paloalto TECHDOCS

Notes de version Prisma Access

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

Informations sur la version de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

À propos des mises à jour de la version de Prisma Access

Les versions et les mises à jour de Prisma Access vous permettent de rester à jour et de sécuriser vos utilisateurs. Certaines des mises à jour sont gérées par Palo Alto Networks, telles que celles de l'infrastructure Prisma Access se met à jour et vous recevrez une notification préalable pour vous organiser en conséquence. Certaines mises à jour relèvent de votre responsabilité et vous devez planifier la version spécifiée de la mise à jour du contenu et de la mise à jour logicielle. Si vous utilisez Panorama pour gérer Prisma Access (au lieu de Prisma Access Cloud Management), vous décidez quand effectuer la mise à niveau vers la dernière version du plug-in, afin de tirer parti des nouvelles fonctionnalités disponibles que le plug-in active pour Panorama.

Si vous utilisez Panorama Managed Prisma Access, reportez-vous aux exigences de Panorama et des plug-ins pour cette version de Panorama Managed.

Versions de GlobalProtect prises en charge à utiliser Prisma Access

Toute version de GlobalProtect qui n'est pas en fin de vie est prise en charge pour une utilisation avec Prisma Access ; cependant, notez que Prisma Access 5.2 dispose également d'un Versions logicielles recommandées pour GlobalProtect ainsi que pour les versions requises.

C'est ici que vous pouvez en savoir plus sur les dernières mises à jour des produits et services inclus ou intégrés à Prisma Access :

Dernières mises à jour de la version de Prisma Access	Versions antérieures de Prisma Access	Mises à jour des services et des modules complémentaires pris en charge par Prisma Access
• Nouvelles fonctionnalités dans Prisma Access 5.2 et 5.2.1 • Nouveautés de Prisma Access Cloud Management	• Prisma Access version 5.1 • Prisma Access version 5.0 • Prisma Access version 4.2 • Prisma Access version 4.1 • Prisma Access version 4.0 • Prisma Access version 3.2 préférée et innovation • Prisma Access version 3.1 préférée et innovation	• Prisma Access Insights • DEM autonome • Sécurité SaaS • Enterprise DLP • GlobalProtect • Plateforme de gestion cloud multilocataire Prisma SASE Multitenant Cloud Management

Dernières mises à jour de la version de Prisma Access	Versions antérieures de Prisma Access	Mises à jour des services et des modules complémentaires pris en charge par Prisma Access
	• Prisma Access version 3.0 préférée et innovation • Prisma Access version 2.2 préférée • Versions de Prisma Access antérieures à la version 2.2 préférée	• Prisma SD-WAN

Nouvelles fonctionnalités dans Prisma Access 5.2 et 5.2.1

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

Cette section vous fournit une liste des nouvelles fonctionnalités des Prisma Access 5.2 et 5.2.1 préférée et innovation, ainsi que les versions logicielles recommandées et requises que vous devez utiliser.

Ce document contient des informations sur la feuille de route et est partagé à des fins d'INFORMATION ET DE PLANIFICATION SEULEMENT. Cet engagement n'est pas contraignant et peut être modifié.

- Versions logicielles recommandées pour Prisma Access 5.2.1 préféré et innovation
- Dépendances de l'infrastructure, des plug-ins et des plans de données pour les fonctionnalités préférées et d'innovation Prisma Access 5.2.1
- Fonctionnalités de Prisma Access 5.2.1

Versions logicielles recommandées pour Prisma Access 5.2.1 préféré et innovation

Il existe deux versions de Prisma Access 5.2.1 :

- La version 5.2.1 préférée exécute un plan de données PAN-OS 10.2.10. Si votre déploiement exécute une version inférieure du plan de données, une mise à niveau du plan de données vers PAN-OS 10.2.10 est nécessaire pour implémenter les fonctionnalités de la version 5.2.1 préférée.
- La version 5.2.1 innovation exécute un plan de données PAN-OS 11.2.4. Une mise à niveau vers PAN-OS 11.2.4 est nécessaire pour implémenter les fonctionnalités de la version 5.2 innovation.

Pour les nouvelles fonctionnalités de Prisma Access 5.2.1 innovation, Prisma Access **vous recommande de mettre à jour votre Prisma Access vers les versions suivantes** avant d'installer le plug-in.

Version de Prisma Access	Version du plug-in Cloud Services	Version requise du plan de données pour 5.2.1	Version de GlobalProtect recommandée	Version de Panorama recommandée
5.2.1	Correctif d'urgence 5.2.0	PAN-OS 10.2.10 (requis pour la version 5.2.1 préférée) PAN-OS 11.2.4 (requis pour la version 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

Versions logicielles recommandées pour Prisma Access 5.2 préféré et innovation

Il existe deux versions de Prisma Access 5.2 :

- La version 5.2 préférée exécute un plan de données PAN-OS 10.2.10. Si votre déploiement exécute une version inférieure du plan de données, une mise à niveau du plan de données vers PAN-OS 10.2.10 sera sans doute nécessaire pour implémenter les fonctionnalités de la version 5.2 préférée. Si vous êtes un client existant, consultez Dépendances de l'infrastructure, des plug-ins et des plans de données pour les fonctionnalités préférées et d'innovation Prisma Access 5.2.1 pour voir si une mise à niveau du plan de données est nécessaire pour une fonctionnalité Prisma Access 5.2.
- La version 5.2 innovation exécute un plan de données PAN-OS 11.2.3. Une mise à niveau vers PAN-OS 11.2.3 est nécessaire pour implémenter les fonctionnalités de la version 5.2 innovation.

Pour les nouvelles fonctionnalités de Prisma Access 5.2 Innovation, Prisma Access **vous recommande de mettre à jour votre Prisma Access vers les versions suivantes** avant d'installer le plug-in.

Version de Prisma Access	Version du plug-in Cloud Services	Version du plan de données requise pour 5.2	Version de GlobalProtect recommandée	Version de Panorama recommandée
5.2	5.2	PAN-OS 10.2.10 (requis pour la version 5.2 préférée) PAN-OS 11.2.3 (requis pour la version 5.2 innovation)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

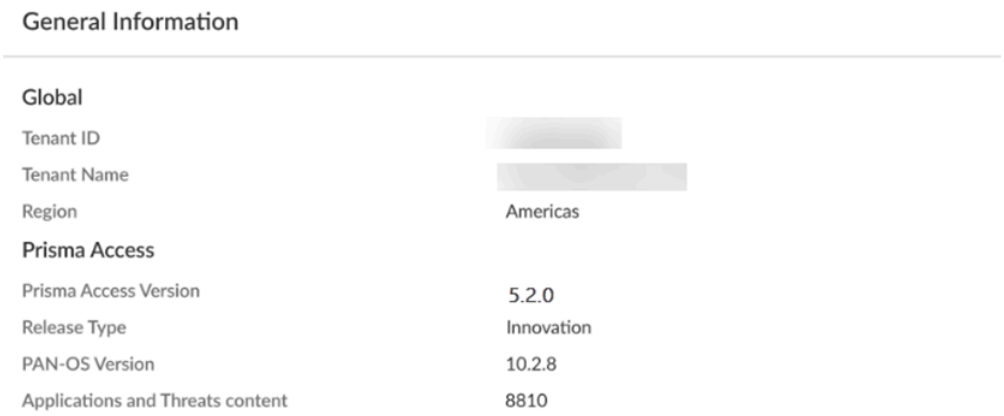
Dépendances de l'infrastructure, des plug-ins et des plans de données pour les fonctionnalités préférées et d'innovation Prisma Access 5.2.1

Les fonctionnalités de Prisma Access 5.2.1 nécessitent l'un des composants suivants pour fonctionner:

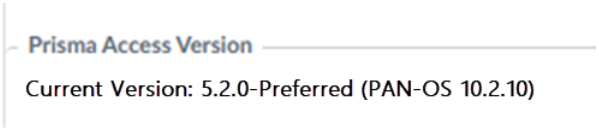
- **Mise à niveau de l'infrastructure** : l'infrastructure comprend l'infrastructure de backend, d'orchestration et de surveillance des services sous-jacents. Prisma Access met à niveau l'infrastructure avant la date de disponibilité générale (GA) d'une version Prisma Access.

  Les fonctionnalités qui nécessitent uniquement une mise à niveau de l'infrastructure pour être déverrouillées prennent effet pour tous les déploiements de Prisma Access, quelle que soit la version, au moment de la mise à niveau de l'infrastructure.
- **Mise à niveau du plug-in (déploiements gérés par Prisma Access Panorama uniquement)** : l'installation du plug-in active les fonctionnalités disponibles avec cette version. Vous téléchargez et installez le plug-in sur le Panorama qui gère Prisma Access.

- **Mise à niveau du plan de données** : le plan de données permet l'inspection du trafic et l'application de politiques de sécurité sur votre réseau et le trafic utilisateur.
  - Pour Prisma Access (Managed by Strata Cloud Manager), accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)**.'



  - Pour les déploiements Prisma Access (Managed by Panorama), vous pouvez afficher la version de votre plan de données en allant dans **Panorama** > **Cloud Services (Services cloud)** > **Configuration** > **Service Setup (Configuration du service)** et en affichant la **version de Prisma Access** . Prisma Access 5.2.1 version préférée exécute PAN-OS 10.2.10 et Prisma Access innovation PAN-OS 11.2.4.



Une mise à niveau du plan de données vers la version 5.2.1 Innovation est facultative et n'est requise que si vous souhaitez profiter des fonctionnalités qui nécessitent une mise à niveau de plan de données.

Ces fonctionnalités sont activées avec la **mise à niveau de l'infrastructure** uniquement pour Prisma Access :

- Visibilité des sites de succursales à haute performance
- Observabilité de l'agent Prisma Access
- RFC6598 Groupe d'adresses des utilisateurs mobiles pour les nouveaux déploiements Prisma Access (Managed by Strata Cloud Manager)
- Visibilité de la table des routes sur les sites des succursales et les connexions aux services
- Mises à jour pour afficher et surveiller les connecteurs ZTNA
- Voir le proxy explicite basé sur l'agent
- Support régional du service de journalisation Strata en Israël et en Arabie Saoudite
- Support IPv6 natif pour les déploiements Prisma Access existants

Ces fonctionnalités nécessitent **une mise à niveau de l'infrastructure** mais pas une mise à niveau du plan de données ; cependant, la version 10.2.4 minimum du plan de données est requise pour ces fonctionnalités :

- Support explicite du proxy pour Colo-Connect
- Support explicite du proxy DNS
- Intégration explicite de proxy avec le connecteur ZTNA
- Mise à jour de la configuration de la politique du connecteur ZTNA avec le FQDN à caractères génériques
- Intégration explicite du navigateur d'entreprise tiers Proxy

Les fonctionnalités 5.2.1 suivantes nécessitent une mise à niveau de l'**infrastructure et des plug-ins** et nécessitent au minimum la version minimale PAN-OS 10.2.10 du plan de données, ce qui en fait les Prisma Access fonctionnalités 5.2.1 préférées :

- Amélioration du connecteur ZTNA pour l'intégration d'applications
- None

Les fonctionnalités 5.2 suivantes nécessitent une mise à niveau de l'**infrastructure, du plug-in et du plan de données** vers PAN-OS 11.2.4, ce qui en fait des fonctionnalités d'innovation Prisma Access 5.2.1 :

- Réseau à distance : support de l'accès aux apps privées hautes performances
- Améliorations de l'adresse IP statique pour les utilisateurs mobiles
- Afficher l'allocation d'adresse IP statique pour les utilisateurs mobiles

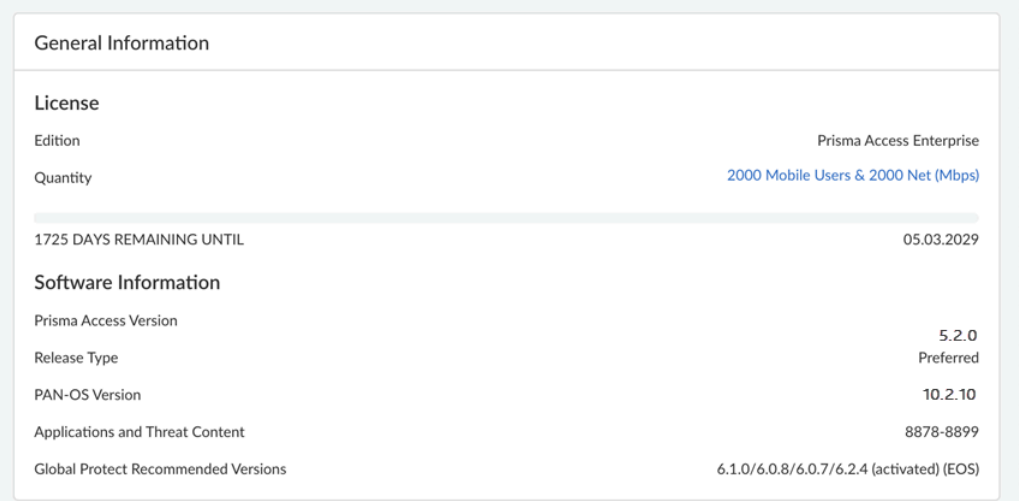
Dépendances de l'infrastructure, des plug-ins et du plan de données pour les fonctionnalités préférées et d'innovation de Prisma Access 5.2

Les fonctionnalités de Prisma Access 5.2 nécessitent l'un des composants suivants pour fonctionner :

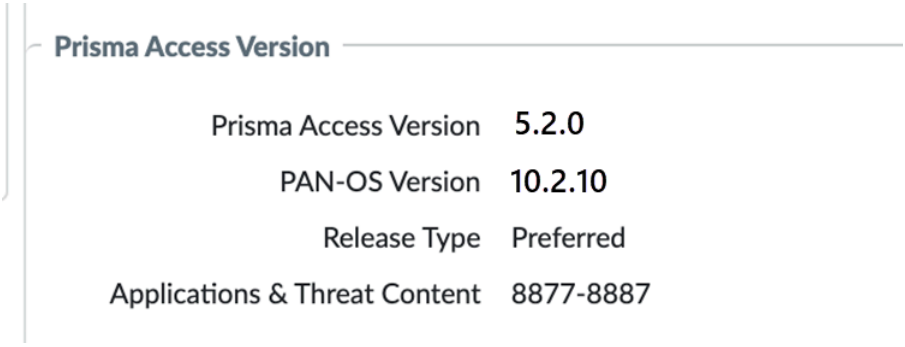
- **Mise à niveau de l'infrastructure** : l'infrastructure comprend l'infrastructure de backend, d'orchestration et de surveillance des services sous-jacents. Prisma Access met à niveau l'infrastructure avant la date de disponibilité générale (GA) d'une version Prisma Access.

  Les fonctionnalités qui nécessitent uniquement une mise à niveau de l'infrastructure pour être déverrouillées prennent effet pour tous les déploiements de Prisma Access, quelle que soit la version, au moment de la mise à niveau de l'infrastructure.
- **Mise à niveau du plug-in (déploiements gérés par Prisma Access Panorama uniquement)** : l'installation du plug-in active les fonctionnalités disponibles avec cette version. Vous téléchargez et installez le plug-in sur le Panorama qui gère Prisma Access.

- **Mise à niveau du plan de données** : le plan de données permet l'inspection du trafic et l'application de politiques de sécurité sur votre réseau et le trafic utilisateur.
  - Pour Prisma Access (Managed by Strata Cloud Manager), accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)**.



  - Pour les déploiements Prisma Access (Managed by Panorama), vous pouvez afficher la version de votre plan de données en allant dans **Panorama** > **Cloud Services (Services cloud)** > **Configuration** > **Service Setup (Configuration du service)** et en affichant la **version de Prisma Access** . Prisma Access 5.2 version préférée exécute PAN-OS 10.2.10 et Prisma Access innovation exécute PAN-OS 11.2.3.



Une mise à niveau de plan de données vers la version 5.2 Innovation est facultative et n'est requise que si vous souhaitez profiter des fonctionnalités qui nécessitent une mise à niveau de plan de données.

Ces fonctionnalités sont activées avec la **mise à niveau de l'infrastructure** uniquement pour Prisma Access :

- DLP de terminal
- Simplifiez la connectivité SaaS Prisma Access avec l'optimisation IP pour les utilisateurs mobiles et aux déploiements explicites de proxy
- Support de TLS 1.3 et de PubSub pour la réplication du trafic
- Afficher et surveiller Colo-Connect

Ces fonctionnalités nécessitent une **mise à niveau de l'infrastructure et du plug-in** mais ne nécessitent pas de mise à niveau du plan de données :

- Support de 25 000 réseaux distants et de 50 000 passerelles IKE
- Visibilité et application de l'adresse IP privée pour le trafic de proxy basé sur l'agent
- Optimisation de l'adresse IP pour les utilisateurs de proxys explicites : déploiements de proxys
- Support RBAC du plug-in Cloud Services
- Connectivité de l'application privée Prisma Access simplifiée :
- Prise en charge de l'intégration des dorsales des fournisseurs de services pour AWS
- Voir les versions de Prisma Access, du plan de données, de l'application et du contenu des menaces dans Strata Cloud Manager

Les fonctionnalités 5.2 suivantes nécessitent une mise à niveau de l'**infrastructure et des plug-ins** et nécessitent au minimum la version PAN-OS 10.2.10 du plan de données, ce qui en fait les fonctionnalités préférées de Prisma Access 5.2 :

- Réseaux distants : haute performance

Les fonctionnalités 5.2 suivantes nécessitent une mise à niveau de l'**infrastructure, du plug-in et du plan de données** vers Prisma Access 11.2.3, ce qui en fait des fonctionnalités d'innovation Prisma Access 5.2 :

- Le support SC-NAT pour Dynamic Privilege Access avec CIAM a
- Support du connecteur ZTNA pour l'intégration d'applis sans engagement

Fonctionnalités de Prisma Access 5.2.1

Le tableau suivant décrit les nouvelles fonctionnalités qui seront généralement disponibles avec Prisma Access 5.2.1.

Support explicite du proxy pour Colo-Connect

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Si vous disposez de grands centres de données avec une connectivité directe aux installations de colocalisation, vous pouvez maintenant vous connecter via le proxy explicite Prisma Access, permettant un accès à haut débit aux applications privées. Grâce à cette amélioration, vous recevrez jusqu'à 20 Gbit/s de débit par région.

L'intégration de Colo-Connect avec le proxy explicite offre les avantages suivants :

- Le proxy explicite se connecte automatiquement à l'emplacement de calcul Prisma Access le plus proche, vous offrant ainsi la meilleure latence possible.
- Élimine les dépendances de réseau et de routage, offrant une gestion et un routage automatisés de tunnel sécurisé pour les applications privées.
- Colo-Connect prend en charge la récupération d'applications privées dans des réseaux superposés, garantissant ainsi flexibilité et accessibilité

Support explicite du proxy DNS

Pris en charge dans : Prisma Access (Managed by Strata Cloud Manager) 5.2.1 version préférée et innovation

Le proxy explicite étend son support à la personnalisation du proxy DNS. Le proxy explicite prend en charge les paramètres DNS tels que les paramètres DNS régionaux, les paramètres DNS personnalisés et ainsi de suite. Vous pouvez également utiliser un résolveur DNS tiers ou un résolveur DNS sur site pour résoudre les applis publiques et privées. Vous pouvez également utiliser le résolveur selon le FQDN. Cette fonctionnalité est actuellement prise en charge sur uniquement.

Intégration sécurisée de navigateurs d’entreprises tierces avec proxy explicite

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Prisma Access peut désormais permettre un accès sécurisé aux applications privées via des navigateurs d’entreprise tiers. Grâce à cette amélioration, les informations utilisateur peuvent être échangées de manière sécurisée et transparente entre le navigateur d’entreprise tiers et Prisma Access, permettant l’application de règles de politique basées sur l’ID utilisateur dans Prisma Access. Cela élimine la nécessité pour les utilisateurs finaux de se réauthentifier auprès de Prisma Access s’ils se sont déjà connectés au navigateur d’entreprise tiers.

Intégration explicite de proxy avec le connecteur ZTNA

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Les utilisateurs se connectant à des applications privées via le connecteur ZTNA peuvent désormais établir une connexion via le proxy explicite Prisma Access. Cette intégration prend en charge les connecteurs ZTNA avec une capacité allant jusqu’à 10 Gbit/s pour le navigateur Prisma Access et le proxy d’agent.

Voici les avantages supplémentaires :

- Le proxy explicite se connecte automatiquement à l’emplacement de calcul Prisma Access le plus proche avec le proxy explicite, garantissant une latence optimale.
- Élimine les dépendances de réseau et de routage, garantissant une gestion et un routage automatisés de tunnel sécurisé pour les applications privées.
- Le connecteur ZTNA prend en charge le moteur d’identité Cloud Identity Engine (CIE), qui permet la découverte automatique d’applications privées.
- Le connecteur ZTNA prend en charge la récupération d’applications privées dans des réseaux qui se chevauchent, garantissant flexibilité et accessibilité.

Visibilité des sites de succursales à haute performance

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Les succursales à haute performance (RN-HP) de Prisma Access ont des fonctionnalités distinctes par rapport aux succursales historiques, et les deux coexisteront au sein des environnements clients. Le système de gestion doit s'adapter au nouveau type de succursale RN-HP pour aider les admins réseau à résoudre les problèmes.

Support IPv6 natif pour les déploiements Prisma Access existants

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation pour tous les déploiements (le support IPv6 pour les nouveaux déploiements est assuré à partir de Prisma Access 5.1.1 ; le support pour les déploiements existants est ajouté dans Prisma Access 5.2.1)

Prisma Access étend sont support pour IPv6 à partir d'applications privées pour inclure un support complet d'IPv6 de bout en bout pour les utilisateurs mobiles, les réseaux distants et les connexions de service, et ajoute le support natif d'IPv6 pour les déploiements Prisma Access existants.

Un aspect avantageux du support IPv6 natif est sa capacité à permettre aux utilisateurs mobiles utilisant des terminaux IPv6 uniquement d'établir des connexions avec Prisma Access via des connexions IPv6 utilisant GlobalProtect. De plus, ce support facilite l'accès aux applications SaaS publiques sur Internet, en particulier lorsque ces destinations nécessitent des connexions IPv6.

IPv6 dispose d'un espace d'adresses plus grand qu'IPv4, ce qui permet d'accueillir un nombre presque illimité d'adresses IP uniques. Grâce au support natif d'IPv6, Prisma Access est conçu pour être compatible avec les connexions IPv6 et double pile, facilitant le processus de migration d'IPv4 vers IPv6. Cette compatibilité garantit la rétrocompatibilité et donne aux entreprises les moyens de passer à des réseaux cloud et compatibles IPv6.

Observabilité de l'agent Prisma Access

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

L'agent Prisma Access Agent est un agent d'accès mobile de nouvelle génération qui vous permet d'utiliser Prisma Access pour sécuriser votre main-d'œuvre mobile. Conçu pour la main-d'œuvre hybride d'aujourd'hui, Prisma Access Agent fournit un accès sécurisé et pratique aux applications d'entreprise et à Internet, et simplifie également les opérations de réseau, d'informatique et de sécurité d'une organisation. Dans Strata Cloud Manager, accédez à **Insights (Informations)** > **Activity Insights (Informations sur l'activité)** > **Users (Utilisateurs)** pour afficher des informations sur votre déploiement d'agent Prisma Access.

Réseaux à distance : support de l'accès aux apps privées hautes performances

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Le réseau distant hautes performances Prisma Access ajoute le support de l'accès privé aux applis, en plus de son support existant pour la sortie vers Internet. Ce support signifie que vous pouvez :

- Récupérer des applis privées à partir d'une succursale connectée par un réseau distant hautes performances

- Communiquer avec une autre succursale (trafic entre succursales) à l'aide de connexions de service
- Communiquer avec des utilisateurs mobiles (trafic mobile d'utilisateur à succursale) à l'aide de connexions de service

Visibilité de la table des routes sur les sites des succursales et les connexions aux services

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Améliorations de l'adresse IP statique pour les utilisateurs mobiles

Pris en charge dans : Prisma Access 5.2.1 innovation

Prisma Access s'ajoute à la fonctionnalité d'adresse IP statique pour les utilisateurs mobiles, où vous pouvez attribuer des adresses IP statiques aux utilisateurs en fonction de la salle ou de l'identifiant utilisateur Prisma Access.

Pour améliorer l'attribution d'adresses IP aux utilisateurs mobiles, vous pouvez désormais utiliser des groupes de localisation et des groupes d'utilisateurs comme critères, en plus de la salle et de l'identifiant utilisateur.

De plus, le nombre de profils de pools d'adresses IP pris en charge est porté à 10 000.

RFC6598 Groupe d'adresses des utilisateurs mobiles pour les nouveaux déploiements Prisma Access (Managed by Strata Cloud Manager)

Pris en charge dans : Prisma Access (Managed by Strata Cloud Manager) 5.2.1 version préférée et innovation

Chaque déploiement Prisma Access nécessite un pool d'adresses IP pour les utilisateurs mobiles. Prisma Access attribue une adresse IP à partir de ce pool à chaque périphérique connecté à GlobalProtect. Pour simplifier l'intégration des utilisateurs mobiles GlobalProtect, Palo Alto Networks fournit de nouveaux déploiements Prisma Access (gérés par Strata Cloud Manager) avec un pool d'adresses IP par défaut à partir du RFC6598. Le pool IP est 100.92.0.0/16. Si vous avez besoin de plus d'adresses ou si vous voulez utiliser vos propres adresses, vous pouvez modifier ce pool ou le supprimer et ajouter des pools d'adresses IP qui vous appartiennent.

Support régional du service de journalisation Strata en Israël et en Arabie Saoudite

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Prisma Access prend en charge les régions de service de journalisation en Israël et en Arabie saoudite.

Mises à jour pour afficher et surveiller les connecteurs ZTNA

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Le connecteur ZTNA (Zero Trust Network Access) simplifie l'accès aux applications privées pour toutes vos applications. La VM du connecteur ZTNA de votre environnement forme automatiquement des tunnels entre vos applications privées et . À compter de Prisma Access 5.2.1, nous avons revu l'apparence de la page ZTNA Connectors (Connecteurs ZTNA) pour votre facilité d'utilisation et ajouté des tableaux avec des détails sur vos cibles de caractères génériques, de FQDN et de sous-réseaux IP.

Voir le proxy explicite basé sur l'agent

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

En attente de description.

Afficher l'allocation d'adresse IP statique pour les utilisateurs mobiles

Pris en charge dans : Prisma Access 5.2.1 innovation

Pour surveiller les pools d'adresses IP statiques, accédez à **Insights (Informations)** > **Activity Insights (Informations sur l'activité)** > **Users (Utilisateurs** pour surveiller les pools d'adresses IP statiques dans le widget **IP Pool Utilization (Utilisation des pools)**. La fonctionnalité d'allocation IP statique vous permet d'attribuer une adresse IP fixe aux utilisateurs mobiles de Prisma Access. Cette fonctionnalité est utile si vos déploiements réseau limitent l'accès des utilisateurs aux ressources à l'aide d'adresses IP dans le cadre de leur conception de réseaux et d'applications. Avec cette fonctionnalité, vous pouvez définir un pool IP en fonction de la salle et de l'utilisateur.

Configuration du FQDN à caractères génériques pour les politiques de sécurité dans le connecteur ZTNA

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

L'utilisation du FQDN à caractères génériques dans les règles de politique de sécurité est actuellement soumise à des limitations de protocole. Par conséquent, seuls les protocoles HTTP et HTTPS sont pris en charge pour le FQDN à caractères génériques dans les règles de politique de sécurité à l'heure actuelle.

Avec cette amélioration :

- Vous pouvez configurer une politique de sécurité basée sur le FQDN de l'application à caractères génériques.
- La même politique de sécurité est appliquée à toutes les applications découvertes qui partagent le même FQDN à caractères génériques.
- Lorsque de nouvelles applications qui correspondent au FQDN à caractères génériques sont découvertes, le trafic peut être transmis sans nécessiter de nouvelle validation.

Amélioration du connecteur ZTNA pour l’intégration d’applications

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Si les utilisateurs de votre entreprise accèdent à un grand nombre d’applis privées, le connecteur ZTNA peut rencontrer des problèmes d’évolutivité lorsque le nombre d’applications dans votre infrastructure dépasse les 15 000.

Le connecteur ZTNA offre une amélioration qui améliore l’évolutivité, permettant aux utilisateurs d’intégrer :

- 20 000 applications par locataire et 4000 par groupe de connecteurs.
- 400 connecteurs sur tous les locataires avec une bande passante de 16 Gbit/s par région de calcul.

Connecteur ZTNA pour l’intégration d’applications

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

Si les utilisateurs de votre entreprise accèdent à un grand nombre d’applis privées, le connecteur ZTNA peut rencontrer des problèmes d’évolutivité lorsque le nombre d’applications dans votre infrastructure dépasse les 15 000.

Le connecteur ZTNA offre une amélioration qui améliore l’évolutivité, permettant aux utilisateurs d’intégrer :

- 20 000 applications par locataire et 4000 par groupe de connecteurs.
- 400 connecteurs sur tous les locataires avec une bande passante de 16 Gbit/s par région de calcul.

Mise à jour de la configuration de la politique du connecteur ZTNA avec le FQDN à caractères génériques

Pris en charge dans : Prisma Access 5.2.1 version préférée et innovation

L’utilisation du FQDN à caractères génériques dans les règles de politique de sécurité est actuellement soumise à des limitations de protocole. Par conséquent, seuls les protocoles HTTP et HTTPS sont pris en charge pour le FQDN à caractères génériques dans les règles de politique de sécurité à l’heure actuelle.

Avec cette amélioration :

- Vous pouvez configurer une politique de sécurité basée sur le FQDN de l’application à caractères génériques.
- La même politique de sécurité est appliquée à toutes les applications découvertes qui partagent le même FQDN à caractères génériques.
- Lorsque de nouvelles applications qui correspondent au FQDN à caractères génériques sont découvertes, le trafic peut être transmis sans nécessiter de nouvelle validation.

Fonctionnalités de Prisma Access 5.2

Cette section décrit les nouvelles fonctionnalités disponibles avec Prisma Access 5.2.

Support de 25 000 réseaux distants et de 50 000 passerelles IKE

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Pour mettre en œuvre cette fonctionnalité, contactez votre équipe de compte Palo Alto Networks, qui ouvrira un dossier SRE pour répondre à la requête.

Visibilité et application de l'adresse IP privée pour le trafic de proxy basé sur l'agent

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Les utilisateurs qui se connectent au proxy explicite Prisma Access via l'agent GlobalProtect à partir de succursales peuvent exploiter les adresses IP privées des terminaux pour la journalisation ou pour l'application basée sur l'adresse IP.

Optimisation de l'adresse IP pour les utilisateurs de proxys explicites : déploiements de proxys

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

L'optimisation des adresses IP est un ensemble d'améliorations architecturales qui réduisent le nombre total d'adresses IP dans votre déploiement, simplifiant vos flux de travail de liste d'autorisation tout en améliorant la résilience et en permettant une intégration plus rapide des locataires Prisma Access.

Adhérence de l'adresse IP

Grâce à l'adhérence des adresses IP, vous pouvez sécuriser les applis SaaS et les sites web qui nécessitent que les sessions utilisateur maintiennent la même adresse IP de sortie de Prisma Access tout au long de la session utilisateur.

Simplifier l'intégration des applications SaaS

L'ajout d'un emplacement Prisma Access ou la survenue d'un événement de mise à l'échelle sur un emplacement Prisma Access existant peut entraîner l'attribution de nouvelles adresses IP à vos déploiements de proxy explicite. Il est recommandé de récupérer les nouvelles adresses IP de sortie et de passerelle et de les ajouter à une liste d'autorisation des applications SaaS. L'optimisation des adresses IP réduit le nombre d'adresses IP que vous devez gérer dans les déploiements de grande envergure.

DLP de terminal

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

L'agent Prisma Access est requis.

Le DLP de terminal permet à vos administrateurs de sécurité de contrôler l'utilisation des périphériques en vous permettant d'autoriser ou de bloquer leur utilisation, ou d'alerter vos administrateurs de sécurité lorsqu'un périphérique est connecté à un terminal de votre organisation. Pour éviter l'exfiltration de données sensibles vers des périphériques, utilisez les méthodes de détection avancées, ainsi que des profils de données personnalisés pour définir vos propres critères de correspondance de trafic ou des profils de données basés sur ML et regex prédéfinis.

Vous installez l' sur les terminaux que vous souhaitez protéger et il détecte le mouvement de fichiers entre le terminal et le périphérique pour évaluer et appliquer vos règles de politique de DLP de terminal lorsqu'il détecte un mouvement de fichier. Si nécessaire, l' transfère le trafic vers le pour l'inspection et le prononcé du verdict. Le communique ensuite le verdict à l' qui exécute ensuite l'action configurée dans la règle de politique de DLP de terminal. De plus, l' est également responsable de l'affichage d'une notification à l'utilisateur final lorsqu'il génère un incident DLP.

L'inspection des terminaux à l'aide du est la suivante. Cela suppose que l' est correctement installé et vous avez configuré vos règles de politique de terminal DLP.

1. Un utilisateur de votre organisation connecte un périphérique à son ordinateur portable.
2. L'utilisateur déplace un fichier de son terminal vers le périphérique connecté.
3. L' enregistre une tentative, par l'utilisateur, de déplacement d'un fichier du terminal vers le périphérique et évalue la votre base de règle de politique de DLP de terminal.
   - **Aucune correspondance de règle de politique** : si aucune correspondance de règle de politique de DLP de terminal n'a été identifiée, la connexion au périphérique est autorisée et le terminal dispose de privilèges d'accès complets en lecture et en écriture au périphérique.
   - **Règle de politique de contrôle des périphériques** : si vous avez créé une règle de politique de contrôle des périphériques pour contrôler l'accès, l' exécute l'action Allow (Autoriser) ou Block (Bloquer) configurée dans la règle de politique.

     Par exemple, si la règle de politique de DLP de terminal bloque la connexion au périphérique, l' révoque les privilèges d'écriture sur le périphérique. Dans ce cas, le terminal ne peut pas charger de fichiers sur le périphérique.

     À l'inverse, si la règle de politique de DLP de terminal autorise la connexion au périphérique, l' accorde au terminal des privilèges d'accès en écriture au périphérique. Dans ce cas, le terminal peut charger des fichiers sur le périphérique.
   - **Règle de politique concernant les données en mouvement** : la connexion au périphérique est autorisée. Lorsque l' détecte le déplacement d'un fichier du terminal vers un périphérique, le fichier est transféré au pour l'inspection et le prononcé du verdict. L' transmet également des métadonnées de fichier importantes, telles que `fileSHA` que le utilise pour identifier chaque fichier transmis.

     Le envoie alors le verdict à l' et l' exécute l'action de règle de politique de DLP de terminal si des données sensibles sont détectées. Si le détecte qu'il s'agit d'un fichier qui a déjà été inspecté sur la base de `fileSHA`, alors le renvoie le verdict existant à l'. Le n'inspecte pas deux fois le même fichier.
4. L' applique l'action de règle de politique de DLP de terminal configurée dans les règles de politique concernant le contrôle des périphériques ou les données en mouvement.
5. Un incident de DLP est généré le cas échéant. Si vous avez configuré le coaching de l'utilisateur final, une notification s'affiche sur le terminal pour alerter l'utilisateur.

Support du proxy explicite en Chine

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Prisma Access prend en charge les déploiements de proxy explicites en Chine.

Support RBAC du plug-in Cloud Services

Pris en charge dans : Prisma Access (Managed by Panorama) 5.2 version préférée et innovation

Réseaux distants : haute performance

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Prisma Access propose une solution complète pour la terminaison IPSec à large bande passante, prenant en charge les grands sites, l'équilibrage de charge automatisé, l'intégration simplifiée, la redondance régionale, la gestion IP de sortie unique et la compatibilité avec diverses solutions SD-WAN, y compris Prisma SD-WAN. Ces fonctionnalités améliorent collectivement l'évolutivité, les performances et la fiabilité de la connectivité des sites distants.

À mesure que votre entreprise évolue et que vos bureaux se dispersent géographiquement, vous pouvez rapidement intégrer un site de succursale avec une bande passante élevée à l'aide d'un réseau distantperformant Prisma Access, également appelé *réseau distant hautes performances*. Ces réseaux offrent les avantages suivants :

- Ils prennent en charge jusqu'à 3 Gbit/s de bande passante globale par adresse IP de service ou adresse de terminal de service, vous offrant ainsi un nombre réduit d'adresses IP ou de FQDN à utiliser pour la terminaison du tunnel IPSec.
- Ils incluent la redondance régionale pour améliorer la disponibilité et la tolérance aux pannes.
- Ils utilisent NAT pour réduire les adresses IP de sortie publique.
- Ils simplifient l'intégration avec des recommandations intégrées au produit pour choisir des emplacements en fonction de la disponibilité géographique.
- Ils incluent le support des mesures de qualité de liaison (LQM), où Prisma SD-WAN détermine la qualité de la liaison en sondant activement les chemins VPN Secure Fabric sur les transports publics et privés et les chemins sous-jacents WAN privés. Les sondes fournissent une mesure constante des paramètres de performances du réseau, tels que la gigue, la latence et la perte de paquets. Ces mesures, ainsi que les mesures de performances spécifiques à l'application et l'accessibilité de la couche 1 à la couche 7, éclairent les décisions de transfert de trafic pour les flux d'applications nouveaux et existants.

Résumé de l'itinéraire de Dynamic Privilege Access

Pris en charge dans : Prisma Access (Managed by Strata Cloud Manager) 5.2 innovation

Sur les locataires Prisma Access activés par Dynamic Privilege Access, vous pouvez résumer les routes lors de la publicité sur les routes de l'utilisateur mobile (MU) à votre réseau local. Le résumé des routes est

bénéfique pour les entreprises qui disposent d'équipements locaux dont la capacité est limitée, tels que des routeurs cloud de base. En réduisant la demande sur ces périphériques, le résumé des routes garantit que les appareils ne dépasseront pas leur capacité d'itinéraire lors de la communication avec le centre de données.

Pour activer le résumé des routes, configurez des pools récapitulatifs globaux composés de listes de grands pools IP utilisables sur plusieurs projets. Ensuite, activez le résumé des routes dans la connexion du service Prisma Access. Lorsqu'un utilisateur utilise l'agent Prisma Access pour se connecter à un projet dont l'adresse IP se trouve dans la plage de pools de résumés globaux configurés, la connexion de service annonce le pool de résumés globaux au lieu de la route au niveau du projet de taille plus réduite. Cela contribue à réduire le nombre de routes envoyées au réseau.

Support SC-NAT de Dynamic Privilege Access avec CIAM

Pris en charge dans : Prisma Access 5.2 innovation

Utilisez le support SC-NAT pour Dynamic Privilege Access (DPA) si vous utilisez DPA et avez créé des connexions aux services pour accéder aux applis privées dans le site de votre centre de données ou de votre siège. Plusieurs projets dans votre environnement DPA peuvent subir un épuisement des adresses IP si les adresses IP du sous-réseau Infrastructure se chevauchent. Pour résoudre ce problème, Prisma Access peut implémenter le NAT source (SNAT) pour les adresses IP, qui :

- Permet à Prisma Access de cartographier une seule adresse IP pour un utilisateur mobile accédant à des applis privées à l'aide d'une connexion de service
- Vous fournit SNAT pour faciliter le routage
- Élimine le chevauchement de pools IP
- Élimine l'épuisement IPv4 entre Prisma Access et le site de votre centre de données ou de votre siège

Connectivité de l'app privée Prisma Access simplifiée

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Une façon d'accéder à une appli privée consiste à utiliser une connexion aux services, également appelée *connexion aux services-nœud d'accès d'entreprise* (SC-CAN). Il peut être difficile de se connecter à des applis privées à l'aide de connexions de service pour les raisons suivantes :

- Débit indéterministe de l'appli privée en raison des goulots d'étranglement SC-CAN
- Latence due à des sauts de transit incorrects
- Complexité opérationnelle dans le déploiement des SC-CAN

Pour résoudre ce problème, Prisma Access a amélioré son infrastructure de routage avec des améliorations de routage qui :

- Éliminent les goulots d'étranglement SC-CAN en améliorant le réseau interne
- Orchestrent une SC-CAN d'ancre lorsque c'est nécessaire, empêchant les sauts de transit incorrects et le routage inefficace

Cette conception offre les avantages suivants :

- Configuration de routage plus facile à déployer

- Configuration facile dès le jour zéro
- Bande passante déterministe de 1 Gbit/s depuis une SC-CAN donnée jusqu'au site du centre de données ou du siège social où se trouve l'appli privée

Simplifiez la connectivité SaaS Prisma Access avec l'optimisation IP pour les utilisateurs mobiles et aux déploiements explicites de proxy

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Prisma Access développe la fonctionnalité d'optimisation IP en l'offrant pour le proxy explicite ainsi que pour Mobile Users (Utilisateurs mobiles)—GlobalProtect.

Pour les déploiements Mobile Users (Utilisateurs mobiles)—Déploiements GlobalProtect, lorsqu'un grand nombre d'utilisateurs accèdent à une passerelle GlobalProtect à partir d'un emplacement, Prisma Access met automatiquement l'emplacement à l'échelle et ajoute une autre passerelle GlobalProtect. L'optimisation IP utilise une couche NAT afin que la passerelle à mise à l'échelle automatiquement utilise la même adresse IP que celle précédemment allouée, éliminant ainsi la nécessité d'ajouter des adresses IP supplémentaires aux listes d'autorisation de votre organisation.

Prisma Access étend la couche NAT aux nœuds de traitement de sécurité des proxys explicites (SPN) ainsi qu'aux SPN des utilisateurs mobiles, réduisant ainsi la nécessité d'autoriser les adresses IP de liste pour les déploiements de proxys explicites. Cette couche NAT de proxy explicite est bénéfique si vous configurez un déploiement d'utilisateurs mobiles et de proxy explicite en mode proxy ou en mode tunnel et proxy.

Prise en charge de l'intégration des dorsales des fournisseurs de services pour AWS

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Pour mettre en œuvre cette fonctionnalité, contactez votre équipe de compte Palo Alto Networks, qui ouvrira un dossier SRE pour répondre à la requête.

À compter de la version 5.2 de Prisma Access, vous (le fournisseur de services) avez désormais la possibilité de sélectionner AWS ainsi que GCP pour le trafic de sortie du cloud public de vos clients. Vous verrez les régions supplémentaires dans l'activation de votre licence, vous verrez différents onglets pour GCP et AWS dans vos connexions et pools d'adresses IP, et vous pourrez également surveiller les clouds publics séparément.

Support de TLS 1.3 et de PubSub pour la réplication du trafic

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Si vous êtes une grande organisation utilisant la réplication de trafic, vous pouvez avoir les défis suivants à relever pour déployer et utiliser cette fonction :

- Les outils qui consomment les fichiers de packet capture (capture de paquet - PCAP) nécessitent des requêtes fréquentes des compartiments pour faire face à un grand nombre de fichiers PCAP. Les outils pourraient créer des frais généraux sur les compartiments et leur utilisation pourrait être limitée par les fournisseurs de cloud.

- Lors de l'utilisation des fichiers PCAP pour l'analyse médico-légale, l'accès au traffic décrypté SSL offre une meilleure efficacité, et une part importante du traffic est cryptée TLS 1.3.

Pour résoudre ces problèmes, Prisma Access propose ces améliorations qui permettent aux outils tiers d'être plus efficaces et plus faciles à mettre à l'échelle :

- **Notifications Pub/Sub** : Prisma Access envoie de manière proactive une notification Pub/Sub lorsqu'un nouveau fichier PCAP est chargé dans le compartiment de stockage. L'utilisation de notifications Pub/Sub pour les nouveaux fichiers PCAP élimine la nécessité de développer des outils qui vous avertissent lorsqu'il y a de nouveaux fichiers dans les compartiments.
- **Support du décryptage TLS 1.3** : Prisma Access utilise TLS 1.3 lors du décryptage des fichiers PCAP, offrant ainsi une visibilité plus profonde sur le trafic. Ce support s'applique aux déploiements de réseaux distants où vous avez activé l'utilisation de règles de politique de décryptage SSL/TLS sur les fichiers PCAP.

Afficher et surveiller Colo-Connect

Pris en charge dans : Prisma Access 5.2 version préférée et innovation

Colo-Connect s'appuie sur le concept de hub de performance basé sur Colo, avec des connexions privées à large bande passante ainsi qu'une connectivité de couche 2/3 à Prisma Access à partir de hubs performants existants. Colo-Connect exploite la technologie d'interconnexion GCP native du cloud pour fournir des connexions de service à large bande passante à vos applications privées. Accédez à **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **Service Connections (Connexions aux services)** pour afficher et surveiller votre connectivité privée au cloud hybride et aux centres de données sur site via des interconnexions cloud.

Voir les versions de Prisma Access, du plan de données, de l'application et du contenu des menaces dans Strata Cloud Manager et Panorama

Pris en charge dans : Prisma Access (Managed by Strata Cloud Manager) 5.2 version préférée et innovation

Pour vous permettre d'obtenir plus d'informations sur vos déploiements de Prisma Access (géré par Strata Cloud Manager), la zone Software Information (Informations logicielles) de la page Overview (Vue d'ensemble) (**Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Vue d'ensemble)** dans Strata Cloud Manager et Prisma Access Version (**Panorama** > **Cloud Services (Services cloud)** > **Configuration** > **Service Setup (Configuration du service)**) dans Panorama vous fournit les informations suivantes :

- Version de Prisma Access
- Version du plan de données PAN-OS
- Type de version (préférée ou innovation)
- Versions du contenu des menaces et des applications

Support du connecteur ZTNA pour l’intégration d’applis sans engagement

Pris en charge dans : Prisma Access 5.2 innovation

Grâce à l’amélioration de l’intégration sans validation, vous bénéficiez d’une expérience améliorée lors de l’intégration, de la modification ou de la suppression d’applications. Le délai précédent de 5 à 10 minutes est éliminé, ce qui accélère le processus. Le temps d’intégration de vos applications prend désormais moins d’une (1) minute, ce qui vous permet de gérer rapidement et efficacement vos applications. En outre, l’échelle améliorée du connecteur ZTNA répond aux besoins des grands clients qui gèrent plus de 10 000 applications. Vous avez la capacité d’intégrer un plus grand nombre d’applications, ce qui vous offre davantage de flexibilité et d’efficacité dans vos opérations.

Modifications du comportement par défaut de Prisma Access 5.2 et 5.2.1

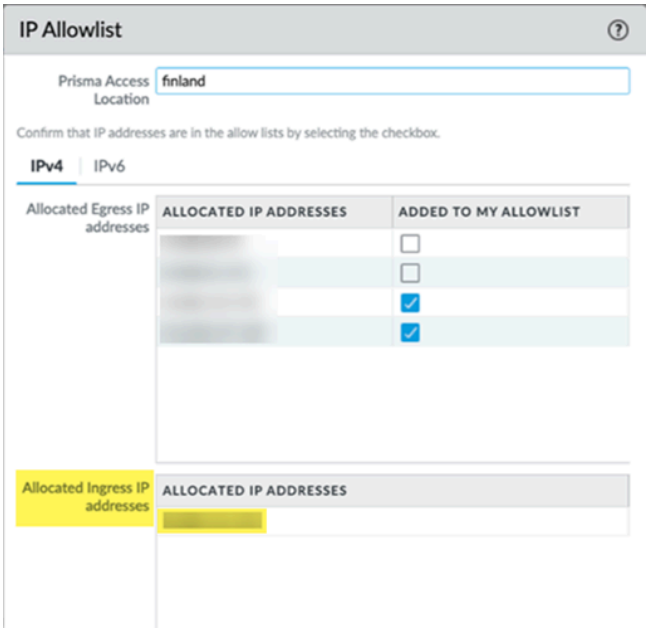
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

Les sections suivantes détaillent les modifications apportées au comportement par défaut des Prisma Access versions 5.2 et Prisma Access 5.2.1.

Modifications du comportement par défaut de Prisma Access 5.2.1

Le tableau suivant détaille les modifications apportées au comportement par défaut de Prisma Access version 5.2.1.

Composant	Changement
Optimisation IP activée pour les nouveaux déploiements de Prisma Access	Pour permettre une intégration plus rapide des locataires Prisma Access et simplifier la liste d'adresses IP autorisées, les nouveaux déploiements Prisma Access ont l'optimisation IP activée. *Les déploiements d'optimisation IP ne prennent pas en charge IPv6 pour l'accès à des applis publiques (externes) ; l'accès à des applis privées est pris en charge. Pour activer IPv6 pour votre nouveau déploiement Prisma Access, contactez l'équipe de votre compte Palo Alto Networks, qui ouvrira un dossier TAC pour répondre à la requête.* Assurez-vous que tous les utilisateurs exécutent une version de l'application GlobalProtect 6.1.4 et ultérieure, 6.2.3 et ultérieure ou 6.3.0 et ultérieure avant de configurer un nouveau déploiement Prisma Access. *L'optimisation IP n'est pas activée dans les nouveaux déploiements FedRAMP.*
Utilisateurs mobiles par défaut : le pool d'adresses IP GlobalProtect a été modifié pour les nouveaux déploiements de Prisma	Nouveaux utilisateurs mobiles de Prisma Access (géré par Strata Cloud Manager) : les déploiements de GlobalProtect disposent d'un nouveau pool d'adresses IP par défaut : 100.92.0.0/16. Il s'agit d'un changement par rapport aux déploiements précédents qui utilisaient un pool d'adresses IP par défaut de 100.127.0.0/16. Vous pouvez utiliser ce pool de RFC6598 pour la majorité des cas d'utilisation, y compris pour

Composant	Changement
Access (géré par Strata Cloud Manager)	l'accès des utilisateurs mobiles aux applis privées. Si vous avez besoin d'autres adresses IP, vous pouvez les ajouter dans l'interface utilisateur de Prisma Access.
Consolidation des adresses IP pour les déploiements qui ont migré vers l'optimisation IP	Si vous disposez d'un système Prisma Access existant qui a eu une ou plusieurs régions migrées dans l'optimisation IP et que vous utilisez la liste d'autorisations de Prisma Access, certaines adresses IP que vous avez incluses dans la liste d'autorisations ont été déplacées de la zone **Allocated Ingress IP addresses (Adresses IP de sortie allouées)** à la zone **Allocated Ingress IP addresses (Adresses IP d'entrées attribuées**) dans l'IU Prisma Access. Ce changement est le résultat de la consolidation des adresses IP dans le cadre de la mise à niveau de l'infrastructure Prisma Access 5.2.1. Vos réseaux peuvent toujours atteindre ces adresses IP et vous n'avez plus besoin de les ajouter à la liste d'autorisations. 

Modifications du comportement par défaut de Prisma Access 5.2

Composant	Changement
Considérations relatives à la mise à niveau du plan de données PAN-OS 10.2.10	Si vous choisissez de faire mettre à niveau votre plan de données à PAN-OS 10.2.10 par Palo Alto Networks pour prendre en charge une fonctionnalité Prisma Access 5.2 préférée, assurez-vous de connaître les remarques ci-après sur les modifications et les mises à niveau spécifiques à la version 10.2 et les considérations de suivantes avant de planifier la mise à niveau : • Modifications du comportement par défaut • Considérations relatives à la mise à niveau/à la rétrogradation

Composant	Changement
	• Problèmes résolus pour PAN-OS 10.2.10 et d’autres versions de PAN-OS 10.2
Considérations relatives à la mise à niveau du plan de données PAN-OS 11.2.3	Si vous choisissez de faire mettre à niveau votre plan de données à PAN-OS 11.2.3 par Palo Alto Networks pour prendre en charge une fonctionnalité Prisma Access 5.2 innovation, assurez-vous de connaître les remarques ci-après sur les modifications et les mises à niveau spécifiques à la version 11.2 et les considérations de suivantes avant de planifier la mise à niveau : • Modifications du comportement par défaut • Considérations relatives à la mise à niveau/à la rétrogradation • Problèmes résolus pour PAN-OS 11.2.2 et d’autres versions de PAN-OS 11.2
Modifications de l’interface web dans Prisma Access 5.1	Quelques Prisma Access (Managed by Strata Cloud Manager) modifications de l’interface web ont été apportées dans Prisma Access 5.1 pour prendre en charge un maximum de 25 000 réseaux distants. Pour plus d’informations, reportez-vous à la sectionSupport de 25 000 réseaux distants et de 50 000 passerelles IKE.

Problèmes connus de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

Prisma Access a les problèmes connus suivants.

ID du problème	Description
AIOPS-11286	Lorsque Colo-Connect est activé, les informations relatives aux connexions croisées et aux connexions peuvent ne pas être à jour sur les sous-locataires dans un environnement multilocataire.
CYR-47139	Les connecteurs ZTNA sont désactivés dans l'intégration ZTNA Connector - Explicit Proxy (Connecteur ZTNA - Proxy explicite) si les blocs d'application de connecteurs ZTNA ou les blocs de connecteurs sont configurés avec des adresses RFC6598 en conflit avec les adresses de proxys explicites. **Solution alternative** : Si vous avez intégré le connecteur ZTNA avec un proxy explicite, n'utilisez pas les sous-réseaux « 100.64.0.0/15 », « 100.72.0.0/15 » ou « 100.88.0.0/15 » pour : • Blocs d'application de connecteur ZTNA • Blocs du connecteur ZTNA • Sous-réseaux IP configurés dans le connecteur ZTNA que vous avez associé à des applications
CYR-46759	Les paramètres UDP pour les requêtes DNS ne sont pas honorés dans le proxy explicite.
CYR-46627	Le proxy explicite n'est pas pris en charge si l'option **Accept Default Route over Service Connection (Accepter l'itinéraire par défaut pour la connexion aux services)** est activée.
CYR-46445	Une erreur transitoire liée au port 6081 qui a été traitée sur un périphérique NAT a provoqué la panne du connecteur ZTNA.

ID du problème	Description
	Solution alternative : Lorsque le trafic du connecteur ZTNA transite par un périphérique NAT, assurez-vous que la session NAT n'est pas mappée sur le port 6081.
CYR-46349	Lorsque vous utilisez des réseaux distants avec un proxy explicite et la redirection du trafic en Chine, ne configurez pas les règles de redirection du trafic avec la catégorie d'URL.
CYR-46191	Si le proxy explicite est configuré avec l'accès aux applications privées activé et que le connecteur ZTNA est ajouté à la configuration, une autre validation depuis Panorama ou Strata Cloud Manager peut être requise. **Solution alternative** : Apportez une petite modification à la configuration du proxy explicite sur Panorama ou Strata Cloud Manager qui gère Prisma Access et transmet (Push) vos modifications.
CYR-46170	Si vous avez activé DDNS et que vous poussez plus tard une modification de sous-réseau de service à vos utilisateurs mobiles, vous devez également redémarrer le plug-in DDNS sur votre passerelle Mobile User (Utilisateur mobile) pour que DDNS capte la modification. **Solution alternative** : Saisissez la commande suivante : **`debug software restart process pl-ddns`**
CYR-46145	Lorsque le numéro de système autonome Prisma Access ou le sous-réseau infra Prisma Access sera mis à jour pour un locataire Prisma Access existant, où le connecteur ZTNA et les applications correspondantes sont intégrés, il y aura une panne pendant environ 5 minutes après la mise à jour.
CYR-46093	Si votre déploiement a implémenté la fonctionnalité pour prendre en charge jusqu'à 25 000 réseaux distants et 50 000 passerelles IKE, les statistiques d'utilisation de la bande passante agrégée affichent `No data for the specified time period (Aucune donnée pour la période spécifiée)` au lieu des statistiques d'utilisation.
CYR-45440	Lors de la configuration des rôles admin, les informations d'accès ne sont pas toujours enregistrées correctement. **Solution alternative** : Cliquez sur Plugins/Cloud Services Plugins (Plug-ins/Plug-ins Cloud Services) deux fois ou plus dans la zone Admin Roles (Rôles admin) pour vous assurer

ID du problème	Description
	que les informations d'accès sont enregistrées correctement. Cliquez à nouveau sur OK et Open (Ouvrir) pour confirmer si les modifications sont enregistrées.
CYR-45415	Les administrateurs disposant d'un accès en lecture seule ou désactivé au plug-in Cloud Services peuvent modifier la configuration en dehors du plug-in Cloud Services qui affecte le comportement des services cloud, tels que les modèles, les groupes de périphériques, la suppression de la configuration des services cloud, la désinstallation du plug-in Cloud Services et le chargement des fichiers de configuration.
CYR-45517	Dans l'onglet Colo-Connect, un utilisateur en lecture seule peut supprimer des entrées d'intégration.
CYR-45440	Lors de la configuration des rôles admin, les informations d'accès ne sont pas toujours enregistrées correctement. **Solution alternative** : Cliquez sur Plugins/Cloud Services Plugins (Plug-ins/Plug-ins Cloud Services) deux fois ou plus dans la zone Admin Roles (Rôles admin) pour vous assurer que les informations d'accès sont enregistrées correctement. Cliquez à nouveau sur **OK** et **Open (Ouvrir)** pour confirmer si les modifications sont enregistrées.
CYR-45415	Les administrateurs disposant d'un accès en lecture seule ou désactivé au plug-in Cloud Services peuvent modifier la configuration en dehors du plug-in Cloud Services qui affecte le comportement des services cloud, tels que les modèles, les groupes de périphériques, la suppression de la configuration des services cloud, la désinstallation du plug-in Cloud Services et le chargement des fichiers de configuration.
CYR-44433	L'état des tâches du réseau distant qui ont réussi peut passer de l'état Succès à l'état En attente.
CYR-44202	Les utilisateurs administratifs ayant accès en lecture seule au plug-in Cloud Services peuvent modifier l'onglet RBI.
CYR-43425	Vous ne pouvez pas spécifier de **routes sortantes pour le service** pour les connexions de service si ces connexions de service utilisent des adresses RFC 6598.
CYR-43400 **Ce problème est maintenant résolu dans Prisma Access 5.2.0. Reportez-**	Pour les connecteurs intégrés dans les groupes de connecteurs ZTNA avec l'option **Preserve User ID (Conserver l'ID)** cochée, la fonction **Actions** > **Diagnostics**

ID du problème	Description
vous à la section Problèmes résolus de Prisma Access 5.2.0.	> **ping**depuis l'interface interne vers les applis du centre de données ne fonctionne pas.
CYR-43262 **Ce problème est maintenant résolu dans la Prisma Access 5.2.0. Reportez-vous à la section Problèmes résolus de Prisma Access 5.2.0.**	Les requêtes d'API réseau distant pour l'intégration de réseaux à distance renvoient une erreur de validation commit sur le plug-in Cloud Services si la configuration BGP est incluse dans la charge utile.
CYR-43222 **Ce problème est maintenant résolu dans Prisma Access 5.2.0. Reportez-vous à la section Problèmes résolus de Prisma Access 5.2.0.**	Les cibles d'application assignées aux groupes de connecteurs ZTNA basés sur l'ID utilisateur ne prennent pas en charge le **type de sondage icmp ping**. **Solution alternative** : Utilisez le **type de sondage none** ou **tcp ping** pour l'application.
CYR-43147	Pour les connecteurs ZTNA mis à échelle automatiquement, lors de la mise à l'échelle, les sessions de longue durée existantes peuvent être abandonnées prématurément qui sont gérées par le connecteur ZTNA marqué pour la mise à l'échelle. Il ne devrait pas y avoir d'impact pour les nouvelles sessions de circulation après la mise à l'échelle.
CYR-43132	Lors de la création de sous-locataires sur Panorama, vous ne pouvez pas configurer les unités pour les réseaux distants si la configuration Utilisateurs mobiles est laissée vide, et inversement.
CYR-42919**Ce problème est maintenant résolu dans Prisma Access 5.2.1. Reportez-vous à la section Problèmes résolus de Prisma Access 5.2.1.**	Lorsque vous tentez de modifier ou de supprimer des blocs IP de connecteur dans le connecteur ZTNA, les modifications ne sont pas appliquées après une validation et une transmission (Push). **Solution alternative** : Effectuez deux autres opérations Commit and Push (Valider et transmettre) pour appliquer les modifications.
CYR-42312	User-ID Across NAT n'est pas pris en charge avec Colo-Connect.
CYR-42259	L'accès à l'appli privée de proxy explicite ne fonctionne pas lorsque RFC6598 est activé.
CYR-42244	Si vous demandez un changement de nom de passerelle Prisma Access dans le cadre de la fonctionnalité Continuité d'activité pour les fusions et acquisitions, le FQDN mis à jour ne s'affiche pas dans Strata Cloud Manager ou Panorama.

ID du problème	Description
	Solution alternative : Contactez votre équipe de compte Palo Alto Networks, qui ouvrira un dossier SRE pour mettre à jour le FQDN de la passerelle.
CYR-42188	Lorsque vous utilisez l'accès à l'appli privée de proxy explicite, DNS sur TCP ne fonctionne pas ; cependant DNS over UDP fonctionne correctement.
CYR-42130	Les informations de routage Colo-Connect ne s'affichent pas dans la zone Commandes de capacité de service.
CYR-42018	Si vous avez activé l'optimisation IP, le support de TLS 1.3 pour GlobalProtect n'est pas assuré. **Solution alternative** : Utilisez au maximum version 1.2 de TLS.
CYR-41990	Le trafic source ou de destination IPv6-vers-IPv6 ou IPv6-vers-IPv4 ne prend pas en charge les actions de filtrage des URL **Continue (Continuer)** et **Override (Remplacer)**.
CYR-41838	L'adresse IP de sortie des déploiements Remote Networks - High Performance (Réseaux distants - Hautes performances) s'affiche deux fois lorsque vous la récupérez à l'aide de l'API Prisma Access. **Solution alternative** : Ignorez l'adresse IP en double.
CYR-41813	L'intégration du connecteur ZTNA n'est pas prise en charge en Suisse, en France, au Qatar ou à Taïwan. Il n'y a pas de solution alternative.
CYR-41228	Si vous avez activé l'optimisation IP, vous ne pouvez pas utiliser la fonctionnalité d'interconnexion SP.
CYR-41067	Une version incorrecte de Prisma Access s'affiche dans la zone Version Prisma Access de l'interface utilisateur. Dans Strata Cloud Manager, la version s'affiche dans **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Vue d'ensemble)** > **Prisma Access Version (Version de Prima Access)**; dans Panorama Managed Prisma Access, la version s'affiche dans **Panorama** > **Cloud Services (Services cloud)** > **Configuration** > **Service Setup (Configuration de service)** > **Prisma Access Version (Version de Prisma Access)**.
CYR-40503	IPv6 n'est pas pris en charge dans les sites Afrique du Sud Centre et Canada Ouest.

ID du problème	Description
CYR-40404	Une cible FQDN correspondant à un caractère générique risque de ne pas être découverte pour un groupe de connecteurs si l'application n'est pas accessible depuis certains des connecteurs ZTNA du groupe de connecteurs. Tous les connecteurs d'un groupe donné doivent pouvoir utiliser DNS pour résoudre l'application et accéder à l'application pour que l'application soit découverte automatiquement dans le groupe. **Solution alternative** : Associez l'objet d'application au groupe de connecteurs requis depuis Strata Cloud Manager.
CYR-39930	Les journaux Cortex Data Lake ne sont pas exportés à partir de locataires dont la fonctionnalité d'optimisation IP est activée.
CYR-39795	Après l'installation du plug-in Cloud Services, un profil du serveur Kerberos de proxy explicite (default_server_profile) est installé par l'utilisateur __cloud_services, même si le proxy explicite n'est pas activé. **Solution alternative** : Ignorez les changements.
CYR-39551	Si vous configurez le DNS dynamique Prisma Access avec un type d'authentification TSIG, vous devez charger un fichier .key pour le fichier de clés TSIG. Le fichier clé est considéré comme non valide s'il contient des caractères non ASCII. Si vous fournissez un fichier .key pour l'authentification TSIG avec des caractères non ASCII et que vous cliquez sur **OK**, une erreur `Please upload a file with the .key extension (Veuillez charger un fichier avec l'extension .key)` s'affiche. **Solution alternative** : Fournissez un fichier de clé tsig valide.
CYR-39153	Lors de l'exécution d'une mise à niveau vers un groupe de connecteurs ZTNA, il peut y avoir des pannes par intermittence pendant l'opération de mise à niveau. Par exemple, l'état de la mise à niveau s'affiche comme `partial_success (réussite partielle)` ou `failed (échec)`, même si certains des connecteurs concernés sont mis à niveau plus tard avec succès. **Solution alternative** : Réessayez la mise à niveau du groupe de connecteurs ultérieurement. Le connecteur ZTNA vérifie

ID du problème	Description
	à nouveau et vous fournit l'état approprié des groupes de connecteurs.
CYR-39148	Lors de la configuration de Colo-Connect, les opérations **Commit and Push (Valider et transmettre)** vers les groupes d'appareils Colo Connect peuvent échouer par intermittence. **Solution alternative** : Réessayez l'opération **Commit and Push (Valider et transmettre)** dans le groupe d'appareils Colo-Connect.
CYR-39028	Si vous mettez à niveau votre connecteur ZTNA de la version 4.1 vers une version Prisma Access ultérieure et que les pools d'applications de connecteurs ZTNA sont configurés dans l'espace d'adresse RFC6598 (100.64.0.0/16 et 100.65.0.0/16), le trafic de connecteurs ZTNA peut être bloqué sur le MU-SPN. **Solution alternative** : Contactez votre équipe Prisma Access pour mettre à jour la version de l'agent SaaS de tous vos locataires Prisma Access.
CYR-38619	Les locataires embarqués en Suisse et en France ne peuvent pas utiliser le connecteur ZTNA.
CYR-38120	Tous les emplacements disponibles ne s'affichent pas dans la vue de liste dans la page de configuration Mobile Users—Explicit Proxy (Utilisateurs mobiles — Proxy explicite). **Solution alternative** : Utilisez la vue de carte pour sélectionner les emplacements manquants.
CYR-38076	L'adresse correcte du routeur EBGP ne s'affiche pas dans la page Remote Networks Network Details (Détails des réseaux distants (**Remote Networks Setup (Configuration des réseaux distants)** > **Remote Networks (Réseaux distants)** > **EBGP Router (Routeur EBGP)**) et affiche à la place l'adresse IP en boucle du réseau distant.
CYR-37983	Si IPv6 est activé pour un utilisateur de l'option Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect), la récupération du rapport HIP provoque un plantage. **Solution alternative** : Si le client GlobalProtect est compatible ipv6, exécutez le rapport HIP à l'aide de l'adresse IPv6 du client. Si le client GlobalProtect est

ID du problème	Description
	compatible IPv4 uniquement, exécutez le rapport HIP à l'aide de l'adresse ipv4 du client.
CYR-37923	Après avoir créé une catégorie d'URL, une règle de sécurité ou une liste dynamique externe (EDL), une validation Panorama locale est requise avant d'utiliser cet objet dans les associations de règles de sécurité RBI.
CYR-37906	Si, lors de la mise à jour des ports pour un objet à caractère générique existant, vous mettez des espaces entre les ports, une erreur `500 serveurs internes` s'affiche. **Solution alternative** : Ne mettez pas d'espaces entre les ports. Par exemple, au lieu de **`1-2, 80, 100-300`**, indiquez **`1-2,80,100-300`**.
CYR-37887	Si vous utilisez le connecteur ZTNA dans le cadre de l'essai de 30 jours et que vous n'avez pas acheté de licence, l'intégration peut échouer avec un message indiquant `Something went wrong (Un problème s'est produit)` passé lorsque vous cliquez sur le bouton **Enable ZTNA Connector (Activer le connecteur ZTNA)**. **Solution alternative** : Actualisez l'interface utilisateur pour terminer l'intégration de la fonctionnalité de connecteur ZTNA.
CYR-37826	Si deux ou plusieurs applications de connecteur ZTNA ont le FQDN, un message de `Application Custom rule conflict (Conflit de règles personnalisées d'application)` pourrait s'afficher dans le portail SD-WAN. **Solution alternative** : Ce message est fallacieux et peut être ignoré.
CYR-37797	La page d'état vous demande un mot de passe à usage unique (one-time password, OTP) après une mise à niveau du plug-in. **Solution alternative** : Supprimez les clés de licence arrivées à expiration, supprimez le certificat Panorama, récupérez les licences et vérifiez si les clés de licence sont valides après les avoir récupérées ; puis, générez l'OTP pour vérifier.
CYR-37755	Si vous configurez une cible à caractère générique dans le connecteur ZTNA et si vous essayez de modifier le port d'une application qui a été découverte à la suite de cette

ID du problème	Description
	cible et a été ajoutée à la cible du FQDN, vous recevez une erreur indiquant que le nom est trop long. **Solution alternative** : Alors que les noms d'applications peuvent contenir au maximum 32 caractères, la modification du numéro de port rend le nom trop long dans l'infrastructure de connecteur ZTNA. Si vous rencontrez cette erreur, essayez de donner un nom plus court à l'application.
CYR-37706	Lorsque vous utilisez le proxy explicite, une quantité excessive de journaux des menaces s'affiche. **Solution alternative** : Ignorez les journaux des menaces. Ces journaux n'ont aucun impact sur la fonctionnalité de proxy explicite.
CYR-37673	Un clic sur le lien **Panorama** > **Cloud Services (Services cloud)** > **Status (État)** > **Status (État)** > **Remote Browser Isolation (Isolation du navigateur distant)** > **Active Isolated Session (Session isolée active)** n'ouvre pas la page **Monitor (Surveiller)** > **Subscription Usage (Utilisation de l'abonnement)** dans Prisma Access Cloud Management ou Strata Cloud Manager.
CYR-37500	Si vous avez activé IPv6 pour les réseaux distants, l'adresse IPv6 publique n'est pas affichée pour les emplacements périphériques.
CYR-37466	Si vous activez Colo-Connect, n'activez pas la détection de transfert bidirectionnel (BFD) sur votre VLAN.
CYR-37356	Si vous renouvelez la licence d'accélération des applis après son expiration (y compris la période de grâce pour la licence), le renouvellement ne prend pas effet immédiatement. **Solution alternative** : Attendez environ une heure après le renouvellement de la licence avant d'utiliser l'accélération des applis.
CYR-37290	Lorsque vous embarquez un connecteur ZTNA, vous recevez une erreur `declaim requested by root (déclamation demandée par la racine)`. **Solution alternative** : Supprimez le connecteur qui avait l'erreur et créez-en un nouveau.
CYR-37227	La création du groupe de connecteurs basé sur le sous-réseau IP échoue parfois avec un message indiquant `group`

ID du problème	Description
	`already exists (le groupe existe déjà)`, même si le groupe n'existe pas. **Solution alternative** : Utilisez un autre nom pour le groupe de connecteurs basé sur le sous-réseau IP.
CYR-37208	Lorsque vous utilisez Prisma Access Clean Pipe, la page **Network Details Détails du réseau)** (**Panorama** > **Cloud Services (Services cloud)** > **Status (État)** > **Status (État)** > **Network Details (Détails du réseau)**) n'affiche pas les entrées Clean Pipe.
CYR-36749	Les journaux de flux du connecteurs ZTNA liés à Netflow peuvent ne pas être visibles dans la visionneuse de journaux Strata Cloud Manager.
CYR-35506	Si vous avez activé IPv6 pour un locataire, la suppression du locataire ne libère pas les préfixes IPv6 qui lui ont été alloués et ces préfixes ne sont plus utilisables. **Solution alternative** : Ne supprimez pas un locataire pour lequel IPv6 est activé.
CYR-34999	Pour les locataires de Panorama Prisma Access, si des connecteurs ZTNA sont intégrés, le progrès de l'approvisionnement pour les connexions de service (**Panorama** > **Cloud Services (Services cloud)** > **Status (État)** > **Status (État)** > **Service Connections (Connexions de service)** > **Provision Progress (Progrès de l'approvisionnement)**) indique le progrès de l'approvisionnement pour les connecteurs ZTNA et les connexions de service.
CYR-34770	Si vous configurez plusieurs portails dans Prisma Access pour le déploiement Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect), vous devez configurer le profil d'authentification sous Client Authentication (Authentification client) sur tous les portails. Si vous ne configurez pas au moins un profil d'authentification, aucun cookie d'authentification ne sera généré et la fonctionnalité à plusieurs portails ne fonctionnera pas comme souhaité.
CYR-34720	La fonctionnalité DDNS GlobalProtect ne fonctionne pas lorsque vous utilisez un Panorama exécutant 10.1.x pour gérer Prisma Access avec le plug-in Cloud Services.
CYR-33877	Si, lors de la configuration du proxy explicite, vous sélectionnez **Skip authentication (Ignorer**

ID du problème	Description
	l'authentification) pour ignorer l'authentification d'un objet d'adresse, puis souhaitez activer l'authentification ultérieurement en désélectionnant **Skip authentication (Ignorer l'authentification)** pour cet objet d'adresse, la prise en compte de la modification peut prendre jusqu'à 24 heures après que vous l'avez effectuée et que vous avez utilisé **Commit and Push (Valider et transmettre)**.
CYR-33471	Si vous activez la multilocation, créez un nouveau sous-locataire, configurez les groupes d'appareils Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect), Remote Networks (Réseaux distants) et Colo-Connect, puis configurez les sous-réseaux et VLAN Colo-Connect, et une validation partielle échoue avec une erreur `Unable to retrieve last in-sync configuration for the device (Impossible de récupérer la dernière configuration de synchronisation du périphérique)`. **Solution alternative** : Effectuez une opération Commit and Push (Valider et transmettre) lors de la première configuration de Colo-Connect au lieu d'une validation partielle.
CYR-33454	Si vous configurez Prisma Access dans un déploiement multilocataire, effectuez une opération Commit and Push (Valider et transmettre), puis configurez Colo-Connect, l'option Commit and Push permettant de valider et transmettre vos modifications est grisée. **Solution alternative** : Cliquez sur **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)**, puis **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques**, cliquez sur **Edit Selections (Modifier les sélections)** et assurez-vous que **Colo-Connect** est sélectionné dans **l'étendue de la transmission** ; puis, réessayez l'opération commit (valider) et push (transmission).
CYR-33199	Les comptes d'utilisateurs actuels et les comptes d'utilisateurs de 90 jours ne sont pas corrects pour les utilisateurs authentifiés Kerberos.
CYR-33145	Lorsqu'une licence Prisma Access pour n'importe quel type de service expire, toute opération Valider tout avec un message d'erreur générique `Commit Failed (Échec de la validation)`.

ID du problème	Description
	Solution alternative : Assurez-vous que toutes vos licences Prisma Access n'ont pas expiré avant d'effectuer des validations.
CYR-32687	Les EDL, les objets d'adresse de type **IP Wildcard Mask (Masquage générique d'IP)** et **FQDN**, et les groupes d'adresses dynamiques ne fonctionnent pas sur les politiques de décryptage lorsque l'authentification Agent ou Kerberos est utilisée avec le proxy explicite. **Solution alternative** : Utilisez les objets Adresse des groupes de masques réseau IP, groupes de plages d'adresses IP ou groupes d'adresses dans les politiques de décryptage.

CYR-32666	Lors de l'importation d'une configuration Panorama précédemment enregistrée qui comprenait une configuration Colo-Connect, ou du retour depuis une configuration précédemment enregistrée, vous recevez des erreurs si les conditions suivantes sont présentes :
	• Vous chargez une configuration dont les connexions de service Colo-Connect sont configurées.
	• Vous chargez une configuration Prisma Access vide.
	• Vous revenez d'une configuration précédemment enregistrée, et les conditions suivantes sont présentes :
	  • Une configuration Colo-Connect (avec connexions de service) existe sur la configuration actuelle et aucune configuration Colo-Connect n'existe sur la configuration vers laquelle vous souhaitez revenir.
	  • Aucune configuration Colo-Connect n'existe sur la configuration actuelle et une configuration Colo-Connect (avec connexions de service) existe sur la configuration vers laquelle vous souhaitez revenir.
	  • Une configuration Colo-Connect (avec connexions de service) existe sur la configuration actuelle et existe également sur la configuration vers laquelle vous souhaitez revenir.
	
	Solution alternative : Les connexions de service Colo-Connect ne peuvent pas être embarquées à moins que leurs VLAN correspondants soient dans un état actif. Supprimez toute connexion de service Colo-Connect avant d'exporter ou de retourner une image Panorama ; ensuite, recréez les connexions de service Colo-Connect après avoir importé la nouvelle image.

ID du problème	Description
CYR-32661	Lorsque GlobalProtect est connecté en mode Proxy ou en mode Tunnel and Proxy (Tunnel et proxy), les connexions d'utilisateurs ne sont pas prises en compte dans le nombre d'utilisateurs actuels ou le nombre d'utilisateurs connectés au cours des 90 derniers jours sous Mobile Users—Explicit Proxy (Utilisateurs mobiles—Proxy explicite).
CYR-32564	Le trafic de l'application Connecteur ZTNA est détecté comme une menace et supprimé pour Prisma Access Cloud Management si la catégorie d'URL par défaut est utilisée. **Solution alternative** : Exécutez une ou plusieurs des étapes suivantes au besoin : **1.** Créez une catégorie d'URL personnalisée et ajoutez des FQDN d'application pour les applications intégrées pour le connecteur ZTNA. **2.** Si vous utilisez un groupe de profils par défaut, clonez un nouveau groupe et joignez la catégorie d'URL personnalisée que vous avez créée à l'étape 1. Si vous utilisez un groupe de profils personnalisé, joignez la catégorie d'URL personnalisée que vous avez créée à l'étape 1. **3.** Assurez-vous de joindre soit le groupe de profils clonés, soit le groupe de profils personnalisés (à partir de l'étape 2) à la politique de sécurité que vous avez créée pour autoriser le trafic destiné aux applications de connecteurs ZTNA.
CYR-32511	Vous pouvez configurer les adresses DNS IPv6 même si IPv6 est désactivé.
CYR-32431	Lors de la configuration du proxy explicite, lorsque vous ajoutez des valeurs d'adresse source approuvée sous Paramètres d'authentification, configurez d'autres paramètres, puis revenez à l'onglet Authentication Settings (Paramètres d'authentification), les adresses source approuvées peuvent ne pas s'afficher correctement. **Solution alternative** : Actualisez le Panorama qui gère Prisma Access, puis revenez à l'onglet Authentication Settings (Paramètres d'authentification) pour voir les adresses.
CYR-32191	Le connecteur ZTNA n'est pas pris en charge dans les environnements multilocataires.

ID du problème	Description
CYR-32004	En raison d'une limitation du nombre de profils IPSec actuellement pris en charge dans Prisma Access, lors du déploiement du connecteur ZTNA, vous pouvez embarquer un maximum de 100 machines virtuelles de connecteur par locataire.
CYR-31603	Les connecteurs ZTNA avec deux interfaces ne sont pas pris en charge dans un groupe de connecteurs activé pour la mise à l'échelle automatique AWS. C'est dû à une limitation de groupe Auto Scale (Mise à l'échelle automatique) AWS qui lie les deux interfaces au même sous-réseau. Consultez cet article pour plus de détails. **Solution alternative :** Les connecteurs ZTNA avec deux interfaces sont pris en charge dans les groupes de connecteurs qui ne sont pas activés pour la mise à l'échelle automatique AWS. Assurez-vous que tous les connecteurs ZTNA avec deux interfaces sont contenus dans un groupe de connecteurs qui n'est pas activé pour la mise à l'échelle automatique AWS.
CYR-31187	Pour utiliser la fonctionnalité de connectivité du proxy explicite Prisma Access dans GlobalProtect pour la fonctionnalité de sécurité Internet toujours active, l'URL du fichier PAC par défaut ne se remplit pas correctement à moins que vous ne fassiez une opération commit and push (valider et transmettre) à la fois vers Mobile Users—GlobalProtect (Utilisateurs mobiles — GlobalProtect) et Mobile Users—Explicit Proxy (Utilisateurs mobiles — Proxy explicite). **Solution alternative** : Lorsque vous effectuez une opération Commit and Push (valider et transmettre), assurez-vous de choisir à la fois Mobile Users—GlobalProtect (Utilisateurs mobiles—GlobalProtect) et Mobile Users—Explicit Proxy (Utilisateurs mobiles—Proxy) explicite dans l'étendue Push (Transmission) lors de la configuration de la connectivité de proxy explicite Prisma Access dans GlobalProtect.
CYR-30414	Si vous avez activé plusieurs portails dans un déploiement multilocataire qui n'a qu'un seul locataire et que vous désactivez ensuite la fonctionnalité à plusieurs portails sur ce locataire unique, vous pouvez voir les deux portails sur l'interface utilisateur. **Solution alternative** : Ouvrez une session CLI sur le Panorama qui gère Prisma Access et entrez les commandes suivantes, puis effectuez une validation locale sur Panorama :

ID du problème	Description

	`set plug-ins cloud_services multi-tenant tenants` <*tenant_name*> `mobile-users multi-portal-multi-auth no`
	
	`demande plug-ins cloud_services gpcs multi-tenant tenant-name` <*tenant_name*> `multi_portail_on_off`

CYR-30044	Les EDL prédéfinis ne sont pas remplis dans la liste Block Settings (Paramètres de bloc) dans un nouveau déploiement de proxy explicite. **Solution alternative** : À bord de votre déploiement de proxy explicite, effectuez une opération de Commit and Push (validation et transmission), puis revenez en arrière et mettez à jour l'EDL dans les paramètres de votre bloc.
CYR-29964	Les tentatives de réutilisation d'une requête de signature de certificat (certificate signing request, CSR) pour générer un certificat entraînent une erreur « `L'entité demandée existe déjà` ». **Solution alternative** : Ne réutilisez pas les CSR.
CYR-29933	Les tentatives d'utilisation de l'appel d'API **`verdicts:all -X "DELETE"`** plus d'une fois par heure aboutissent au message d'erreur`{"code" :8, "message" : Erreur « Trop de requêtes »`. **Solution alternative** : N'utilisez pas cet appel d'API plus d'une fois par heure.
CYR-29700	Si vous configurez plusieurs portails GlobalProtect dans un déploiement multilocataire géré par Prisma Access Panorama, la validation des modifications par nom d'utilisateur échoue avec une erreur « `global-protect-portal-8443 devrait avoir la valeur « GlobalProtect_Portal_8443 » mais la valeur est [Aucun]` ». **Solution alternative** : Si vous avez activé plusieurs portails GlobalProtect et que vous disposez d'un déploiement multilocataire Prisma Access, effectuez des opérations de validation Valider tout au lieu de valider par utilisateur.
CYR-29160	Si le Panorama qui gère Prisma Access est configuré en mode FIPS et que vous sélectionnez **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM (Générer un certificat pour la collecte de journaux**

ID du problème	Description
	de l’application GlobalProtect et DEM autonome), le certificat n’est pas téléchargé. **Solution alternative** : Cette fonctionnalité n’est pas disponible sur les appareils Panorama en mode FIPS tant que votre plan de données Prisma Access n’est pas mis à niveau vers la version 10.2.4.
CYR-26112	Si vous ne possédez pas de licence Net Interconnect (interconnexion de réseaux), tous les réseaux distants d’une salle sont entièrement maillés, mais si vous n’avez pas intégré de connexion de service dans une salle, les réseaux distants ne peuvent pas être atteints à partir des réseaux distants d’autres salles. **Solution alternative** : Achetez une licence Net Interconnect ou embarquez une connexion de service dans un théâtre pour que les réseaux distants communiquent avec d’autres salles.

Problèmes connus pour Dynamic Privilege Access

ID du problème	Description
PANG-4881	Si le navigateur Web que l’utilisateur a utilisé pour authentifier l’agent Prisma Access reste ouvert, le trafic du navigateur Web vers l’agent Prisma Access sera envoyé **sur** le tunnel, quelle que soit la configuration du profil de transfert.
PANG-4870	Sur les périphériques macOS sur lesquels l’agent Prisma Access est installé, si vous supprimez l’accès au disque complet pour l’extension de sécurité pour l’agent Prisma Access (après avoir accordé un accès au disque complet précédemment), l’agent Prisma Access restera bloqué en mode désactivé. **Workaround (Solution alternative) :** Accordez l’accès à l’extension de sécurité en sélectionnant **System Settings (Paramètres système** > **Privacy & Security (Confidentialité et sécurité)** > **Accès complet au disque Full Disk Access** et en activant **securityExtension** depuis la liste des applis.
PANG-4825	Lors de la configuration de profils de transfert, un problème existe lorsque la configuration d’un grand nombre de règles de transfert pour les applications sources, les domaines de

ID du problème	Description
	destination et les adresses IP (routes) peut provoquer une utilisation élevée du processeur. **Solution alternative** : Ne configurez pas plus de 100 règles de transfert pour les applications sources, les domaines de destination et les adresses IP.
NETVIS-1363	Dans Insights (Informations) sur Strata Cloud Manager, la vue **Project Connectivity History (Historique de connectivité du projet)** dans la page de détails de l'utilisateur affiche uniquement le nom du projet et aucun autre détail lorsque l'utilisateur de l'agent Prisma Access est connecté. L'historique de connectivité du projet est vide lorsque l'utilisateur n'est pas connecté.
NETVIS-1293	Dans Insights (Informations), la zone **Project Connectivity History (Historique de connectivité du projet)** n'affiche pas les données correctes lorsque le paramètre **Time Range (Plage de temps)** est défini sur **Past 3 Hours (3 dernières heures)**, **Past 1 Hour (Dernière heure)** et **Past 15 Minutes (15 dernières minutes)**.
NETVIS-1263	Dans Informations, le nombre d'utilisateurs connectés répertoriés dans l'onglet Projects (Projets) peut ne pas être exact. Dans certains cas, le nombre d'utilisateurs connectés dans l'onglet Project (Projet) ne correspond pas au nombre d'utilisateurs dans l'onglet Utilisateurs. Par exemple, lorsqu'un même utilisateur est connecté à deux projets sur des périphériques différents, le nombre d'utilisateurs connectés dans l'onglet Projects (Projets) ne correspond pas au nombre d'utilisateurs dans l'onglet Users (Utilisateurs).
NETVIS-1207	Dans Insights (Informations), l'onglet Projects (Projets) n'affiche pas tous les pools IP configurés pour un projet. Seuls les pools IP utilisés sont affichés.
EPM-1589	Lors de la configuration de profils de transfert, même si Strata Cloud Manager vous permet de configurer des adresses IP avec des caractères génériques, l'utilisation de caractères génériques dans les adresses IP de destination, comme **`10.*.*.*`**, n'est pas prise en charge car elle entraînera un comportement incohérent dans les profils de transfert.
EPM-1399	La modification d'un nom de projet dans l'onglet **Projects (Projets)** de la page Dynamic Privilege Access dans Strata Cloud Manager n'est pas prise en charge pour le moment.

ID du problème	Description
	Workaround (Solution alternative) : Pour renommer un projet, supprimez le projet existant et effectuez une configuration push d'agent d'accès, puis créez le projet avec le nouveau nom et effectuez une configuration push d'agent d'accès.
EPM-646	Sur un locataire Prisma Access où Dynamic Privilege Access est activé, un push de configuration échouera si vous essayez de pousser la configuration de l'infrastructure Prisma Access Agent sans configurer au préalable aucun projet. **Solution alternative** : Configurez au moins un projet avant de faire une configuration push.
DRS-4691	Lorsque vous recherchez un groupe d'utilisateurs dans Cloud Identity Engine (moteur d'identité sur le cloud) ou Strata Cloud Manager à l'aide de l'option **Text Search (Recherche de texte)**, entourez le nom du groupe d'utilisateurs de guillemets doubles. Par exemple, lorsque vous recherchez un groupe d'utilisateurs nommé EXEMPLE.Groupe_utilisateurs, entrez « EXEMPLE.Groupe_utilisateurs ».
DRS-4406	Lors de la configuration d'un projet dans Strata Cloud Manager, vous ne pouvez pas rechercher de **groupe d'utilisateurs** en fournissant un nom de groupe d'utilisateurs partiel. **Workaround (Solution alternative) :** Pour rechercher un groupe d'utilisateurs, saisissez le nom complet du **groupe d'utilisateurs**.
DOCS-5681	L'activation du connecteur ZTNA sur un locataire compatible Dynamic Privilege Access n'est pas prise en charge dans Prisma Access 5.2. L'activation du connecteur ZTNA sur un locataire compatible Dynamic Privilege Access peut causer des problèmes de routage. Le service peut également être affecté, car Strata Cloud Manager ne prend pas en charge la suppression du connecteur ZTNA une fois qu'il a été créé.
DOCS-5611	Lorsque vous autorisez le mappage de groupes d'utilisateurs dans Cloud Identity Engine (moteur d'identité sur le cloud) pour Dynamic Privilege Access, lorsque vous sélectionnez les attributs SAML que vous souhaitez que Prisma Access utilise pour l'authentification, assurez-vous de sélectionner

ID du problème	Description
	un **attribut de nom d'utilisateur** qui contient **/identity/claims/name**. Si vous sélectionnez le mauvais attribut de nom d'utilisateur, vos utilisateurs ne pourront pas s'authentifier auprès de leurs projets.
DOCS-5463	Un problème existe lorsque des déconnexions aléatoires de tunnel peuvent se produire si l'option **Collect HIP Data (Collecter des données HIP)** n'est pas activée dans la page Agent Settings (Paramètres de l'agent). Par conséquent, ne désactivez pas **Collect HIP Data (Collecter des données HIP)** dans la section Host Information Profile (profil d'informations sur l'hôte - HIP) de la page Access Agent Settings (Paramètres de l'agent d'accès).
DOCS-3650	Pour que l'authentification Cloud Identity Engine (moteur d'identité sur le cloud) fonctionne sur un locataire Prisma Access compatible avec Dynamic Privilege Access, assurez-vous qu'aucun groupe d'utilisateurs n'est mappé à plusieurs applications SAML dans le fournisseur d'identité (IdP). Si plusieurs applis sont mappées à un groupe d'utilisateurs, Cloud Identity Engine (moteur d'identité sur le cloud) ne peut pas déterminer à quelle appli SAML se connecter lors de l'authentification, car il n'existe pas de mappage unique.
ADI-33262	Sur un locataire Prisma Access où Dynamic Privilege Access est activé, un push de configuration **Mobile User Container (Conteneur d'utilisateurs mobiles)** > **Access Agent (Agent d'accès)** échouera sans avoir préalablement configuré un projet dans Strata Cloud Manager. **Solution alternative** : Configurez au moins un projet avant de faire une configuration push.
ADI-31750	Le nombre de pools IP pris en charge par projet est de 50. Les performances seront affectées si le nombre de pools IP par projet dépasse 50. **Solution alternative** : N'allouez pas plus de 50 pools IP par projet.
ADI-31601	Sur un locataire compatible Dynamic Privilege Access, Strata Cloud Manager vous permet de configurer plus de 100 pools IP par projet, même s'il entraîne l'échec de la configuration push avec une erreur générique. **Solution alternative** : Ne configurez pas plus de 100 pools IP par projet.

ID du problème	Description
ADI-31538	Un problème existe quand, lors de la configuration d'un profil de transfert, le **type** de profil de transfert est affiché comme « Agent ZTNA », et non « Agent Prisma Access ». En outre, si vous sélectionnez **Add Forwarding Profile (Ajouter un profil de transfert)**, la liste déroulante affiche « Agent ZTNA », et non « Agent Prisma Access ». **Solution alternative** : Aucun. Le type de profil de transfert sera changé en « Agent Prisma Access » à l'avenir.
ADI-31523	Ne créez pas d'extraits avec des descriptions contenant des caractères spéciaux. Les descriptions des extraits qui contiennent des caractères spéciaux tels que `! ~ @ # $ % ^ & * ( ) _ +` ne sont pas prises en charge.
ADI-31306	Lors de la configuration d'un profil de transfert, un problème se pose lorsque toutes les options de la section **Traffic Enforcement (Application du trafic)** de la page Forwarding Profile (Profil de transfert) sont activées par défaut. L'activation de toutes ces options par défaut peut provoquer un comportement inattendu ou indésirable. **Workaround (Solution alternative) :** Désactivez ces options pour Dynamic Privilege Access.
ADI-31305	Lors de la configuration d'un profil de transfert, un problème se pose lorsque les options **Enforce FQDN DNS resolution using tunnel DNS servers (Appliquer la résolution DNS FQDN à l'aide de serveurs DNS tunnel)** et **Resolve all FQDNs using DNS servers that are assigned by the tunnel (Windows agents only) (Résoudre tous les noms de domaine complets à l'aide de serveurs DNS qui sont assignés par le tunnel (agents Windows uniquement))** sont affichées dans la section **Traffic Enforcement (Application du trafic)** de la page Forwarding Profile (Profil de transfert). Ces deux options ne doivent pas être affichées puisque la fonctionnalité prévue de ces options peut être configurée à l'aide des règles de profil de transfert.
ADI-30902	Strata Cloud Manager utilise les informations relatives aux utilisateurs et aux groupes d'utilisateurs d'un répertoire Cloud Identity Engine dans plusieurs configurations, telles que les configurations de projet Dynamic Privilege Access, les paramètres de l'agent Prisma Access, les politiques de sécurité et les configurations de déploiement par étapes. Après avoir effectué ces configurations, si vous supprimez

ID du problème	Description
	le répertoire de Cloud Identity Engine (moteur d'identité cloud) mais ne supprimez pas les configurations Strata Cloud Manager qui font référence à ces utilisateurs et groupes d'utilisateurs, vous pourriez rencontrer des erreurs inattendues, telles que "500 Internal Server Error" « 500 Erreur système interne ». **Solution alternative** : Lorsque vous supprimez un répertoire de Cloud Identity Engine (moteur d'identité cloud), vous devez également supprimer les configurations de Strata Cloud Manager qui font référence aux utilisateurs et aux groupes d'utilisateurs de ce répertoire.
ADI-30468	Un problème existe dans la page **Access Agent (Agent d'accès)** > **Infrastructure Settings (Paramètres d'infrastructure)** dans Strata Cloud Manager, où les options **Prisma Access Managed (Prima Access géré)** et **OnPrem DHCP Server (Serveur DHCP local)** apparaissent dans la section Client IP Pool Allocation (Attribution de pools d'adresses IP du client). Lorsque vous approvisionnez des utilisateurs sur un locataire Prisma Access à disponibilité générale avec Dynamic Privilege Access activé, assurez-vous de **ne pas** sélectionner **OnPrem DHCP Server (Serveur DHCP local)**, car la configuration ne peut pas être rétablie une fois que vous l'avez enregistrée. L'option **OnPrem DHCP Server (Serveur DHCP local)** n'est **pas pris en** charge par les locataires de Dynamic Privilege Access General Availability et sera supprimée de Strata Cloud Manager dans une prochaine version. Si vous sélectionnez **OnPrem DHCP Server (Serveur DHCP local)**, votre locataire sera rendu inutilisable pour les flux de production Dynamic Privilege Access de base.
ADI-29665	N'utilisez pas de caractères spéciaux dans les noms de projet, sinon Strata Cloud Manager émettra un message d'erreur « Malformed Request » (« Requête malformée ») lorsque vous essaierez d'enregistrer la configuration du projet.
ADI-29434	Dans la page Agent Settings (Paramètres de l'agent) dans Strata Cloud Manager, la valeur recommandée pour **Session timeout (Délai d'expiration de la session)** est de 7 jours.
ADI-29272	Lorsque vous créez un extrait, si vous désactivez l'option **Add prefix to object names (Ajouter un préfixe aux noms d'objets)**, assurez-vous de ne pas utiliser de noms de

ID du problème	Description
	paramètres d'agent en double dans deux extraits différents, car cela peut entraîner un comportement inattendu.
ADI-26493	Dans **Access Agent (Agent d'accès)** > **Infrastructure Settings (Paramètres d'infrastructure)** dans Strata Cloud Manager, l'option **OnPrem DHCP Server (Serveur DHCP local)** dans la section Client IP Pool Allocation (Attribution de pools IP du client) n'est pas sélectionnable. Cela fonctionne comme prévu puisque l'option **OnPrem DHCP Server (Serveur DHCP local)** n'est **pas prise en charge** pour Dynamic Privilege Access. Cette option sera renommée en **OnPrem DHCP Server Preview Only) ((Serveur DHCP local (Aperçu uniquement))** afin que les locataires Prisma Access existants puissent fonctionner correctement.
ADI-24562	Un problème existe lorsque vous êtes autorisé à créer plus d'un projet avec le même domaine et le même groupe d'utilisateurs si ces projets ont été configurés à partir de différents extraits de configuration. Évitez cette configuration, car elle peut provoquer un comportement inattendu dans certains flux de travail Strata Cloud Manager. **Solution alternative** : Ne configurez pas différents projets en utilisant le même domaine et le même groupe d'utilisateurs.

Problèmes connus de Prisma Access 5.2.1

ID du problème	Description
CYR-47139	Les connecteurs ZTNA sont désactivés dans une intégration ZTNA Connector—Explicit Proxy (Connecteur ZTNA—Proxy explicite) si les blocs d'applications de connecteurs ZTNA, blocs de connecteurs ou sous-réseaux IP Connector utilisés pour se connecter à des applications sont configurés avec des adresses RFC6598 en conflit avec les adresses proxy explicites. Solution alternative : N'utilisez pas les sous-réseaux 100.64.0.0/15, 100.72.0.0/15 ou 100.88.0.0/15 pour les blocs d'applications ou de connecteurs lorsque vous configurez le connecteur ZTNA pour une utilisation avec un proxy explicite.

ID du problème	Description
CYR-46759	Les paramètres UDP pour les requêtes DNS ne sont pas honorés dans le proxy explicite.
CYR-46627	Le proxy explicite n’est pas pris en charge si l’option **Accept Default Route over Service Connection (Accepter l’itinéraire par défaut pour la connexion aux services)** est activée.
CYR-46349	Lorsque vous utilisez des réseaux distants avec un proxy explicite et la redirection du trafic en Chine, ne configurez pas les règles de redirection du trafic avec la catégorie d’URL.
CYR-46191	Si le proxy explicite est configuré avec l’accès aux applications privées activé et que le connecteur ZTNA est ajouté à la configuration, une autre validation depuis Panorama ou Strata Cloud Manager peut être requise. **Solution alternative** : Apportez une petite modification à la configuration du proxy explicite sur Panorama ou Strata Cloud Manager qui gère Prisma Access et transmet (Push) vos modifications.

Problèmes résolus de Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

Les rubriques suivantes décrivent les problèmes qui ont été abordés dans Prisma Access 5.2 et Prisma Access 5.2.1.

Problèmes résolus de Prisma Access 5.2.1

ID du problème	Description
CYR-45847	Correction d'un problème où, lorsqu'un sous-réseau de service était modifié, il faisait l'objet d'une mise à jour sur les passerelles GlobalProtect de Prisma Access, mais le tunnel GlobalProtect tombait en panne car NAT n'était pas correctement implémenté.
CYR-45341	Correction d'un problème à cause duquel les travaux de validation et d'envoi vers les groupes d'appareils Colo-Connect expiraient, ce qui empêchait la suppression des VLAN.
CYR-44391	Correction d'un problème à cause duquel les déploiements de proxy explicite en Chine ne prenaient pas en charge l'utilisation de Cloud Identity Engine (moteur d'identité sur le cloud) ou de SAML pour l'authentification.
CYR-43690	Correction d'un problème où, lors de la tentative de modification ou de suppression de blocs IP de connecteur dans le connecteur ZTNA, les modifications n'étaient pas appliquées après une validation et une transmission (Push).
CYR-42919	Correction d'un problème où, lors d'une tentative de modification ou de suppression de blocs IP de connecteur dans le connecteur ZTNA, les modifications ne sont pas appliquées après une validation et une transmission (Push).

Problèmes résolus de Prisma Access 5.2.0-h14

ID du problème	Description
CYR-46782	Correction d’un problème à cause duquel les noms de domaine contenant des caractères non ASCII et se trouvant dans le cache Panorama provoquaient des erreurs lors du traitement des commandes nsupdate dans la fonctionnalité DDNS de GlobalProtect.
CYR-46358	Correction d’un problème où une erreur `Failed plug-in validation (Échec de la validation du plug-in)` s’est produite sur un locataire non Prisma Access Edition lors d’une mise à niveau vers un plug-in de Cloud Services qui a subi des modifications de Colo-Connect.
CYR-45949	Correction d’un problème où, si l’interface utilisateur ne pouvait pas accéder à l’infrastructure Prisma Access, l’onglet Utilisateurs mobiles - Emplacement d’intégration du proxy explicite ne se chargeait pas et continuait la mise en mémoire tampon.
CYR-45932	Correction d’un problème à cause duquel la vérification OTP (Push unique) échouait avec l’erreur suivante : `[get-panorama-cert.py:288] <class 'AttributeError'> ("'Pan_plug-in_Client'objet object has no attribute 'whitelist_keys' (l’objet « Pan_plug-in_Client » n’a pas d’attribut 'whitelist_keys'`
CYR-44969	Correction d’un problème à cause duquel un utilisateur créé à l’aide d’un administrateur basé sur un rôle ne pouvait pas voir la configuration des services cloud dans l’interface utilisateur.
CYR-44766	Correction d’un problème à cause duquel la suppression d’IKE et du profil crypto IPSec à l’aide d’API communes échouait et les profils n’étaient pas supprimés de la configuration.

Problèmes résolus de Prisma Access 5.2.0

ID du problème	Description
CYR-45112	Correction d'un problème à cause duquel la configuration de la passerelle externe était grisée lors de la mise à niveau du plug-in Cloud Services vers les versions 5.1.0 ou ultérieures.
CYR-44598	Correction d'un problème à cause duquel l'état du service de journalisation des strates pour les déploiements de Prisma Access géré par Panorama affichait une erreur `Exception` *<customer-id>*.
CYR-43673	Correction d'un problème où toutes les configurations non valides de l'API étaient relayées à l'administrateur système via un appel GET.
CYR-43400	Correction d'un problème où, pour les connecteurs intégrés dans les groupes de connecteurs ZTNA avec **Preserve User ID (Conserver l'ID utilisateur)** coché **Actions** > **Diagnostic** > **ping** de l'interface interne aux apps du centre de données ne fonctionnaient pas.
CYR-43280	Correction d'un problème à cause duquel une erreur de données base64 illégale empêchait le DSP de générer un diff, même si des modifications étaient présentes.
CYR-43262	Correction d'un problème à cause duquel les requêtes d'API de réseau distant pour l'intégration du réseau distant généraient une erreur de validation de validation dans le plug-in lorsque la configuration BGP était incluse dans la charge utile.
CYR-43222	Correction d'un problème où les cibles d'application attribuées à des groupes de connecteurs ZTNA basés sur l'ID utilisateur ne prenaient pas en charge le **type de sondage icmp ping**.
CYR-42377	Correction d'un problème où, lors de la configuration du support de l'enregistrement DNS dynamique pour le dépannage et les mises à jour à distance, un fichier de clé Kerberos non chiffré ne

ID du problème	Description
	pouvait pas être chargé sur le Panorama qui gère Prisma Access lorsque le **type d'authentification** était **Kerberos**. Si vous exécutez un déploiement géré par Panorama avec une version de plug-in 5.2.0 ou supérieure et que vous choisissez un type d'authentification Kerberos, chargez une clé d'authentification via un fichier .key contenant la chaîne encodée en base64 de la clé Kerberos récupérée à partir du serveur DNS, par exemple : `"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcD` Si vous exécutez un déploiement géré par Panorama avec une version de plug-in inférieure à 5.1.0 et que vous choisissez un type d'authentification Kerberos, chargez une clé d'authentification via un fichier .key contenant le fichier keytab Kerberos non codé récupéré à partir du serveur DNS.
CYR-42191	Correction d'un problème où, lors de la configuration du support DNS dynamique, un fichier Kerberos valide n'était pas correctement chargé et n'était pas enregistré dans la configuration du système.
CYR-41740	Correction d'un problème où, si plus de 100 connecteurs étaient intégrés dans la même région dans un court laps de temps, l'accès à l'app privée via certains connecteurs ZTNA pouvait ne pas fonctionner.
CYR-38418	Correction d'un problème où, après l'activation d'IPv6, une mise à niveau du plan de données Prisma Access de la version 10.2.8-h1 vers la version 10.2.8-h2 échouait.
CYR-38386	Correction d'un problème où, après qu'une opération de mise à l'échelle automatique avait entraîné la création de passerelles d'utilisateurs mobiles supplémentaires, une opération Commit (validation) et Push (transmission) échouait.
CYR-37913	Correction d'un problème où, si vous désactiviez la réplication du trafic dans un calcul et que vous la réactiviez dans le même calcul, la fonctionnalité de réplication du trafic était affectée et vous ne voyiez aucun utilisateur mobile ou trafic réseau

ID du problème	Description
	distant répliqué sans qu'aucun échec de validation ou de configuration ne s'affiche.
CYR-37791	Correction d'un problème où, après qu'un utilisateur est passé d'un projet à un autre et s'est connecté au même emplacement Prisma Access, la page Monitor > Users (Surveiller > utilisateurs) de Strata Cloud Manager ne reflétait pas le nom de projet correct vers lequel l'utilisateur a basculé pour les plages horaires suivantes : 3 heures, 24 heures, 7 jours et 30 jours.
CYR-36930	Correction d'un problème où, si un utilisateur mobile GlobalProtect avait activé la double pile (IPv4 et IPv6) et qu'il se connectait à un emplacement GlobalProtect Prisma Access sur lequel IPv6 était activé et que IPv6 était ensuite désactivé pour cet emplacement, l'utilisateur à double pile ne pouvait pas se connecter à cet emplacement.
CYR-27734	Correction d'un problème à cause duquel l'optimiseur de politique pour les statistiques d'utilisation des règles inutilisées n'était pas visible dans Panorama pour les groupes d'appareils réseau distants.

Prise en charge de Panorama pour Prisma Access 5.2 et 5.2.1

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

Les versions 5.2 et 5.2.1 de Prisma Access (Managed by Panorama) utilisent le plug-in **Cloud Services 5.2** Cloud Services. Prisma Access 5.2.1 est activé à l'aide d'une version de correctif d'urgence du plug-in 5.2. Si vous utilisez Panorama pour gérer Prisma Access et si vous devez effectuer une mise à niveau vers le plug-in 5.2, vous devez :

1. Consulter les versions logicielles requises pour que Panorama prenne en charge Prisma Access 5.2 version préférée et innovation
2. Déterminer le chemin de mise à niveau que vous devrez suivre pour le plug-in Cloud Services
3. Mettre à jour le plug-in Cloud Services

Versions logicielles requises et recommandées pour Panorama Managed Prisma Access 5.2 et 5.2.1

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

Versions logicielles recommandées pour Prisma Access 5.2.1 préféré et innovation

Il existe deux versions de Prisma Access 5.2.1 :

- La version 5.2.1 préférée exécute un plan de données PAN-OS 10.2.10. Si votre déploiement exécute une version inférieure du plan de données, une mise à niveau du plan de données vers PAN-OS 10.2.10 est nécessaire pour implémenter les fonctionnalités de la version 5.2.1 préférée.
- La version 5.2.1 innovation exécute un plan de données PAN-OS 11.2.4. Une mise à niveau vers PAN-OS 11.2.4 est nécessaire pour implémenter les fonctionnalités de la version 5.2 innovation.

Pour les nouvelles fonctionnalités de Prisma Access 5.2.1 innovation, Prisma Access **vous recommande de mettre à jour votre Prisma Access vers les versions suivantes** avant d'installer le plug-in.

Version de Prisma Access	Version du plug-in Cloud Services	Version requise du plan de données pour 5.2.1	Version de GlobalProtect recommandée	Version de Panorama recommandée
5.2.1	Correctif d'urgence 5.2.0	PAN-OS 10.2.10 (requis pour la version 5.2.1 préférée) PAN-OS 11.2.4 (requis pour la version 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

Versions logicielles recommandées pour Prisma Access 5.2 préféré et innovation

Il existe deux versions de Prisma Access 5.2 :

- La version 5.2 préférée exécute un plan de données PAN-OS 10.2.10. Si votre déploiement exécute une version inférieure du plan de données, une mise à niveau du plan de données vers PAN-OS 10.2.10 sera sans doute nécessaire pour implémenter les fonctionnalités de la version 5.2 préférée. Si vous êtes un client existant, consultez Dépendances de l'infrastructure, des plug-ins et des plans de données pour les

fonctionnalités préférées et d'innovation Prisma Access 5.2.1 pour voir si une mise à niveau du plan de données est nécessaire pour une fonctionnalité Prisma Access 5.2.

- La version 5.2 innovation exécute un plan de données PAN-OS 11.2.3. Une mise à niveau vers PAN-OS 11.2.3 est nécessaire pour implémenter les fonctionnalités de la version 5.2 innovation.

Pour les nouvelles fonctionnalités de Prisma Access 5.2 Innovation, Prisma Access **vous recommande de mettre à jour votre Prisma Access vers les versions suivantes** avant d'installer le plug-in.

Version de Prisma Access	Version du plug-in Cloud Services	Version du plan de données requise pour 5.2	Version de GlobalProtect recommandée	Version de Panorama recommandée
5.2	5.2	PAN-OS 10.2.10 (requis pour la version 5.2 préférée) PAN-OS 11.2.3 (requis pour la version 5.2 innovation)	6.0.7+ 6.1.3+ 6.2.1+	10.2.10+ 11.0.1+ 11.1.0 11.2.3

Considérations relatives à la mise à niveau de Panorama Managed Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

Pour mettre à niveau votre plug-in Cloud Services vers Prisma Access 5.2 ou 5.2.1, utilisez l'un des chemins de mise à niveau suivants. Pour trouver la version actuelle de votre plug-in dans Panorama, sélectionnez **Panorama** > **Cloud Services** > **Configuration** > **Service Setup (Configuration du service)** et vérifiez la version du plug-in dans la zone **Plugin Alert (Alerte du plug-in)**.

Assurez-vous de suivre les versions minimales de Panorama pour chaque version de plug-in lors de la mise à niveau.

Version du plug-in Cloud Services installé	Version ciblée	Chemin de mise à niveau du plug-in
5.1	5.2 ou 5.2.1	Mettez à niveau votre plug-in de Prisma Access 5.1 vers Prisma Access 5.2, puis validez et transmettez vos modifications.
5.0	5.2 ou 5.2.1	**1.** Mettez à niveau votre plug-in de Prisma Access 5.0 vers Prisma Access 5.1, puis validez et transmettez vos modifications. **2.** Mettez à niveau votre plug-in de Prisma Access 5.1 vers Prisma Access 5.2, puis validez et transmettez vos modifications.
4.1 et 4.2	5.2 ou 5.2.1	**1.** Mettez à niveau votre plug-in de Prisma Access 4.1 vers Prisma Access 5.0, puis validez et transmettez vos modifications. **2.** Mettez à niveau votre plug-in de Prisma Access 5.0 vers Prisma Access 5.1, puis validez et transmettez vos modifications. **3.** Mettez à niveau votre plug-in de Prisma Access 5.1 vers Prisma Access 5.2, puis validez et transmettez vos modifications.
4.0	5.2 ou 5.2.1	**1.** Mettez à niveau votre plug-in vers Prisma Access 4.1, puis validez et transmettez vos modifications.

Version du plug-in Cloud Services installé	Version ciblée	Chemin de mise à niveau du plug-in
		2. Mettez à niveau votre plug-in vers Prisma Access 5.0, puis validez et transmettez vos modifications. 3. Mettez à niveau votre plug-in de Prisma Access 5.0 vers Prisma Access 5.1, puis validez et transmettez vos modifications. 4. Mettez à niveau votre plug-in de Prisma Access 5.1 vers Prisma Access 5.2, puis validez et transmettez vos modifications.
Versions 3.0, 3.1 et 3.2 préférées	5.2 ou 5.2.1	1. (Plug-ins 3.0 uniquement) Mettez à niveau votre plug-in vers Prisma Access 3.1 et validez, puis transmettez vos modifications. 2. (Plug-ins 3.1 uniquement) Mettez à niveau votre plug-in vers Prisma Access 3.2 ou 3.2.1, puis validez et transmettez vos modifications. 3. Mettez à niveau votre plug-in vers Prisma Access 3.2 ou 3.2.1, puis validez et transmettez vos modifications. 4. Mettez à niveau votre plug-in vers Prisma Access 4.0, puis validez et transmettez vos modifications. 5. Mettez à niveau votre plug-in vers Prisma Access 4.1, puis validez et transmettez vos modifications. 6. Mettez à niveau votre plug-in vers Prisma Access 5.0, puis validez et transmettez vos modifications. 7. Mettez à niveau votre plug-in de Prisma Access 5.0 vers Prisma Access 5.1, puis validez et transmettez vos modifications. 8. Mettez à niveau votre plug-in de Prisma Access 5.1 vers Prisma Access 5.2, puis validez et transmettez vos modifications.
2.2 Préféré	5.2 ou 5.2.1	1. Mettez à niveau votre plug-in vers Prisma Access 3.0, puis validez et transmettez vos modifications. 2. Mettez à niveau votre plug-in vers Prisma Access 3.1, puis validez et envoyez vos modifications. 3. Mettez à niveau votre plug-in vers Prisma Access 3.2 ou 3.2.1, puis validez et transmettez vos modifications. 4. Mettez à niveau votre plug-in vers Prisma Access 4.0, puis validez et transmettez vos modifications. 5. Mettez à niveau votre plug-in vers Prisma Access 4.1, puis validez et transmettez vos modifications. 6. Mettez à niveau votre plug-in vers Prisma Access 5.0, puis validez et transmettez vos modifications.

Version du plug-in Cloud Services installé	Version ciblée	Chemin de mise à niveau du plug-in
		7. Mettez à niveau votre plug-in de Prisma Access 5.0 vers Prisma Access 5.1, puis validez et transmettez vos modifications. **8.** Mettez à niveau votre plug-in de Prisma Access 5.1 vers Prisma Access 5.2, puis validez et transmettez vos modifications.
Versions antérieures à la version 2.2 préférée	5.2 ou 5.2.1	**1.** Mettez à niveau votre plug-in vers Prisma Access 2.2, puis validez et transmettez vos modifications. Si votre déploiement s'effectue sur une version de Prisma Access antérieure à la version 2.2 préférée, vous devez d'abord effectuer une mise à niveau vers la version 2.2 avant de pouvoir effectuer une mise à niveau vers la version 3.2. Les mises à niveau des versions 2.0 ou 2.1 de Prisma Access ne sont pas prises en charge. **2.** Mettez à niveau votre plug-in vers Prisma Access 3.0, puis validez et transmettez vos modifications. **3.** Mettez à niveau votre plug-in vers Prisma Access 3.1, puis validez et envoyez vos modifications. **4.** Mettez à niveau votre plug-in vers Prisma Access 3.2 ou 3.2.1, puis validez et transmettez vos modifications. **5.** Mettez à niveau votre plug-in vers Prisma Access 4.0, puis validez et transmettez vos modifications. **6.** Mettez à niveau votre plug-in vers Prisma Access 4.1, puis validez et transmettez vos modifications. **7.** Mettez à niveau votre plug-in vers Prisma Access 5.0, puis validez et transmettez vos modifications. **8.** Mettez à niveau votre plug-in de Prisma Access 5.0 vers Prisma Access 5.1, puis validez et transmettez vos modifications. **9.** Mettez à niveau votre plug-in de Prisma Access 5.1 vers Prisma Access 5.2, puis validez et transmettez vos modifications.

Mettre à jour le plug-in Cloud Services

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 ou 5.2.1 préférée ou innovation

Utilisez la procédure suivante pour mettre à niveau le plug-in Cloud Services.

Prisma Access utilise le plug-in Cloud Services de Panorama pour activer ses fonctionnalités.

Pour obtenir la liste des versions du logiciel Panorama prises en charge par Prisma Access, reportez-vous à la section Versions minimales requises du logiciel Panorama dans la matrice de compatibilité de Palo Alto Networks.

Avant de mettre à niveau le plug-in, supprimez tous les modèles non Prisma Access des piles de modèles Prisma Access afin d'éviter les erreurs de validation après la mise à niveau et assurez-vous que le Panorama qui gère Prisma Access exécute une version PAN-OS prise en charge.

Utilisez l'une des tâches suivantes pour télécharger et installer le plug-in Cloud Services.

***Déploiements HA uniquement** : si vous disposez de deux appareils Panorama configurés en mode High Availability (haute disponibilité - HA), installez d'abord le plug-in sur la paire HA principale, puis sur la secondaire.*

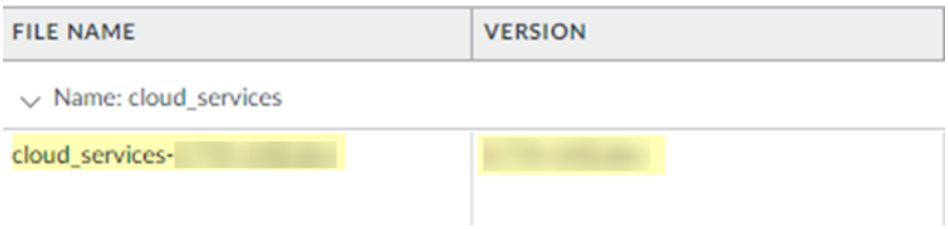
STEP 1 | Déterminez le chemin de mise à niveau du plug-in vers lequel vous souhaitez effectuer la mise à niveau.

Pour certains chemins de mise à niveau, vous devez mettre à niveau votre plug-in de manière séquentielle. Par exemple, pour effectuer une mise à niveau d'un plug-in à la version 3.0 préférée vers un plug-in à la version 5.2, vous devez d'abord effectuer des mises à niveau intermédiaires vers les versions 3.1, 4.0, 4.1, 5.0 et 5.1 avant de passer à la version 5.2.

STEP 2 | Téléchargez et installez les versions du plug-in Cloud Services dont vous avez besoin.

- Pour télécharger et installer le plug-in Cloud Services en le téléchargeant à partir du portail de support client, procédez comme suit.
  1. Connectez-vous au portail de support client et sélectionnez **Mises à jour logicielles**,
  2. Recherchez le plug-in Cloud Services dans la section Panorama Integration Plug-In (Plug-in d'intégration Panorama) et téléchargez-le.

     Ne renommez pas le fichier du plug-in ou vous ne pourrez pas l'installer sur Panorama.
  3. Connectez-vous à l'interface web Panorama du Panorama que vous êtes autorisé à utiliser avec Prisma Access, sélectionnez **Panorama** > **Plugins (Plug-ins)** > **Upload (Charger)** et **Browse (Parcourir)** pour le **fichier** du plug-in, fichier que vous avez téléchargé à partir du CSP.
  4. **Installez** le plugin.
- Pour télécharger et installer la nouvelle version du plug-in Cloud Services directement depuis Panorama, procédez comme suit :
  1. Choisir **Panorama** > **Plugins (Plug-ins)** et cliquez sur **Check Now (Vérifier maintenant)** pour afficher les dernières mises à jour du plug-in Cloud Services.

  2. **Téléchargez** la version du plug-in que vous souhaitez installer.
  3. Après avoir téléchargé le plug-in, **Installez-le**.

STEP 3 | (Mises à niveau des versions antérieures à la version 3.2 vers les versions 3.2 ou ultérieures) Sélectionnez **Commit (Valider)** > **Commit to Panorama (Valider vers Panorama)** pour enregistrer vos modifications localement sur le Panorama qui gère Prisma Access.

Vous n'avez besoin d'effectuer une validation locale dans Panorama que si vous effectuez une mise à niveau d'un plug-in Cloud Services antérieur à la version 3.2 vers un plug-in 3.2 ou ultérieur. Les mises à niveau à partir d'une version ultérieure à la version 3.2 ne nécessitent pas de validation locale.

Obtenir de l’aide

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Licence Prisma Access ❑ Minimum Required Prisma Access Version 5.2 préférée et innovation

Les rubriques suivantes fournissent des informations sur les endroits où trouver plus d’informations sur cette version et la manière de demander du soutien :

- Documentation connexe :
- Requête de soutien

Documentation connexe :

Utilisez les documents suivants pour configurer et mettre en œuvre votre déploiement Prisma Access :

- Utilisez le Guide administrateur Prisma Access pour planifier, installer et configurer Prisma Access afin de sécuriser votre réseau.
- Utilisez les tâches spécifiques au fournisseur dans le Guide d’intégration de Prisma Access pour configurer l’authentification des utilisateurs mobiles et sécuriser vos déploiements SD-WAN tiers et cloud public.
- Utilisez le Guide de démarrage du service de journalisation Strata pour apprendre à déployer Strata Logging Service (anciennement Cortex Data Lake) et commencer à transférer les journaux de vos pare-feux locaux vers Cortex Data Lake.

Visitez le site https://docs.paloaltonetworks.com pour plus d’informations sur nos produits.

Requête de soutien

Pour contacter le support technique, obtenir des informations sur les programmes de support technique, gérer votre compte ou vos appareils ou ouvrir un dossier de support technique, accédez à https://support.paloaltonetworks.com.

Pour nous faire part de vos commentaires sur la documentation, veuillez nous écrire à l’adresse : documentation@paloaltonetworks.com.

Coordonnées

Siège de l’entreprise :

Palo Alto Networks

3000 Tannery Way

Santa Clara, Californie 95054

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

