paloalto TECHDOCS

Prisma Access Notas de la versión

5.2.0-h14 and 5.2.1

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

October 24, 2024

Table of Contents

Información de la versión de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

Acerca de las Actualizaciones de la versión de Prisma Access

Las versiones y actualizaciones de Prisma Access le permiten mantenerse al día y proteger a sus usuarios. Algunas de las actualizaciones son gestionadas por Palo Alto Networks, como actualizaciones de la infraestructura de Prisma Access y usted recibirá una notificación anticipada para que pueda planificar en torno a ellas. Algunas actualizaciones son su responsabilidad y debe programar la versión especificada de la actualización de contenido y la actualización de software. Si usa Panorama para gestionar Prisma Access (en lugar de la gestión en la nube de Prisma Access), usted decide cuándo actualizar a la última versión del complemento, con el fin de aprovechar las nuevas funciones disponibles que el complemento habilita para Panorama.

Si utiliza Prisma Access gestionado por Panorama, Vea los requisitos de Panorama y el complemento para esta versión gestionada por Panorama.

Versiones de GlobalProtect compatibles con Prisma Access

Cualquier versión de GlobalProtect que no sea Fin de vida útil (EoL) es compatible con su uso con Prisma Access; sin embargo, tenga en cuenta que Prisma Access 5.2 también tiene Versiones de software recomendadas para GlobalProtect, así como para las versiones requeridas.

Aquí es donde puede obtener más información sobre las últimas actualizaciones de los productos y servicios que se incluyen o se integran con Prisma Access:

Últimas actualizaciones de la versión de Prisma Access	Versiones de Prisma Access anteriores	Actualizaciones de servicios y complementos compatibles con Prisma Access
• Nuevas características en las versiones 5.2 y 5.2.1 de Prisma Access • Novedades de la Gestión en la nube de Prisma Access	• Prisma Access versión 5.1 • Prisma Access versión 5.0 • Prisma Access versión 4.2 • Prisma Access versión 4.1 • Prisma Access versión 4.0 • Prisma Access versión 3.2 Preferred e Innovation • Prisma Access versión 3.1 Preferred e Innovation	• Insights de Prisma Access • Autonomous DEM • SaaS Security • DLP empresarial • GlobalProtect • Plataforma de gestión en la nube de varios inquilinos de Prisma SASE

Últimas actualizaciones de la versión de Prisma Access	Versiones de Prisma Access anteriores	Actualizaciones de servicios y complementos compatibles con Prisma Access
	• Prisma Access versión 3.0 Preferred e Innovation • Prisma Access versión 2.2 Preferred • Versiones de Prisma Access anteriores a la versión 2.2 Preferred	• Prisma SD-WAN

Nuevas características en las versiones 5.2 y 5.2.1 de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

Esta sección le proporciona una lista de las nuevas características en Prisma Access 5.2 y 5.2.1 Preferred e Innovation; junto con las versiones de software recomendadas y requeridas que necesita usar.

Este documento contiene información sobre la hoja de ruta y se comparte SOLO CON FINES INFORMATIVOS Y DE PLANIFICACIÓN. No es un compromiso vinculante y está sujeto a cambios.

- Versiones de software recomendadas para las versiones 5.2.1 Preferred e Innovation de Prisma Access
- Dependencias de infraestructura, complementos y plano de datos para características de la versión 5.2.1 Preferred e Innovation de Prisma Access
- Características de Prisma Access 5.2.1

Versiones de software recomendadas para las versiones 5.2.1 Preferred e Innovation de Prisma Access

Existen dos versiones de Prisma Access 5.2.1:

- 5.2.1 Preferred ejecuta un plano de datos PAN-OS 10.2.10. Si su implementación está ejecutando una versión de plano de datos inferior, se necesita una actualización de plano de datos a PAN-OS 10.2.10 para implementar las características de 5.2.1 Preferred.
- 5.2.1 Innovation ejecuta un plan de datos PAN-OS 11.2.4. Se requiere una actualización a PAN-OS 11.2.4 para implementar las características de 5.2 Innovation.

Para las nuevas características de Prisma Access 5.2.1 Innovation, Prisma Access **recomienda que actualice su Prisma Access a las siguientes versiones** antes de instalar el complemento.

Versión Prisma Access	Versión del complemento de servicios en la nube	Versión de plano de datos requerida para 5.2.1	Versión recomendada de GlobalProtect	Versión recomendada de Panorama
5.2.1	Revisión de 5.2.0	PAN-OS 10.2.10 (necesaria para 5.2.1 Preferred)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.4

Versión Prisma Access	Versión del complemento de servicios en la nube	Versión de plano de datos requerida para 5.2.1	Versión recomendada de GlobalProtect	Versión recomendada de Panorama
		PAN-OS 11.2.4 (necesaria para 5.2.1 Innovation)		

Versiones de software recomendadas para las versiones 5.2 Preferred e Innovation de Prisma Access

Existen dos versiones de Prisma Access 5.2:

- 5.2 Preferred ejecuta un plano de datos PAN-OS 10.2.10. Si su implementación está ejecutando una versión de plano de datos inferior, es posible que se necesite una actualización de plano de datos a PAN-OS 10.2.10 para implementar las características de 5.2 Preferred. Si es un cliente existente, consulte Dependencias de infraestructura, complementos y plano de datos para características de la versión 5.2.1 Preferred e Innovation de Prisma Access para ver si se requiere una actualización de plano de datos para una función de Prisma Access 5.2.
- 5.2 Innovation ejecuta un plan de datos PAN-OS de 11.2.3. Se requiere una actualización a PAN-OS 11.2.3 para implementar las características de 5.2 Innovation.

Para las nuevas características de Prisma Access 5.2 Innovation, Prisma Access **recomienda que actualice su Prisma Access a las siguientes versiones** antes de instalar el complemento.

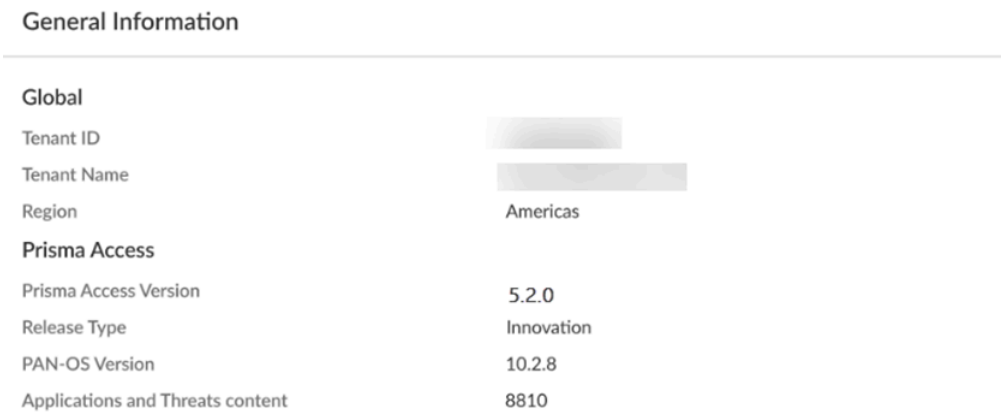
Versión Prisma Access	Versión del complemento de servicios en la nube	Versión de plano de datos requerida para 5.2	Versión recomendada de GlobalProtect	Versión recomendada de Panorama
5.2	5.2	PAN-OS 10.2.10 (necesaria para 5.2 Preferred) PAN-OS 11.2.3 (necesaria para 5.2 Innovation)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

Dependencias de infraestructura, complementos y plano de datos para características de la versión 5.2.1 Preferred e Innovation de Prisma Access

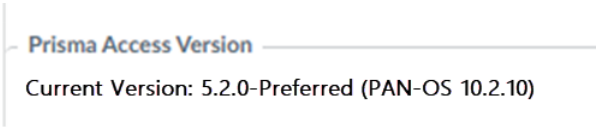
Las características de la versión 5.2.1 de Prisma Access requieren uno o más de los siguientes componentes para funcionar:

- **Actualización de infraestructura**: la infraestructura incluye el backend del servicio subyacente, la orquestación y la infraestructura de supervisión. Prisma Access actualiza la infraestructura antes de la fecha de disponibilidad general (GA) de una versión de Prisma Access.

  Las funciones que requieren solo una actualización de infraestructura para desbloquearse entran en vigor para todas las implementaciones de Prisma Access, independientemente de la versión, en el momento de la actualización de infraestructura.
- **Actualización del complemento (Implementaciones de Prisma Access gestionado por Panorama únicamente)**: la instalación del complemento activa las funciones disponibles con esa versión. Descargue e instale el complemento en el Panorama que gestiona Prisma Access.
- **Actualización del plano de datos**: el plano de datos permite la inspección del tráfico y la aplicación de políticas de seguridad en la red y el tráfico de usuarios.
  - Para Prisma Access (Managed by Strata Cloud Manager), vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Descripción general)**.'



  - Para las implementaciones de Prisma Access (Managed by Panorama), puede ver la versión del plano de datos yendo a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y viendo la **versión de Prisma Access**. Prisma Access 5.2.1 Preferred ejecuta PAN-OS 10.2.10 y Prisma Access Innovation ejecuta PAN-OS 11.2.4.



La actualización del plano de datos a 5.2.1 Innovation es opcional y solo se requiere si desea aprovechar las características que requieren una actualización del plano de datos.

Estas características se activan con la **actualización de infraestructura** solo para Prisma Access:

- Visibilidad de sucursales de alto rendimiento
- Observabilidad del agente de Prisma Access
- RFC6598 Grupo de direcciones de usuarios móviles para nuevas implementaciones de Prisma Access (Managed by Strata Cloud Manager)
- Visibilidad de la tabla de rutas en sucursales y conexiones de servicio

- Actualizaciones para ver y supervisar los conectores ZTNA
- Ver el proxy explícito basado en agentes
- Soporte regional del Servicio de creación de logs de Strata de Israel y Arabia Saudí
- Soporte IPv6 nativo para implementaciones de Prisma Access existentes

Estas características requieren una **actualización de infraestructura** pero no requieren una actualización del plano de datos; sin embargo, se requiere una versión mínima del plano de datos de 10.2.4 para estas características:

- Soporte de proxy explícito para Colo-Connect
- Soporte de proxy explícito para Proxy DNS
- Integración de proxy explícito con el Conector ZTNA
- Actualización de la configuración de la política del Conector de ZTNA con FQDN comodín
- Integración de navegadores empresariales de terceros con proxy explícito

Las siguientes características 5.2.1 requieren una actualización de la **infraestructura y los complementos**, y requieren una versión mínima del plano de datos de PAN-OS 10.2.10, lo que las convierte en características de la versión 5.2.1 Preferred de Prisma Access:

- Mejora del Conector ZTNA para aplicaciones de incorporación
- ninguno

Las siguientes características de la versión 5.2 requieren una actualización de **infraestructura, complemento y plano de datos** a PAN-OS 11.2.4, lo que las convierte en características de Prisma Access 5.2.1 Innovation:

- Red remota—Alto rendimiento, compatibilidad de acceso a aplicaciones privadas
- Mejoras estáticas de direcciones IP para usuarios móviles
- Ver la asignación estática de direcciones IP para usuarios móviles

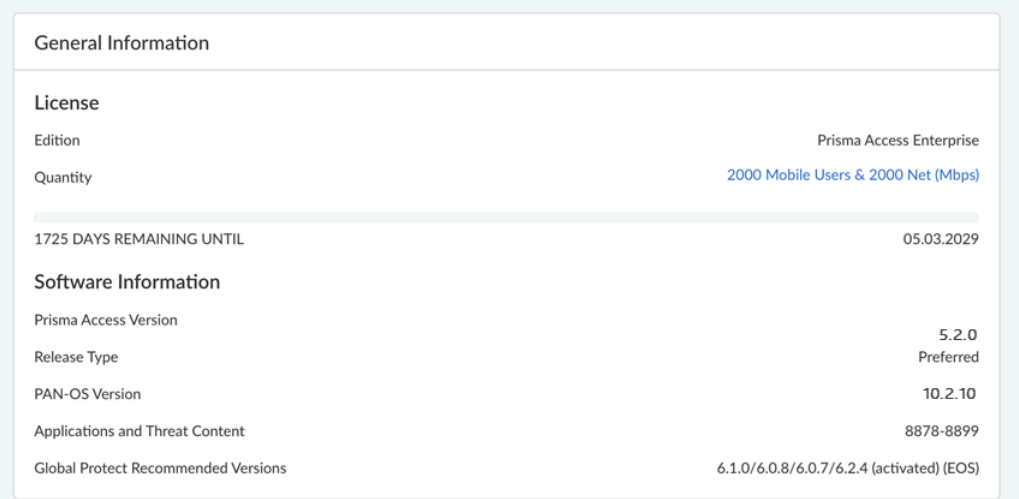
Dependencias de infraestructura, complementos y plano de datos para características de la versión 5.2 Preferred e Innovation de Prisma Access

Las características de la versión 5.2 de Prisma Access requieren uno o más de los siguientes componentes para funcionar:

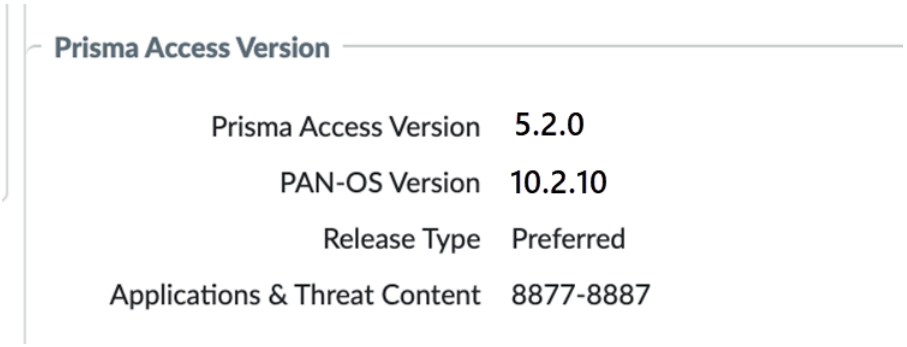
- **Actualización de infraestructura**: la infraestructura incluye el backend del servicio subyacente, la orquestación y la infraestructura de supervisión. Prisma Access actualiza la infraestructura antes de la fecha de disponibilidad general (GA) de una versión de Prisma Access.

  Las funciones que requieren solo una actualización de infraestructura para desbloquearse entran en vigor para todas las implementaciones de Prisma Access, independientemente de la versión, en el momento de la actualización de infraestructura.
- **Actualización del complemento (Implementaciones de Prisma Access gestionado por Panorama únicamente)**: la instalación del complemento activa las funciones disponibles con esa versión. Descargue e instale el complemento en el Panorama que gestiona Prisma Access.

- **Actualización del plano de datos**: el plano de datos permite la inspección del tráfico y la aplicación de políticas de seguridad en la red y el tráfico de usuarios.
  - Para Prisma Access (Managed by Strata Cloud Manager), vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Descripción general)**



  - Para las implementaciones de Prisma Access (Managed by Panorama), puede ver la versión del plano de datos yendo a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** y viendo la **versión de Prisma Access**. Prisma Access 5.2 Preferred ejecuta PAN-OS 10.2.10 y Prisma Access Innovation ejecuta PAN-OS 11.2.3.



La actualización del plano de datos a 5.2 Innovation es opcional y solo se requiere si desea aprovechar las características que requieren una actualización del plano de datos.

Estas características se activan con la **actualización de infraestructura** solo para Prisma Access:

- Endpoint DLP
- Simplifique la conectividad SaaS de Prisma Access con optimización de IP para usuarios móviles e implementaciones de proxy explícito
- Soporte de TLS 1.3 y PubSub para la replicación de tráfico
- Ver y supervisar Colo-Connect

Estas características requieren una **actualización de infraestructura y complemento** pero no requieren una actualización del plano de datos:

- Compatibilidad con 25.000 redes remotas y 50.000 puertas de enlace de IKE
- Visibilidad y aplicación de direcciones IP privadas para tráfico proxy basado en agentes
- Optimización de direcciones IP para usuarios de proxy explícito: Implementaciones de proxy
- Compatibilidad con RBAC para el complemento de servicios en la nube
- Conectividad de aplicaciones privadas simplificadas de Prisma Access
- Soporte de integración de la red troncal SP para AWS
- Ver versiones de Prisma Access, plano de datos y contenido de aplicaciones y amenazas en Strata Cloud Manager

Las siguientes características 5.2 requieren una actualización de la **infraestructura y los complementos**, y requieren una versión mínima del plano de datos de PAN-OS 10.2.10, lo que las convierte en características de la versión 5.2 Preferred de Prisma Access

- Redes remotas—Alto rendimiento

Las siguientes características de la versión 5.2 requieren una actualización de **infraestructura, complemento y plano de datos** a Prisma Access 11.2.3, lo que las convierte en características de Prisma Access 5.2 Innovation:

- Compatibilidad de SC-NAT con el Acceso con privilegios dinámicos con CIAM
- Compatibilidad del conector ZTNA con la Incorporación de aplicaciones sin compromiso

Características de Prisma Access 5.2.1

En la siguiente tabla se describen las nuevas características que estarán disponibles en general con Prisma Access 5.2.1.

Soporte de proxy explícito para Colo-Connect

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Si tiene grandes centros de datos con conectividad directa a instalaciones de coubicación, ahora puede conectarse a través del Proxy explícito de Prisma Access , lo que permite acceso de alta velocidad a aplicaciones privadas. Con la mejora, recibirá hasta 20 Gbps de rendimiento por región.

La integración de Colo-Connect con el proxy explícito ofrece los siguientes beneficios:

- El proxy explícito se conecta automáticamente a la ubicación de cómputo de Prisma Access más cercana, lo que le ofrece la mejor latencia posible.
- Elimina las dependencias de red y enrutamiento, ofreciendo gestión y enrutamiento de túneles seguros y automatizados para aplicaciones privadas.
- Colo-Connect admite la recuperación de aplicaciones privadas en redes superpuestas, lo que garantiza flexibilidad y accesibilidad.

Soporte de proxy explícito para Proxy DNS

Compatible con: Prisma Access (Managed by Strata Cloud Manager) 5.2.1 Preferred e Innovation

El proxy explícito amplía su compatibilidad para incluir Personalización del proxy DNS. El proxy explícito admite la configuración DNS, como DNS regional, DNS personalizado, etc. También puede usar un solucionador DNS de terceros o un solucionador DNS local para resolver aplicaciones públicas y privadas, y puede usar por FQDN. Esta funcionalidad es actualmente compatible solo en .

Integración segura de navegadores empresariales de terceros con proxy explícito

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Prism Access ahora puede habilitar el acceso seguro a aplicaciones privadas a través de navegadores empresariales de terceros. Con esta mejora, la información del usuario puede intercambiarse de forma segura y transparente entre el navegador empresarial de terceros y Prisma Access, lo que permite la ejecución de las reglas de política basadas en User-ID dentro de Prisma Access. Esto elimina la necesidad de que los usuarios finales se vuelvan a autenticar con Prisma Access si ya han iniciado sesión en el navegador de empresa externo.

Integración de proxy explícito con el Conector ZTNA

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Los usuarios que se conectan a aplicaciones privadas a través de ZTNA Connector ahora pueden establecer una conexión a través del proxy explícito de Prisma Access. Esta integración es compatible con conectores ZTNA con una capacidad de hasta 10 Gbps para Prisma Access Browser y Proxy de agente.

A continuación se detallan los beneficios adicionales:

- El proxy explícito se conecta automáticamente a la ubicación de cómputo de Prisma Access más cercana con proxy explícito, lo que garantiza una latencia óptima.
- Elimina las dependencias de red y enrutamiento, lo que garantiza la gestión segura y automatizada de túneles y el enrutamiento para aplicaciones privadas.
- ZTNA Connector es compatible con Cloud Identity Engine (CIE), lo que permite la detección automática de aplicaciones privadas.
- ZTNA Connector admite la recuperación de aplicaciones privadas en redes superpuestas, lo que garantiza flexibilidad y accesibilidad.

Visibilidad de sucursales de alto rendimiento

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Las sucursales de alto rendimiento (RN-HP) en Prisma Access tienen características distintas en comparación con las sucursales heredadas, y ambas coexistirán dentro de los entornos de los clientes. El sistema de gestión debe adaptarse al nuevo tipo de sucursal RN-HP para ayudar a los administradores de red con la resolución de problemas.

Compatibilidad nativa con IPv6 para implementaciones de Prisma Access existentes

Compatible con: Prisma Access 5.2.1 Preferred e Innovation para todas las implementaciones (la compatibilidad con IPv6 para las nuevas implementaciones es compatible a partir de Prisma Access 5.1.1; compatibilidad para las implementaciones existentes añadida en la versión 5.2.1 de Prisma Access)

Prisma Access amplia su soporte para IPv6 desde aplicaciones privadas para abarcar soporte integral de IPv6 de extremo a extremo para usuarios móviles, redes remotas y conexiones de servicio, y añade compatibilidad nativa con IPv6 para implementaciones de Prisma Access existentes.

Un aspecto beneficioso de la compatibilidad nativa de IPv6 es su capacidad de permitir a los usuarios móviles que utilizan endpoints IPv6 únicamente establecer conexiones con Prisma Access a través de conexiones IPv6 que utilizan GlobalProtect. Además, esta compatibilidad facilita el acceso a aplicaciones SaaS públicas a través de Internet, especialmente cuando esos destinos requieren conexiones IPv6.

IPv6 cuenta con un espacio de direcciones mayor en comparación con IPv4, lo que permite albergar un número casi ilimitado de direcciones IP únicas. Gracias al soporte nativo de IPv6, Prisma Access está diseñado para ser compatible con conexiones IPv6 y de pila doble, lo que facilita el proceso de migración de IPv4 a IPv6. Esta compatibilidad garantiza la compatibilidad con versiones anteriores y empodera a las organizaciones en su transición a redes basadas en la nube y habilitadas para IPv6.

Observabilidad del agente de Prisma Access

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

El Agente de Prisma Access es un agente de acceso móvil de nueva generación que le permite usar Prisma Access para proteger su fuerza de trabajo móvil. Diseñado para la fuerza laboral híbrida de hoy en día, el agente de Prisma Access ofrece un acceso seguro y práctico a las aplicaciones empresariales y a Internet, y también simplifica las operaciones de red, TI y seguridad para una organización. En Strata Cloud Manager, vaya a **Insights** > **Activity Insights (Información sobre la actividad)** > **Users (Usuarios)** para ver información sobre la implementación del agente de Prisma Access.

Redes remotas—compatibilidad con acceso a aplicaciones privadas de alto rendimiento

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Red remota—Alto rendimiento de Prisma Access añade compatibilidad con el acceso a aplicaciones privadas, además de su compatibilidad existente para la salida a Internet. Este soporte significa que usted puede:

- Recuperar aplicaciones privadas de una sucursal conectada por una red remota de alto rendimiento
- Comunicarse con otra sucursal (tráfico de sucursal a sucursal) mediante conexiones de servicio
- Comunicarse con usuarios móviles (tráfico móvil de usuario a sucursal) mediante conexiones de servicio

Visibilidad de la tabla de rutas en sucursales y conexiones de servicio

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Mejoras estáticas de direcciones IP para usuarios móviles

Compatible con: Prisma Access 5.2.1 Innovación

Prisma Access se suma a la funcionalidad de dirección IP estática para usuarios móviles, donde puede asignar direcciones IP estáticas a los usuarios en función del entorno de Prisma Access o el User-ID.

Para mejorar la asignación de direcciones IP para los usuarios móviles, ahora puede usar grupos de ubicaciones y grupos de usuarios como criterio, además de entorno y User-ID.

Además, el número de perfiles de grupo de direcciones IP admitidos aumenta a 10.000.

RFC6598 Grupo de direcciones de usuarios móviles para nuevas implementaciones de Prisma Access (Managed by Strata Cloud Manager)

Compatible con: Prisma Access (Managed by Strata Cloud Manager) 5.2.1 Preferred e Innovation

Cada implementación de Prisma Access requiere un Grupo de direcciones IP de usuarios móviles. Prisma Access asigna una dirección IP de este grupo a cada dispositivo conectado a GlobalProtect. Para simplificar la incorporación de los usuarios móviles de GlobalProtect, Palo Alto Networks proporciona nuevas implementaciones de Prisma Access (gestionadas por Strata Cloud Manager) con un grupo de direcciones IP predeterminado del RFC6598. El pool IP es 100.92.0.0/16. Si necesita más direcciones o desea utilizar sus propias direcciones, puede modificar este grupo o eliminarlo y añadir grupos de direcciones IP propios.

Soporte regional del Servicio de creación de logs de Strata de Israel y Arabia Saudí

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Prisma Access es compatible con las regiones de Strata Logging Service de Israel y Arabia Saudita.

Actualizaciones para ver y supervisar los conectores ZTNA

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

El conector de acceso a la red de confianza cero (ZTNA) simplifica el acceso privado a aplicaciones para todas sus aplicaciones. La máquina virtual de ZTNA Connector en su entorno forma automáticamente túneles entre sus aplicaciones privadas y . A partir de Prisma Access 5.2.1, hemos revisado el aspecto de la página Conectores ZTNA para facilitar su uso y hemos añadido tablas con detalles sobre su comodín, FQDN y objetivos de subred IP.

Ver el proxy explícito basado en agentes

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Esperando la descripción.

Ver la asignación estática de direcciones IP para usuarios móviles

Compatible con: Prisma Access 5.2.1 Innovación

Para supervisar los grupos de IP estáticas, vaya a **Insights** > **Activity Insights (Actividad de Insights)** > **Users (Usuarios)** para supervisar los grupos de IP estáticas en el widget de **IP Pool Utilization (Utilización del grupo de IP)**. La función de asignación de IP estática le permite asignar una dirección IP fija a los usuarios móviles de Prisma Access. Esto es útil si sus implementaciones de red restringen el acceso de los usuarios a los recursos utilizando direcciones IP como parte de su diseño de red y aplicación. Con esta funcionalidad, puede definir el grupo de IP en función del escenario y el usuario.

Configuración de FQDN comodín para políticas de seguridad en el conector ZTNA

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

El uso de FQDN comodín en las reglas de la política de seguridad está actualmente restringido debido a limitaciones de protocolo. Como resultado, en este momento, solo se admiten los protocolos HTTP y HTTPS para el FQDN comodín en las reglas de la política de seguridad.

Con esta mejora:

- Puede configurar una política de seguridad basada en el FQDN de la aplicación comodín.
- Se aplica la misma política de seguridad a todas las aplicaciones detectadas que comparten el mismo FQDN comodín.
- Cuando se detectan nuevas aplicaciones que coinciden con el FQDN comodín, el tráfico puede pasar sin necesidad de una nueva confirmación.

Mejora del Conector ZTNA para aplicaciones de incorporación

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Si los usuarios de su empresa acceden a un gran número de aplicaciones privadas, el conector ZTNA puede experimentar problemas de escalabilidad cuando el número de aplicaciones de la infraestructura supera las 15000.

ZTNA Connector ofrece una mejora que mejora la escalabilidad, lo que permite a los usuarios incorporar:

- 20.000 aplicaciones por inquilino y 4000 por grupo de conectores.
- 400 conectores entre inquilinos con un ancho de banda de 16 Gbps por región de proceso.

ZTNA Connector para aplicaciones de incorporación

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

Si los usuarios de su empresa acceden a un gran número de aplicaciones privadas, el conector ZTNA puede experimentar problemas de escalabilidad cuando el número de aplicaciones de la infraestructura supera las 15000.

ZTNA Connector ofrece una mejora que mejora la escalabilidad, lo que permite a los usuarios incorporar:

- 20.000 aplicaciones por inquilino y 4000 por grupo de conectores.
- 400 conectores entre inquilinos con un ancho de banda de 16 Gbps por región de proceso.

Actualización de la configuración de la política del Conector de ZTNA con FQDN comodín

Compatible con: Prisma Access 5.2.1 Preferred e Innovation

El uso de FQDN comodín en las reglas de la política de seguridad está actualmente restringido debido a limitaciones de protocolo. Como resultado, en este momento, solo se admiten los protocolos HTTP y HTTPS para el FQDN comodín en las reglas de la política de seguridad.

Con esta mejora:

- Puede configurar una política de seguridad basada en el FQDN de la aplicación comodín.
- Se aplica la misma política de seguridad a todas las aplicaciones detectadas que comparten el mismo FQDN comodín.
- Cuando se detectan nuevas aplicaciones que coinciden con el FQDN comodín, el tráfico puede pasar sin necesidad de una nueva confirmación.

Características de Prisma Access 5.2

Esta sección describe las nuevas características que están disponibles con la versión 5.2 de Prisma Access.

Compatibilidad con 25.000 redes remotas y 50.000 puertas de enlace de IKE

Compatible con: Prisma Access 5.2 Preferred e Innovation

Para implementar esta función, comuníquese con su equipo de cuentas de Palo Alto Networks, quien abrirá un caso de SRE para gestionar la solicitud.

Visibilidad y aplicación de direcciones IP privadas para tráfico proxy basado en agentes

Compatible con: Prisma Access 5.2 Preferred e Innovation

Los usuarios que se conectan al proxy explícito de Prisma Access a través del agente de GlobalProtect desde las sucursales, pueden aprovechar las Direcciones IP privadas de endpoints para el registro de logs o para aplicar la ejecución basada en direcciones IP.

Optimización de direcciones IP para usuarios de proxy explícito: Implementaciones de proxy

Compatible con: Prisma Access 5.2 Preferred e Innovation

La optimización de direcciones IP es un conjunto de mejoras de la arquitectura que reducen el número total de direcciones IP en la implementación, lo que simplifica los flujos de trabajo de listas de permitidos al tiempo que mejora la resiliencia y permite una incorporación más rápida de los inquilinos de Prisma Access, permitiendo una incorporación más rápida de los inquilinos de Prisma Access.

Persistencia de la dirección IP

Con la adherencia, o persistencia, de la dirección IP, puede proteger las aplicaciones SaaS y los sitios web que requieren que las sesiones de usuario mantengan la misma dirección IP de salida de Prisma Access durante toda la sesión de usuario.

Simplifique la incorporación de aplicaciones SaaS

Añadir una ubicación de Prisma Access o experimentar un Evento de escalado en una ubicación existente de Prisma Access podría llevar a que se asignen nuevas direcciones IP a sus implementaciones de proxy explícito. Es una práctica recomendada recuperar las nuevas direcciones IP de salida y puerta de enlace y añadirlas a una lista de permitidos de las aplicaciones SaaS. La optimización de direcciones IP reduce el número de direcciones IP que tiene que gestionar en implementaciones grandes.

Endpoint DLP

Compatible con: Prisma Access 5.2 Preferred e Innovation

Se requiere Agente de Prisma Access.

Endpoint DLP permite a sus administradores de seguridad controlar el uso de dispositivos periféricos, permitiéndole permitir o bloquear su uso, o alertar a sus administradores de seguridad cuando un dispositivo periférico está conectado a un endpoint en su organización. Para evitar la exfiltración de datos confidenciales a dispositivos periféricos, utilice los métodos de detección avanzados de , así como perfiles de datos personalizados para definir sus propios criterios de coincidencia de tráfico o perfiles de datos predefinidos basados en aprendizaje automático y regex.

Instala el en los endpoints que desea proteger y detecta el movimiento de archivos entre el endpoint y el dispositivo periférico para evaluar y aplicar las reglas de la política de Endpoint DLP cuando detecta cualquier movimiento de archivos. Cuando es necesario, reenvía el tráfico a para su inspección e interpretación del veredicto. luego comunica el veredicto al que luego toma la acción configurada en la regla de políticas de Endpoint DLP. Adicionalmente, el también es responsable de mostrar al usuario final una notificación cuando generan un incidente de DLP.

La inspección de los endpoints mediante es la siguiente. Esto supone que el se ha instalado correctamente y que usted ha configurado las reglas de la política de Endpoint DLP.

1. Un usuario de su organización conecta un dispositivo periférico a su portátil.

2. El usuario mueve un archivo desde su endpoint al dispositivo periférico conectado.
3. El registra que el usuario intentó mover un archivo desde el endpoint al dispositivo periférico y evalúa su base de reglas de política de Endpoint DLP.
   - **Sin coincidencia de reglas de política**: si no se identifica la coincidencia de reglas de la política de Endpoint DLP, se permite la conexión del dispositivo periférico y el endpoint tiene privilegios completos de acceso de lectura y escritura al dispositivo periférico.
   - **Regla de política de control periférico**: si ha creado una regla de política de control periférico para controlar el acceso, entonces el toma la acción permitir o bloquear configurada en la regla de la política.

     Por ejemplo, si la regla de la política de Endpoint DLP bloquea la conexión al dispositivo periférico, el revoca los privilegios de escritura del dispositivo periférico. En este caso, el endpoint no puede cargar archivos en el dispositivo periférico.

     Por lo contrario, si la regla de políticas de Endpoint DLP permite la conexión al dispositivo periférico, el concede los privilegios de acceso de escritura de endpoints al dispositivo periférico. En este caso, el endpoint puede cargar archivos en el dispositivo periférico.
   - **Data in Motion Policy Rule**: se permite la conexión al dispositivo periférico. Cuando el detecta el movimiento del archivo desde el endpoint a un dispositivo periférico, el archivo se reenvía al para su inspección e interpretación de veredictos. El también reenvía metadatos de archivos importantes, como el `fileSHA`, que utiliza para identificar cada archivo reenviado.

     envía entonces el veredicto al y el toma la acción de la regla de la política de Endpoint DLP si se detectan datos sensibles. Si detecta que se trata de un archivo que ya se ha inspeccionado en base a `fileSHA`, devuelve el veredicto existente al . no inspecciona el mismo archivo dos veces.
4. El ejecuta la acción de regla de política de Endpoint DLP configurada en las reglas de la política de Control periférico o Datos en movimiento.
5. Se genera un incidente de DLP cuando es apropiado. Si ha configurado el entrenamiento del usuario final, se mostrará una notificación en el endpoint para alertar al usuario.

Soporte de proxy explícito de China

Compatible con: Prisma Access 5.2 Preferred e Innovation

Prisma Access es compatible con implementaciones de Proxy explícito en China.

Compatibilidad con RBAC para el complemento de servicios en la nube

Compatible con: Prisma Access (Managed by Panorama) 5.2 Preferred e Innovation

Redes remotas—Alto rendimiento

Compatible con: Prisma Access 5.2 Preferred e Innovation

Prisma Access ofrece una solución integral para la terminación IPSec de gran ancho de banda, compatible con sitios grandes, equilibrio de carga automatizado, incorporación simplificada, redundancia regional,

gestión de IP de salida única y compatibilidad con varias soluciones SD-WAN, incluida Prisma SD-WAN. Estas características mejoran colectivamente la escalabilidad, el rendimiento y la fiabilidad de la conectividad del sitio remoto.

A medida que su negocio crece y sus oficinas se distribuyen geográficamente, puede incorporar rápidamente una sucursal con un alto ancho de banda utilizando una red remotade alto rendimiento de Prisma Access, también conocida como *Red remota—Alto rendimiento*. Estas redes ofrecen los siguientes beneficios:

- Admite un ancho de banda agregado de hasta 3 Gbps por dirección IP de servicio o dirección de endpoints de servicio; lo que le proporciona una cantidad reducida de direcciones IP o FQDN para usar en la terminación del túnel IPSec.
- Incluye redundancia regional para mejorar la disponibilidad y la tolerancia a fallos.
- Utiliza NAT para reducir las direcciones IP de salida públicas.
- Simplifica la incorporación con recomendaciones dentro del producto para elegir ubicaciones según la disponibilidad geográfica.
- Incluye soporte para Link Quality Metrics (LQM), donde Prisma SD-WAN determina la calidad del enlace al sondear activamente las rutas VPN de Secure Fabric sobre transportes público y privado y las rutas subyacentes de WAN privada. Las sondas proporcionan una medición constante de las métricas de rendimiento de la red, como la fluctuación, la latencia y la pérdida de paquetes. Estas métricas, junto con las métricas de rendimiento específicas de la aplicación y la accesibilidad de las Capas 1 a 7, informan las decisiones de reenvío de tráfico para flujos de aplicaciones nuevos y existentes.

Resumen de rutas para el Acceso con privilegios dinámicos

Compatible con: Prisma Access (Managed by Strata Cloud Manager) 5.2 Innovación

En los inquilinos de Prisma Access habilitados para Acceso con privilegios dinámicos, puede resumir rutas al anunciar las rutas de usuario móvil (MU) a su red local. El resumen de rutas es beneficioso para las empresas que tienen equipos locales con capacidad limitada, como enrutadores básicos en la nube. Al reducir la demanda de estos dispositivos, el resumen de ruta garantiza que los dispositivos no superen su capacidad de ruta cuando se comuniquen con el centro de datos.

Para habilitar el resumen de rutas, configure grupos de resumen globales que consisten en listas de grupos de IP grandes que se pueden usar en múltiples proyectos. Luego, habilite el resumen de ruta en la conexión del servicio Prisma Access. Cuando un usuario utiliza el agente de Prisma Access para conectarse a un proyecto que tiene una dirección IP dentro del rango de los grupos de resumen global configurados, la conexión de servicio anunciará el grupo de resumen global en lugar de la ruta más pequeña a nivel de proyecto. Esto ayuda a reducir el número de rutas que se envían a la red.

Compatibilidad con SC-NAT para el Acceso con privilegios dinámicos con CIAM

Compatible con: Prisma Access 5.2 Innovación

Use Compatibilidad con SC-NAT para el Acceso con privilegios dinámicos (DPA) si utiliza DPA y ha creado conexiones de servicio para acceder a aplicaciones privadas en su centro de datos o sede central. Varios proyectos en su entorno de DPA pueden experimentar el agotamiento de direcciones IP si las

direcciones IP de la subred de infraestructura se superponen. Para solucionar este problema, Prisma Access puede implementar NAT de origen (SNAT) para las direcciones IP, que:

- Permite que Prisma Access asigne una sola dirección IP para un usuario móvil que accede a aplicaciones privadas mediante una conexión de servicio
- Le proporciona SNAT para facilitar el enrutamiento
- Elimina la superposición de grupos de IP
- Elimina el agotamiento de grupos de IP IPv4 entre Prisma Access y su centro de datos o sede central

Conectividad de aplicaciones privadas simplificadas de Prisma Access

Compatible con: Prisma Access 5.2 Preferred e Innovation

Una forma de acceder a una aplicación privada es mediante una conexión de servicio, también conocida como *Nodo de conexión de servicio - acceso corporativo* (SC-CAN). Puede resultar difícil conectarse a aplicaciones privadas mediante conexiones de servicio porque:

- Rendimiento indeterminista de la aplicación privada debido a cuellos de botella de SC-CAN
- Latencia debido a saltos de tránsito incorrectos
- Complejidad operativa en la implementación de SC-CAN

Para solucionar este problema, Prisma Access ha mejorado su infraestructura de enrutamiento con mejoras de enrutamiento que:

- Eliminan los cuellos de botella de SC-CAN mediante la mejora de la red interna
- Organizan un SC-CAN de anclaje cuando es necesario, lo que evita saltos de tránsito incorrectos y enrutamiento ineficiente

Este diseño ofrece los siguientes beneficios:

- Configuración de enrutamiento más fácil de implementar
- Configuración sencilla del día cero
- Ancho de banda determinista de 1 Gbps desde un SC-CAN específico hasta el centro de datos o la ubicación de la sede donde se encuentra la aplicación privada

Simplifique la conectividad SaaS de Prisma Access con optimización de IP para usuarios móviles e implementaciones de proxy explícito

Compatible con: Prisma Access 5.2 Preferred e Innovation

Prisma Access amplía la funcionalidad de optimización de IP ofreciéndole tanto para proxy explícito como para Usuarios móviles—GlobalProtect.

Para las implementaciones de Usuarios móviles— GlobalProtect, cuando un gran número de usuarios acceden a una puerta de enlace de GlobalProtect desde una ubicación, Prisma Access escala automáticamente la ubicación y añade otra puerta de enlace de GlobalProtect. La optimización de IP utiliza una capa NAT para que la puerta de enlace con escalado automático utilice la misma dirección IP que la dirección IP asignada anteriormente, eliminando así la necesidad de añadir direcciones IP adicionales a las listas de permisos de su organización.

Prisma Access expande la capa NAT a los nodos de procesamiento de seguridad de proxy explícito (SPN), así como a los SPN de usuario móvil, lo que reduce la necesidad de permitir direcciones IP de lista para implementaciones de proxy explícito. Esta capa de NAT de proxy explícito es beneficiosa si está configurando una implementación de usuarios móviles y proxy explícito en Modo proxy o Modo túnel y proxy.

Soporte de integración de la red troncal SP para AWS

Compatible con: Prisma Access 5.2 Preferred e Innovation

Para implementar esta función, comuníquese con su equipo de cuentas de Palo Alto Networks, quien abrirá un caso de SRE para gestionar la solicitud.

A partir de la versión 5.2 de Prisma Access, usted (el proveedor de servicios) ahora tiene la flexibilidad de seleccionar AWS y GCP para el tráfico de salida de la nube pública de sus clientes. Verá las regiones adicionales en la activación de su licencia, verá diferentes pestañas para GCP y AWS en sus conexiones y grupos de direcciones IP, y también podrá supervisar las nubes públicas por separado.

Soporte de TLS 1.3 y PubSub para la replicación de tráfico

Compatible con: Prisma Access 5.2 Preferred e Innovation

Si es una organización grande que utiliza Replicación de tráfico, puede tener los siguientes desafíos al implementarlo y usarlo:

- Las herramientas que consumen los archivos de captura de paquetes (PCAP) requieren consultas frecuentes de los depósitos para hacer frente a un gran número de archivos PCAP. Las herramientas pueden crear una sobrecarga en los depósitos y los proveedores de la nube pueden limitar su uso.
- Cuando se utilizan los archivos PCAP para el análisis forense, el acceso al tráfico descifrado SSL proporciona una mejor eficacia, y una cantidad significativa del tráfico está cifrado con TLS 1.3.

Para resolver estos problemas, Prisma Access ofrece estas mejoras que permiten que las herramientas de terceros sean más eficientes y fáciles de escalar:

- **Notificaciones de Pub/Sub**: Prisma Access envía de manera proactiva una notificación de Pub/Sub cuando se sube un nuevo archivo PCAP al depósito de almacenamiento. El uso de notificaciones de Pub/Sub para nuevos archivos PCAP elimina la necesidad de desarrollar herramientas que le notifiquen cuando hay nuevos archivos en los depósitos.
- **Compatibilidad con el descifrado TLS 1.3**: Prisma Access utiliza TLS 1.3 al descifrar archivos PCAP, lo que proporciona una visibilidad más profunda del tráfico. Esta compatibilidad se aplica a las implementaciones de red remotas en las que se ha habilitado el uso de reglas de política de descifrado SSL/TLS en archivos PCAP.

Ver y supervisar Colo-Connect

Compatible con: Prisma Access 5.2 Preferred e Innovation

Colo-Connect se basa en el concepto de hub, o centro, de rendimiento basado en Colo, con conexiones privadas de gran ancho de banda junto con conectividad de Capa 2/3 a Prisma Access desde centros de rendimiento existentes. Colo-Connect aprovecha la tecnología de interconexión GCP nativa de la nube para proporcionar conexiones de servicio de gran ancho de banda a sus aplicaciones privadas. Vaya a **Monitor (Supervisar)** > **Data Center (Centros de datos)** > **Service Connections (Conexiones de servicio)** para ver y supervisar su conectividad privada a la nube híbrida y a los centros de datos locales a través de interconexiones en la nube.

Ver versiones de Prisma Access, plano de datos y contenido de aplicaciones y amenazas en Strata Cloud Manager y Panorama

Compatible con: Prisma Access (Managed by Strata Cloud Manager) 5.2 Preferred e Innovation

Para permitirle obtener más información sobre sus implementaciones de Prisma Access (gestionado por Strata Cloud Manager), la zona de Información de software de la página Descripción general [**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Overview (Descripción general)**] en versiones de Strata Cloud Manager y Prisma Access [**Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración de servicios)**] en Panorama le proporcionan la siguiente información:

- Versión de Prisma Access
- Versión de plano de datos de PAN-OS
- Tipo de versión (Preferred o Innovation)
- Versión de Contenido de aplicaciones y amenazas

Compatibilidad del conector ZTNA con la Incorporación de aplicaciones sin compromiso

Compatible con: Prisma Access 5.2 Innovación

Con la mejora de la incorporación sin compromiso, tiene una experiencia mejorada a la hora de incorporar, modificar o eliminar aplicaciones. Se elimina el retraso anterior de 5-10 minutos, lo que resulta en un proceso más rápido. El tiempo necesario para la Incorporación de aplicaciones ahora es menos de 1 minuto, lo que le permite gestionar sus aplicaciones de manera rápida y eficiente. Además, la escala mejorada de ZTNA Connector satisface las necesidades de los grandes clientes que gestionan más de 10.000 aplicaciones. Tiene la capacidad de incorporar un mayor número de aplicaciones, lo que le proporciona una mayor flexibilidad y eficiencia en sus operaciones.

Cambios en el comportamiento predeterminado para las versiones 5.2 y 5.2.1 de Prisma Access

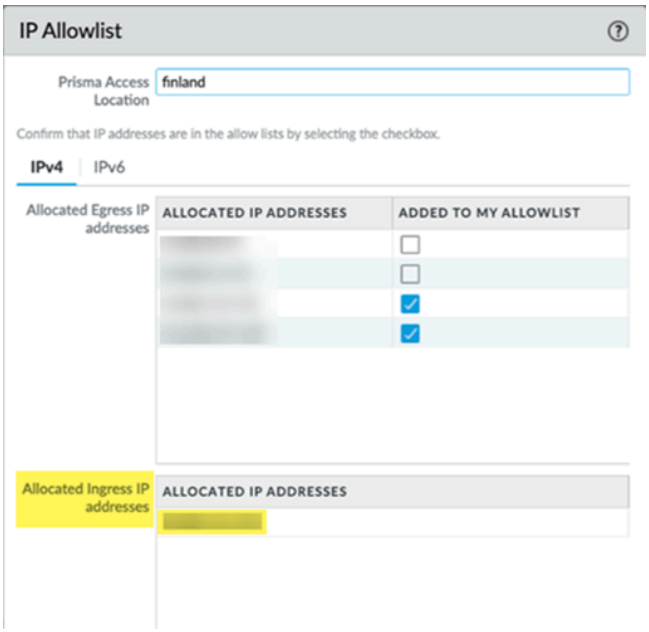
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

En las secciones siguientes se detallan los cambios en el comportamiento predeterminado para las versiones Prisma Access5.2 y Prisma Access 5.2.1.

Cambios en el comportamiento por defecto de la versión 5.2.1 de Prisma Access

En la tabla siguiente se detallan los cambios en el comportamiento predeterminado para la versión 5.2.1 de Prisma Access.

Componente	Cambio
Optimización de IP habilitada para nuevas implementaciones de Prisma Access	Para permitir una incorporación más rápida de los inquilinos de Prisma Access y simplificar el listado de direcciones IP, las nuevas implementaciones de Prisma Access tienen habilitada la optimización IP. *Las implementaciones de Optimización IP no son compatibles con IPv6 para el acceso a aplicaciones públicas (externas); el acceso a aplicaciones privadas es compatible. Para habilitar IPv6 para su nueva implementación de Prisma Access, comuníquese con su equipo de cuentas de Palo Alto Networks, ellos abrirán un caso TAC para gestionar la solicitud.* Asegúrese de que todos los usuarios estén ejecutando una versión de la aplicación GlobalProtect 6.1.4 y posterior, 6.2.3 y posterior o 6.3.0 y posterior antes de configurar una nueva implementación de Prisma Access. *Las nuevas implementaciones de FedRAMP no tienen habilitada la optimización de IP.*
Usuarios móviles predeterminados—GlobalProtect, el grupo de direcciones IP se	Las nuevas implementaciones de Usuarios móviles—GlobalProtect de Prisma Access (gestionado por Strata Cloud Manager) tiene un nuevo grupo de direcciones IP predeterminado: 100.92.0.0/16. Este es un cambio con respecto a implementaciones anteriores que usaban un

Componente	Cambio
cambia para nuevas implementaciones de Prisma Access (gestionado por Strata Cloud Manager)	grupo de direcciones IP predeterminado de 100.127.0.0/16. Puede usar este grupo de RFC6598 para la mayoría de los casos de uso, incluido el acceso a aplicaciones privadas para usuarios móviles. Si necesita más direcciones IP, puede añadirlas en la interfaz de usuario de Prisma Access.
Consolidación de direcciones IP para implementaciones que han migrado a la Optimización de IP	Si tiene un Prisma Access existente que ha migrado una o más regiones a la Optimización de IP y está utilizando la lista de permitidos de Prisma Access, algunas direcciones IP que ha permitido enumerar se han movido desde el área de **Allocated Egress IP addresses (Direcciones IP de salida asignadas)** al área **Allocated Ingress IP addresses (Direcciones IP de entrada asignadas)** en la IU de Prisma Access. Este cambio es el resultado de la consolidación de direcciones IP como parte de la actualización de infraestructura de Prisma Access 5.2.1. Sus redes todavía pueden alcanzar estas direcciones IP y ya no tiene que colocarlas en la lista de permitidos. 

Cambios en el comportamiento predeterminado de Prisma Access 5.2

Componente	Cambio
Consideraciones de actualización para el Plano de datos de PAN-OS 10.2.10	Si elije que Palo Alto Networks actualice su plano de datos a PAN-OS 10.2.10 para que sea compatible con una característica de Prisma Access 5.2 Preferred, asegúrese de conocer los siguientes cambios específicos de 10.2 y consideraciones de actualización antes de programar la actualización: • Cambios en el comportamiento predeterminado • Consideraciones sobre el cambio a versiones anteriores/posteriores

Componente	Cambio
	• Problemas abordados para PAN-OS 10.2.10 y otras versiones de PAN-OS 10.2
Consideraciones de actualización para el Plano de datos de PAN-OS 11.2.3	Si elije que Palo Alto Networks actualice su plano de datos a PAN-OS 11.2.3 para que sea compatible con una característica Innovación de Prisma Access 5.2, asegúrese de conocer los siguientes cambios específicos de 11.2 y consideraciones de actualización antes de programar la actualización: • Cambios en el comportamiento predeterminado • Consideraciones sobre el cambio a versiones anteriores/posteriores • Problemas abordados para PAN-OS 11.2.2 y otras versiones de PAN-OS 11.2
Cambios en la interfaz web en Prisma Access 5.1	Se han introducido algunos cambios en la interfaz web de Prisma Access (Managed by Strata Cloud Manager), en Prisma Access 5.1 para admitir un máximo de 25.000 redes remotas. Consulte Compatibilidad con 25.000 redes remotas y 50.000 puertas de enlace de IKE para obtener más detalles.

Problemas conocidos de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

Prisma Access tiene los siguientes problemas conocidos.

ID del problema	Description (Descripción)
AIOPS-11286	Cuando tiene Colo-Connect habilitado, es posible que la información relacionada con las conexiones cruzadas y las conexiones no esté actualizada en los subinquilinos en un entorno de varios inquilinos.
CYR-47139	En una integración de proxy explícito del conector ZTNA, los conectores ZTNA se deshabilitan si los bloques de aplicación o los bloques de conectores del conector ZTNA están configurados con direcciones RFC6598 que entran en conflicto con las direcciones de proxy explícito. **Solución alternativa**: Si ha integrado ZTNA Connector con proxy explícito, no utilice las subredes "100.64.0.0/15", "100.72.0.0/15" o "100.88.0.0/15" para: • Bloques de aplicación de ZTNA Connector • Bloques de conectores de ZTNA Connector • Subredes IP configuradas en ZTNA Connector que tiene asociadas a aplicaciones
CYR-46759	La configuración de UDP para las consultas DNS no se respeta en el proxy explícito.
CYR-46627	El proxy explícito no es compatible si **Accept Default Route over Service Connection (Aceptar ruta predeterminada a través de la conexión de servicio)** está habilitado.
CYR-46445	Un error transitorio relacionado con el puerto 6081 que se procesó en un dispositivo NAT hizo que ZTNA Connector se cayera.

ID del problema	Description (Descripción)
	Solución alternativa: Cuando el tráfico de ZTNA Connector pasa a través de un dispositivo NAT, asegúrese de que la sesión NAT no esté asignada al puerto 6081.
CYR-46349	Al utilizar Redes remotas con proxy explícito con direccionamiento de tráfico en China, no configure reglas de direccionamiento de tráfico con categoría de URL.
CYR-46191	Si el Proxy explícito está configurado con el acceso a aplicaciones privadas habilitado y se añade el Conector ZTNA a la configuración, es posible que se requiera otra confirmación de Panorama o Strata Cloud Manager. **Solución alternativa**: Realice una pequeña modificación en la configuración de proxy explícito en Panorama o el Strata Cloud Manager que gestiona Prisma Access y envíe sus cambios.
CYR-46170	Si ha habilitado DDNS y posteriormente envía un cambio de subred de servicio a sus usuarios móviles, también debe reiniciar el complemento DDNS en la puerta de enlace de usuario móvil para que DDNS recoja el cambio. **Solución alternativa**: Introduzca el siguiente comando: **`debug software restart process pl-ddns`**
CYR-46145	Cuando el número de sistema autónomo de Prisma Access o la subred de infraestructura de Prisma Access se actualiza para un inquilino de Prisma Access existente, donde se incorporan el conector ZTNA y las aplicaciones correspondientes, se producirá una interrupción de unos 5 minutos tras la actualización.
CYR-46093	Si su implementación ha implementado la funcionalidad para admitir hasta 25.000 redes remotas y 50.000 puertas de enlace IKE, las estadísticas de uso de ancho de banda agregada muestran `No hay datos para el período de tiempo especificado` en lugar de las estadísticas de uso.
CYR-45440	Al configurar las Funciones de gestor, la información de acceso no siempre se guarda correctamente. **Solución alternativa**: Haga clic en los Complementos/ Complementos de servicios en la nube en la zona de Funciones de gestor dos o más veces para asegurarse de que la información de acceso se guarde correctamente. Haga clic

ID del problema	Description (Descripción)
	en Aceptar y Abrir de nuevo para confirmar que se hayan guardado los cambios.
CYR-45415	Los administradores con acceso deshabilitado o de solo lectura al complemento de servicios en la nube pueden modificar la configuración fuera del complemento de servicios en la nube que afecta al comportamiento de los servicios en la nube, tales como plantillas, grupos de dispositivos, eliminación de la configuración de servicios en la nube, desinstalación del complemento de servicios en la nube y carga de archivos de configuración.
CYR-45517	En la pestaña Colo-Connect, un usuario de solo lectura puede eliminar entradas de incorporación.
CYR-45440	Al configurar las Funciones de gestor, la información de acceso no siempre se guarda correctamente. **Solución alternativa**: Haga clic en los Complementos/ Complementos de servicios en la nube en la zona de Funciones de gestor dos o más veces para asegurarse de que la información de acceso se guarde correctamente. Haga clic en **OK (Aceptar)** y **Open (Abrir)** de nuevo para confirmar que se hayan guardado los cambios.
CYR-45415	Los administradores con acceso deshabilitado o de solo lectura al complemento de servicios en la nube pueden modificar la configuración fuera del complemento de servicios en la nube que afecta al comportamiento de los servicios en la nube, tales como plantillas, grupos de dispositivos, eliminación de la configuración de servicios en la nube, desinstalación del complemento de servicios en la nube y carga de archivos de configuración.
CYR-44433	El estado de los trabajos de Red remota que se realizaron correctamente puede cambiar de estado de Correcto a Pendiente.
CYR-44202	Los usuarios administrativos con acceso de solo lectura al complemento de Servicios en la nube pueden modificar la pestaña RBI.
CYR-43425	No es posible especificar **Outbound Routes for the Service (Rutas de salida para el servicio)** para conexiones de servicio si esas conexiones de servicio utilizan direcciones RFC 6598.
CYR-43400	Para conectores incorporados en grupos de conectores ZTNA con **Preserve User ID (Conservar el ID de usuario)**

ID del problema	Description (Descripción)
Este problema se ha resuelto en la versión 5.2.0 de Prisma Access. Consulte Problemas abordados de la versión 5.2.0 de Prisma Access.	marcado, **Actions (Acciones)** > **Diagnostics (Diagnósticos)** > **ping** desde la interfaz interna a las aplicaciones del centro de datos no funciona.
CYR-43262 **Este problema se ha resuelto en la versión 5.2.0 de Prisma Access. Consulte Problemas abordados de la versión 5.2.0 de Prisma Access.**	Las solicitudes de API de red remota para la incorporación de red remota devuelven un error de validación de confirmación en el complemento de Cloud Services si la configuración de BGP está incluida en la carga útil.
CYR-43222 **Este problema se ha resuelto en la versión 5.2.0 de Prisma Access. Consulte Problemas abordados de la versión 5.2.0 de Prisma Access.**	Los destinos de aplicación asignados a los grupos de conectores ZTNA basados en ID de usuario no admiten un **Probing Type (Tipo de sondeo)** de **ping icmp**. **Solución alternativa**: Utilice un **Probing Type (Tipo de sondeo)** de **none (ninguno)** o **tcp ping (ping de tcp)** para la aplicación.
CYR-43147	En el caso de los conectores ZTNA de escalado automático, durante la reducción horizontal, es posible que se eliminen prematuramente las sesiones de larga duración existentes que se controlan mediante el conector ZTNA marcado para la reducción horizontal. No debería haber ningún impacto en las nuevas sesiones de tráfico posteriores a la reducción horizontal.
CYR-43132	Durante la creación de subinquilinos en Panorama, no puede configurar unidades para redes remotas si la configuración de usuarios móviles se deja en blanco y viceversa.
CYR-42919**Este problema ahora se ha resuelto en la versión 5.2.1 de Prisma Access. Consulte Problemas abordados de la versión 5.2.1 de Prisma Access.**	Al intentar modificar o eliminar bloques IP de conector en ZTNA Connector, los cambios no se aplicaban después de una confirmación y un envío. **Solución alternativa**: Realice dos operaciones más de confirmación y envío para aplicar los cambios.
CYR-42312	User-ID en NAT no es compatible con Colo-Connect.
CYR-42259	El acceso a aplicaciones privadas para proxy explícito no funciona cuando RFC6598 está habilitado.
CYR-42244	Si solicita un cambio de nombre de la puerta de enlace de Prisma Access como parte de la función de Continuidad del negocio para fusiones y adquisiciones, el FQDN actualizado no se muestra en Strata Cloud Manager ni en Panorama.

ID del problema	Description (Descripción)
	Solución alternativa: Póngase en contacto con el equipo de cuentas de Palo Alto Networks, que abrirá un caso de SRE para actualizar el FQDN para la puerta de enlace.
CYR-42188	Cuando se utiliza el acceso a aplicaciones privadas para proxy explícito, DNS sobre TCP no funciona; sin embargo, DNS sobre UDP funciona correctamente.
CYR-42130	La información de enrutamiento de Colo-Connect no se muestra en el área de Comandos de capacidad de servicio.
CYR-42018	Si tiene habilitada la Optimización de IP, la compatibilidad con TLS 1.3 para GlobalProtect no es compatible. **Solución alternativa**: Utilice una versión máxima de TLS de 1.2.
CYR-41990	El tráfico de origen o destino de IPv6 a IPv6 o de IPv6 a IPv4 no admite las acciones de filtrado de URL **Continue (Continuar)** y **Override (Anular)**.
CYR-41838	La dirección IP de salida para las implementaciones de Redes remotas - Alto rendimiento se muestra dos veces cuando se recupera mediante la API de Prisma Access. **Solución alternativa**: Ignore la dirección IP duplicada.
CYR-41813	La incorporación de ZTNA Connector no es compatible con las ubicaciones de Suiza, Francia, Qatar o Taiwán. No hay una solución alternativa.
CYR-41228	Si tiene habilitada la optimización de IP, no puede utilizar la función de interconexión SP.
CYR-41067	Se muestra una versión incorrecta de Prisma Access en el área Versión de Prisma Access de la interfaz de usuario. En Strata Cloud Manager, la versión se muestra en **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (Acceso a NGFW y Prisma)** > **Overview (Descripción general)** > **Prisma Access Version (Versión de acceso de Prisma)**; en Prisma Access gestionado por Panorama, la versión se muestra en **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración del servicio)** > **Prisma Access Version (Versión de Prisma Access)**.
CYR-40503	IPv6 no es compatible en las regiones del Centro de Sudáfrica y Oeste de Canadá.

ID del problema	Description (Descripción)
CYR-40404	Es posible que no se detecte un destino FQDN que coincida con un comodín para un grupo de conectores si no se puede acceder a la aplicación desde algunos de los conectores ZTNA del grupo de conectores. Todos los conectores de un grupo determinado deben poder usar DNS para resolver la aplicación y acceder a la aplicación para que esta se detecte automáticamente en el grupo. **Solución alternativa**: Asocie el objeto de aplicación al grupo de conectores requerido desde Strata Cloud Manager.
CYR-39930	Los logs de Cortex Data Lake no se exportan desde inquilinos que tienen habilitada la función de Optimización de IP.
CYR-39795	Después de la instalación del complemento de servicios en la nube, el usuario __cloud_services instala un perfil de servidor Kerberos de proxy explícito (default_server_profile), a pesar de que el proxy explícito no esté habilitado. **Solución alternativa**: Ignore los cambios.
CYR-39551	Si configura el DNS dinámico de Prisma Access con un tipo de autenticación de TSIG, deberá cargar un archivo .key para el archivo de clave TSIG. El archivo de claves se considera no válido si tiene caracteres no ASCII en el contenido. Si proporciona un archivo .key para la autenticación TSIG con caracteres no ASCII y hace clic en **OK (Aceptar)**, se muestra un error `Please upload a file with the .key extension`, cargue un archivo con la extensión .key. **Solución alternativa**: Proporcione un archivo de clave tsig válido.
CYR-39153	Al realizar una actualización a un grupo de ZTNA Connector, puede haber errores de forma intermitente durante la operación de actualización. Por ejemplo, el estado de actualización se muestra como `partial_success` o `failed`, aunque algunos de los conectores afectados se actualicen posteriormente con éxito. **Solución alternativa**: Vuelva a intentar la actualización del grupo de conectores más adelante. ZTNA Connector vuelve a comprobar y le proporciona el estado adecuado de los grupos de conectores.

ID del problema	Description (Descripción)
CYR-39148	Al configurar Colo-Connect, las operaciones de **Commit and Push (Confirmar y enviar)** a los grupos de dispositivos Colo Connect pueden fallar de forma intermitente. **Solución alternativa**: Vuelva a intentar la operación de **Commit and Push (Confirmar y enviar)** al grupo de dispositivos Colo-Connect.
CYR-39028	Si está actualizando su conector ZTNA de la versión 4.1 a una versión posterior de Prisma Access y los grupos de aplicaciones del conector ZTNA están configurados dentro del espacio de direcciones RFC6598 (100.64.0.0/16 y 100.65.0.0/16), el tráfico del conector ZTNA puede estar bloqueado en el MU-SPN. **Solución alternativa**: Póngase en contacto con su equipo de Prisma Access para actualizar la versión del agente SaaS de todos sus inquilinos de Prisma Access.
CYR-38619	Los inquilinos incorporados en Suiza y Francia no pueden utilizar ZTNA Connector.
CYR-38120	Todas las ubicaciones disponibles no se muestran en la vista de lista de la página de configuración Usuarios móviles—Proxy explícito. **Solución alternativa**: Utilice la vista de mapa para seleccionar las ubicaciones que faltan.
CYR-38076	La dirección correcta del enrutador EBGP no se muestra en la página Detalles de red de redes remotas [**Remote Networks Setup (Configuración de redes remotas)** > **Remote Networks (Redes remotas)** > **EBGP Router (Enrutador EBGP)**] y, en su lugar, muestra la dirección IP de bucle invertido de la red remota.
CYR-37983	Si tiene IPv6 habilitado para un usuario de Usuarios móviles—GlobalProtect, la recuperación del informe HIP provoca un bloqueo. **Solución alternativa**: Si el cliente de GlobalProtect está habilitado para ipv6, ejecute el informe HIP utilizando la dirección IPv6 del cliente. Si el cliente de GlobalProtect solo es IPv4, ejecute el informe HIP utilizando la dirección IPv4 del cliente.
CYR-37923	Después de crear una nueva categoría de URL o regla de seguridad, o una EDL, se requiere una confirmación de

ID del problema	Description (Descripción)
	Panorama local antes de usar ese objeto en las asociaciones de reglas de seguridad de RBI.
CYR-37906	Si, al actualizar los puertos de un objeto comodín existente, se colocan espacios entre los puertos, se muestra un mensaje de error `500 internal server`. **Solución alternativa**: No coloque espacios entre los puertos. Por ejemplo, en lugar de **`1-2, 80, 100-300`**, ponga **`1-2,80,100-300`**.
CYR-37887	Si está utilizando el conector ZTNA como parte de la prueba de 30 días y no ha comprado una licencia, es posible que se produzca un error en la incorporación con un mensaje que indica que `Algo salió mal` al hacer clic en el botón **Enable ZTNA Connector (Habilitar el conector ZTNA)**. **Solución alternativa**: Actualice la interfaz de usuario para completar la incorporación de la función ZTNA Connector.
CYR-37826	Si dos o más aplicaciones de conector ZTNA tienen el mismo FQDN, un mensaje de `Application Custom rule conflict` podría aparecer en el portal de SD-WAN. **Solución alternativa**: Este mensaje es falso y se puede ignorar.
CYR-37797	La página de estado le pide una contraseña de un solo uso (OTP) después de una actualización del complemento. **Solución alternativa**: Elimine las claves de licencia caducadas, elimine el certificado de Panorama, recupere las licencias y compruebe si las claves de licencia son válidas después de recuperarlas; luego, genere la OTP para verificar.
CYR-37755	Si configura un destino comodín en el conector ZTNA y si intenta cambiar el puerto de una aplicación que se detectó como resultado de ese destino y se añadió al destino FQDN, recibirá un error que indica que el nombre es demasiado largo. **Solución alternativa**: Si bien los nombres de las aplicaciones pueden tener un máximo de 32 caracteres, cambiar el número de puerto hace que el nombre sea demasiado largo en la infraestructura del conector ZTNA. Si encuentra este error, intente dar a la aplicación un nombre más corto.

ID del problema	Description (Descripción)
CYR-37706	Cuando se utiliza el proxy explícito, se muestra una cantidad excesiva de logs de amenazas. **Solución alternativa**: Ignore los logs de amenazas. Estos logs no tienen ningún impacto en la funcionalidad del proxy explícito.
CYR-37673	Hacer clic en el enlace **Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)** > **Remote Browser Isolation (Aislamiento remoto del navegador)** > **Active Isolated Session (Activar sesión aislada)** no abre la página **Monitor (Supervisor)** > **Subscription Usage (Uso de la suscripción)** en la gestión en la nube de Prisma Access o Strata Cloud Manager.
CYR-37500	Si ha habilitado IPv6 para redes remotas, la dirección IPv6 pública no se muestra para las ubicaciones perimetrales.
CYR-37466	Si habilita Colo-Connect, no habilite la detección de reenvío bidireccional (BFD) en su VLAN.
CYR-37356	Si renueva la licencia de App Acceleration después de que haya caducado (incluido el período de gracia de la licencia), la renovación no surtirá efecto inmediatamente. **Solución alternativa**: Espere aproximadamente una hora después de la renovación de la licencia antes de usar App Acceleration.
CYR-37290	Al incorporar ZTNA Connector, recibe un error `declaim requested by root`. **Solución alternativa**: Elimine el conector que tenía el error y cree uno nuevo.
CYR-37227	La creación del grupo de conectores basado en subred IP a veces falla con un mensaje `group already exists`, aunque el grupo no exista. **Solución alternativa**: Utilice otro nombre para el grupo de conectores basado en subred IP.
CYR-37208	Al usar Prisma Access Clean Pipe, la página **Detalles de la red** [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)** > **Network Details (Detalles de la red)**] no muestra las entradas de Clean Pipe.

ID del problema	Description (Descripción)
CYR-36749	Es posible que los registros de flujo del conector ZTNA relacionados con el flujo de red no estén visibles en el visor de logs de Strata Cloud Manager.
CYR-35506	Si ha habilitado IPv6 para un inquilino, la eliminación del inquilino no libera los prefijos IPv6 que se le asignaron y esos prefijos no se pueden volver a usar. **Solución alternativa**: No elimine un inquilino que tenga IPv6 habilitado.
CYR-34999	En el caso de los inquilinos de Prisma Access de Panorama, si se incorporan conectores ZTNA, el progreso de aprovisionamiento para conexiones de servicio [**Panorama** > **Cloud Services (Servicios en la nube)** > **Status (Estado)** > **Status (Estado)** > **Service Connections (Conexiones de servicio)** > **Provision Progress (Progreso de aprovisionamiento)**] muestra el progreso del aprovisionamiento tanto para los conectores ZTNA como para las conexiones de servicio.
CYR-34770	Si configura varios portales en Prisma Access para la implementación de Usuarios móviles—GlobalProtect, debe configurar el perfil de autenticación en Autenticación de clientes en todos los portales. Si no configura al menos un perfil de autenticación, no se generará una cookie de autenticación y la función de varios portales no funcionará como se desea.
CYR-34720	La funcionalidad DDNS de GlobalProtect no funciona cuando se utiliza un Panorama con 10.1.x para gestionar Prisma Access con el complemento de Servicios en la nube.
CYR-33877	Si, durante la configuración del proxy explícito, selecciona **Skip authentication (Omitir la autenticación)** para omitir la autenticación de un objeto de dirección y más adelante desea habilitar la autenticación anulando la selección **Skip authentication (Omitir la autenticación)** para ese objeto de dirección, el cambio puede tardar hasta 24 horas en surtir efecto después de realizarlo y **Commit and Push (Confirmar y enviar)** sus cambios.
CYR-33471	Si habilita varios inquilinos, cree un nuevo subinquilino, configure los grupos de dispositivos Usuarios móviles—GlobalProtect, redes remotas y Colo-Connect y, a continuación, configure las subredes de Colo-Connect y VLAN, y un error de envío parcial con un error `No es posible recuperar la última`

ID del problema	Description (Descripción)
	`configuración sincronizada para el dispositivo` **Solución alternativa**: Realice una operación de confirmación y envío cuando configure Colo-Connect por primera vez en lugar de una confirmación parcial.
CYR-33454	Si configura Prisma Access en una implementación de varios inquilinos, multitenencia, realice una Confirmación y envío, y luego configure Colo-Connect; la opción Confirmar y enviar los cambios aparece atenuada. **Solución alternativa**: Haga clic en **Commit (Confirmar)** > **Commit to Panorama (Confirmar con Panorama)**, luego **Commit (Confirmar)** > **Push to Devices (Enviar a dispositivos)**, haga clic en **Edit Selections (Editar selecciones)** y asegúrese de que **Colo-Connect** se selecciona en el archivo **Push Scope (Ámbito de envío)**; a continuación, vuelva a intentar la operación de confirmación y envío.
CYR-33199	Los recuentos de usuarios actuales y los recuentos de usuarios de 90 días no son correctos para los usuarios autenticados por Kerberos.
CYR-33145	Cuando una licencia de Prisma Access para cualquier tipo de servicio caduca, cualquier operación de Confirmar todo genera un mensaje de error genérico `Error de confirmación`. **Solución alternativa**: Asegúrese de que todas sus licencias de Prisma Access no hayan caducado antes de realizar las confirmaciones.
CYR-32687	Las Listas dinámicas externas (EDL), los objetos de dirección de tipo **IP Wildcard Mask (Máscara de comodín IP)** y **FQDN**, y los grupos de direcciones dinámicas no funcionan en las políticas de descifrado cuando se utiliza la autenticación de agente o Kerberos con proxy explícito. **Solución alternativa**: Utilice objetos de dirección de máscara de red IP, intervalo de direcciones IP o grupos de direcciones en las políticas de descifrado.
CYR-32666	Al importar una configuración de Panorama guardada anteriormente que incluía una configuración de Colo-Connect, o al revertir una configuración guardada anteriormente, recibirá errores si se dan las siguientes condiciones:

ID del problema	Description (Descripción)

	• Está cargando una Configuración que tiene configuradas las conexiones de servicio de Colo-Connect.
	• Está cargando una configuración vacía de Prisma Access.
	• Se revierte de una configuración previamente guardada y se dan las siguientes condiciones:
	  • Existe una configuración de Colo-Connect (con conexiones de servicio) en la configuración actual y no existe una configuración de Colo-Connect en la configuración a la que desea volver.
	  • No existe una configuración de Colo-Connect en la configuración actual y existe una configuración de Colo-Connect (con conexiones de servicio) en la configuración a la que desea volver.
	  • Existe una configuración de Colo-Connect (con conexiones de servicio) en la configuración actual y también en la configuración a la que desea volver.
	Solución alternativa: Las conexiones de servicio Colo-Connect no se pueden incorporar a menos que sus VLAN correspondientes estén en estado activo. Elimine cualquier conexión de servicio de Colo-Connect antes de exportar o revertir una imagen de Panorama; a continuación, vuelva a crear las conexiones de servicio de Colo-Connect después de importar la nueva imagen.

CYR-32661	Cuando GlobalProtect se conecta en modo Proxy o en modo Túnel y Proxy, los inicios de sesión de los usuarios no contarán para el número de usuarios actuales ni para el número de usuarios que hayan iniciado sesión en los últimos 90 días en Usuarios móviles—Proxy explícito.
CYR-32564	El tráfico de la aplicación ZTNA Connector se detecta como una amenaza y se descarta para la Gestión en la nube de Prisma Access si se utiliza la categoría de URL predeterminada. **Solución alternativa**: Realice uno o más de los siguientes pasos según sea necesario: **1.** Cree una categoría de URL personalizada y añada los FQDN de aplicación para las aplicaciones incorporadas para el conector ZTNA. **2.** Si está utilizando un grupo de perfiles predeterminado, duplique un nuevo grupo y adjunte la categoría de URL personalizada que creó en el paso 1. Si utiliza un grupo de perfiles personalizados, adjunte la categoría de URL personalizada que creó en el paso 1.

ID del problema	Description (Descripción)
	3. Asegúrese de adjuntar el grupo de perfiles duplicado o el grupo de perfiles personalizados (desde el paso 2) a la política de seguridad que creó para permitir el tráfico destinado a las aplicaciones de conectores ZTNA.
CYR-32511	Puede configurar direcciones DNS IPv6 incluso si IPv6 está deshabilitado.
CYR-32431	Al configurar el proxy explícito, al agregar valores de dirección de origen de confianza en la Configuración de autenticación, configure otros ajustes y luego vuelva a la pestaña Configuración de autenticación, es posible que las direcciones de origen de confianza no se muestren correctamente. **Solución alternativa**: Actualice el Panorama que gestiona Prisma Access y, a continuación, vuelva a la pestaña Configuración de autenticación para ver las direcciones.
CYR-32191	ZTNA Connector no es compatible con entornos de varios inquilinos.
CYR-32004	Debido a una limitación en el número de perfiles IPSec actualmente compatibles con Prisma Access, al implementar el conector ZTNA, puede incorporar un máximo de 100 máquinas virtuales de conector por inquilino.
CYR-31603	Los conectores ZTNA con dos interfaces no son compatibles con un grupo de conectores habilitado para el escalado automático de AWS. Esto se debe a una limitación del grupo de escalado automático de AWS que vincula ambas interfaces a la misma subred. Consulte Este artículo para obtener más detalles. **Solución alternativa:** Los conectores ZTNA con dos interfaces son compatibles con los grupos de conectores que no están habilitados para el escalado automático de AWS. Asegúrese de que todos los conectores ZTNA con dos interfaces estén contenidos en un grupo de conectores que no esté habilitado para el escaldo automático de AWS.
CYR-31187	Para utilizar la conectividad de proxy explícito de Prisma Access en la funcionalidad de GlobalProtect para la seguridad en Internet siempre activa, la URL del archivo PAC predeterminada no se rellena correctamente a menos que realice una confirmación y envío al proxy explícito de los usuarios móviles, GlobalProtect y usuarios móviles.

ID del problema	Description (Descripción)
	Solución alternativa: Al confirmar y enviar, asegúrese de elegir el proxy explícito de ambos Usuarios móviles (GlobalProtect y usuarios móviles) en el ámbito de envío al configurar la conectividad de Proxy explícito de Prisma Access en GlobalProtect.

CYR-30414	Si ha habilitado varios portales en una implementación multiinquilino que solo tiene un inquilino y, a continuación, deshabilita la funcionalidad de varios portales en ese único inquilino, podrá ver ambos portales en la interfaz de usuario.
	Solución alternativa: Abra una sesión de la CLI en Panorama que gestione Prisma Access e introduzca los siguientes comandos, luego realice una confirmación local en Panorama:
	`set plugins cloud_services multi-tenant tenants` <*tenant_name*> `mobile-users multi-portal-multi-auth no`
	`request plugins cloud_services gpcs multi-tenant tenant-name` <*tenant_name*> `multi_portal_on_off`

CYR-30044	Las EDL predefinidas no se rellenan en la lista Configuración de bloques en una nueva implementación de proxy explícito. **Solución alternativa**: Incorpore la implementación de proxy explícito, realice una operación de confirmación y envío y, a continuación, vuelva atrás y actualice la EDL en la configuración del bloque.
CYR-29964	Los intentos de reutilizar una solicitud de firma de certificado (CSR) para generar un certificado dan como resultado un error que indica que la solicitud de entidad ya existe `"Requested entity already exists"`. **Solución alternativa**: No reutilice las CSR.
CYR-29933	Los intentos de usar la llamada a la API **`verdicts:all -X "DELETE"`** más de una vez por hora da como resultado el error `{"code" :8, "message" : "Too many requests"`. **Solución alternativa**: No utilice esta llamada a la API más de una vez por hora.
CYR-29700	Si configura varios portales de GlobalProtect en una implementación de varios inquilinos de Prisma Access

ID del problema	Description (Descripción)
	multiinquilino gestionado por Panorama, la confirmación de cambios por nombre de usuario falla con un error `"global-protect-portal-8443 should have the value "GlobalProtect_Portal_8443" but it is [None]"`. **Solución alternativa**: Si ha habilitado varios portales de GlobalProtect y tiene una implementación de multitenencia de Prisma Access, realice operaciones de confirmación de Confirmar todo en lugar de confirmar cada usuario.
CYR-29160	Si el Panorama que gestiona Prisma Access está configurado en modo FIPS y usted selecciona **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM (Generar certificado para la recopilación de logs de aplicaciones de GlobalProtect y Autonomous DEM)**, el certificado no se descarga. **Solución alternativa**: Esta funcionalidad no está disponible en los dispositivos Panorama en modo FIPS hasta que el plano de datos de Prisma Access se actualice a la versión 10.2.4.
CYR-26112	Si no tiene una licencia de interconexión de red, todas las redes remotas en un entorno están completamente malladas, pero si no ha incorporado una conexión de servicio en un entorno, no se puede acceder a las redes remotas desde las redes remotas de otros entornos. **Solución alternativa**: Compre una licencia de interconexión de red o incorpore una conexión de servicio en un entorno para que las redes remotas se comuniquen con otros entornos.

Problemas conocidos para el Acceso con privilegios dinámicos

ID del problema	Description (Descripción)
PANG-4881	Si el navegador web que el usuario utilizó para autenticar el agente de Prisma Access permanece abierto, se enviará el tráfico del navegador web al agente de Prisma Access **sobre** el túnel, independientemente de cómo esté configurado el perfil de reenvío.
PANG-4870	En los dispositivos macOS que tienen instalado el agente de Prisma Access, si elimina el acceso completo al disco para la extensión de seguridad del agente de Prisma Access

ID del problema	Description (Descripción)
	(después de otorgar acceso completo al disco anteriormente), el agente de Prisma Access se bloqueará en el modo deshabilitado. **Solución alternativa:** Para conceder acceso a la extensión de seguridad, seleccione **System Settings (Configuración del sistema)** > **Privacy & Security (Privacidad y seguridad)** > **Full Disk Access (Acceso completo al disco)** y habilitando la **securityExtension (Extensión de seguridad)** de la lista de aplicaciones.
PANG-4825	Cuando configura perfiles de reenvío, existe un problema en el que la configuración de un gran número de reglas de reenvío para aplicaciones de origen, dominios de destino y direcciones IP (rutas) puede provocar un uso elevado de la CPU. **Solución alternativa**: No configure más de 100 reglas de reenvío para aplicaciones de origen, dominios de destino y direcciones IP.
NETVIS-1363	En Insights on Strata Cloud Manager, el **Project Connectivity History (Historial de conectividad del proyecto)** en la página de detalles del usuario muestra solo el nombre del proyecto y ningún otro detalle cuando el usuario del agente de Prisma Access está conectado. El historial de conectividad del proyecto está en blanco cuando el usuario no está conectado.
NETVIS-1293	En Insights, el **Project Connectivity History (Historial de conectividad del proyecto)** no muestra los datos correctos cuando el **Time Range (Rango de tiempo)** se establece en **Past 3 Hours (Últimas 3 horas)**, **Past 1 Hour (Última hora)**y **Past 15 minutes (Últimos 15 minutos)**.
NETVIS-1263	En Insights, es posible que el número de usuarios conectados que aparecen en la pestaña Proyectos no sea preciso. En algunos casos, el número de usuarios conectados en la pestaña Proyecto no coincide con el número de usuarios en la pestaña Usuarios. Por ejemplo, cuando el mismo usuario está conectado a dos proyectos en dispositivos diferentes, el número de usuarios conectados en la pestaña Proyectos no coincide con el número de usuarios en la pestaña Usuarios.
NETVIS-1207	En Insights, la pestaña Proyectos no muestra todos los grupos de direcciones IP configurados para un proyecto. Solo se muestran los grupos de direcciones IP que están en uso.

ID del problema	Description (Descripción)
EPM-1589	Al configurar perfiles de reenvío, aunque Strata Cloud Manager le permite configurar direcciones IP con comodines, el uso de caracteres comodín en las direcciones IP de destino, como **`10.*.*.*`**, no es compatible ya que provocará un comportamiento incoherente en los perfiles de reenvío.
EPM-1399	Cambiar el nombre de un proyecto en el archivo **Proyectos** de la página Acceso con privilegios dinámicos en Strata Cloud Manager no se admite en este momento. **Solución alternativa:** Para cambiar el nombre de un proyecto, elimine el proyecto existente y realice una configuración de envío del Agente de acceso, luego cree el proyecto con el nuevo nombre y realice una configuración de envío del agente de acceso.
EPM-646	En un inquilino de Prisma Access en el que está habilitado el Acceso con privilegios dinámicos, se producirá un error en un envío de configuración si intenta enviar la configuración de la infraestructura del agente de Prisma Access sin configurar primero ningún proyecto. **Solución alternativa**: Configure al menos un proyecto antes de realizar una configuración de envío.
DRS-4691	Al buscar un grupo de usuarios en Cloud Identity Engine o Strata Cloud Manager mediante la opción **Text Search (Búsqueda de texto)**, señale el nombre del grupo de usuarios con comillas dobles. Por ejemplo, al buscar un grupo de usuarios denominado EXAMPLE. User_Group, escriba "EXAMPLE.User_Group".
DRS-4406	Al configurar un proyecto en Strata Cloud Manager, no puede buscar un **User group (Grupo de usuarios)** proporcionando un nombre de grupo de usuario parcial. **Solución alternativa:** Para buscar un grupo de usuarios, introduzca el nombre completo **User group (Grupo de usuarios)**.
DOCS-5681	La habilitación de ZTNA Connector en un inquilino habilitado para el Acceso con privilegios dinámicos no es compatible con Prisma Access 5.2. La habilitación de ZTNA Connector en un inquilino habilitado para el acceso con privilegios dinámicos puede causar problemas en el enrutamiento. El servicio también puede verse afectado porque Strata Cloud Manager no

ID del problema	Description (Descripción)
	admite la eliminación de ZTNA Connector una vez que se ha creado.
DOCS-5611	Al autorizar la asignación de grupos de usuarios en Cloud Identity Engine para el Acceso con privilegios dinámicos, al seleccionar los atributos SAML que desea que Prisma Access use para la autenticación, asegúrese de seleccionar un **Username Attribute (Atributo de nombre de usuario)** que contiene **/identity/claims/name (/identidad/reclamaciones/nombre)**. Si selecciona el atributo de nombre de usuario incorrecto, los usuarios no podrán autenticarse en sus proyectos.
DOCS-5463	Existe un problema en el que pueden producirse desconexiones aleatorias del túnel si la opción **Collect HIP Data (Recopilar datos de HIP)** no está habilitada en la página Configuración del agente. Por lo tanto, no deshabilite **Collect HIP Data (Recopilar datos de HIP)** en la sección Perfil de información del host (HIP) de la página Configuración del agente de acceso.
DOCS-3650	Para que la autenticación de Cloud Identity Engine funcione en un inquilino de Prisma Access habilitado para el Acceso con privilegios dinámicos, asegúrese de que un grupo de usuarios no esté asignado a varias aplicaciones SAML en el proveedor de identidad (IdP). Si se asignan varias aplicaciones a un grupo de usuarios, Cloud Identity Engine no puede determinar a qué aplicación SAML conectarse durante la autenticación porque no hay una asignación única.
ADI-33262	En un inquilino de Prisma Access en el que está habilitado el Acceso con privilegios dinámicos, una configuración de envío **Mobile User Container (Contenedor de usuario móvil)** > **Access Agent (Agente de acceso)** fallará sin primero configurar un proyecto en Strata Cloud Manager. **Solución alternativa**: Configure al menos un proyecto antes de realizar una configuración de envío.
ADI-31750	El número de grupos de direcciones IP que se admiten por proyecto es 50. El rendimiento se verá afectado si el número de grupos de direcciones IP por proyecto supera los 50. **Solución alternativa**: No asigne más de 50 grupos de IP por proyecto.

ID del problema	Description (Descripción)
ADI-31601	En un inquilino habilitado para el Acceso con privilegios dinámicos, Strata Cloud Manager le permite configurar más de 100 grupos de IP por proyecto, aunque esto hará que la configuración de envío falle con un error genérico. **Solución alternativa**: No configure más de 100 grupos de direcciones IP por proyecto.
ADI-31538	Existe un problema en el que, al configurar un perfil de reenvío, el **Type (Tipo)** de perfil de reenvío se muestra como "Agente ZTNA" en lugar de "Agente de Prisma Access". Además, si selecciona **Add Forwarding Profile (Añadir perfil de reenvío)**, el menú desplegable muestra "Agente ZTNA" en lugar de "Agente de Prisma Access". **Solución alternativa**: Ninguno. El tipo de perfil de reenvío se cambiará a "Agente de Prisma Access" en el futuro.
ADI-31523	No cree fragmentos con descripciones que contengan caracteres especiales. Descripciones de fragmentos que contienen caracteres especiales como **! ~ @ # $ % ^ & * ( ) _ +** no son compatibles.
ADI-31306	Al configurar un perfil de reenvío, existe un problema en el que todas las opciones en la sección **Traffic Enforcement (Aplicación del tráfico)** de la página Perfil de reenvío están habilitadas de forma predeterminada. Habilitar todas estas opciones de forma predeterminada puede provocar un comportamiento inesperado o no deseado. **Solución alternativa:** Deshabilite estas opciones para el Acceso con privilegios dinámicos.
ADI-31305	Al configurar un perfil de reenvío, existe un problema en el que las opciones **Enforce FQDN DNS resolution using tunnel DNS servers (Aplicar la resolución DNS de FQDN a través de servidores DNS de túnel)** y **Resolve all FQDNs using DNS servers that are assigned by the tunnel (Windows agents only) [Resolver todos los FQDN mediante servidores DNS asignados por el túnel (solo agentes de Windows)]** se muestran en la sección **Traffic Enforcement (Aplicación del tráfico)** de la página Perfil de reenvío. Estas dos opciones no deben mostrarse, ya que la funcionalidad prevista de estas opciones se puede configurar mediante las reglas del perfil de reenvío.

ID del problema	Description (Descripción)
ADI-30902	Strata Cloud Manager utiliza la información de usuarios y grupos de usuarios de un directorio de Cloud Identity Engine en varias configuraciones, como configuraciones de proyectos de Acceso con privilegios dinámicos, configuraciones del agente de Prisma Access, políticas de seguridad y configuraciones de implementación por etapas. Después de realizar estas configuraciones, si elimina el directorio de Cloud Identity Engine, pero no elimina las configuraciones de Strata Cloud Manager que hacen referencia a esos usuarios y grupos de usuarios, es posible que encuentre errores inesperados, como "500 Internal Server Error". **Solución alternativa**: Cuando elimina un directorio de Cloud Identity Engine, también debe eliminar las configuraciones de Strata Cloud Manager que hacen referencia a los usuarios y grupos de usuarios de ese directorio.
ADI-30468	Existe un problema en la página **Access Agent (Agente de acceso)** > **Infrastructure Settings (Configuración de la infraestructura)** en Strata Cloud Manager, donde tanto la opción **Prisma Access Managed (Prisma Access gestionado)** como la opción **OnPrem DHCP Server (Servidor DHCP local)** aparecen en la sección Asignación de grupo de direcciones IP de cliente. Al aprovisionar usuarios en un inquilino de Prisma Access de disponibilidad general con el Acceso con privilegios dinámicos habilitado, asegúrese de **No** escoger **OnPrem DHCP Server (Servidor DHCP local)** porque la configuración no se puede revertir una vez guardada. **OnPrem DHCP Server (Servidor DHCP local)** no es **compatible** con los inquilinos de disponibilidad general de Acceso con privilegios dinámicos y se eliminarán de Strata Cloud Manager en una versión futura. Si selecciona **Servidor DHCP local**, el inquilino quedará inutilizable para los flujos de trabajo básicos de Acceso con privilegios dinámicos.
ADI-29665	No utilice caracteres especiales en los nombres de los proyectos, de lo contrario, Strata Cloud Manager emitirá un mensaje de error "Solicitud con formato incorrecto" cuando intente guardar la configuración del proyecto.
ADI-29434	En la página Configuración del agente de Strata Cloud Manager, el valor recomendado para el **Session timeout (Tiempo de espera de la sesión)** es de 7 días.

ID del problema	Description (Descripción)
ADI-29272	Al crear un fragmento de código, si deshabilita la opción **Add prefix to object names (Agregar prefijo a los nombres de los objetos)**, asegúrese de no utilizar nombres de configuración de agente duplicados en dos fragmentos diferentes, ya que puede dar lugar a un comportamiento inesperado.
ADI-26493	En **Access Agent (Agente de acceso)** > **Infrastructure Settings (Configuración de infraestructura)** en Strata Cloud Manager, la opción **OnPrem DHCP Server (Servidor DHCP local)** en la sección Asignación de grupo de IP de cliente no se puede seleccionar. Esto está funcionando según lo previsto ya que **Servidor DHCP local** es **No se admite** para el Acceso con privilegios dinámicos. Se cambiará el nombre de esta opción a **OnPrem DHCP Server (Preview Only) [Servidor DHCP local (solo versión preliminar)]** para que los inquilinos existentes de Prisma Access habilitados para el Acceso con privilegios dinámicos puedan funcionar correctamente.
ADI-24562	Existe un problema en el que se permite crear más de un proyecto con el mismo dominio y grupo de usuarios si esos proyectos se configuraron a partir de diferentes fragmentos de configuración. Evite esta configuración porque puede provocar un comportamiento inesperado en algunos flujos de trabajo de Strata Cloud Manager. **Solución alternativa**: No configure diferentes proyectos utilizando el mismo dominio y grupo de usuarios.

Problemas conocidos para la versión 5.2.1 de Prisma Access

ID del problema	Description (Descripción)
CYR-47139	En una integración de conector ZTNA con proxy explícito, los conectores ZTNA se desactivan si los bloques de aplicaciones, los bloques de conectores o las subredes IP del conector ZTNA utilizados para conectarse a las aplicaciones están configurados con direcciones RFC6598 que entran en conflicto con las direcciones de proxy explícito. Solución alternativa: No utilice las subredes 100.64.0.0/15, 100.72.0.0/15 o 100.88.0.0/15 para bloques de aplicaciones o conectores al configurar el conector ZTNA para su uso con proxy explícito.

ID del problema	Description (Descripción)
CYR-46759	La configuración de UDP para las consultas DNS no se respeta en el proxy explícito.
CYR-46627	El proxy explícito no es compatible si **Accept Default Route over Service Connection (Aceptar ruta predeterminada a través de la conexión de servicio)** está habilitado.
CYR-46349	Al utilizar Redes remotas con proxy explícito con direccionamiento de tráfico en China, no configure reglas de direccionamiento de tráfico con categoría de URL.
CYR-46191	Si el Proxy explícito está configurado con el acceso a aplicaciones privadas habilitado y se añade el Conector ZTNA a la configuración, es posible que se requiera otra confirmación de Panorama o Strata Cloud Manager. **Solución alternativa**: Realice una pequeña modificación en la configuración de proxy explícito en Panorama o el Strata Cloud Manager que gestiona Prisma Access y envíe sus cambios.

Problemas abordados de Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

En los temas a continuación se describen los problemas que se han abordado en las versiones 5.2 de Prisma Access y 5.2.1 de Prisma Access.

Problemas abordados de la versión 5.2.1 de Prisma Access

ID del problema	Description (Descripción)
CYR-45847	Se solucionó un problema por el cual, cuando se cambiaba una subred de servicio, se actualizaba en las puertas de enlace de Prisma Access GlobalProtect, pero el túnel de GlobalProtect se desactivaba porque NAT no se implementaba correctamente.
CYR-45341	Se solucionó un problema por el cual se agotaba el tiempo de espera de los trabajos de confirmación y envío a grupos de dispositivos Colo-Connect, lo que provocaba que las VLAN no se eliminaran.
CYR-44391	Se solucionó un problema por el cual las implementaciones de proxy explícito en China no admitían el uso de Cloud Identity Engine o SAML para la autenticación.
CYR-43690	Se solucionó un problema por el cual, al intentar modificar o eliminar bloques IP de conectores en ZTNA Connector, los cambios no se aplicaban después de una Confirmación y envío.
CYR-42919	Se solucionó un problema por el cual, al intentar modificar o eliminar bloques IP de conector en el Conector ZTNA, los cambios no se aplicaban después de una confirmación y un envío.

Problemas abordados de la versión 5.2.0-h14 de Prisma Access

ID del problema	Description (Descripción)
CYR-46782	Se ha solucionado un problema por el que los nombres de dominio que contenían caracteres no ASCII y estaban en la caché de Panorama causaban errores durante el procesamiento de comandos nsupdate en la función DDNS de GlobalProtect.
CYR-46358	Se ha corregido un problema por el que un error `Failed Plugin validation` se producía en un inquilino que no era de Prisma Access Edition durante una actualización a un complemento de Servicios en la nube que tenía cambios de Colo-Connect.
CYR-45949	Se ha solucionado un problema por el cual, si la interfaz de usuario no podía acceder a la infraestructura de Prisma Access, la pestaña de ubicación de incorporación de usuarios móviles: proxy explícito no se cargaba y permanecía en el búfer.
CYR-45932	Se ha corregido un problema por el que la verificación de envío de un solo uso (OTP) fallaba con el siguiente error: `[get-panorama-cert.py:288] <class 'AttributeError'> ("'Pan_Plugin_Client' no tiene atributo 'whitelist_keys'`
CYR-44969	Se ha corregido un problema por el que un usuario creado con un administrador basado en roles no podía ver la configuración de Servicios en la nube en la interfaz de usuario.
CYR-44766	Se ha corregido un problema por el que se producía un error al eliminar el perfil criptográfico IKE e IPSec mediante API comunes y los perfiles no se eliminaban de la configuración.

Problemas abordados de la versión 5.2.0 de Prisma Access

ID del problema	Description (Descripción)
CYR-45112	Se ha corregido un problema por el que la configuración de la puerta de enlace externa estaba atenuada al actualizar el complemento de Cloud Services a las versiones 5.1.0 o posteriores.
CYR-44598	Se solucionó un problema por el cual el estado del Servicio de creación de logs de Strata para las implementaciones de Prisma Access gestionado por Panorama mostraba un error de `Excepción <customer-id>`.
CYR-43673	Se ha corregido un problema por el que todas las configuraciones no válidas de la API se retransmitían de vuelta al administrador del sistema a través de una llamada GET.
CYR-43400	Se ha solucionado un problema en el que, para los conectores incorporados en grupos de conectores ZTNA con **Preserve User ID (Conservar el ID de usuario)** seleccionado, **Actions (Acciones)** > **Diagnostics (Diagnósticos)** > **ping** desde la interfaz interna hasta las aplicaciones del centro de datos no funcionaban.
CYR-43280	Se ha corregido un problema por el que un error de datos base64 ilegal provocaba que el DSP no generara una diferencia, diff, a pesar de que habían cambios presentes.
CYR-43262	Se ha corregido un problema por el que las solicitudes de API de red remota para la incorporación de redes remotas arrojaban un error de validación de confirmación en el complemento cuando la configuración de BGP se incluía en la carga útil.
CYR-43222	Se ha corregido un problema por el que los objetivos de aplicación asignados a los grupos de ZTNA Connector basados en ID de usuario no admitían un **Probing Type (Tipo de sondeo)** de **icmp ping (ping de icmp)**.
CYR-42377	Se corrigió un problema por el cual, al configurar la compatibilidad con el registro de DNS dinámico para la solución de problemas y actualizaciones

ID del problema	Description (Descripción)
	remotas, no se podía cargar un archivo de clave Kerberos no cifrado en el Panorama que gestiona Prisma Access cuando el **Authentication Type (Tipo de autenticación)** era **Kerberos**. Si ejecuta una implementación gestionada de Panorama con una versión de complemento 5.2.0 o superior y elige un tipo de autenticación Kerberos, cargue una clave de autenticación a través de un archivo .key que tenga la cadena codificada en base64 de la clave Kerberos recuperada del servidor DNS, por ejemplo: `"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcD` Si está ejecutando una implementación gestionada de Panorama con una versión de complemento inferior a 5.1.0 y elige un tipo de autenticación Kerberos, cargue una clave de autenticación a través de un archivo .key que tenga el archivo keytab de Kerberos sin codificar recuperado del servidor DNS.
CYR-42191	Se ha corregido un problema por el que, al configurar la compatibilidad con DNS dinámico, un archivo Kerberos válido no se cargaba correctamente y no se guardaba en la configuración del sistema.
CYR-41740	Se ha corregido un problema por el que, si había más de 100 conectores incorporados en la misma región en un corto período de tiempo, el acceso a aplicaciones privadas a través de algunos de los conectores ZTNA podía no funcionar.
CYR-38418	Se solucionó un problema por el cual, después de habilitar IPv6, una actualización del plano de datos de Prisma Access de 10.2.8-h1 a 10.2.8-h2 fallaba.
CYR-38386	Se ha corregido un problema por el que, después de que una operación de escalado automático provocara la creación de más puertas de enlace de usuario móvil, se producía un error en una operación de confirmación y envío.
CYR-37913	Se ha corregido un error por el que, si se deshabilitaba la replicación de tráfico en un proceso y se volvía a habilitar en el mismo proceso, la funcionalidad de replicación de

ID del problema	Description (Descripción)
	tráfico se veía afectada y no se replicaba ningún tráfico de red remota o de usuario móvil sin que se mostraran errores de confirmación o configuración.
CYR-37791	Se solucionó un problema por el cual, después de que un usuario cambiaba de un proyecto a otro y se conectaba a la misma ubicación de Prisma Access, la página Supervisar > Usuarios en Strata Cloud Manager no reflejaba el nombre correcto del proyecto al que el usuario cambió para los siguientes intervalos de tiempo: 3 horas, 24 horas, 7 días y 30 días.
CYR-36930	Se solucionó un problema por el cual, si un usuario móvil de GlobalProtect tenía habilitada la pila doble (IPv4 e IPv6) y se conectaba a una ubicación de Prisma Access GlobalProtect que tenía IPv6 habilitado, e IPv6 se deshabilitó posteriormente para esa ubicación, el usuario de pila doble no podía conectarse a esa ubicación.
CYR-27734	Se ha corregido un problema por el que el Optimizador de políticas para las estadísticas de uso de reglas no utilizadas no estaba visible en Panorama para grupos de dispositivos de red remotos.

Compatibilidad de Panorama con Prisma Access 5.2 y 5.2.1

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

Las versiones 5.2 y 5.2.1 de Prisma Access (Managed by Panorama) utilizan el complemento de Servicios en la nube **Cloud Services Plugin 5.2**. Prisma Access 5.2.1 se activa mediante una versión de revisión del complemento 5.2. Si usa Panorama para gestionar Prisma Access y necesita actualizar al complemento 5.2, necesita:

1. Revisar las versiones de software necesarias para que Panorama sea compatible con Prisma Access 5.2 Preferred e Innovation
2. Determinar la ruta de actualización que deberá seguir para el complemento de Servicios en la nube
3. Actualice el complemento de servicios en la nube

Versiones de software necesarias y recomendadas para Prisma Access 5.2 y 5.2.1 (gestionado por Panorama)

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

Versiones de software recomendadas para las versiones 5.2.1 Preferred e Innovation de Prisma Access

Existen dos versiones de Prisma Access 5.2.1:

- 5.2.1 Preferred ejecuta un plano de datos PAN-OS 10.2.10. Si su implementación está ejecutando una versión de plano de datos inferior, se necesita una actualización de plano de datos a PAN-OS 10.2.10 para implementar las características de 5.2.1 Preferred.
- 5.2.1 Innovation ejecuta un plan de datos PAN-OS 11.2.4. Se requiere una actualización a PAN-OS 11.2.4 para implementar las características de 5.2 Innovation.

Para las nuevas características de Prisma Access 5.2.1 Innovation, Prisma Access **recomienda que actualice su Prisma Access a las siguientes versiones** antes de instalar el complemento.

Versión Prisma Access	Versión del complemento de servicios en la nube	Versión de plano de datos requerida para 5.2.1	Versión recomendada de GlobalProtect	Versión recomendada de Panorama
5.2.1	Revisión de 5.2.0	PAN-OS 10.2.10 (necesaria para 5.2.1 Preferred) PAN-OS 11.2.4 (necesaria para 5.2.1 Innovation)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.4

Versiones de software recomendadas para las versiones 5.2 Preferred e Innovation de Prisma Access

Existen dos versiones de Prisma Access 5.2:

- 5.2 Preferred ejecuta un plano de datos PAN-OS 10.2.10. Si su implementación está ejecutando una versión de plano de datos inferior, es posible que se necesite una actualización de plano de datos a PAN-OS 10.2.10 para implementar las características de 5.2 Preferred. Si es un cliente existente, consulte Dependencias de infraestructura, complementos y plano de datos para características de la

versión 5.2.1 Preferred e Innovation de Prisma Access para ver si se requiere una actualización de plano de datos para una función de Prisma Access 5.2.

- 5.2 Innovation ejecuta un plan de datos PAN-OS de 11.2.3. Se requiere una actualización a PAN-OS 11.2.3 para implementar las características de 5.2 Innovation.

Para las nuevas características de Prisma Access 5.2 Innovation, Prisma Access **recomienda que actualice su Prisma Access a las siguientes versiones** antes de instalar el complemento.

Versión Prisma Access	Versión del complemento de servicios en la nube	Versión de plano de datos requerida para 5.2	Versión recomendada de GlobalProtect	Versión recomendada de Panorama
5.2	5.2	PAN-OS 10.2.10 (necesaria para 5.2 Preferred) PAN-OS 11.2.3 (necesaria para 5.2 Innovation)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

Consideraciones de actualización para Prisma Access gestionado por Panorama

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

Para actualizar su complemento de servicios en la nube a Prisma Access 5.2 o 5.2.1, utilice una de las siguientes rutas de actualización. Para encontrar la versión actual de su complemento en Panorama, seleccione **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Service Setup (Configuración en la nube)** y verifique la versión del complemento en el área **Plugin Alert (Alerta de complemento)** .

Asegúrese de seguir las versiones mínimas de Panorama para cada versión del complemento durante la actualización.

Versión del complemento de servicios en la nube instalado	Versión específica	Ruta de actualización del complemento
5.1	5.2 o 5.2.1	Actualice su complemento de Prisma Access 5.1 a Prisma Access 5.2 y confirme y envíe sus cambios.
5.0	5.2 o 5.2.1	**1.** Actualice su complemento de Prisma Access 5.0 a Prisma Access 5.1 y confirme y envíe sus cambios. **2.** Actualice su complemento de Prisma Access 5.1 a Prisma Access 5.2 y confirme y envíe sus cambios.
4.1 y 4.2	5.2 o 5.2.1	**1.** Actualice su complemento de Prisma Access 4.1 a Prisma Access 5.0 y confirme y envíe sus cambios. **2.** Actualice su complemento de Prisma Access 5.0 a Prisma Access 5.1 y confirme y envíe sus cambios. **3.** Actualice su complemento de Prisma Access 5.1 a Prisma Access 5.2 y confirme y envíe sus cambios.
4.0	5.2 o 5.2.1	**1.** Actualice su complemento a Prisma Access 4.1 y confirme y envíe sus cambios. **2.** Actualice su complemento a Prisma Access 5.0 y confirme y envíe sus cambios. **3.** Actualice su complemento de Prisma Access 5.0 a Prisma Access 5.1 y confirme y envíe sus cambios.

Versión del complemento de servicios en la nube instalado	Versión específica	Ruta de actualización del complemento
		4. Actualice su complemento de Prisma Access 5.1 a Prisma Access 5.2 y confirme y envíe sus cambios.
3.0, 3.1 y 3.2 Preferred	5.2 o 5.2.1	**1.** (Solo complementos 3.0) Actualice su complemento a Prisma Access 3.1 y confirme y envíe sus cambios. **2.** (Solo complementos 3.1) Actualice su complemento a Prisma Access 3.2 o 3.2.1 y confirme y envíe sus cambios. **3.** Actualice su complemento a Prisma Access 3.2 o 3.2.1 y confirme y envíe sus cambios. **4.** Actualice su complemento a Prisma Access 4.0 y confirme y envíe sus cambios. **5.** Actualice su complemento a Prisma Access 4.1 y confirme y envíe sus cambios. **6.** Actualice su complemento a Prisma Access 5.0 y confirme y envíe sus cambios. **7.** Actualice su complemento de Prisma Access 5.0 a Prisma Access 5.1 y confirme y envíe sus cambios. **8.** Actualice su complemento de Prisma Access 5.1 a Prisma Access 5.2 y confirme y envíe sus cambios.
2.2 Preferred	5.2 o 5.2.1	**1.** Actualice su complemento a Prisma Access 3.0 y confirme y envíe sus cambios. **2.** Actualice su complemento a Prisma Access 3.1 y confirme y envíe sus cambios. **3.** Actualice su complemento a Prisma Access 3.2 o 3.2.1 y confirme y envíe sus cambios. **4.** Actualice su complemento a Prisma Access 4.0 y confirme y envíe sus cambios. **5.** Actualice su complemento a Prisma Access 4.1 y confirme y envíe sus cambios. **6.** Actualice su complemento a Prisma Access 5.0 y confirme y envíe sus cambios. **7.** Actualice su complemento de Prisma Access 5.0 a Prisma Access 5.1 y confirme y envíe sus cambios. **8.** Actualice su complemento de Prisma Access 5.1 a Prisma Access 5.2 y confirme y envíe sus cambios.

Versión del complemento de servicios en la nube instalado	Versión específica	Ruta de actualización del complemento
Versiones anteriores a 2.2 Preferred	5.2 o 5.2.1	**1.** Actualice su complemento a Prisma Access 2.2 y confirme y envíe sus cambios. Si su implementación está en una versión de Prisma Access anterior a 2.2 Preferred, primero debe actualizar a 2.2 antes de poder actualizar a 3.2. No se admiten actualizaciones de las versiones 2.0 o 2.1 de Prisma Access. **2.** Actualice su complemento a Prisma Access 3.0 y confirme y envíe sus cambios. **3.** Actualice su complemento a Prisma Access 3.1 y confirme y envíe sus cambios. **4.** Actualice su complemento a Prisma Access 3.2 o 3.2.1 y confirme y envíe sus cambios. **5.** Actualice su complemento a Prisma Access 4.0 y confirme y envíe sus cambios. **6.** Actualice su complemento a Prisma Access 4.1 y confirme y envíe sus cambios. **7.** Actualice su complemento a Prisma Access 5.0 y confirme y envíe sus cambios. **8.** Actualice su complemento de Prisma Access 5.0 a Prisma Access 5.1 y confirme y envíe sus cambios. **9.** Actualice su complemento de Prisma Access 5.1 a Prisma Access 5.2 y confirme y envíe sus cambios.

Actualice el complemento de servicios en la nube

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia Prisma Access ❑ Versión 5.2 o 5.2.1 Preferred o Innovation de Minimum Required Prisma Access Version

Utilice el siguiente procedimiento para actualizar el complemento de servicios en la nube.

Prisma Access utiliza el complemento de servicios en la nube en Panorama para activar su funcionalidad.

Para obtener una lista de las versiones de software de Panorama compatibles con Prisma Access, consulte Versiones mínimas requeridas del software de Panorama en la Matriz de compatibilidad de Palo Alto Networks.

Antes de actualizar el complemento, elimine cualquier plantilla que no sea de Prisma Access de las pilas de plantillas de Prisma Access, para evitar cometer errores de validación después de la actualización, y asegúrese de que el Panorama que gestiona Prisma Access está ejecutando una versión de PAN-OS compatible.

Utilice una de las siguientes tareas para descargar e instalar el complemento de servicios en la nube.

***Solo implementaciones HA**: si tiene dos dispositivos Panorama configurados en modo de Alta disponibilidad (HA), instale el complemento en el par HA primario primero y luego en el secundario.*

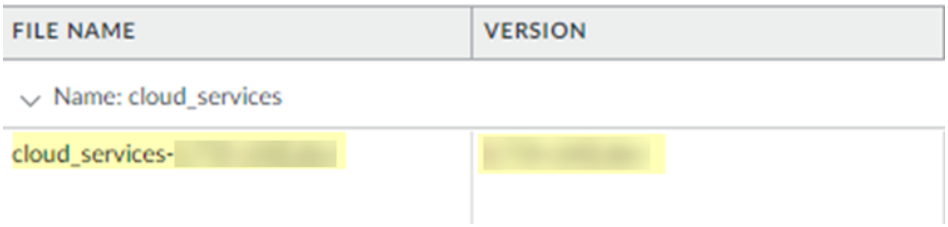
STEP 1 | Determine la ruta de actualización del complemento al que desea actualizar.

Para algunas rutas de actualización, necesita actualizar su complemento secuencialmente. Por ejemplo, para actualizar de un complemento 3.0 Preferred a un complemento 5.2, primero debe realizar actualizaciones provisionales a 3.1, 4.0, 4.1, 5.0 y 5.1 antes de actualizar a 5.2.

STEP 2 | Descargue e instale las versiones del complemento de servicios en la nube que necesite.

- Para descargar e instalar el complemento de servicios en la nube, descárguelo desde el Portal de atención al cliente, complete los siguientes pasos.
  1. Inicie sesión en el Portal de atención al cliente y seleccione **Software Updates (Actualizaciones de software)**,
  2. Busque el complemento de servicios en la nube en la sección Panorama Integration Plug In y descárguelo.

     No cambie el nombre del archivo del complemento o no podrá instalarlo en Panorama.
  3. Inicie sesión en la Interfaz Web de Panorama del Panorama que autorizó para usar con Prisma Access, seleccione **Panorama** > **Plugins (Complementos)** > **Upload (Cargar)** y **Browse (Examinar)** el **File (Archivo)** de complemento que descargó del CSP.
  4. Haga clic en **Install (Instalar)** para instalar el plugin.
- Para descargar e instalar la nueva versión del complemento de servicios en la nube directamente desde Panorama, realice los siguientes pasos:
  1. Seleccione **Panorama** > **Plugins (Complementos)** y haga clic en **Check Now (Comprobar ahora)** para mostrar las últimas actualizaciones del complemento de servicios en la nube.

  2. Proceda a **Download (Descargar)** la versión del complemento que desea instalar.
  3. Después de descargar el complemento, seleccione **Install (Instalar)** para instalarlo.

STEP 3 | (Actualizaciones de versiones inferiores a 3.2 a versiones 3.2 o posteriores) Seleccione **Commit (Confirmar)** > **Commit to Panorama (Confirmar con Panorama)** para guardar los cambios localmente en el Panorama que gestiona Prisma Access.

Solo necesita hacer una confirmación local a Panorama si vas a actualizar de un complemento de servicios en la nube anterior a 3.2 a un complemento que sea 3.2 o posterior. Las actualizaciones de una versión posterior a 3.2 no requieren una confirmación local.

Obtener ayuda

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licencia Prisma Access ❑ Minimum Required Prisma Access Version 5.2 Preferred e Innovation

Los siguientes temas proporcionan información sobre dónde encontrar más información sobre esta versión y cómo solicitar asistencia:

- Documentación relacionada:
- Solicitar asistencia

Documentación relacionada:

Utilice los siguientes documentos para configurar e implementar su implementación de Prisma Access:

- Utilice la Guía del administrador de Prisma Access para planificar, instalar, organizar y configurar Prisma Access para proteger su red.
- Utilice las tareas específicas del proveedor de la Guía de integración de Prisma Access para configurar la autenticación de usuario móvil y proteger sus implementaciones de nube pública y SD-WAN de terceros.
- Utilice la Guía de inicio de Strata Logging Service para aprender a implementar el Strata Logging Service (anteriormente Cortex Data Lake) y comenzar a reenviar logs desde sus cortafuegos locales a Cortex Data Lake.

Visite https://docs.paloaltonetworks.com para obtener más información sobre nuestros productos.

Solicitar asistencia

Para ponerse en contacto con la asistencia, para obtener información sobre programas de asistencia, gestionar su cuenta o dispositivos o abrir un caso de asistencia técnica, vaya a https://support.paloaltonetworks.com.

Para proporcionar comentarios sobre la documentación, escríbanos a: documentation@paloaltonetworks.com.

Información de contacto

Sede corporativa:

Redes de Palo Alto

3000 Tannery Way

Santa Clara, CA 95054

https://www.paloaltonetworks.com/company/contact-support

Palo Alto Networks, Inc.

www.paloaltonetworks.com

