habilitar Enterprise DLP para Prisma Access.
  3. Editar el contenido en la nube, filtrado de datos y configuraciones de fragmentos de Enterprise DLP según sea necesario.
- **Prisma Access (Managed by Strata Cloud Manager)**
  1. Habilitar Enterprise DLP para NGFW.
  2. Edita el filtrado de datos y la configuración de fragmentos de Enterprise DLP según sea necesario.

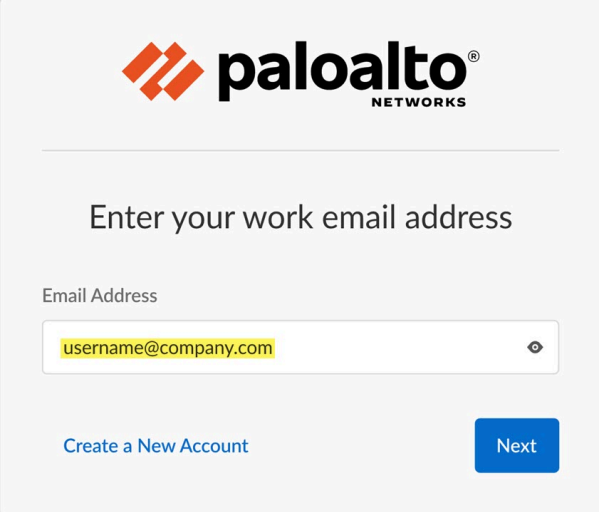
STEP 4 | Haga clic en el enlace mágico proporcionado por Palo Alto Networks cuando compra la suscripción de AI Access Security.

STEP 5 | Haga clic en **Activate Subscription (Activar suscripción)** para comenzar a activar AI Access Security.

STEP 6 | Introduzca la **Email Address (Dirección de correo electrónico)**. del Portal de asistencia al cliente (CSP) de Palo Alto Networks Esta dirección de correo electrónico debe coincidir con la dirección de correo electrónico que recibió el enlace mágico para activar AI Access Security.

Deberá **Create a New Account (Crear una nueva cuenta)** si la dirección de correo electrónico que recibió el enlace de activación de AI Access Security no tiene ya una cuenta CSP válida.

La cuenta recién creada se asocia automáticamente con el mismo inquilino para el cual está activando AI Access Security y se le asigna un rol de superusuario multiinquilino.



STEP 7 | (Multitenencia solo) En la sección **Customer Support Account (Cuenta de servicio de atención al cliente)**, seleccione la Cuenta de servicio de atención al cliente de Palo Alto Networks asociada con el inquilino para el cual estás activando la licencia de AI Access Security.

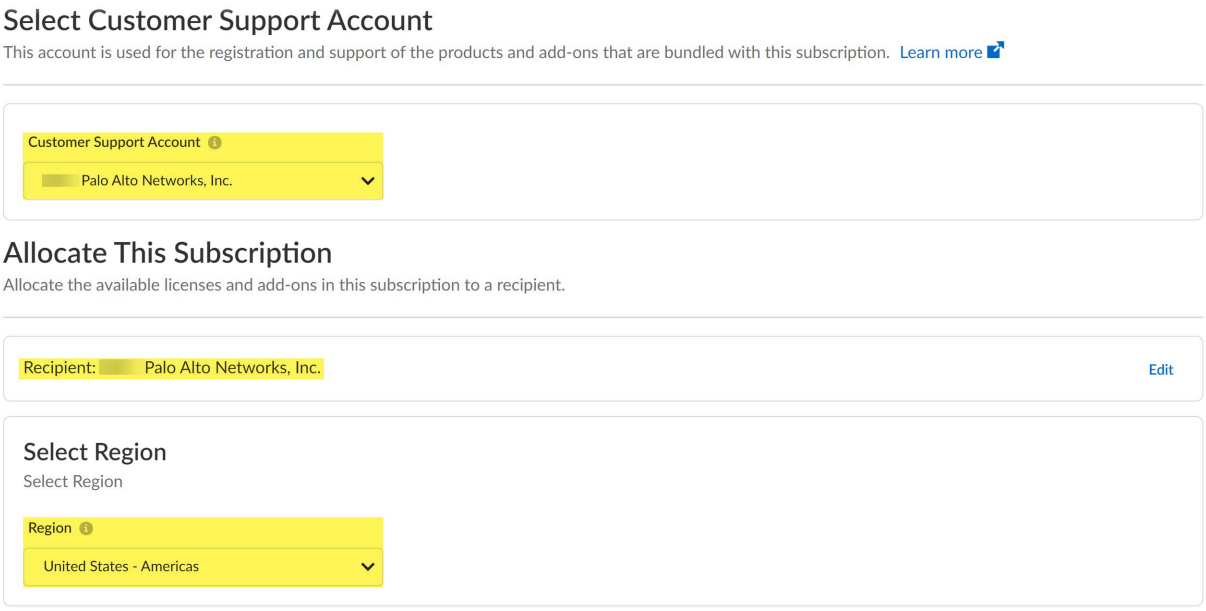
Sáltese este paso si tiene una cuenta de Cuenta de servicio de atención al cliente de un solo inquilino. Su Cuenta de servicio de atención al cliente está seleccionada por defecto.

STEP 8 | (Multitenencia solo) En la sección **Allocate This Subscription (Asignar esta suscripción)**, seleccione el grupo de servicios de inquilino (TSG) para el cual desea activar AI Access Security. Puede seleccionar el inquilino principal o un inquilino secundario.

AI Access Security está activado solo para el inquilino seleccionado. Si selecciona un inquilino principal, AI Access Security no se activa para ningún inquilino secundario.

Sáltese este paso si solo tiene una cuenta de Cuenta de servicio de atención al cliente de un solo inquilino. Está seleccionado por defecto.

STEP 9 | Revisa la **Region (Región)** del inquilino. Esta región se completa automáticamente según la región del inquilino de NGFW o Prisma Access implementado y no se puede cambiar.

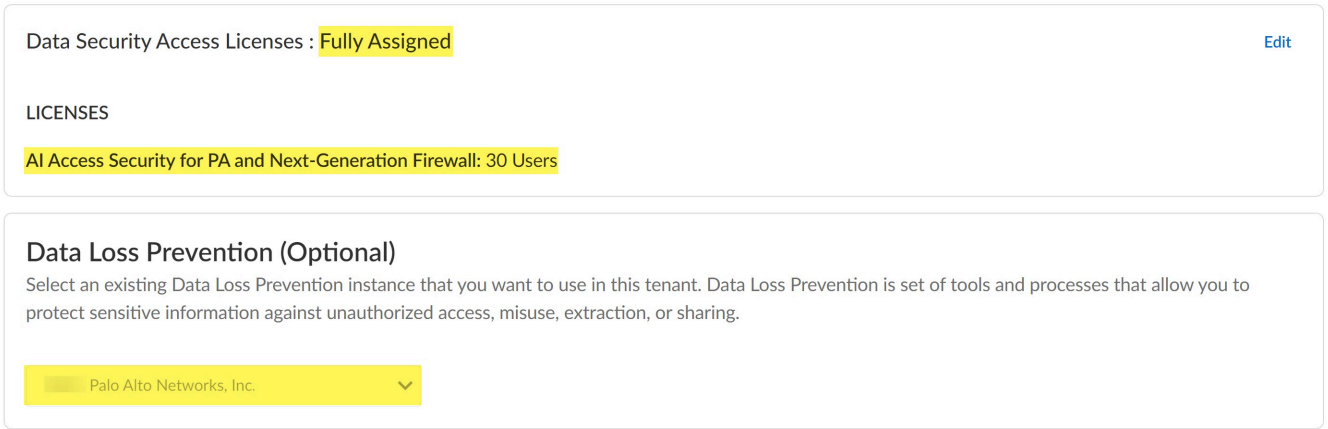


STEP 10 | En la sección **Assign Licenses (Asignar licencias)**, haga clic en **Done (Listo)** para asignar todas sus licencias de AI Access Security. Verifique que su **Licencia de AI Access Security** esté `Completamente asignada`

STEP 11 | Verifique que su instancia de **Data Loss Prevention** esté seleccionada si tiene Enterprise Data Loss Prevention (E-DLP) activa en su inquilino.

Su Enterprise DLP está seleccionada de forma predeterminada si ya está activa en su inquilino.

Sáltese este paso si no tiene Enterprise DLP ya activa. Enterprise DLP no es necesario para habilitar AI Access Security. Si la instancia de Enterprise DLP no está ya activa, se crea una como parte de la activación de la licencia. Revise qué sucede con Enterprise DLP si no renueva su licencia de AI Access Security.

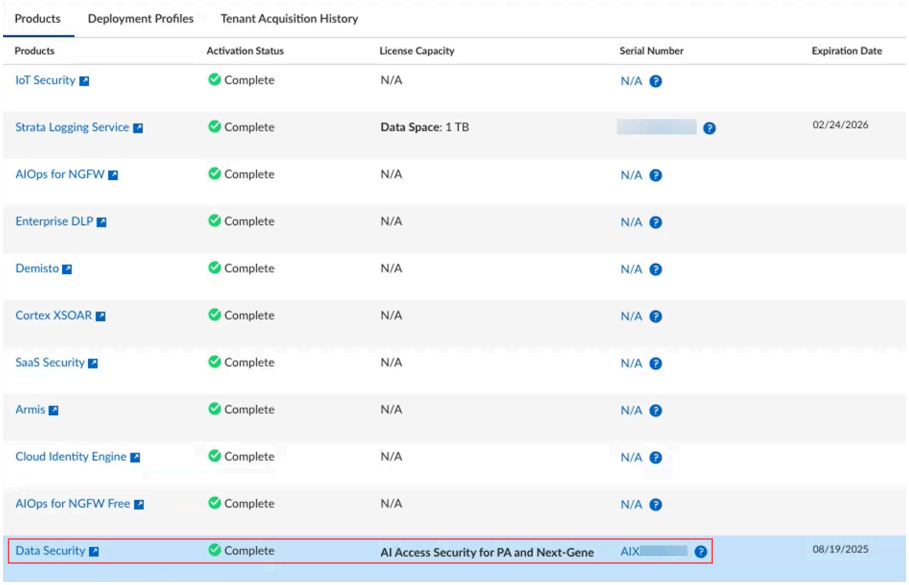


STEP 12 | Deberá **Agree to the Terms and Conditions (Aceptar las condiciones)**.

STEP 13 | **Activate (Activar)**.

Es redirigido a la página de Gestión de inquilinos donde el **Activation Status (Estado de activación)** de AI Access Security comienza `Inicializando`.

La licencia de AI Access Security se muestra como **Data Security (Seguridad de los datos)** y tiene un número de serie que comienza con `AIX`. Continúe al siguiente paso después de que el **Activation Status (Estado de activación)** esté `Completo`.



STEP 14 | (Solo NGFW) Asocia la licencia AI Access Security con su NGFW.

Es necesario asociar la licencia de AI Access Security para activar la licencia para su NGFW.

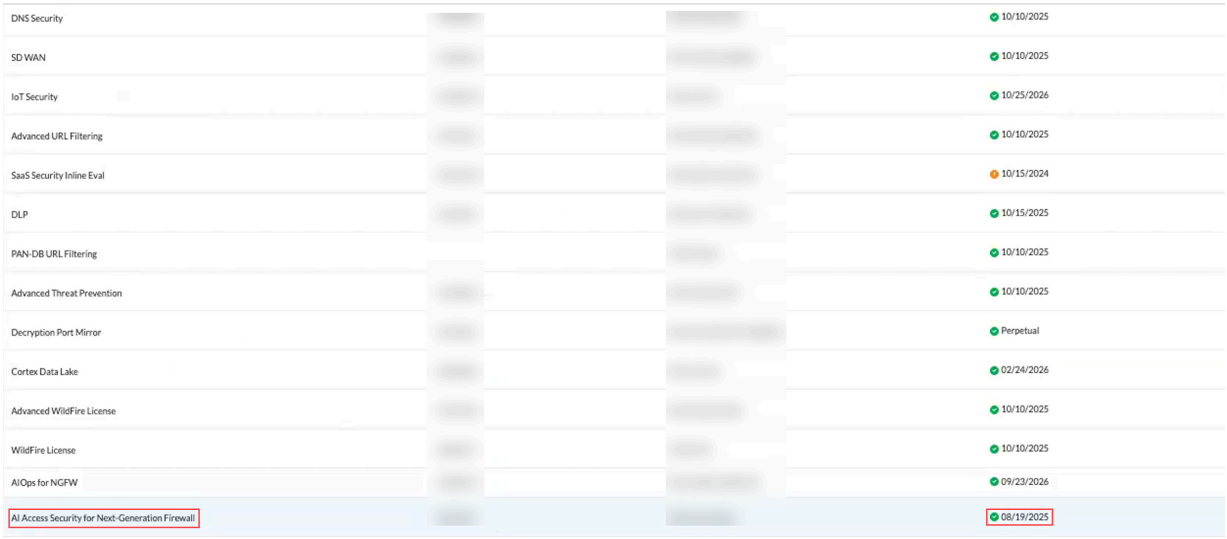
1. En el menú Strata Cloud Manager, seleccione **Settings (Configuración)** > **Device Associations (Asociaciones de dispositivos)**.

   El menú de Strata Cloud Manager se encuentra en la esquina inferior izquierda de Strata Cloud Manager.
2. En el menú Strata Cloud Manager, seleccione **System Settings (Configuración del sistema)** > **Device Associations (Asociaciones de dispositivos)**.

   El menú de Strata Cloud Manager se encuentra en la esquina inferior izquierda de Strata Cloud Manager.
3. **Associate Apps (Asociar aplicaciones)**.
4. En los Productos con licencia, seleccione **Data Security (Seguridad de datos)**.
5. Seleccione el NGFW para el cual desea activar AI Access Security.
6. **Save (Guardar)**.

STEP 15 | Verifique que activó AI Access Security correctamente.

1. Inicie sesión en el Portal de atención al cliente (CSP) de Palo Alto Networks.
2. Seleccione **Products (Productos)** > **Assets (Activos)**.
3. Seleccione el inquilino **NGFW** o **Prisma Access** basado en el punto de aplicación para el cual activó AI Access Security.
4. Utilice los filtros para localizar su NGFW o inquilino Prisma Access.
5. Expanda la lista de licencias activas o haga clic en **Licenses & Subscriptions (Licencias y suscripciones)**.
6. Verifique que la licencia de AI Access Security esté activa.



STEP 16 | Empezar con AI Access Security

Activar la licencia AI Access Security (implementaciones existentes)

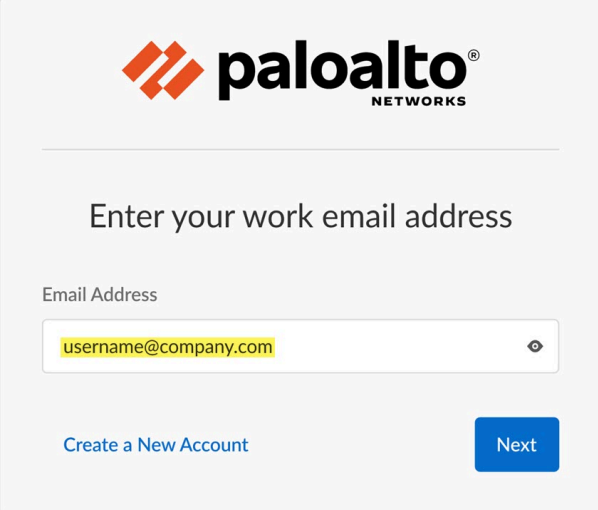
Este procedimiento asume que solo necesita activar la licencia de AI Access Security y que todas las licencias de requisitos previos están activadas y han configurado correctamente sus NGFW, Prisma Access, Panorama® management server y Strata Cloud Manager según sea necesario.

STEP 1 | Haga clic en el enlace mágico proporcionado por Palo Alto Networks cuando compra la suscripción de AI Access Security.

STEP 2 | Haga clic en **Activate Subscription (Activar suscripción)** para comenzar a activar AI Access Security.

STEP 3 | Introduzca la **Email Address (Dirección de correo electrónico)**. del Portal de asistencia al cliente (CSP) de Palo Alto Networks Esta dirección de correo electrónico debe coincidir con la dirección de correo electrónico que recibió el enlace mágico para activar AI Access Security.

Deberá **Create a New Account (Crear una nueva cuenta)** si la dirección de correo electrónico que recibió el enlace de activación de AI Access Security no tiene ya una cuenta CSP válida. La cuenta recién creada se asocia automáticamente con el mismo inquilino para el cual está activando AI Access Security y se le asigna un rol de superusuario multiinquilino.



STEP 4 | (Multitenencia solo) En la sección **Customer Support Account (Cuenta de servicio de atención al cliente)**, seleccione la Cuenta de servicio de atención al cliente de Palo Alto Networks asociada con el inquilino para el cual estás activando la licencia de AI Access Security.

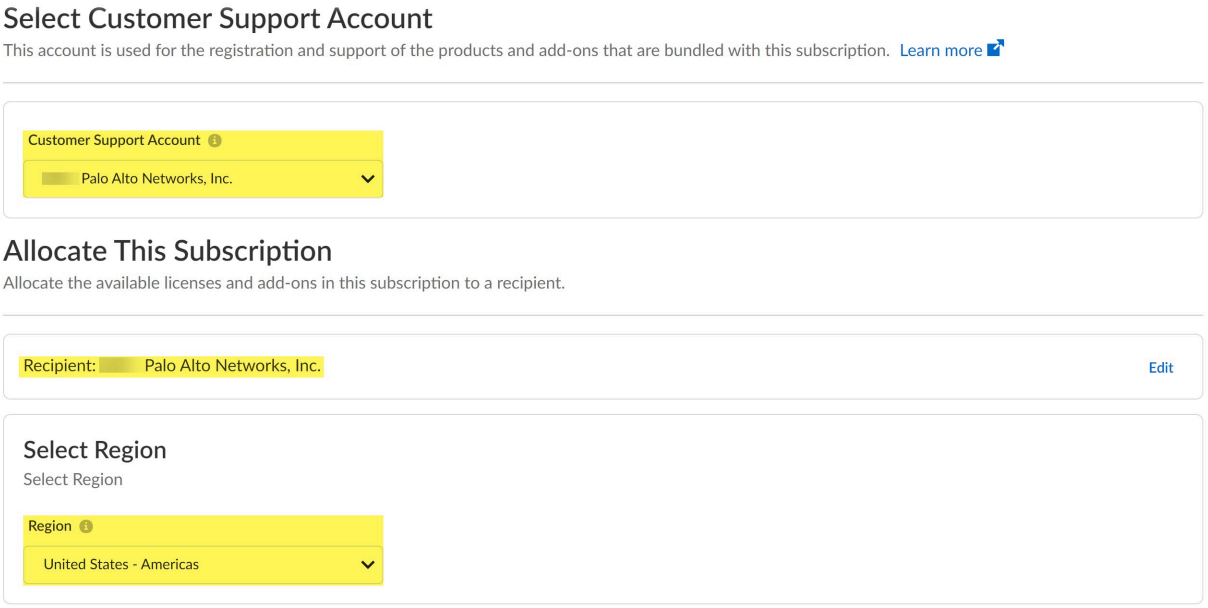
Sáltese este paso si tiene una cuenta de Cuenta de servicio de atención al cliente de un solo inquilino. Su Cuenta de servicio de atención al cliente está seleccionada por defecto.

STEP 5 | (Multitenencia solo) En la sección **Allocate This Subscription (Asignar esta suscripción)**, seleccione el grupo de servicios de inquilino (TSG) para el cual desea activar AI Access Security. Puede seleccionar el inquilino principal o un inquilino secundario.

AI Access Security está activado solo para el inquilino seleccionado. Si selecciona un inquilino principal, AI Access Security no se activa para ningún inquilino secundario.

Sáltese este paso si solo tiene una cuenta de Cuenta de servicio de atención al cliente de un solo inquilino. Está seleccionado por defecto.

STEP 6 | Revisa la **Region (Región)** del inquilino. Esta región se completa automáticamente según la región del inquilino de NGFW o Prisma Access implementado y no se puede cambiar.



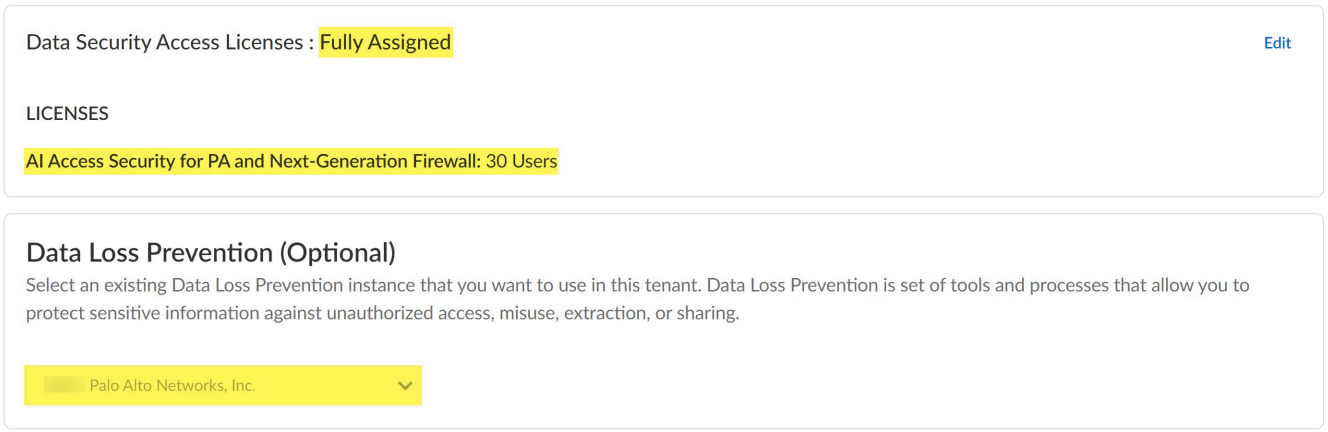
STEP 7 | En la sección **Assign Licenses (Asignar licencias)**, haga clic en **Done (Listo)** para asignar todas sus licencias de AI Access Security. Verifique que la **licencia de AI Access Security** esté `completamente asignada`

STEP 8 | Verifique que su instancia de **Data Loss Prevention** esté seleccionada si tiene Enterprise Data Loss Prevention (E-DLP) activa en su inquilino.

Su Enterprise DLP está seleccionada de forma predeterminada si ya está activa en su inquilino.

Sáltese este paso si no tiene Enterprise DLP ya activa. Enterprise DLP no es necesario para habilitar AI Access Security. Si la instancia de Enterprise DLP no está ya activa, se crea una

como parte de la activación de la licencia. Revise qué sucede con Enterprise DLP si no renueva su licencia de AI Access Security.

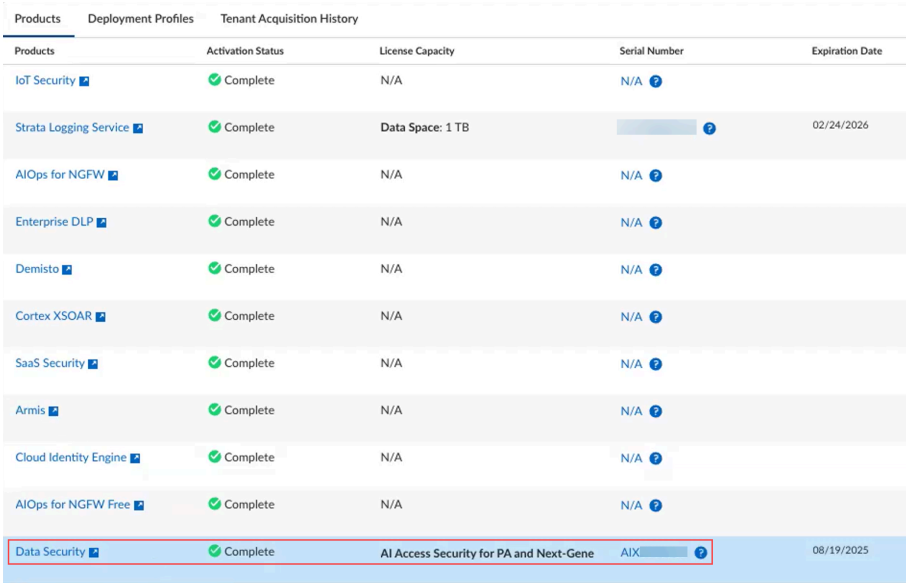


STEP 9 | Deberá **Agree to the Terms and Conditions (Aceptar las condiciones)**.

STEP 10 | **Activate (Activar)**.

Es redirigido a la página de Gestión de inquilinos donde el **Activation Status (Estado de activación)** de AI Access Security comienza `Inicializando`.

La licencia de AI Access Security se muestra como **Data Security (Seguridad de los datos)** y tiene un número de serie que comienza con `AIX`. Continúe al siguiente paso después de que el **Activation Status (Estado de activación)** esté `Completo`.



STEP 11 | (Solo NGFW) Asocia la licencia AI Access Security con su NGFW.

Es necesario asociar la licencia de AI Access Security para activar la licencia para su NGFW.

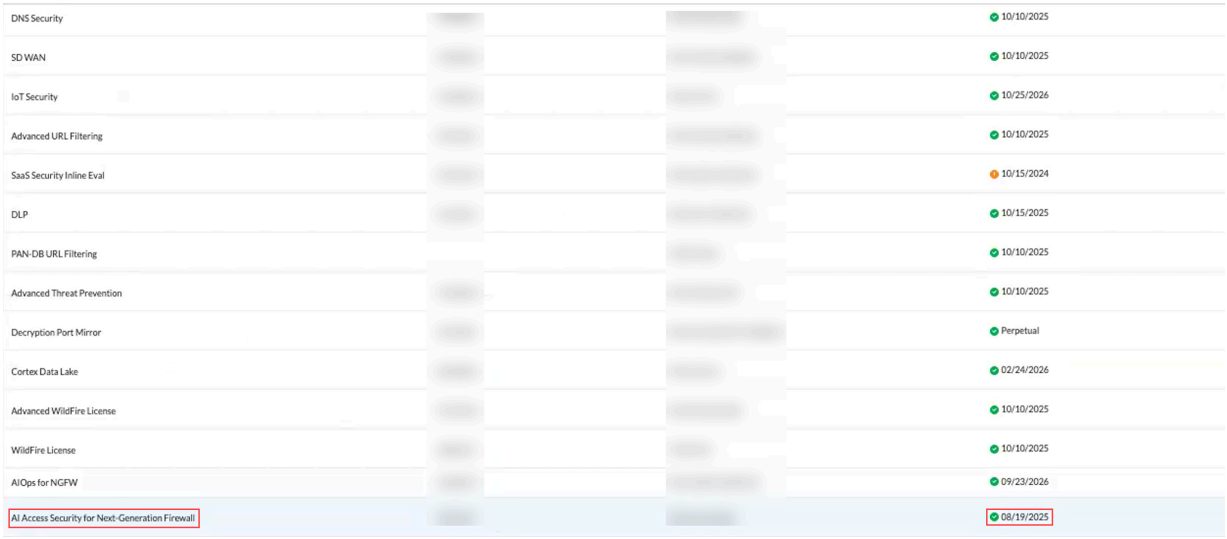
1. En el menú Strata Cloud Manager, seleccione **Settings (Configuración)** > **Device Associations (Asociaciones de dispositivos)**.

   El menú de Strata Cloud Manager se encuentra en la esquina inferior izquierda de Strata Cloud Manager.
2. En el menú Strata Cloud Manager, seleccione **System Settings (Configuración del sistema)** > **Device Associations (Asociaciones de dispositivos)**.

   El menú de Strata Cloud Manager se encuentra en la esquina inferior izquierda de Strata Cloud Manager.
3. **Associate Apps (Asociar aplicaciones)**.
4. En los Productos con licencia, seleccione **Data Security (Seguridad de datos)**.
5. Seleccione el NGFW para el cual desea activar AI Access Security.
6. **Save (Guardar)**.

STEP 12 | Verifique que activó AI Access Security correctamente.

1. Inicie sesión en el Portal de atención al cliente (CSP) de Palo Alto Networks.
2. Seleccione **Products (Productos)** > **Assets (Activos)**.
3. Seleccione el inquilino **NGFW** o **Prisma Access** basado en el punto de aplicación para el cual activó AI Access Security.
4. Utilice los filtros para localizar su NGFW o inquilino Prisma Access.
5. Expanda la lista de licencias activas o haga clic en **Licenses & Subscriptions (Licencias y suscripciones)**.
6. Verifique que la licencia de AI Access Security esté activa.



STEP 13 | Empezar con AI Access Security

Convertir una licencia de evaluación de AI Access Security a otra de Producción.

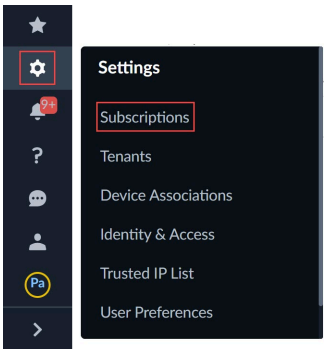
Si tiene activa la licencia EVAL de AI Access Security, debe convertir la licencia de evaluación en una licencia de producción para continuar controlando de forma segura el acceso a las aplicaciones GenAI y adoptarlas una vez que finalice el período de evaluación. Si no convierte la licencia de evaluación en una licencia de producción:

- El tráfico que contiene datos confidenciales ya no se envía a Enterprise Data Loss Prevention (E-DLP) para su inspección y emisión de veredictos.
- Enterprise DLP ya no es accesible.
  - **Panorama® management server**: **Objects (Objetos)** > **DLP**
  - **Strata Cloud Manager**: **Manage (Gestionar)** > **Configuration (Configuración)** > **Data Loss Prevention (Prevención de pérdida de datos)**
- Se conservan las reglas de seguridad web y políticas de seguridad creadas para AI Access Security.

STEP 1 | Inicie sesión en Strata Cloud Manager.

STEP 2 | En el menú Strata Cloud Manager, seleccione **Settings (Configuración)** > **Subscriptions (Suscripciones)**.

El menú de Strata Cloud Manager se encuentra en la esquina inferior izquierda de Strata Cloud Manager.



STEP 3 | Seleccione **System Settings (Configuración del sistema)** > **Subscriptions (Suscripciones)**.

STEP 4 | Busque la licencia de evaluación de AI Access Security y seleccione **Actions (Acciones)** > **Eval to Prod Request (Solicitud de cambio de Eval a Prod)**.

STEP 5 | Especifique los términos de licencia de producción que desea para su inquilino. La solicitud la revisa el representante de su cuenta de Palo Alto Networks para crear un presupuesto.

Indique la siguiente información en su solicitud de licencia de producción.

- **Número de licencias**: número de personas que pueden usar AI Access Security.
- **Plazo**: duración de la suscripción a AI Access Security.

STEP 6 | **Send Request (Enviar solicitud)**.

Renovar una licencia AI Access Security

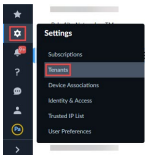
Puede renovar su licencia de AI Access Security que caduca para continuar adoptando aplicaciones GenAI de forma segura. Una AI Access Security que vence no se renueva automáticamente y requiere la renovación manual. Si AI Access Security caduca:

- El tráfico que contiene datos confidenciales ya no se envía a Enterprise Data Loss Prevention (E-DLP) para su inspección y emisión de veredictos.
- Enterprise DLP ya no es accesible.
  - **Panorama® management server**: **Objects (Objetos)** > **DLP**
  - **Strata Cloud Manager**: **Manage (Gestionar)** > **Configuration (Configuración)** > **Data Loss Prevention (Prevención de pérdida de datos)**
- Se conservan las reglas de seguridad web y políticas de seguridad creadas para AI Access Security.

STEP 1 | Póngase en contacto con su representante de ventas de Palo Alto Networks y solicite una renovación de su licencia AI Access Security.

STEP 2 | Inicie sesión en Strata Cloud Manager.

STEP 3 | En el menú inferior izquierdo, seleccione **Settings (Configuración)** > **Tenants (Inquilinos)**.



STEP 4 | Seleccione **System Settings (Configuración del sistema)** > **Tenants (Inquilinos)**.

STEP 5 | Seleccione el inquilino para el que va a renovar la licencia de AI Access Security.

Puede seleccionar un inquilino principal o secundario. Un inquilino con una licencia que requiere una acción inmediata para renovar la licencia está marcado con un círculo azul.

STEP 6 | Seleccione **Edit (Editar)** las licencias de inquilino.

STEP 7 | Deberá **Agree to the Terms and Conditions (Aceptar las condiciones)** y **Activate Now (Activar ahora)**.