paloalto TECHDOCS

Activer et intégrer Prisma Access Browser

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 15, 2024

Table of Contents

Activer une nouvelle licence groupée entreprise Prisma Access Browser avec Prisma Access 5

Activer la licence autonome de Prisma Access Browser 9

Intégrer le Prisma Access Browser sur l'application Strata Cloud Manager 13

Terminer les tâches de pré-intégration 14

Ajouter une configuration IdP 14

Intégrer le Prisma Access Browser 16

Étape 1 - Utilisateurs 16

Étape 2 - Intégration Prisma Access 16

Étape 3 - Routage 17

Étape 4 - Appliquer les applications SSO 17

Étape 5 - Télécharger et distribuer 18

Étape 6 - Politique du navigateur 18

Intégration de nouveaux utilisateurs 19

Attribuer des rôles Prisma Access Browser 21

Activer une nouvelle licence groupée entreprise Prisma Access Browser avec Prisma Access

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Strata Cloud Manager • Panorama	• Lien d’activation pour votre produit • Strata Logging Service (SLS) est nécessaire pour l’activation • Cloud Identity Engine (CIE) est inclus et lancé lors de l’activation • Compte du portail de support client

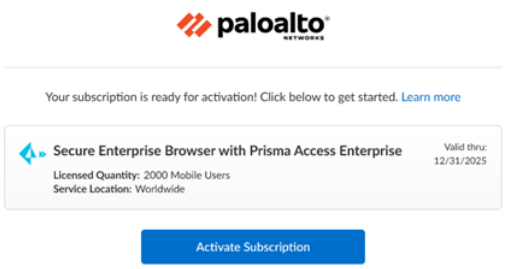
Voir les prérequis avant de commencer cette tâche.

- Cloud
- Panorama

Licence groupée du Prisma Access Browser géré dans le cloud

Après avoir reçu un e-mail de Palo Alto Networks identifiant la licence que vous activez, utilisez le lien d'activation pour commencer le processus d'activation.

STEP 1 | Sélectionnez **Activate Subscription (Activer l'abonnement)** dans votre e-mail.



STEP 2 | Suivez les instructions suivantes pour activer une licence Prisma Access, les instructions suivantes pour attribuer une licence Prisma Accessет les instructions suivantes pour planifier les connexions de service.

STEP 3 | Continuer à attribuer les licences et modules complémentaires de Prisma Access Secure Enterprise Browser. Les **Products (Produits)** ou **Add-ons (modules complémentaires)** sont activés par défaut en fonction de votre contrat.

STEP 4 | Sélectionnez le **Secure Enterprise Browser with (Navigateur d'entreprise sécurisé avec) Prisma Access Entreprise**.

Ce processus est similaire au processus d'attribution des licences utilisateur mobile PA. Vous pourrez attribuer et activer partiellement des licences Prisma Access Browser sur plusieurs locataires Prisma Access. Par exemple :

- Vous pouvez acheter 5 000 unités d'utilisateurs mobile entreprise de Prisma Access Browser.
- Vous pouvez en attribuer :
  - 1 000 à un locataire PoC (il s'agit de la quantité minimale requise)
  - 3 000 à un locataire de production
  - Laissez 1 000 unités non activées pour une utilisation ultérieure

STEP 5 | Allez sur le Guide administrateur Prisma Access Browser pour gérer votre Prisma Access Browser.

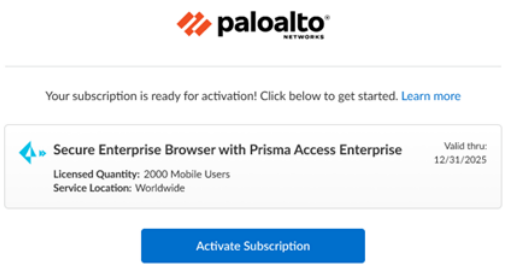
STEP 6 | (Facultatif) Attribuez des rôles afin que vos administrateurs puissent gérer le Prisma Access Browser.

Licence groupée de Prisma Access Browser géré par Panorama

Après avoir reçu un e-mail de Palo Alto Networks identifiant la licence que vous activez, utilisez le lien d'activation pour commencer le processus d'activation.

Non disponible pour le multilocataire Panorama.

STEP 1 | Sélectionnez **Activate Subscription (Activer l'abonnement)** dans votre e-mail.



STEP 2 | Suivez les instructions suivantes pour activer une licence Prisma Access (gérée par Panorama).

STEP 3 | Continuer à activer les modules complémentaires disponibles. Les **Products (Produits)** ou **Add-ons (modules complémentaires)** sont activés par défaut en fonction de votre contrat.

STEP 4 | Sélectionnez l'icône **Secure Enterprise Browser with Prisma Access Enter (Navigateur d'entreprise sécurisé avec Prisma Access Entreprise)**.

STEP 5 | Dans Panorama, allez dans l'onglet**Panorama** > **Cloud Services Plugin (Plug-in Cloud Services)** > **onglet Prisma Access Browser**.

Cela lance un nouvel onglet avec une version allégée de Strata Cloud Manager qui ne contient que les vues spécifiques de Prisma Access Browser.

STEP 6 | Allez sur le Guide administrateur Prisma Access Browser pour gérer votre Prisma Access Browser.

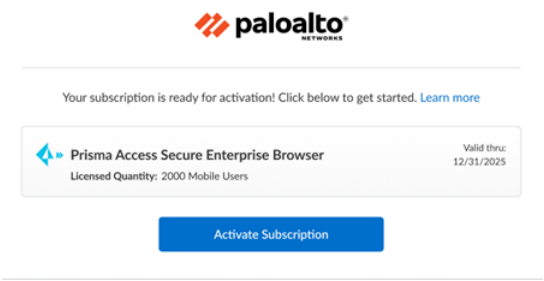
STEP 7 | (Facultatif) Attribuez des rôles afin que vos administrateurs puissent gérer le Prisma Access Browser.

Activer la licence autonome de Prisma Access Browser

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Strata Cloud Manager	• Lien d'activation pour votre produit • Cloud Identity Engine (CIE) est inclus et lancé lors de l'activation • Compte du portail de support client

Voir les prérequis avant de commencer cette tâche.

Après avoir reçu un e-mail de Palo Alto Networks identifiant la licence que vous activez, utilisez le lien d'activation pour commencer le processus d'activation.



STEP 1 | Connectez-vous avec votre adresse e-mail.

- Si vous possédez un compte d'assistance clientèle Palo Alto Networks, inscrivez l'adresse e-mail que vous avez utilisée lors de votre inscription à ce compte et sélectionnez **Next (Suivant)**.
- Si vous ne possédez pas de compte de support client Palo Alto Networks, sélectionnez alors **Create a New Account (Créer un nouveau compte)** > **Password (Mot de passe)** > **Next (Suivant)**.

Le service utilise cette adresse e-mail pour le compte utilisateur attribué au locataire que vous utilisez pour cette licence. Ce locataire, ainsi que tout autre créé par cette adresse e-mail, aura le rôle de `Super utilisateur`.

STEP 2 | Si vous n'avez qu'un seul compte du portail de support client associé à votre nom d'utilisateur, le **Customer Support Account (Compte de support client)** est prérempli.

Si vous avez plusieurs compte de portail de support client, vous pouvez vous attendre à d'autres comportements.

STEP 3 | Attribuez le produit au **Recipient (Destinataire)** de votre choix.

Pour plus de commodité, le nom fourni correspond à votre compte du portail de support client. Vous pouvez utiliser le nom fourni ou le modifier.

STEP 4 | Choisissez la **Region (Région)** d'ingestion des données où vous souhaitez déployer votre produit.

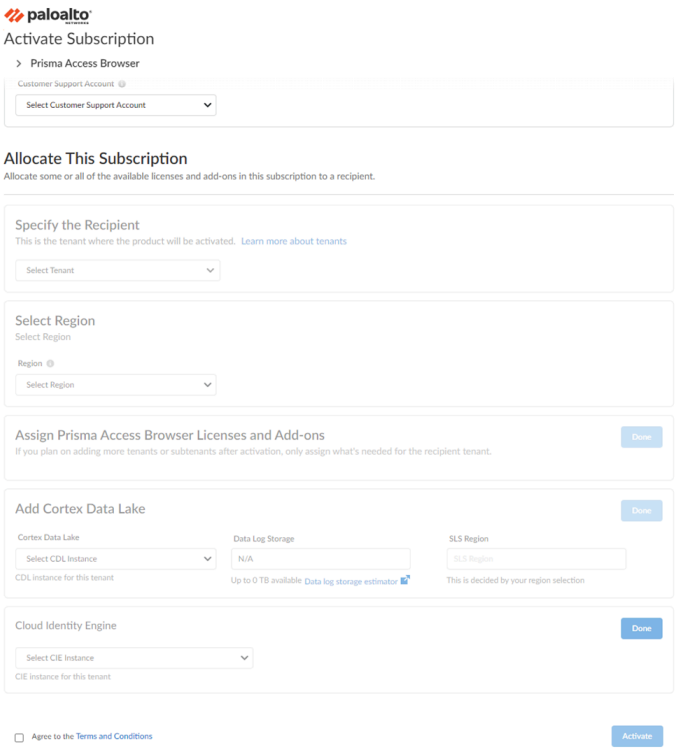
STEP 5 | Attribuer les licences Prisma Access Secure Enterprise Browser et les modules complémentaires

1. Sélectionnez **Prisma Access Secure Enterprise Browser**.
2. Ce processus est similaire au processus d'attribution des licences utilisateur mobile PA https://docs.paloaltonetworks.com/content/techdocs/en_US/common-services/subscription-and-tenant-management/cloud-managed-prisma-access-and-add-ons-license-activation/activate-a-license-for-cloud-managed-prisma-access-and-add-ons/allocate-licenses-cloud-managed-prisma-access. Vous pourrez attribuer et activer partiellement des licences Prisma Access Browser sur plusieurs locataires Prisma Access. Par exemple :
   - Vous pouvez acheter 1 000 unités de licences autonomes Prisma Access Browser
   - Vous pouvez en attribuer :
     - 200 à un locataire PoC (il s'agit de la quantité minimale requise)
     - 600 à un locataire de production
     - Laissez 200 unités inactivées pour une utilisation ultérieure

STEP 6 | Ajouter des Strata Logging Service (anciennement appelés Cortex Data Lake) pour stocker les données des locataires telles que la configuration, les journaux de télémétrie, les journaux système et les statistiques. Vous pouvez sélectionner une instance existante ou en créer une nouvelle.

STEP 7 | Sélectionnez Cloud Identity Engine ou créez une nouvelle instance CIE pour identifier et vérifier tous les utilisateurs de votre infrastructure.

STEP 8 | **Agree to the terms and conditions (Accepter les termes et conditions)**, et **Activate (Activer)**.



STEP 9 | Allez sur le Guide administrateur Prisma Access Browser pour gérer votre Prisma Access Browser.

STEP 10 | (Facultatif) Attribuez des rôles afin que vos administrateurs puissent gérer le Prisma Access Browser.

Intégrer le Prisma Access Browser sur l’application Strata Cloud Manager

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Strata Cloud Manager	❑ Prisma Access avec licence groupée Prisma Access Browser ❑ Super utilisateur ou Prisma Access Browser rôle

Voir les prérequis avant de commencer cette tâche.

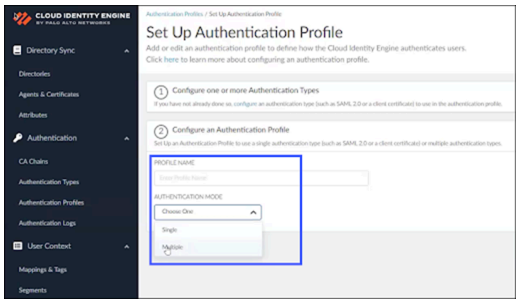
Terminer les tâches de pré-intégration

Avant l’intégration Prisma Access Browser, il y a quelques tâches que vous devez effectuer avant de pouvoir continuer.

STEP 1 | Définir les entités Cloud Identity Engine. Les entités peuvent être configurées à l’aide du Cloud Identity Engine que vous avez sélectionné lors du processus d’activation.

STEP 2 | Vous avez besoin du profil d’authentification et des groupes d’utilisateurs qui font partie de votre processus d’intégration. Ceux-ci sont configurés dans Cloud Identity Engine. Pour plus d’informations, reportez-vous au profil d’authentification et aux groupes d’utilisateurs.

*Vous ne pouvez avoir qu’un seul profil d’authentification. Si vous utilisez plusieurs fournisseurs d’identité (IdP), vous pouvez configurer plusieurs IdP par profil. Cela peut être fait avec le choix du **Authentication Mode (Mode d’authentification) Multiple** lorsque vous configurez le profil d’authentification.*

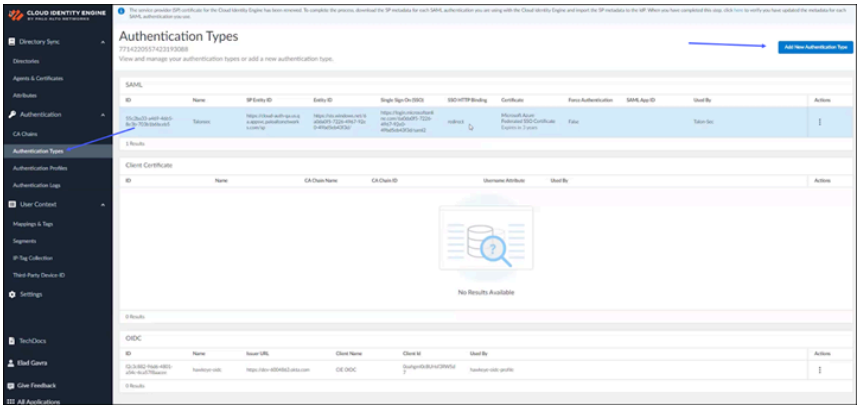


Ajouter une configuration IdP

Vous pouvez utiliser votre IdP SAML actuel pour gérer un seul ensemble d’identifiants de connexion au sein de votre réseau. La configuration IdP est un composant du Cloud Identity Engine, que vous pouvez gérer dans cet outil.

STEP 1 | Dans Cloud Identity Engine, sélectionnez **Authentication Type (Type d’authentification)**.

STEP 2 | Cliquez sur **Add New Authentication Type (Ajouter un nouveau type d’authentification)**.



Lorsque vous utilisez les informations de l’IdP pour remplir vos groupes d’utilisateurs, vous devez vous assurer d’inscrire correctement une adresse e-mail valide. L’UPN n’est pas suffisant.

STEP 3 | Dans Configurer le type d’authentification, cliquez sur **Configurer** SAML 2.0.

STEP 4 | Pour poursuivre la configuration de votre authentificateur SAML, reportez-vous à la section Configurer un type d’authentification SAML 2.0 dans Cloud Identity Engine.

STEP 5 | (Facultatif) Utilisez l’intégration Google Workspace .

Intégrer le Prisma Access Browser

Après avoir effectué les étapes de pré-intégration, vous pouvez intégrer le Prisma Access Browser sur l’appli Strata Cloud Manager.

Vous devez activer et configurer le Prisma Access Browser dans l’appli Strata Cloud Manager avant de pouvoir ajouter des utilisateurs. En général, il s’agit d’une procédure unique que vous n’avez besoin d’effectuer qu’une seule fois après l’activation, mais vous pouvez revenir pour effectuer ces tâches chaque fois que vous devez les modifier.

Il existe un assistant que vous pouvez utiliser pour ce processus et vous pouvez modifier la configuration globale à tout moment. L’Assistant fournit des instructions détaillées sur la réalisation de chaque étape de l’intégration.

Les commandes que vous voyez dépendent de votre licence Prisma Access Browser ; toutes les fonctionnalités d’intégration ne sont pas disponibles dans l’application Strata Cloud Manager pour toutes les licences.

Depuis l’application Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration)** > **Prisma Access Browser (Navigateur Prisma Access).**

Étape 1 - Utilisateurs

Définissez la méthode d’authentification de l’utilisateur et intégrez les groupes d’utilisateurs.

STEP 1 | Dans la liste déroulante, sélectionnez le **CIE profile that will be used for User Authentication (Profil CIE qui sera utilisé pour l’authentification de l’utilisateur)**.

STEP 2 | Dans la liste déroulante Groupes d’utilisateurs, sélectionnez les **User groups (Groupes d’utilisateurs)** qui pourront accéder au Prisma Access Browser.

STEP 3 | **Next (Suivant) : Prisma Access Integration (Intégration)**.

Étape 2 - Intégration Prisma Access

STEP 1 | Activez la connectivité externe pour Prisma Access.

1. Sélectionner **Go to Explicit Proxy settings (Aller dans les paramètres de proxy explicite)**.
2. Cela vous amène sur **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration)** > **Explicit Proxy (Proxy explicite)** .
3. Activez le Prisma Access Browser.
4. **Done (Terminé)**.

STEP 2 | Autorisez le Prisma Access Browser dans la politique de sécurité Prisma Access.

1. Sélectionnez **Manage (Gérer) > Prisma Access > Security Policy (Politique de sécurité)**.
2. Cela vous amène sur **Manage (Gérer)** > **Prisma Access** > **Security policy (Politique de sécurité).**
3. Ajoutez une règle qui autorise le trafic Web dans votre politique de sécurité.
4. Appliquez la configuration pour accepter la règle.
5. **Done (Terminé)**.

STEP 3 | Créez une connexion de service.

1. Sélectionnez **Create a service connection (Créer une connexion de service)**.
2. Cela vous amène sur **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration)** > **Service Connections (Connexions de service)** et **Add Service Connection (Ajouter une connexion de service)**.
3. **Done (Terminé)**.
4. **Ensuite : Routage.**

Étape 3 - Routage

La commande de routage vous permet de gérer la façon dont le Prisma Access Browser gère le trafic réseau. Cette fonctionnalité configure la configuration par défaut pour le Prisma Access Browser. Si vous devez ajuster la granularité de la commande pour une règle spécifique, reportez-vous à la section Commandes de personnalisation du navigateur pour les flux de trafic.

STEP 1 | Sélectionnez l’une des options suivantes :

- **Only route private application traffic through Prisma Access (Acheminer uniquement le trafic des applications privées via Prisma Access)**.
- **Route all traffic through (Acheminer l’intégralité du trafic via) Prisma Access**.

STEP 2 | (Facultatif) Veillez à ce que les flux de trafic du Prisma Access Browser circulent de manière optimale lorsque le navigateur détecte qu’il fonctionne au sein du réseau interne. Cette identification est basée sur l’établissement d’une connexion avec un hôte qui n’est disponible qu’au sein du réseau interne.

- Inscrivez le FQDN à résoudre.
- Inscrivez l’adresse IP attendue.

STEP 3 | **Next (Suivant) : Enforce SSO applications (Appliquer les applications SSO)**.

Étape 4 - Appliquer les applications SSO

Il est important que le seul moyen pour vos utilisateurs de s’authentifier sur les applications compatibles SSO soit d’utiliser le Prisma Access Browser. Cela garantira que les acteurs externes n’auront pas accès à vos applications d’entreprise. Pour sélectionner votre IdP :

STEP 1 | Dans la section Sélectionner et configurer vos fournisseurs d’identité, sélectionnez l’IdP disponible. Les options à votre disposition sont les suivantes :

- Okta
- Microsoft Azure Active Directory
- PingID
- OneLogin
- VMware workspace ONE Access

STEP 2 | Lorsque vous configurez vos paramètres locaux, veillez à prendre note des adresses IP de sortie.

STEP 3 | **Ensuite : Télécharger et distribuer.**

Étape 5 - Télécharger et distribuer

Vous pouvez télécharger les fichiers d’installation à tester du Prisma Access Browser sur votre propre périphérique avant de les envoyer à vos utilisateurs. Une fois que vous êtes satisfait de vos tests, vous pouvez télécharger le programme d’installation approprié qui sera distribué par votre application de gestion des appareils mobiles (MDM).

Vous pouvez également envoyer à vos utilisateurs le lien de téléchargement afin qu’ils puissent télécharger le Prisma Access Browser de leur côté. Il s’agit d’un lien unique pour les utilisateurs de macOS et Windows uniquement.

STEP 1 | Sélectionnez parmi les options disponibles :

- Bureau :
  - macOS
  - Windows
- Mobile :
  - iOS
  - Android

Vous pouvez également envoyer à vos utilisateurs le lien de téléchargement afin qu’ils puissent télécharger le Prisma Access Browser de leur côté. Il s’agit d’un lien unique pour les utilisateurs de macOS et Windows uniquement.

Si vous envoyez à vos utilisateurs le lien de téléchargement, rappelez-leur qu’ils ne peuvent se connecter qu’avec l’adresse e-mail configurée dans le service IdP.

STEP 2 | **Next (Suivant) : Browser Policy (Politique du navigateur)**.

Étape 6 - Politique du navigateur

Vous pouvez maintenant commencer à explorer et à configurer le moteur de la politique du Prisma Access Browser pour créer un environnement utilisateur sûr et sécurisé.

STEP 1 | Sélectionnez **Browser Policy (Politique du navigateur)**.

STEP 2 | Cela vous dirige vers **Manage (Gérer)** > **Configuration** > **Browser (Navigateur)Prisma Access** > **Policy (Politique)** > **Rules (Règles)**.

STEP 3 | Gérer les règles de la politique Prisma Access Browser.

Intégration de nouveaux utilisateurs

Le flux de travail d’intégration est une série configurable de fenêtres qui s’affichent lorsqu’un nouvel utilisateur final commence à utiliser le navigateur.

En fonction des besoins et des exigences informatiques, vous pouvez sélectionner jusqu’à huit pages individuelles qui permettent aux utilisateurs finaux de personnaliser le navigateur avec leurs photos et leurs signets, et de trouver des informations de base sur le navigateur – une sorte de guide de « démarrage rapide ».

Le contrôle de personnalisation de l’Assistant d’intégration configure le flux de travail d’intégration. Vous pouvez sélectionner les fenêtres qui seront affichées dans votre réseau.

Vous pouvez les configurer dans **Manage (Gérer)** > **Configuration** > **Prisma Access Browser (Navigateur)** > **Policy (Politique)** > **Profiles (Profils)** lorsque vous créez ou modifiez un profil de **Browser Customization (Personnalisation du navigateur)** et sélectionnez **Onboarding Wizard (Assistant d’intégration)**. Pour plus de détails sur la configuration, consultez les commandes de personnalisation du navigateur pour l’Assistant d’intégration.

Attribuer des rôles Prisma Access Browser

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Strata Cloud Manager	❑ Prisma Access avec licence groupée Prisma Access Browser ou licence autonome Prisma Access Browser ❑ Role (Rôle) : Super utilisateur multi-locataire ou Super utilisateur avec accès au portail de support client

Vous pouvez créer et gérer le contrôle d'accès basé sur les rôles pour différents types d'administrateurs de Prisma Access Browser. Cela permet à l'administrateur principal d'une grande organisation de nommer des administrateurs supplémentaires disposant des autorisations appropriées pour leurs rôles spécifiques, y compris la visibilité et l'accès.

Après avoir activé votre licence, vous pouvez gérer l'accès des utilisateurs administrateurs et attribuer l'un des rôles suivants qui leur sont spécifiques. Prisma Access Browser :

Rôles d'entreprise	Autorisations	Applications prises en charge
Administrateur d'accès au navigateur PA et de données	Accès en lecture et écriture pour définir et gérer les politiques d'accès et de données, définir des applications personnalisées ou privées, traiter les requêtes des utilisateurs finaux liées aux politiques et autorisation en lecture seule d'inventorier les aspects (utilisateurs, périphériques, extensions) et de tout aspect de visibilité (tableaux de bord, événements de l'utilisateur final) dans les sections de gestion du navigateur Prisma Access	• Navigateur Prisma Access
Administrateur de personnalisation du navigateur PA	Accès en lecture et écriture pour définir et gérer les politiques de personnalisation du navigateur, et autorisation en lecture seule d'inventorier les aspects (utilisateurs, périphériques, applications, extensions) et de tout aspect de visibilité (tableaux de bord, événements de l'utilisateur final) dans les sections de gestion du navigateur Prisma Access.	• Navigateur Prisma Access
Administrateur de demande	Accès en lecture et écriture pour traiter les requêtes des utilisateurs finaux liées aux politiques et autorisation en lecture seule aux aspects de visibilité (tableaux de bord, événements de l'utilisateur final)	• Navigateur Prisma Access

Rôles d’entreprise	Autorisations	Applications prises en charge
d’autorisation du navigateur PA	dans les sections de gestion du navigateur Prisma Access.	
Administrateur de la sécurité du navigateur PA	Accès en lecture et écriture pour définir et gérer les politiques de sécurité du navigateur, et autorisation en lecture seule d’inventorier les aspects (utilisateurs, périphériques, applications, extensions) et de tout aspect de visibilité (tableaux de bord, événements de l’utilisateur final) dans les sections de gestion du navigateur Prisma Access.	• Navigateur Prisma Access
Administrateur de la sécurité du navigateur PA et de la posture des périphériques	Accès en lecture et en écriture pour définir et gérer les politiques de sécurité du navigateur, gérer les groupes de posture des périphériques et définir les règles de connexion. Il fournit également une autorisation en lecture seule pour l’inventaire des aspects (utilisateurs, applications, extensions) et pour tous les aspects de visibilité (tableaux de bord, événements de l’utilisateur final) dans les sections de gestion du navigateur Prisma Access.	• Navigateur Prisma Access
Voir uniquement les analyses du navigateur PA	Accès en lecture à tous les aspects de la visibilité dans les sections de gestion du navigateur Prisma Access, y compris les tableaux de bord, les événements détaillés de l’utilisateur final et les aspects d’inventaire (utilisateurs, périphériques, applications et extensions).	• Navigateur Prisma Access