paloalto TECHDOCS

Guide de l'administrateur GlobalProtect

Version 10.1

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2024-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

February 25, 2025

Table des matières

Chapitre 1 : Configurer le pare-feu 9

Créer des interfaces et des zones pour GlobalProtect 10
Activer SSL entre les composants GlobalProtect 13
À propos du Déploiement de Certificats GlobalProtect 13
Procédures recommandées pour les certificats GlobalProtect 14
Déployer les certificats de serveur sur les composants GlobalProtect 18
Remplacer un certificat de portail ou de passerelle GlobalProtect expiré 25

Chapitre 2 : Authentification de l'utilisateur GlobalProtect 29

Comment l'application sait-elle quelles sont les informations d'identification elle doit fournir ? 31
Comment l'application sait-elle quel certificat elle doit fournir ? 33
Configurer l'authentification externe 35
Configurer l'authentification LDAP 35
Configurer l'authentification SAML 38
Configurer l'authentification Kerberos 56
Configurer l'authentification RADIUS ou TACACS+ 64
Configurer l'authentification du certificat client 68
Déployer des certificats clients partagés pour l'authentification 69
Déployer des certificats d'ordinateur pour l'authentification 70
Déployer des certificats clients spécifiques à l'utilisateur pour l'authentification 83
Activer la sélection des certificats en fonction de l'OID 87
Prise en charge du magasin de certificats natif pour Prisma Access et l'application GlobalProtect sur les terminaux Linux 89
Configurer l'authentification à deux facteurs 92
Activer l'authentification à deux facteurs à l'aide de profils de certificat et d'authentification 92
Activer l'authentification à deux facteurs basée sur les mots de passe à usage unique (MPUU) 95
Activer l'authentification à deux facteurs pour GlobalProtect basée sur les cartes à puce intelligentes 103
Activer l'authentification à deux facteurs basée sur une application de jetons logiciels 112
Configurer l'authentification pour les points de terminaison strongSwan Ubuntu et CentOS 118
Activer l'authentification par certificat pour les terminaux strongSwan 118
Activer la prise en charge X-Auth des terminaux strongSwan 121
Activer l'authentification à deux facteurs par certificat pour les terminaux strongSwan 124

 ©2026 Palo Alto Networks, Inc.

Configurer l'authentification du moteur d'identité cloud....127
Authentification SAML du moteur d'identité sur le cloud avec affichage web intégré....127
Multi-authentification du moteur d'identité cloud....129
Configurer GlobalProtect pour faciliter les notifications d'authentification multifacteur....130
Activer la transmission des ASV vers un serveur RADIUS....135
Activer le mappage des groupes....136
Chapitre 3 : Passerelles GlobalProtect....139
Priorité de passerelle dans une configuration de passerelle multiple....141
Meilleurs critères de sélection de passerelle....143
Configurer une passerelle GlobalProtect....146
Attribution et gestion d'adresses IP basées sur DHCP pour GlobalProtect....166
Configurer le serveur DHCP sur la passerelle GlobalProtect pour attribuer des adresses IP DHCP aux terminaux....167
Configurer un serveur DHCP sur le serveur Windows ou sur le serveur Infoblox....178
Personnaliser les paramètres de délai d'expiration de la session du terminal....194
Modifier les paramètres de délai d'expiration de la session du terminal....195
Activer les notifications des utilisateurs finaux concernant la déconnexion de la session GlobalProtect....196
Configurer l'extension de session utilisateur....198
Séparation du trafic tunnel sur les passerelles GlobalProtect....200
Configuration d'un tunnel séparé en fonction de l'itinéraire d'accès....201
Configuration d'un tunnel séparé en fonction du domaine et de l'application....207
Configurer le DNS segmenté....215
Exclusion du trafic vidéo à partir du tunnel VPN GlobalProtect....224
Héberger un fichier de configuration pour la segmentation de tunnel sur un serveur web....227
GlobalProtect MIB support....233
Chapitre 4 : Portails GlobalProtect....235
Paramétrer l'accès au portail GlobalProtect....236
Définir les configurations d'authentification client GlobalProtect....242
Définir les configurations de l'agent GlobalProtect....246
Configurer la sélection intelligente du portail....258
Personnaliser l'application GlobalProtect....263
Configurer l'application cohérente des politiques....295
Configurer la détection du portail captif en mode proxy et hybride....297
Connexions de tunnel via des proxys....298

 ©2026 Palo Alto Networks, Inc.

Personnaliser les pages d'accès, de bienvenue et d'aide du Portail GlobalProtect 302
Application de GlobalProtect pour l'accès au réseau 310
Application de la stratégie de trafic des points de terminaison 312
Configurer l'application de la politique de trafic des terminaux 313
Application de la politique de trafic des terminaux sans accès direct au réseau local 315
Cas pratiques de l'application de la politique de trafic des terminaux 317
Exclure les domaines consommant beaucoup de bande passante et permettre l'accès aux ressources locales tout en empêchant le trafic sur l'adaptateur physique 318
Limitations des fonctionnalités 319
Chapitre 5 : Applications GlobalProtect 321
Déployer l'application GlobalProtect sur les ordinateurs de bureau 322
Configuration matérielle minimale requise pour l'application GlobalProtect 325
Télécharger le package logiciel de l'application GlobalProtect pour l'hébergement sur le portail 326
Mises à jour de l'application hôte 327
Tester l'installation de l'application 330
Télécharger et installer l'application mobile GlobalProtect 335
Lanceur CLI pour GlobalProtect 338
Afficher et collecter les journaux d'application GlobalProtect 340
Déployer l'application GlobalProtect sur les périphériques mobiles 346
Aperçu de la gestion des périphériques mobiles 347
Paramétrer l'intégration MDM avec GlobalProtect 351
Fournisseurs MDM qualifiés 352
Gérer l'application GlobalProtect à l'aide de Workspace ONE 354
Gérer l'application GlobalProtect à l'aide de Microsoft Intune 456
Gérer l'application GlobalProtect à l'aide de MobileIron 515
Gérer l'application GlobalProtect à l'aide de la console Google Admin 520
Gérer l'application GlobalProtect à l'aide de Jamf Pro 532
Supprimer les notifications sur l'application GlobalProtect pour les terminaux macOS 605
Gérer l'application GlobalProtect à l'aide d'autres MDM tiers 608
Déployer les paramètres d'application de façon transparente 616
Paramètres d'application personnalisables 617
Configurer la méthode de connexion conditionnelle en fonction du type de réseau 635
Déployer les paramètres d'application sur des points de terminaison Windows 635

 ©2026 Palo Alto Networks, Inc.

Déployer les paramètres de l'application sur les points de terminaison Linux....660
Processus GlobalProtect à mettre sur liste blanche dans les déploiements EDR.... 663

Chapitre 6 : VPN sans client GlobalProtect.... 665

Aperçu du VPN sans client.... 666
Technologies prises en charge.... 669
Configurer le VPN sans client.... 671
Configurer le VPN sans client – Panorama....671
Configurer le VPN sans client – SCM....680
Résoudre les problèmes du VPN sans client.... 681

Chapitre 7 : Informations sur l'hôte.... 687

Host Information Profile (profil d'informations sur l'hôte - HIP) dans l'application de la politique de sécurité....688
Assurer la conformité des terminaux avec les vérifications HIP....688
Configurer la mise en œuvre des politiques basées sur HIP....708
Configurer les exceptions HIP pour la gestion des correctifs....722
Collecter des données d'application et de processus sur des points de terminaison....725
Configurer la correction du processus HIP....735
Redistribution des rapports HIP....744
Configurer l'agent User-ID Windows pour collecter des informations d'hôte....747
Périphériques en quarantaine utilisant les informations de l'hôte....756
Résoudre les problèmes HIP....771
Service de conformité de l'hôte....775
Activer le service de conformité de l'hôte....776
Configurer la redistribution du cloud....777
Configurer CIE pour HCS....779
Configurer la politique de sécurité basée sur les services de conformité des hôtes....779

Chapitre 8 : Surveillance et dépannage de GlobalProtect.... 793

Surveillance de GlobalProtect à l'aide du service de journalisation Strata....794
Liste de vérification Collecte de journaux de l'application GlobalProtect pour le dépannage....795
Configurer la connectivité GlobalProtect vers Strata Logging Service....797
Configurer les paramètres de collecte des journaux de l'application sur le portail GlobalProtect....807
Afficher les journaux de dépannage et de diagnostic de l'application GlobalProtect sur l'application Explore....809
Surveillance de GlobalProtect à l'aide de PAN-OS....822

 ©2026 Palo Alto Networks, Inc.

Afficher un affichage graphique de l'activité des utilisateurs de GlobalProtect dans PAN-OS....822
Afficher tous les journaux GlobalProtect sur une page dédiée dans PAN-OS....824
Descriptions des événements pour les journaux GlobalProtect dans PAN-OS....825
Filtrer les journaux GlobalProtect pour la latence de la passerelle dans PAN-OS....829
Restreindre l'accès aux journaux GlobalProtect dans PAN-OS....830
Transférer les journaux GlobalProtect vers un service externe dans PAN-OS....831
Configuration de rapports personnalisés pour GlobalProtect dans PAN-OS....832

Chapitre 9 : Exigences de GlobalProtect pour les périphériques IoT....835

Configuration des portails et des passerelles GlobalProtect pour les périphériques IoT....836
Installation GlobalProtect pour IoT sur Android....842
Installation GlobalProtect pour IoT sur Raspbian....845
Installation GlobalProtect pour IoT sur Ubuntu....847
Installation GlobalProtect pour IoT sur Windows....849
Téléchargez le fichier MSIEXEC sur le périphérique IoT et installez-le....849
Modifiez les clés de registre sur le périphérique IoT (à la demande ou toujours actif)....849
Modifiez les clés de registre sur le périphérique IoT (Toujours actif avec préouverture de session)....851

Chapitre 10 : Certification FIPS-CC de GlobalProtect....853

Activation et vérification du mode FIPS-CC....854
Fonctions de sécurité FIPS-CC....879
Résolution des problèmes du mode FIPS-CC....881

Chapitre 11 : Cryptographie de GlobalProtect....889

Échange de chiffrement entre l'application GlobalProtect et la passerelle....890
Fonctions cryptographiques de l'application GlobalProtect....893
Suites de chiffrement TLS prises en charge par les applications GlobalProtect....895
Chiffrements utilisés pour configurer les tunnels IPsec....902
API SSL....904

Chapitre 12 : Configurations rapides GlobalProtect....905

VPN d'accès à distance (Profil d'authentification)....906
VPN d'accès à distance (profil de certificat)....910
VPN d'accès à distance avec l'authentification à deux facteurs....915

 ©2026 Palo Alto Networks, Inc.

GlobalProtect : configuration de VPN toujours activée 921
VPN d'accès à distance avec pré-ouverture de session 922
Connexion préouverture de session initiée par l'utilisateur 932
Configuration de plusieurs passerelles GlobalProtect 941
GlobalProtect pour l'archivage HIP interne et l'accès basé sur l'utilisateur 945
Configuration mixte de passerelles internes et externes 952
Portail captif et application de GlobalProtect pour l'accès au réseau 960
GlobalProtect sur les PC Cloud Windows 365 965
Fonctionnalités et limites prises en charge 968

 ©2026 Palo Alto Networks, Inc.

Configurer le pare-feu

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour que GlobalProtect™ fonctionne, vous devez configurer l'infrastructure qui permet à tous les composants de communiquer. À un niveau de base, cela signifie la mise en place des interfaces et des zones auxquelles les utilisateurs finaux GlobalProtect se connectent pour accéder au portail et aux passerelles vers le réseau. Comme les composants GlobalProtect communiquent sur des canaux sécurisés, vous devez acquérir et déployer tous les certificats SSL requis sur les différents composants. Les sections suivantes vous guident tout au long de la configuration de l'infrastructure de GlobalProtect :

- Créer des interfaces et des zones pour GlobalProtect
- Activer SSL entre les composants GlobalProtect

Créer des interfaces et des zones pour GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous devez configurer les interfaces et les zones suivantes pour votre infrastructure GlobalProtect :

- **Portail GlobalProtect** — requiert une interface de couche 3 ou de retour en boucle pour la connexion des applications GlobalProtect. Si le portail et la passerelle se trouvent sur le même pare-feu, ils peuvent utiliser la même interface. Le portail doit être dans une zone qui est accessible depuis l'extérieur de votre réseau, par exemple une zone DMZ.
- **Passerelles GlobalProtect** : l'interface et les exigences de zone pour la passerelle dépendent de savoir si la passerelle que vous configurez est externe ou interne, comme suit :
  - **Passerelles externes** : Exige une interface avec une couche 3 ou retour de boucle et une interface de tunnel logique pour que l'application s'y connecte pour établir une connexion. L'interface avec couche 3/retour de boucle doit être dans une zone externe, telle qu'une zone DMZ. Une interface de tunnel peut être dans la même zone que l'interface de connexion à vos ressources internes (par exemple, **`trust`**). Pour une sécurité accrue et une meilleure visibilité, vous pouvez créer une zone distincte, telle que **`corp-vpn`**. Si vous créez une zone séparée pour votre interface de tunnel, vous devrez créer des politiques de sécurité pour autoriser le trafic à circuler entre la zone VPN et la zone de confiance.
  - **Passerelles internes** : Exige une interface avec couche 3 ou retour de boucle dans votre zone de confiance. Vous pouvez aussi créer une interface de tunnel pour l'accès à vos passerelles internes, mais cela n'est pas obligatoire.

Pour des astuces concernant l'utilisation d'une interface avec retour de boucle pour permettre l'accès à GlobalProtect sur différents ports et adresses, consultez le document Can GlobalProtect Portal Page be Configured to be Accessed on any Port?

1. Configurez une interface de couche 3 pour chaque portail et/ou passerelle que vous prévoyez déployer.

   Si la passerelle et le portail sont sur le même pare-feu, vous pouvez utiliser une seule interface pour les deux.

   Selon la procédure recommandée, utilisez des adresses IP statiques pour le portail et la passerelle.

   N'attachez pas de profil de gestion d'interface qui autorise HTTP, HTTPS, Telnet ou SSH sur l'interface où vous avez configuré un portail ou une passerelle GlobalProtect, car cela permet d'accéder à votre interface de gestion depuis Internet. Suivez les Meilleures pratiques pour

 ©2026 Palo Alto Networks, Inc.

sécuriser l'accès administratif *afin de vous assurer que vous sécurisez l'accès administratif à vos pare-feu d'une manière qui empêchera la réussite des attaques.*

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** ou **Network (Réseau)** > **Interfaces** > **Loopback (Retour de boucle)**, puis sélectionnez l'interface que vous souhaitez configurer pour GlobalProtect. Dans cet exemple, nous configurons **`ethernet1/1`** en tant qu'interface de portail.
2. (Ethernet uniquement) Définissez le paramètre **Interface Type (Type d'interface)** sur **Layer3 (Couche 3)**.
3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** à laquelle l'interface de portail ou de passerelle appartient de la manière suivante :
   - Placez les portails et les passerelles externes dans une zone non approuvée pour l'accès par des hôtes à l'extérieur de votre réseau, tel que **`l3-untrust`**.
   - Placez les passerelles internes dans une zone interne, telle que **`l3-trust`**.
   - Si vous n'avez pas créé la zone, ajoutez une **New Zone (Nouvelle zone)**. Dans la boîte de dialogue Zone, donnez un **Nom** à la nouvelle zone, puis cliquez sur **OK**.
4. Sélectionnez le **Virtual Router (Routeur virtuel)** par défaut.
5. Affectez une adresse IP à l'interface :
   - Pour une adresse IPv4, sélectionnez **IPv4** et **Add (Ajouter)** l'adresse IP et le masque de réseau à affecter à l'interface, par exemple 203.0.11.100/24.
   - Pour une adresse IPv6, sélectionnez **IPv6**, **Enable IPv6 on the interface (Activez IPv6 sur l'interface)**, et **Add (Ajoutez)** l'adresse IP et le masque réseau à affecter à l'interface, par exemple 2001:1890:12f2:11::10.1.8.160/80.
6. Cliquez sur **OK** pour enregistrer la configuration de l'interface.

2. Sur les pare-feu hébergeant les passerelles GlobalProtect, configurez l'interface de tunnel logique qui terminera les tunnels VPN établis par les applications GlobalProtect.

   Les adresses IP ne sont pas obligatoires sur l'interface de tunnel sauf si vous exigez un routage dynamique. En outre, l'attribution d'une adresse IP à l'interface de tunnel peut être utile pour le dépannage des problèmes de connectivité.

   Veillez à activer l'ID utilisateur dans la zone dans laquelle les tunnels VPN se terminent.

   1. Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** et **Add (Ajoutez)** une interface de tunnel.
   2. Dans le champ **Interface Name (Nom de l'interface)**, saisissez un suffixe numérique, tel que **`.2`**.
   3. Dans l'onglet **Config (Configuration)**, sélectionnez la **Security Zone (Zone de sécurité)** pour la terminaison du tunnel VPN, comme suit :
      - Pour utiliser votre zone approuvée comme point de terminaison du tunnel, sélectionnez la zone dans la liste déroulante.
      - (Recommandé) Pour créer une zone séparée pour la terminaison du tunnel VPN, ajoutez une **New Zone (Nouvelle zone)**. Dans la boîte de dialogue, donnez un **Name**

 ©2026 Palo Alto Networks, Inc.

(Nom) à la nouvelle zone (par exemple, **`corp-vpn`**), **Enable User Identification (Activer l'identification utilisateur)**, puis cliquez sur **OK**.

4. Définissez le **Virtual Router (Routeur virtuel)** sur **None (Aucun)**.
5. Affectez une adresse IP à l'interface :
   - Pour une adresse IPv4, sélectionnez **IPv4** et **Add (Ajouter)** l'adresse IP et le masque de réseau à affecter à l'interface, par exemple 203.0.11.100/24.
   - Pour une adresse IPv6, sélectionnez **IPv6**, **Enable IPv6 on the interface (Activez IPv6 sur l'interface)**, et **Add (Ajoutez)** l'adresse IP et le masque réseau à affecter à l'interface, par exemple 2001:1890:12f2:11::10.1.8.160/80.
6. Cliquez sur **OK** pour enregistrer la configuration de l'interface.

3. Si vous avez créé une zone distincte pour le point de terminaison du tunnel de connexions VPN, créez une politique de sécurité afin d'autoriser le flux de trafic entre la zone VPN et votre zone de confiance.

Par exemple, la règle de politique suivante active le trafic entre la zone **`corp-vpn`** et la zone **`l3-de confiance`**.

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

4. **Commit (Validez)** la configuration.

 ©2026 Palo Alto Networks, Inc.

Activer SSL entre les composants GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Toute interaction entre les composants GlobalProtect se produit via une connexion SSL/TLS. C'est pourquoi vous devez générer et installer les certificats requis avant de configurer chaque composant pour que vous puissiez référencer le certificat approprié dans les configurations. Les sections suivantes décrivent les méthodes de déploiement de certificat prises en charge, les descriptions et les directives relatives aux divers certificats GlobalProtect, et fournissent des instructions sur la génération et le déploiement des certificats nécessaires :

- À propos du Déploiement de Certificats GlobalProtect
- Procédures recommandées pour les certificats GlobalProtect
- Déployer les certificats de serveur sur les composants GlobalProtect

À propos du Déploiement de Certificats GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Il existe trois approches fondamentales pour déployer des certificats serveur sur les composants GlobalProtect :

- (Recommandé) **Combinaison de certificats indépendants et de certificats auto-signés** : Comme l'application GlobalProtect accédera au portail avant la configuration de GlobalProtect, l'application doit faire confiance au certificat pour établir une connexion HTTPS.
- **CA d'entreprise** : si vous avez déjà votre propre Certificate Authority (autorité de certification - CA) d'entreprise, vous pouvez utiliser cette CA interne pour générer des certificats pour chacun des composants GlobalProtect puis les importer sur les pare-feu hébergeant votre portail et vos passerelles. Dans ce cas, vous devez aussi veiller à ce que les points de terminaison fassent confiance au certificat AC racine utilisé pour générer les certificats pour les services GlobalProtect auxquels ils doivent se connecter.
- **Certificats auto-signés** : vous pouvez générer un certificat CA auto-signé sur le portail et l'utiliser pour générer des certificats pour tous les composants GlobalProtect. Toutefois, cette solution n'est pas recommandée puisqu'elle est moins sécurisée que les autres options. Si vous choisissez néanmoins cette option, les utilisateurs finaux verront une erreur de certificat

 ©2026 Palo Alto Networks, Inc.

la première fois qu'ils se connecteront au portail. Pour empêcher l'affichage de cette erreur, vous pouvez déployer le certificat AC racine auto-signé sur tous les points de terminaison manuellement ou avoir recours à certaines fonctions de déploiement centralisé, par exemple une stratégie de groupe Active Directory Group Policy Object (GPO).

Procédures recommandées pour les certificats GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Les composants GlobalProtect doivent avoir des certificats valides pour établir une connexion en utilisant SSL/TLS. La connexion échoue si vos certificats sont invalides ou expirés.

Le tableau suivant résume les certificats SSL/TLS dont vous aurez besoin, selon les fonctions que vous envisagez d'utiliser :

certificate	Usage	Génération de processus et meilleures pratiques
Certificat AC	Utilisé pour signer les certificats générés pour les composants GlobalProtect.	Si vous prévoyez d'utiliser des certificats auto-signés, générez un certificat CA au moyen de votre serveur CA dédié ou de votre pare-feu Palo Alto Networks, puis émettez des certificats de portail et de passerelle GlobalProtect signés par la CA ou une CA intermédiaire.
Certificat du serveur de portail	Autorise les applications GlobalProtect à établir une connexion HTTPS avec le portail.	• Ce certificat est identifié dans un profil de service SSL/TLS. Vous attribuez le certificat du serveur de portail en sélectionnant son profil de service associé dans une configuration de portail. • Importez un certificat de serveur d'une autorité de certification tierce bien connue. Il s'agit de l'option la plus sécurisée et garantit que les points d'extrémité utilisateur peuvent établir une relation de confiance avec le portail et sans vous obliger à déployer le certificat AC racine. • Si vous n'utilisez pas une autorité de certification publique bien connue, vous devez exporter le certificat CA racine utilisé pour générer le certificat du serveur de portail à tous les terminaux qui exécutent l'application GlobalProtect. L'exportation de

 ©2026 Palo Alto Networks, Inc.

certificate	Usage	Génération de processus et meilleures pratiques
		ce certificat empêche les utilisateurs finaux de voir les avertissements de certificat lors de la connexion initiale du portail. • Les champs CN (Common Name) et Subject Alternative Name (SAN) du certificat doivent correspondre exactement à l'adresse IP ou au nom de domaine complet (FQDN) de l'interface hébergeant le portail. • En général, un portail doit posséder son propre certificat de serveur. Toutefois, si vous déployez une seule passerelle et un portail sur la même interface, vous devez utiliser le même certificat pour la passerelle et le portail. • Si vous configurez une passerelle et un portail sur la même interface, nous vous recommandons également d'utiliser le même profil de certificat et le même profil de service SSL/TLS pour la passerelle et le portail. S'ils n'utilisent pas le même profil de certificat ni le même profil de service SSL/TLS, la configuration de la passerelle est prioritaire sur la configuration du portail lors de la connexion SSL.
Certificat du serveur de passerelle	Autorise les applications GlobalProtect à établir une connexion HTTPS avec la passerelle.	• Ce certificat est identifié dans un profil de service SSL/TLS. Vous attribuez le certificat du serveur de passerelle en sélectionnant son profil de service associé dans une configuration de passerelle. • Générer un certificat CA sur le pare-feu ou le serveur de CA et utiliser ce certificat CA pour générer tous les certificats de passerelle. • Les champs CN (Common Name) et Subject Alternative Name (SAN) du certificat doivent correspondre exactement à l'adresse IP ou au nom de domaine complet (FQDN) de l'interface sur laquelle vous envisagez de configurer la passerelle. • Le portail peut distribuer le certificat CA racine de la passerelle à l'application GlobalProtect en fonction de la configuration (Liste des CA racine de confiance à l'onglet Agent de la configuration du portail). Cependant, il n'est pas obligatoire de préinstaller le certificat CA racine de la

 ©2026 Palo Alto Networks, Inc.

certificate	Usage	Génération de processus et meilleures pratiques
		passerelle dans le magasin de certificats de confiance de l'utilisateur ou d'émettre le certificat de la passerelle au moyen d'une CA publique. • En général, chaque passerelle doit posséder son propre certificat de serveur. Néanmoins, si vous déployez une seule passerelle et un seul portail sur la même interface pour l'accès VPN de base, vous devez utiliser un seul certificat de serveur pour les deux composants. En tant que meilleure pratique, utilisez un certificat signé par une CA publique. • Si vous configurez une passerelle et un portail sur la même interface, nous vous recommandons également d'utiliser le même profil de certificat et le même profil de service SSL/TLS pour la passerelle et le portail. S'ils n'utilisent pas le même profil de certificat ni le même profil de service SSL/TLS, la configuration de la passerelle est prioritaire sur la configuration du portail lors de la connexion SSL.

(Facultatif) Certificat client	Utilisé pour activer l'authentification mutuelle lors de l'établissement d'une session HTTPS entre les applications GlobalProtect et les passerelles / le portail. Cela garantit que seuls les points de terminaison dotés de certificats clients valides peuvent s'authentifier et se connecter au réseau.	• Pour un déploiement simplifié des certificats clients, configurez le portail pour déployer le certificat client sur les applications lors d'une connexion réussie en utilisant l'une des méthodes suivantes :
		  • Utilisez un certificat de client unique sur toutes les applications GlobalProtect qui reçoivent la même configuration. Attribuez le certificat de client **Local** en téléchargeant le certificat sur le portail et en le sélectionnant dans une configuration d'agent de portail.
		  • Utilisez un protocole d'inscription de certificat simple (**SCEP**) pour permettre au portail GlobalProtect de déployer des certificats de clients uniques à vos applications GlobalProtect. Activez cette option en configurant un profil SCEP, puis en sélectionnant ce profil dans une configuration de l'agent de portail.
		• Utilisez l'un des algorithmes de synthèse suivants lors de la génération des certificats

 ©2026 Palo Alto Networks, Inc.

certificate	Usage	Génération de processus et meilleures pratiques
		clients pour les points de terminaison GlobalProtect : sha1, sha256, sha384 ou sha512. • Vous pouvez utiliser d'autres mécanismes pour déployer des certificats clients uniques sur chaque point de terminaison lors de l'authentification de l'utilisateur final. • Songez à tester votre configuration sans le certificat client d'abord, puis ajoutez le certificat client après avoir vérifié que les autres paramètres de configuration sont corrects.
(Facultatif) Certificats machines	Un certificat de machine est un certificat de client qui est émis par un terminal qui se trouve dans le magasin de l'ordinateur local ou dans System Keychain. Chaque certificat de machine identifie le point de terminaison dans le champ sujet (par exemple, CN = laptop1.example.com) au lieu d'un utilisateur. Le certificat garantit que seuls les points de terminaison approuvés peuvent se connecter aux passerelles ou au portail. Les certificats de machine sont requis pour les utilisateurs qui sont configurés au moyen de la méthode de connexion avant ouverture de session.	• Utilisez l'un des algorithmes de synthèse suivants lors de la génération des certificats clients pour les points de terminaison GlobalProtect : sha1, sha256, sha384 ou sha512. • Si vous envisagez d'utiliser la fonction de pré-connexion (avant ouverture de session), vous devez utiliser votre propre infrastructure CPI pour déployer les certificats machines sur chaque point de terminaison avant d'activer l'accès à GlobalProtect. Cette démarche est importante pour assurer la sécurité. Pour plus d'informations, voir VPN d'accès distant avec pré-connexion.

Tableau : Conditions exigées pour les certificats GlobalProtect

Pour plus de détails sur les types de clés utilisées pour établir une communication sécurisée entre l'agent GlobalProtect et les portails et passerelles, reportez-vous à la section Référence : Fonctions cryptographiques de l'application GlobalProtect.

©2026 Palo Alto Networks, Inc.

Déployer les certificats de serveur sur les composants GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Pour le protocole TLS v1.3 : • PAN-OS 11.1 ou version ultérieure • Version GlobalProtect 6.0.8 et ultérieure, version GlobalProtect 6.1.3 et ultérieure, ou version GlobalProtect 6.2.1 et ultérieure • TLSv1.3 n'est pas pris en charge en mode FIPS-CC

Les composants GlobalProtect doivent avoir des certificats valides pour établir une connexion en utilisant SSL/TLS. La connexion échoue si vos certificats sont invalides ou expirés.

L'action suivante décrit les étapes de la procédure recommandée pour déployer les certificats SSL/TLS sur les composants GlobalProtect :

Importez un certificat de serveur d'une autorité de certification tierce reconnue.

Utilisez un certificat de serveur d'une AC indépendante reconnue pour le portail GlobalProtect. Cette pratique garantit que les utilisateurs finaux sont en mesure d'établir une connexion HTTPS sans voir les avertissements sur des certificats non fiables.

Le NC et, le cas échéant, les champs ASR du certificat doivent correspondre au FQDN ou à l'adresse IP de l'interface où vous prévoyez de configurer le portail ou l'interface d'archivage du périphérique sur un système de gestion de terminaux mobiles tiers. Les correspondances Wildcard sont prises en charge.

Avant d'importer un certificat, assurez-vous que le certificat et les fichiers clés sont accessibles à partir de votre système de gestion et que vous avez le mot de passe pour décrypter la clé privée.

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importer)** un nouveau certificat.
   - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW et Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** et **Import (Importer)** un nouveau certificat.
2. Utilisez le type de certificat **Local (local)** (par défaut).
3. Saisissez un **Certificate Name (Nom de certificat)**.

 ©2026 Palo Alto Networks, Inc.

4. Saisissez le chemin et le nom du **Certificate File (Fichier du certificat)** envoyé par l'AC, ou **Browse (Naviguez)** pour trouver le fichier.
5. Définissez le **File Format (Format de fichier)** sur **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))**.
6. Saisissez le chemin et le nom du fichier PKCS#12 dans le champ **Key File (Fichier de clé)** ou **Browse (Naviguez)** pour le trouver.
7. Saisissez et confirmez la **Passphrase (Phrase secrète)** qui a été utilisée pour crypter la clé privée.
8. Cliquez sur **OK** pour importer le certificat et la clé.

Créer le certificat CA racine pour générer les certificats auto-signés pour les composants GlobalProtect

Créez le certificat CA racine sur le portail et utilisez-le pour générer les certificats de serveur pour les passerelles et, facultativement, pour les clients.

Avant de déployer des certificats auto-signés, vous devez créer le certificat d'autorité de racine qui signe les certificats pour les composants GlobalProtect :

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importer)** un nouveau certificat.
   - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW et Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** et **Import (Importer)** un nouveau certificat.
2. Utilisez le type de certificat **Local (local)** (par défaut).
3. Saisissez un **Certificate Name (nom de certificat)**, tel que GlobalProtect_CA. Le nom du certificat ne doit pas contenir d'espace.
4. Ne sélectionnez pas de valeur dans le champ **Signed By (signé par)**. Sans une sélection pour **Signed By (Signé par)**, le certificat est auto-signé.
5. Activez l'option **Certificate Authority (Autorité de certificat)**.
6. Cliquez sur **OK** pour générer le certificat.

Utilisez l'autorité de certification racine sur le portail pour générer un certificat de serveur auto-signé.

Générez des certificats de serveur pour chaque passerelle que vous prévoyez déployer et éventuellement pour l'interface de gestion du système de gestion de points de terminaison mobiles tiers (si cette interface est à l'endroit où les passerelles récupèrent les rapports HIP).

Dans les certificats de serveur Gateway, les valeurs des champs NC et ASR doivent être identiques. Si les valeurs diffèrent, l'agent GlobalProtect détecte l'incompatibilité et ne fait pas

 ©2026 Palo Alto Networks, Inc.

*confiance au certificat. Les certificats signés ne contiennent un champ ASR que si vous ajoutez un attribut de **Host Name (nom d'hôte)**.*

Vous pouvez également utiliser le protocole Simple Certificate Enrollment Protocol (protocole simple d'enregistrement de certificat - SCEP) pour demander un certificat de serveur auprès de votre CA d'entreprise.

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importer)** un nouveau certificat.
   - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW et Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** et **Import (Importer)** un nouveau certificat.
2. Utilisez le type de certificat **Local (local)** (par défaut).
3. Saisissez un **Certificate Name (Nom de certificat)**. Ce nom ne peut pas contenir d'espaces.
4. Dans le champ **Common Name (nom commun)**, saisissez le FQDN (recommandé) ou l'adresse IP de l'interface dans laquelle vous prévoyez de configurer la passerelle.
5. Dans le champ **Signed By (Signé par)**, sélectionnez l'AC GlobalProtect créée précédemment.
6. Dans la zone Certificate Attributes (Attributs du certificat), **Add (Ajoutez)** et définissez les attributs pour identifier la passerelle de façon unique. N'oubliez pas que si vous ajoutez un attribut **Host Name (Nom d'hôte)** (qui renseigne le champ ASR du certificat), il doit correspondre exactement à la valeur que vous avez définie pour le **Common Name (Nom commun)**.
7. Configurez les paramètres cryptographiques pour le certificat de serveur, y compris l'**Algorithm (Algorithme)** de chiffrement, la longueur de clé (**Number of Bits (Nombre de bits)**), l'algorithme **Digest (Résumé)** et l'**Expiration (Expiration)** (jours).
8. Cliquez sur **OK** pour générer le certificat.

Utiliser le Simple Certificate Enrollment Protocol (protocole simple d'enregistrement de certificat - SCEP) pour demander un certificat de serveur à partir de votre CA d'entreprise

Configurez des profils SCEP distincts pour chaque portail et passerelle que vous prévoyez déployer. Utilisez ensuite le profil SCEP spécifique pour générer le certificat serveur pour chaque composant GlobalProtect.

*Dans les certificats de serveur, de portail et de passerelle, la valeur du champ NC doit inclure le FQDN (**recommandé**) ou l'adresse IP de l'interface où vous envisagez de configurer le portail ou la passerelle et doit être identique au champ ASR.*

 ©2026 Palo Alto Networks, Inc.

Pour vous conformer à la norme FIPS (U.S. Federal Information Processing Standard), vous devez également activer l'authentification SSL mutuelle entre le serveur SCEP et le portail GlobalProtect. (L'opération FIPS-CC est indiquée sur la page de connexion du pare-feu et dans la barre d'état du pare-feu.)

Une fois la configuration validée, le portail tente de demander un certificat d'AC à l'aide des paramètres du profil SCEP. En cas de succès, le pare-feu hébergeant le portail enregistre le certificat de l'AC et l'affiche dans la liste des **Device Certificates (certificats de périphérique)**.

1. Configurez un profil SCEP pour chaque portail ou passerelle GlobalProtect :
   1. Choisissez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SCEP** et **Add (Ajouter)** un nouveau certificat.
      - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** puis cliquez sur **Add SCEP (Ajouter SCEP)**.
   2. Entrez un **Name (Nom)** qui identifie le profil SCEP et le composant pour lequel vous déployez le certificat serveur. S'il s'agit du profil d'un pare-feu pouvant prendre en charge de multiples systèmes virtuels, sélectionnez un système virtuel ou sélectionnez l'option **Shared (Partagé)** en tant que **Location (Emplacement)** où le profil est disponible.
   3. (Facultatif) Configurez un mécanisme de **SCEP Challenge (Stimulation SCEP)** entre la PKI et le portail pour chaque demande de certificat. Utilisez soit un mot de passe de défi **Fixed (Fixe)** que vous obtenez à partir du serveur SCEP ou un mot de passe **Dynamic (Dynamique)** où le client Portail soumet un nom d'utilisateur et un MPUU de votre choix au serveur SCEP. Pour un défi SCEP dynamique, il peut s'agir des informations d'identification de l'administrateur CPI.
   4. Configurez la **Server URL (URL du serveur)** que le portail utilise pour atteindre le serveur SCEP dans la PKI (par exemple, **`http://10.200.101.1/certsrv/mscep/`**).
   5. Saisissez une chaîne (jusqu'à 255 caractères de longueur) dans le champ **CA-IDENT Name (Nom AC-IDENT)** pour identifier le serveur SCEP.
   6. Saisissez le nom de **Subject (Sujet)** à utiliser pour les certificats générés par le serveur SCEP. Le sujet doit inclure une clé de nom commun (NC) au format **`CN=<valeur>`** où **`<valeur>`** est le FQDN ou l'adresse IP du portail ou de la passerelle.
   7. Sélectionnez le **Subject Alternative Name Type (Type de nom alternatif de sujet)**. Pour entrer le nom de l'adresse de messagerie d'un certificat ou d'une autre extension de nom de sujet, sélectionnez le **RFC 822 Name (Nom RFC 822)**. Vous pouvez également entrer le **DNS Name (Nom DNS)** à utiliser pour évaluer les certificats, ou l'**Uniform Resource**

 ©2026 Palo Alto Networks, Inc.

Identifier (Identificateur de ressource uniforme) pour identifier la ressource à partir duquel le client obtiendra le certificat.

8. Configurez des paramètres cryptographiques additionnels, y compris la longueur de clé (**Number of Bits (Nombre de bits)**) et l'algorithme **Digest (Résumé)** pour la demande de signature de certificat.
9. Configurez les utilisations autorisées du certificat, soit pour la signature (**Use as digital signature (utiliser comme signature numérique)**) ou le cryptage (**Use for key encipherment (utiliser pour le chiffrement de clé)**).
10. (Facultatif) Pour veiller à ce que le portail se connecte au bon serveur SCEP, saisissez l'**CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**. Vous pouvez obtenir cette empreinte auprès de l'interface du serveur SCEP dans le champ « Empreinte numérique ».
11. Activer l'authentification SSL mutuelle entre le serveur SCEP et le portail GlobalProtect.
12. Cliquez sur **OK**, puis **Commit (validez)** la configuration.

2. **Generate (Générez)** un nouveau certificat d'autorité de certification.
3. Saisissez un **Certificate Name (Nom de certificat)**. Ce nom ne peut pas contenir d'espaces.
4. Sélectionnez le **SCEP Profile (profil SCEP)** à utiliser pour automatiser le processus de délivrance d'un certificat de serveur qui est signé par l'autorité de certification Enterprise vers un portail ou une passerelle, puis cliquez sur **OK** pour générer le certificat. Le portail GlobalProtect utilise les paramètres du profil SCEP pour soumettre un CSR à votre CPI d'Enterprise.

Affecter le certificat de serveur que vous avez importé ou généré à un profil de service SSL/TLS

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)** et **Add (Ajouter)** un nouveau profil de service SSL/TLS.
   - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** puis cliquez sur **Add Profile (Ajouter un profil)** dans la section Profils de service SSL/TLS.
2. Saisissez un **Name (Nom)** pour identifier le profil et sélectionnez le **Certificate (Certificat)** de serveur que vous venez d'importer ou de générer.
3. Définissez la gamme des versions SSL/TLS (**Min Version (version min)** à **Max Version (version max)**) pour la communication entre les composants GlobalProtect.

   *La **Max Version (version maximale)** compatible est **TLSv1.2**.*

   *Pour une sécurité renforcée, définissez la **Min Version (Version minimale)** sur **TLSv1.2**.*
4. Cliquez sur **OK** pour enregistrer le profil de service SSL/TLS.

 ©2026 Palo Alto Networks, Inc.

5. **Commit (Validez)** les modifications.

Affecter le certificat de serveur que vous avez importé ou généré à un profil de service SSL/TLS

GlobalProtect prend en charge les profils de service SSL/TLS avec une version TLS maximale de TLSv1.3. Vous pouvez créer des profils de service SSL/TLS sur le pare-feu qui héberge le portail ou la passerelle en spécifiant la plage des versions SSL/TLS prises en charge (de la version minimale prise en charge à la version maximale prise en charge) pour la communication entre les composants GlobalProtect.

Configurez les profils de service SSL/TLS avec TLSv1.3 pour fournir une sécurité renforcée et un échange TLS plus rapide lors de l'établissement de la connexion entre les composants GlobalProtect. TLSv1.3 est la version maximale prise en charge. Utilisée, elle offre une sécurité accrue en supprimant les chiffrements faibles pris en charge dans les versions TLS antérieures et en ajoutant des suites de chiffrement plus sécurisées.

1. Pour activer la connexion SSL entre les composants GlobalProtect, vous devez générer ou importer un certificat.

2. Effectuez l'une des actions suivantes sur le pare-feu qui héberge le portail et la passerelle GlobalProtect :

   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)** et **Add (Ajouter)** un nouveau profil de service SSL/TLS.
   - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** puis cliquez sur **Add Profile (Ajouter un profil)** dans la section Profils de service SSL/TLS.

3. Donnez un **Name (Nom)** au nouveau profil.

4. Sélectionnez le **Certificate (Certificat)** que vous avez importé.

5. Dans les Paramètres du protocole, définissez la gamme des versions SSL/TLS (**Min Version (Version min)** à **Max Version (Version max)**) pour la communication entre les composants GlobalProtect. Définissez la version TLS maximale prise en charge sur TLSv1.3.

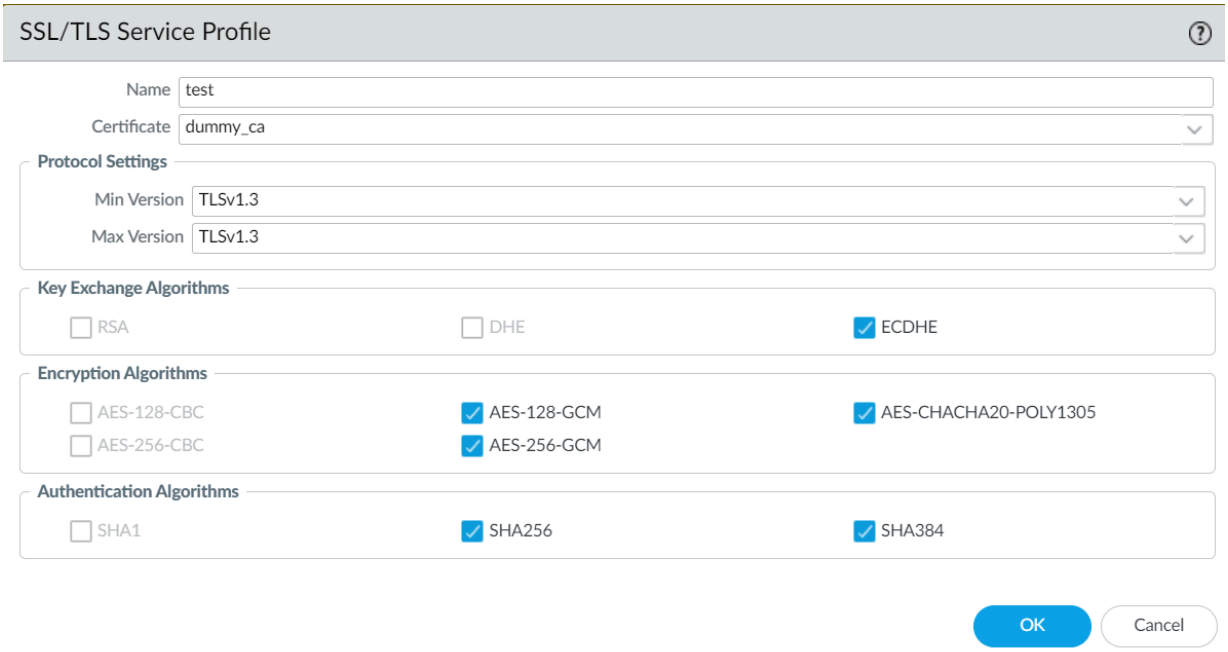
   *Pour fournir la sécurité la plus importante, définissez à la fois la **Min Version (Version min)** et la **Max Version (Version max)** sur TLSv1.3.*

Les algorithmes de chiffrement et les algorithmes d'authentification sont remplis automatiquement à partir des chiffres disponibles en fonction de vos paramètres de protocole TLS.

Le chiffrement TLSv1.3 **aes-chacha20-poly1305** n'est pas activé par défaut sur les périphériques exécutant Windows 11. Vous devez activer manuellement le chiffrement sur les terminaux GlobalProtect exécutant Windows 11.

 ©2026 Palo Alto Networks, Inc.

6. (Facultatif) Modifiez les chiffrement dans la section Algorithmes de chiffrement et Algorithmes d'authentification selon vos besoins.



7. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.

Déployer les certificats de serveur auto-signés

- *Exportez les certificats de serveur auto-signés générés par l'AC racine sur le portail et importez-les sur les passerelles.*
- *Veillez à générer un certificat de serveur unique pour chaque passerelle.*
- *Lors de l'utilisation des certificats auto-signés, vous devez distribuer le certificat CA racine aux clients finaux dans les configurations de client du portail.*

1. Exportez le certificat à partir du portail :
   1. Accédez à la section des certificats.
   2. Sélectionnez le certificat de passerelle que vous souhaitez déployer, puis cliquez sur **Export Certificate (Exporter le certificat)**.
   3. Définissez le **File Format (Format de fichier)** sur **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))**.
   4. Saisissez et confirmez une **Passphrase (Phrase secrète)** pour chiffrer la clé privée.
   5. Cliquez sur **OK** pour télécharger le fichier PKCS12 vers un emplacement de votre choix.

 ©2026 Palo Alto Networks, Inc.

2. Importez le certificat sur la passerelle:
   1. Accédez à la section des certificats.
   2. Saisissez un **Certificate Name (Nom de certificat)**.
   3. **Browse (Parcourez)** pour trouver et sélectionner le **Certificate File (Fichier de certificat)** que vous avez téléchargé dans l'étape précédente.
   4. Définissez le **File Format (Format de fichier)** sur **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))**.
   5. Saisissez et confirmez la **Passphrase (Phrase secrète)** que vous avez utilisée pour chiffrer la clé privée lorsque vous l'avez exportée à partir du portail.
   6. Cliquez sur **OK** pour importer le certificat et la clé.
   7. **Commit (Validez)** les modifications apportées à la passerelle.

Remplacer un certificat de portail ou de passerelle GlobalProtect expiré

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Si le certificat de votre portail ou passerelle GlobalProtect a expiré ou est sur le point d'expirer, vous avez plusieurs options pour le remplacer.

Pour les déploiements Prisma Access, les certificats de portail et de passerelle ainsi que leurs renouvellements sont gérés automatiquement dans le cadre de l'infrastructure, ainsi vous n'avez rien à faire pour remplacer un certificat expiré.

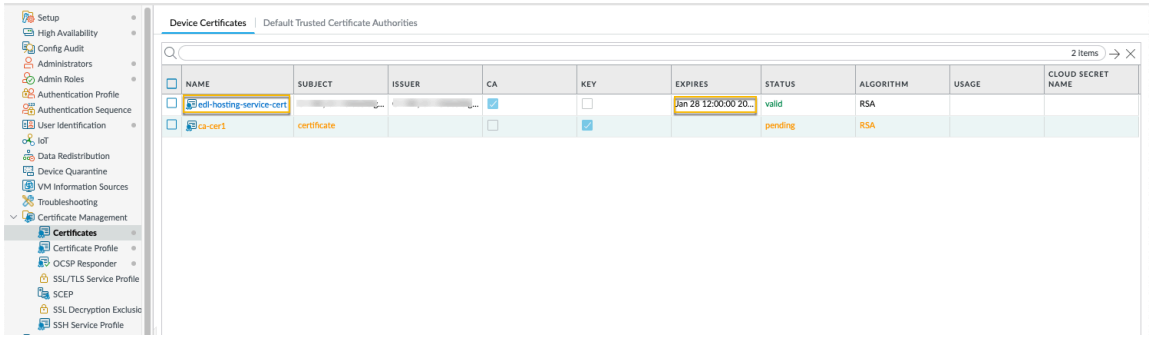
> *Si vous utilisez des certificats tiers pour votre portail ou passerelle, vous devrez gérer et renouveler vos certificats lorsque ces derniers expirent.*

Si le pare-feu est l'autorité de certification (CA) qui a émis le certificat pour votre portail et vos passerelles, le pare-feu remplace le certificat expiré par un nouveau certificat avec les mêmes attributs que l'ancien certificat mais avec un numéro de série différent. Depuis l'interface web qui héberge le portail ou la passerelle, Renouvelez le certificat et validez les modifications pour pousser le certificat vers le portail ou la passerelle.

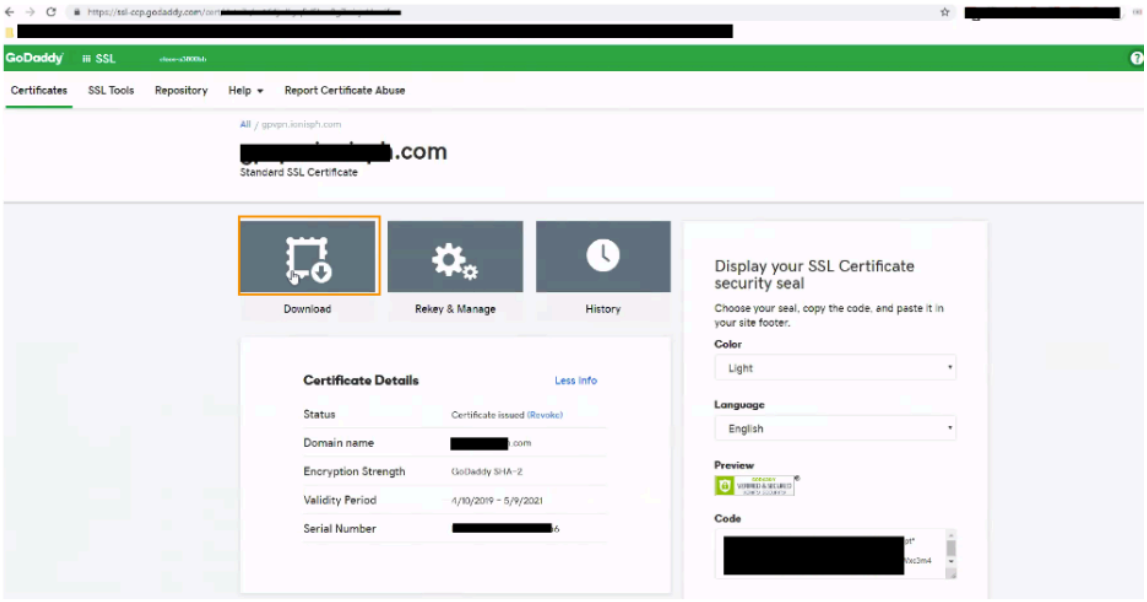
Pour les déploiements sur site qui utilisent des certificats SSL émis par une CA tierce, vous devez importer le certificat renouvelé que vous avez téléchargé depuis votre CA en utilisant la procédure suivante :

 ©2026 Palo Alto Networks, Inc.

1. Notez le nom et la date d'expiration du certificat de portail ou de passerelle.
   1. Depuis le pare-feu qui héberge la passerelle ou le portail avec le certificat expirant, connectez-vous à l'interface web.
   2. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
   3. Localisez le certificat dans l'onglet **Device Certificates (Certificats de périphérique)** et notez le nom du certificat et sa date d'expiration.



2. Téléchargez le certificat renouvelé depuis votre CA tierce. Pour vous donner un exemple, voici les étapes à suivre pour télécharger le certificat renouvelé depuis GoDaddy :
   1. Connectez-vous au portail godaddy.com.
   2. Allez sur l'onglet **Certificates (Certificats)**.
   3. Sélectionnez le certificat CA, puis cliquez sur **Download (Télécharger)**.



   4. Dans la fenêtre Télécharger le certificat, pour **Server type (Type de serveur)**, sélectionnez **Other (Autre)** et téléchargez le certificat au format **.crt**.

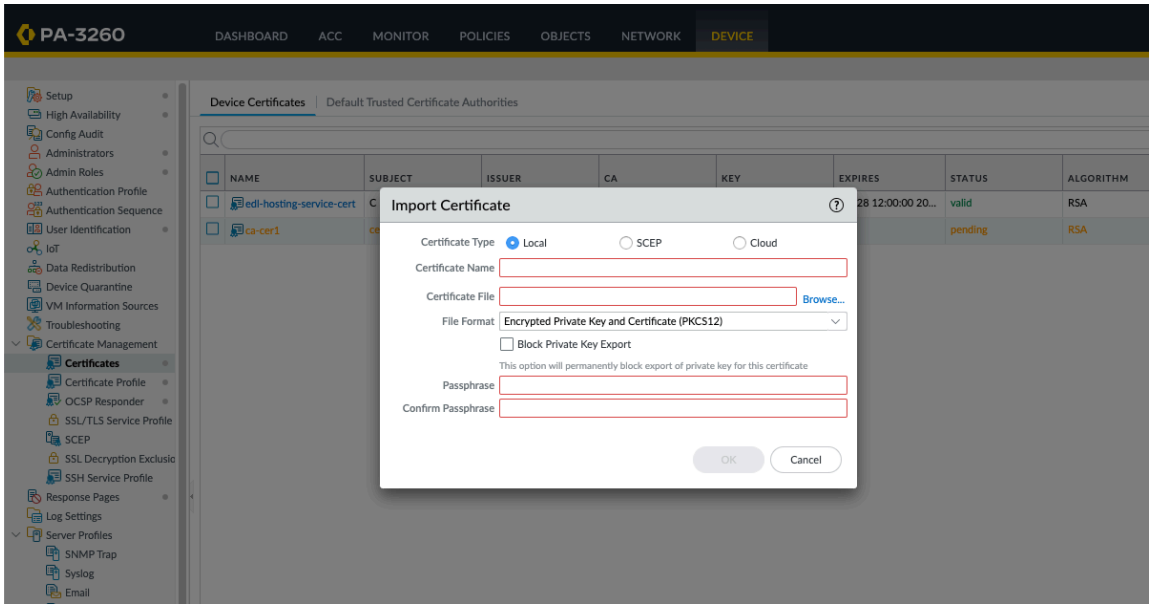
      Le certificat est enregistré dans votre dossier de téléchargements.

 ©2026 Palo Alto Networks, Inc.

3. Importez le certificat téléchargé sur le pare-feu qui héberge votre portail ou passerelle.

   Si vous avez déployé deux pare-feu dans une paire HA au sein d'un déploiement actif/passif, vous devez importer le certificat sur chaque pare-feu.

   1. Depuis l'interface web, accédez à **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**.
   2. Surlignez le certificat à renouveler et cliquez sur **Import (Importer)**.
   3. Entrez le **Certificate Name (Nom du certificat)** exact pour le certificat du portail ou de la passerelle que vous allez remplacer.
   4. Pour le **Certificate Name (Nom du certificat)**, recherchez et sélectionnez le certificat que vous avez téléchargé depuis le CA.
   5. Pour le **File Format (format de fichier)**, sélectionnez **Base64 Encoded Certificate (PEM) (Certificat codé en Base64 (PEM))**.



   6. Cliquez sur **OK**.

      Après que l'importation du certificat, vous verrez la nouvelle date d'expiration pour le certificat.

   7. **Commit (Valider)** vos modifications pour pousser le certificat vers le portail ou la passerelle.

©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

Authentification de l’utilisateur GlobalProtect

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l’abonnement Utilisateur mobile

La première fois qu'une application GlobalProtect se connecte au portail, l'utilisateur est invité à s'authentifier sur le portail. Si l'authentification réussit, le portail GlobalProtect envoie la configuration GlobalProtect, qui inclut la liste des passerelles auxquelles l'application peut se connecter, et éventuellement un certificat client pour la connexion aux passerelles. Dès la fin du téléchargement et de la mise en cache de la configuration, l'application tente de se connecter à l'une des passerelles indiquées dans la configuration. Comme ces composants donnent accès à vos ressources et paramètres réseau, ils exigent aussi que l'utilisateur final s'authentifie. Le niveau de sécurité adéquat requis sur le portail et les passerelles varie selon la sensibilité des ressources que la passerelle protège. GlobalProtect fournit un cadre d'authentification flexible qui vous permet de choisir le profil d'authentification et le profil de certificat qui conviennent à chaque composant. GlobalProtect fournit les méthodes d’authentification suivantes :

- **Local Authentication (Authentification locale)** : les informations d’identification du compte utilisateur et les mécanismes d’authentification se trouvent tous localement sur le pare-feu. Ce mécanisme d’authentification n’est pas évolutif parce qu’il exige un compte pour chaque utilisateur final GlobalProtect et est, par conséquent, uniquement recommandé dans les petits déploiements.
- **External Authentication (Authentification externe)** : les fonctions d’authentification de l’utilisateur sont réalisées par les services externes LDAP, Kerberos, TACACS+, SAML ou RADIUS (incluant la prise en charge des mécanismes d’authentification basée sur jeton à deux facteurs tels que l’authentification One-Time Password [mot de passe à usage unique - OTP]). Pour Configurer l’authentification externe vous devez créer un profil de serveur avec des paramètres pour l’accès au service d’authentification externe, créer un profil d’authentification qui fait référence au profil de serveur, et spécifier l’authentification client dans les configurations du portail et de la passerelle. En option, vous pouvez spécifier le système d’exploitation du terminal qui utilisera ces paramètres. Vous pouvez utiliser des profils d'authentification différents pour chaque composant GlobalProtect.
- **Authentification du certificat client** : pour une sécurité renforcée, vous pouvez configurer le portail ou la passerelle pour utiliser un certificat client pour obtenir le nom d’utilisateur et authentifier l’utilisateur avant d’octroyer l’accès au système. GlobalProtect prend également en charge l'authentification par les cartes d'accès communes (CAC) et les cartes à puce, qui reposent sur un profil de certificat. Dans ce cas, le profil de certificat doit contenir le certificat AC racine qui a généré le certificat dans la carte à puce intelligente ou CAC.

- **Authentification à deux facteurs** : avec l'authentification à deux facteurs, le portail ou la passerelle utilise deux mécanismes pour authentifier les utilisateurs, tel qu'un One-Time Password (mot de passe à usage unique - OTP) en plus des informations d'identification de connexion Active Directory (AD). Vous pouvez activer l'authentification à deux facteurs en configurant et en ajoutant à la fois un profil de certificat et un profil d'authentification au portail et/ou à la passerelle. Vous pouvez configurer le portail et les passerelles pour utiliser les mêmes méthodes d'authentification ou des méthodes d'authentification différentes. Peu importe, les utilisateurs doivent réussir à s'authentifier via les deux mécanismes exigés avant d'avoir accès aux ressources du réseau.
- (Windows et macOS uniquement **Authentification multifacteur pour les applications non basées sur un navigateur** : pour les ressources réseaux sensibles non basées sur un navigateur (par exemple, les applications financières ou les applications de développement de logiciels) pouvant nécessiter une authentification supplémentaire, l'application GlobalProtect peut notifier et inviter l'utilisateur à effectuer l'authentification multifacteur opportune et requise pour accéder à ces ressources.
- (Windows et macOS uniquement **Single Sign-On (ouverture de session unique - SSO)** : grâce à l'ouverture de session unique est activée (par défaut), l'application GlobalProtect utilise les informations d'identification de connexion du système d'exploitation de l'utilisateur pour s'authentifier automatiquement et se connecter au portail et à la passerelle GlobalProtect. Vous pouvez également configurer l'application pour qu'elle englober les informations d'identification indépendantes pour veiller à ce que les utilisateurs Windows puissent s'authentifier et se connecter même lorsqu'un fournisseur d'informations d'identification indépendantes est utilisé.

  Le SSO SAML n'est pas pris en charge sur macOS.
- (Prisma Access uniquement) **Moteur d'identité sur le cloud** : le moteur d'identité cloud fournit à la fois l'identification des utilisateurs et l'authentification des utilisateurs pour les utilisateurs mobiles dans le cadre d'un déploiement Prisma Access géré par Panorama, GlobalProtect. L'utilisation du Moteur d'identité sur le cloud pour l'authentification des utilisateurs et le mappage des noms d'utilisateur aux groupes d'utilisateurs vous permet de rédiger des politiques de sécurité basées sur les utilisateurs et les groupes, et non sur les adresses IP, et contribue à sécuriser vos actifs en appliquant des mesures de sécurité basées sur le comportement. En synchronisant en permanence les informations de vos répertoires, le moteur d'identité sur le cloud garantit l'exactitude et la mise à jour de vos informations utilisateur, ainsi que l'application continue des politiques basées sur les mappages, même si le fournisseur d'identité SAML (IdP) est temporairement indisponible. Les utilisateurs de Prisma Access doivent exécuter l'application GlobalProtect 6.0 ou une version ultérieure avec une version d'innovation Prisma Access 3.0 ou ultérieure.

  Le moteur d'identité sur le cloud prend en charge les méthodes d'authentification suivantes pour GlobalProtect :

  - SAML
  - Certificat client
  - OIDC (À partir des versions de l'application GlobalProtect 6.2.6 et ultérieures et 6.3.2 et ultérieures)

 ©2026 Palo Alto Networks, Inc.

Comment l'application sait-elle quelles sont les informations d'identification elle doit fournir ?

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Par défaut, l'application GlobalProtect tente d'utiliser les mêmes identifiants de connexion pour la passerelle que ceux utilisés pour la connexion au portail. Dans le cas le plus simple, où la passerelle et le portail utilisent les mêmes profils d'authentification ou profil de certificat, l'application se connecte à la passerelle de façon transparente.

Sur une base de configuration par application, vous pouvez également personnaliser les portails GlobalProtect et les passerelles - internes, externes ou manuelles - qui nécessitent des informations d'identification différentes (telles que les MPUU). Cela permet au portail GlobalProtect ou à la passerelle de demander le MPUU sans demander d'abord les informations d'identification spécifiées dans le profil d'authentification.

Vous pouvez modifier le comportement d'authentification par défaut de l'application soit en configurant les paramètres d'authentification par cookie, soit avec une authentification à deux facteurs afin que l'authentification soit à la fois plus forte et plus rapide :

Authentification par cookie sur le portail ou la passerelle

L'authentification par cookie simplifie le processus d'authentification pour les utilisateurs finaux parce qu'ils n'auront plus besoin de se connecter au portail ainsi qu'à la passerelle successivement ou de saisir plusieurs mots de passe à usage unique pour l'authentification sur chacun. Cela améliore l'expérience utilisateur en minimisant le nombre de fois que les utilisateurs doivent entrer des informations d'identification. En outre, les cookies permettent l'utilisation d'un mot de passe temporaire pour réactiver l'accès VPN après l'expiration du mot de passe de l'utilisateur.

Vous pouvez configurer les paramètres d'authentification par cookie indépendamment pour le portail et pour les passerelles individuelles (par exemple, vous pouvez imposer une durée de vie de cookie plus courte sur les passerelles qui protègent les ressources sensibles). Une fois que le portail ou les passerelles déploient un cookie d'authentification au point de terminaison, le portail et les passerelles reposent tous deux sur le même cookie pour authentifier l'utilisateur. Lorsque l'application présente le cookie, le portail ou la passerelle évalue si le cookie est valide en fonction de la durée de vie configurée du cookie. Si le cookie expire, GlobalProtect invite automatiquement l'utilisateur à s'authentifier auprès du portail ou de la passerelle. Lorsque l'authentification réussit, le portail ou la passerelle émet le cookie d'authentification de remplacement au point de terminaison et la période de validité recommence.

Considérez l'exemple suivant dans lequel vous configurez la durée de vie des cookies pour le portail, qui ne protège pas d'informations sensibles (15 jours), mais configurez la durée de vie des cookies pour les passerelles, qui protègent les informations sensibles, à 24 heures. Lorsque l'utilisateur s'authentifie d'abord avec le portail, le portail émet le cookie d'authentification. Si

 ©2026 Palo Alto Networks, Inc.

l’utilisateur tentait de se connecter au portail après cinq jours, le cookie d’authentification serait toujours valide. Cependant, si l’utilisateur tentait de se connecter à la passerelle après cinq jours, celle-ci évaluerait la durée de vie du cookie et déterminerait qu’il a expiré (5 jours > 24 heures). L'agent invitera alors automatiquement l'utilisateur à s'authentifier auprès de la passerelle et, si l'authentification est réussie, recevra un cookie d'authentification de remplacement. Le nouveau cookie d'authentification serait alors valable pour 15 autres jours sur le portail et encore 24 heures sur les passerelles.

Pour obtenir un exemple d'utilisation de cette option, consultez la section Configuration d'une authentification à deux facteurs.

Transfert d’informations d’identification vers certaines ou toutes les passerelles

Avec l’authentification à deux facteurs, vous pouvez spécifier le portail et les types de passerelles (internes, externes ou manuelles uniquement) qui demandent leur propre ensemble d’informations d’identification. Cette option accélère le processus d’authentification lorsque le portail et la passerelle exigent des informations d’identification différentes (soit des mots de passe à usage unique différents soit des informations d’identification d’ouverture de session différentes, entièrement). Pour chaque portail ou passerelle que vous sélectionnez, l’application ne transmet pas les informations d’identification, vous permettant de personnaliser la sécurité des différents composants GlobalProtect. Par exemple, vous pouvez avoir la même sécurité sur vos portails et passerelles internes, tout en exigeant un second facteur de MPUU ou un mot de passe différent pour l’accès à ces passerelles qui fournissent l’accès à vos ressources les plus sensibles.

Pour obtenir un exemple d'utilisation de cette option, consultez la section Configuration d'une authentification à deux facteurs.

 ©2026 Palo Alto Networks, Inc.

Comment l'application sait-elle quel certificat elle doit fournir ?

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Lorsque vous configurez GlobalProtect pour utiliser des certificats clients pour l'authentification sur des terminaux macOS ou Windows, GlobalProtect doit présenter un certificat client valide pour s'authentifier auprès du portail et des passerelles.

Pour qu'un certificat client soit valide, il doit répondre aux exigences suivantes :

- Le certificat est émis par l'autorité de certification (CA) que vous avez définie dans le profil de certificat de vos configurations de portail et de passerelles.
- Le certificat spécifie l'objectif d'authentification du client, que l'administrateur du certificat spécifie lors de la création du certificat.
- Le certificat est situé dans le magasin de certificats tel que configuré dans la configuration de l'agent de portail GlobalProtect. Par défaut, l'application GlobalProtect cherche d'abord un certificat valide dans le magasin d'utilisateur. Si aucun n'existe, l'application cherche alors dans le magasin de la machine. Si l'application GlobalProtect localise un certificat dans le magasin de l'utilisateur, il ne regarde pas dans le magasin de la machine, car le magasin de l'utilisateur est prioritaire. Pour forcer l'application GlobalProtect à rechercher des certificats dans un seul magasin de certificats, configurez l'option **Client Certificate Store Lookup (Recherche dans le magasin de certificats clients)** dans la configuration de l'agent de portail GlobalProtect appropriée.
- Le certificat correspond à tout objectif supplémentaire spécifié dans la configuration de l'agent de portail GlobalProtect. Pour spécifier un objectif supplémentaire, vous devez identifier l'identificateur d'objet (OID) du certificat et configurer la valeur **Extended Key Usage OID (OID d'utilisation de clé étendue)** dans la configuration de l'agent de portail GlobalProtect appropriée. Un OID est une valeur numérique qui identifie l'application ou le service pour lequel utiliser un certificat et qui est automatiquement attaché à un certificat lorsqu'il est créé par une autorité de certification (CA). Pour plus d'informations sur la spécification d'un OID commun ou personnalisé, consultez Activer la sélection des certificats en fonction de l'OID.

Lorsqu'un seul certificat client répond aux exigences ci-dessus, l'application sélectionne automatiquement ce certificat client pour l'authentification. Toutefois, lorsque plusieurs certificats clients répondent à ces exigences, GlobalProtect invite l'utilisateur à sélectionner le certificat client à partir d'une liste de certificats clients valides sur le terminal. Bien que GlobalProtect exige que les utilisateurs sélectionnent le certificat client uniquement lors de leur première connexion, les utilisateurs peuvent ne pas savoir quel certificat sélectionner. Dans ce cas, nous vous recommandons de restreindre la liste des certificats clients disponibles en fonction de l'objectif du certificat (tel qu'indiqué par l'OID) et du magasin de certificats. Pour plus d'informations sur

 ©2026 Palo Alto Networks, Inc.

ces paramètres et d'autres paramètres que vous pouvez configurer pour personnaliser votre application, voir la section Personnaliser l'agent GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Configurer l'authentification externe

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Les flux de travail suivants décrivent comment configurer le portail GlobalProtect et les passerelles pour utiliser un service d'authentification externe. Les services d'authentification pris en charge comprennent LDAP, Kerberos, RADIUS, SAML et TACACS +.

> *GlobalProtect prend aussi en charge l'authentification locale. Pour utiliser l'authentification locale, créez une base de données utilisateur locale (**Device (Périphérique)** > **Local User Database (base locale de données utilisateur)**) qui contient les utilisateurs et les groupes auxquels vous souhaitez autoriser l'accès GlobalProtect, puis reportez-vous à cette base de données dans le profil d'authentification.*

Reportez-vous aux sections ci-dessous pour plus d'informations :

- Configurer l'authentification LDAP
- Configurer l'authentification SAML
- Configurer l'authentification Kerberos
- Configurer l'authentification RADIUS ou TACACS+

Configurer l'authentification LDAP

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect

Les organisations utilisent souvent LDAP comme service d'authentification et référentiel central pour les informations d'utilisateur. Elles peuvent également utilisées LDAP pour stocker les informations de rôle pour les utilisateurs de l'application.

 ©2026 Palo Alto Networks, Inc.

1. Créez un profil de serveur.

Le profil de serveur identifie le service d'authentification externe et indique au pare-feu comment se connecter à ce service d'authentification et accéder aux informations d'authentification pour vos utilisateurs.

Lorsque vous utilisez LDAP pour vous connecter à Active Directory (AD), vous devez créer un profil de serveur LDAP distinct pour chaque domaine AD.

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Server Profiles (Profils serveur)** > **LDAP**, puis **Add (Ajouter)** un profil de serveur LDAP.
   - Sur Strata Cloud Manager, suivez les étapes ci-dessous :
     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma AccessGlobalProtect** > **GlobalProtect**.
     2. Sélectionnez **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Server Profiles (Profils de serveur)** > **LDAP**.
2. Saisissez un **Profile Name (Nom de profil)**, par exemple **`GP-User-Auth`**.
3. S'il s'agit du profil d'un pare-feu pouvant prendre en charge de multiples systèmes virtuels, sélectionnez un système virtuel ou sélectionnez l'option **Shared (Partagé)** en tant que **Location (Emplacement)** où le profil est disponible.
4. Cliquez sur **Add (Ajouter)** dans la zone **Server List (Liste de serveurs)**, puis fournissez les informations nécessaires pour vous connecter au service d'authentification, notamment le **Name (Nom)**, l'adresse IP ou le FQDN du **LDAP Server (Serveur LDAP)** et le **Port**.
5. Sélectionnez le **Type** de serveur LDAP.
6. Saisissez le **Bind DN (DN de liaison)** et le **Password (Mot de passe)** pour activer le service d'authentification permettant d'authentifier le pare-feu.
7. (Facultatif) Si vous souhaitez que le point de terminaison utilise le protocole SSL ou TLS pour une connexion plus sécurisée au serveur d'annuaires, activez l'option **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)** (activée par défaut). Le protocole utilisé par le point de terminaison varie selon le Port de serveur :
   - 389 (par défaut) : TLS (le périphérique utilise plus précisément l'opération StartTLS, qui met à niveau la connexion en texte brut initiale en TLS).
   - 636 : SSL.
   - Tout autre port : le périphérique tente tout d'abord d'utiliser TLS. Si le serveur d'annuaires ne prend pas en charge TLS, le périphérique fera appel à SSL.
8. (Facultatif) Pour une sécurité supplémentaire, activez l'option **Verify Server Certificate for SSL sessions (Vérifier le certificat du serveur pour les sessions SSL)** afin que le point de terminaison vérifie le certificat que le serveur d'annuaire présente pour les connexions SSL/TLS. Pour activer la vérification, vous devez également activer l'option visant à **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**. Pour une vérification réussie, le certificat doit remplir l'une des conditions suivantes :
   - Il se trouve dans la liste des certificats de périphérique : **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device**

 ©2026 Palo Alto Networks, Inc.

Certificates (Certificats de périphérique) Si nécessaire, importez le certificat dans le périphérique.

- Le signataire du certificat figure dans la liste des autorités de certification de confiance : **Device (Périphérique)** > **Certificate Management (Gestion de Certificats)** > **Certificates (Certificats)** > **Default Trusted Certificate Authorities (Autorités de certificats fiables par défaut)**.

9. Cliquez sur **OK** pour enregistrer le profil de serveur.

2. (Facultatif) Créez un profil d'authentification.

Le profil d'authentification spécifie le profil du serveur pour le portail ou les passerelles à utiliser lorsqu'ils authentifient les utilisateurs. Sur un portail ou une passerelle, vous pouvez attribuer un ou plusieurs profils d'authentification dans un ou plusieurs profils d'authentification client. Pour obtenir une description de la façon dont un profil d'authentification dans un profil d'authentification client prend en charge l'authentification utilisateur granulaire, voir Configurer une passerelle GlobalProtect et Paramétrer l'accès au portail GlobalProtect.

Pour permettre aux utilisateurs de se connecter et de modifier leur mot de passe expiré sans l'intervention d'un administrateur, songez à utiliser un VPN d'accès distant avec pré-connexion.

*Si le mot de passe d'un utilisateur expire, vous pouvez affecter un mot de passe LDAP temporaire afin de lui permettre de se connecter à GlobalProtect. Dans ce cas, le mot de passe temporaire peut être utilisé pour l'authentification sur le portail, mais la connexion à la passerelle peut échouer car le même mot de passe temporaire ne peut pas être réutilisé. Pour éviter ce problème, configurez une substitution d'authentification dans la configuration du portail (**Network (Réseau)** > **GlobalProtect** > **Portal (Portail)**) pour permettre à l'application GlobalProtect app d'utiliser un cookie pour s'authentifier sur le portail et le mot de passe temporaire pour authentifier la passerelle.*

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis **Add (Ajoutez)** un nouveau profil.
2. Saisissez un **Name (Nom)** pour le profil.
3. Définissez le **Authentication Type (Type d'authentification)** sur **LDAP**.
4. Sélectionnez le **Server Profile (Profil de serveur)** de l'authentification LDAP que vous avez créé à l'étape 1.
5. Saisissez **sAMAccountName** comme **Login Attribute (Attribut de connexion)**.
6. Définissez le **Password Expiry Warning (Avertissement d'expiration du mot de passe)** pour indiquer le nombre de jours avant l'expiration du mot de passe auquel les utilisateurs sont informés. Par défaut, les utilisateurs sont avisés sept jours avant l'expiration du mot de passe (la plage est de 1 à 255). Étant donné que les utilisateurs doivent modifier leur mot de passe avant la fin de la période d'expiration, vous devez indiquer une période de notification appropriée pour vos utilisateurs pour garantir un accès permanent à GlobalProtect. Pour utiliser cette fonctionnalité, vous devez spécifier l'un des types de serveurs LDAP suivants dans votre profil de serveur LDAP :**active-directory**, **e-directory** ou **sun**.

   À moins que vous n'activiez la préouverture de session, les utilisateurs ne peuvent accéder à GlobalProtect lorsque leur mot de passe est expiré.

 ©2026 Palo Alto Networks, Inc.

7. Spécifiez le **User Domain (Domaine d'utilisateur)** et le **Username Modifier (Modificateur d'utilisateur)**. Le terminal combine les valeurs **User Domain (Domaine utilisateur)** et **Username Modifier (Modificateur du nom d'utilisateur)** pour modifier la chaîne domaine et nom d'utilisateur qu'un utilisateur saisit lors de la connexion. Le point de terminaison utilise la chaîne modifiée pour l'authentification et la valeur **User Domain (Domaine utilisateur)** pour le mappage de groupe User-ID. Il s'avère utile de modifier la saisie utilisateur lorsque le service d'authentification demande que la chaîne domaine/nom d'utilisateur soit indiquée dans un format spécifique ; vous ne voulez toutefois pas que les utilisateurs aient à saisir correctement le domaine. Vous devez faire une sélection parmi les options suivantes :

   - Pour envoyer uniquement l'entrée non modifiée de l'utilisateur, laissez vide le **domaine utilisateur** (par défaut) et définissez le **Modificateur d'utilisateur** à la variable **% USERINPUT%** (la valeur par défaut).
   - Pour ajouter initialement un domaine sur la saisie utilisateur, saisissez un **User Domain (Domaine utilisateur)** et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** sur **%USERDOMAIN%\%USERINPUT% (%DOMAINEUTILISATEUR%\%SAISIEUTILISATEUR%)**.
   - Pour ajouter un domaine sur la saisie utilisateur, saisissez un **User Domain (Domaine utilisateur)** et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** sur **%USERINPUT%@%USERDOMAIN% (%SAISIEUTILISATEUR%@ %DOMAINEUTILISATEUR%)**.

     *Si le **Username Modifier (Modificateur du nom d'utilisateur)** inclut la variable **%USERDOMAIN% (%DOMAINEUTILISATEUR%)**, la valeur **User Domain (Domaine utilisateur)** remplace toute chaîne de domaine saisie par l'utilisateur. Si le **User Domain (Domaine utilisateur)** est vide, le périphérique supprime toute chaîne de domaine saisie par l'utilisateur.*

8. À l'onglet **Advanced (Avancé)**, **Add (Ajoutez)** une **Allow List (Liste d'autorisation)** pour sélectionner les utilisateurs et les groupes d'utilisateurs à authentifier au moyen de ce profil. L'option **all (tous)** permet à tous les utilisateurs de s'authentifier à l'aide de ce profil. Par défaut, la liste est vide, ce qui signifie qu'aucun utilisateur ne peut s'authentifier.
9. Cliquez sur **OK**.

3. Commit (Validez) la configuration.

   Cliquez sur **Commit (Valider)**.

Configurer l'authentification SAML

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

Le langage SAML (Security Assertion Markup Language) est un format de données à norme ouverte basé sur XML utilisé pour l'échange de données d'authentification et d'autorisation entre des parties, en particulier entre un fournisseur d'identité (IdP) et un fournisseur de services. SAML est un produit du comité technique des services de sécurité OASIS.

(Terminaux Windows uniquement ; nécessite l'application GlobalProtect 6.3.3 et ultérieure ; pris en charge uniquement sur le navigateur intégré GlobalProtect)À partir de la version 6.3.3 de GlobalProtect, vous pouvez imposer que l'authentification SAML réussisse uniquement si la demande d'autorisation provient d'adresses IP de confiance. Les utilisateurs qui s'authentifient via des adresses IP non approuvées à partir de dispositifs non gérés n'ont pas accès aux applications et autres ressources. Pour que cela fonctionne, vous pouvez spécifier soit un serveur proxy, soit un fichier de configuration automatique de proxy (PAC) via le paramètre de pré-déploiement SAMLAUTHPROXY. Pour plus d'informations sur les paramètres, reportez-vous à Options de comportement de l'application.

1. Créez un profil de serveur.

   Le profil de serveur identifie le service d'authentification externe et indique au pare-feu comment se connecter à ce service d'authentification et accéder aux informations d'authentification pour vos utilisateurs.

   Les étapes suivantes décrivent la manière d'importer un fichier de métadonnées SAML de l'IdP, pour que le pare-feu puisse automatiquement créer un profil de serveur et renseigner les informations de connexion, d'enregistrement et de certificat IdP. Si l'IdP de fournit pas de fichier de métadonnées, sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de**

 ©2026 Palo Alto Networks, Inc.

serveur) > **SAML Identity Provider (Fournisseur d'identité SAML)**, puis **Add (Ajoutez)** un profil de serveur manuellement.

1. Exportez le fichier de métadonnées SAML de l'IdP vers un point de terminaison auquel le pare-feu peut accéder.

   Consultez votre documentation sur l'IdP pour connaître les instructions sur la manière d'exporter un fichier.
2. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)**, puis **Add (Ajouter)** un profil de serveur LDAP.
   - Sur Strata Cloud Manager, suivez les étapes ci-dessous :
     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma AccessGlobalProtect** > **GlobalProtect**.
     2. Sélectionnez **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Server Profiles (Profils de serveur)** > **LDAP**.
3. **Import (Importez)** le fichier de métadonnées sur le pare-feu.
4. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur, par exemple **`GP-User-Auth`**.
5. **Browse (Accédez)** au fichier de métadonnées.
6. Sélectionnez **Validate Identity Provider Certificate (Valider le certificat du fournisseur d'identité)** (par défaut) pour que le pare-feu valide le certificat IdP.

   La validation se produit uniquement après avoir affecté le profil de serveur à un profil d'authentification et après **Commit (Validé)** les changements. Le pare-feu utilise le profil de certificat qui se trouve dans le profil d'authentification pour valider le certificat.
7. Saisissez le **Maximum Clock Skew (Décalage d'horloge maximum)**, c'est-à-dire l'écart (en secondes) permis entre l'heure système de l'IdP et du pare-feu au moment où le pare-feu valide les messages IdP. La valeur par défaut est 60 secondes, et la plage est comprise entre 1 et 900 secondes. Si l'écart est supérieur à cette valeur, l'authentification échoue.
8. Cliquez sur **OK** pour enregistrer le profil de serveur.

2. (Facultatif) Créez un profil d'authentification.

Le profil d'authentification spécifie le profil du serveur pour le portail ou les passerelles à utiliser lorsqu'ils authentifient les utilisateurs. Sur un portail ou une passerelle, vous pouvez attribuer un ou plusieurs profils d'authentification dans un ou plusieurs profils d'authentification client. Pour obtenir de plus amples renseignements sur la façon dont un profil d'authentification dans un profil d'authentification client prend en charge

 ©2026 Palo Alto Networks, Inc.

l'authentification utilisateur granulaire, voir les sections Configurer une passerelle GlobalProtect et Paramétrer l'accès au portail GlobalProtect.

L'authentification SAML prend en charge le VPN d'accès à distance avec pré-ouverture de session *avec les versions 5.0 ou ultérieures de l'application GlobalProtect.*

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis **Add (Ajouter)** un nouveau profil d'authentification.
   - Sur Strata Cloud Manager, suivez les étapes ci-dessous :
     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma AccessGlobalProtect** > **GlobalProtect**.
     2. Sélectionnez **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Authentication Profiles (Profils d'authentification)** puis **Add (Ajouter)** un nouveau profil d'authentification.
2. Donnez un **Name (Nom)** au profil d'authentification.
3. Définissez le **AuthenticationType (Type d'authentification)** sur **SAML**.
4. Sélectionnez le **IdP Server Profile (Profil de serveur IdP)** SAML que vous avez créé à l'étape 1.
5. Configurez les options suivantes pour activer l'authentification de certificat entre le pare-feu et le fournisseur d'identité SAML.
   - Le **Certificate for Signing Requests (Certificat de demande de signature)** que le pare-feu utilise pour signer les messages qu'il envoie à l'IdP.
   - Le **Certificate Profile (Profil de certificat)** que le pare-feu utilise pour valider le certificat IdP.
6. Indiquez le nom d'utilisateur et les formats de rôle d'administrateur.
   - Spécifiez le **Username Attribute (Attribut du nom d'utilisateur)** et un **User Group Attribute (Attribut du groupe d'utilisateurs)**.

     Contrairement aux autres types d'authentification externes, le profil d'authentification SAML ne possède aucun attribut de ***User Domain (Domaine d'utilisateur)****.*
   - (Facultatif) Si vous prévoyez d'utiliser ce profil pour authentifier les comptes administratifs que vous gérez dans le magasin d'identités de l'IdP, indiquez l'**Admin Role Attribute (Attribut de rôle d'administrateur)** et l'**Access Domain Attribute (Attribut de domaine d'accès)**.
7. À l'onglet **Advanced (Avancé)**, **Add (Ajoutez)** une **Allow List (Liste d'autorisation)** pour sélectionner les utilisateurs et les groupes qui sont autorisés à s'authentifier au moyen de ce profil. L'option **all (tous)** permet à tous les utilisateurs de s'authentifier à l'aide de ce profil. Par défaut, la liste est vide, ce qui signifie qu'aucun utilisateur ne peut s'authentifier.

   Assurez-vous que le nom d'utilisateur qui figure dans la **Allow List (Liste d'autorisations)** correspond au nom d'utilisateur renvoyé par le serveur de l'IdP SAML.
8. Cliquez sur **OK**.

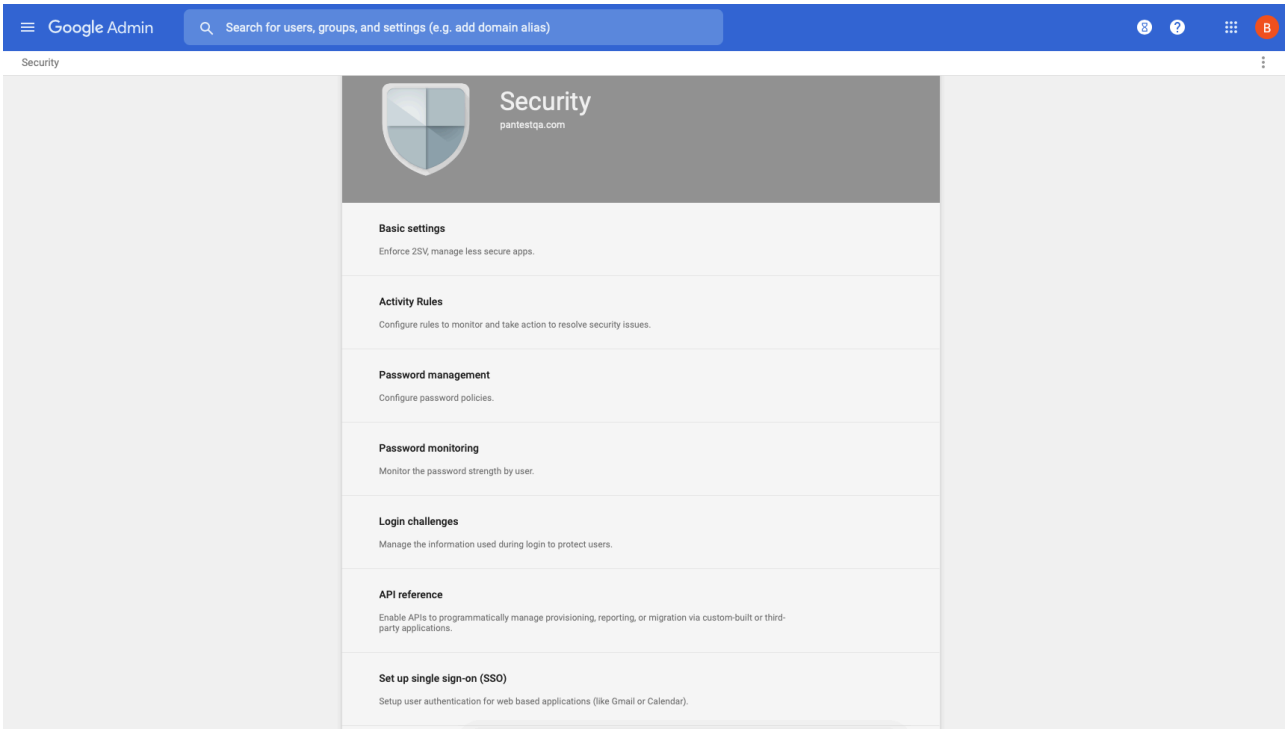
 ©2026 Palo Alto Networks, Inc.

3. **Commit (Validez)** la configuration.

4. (Chromebook uniquement) Activez le SSO SAML pour les Chromebooks.

Ces étapes vous permettent de configurer le SSO SAML pour l'application GlobalProtect pour Android sur Chromebook.

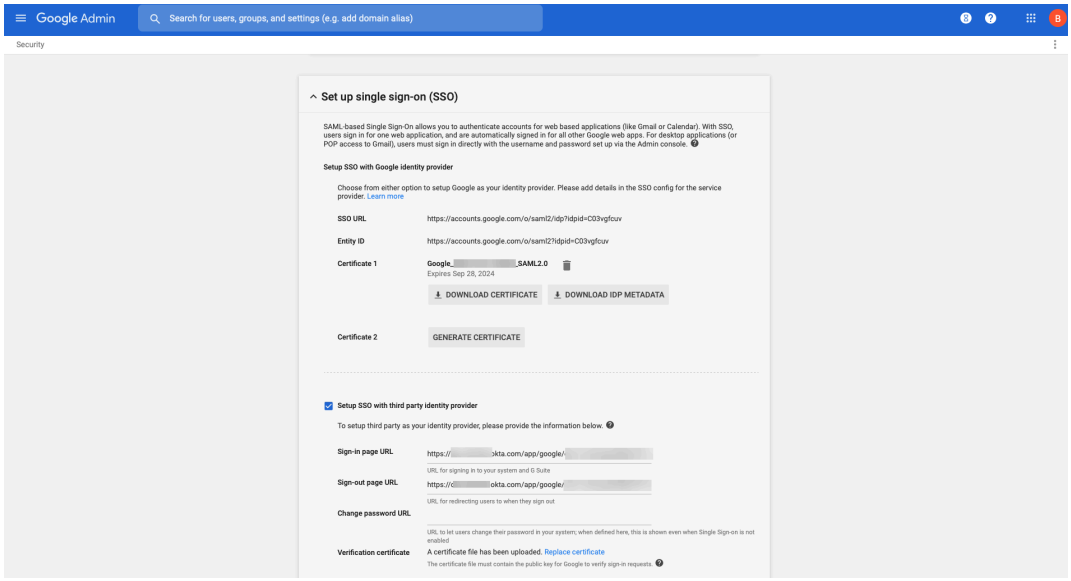
1. Connectez-vous à la console Google Admin, puis sélectionnez **Sécurité**.



2. Sélectionnez **Configurer l'ouverture de session unique SSO**.
3. (Facultatif) Si vous souhaitez établir l'ouverture de session unique auprès d'un fournisseur autre que Google, sélectionnez **Setup SSO with third party identity provider (Configurer l'ouverture de session unique SSO auprès d'un fournisseur d'identité tiers)**, puis spécifiez la **Page d'URL de connexion (Sign-in page URL)** et la **Sign-out page**

 ©2026 Palo Alto Networks, Inc.

URL (Page d'URL de déconnexion) et chargez un **Verification certificate (Certificat de vérification)** valide.



4. Configurez le fournisseur d'identité SAML dans GlobalProtect.
   1. Choisissez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)**.
      - Sur Strata Cloud Manager, suivez les étapes ci-dessous :
        1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma AccessGlobalProtect** > **GlobalProtect**.
        2. Sélectionnez **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Server Profiles (Profils de serveur)** > **LDAP**.
   2. Faites correspondre les valeurs que vous avez saisies pour l'IdP dans la console Google Admin.

Authentification SAML pour les portails GlobalProtect sur des ports non standards

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager)	Licence d'abonnement GlobalProtect PAN-OS 11.2.9 ou versions ultérieures

GlobalProtect prend en charge l'authentification SAML lorsque le portail est accessible de l'extérieur sur un port non standard (c'est-à-dire un port autre que celui par défaut : TCP/443). Cela permet à GlobalProtect d'utiliser l'authentification SAML sur des ports personnalisés et offre des options de déploiement plus flexibles dans les réseaux qui nécessitent que les services fonctionnent sur des ports spécifiques et non standards.

En tant que meilleure pratique, configurez vos applications pour utiliser des ports en dehors des plages bien connues et enregistrées.

 ©2026 Palo Alto Networks, Inc.

Vous devez configurer un port personnalisé sur l'IdP pour que GlobalProtect prenne en charge l'authentification SAML lors de l'accès via un port non standard. Vous devez également configurer le même port personnalisé sur le pare-feu. La configuration du pare-feu et les paramètres de l'IdP doivent être synchronisés. Le numéro de port que vous configurez pour le portail GlobalProtect sur le pare-feu doit être identique à celui que vous utilisez dans l'URL (ACS) sur l'IdP.

Mettre à jour la configuration du fournisseur d'identité (IdP) avec un port personnalisé

1. Connectez-vous au tableau de bord administratif de votre fournisseur d'identité.
2. Modifiez l'URL pour inclure le nom d'hôte (ou l'adresse IP) de votre portail et le numéro de port personnalisé, non 443. L'URL doit utiliser le format suivant :

   https://<portal-ip>:<saml-port>/SAML20/SP

   - <*portal-hostname*> : Remplacez par le FQDN de votre portail GlobalProtect.
   - <*custom-port*> : Remplacez par le port TCP que vous avez configuré pour le portail.

Télécharger la configuration depuis le fournisseur d'identité (IdP)

Vous devez télécharger les configurations depuis l'IdP. Cliquez sur le lien de téléchargement en regard de **Federation Metadata XML (Métadonnées XML de la Fédération)** pour télécharger le fichier de métadonnées SAML depuis l'IdP vers un système client à partir duquel vous pouvez télécharger les métadonnées vers le pare-feu.

Importer les configurations dans le pare-feu

Après avoir téléchargé la configuration depuis l'IdP, vous devez ajouter un profil de serveur IdP SAML et télécharger la configuration vers le pare-feu.

1. Sélectionnez Périphérique > Profils de serveur > Fournisseur d'identité SAML.
2. Saisissez un Nom de profil pour identifier le profil de serveur.
3. Accédez au fichier de métadonnées du fournisseur d'identité et importez le fichier de métadonnées sur le pare-feu.
4. Sélectionnez Valider le certificat du fournisseur d'identité (par défaut).
5. Saisissez le Décalage d'horloge maximum, c'est-à-dire l'écart en secondes permis entre l'heure système de l'IdP et du pare-feu au moment où le pare-feu valide les messages IdP (par défaut : 60 ; plage comprise entre 1 et 900). Si l'écart est supérieur à cette valeur, l'authentification échoue.
6. Cliquez sur OK pour enregistrer le profil de serveur.

Configurez le port personnalisé sur le pare-feu

Configurez le même port SAML personnalisé sur le pare-feu que celui que vous avez défini sur l'IdP en utilisant la commande CLI `set global-protect saml-custom-port <1-65535>`. Sinon, GlobalProtect utilisera le port par défaut 443.

 ©2026 Palo Alto Networks, Inc.

Le port TCP personnalisé configuré pour le portail GlobalProtect sur le pare-feu doit correspondre exactement au port utilisé dans les paramètres SAML de votre fournisseur d'identité.

Commande CLI	Description
set global-protect saml-custom-port <1-65535>	Configure le port personnalisé sur le pare-feu. Cela doit être le même port que celui que vous avez défini sur l'IdP.
show gp-broker panos-config	Pour vérifier que le port personnalisé est défini dans gp-broker, vous pouvez vérifier la clé « saml_custom_port » dans panos-config.

Configurer la règle de traductions NAT

Vous devez configurer les règles de traduction NAT sur le pare-feu pour traduire le port de destination en 443.

1. Sur le pare-feu, cliquez sur **Policies > (Politiques >)** > **NAT** et ajoutez un nouveau service avec le port personnalisé pour l'inclure dans la règle NAT.
2. Créez un nouveau service avec le port personnalisé à inclure dans la règle NAT.
3. Dans l'onglet Paquet traduit, sélectionnez l'IP du portail GlobalProtect dans Adresse traduite et entrez 443 dans Port traduit.

Configurer la politique de sécurité

Vous devez configurer une règle de politique de sécurité pour le trafic. Pour plus d'informations, voir Créer une règle de politique de sécurité.

À propos du navigateur intégré pour l'authentification SAML

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

À partir des versions 6.0.9 et ultérieures, 6.2.3 et ultérieures, et 6.3 et ultérieures de l'application GlobalProtect, le framework du navigateur intégré pour l'authentification SAML a été mis à niveau vers Microsoft Edge WebView2 (Windows) et WKWebView (macOS). Cela offre une expérience cohérente entre le navigateur intégré et le client GlobalProtect. Par défaut, les locataires utilisant l'authentification SAML sont configurés pour utiliser WebView2 intégré (Windows) ou WKWebView (macOS) au lieu de s'appuyer sur le navigateur par défaut du système. Grâce à cette amélioration, les utilisateurs finaux n'ont plus besoin de configurer une page d'accueil

 ©2026 Palo Alto Networks, Inc.

SAML, ce qui retire la nécessité de fermer manuellement le navigateur. Cela simplifie le processus d'authentification.

(Terminaux Windows uniquement) Dans un environnement joint à Microsoft Entra avec SSO activé, les utilisateurs ne sont pas tenus de saisir leurs identifiants pour s'authentifier à Prisma Access via GlobalProtect. Cette expérience fluide est vraie que l'utilisateur se connecte à son environnement pour la première fois ou pour la énième fois. Si une erreur survient lors de l'authentification, elle s'affiche dans le navigateur intégré. Ce processus d'authentification fonctionne sur tous les états du périphérique. Dans un environnement non joint à Entra avec SSO activé, les utilisateurs doivent saisir leurs identifiants lors de la première connexion. Lors des connexions suivantes, les identifiants sont remplis automatiquement tant que la session du fournisseur d'identité SAML (IdP) est active et n'a pas expiré.

Gérer la sélection du navigateur pour l'authentification SAML

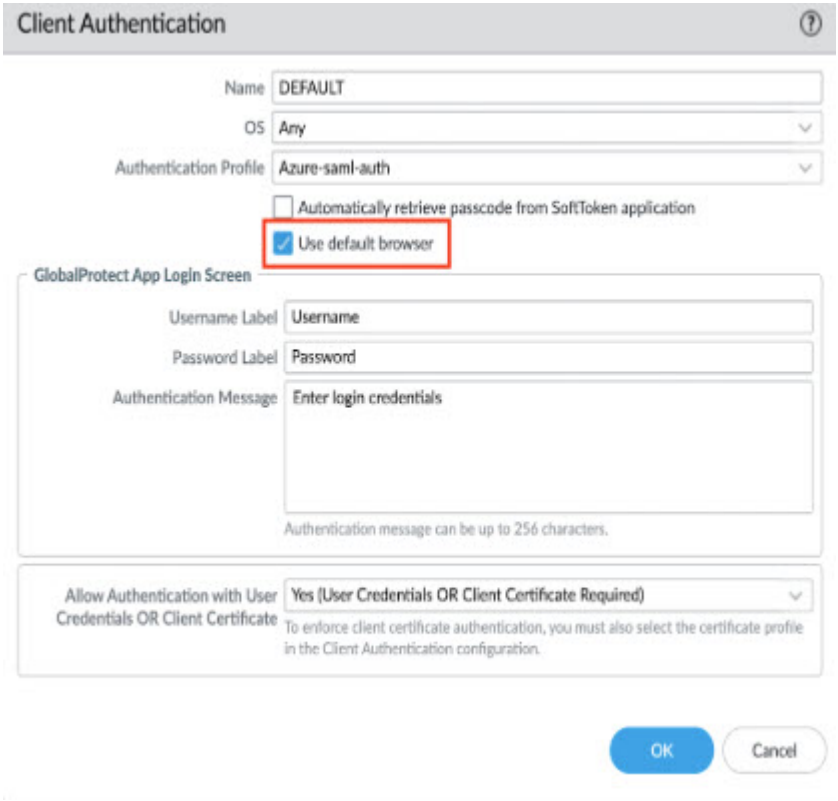
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	PAN-OS 11.1.0 et versions ultérieures Pour les versions antérieures de PAN-OS, utilisez la clé de registre/plist de pré-déploiement GlobalProtect 6.0.x, 6.1.x, 6.2.x ou 6.3.x Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

À partir de la version 11.1.0 de PAN-OS, la sélection du navigateur pour l'authentification SAML est définie dans la configuration d'authentification client GlobalProtect. Ce paramètre contrôle si l'application GlobalProtect utilise le navigateur par défaut du périphérique ou le navigateur intégré de GlobalProtect pour l'authentification SAML ou CAS au portail. Le nouveau paramètre a la priorité sur le paramètre de configuration de l'agent désormais obsolète

Pour spécifier le navigateur, suivez les étapes ci-dessous :

 ©2026 Palo Alto Networks, Inc.

- Sur Panorama :
  1. Accédez à **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<portal-config>** > **Authentication (Authentification)** > **<client-authentication-config>**

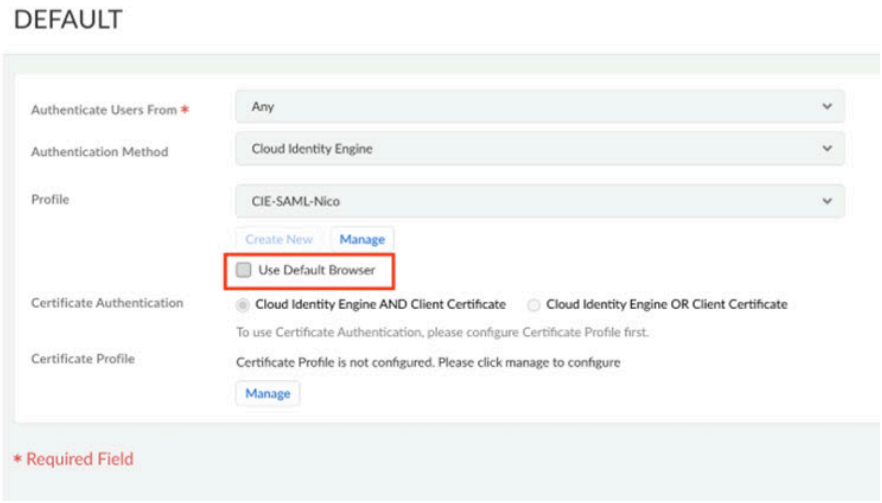


  2. Sélectionnez l'option **Use Default Browser (Utiliser le navigateur par défaut)** pour utiliser le navigateur par défaut pour l'authentification SAML ou CAS. Laissez la case décochée pour utiliser le navigateur intégré.
  3. Validez et appliquez vos mises à jour.

 ©2026 Palo Alto Networks, Inc.

- L'option **Use Default Browser (Utiliser le navigateur par défaut)** est masquée sous un indicateur de fonctionnalité dans les environnements Strata Cloud Manager. Contactez votre représentant du support client pour l'activer. Ensuite, suivez les étapes ci-dessous.

  1. Accédez à **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope GlobalProtect (Portée de configuration GlobalProtect)** > **Infrastructure** > **Add Authentication (Ajouter une authentification)**
  2. Sélectionnez l'option **Use Default Browser (Utiliser le navigateur par défaut)** pour utiliser le navigateur par défaut pour l'authentification SAML ou CAS. Laissez la case décochée pour utiliser le navigateur intégré.

  3. Validez et appliquez vos mises à jour.

Logique de comportement après mise à niveau

Lorsque vous mettez à niveau d'une version antérieure de PAN-OS vers 11.1.0 ou version ultérieure, le système effectue une vérification de toutes les configurations d'agent GlobalProtect existantes :

- Si une ou plusieurs configurations d'agent de portail avaient l'option obsolète **Use Default Browser for SAML Authentication (Utiliser le navigateur par défaut pour l'authentification SAML)** activée, la nouvelle option **Use Default Browser (Utiliser le navigateur par défaut)** est automatiquement sélectionnée après la mise à niveau. Cela vaut aussi bien pour les environnements Panorama que Strata Cloud Manager.
- Si toutes les configurations d'agent de portail avaient le paramètre **Use Default Browser for SAML Authentication (Utiliser le navigateur par défaut pour l'authentification SAML)** désactivé, l'option **Use Default Browser (Utiliser le navigateur par défaut)** est décochée pour toutes les configurations d'authentification client après la mise à niveau.

Exemple de scénario de mise à niveau 1 (le navigateur par défaut est activé)

Ce scénario montre le résultat d'une configuration mixte après migration.

 ©2026 Palo Alto Networks, Inc.

Version PAN-OS 11.0.x ou antérieure	Après la mise à niveau vers la version PAN-OS 11.1.x et ultérieure
La configuration du portail (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > **Agent** > **<agent>** > **App [Application]**) est la suivante : **1.** Agent-config-windows : Navigateur intégré **2.** Agent-config-macos : Navigateur par défaut **3.** Agent-config-default : Navigateur par défaut Paramètre d'authentification client : (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > **Authentication [Authentification]**): SAML auth - default: os=all Avec cette configuration, les utilisateurs Windows utilisent le navigateur intégré et tous les autres utilisent le navigateur par défaut.	L'option **Use Default Browser (Utiliser le navigateur par défaut)** est automatiquement activée dans la configuration d'authentification client. Tous les utilisateurs commenceront maintenant à utiliser le navigateur par défaut, remplaçant le paramètre spécifique à Windows.

Exemple de scénario 2

Version PAN-OS 11.0.x ou antérieure	Après la mise à niveau vers la version PAN-OS 11.1.x et ultérieure
La configuration du portail (**Network [Réseau]** > **GlobalProtect** > **A** > **Agent** > **<agent>** > **App [Application]**) est la suivante : **1.** Agent-config-windows : Navigateur intégré **2.** Agent-config-macos : Navigateur par défaut **3.** Agent-config-default : Navigateur par défaut Paramètre d'authentification client (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > **Authentication [Authentification]**) : SAML auth - default: os=all, use-default-browser=yes (Navigateur par défaut)	L'option **Use Default Browser (Utiliser le navigateur par défaut)** a la priorité sur le paramètre de configuration de l'agent. Tous les utilisateurs commenceront maintenant à utiliser le navigateur par défaut.

Pour conserver le comportement précédent la mise à niveau, définissez l'authentification client comme suit :

- SAML auth - windows: os=windows, use-default-browser=no (Navigateur intégré)
- SAML auth - macos: os=macos, use-default-browser=yes (Navigateur par défaut)

 ©2026 Palo Alto Networks, Inc.

- SAML auth - default: os=all, use-default-browser=yes (Navigateur par défaut)

Ces paramètres permettront aux utilisateurs de Windows d'utiliser le navigateur intégré pour l'authentification SAML et à tous les autres utilisateurs des autres systèmes d'exploitation d'utiliser le navigateur par défaut.

Comportement de rétrogradation

Si vous rétrogradez la version de PAN-OS de 11.1.0 à une version antérieure, la configuration **Use Default Browser (Utiliser le navigateur par défaut)** dans le paramètre d'authentification client sera automatiquement supprimée. Vous devez revenir à l'option d'agent de portail **Use Default Browser for SAML Authentication (Utiliser le navigateur par défaut pour l'authentification SAML)**.

Les configurations d'authentification de la passerelle GlobalProtect ne sont pas affectées lors des scénarios de mise à niveau ou de rétrogradation. L'utilisation par le client du navigateur par défaut/intégré pour l'authentification SAML est contrôlée via les paramètres du portail.

Personnaliser la page de destination SAML/CAS ACS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager)	PAN-OS 10.2.11 ou version ultérieure Application GlobalProtect fonctionnant sur les terminaux Windows, macOS, iOS, Android et Linux.

Vous pouvez désormais personnaliser la page de destination SAML/CAS ACS affichée sur le navigateur par défaut lorsque vous utilisez la méthode d'authentification SAML/CAS pour vous authentifier sur l'application GlobalProtect. Vous pouvez configurer la modification ou la suppression de la marque de la page de destination SAML/CAS ACS sur le navigateur par défaut en utilisant les commandes Command Line Interface (interface de ligne de commande - CLI). Par défaut, la fonctionnalité n'est pas activée pour l'application.

Cette fonctionnalité n'est pas disponible sur Panorama.

Avant de personnaliser la page de destination SAML/CAS ACS, vous devez :

1. Assurez-vous que le Portail GlobalProtect est configuré.
2. Assurez-vous que la Passerelle GlobalProtect est configurée.

 ©2026 Palo Alto Networks, Inc.

3. Assurez-vous que le navigateur par défaut pour l'authentification SAML est activé dans la configuration du portail par l'une ou l'autre des méthodes suivantes ou les deux :

   - Définissez l'option **Use Default Browser for SAML Authentication (Utiliser le navigateur par défaut pour l'authentification SAML)** sur **Yes (Oui)** dans les paramètres de l'application de la configuration du portail GlobalProtect.
   - Activez l'option **Use Default-Browser (Utiliser le navigateur par défaut)** dans le paramètre d'authentification client de la configuration du portail.

   Pour configurer le portail GlobalProtect de façon à modifier ou à supprimer la marque de la page de destination SAML/CAS ACS sur le navigateur par défaut, utilisez les commandes CLI suivantes :

   Sur le pare-feu hébergeant le portail, saisissez les commandes CLI suivantes.

   ```
   <username@hostname> définir global-protect auth-response-page
   ```

   L'écran affiche les commandes CLI pour la fonctionnalité de personnalisation de page SAML/CAS ACS :

   ```
   [redacted]> set global-protect auth-response-page
   > auth-message          Set auth message on the auth response page
   > background-image      URL to fetch background image on the auth response page
   > footer-logo           URL to fetch footer logo image on the auth response page
   > footer-text           Set footer text on the auth response page
   > main-logo             URL to fetch main logo image on the auth response page
   > show                  Show all auth response page parameters
   > type                  Set auth response page type to (default|none|custom)
   ```

   Utilisez les commandes CLI suivantes pour personnaliser la page de destination SAML/CAS ACS :

   ```
   définir global-protect auth-response-page type <default | none |
    custom>
   ```

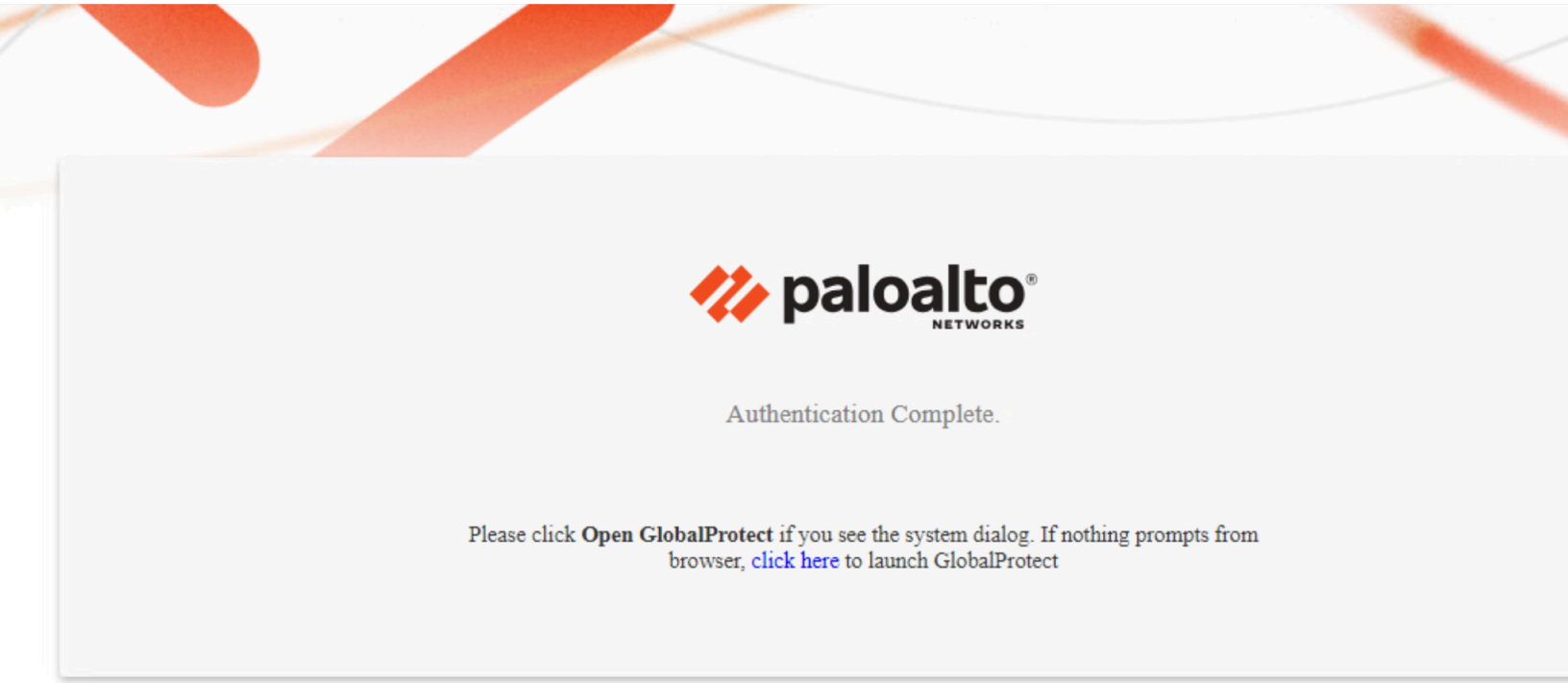
   - Pour continuer à utiliser la page ACS par défaut, laissez le type vide ou utilisez la commande CLI :

     ```
     définir global-protect auth-response-page type <default>
     ```

     Lorsque vous configurez le **type global-protect auth-response-page** comme **<default>** et que l'authentification est réussie, la page ACS par défaut s'affiche avec le

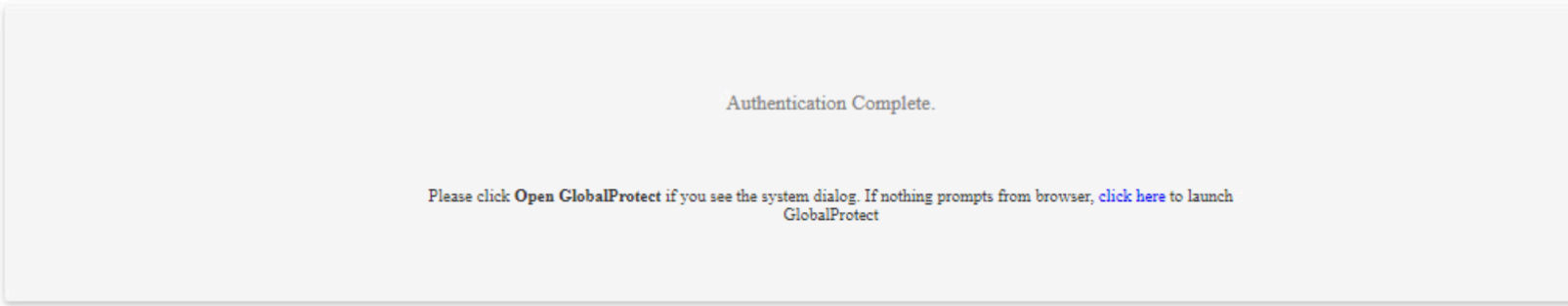
 ©2026 Palo Alto Networks, Inc.

message **Authentication Complete (Authentication terminée)**. Si l'authentification échoue, l'écran affiche le message **Authentication Failed (Authentification échouée)**.



- Pour supprimer le logo par défaut, l'image d'arrière-plan, le logo de pied de page et le texte de pied de page, utilisez la commande CLI :

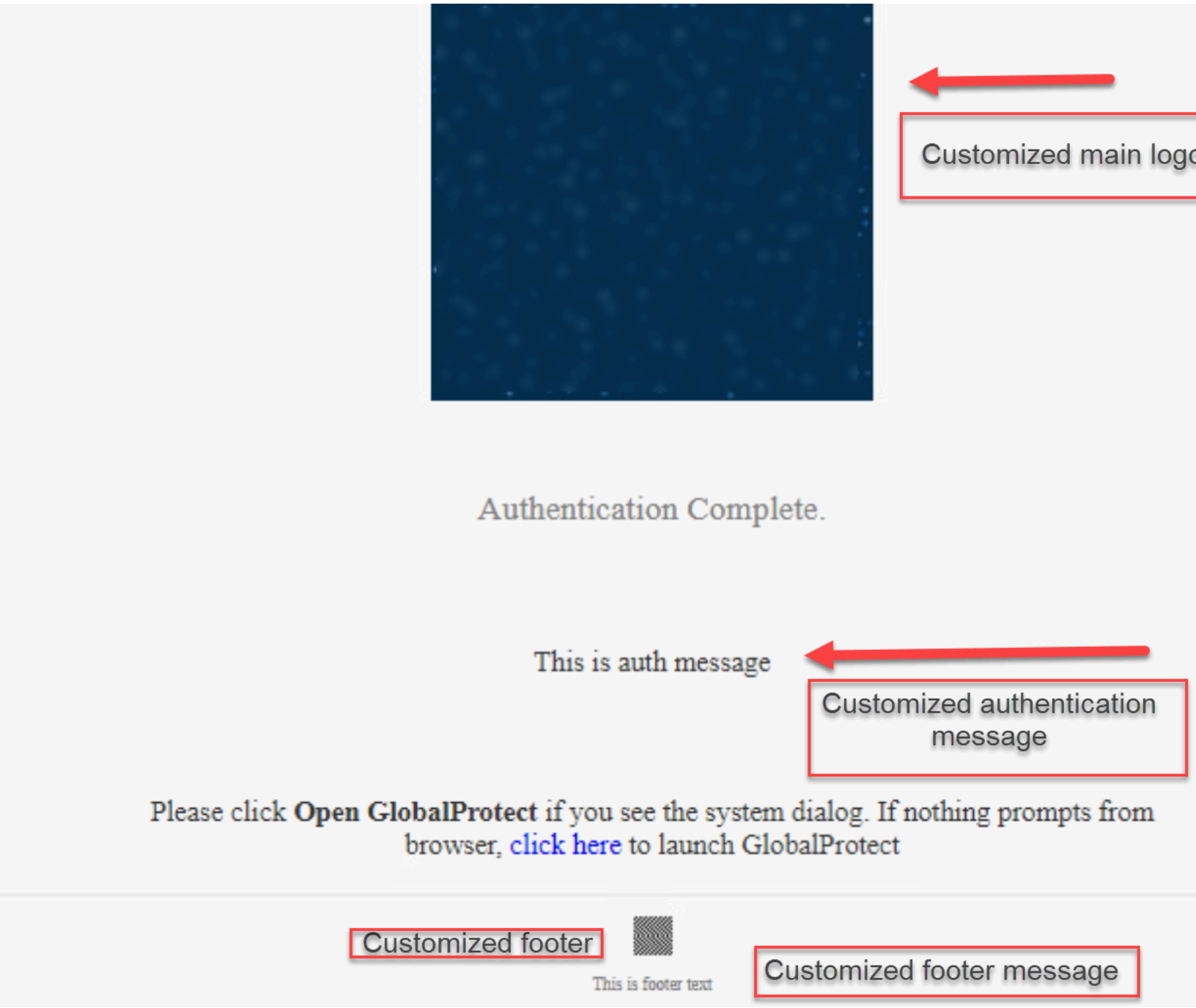
```
définir global-protect auth-response-page type <none>
```



- Pour personnaliser la page, utilisez la commande CLI :

```
définir global-protect auth-response-page type <custom>
```

 ©2026 Palo Alto Networks, Inc.



Utilisez les commandes CLI suivantes pour personnaliser les champs de la page de destination SAML/CAS ACS :

```
définir global-protect auth-response-page background-image <value>
```

```
définir global-protect auth-response-page main-logo <value>
```

 ©2026 Palo Alto Networks, Inc.

```
définir global-protect auth-response-page auth-message <value>
```

```
définir global-protect auth-response-page footer-logo <value>
```

```
définir global-protect auth-response-page footer-text <value>
```

```
[redacted]> set global-protect auth-response-page
> auth-message        Set auth message on the auth response page
> background-image    URL to fetch background image on the auth response page
> footer-logo         URL to fetch footer logo image on the auth response page
> footer-text         Set footer text on the auth response page
> main-logo           URL to fetch main logo image on the auth response page
```

- *Vous pouvez laisser les valeurs vides pour tous les champs sauf pour le type <value>*
- *Pour l'image <value>, vous devez entrer une URL HTTP ou HTTPS valide*
- *Pour le texte <value>, ne saisissez aucun caractère de contrôle tel que \n, \r, \t, \0 ou caractères dont la valeur ascii est < 0x1F*

Utilisez la commande CLI suivante pour afficher les paramètres actuels de la page de réponse de l'authentification :

```
définir global-protect auth-response-page <show>
```

```
[redacted]> set global-protect auth-response-page show

n response page type              : custom
n response page background image : https://[redacted]
n response page main logo         : https://[redacted].png
n response page auth message      : This is auth message
n response page footer logo       : https://[redacted].png
n response page footer text       : This is footer text
```

Limites de caractères pour les champs personnalisés

Le tableau suivant répertorie les limites maximales de caractères pour les champs que vous pouvez personnaliser et l'écran affiche des messages d'erreur lorsque vous saisissez une valeur qui dépasse la limite de caractères.

Champ	Limite de caractère	Messages d'erreur (Quand la limite de caractères dépasse)
URL de l'image d'arrière-plan	2 000	Doit être inférieur ou égal à 2 000 caractères
URL du logo principal	2 000	Doit être inférieur ou égal à 2 000 caractères

 ©2026 Palo Alto Networks, Inc.

Champ	Limite de caractère	Messages d'erreur (Quand la limite de caractères dépasse)
Logo de pied de page	2 000	Doit être inférieur ou égal à 2 000 caractères
Message d'authentification	500	Doit être inférieur ou égal à 500 caractères
Texte de pied de page	256	Doit être inférieur ou égal à 256 caractères

Résolution d'image et types pour les champs personnalisés

La fonctionnalité prend en charge tous les types d'image tels que .png, .jpeg/.jpg et .svg en fonction de la compatibilité du navigateur. Vous devez utiliser une résolution d'image appropriée (largeur × hauteur) en fonction des dimensions des appareils.

Le tableau suivant répertorie la résolution d'image que vous pouvez appliquer lors de la personnalisation de la page :

Image	Résolution d'image
Image de fond	La largeur du bloc d'image d'arrière-plan correspond à 100 % de la largeur de la fenêtre de l'appareil/navigateur, et la hauteur est calculée par le navigateur à l'aide du ratio d'aspect de l'image.
Logo principal	La largeur du bloc d'image du logo principal est d'environ 50 % de la largeur de la fenêtre du périphérique/navigateur avec une largeur maximale de 340 px, et la hauteur est calculée par le navigateur à l'aide du ratio d'aspect de l'image.
Logo de pied de page	La largeur du bloc d'image du logo de pied de page est fixée à 30 px, et la hauteur est calculée par le navigateur à l'aide du ratio d'aspect de l'image. Pour l'image du logo de pied de page, le rapport d'aspect pour la largeur: hauteur ne doit pas être plus de trois fois la largeur (1:3). Si le rapport de hauteur augmente comme 1:4, le texte du pied de page peut ne pas être correctement affiché à l'écran.

 ©2026 Palo Alto Networks, Inc.

Configurer l'authentification Kerberos

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Kerberos est un protocole d'authentification de réseau informatique qui utilise des *tickets* pour permettre aux nœuds communiquant sur un réseau non sécurisé de prouver leur identité les uns aux autres de manière sécurisée. Le SSO Kerberos maintient une expérience de connexion transparente en fournissant des informations précises sur User-ID sans interaction de l'utilisateur. Les réseaux qui prennent en charge le SSO Kerberos exigent que les utilisateurs finaux se connectent uniquement lors de l'accès initial au réseau. Après la connexion initiale, les utilisateurs finaux peuvent accéder à tout service activé par Kerberos dans le réseau (tel que le webmail) sans avoir à se reconnecter jusqu'à l'expiration de la session SSO (la durée de la session SSO est établie par l'administrateur Kerberos). Cette méthode d'authentification aide à identifier les utilisateurs pour l'application des politiques utilisateur et HIP.

L'authentification Kerberos est prise en charge sur les points de terminaison Windows (7, 8 et 10) et MacOS (version 10.10 et versions ultérieures). Pour l'authentification Kerberos sur les points de terminaison MacOS, il faut disposer de la version 4.1.0 de l'application GlobalProtect ou de toute version ultérieure.

L'authentification Kerberos n'est pas prise en charge en mode FIPS-CC.

Si vous activez à la fois le SSO Kerberos et un Configurer l'authentification externe (tel que RADIUS), GlobalProtect tente d'abord le SSO. Vous pouvez configurer GlobalProtect pour qu'il revienne à un service d'authentification externe lorsque le SSO échoue ou vous pouvez configurer GlobalProtect pour n'utiliser que le SSO Kerberos pour l'authentification.

Dans cette mise en œuvre, le portail et la passerelle GlobalProtect agissent en tant que principaux de service Kerberos et l'application GlobalProtect agit en tant que principal utilisateur qui authentifie les utilisateurs finaux avec un ticket de service Kerberos du Key Distribution Center (centre de distribution de clé - KDC).

Les éléments suivants doivent être en place pour que l'application GlobalProtect pour les terminaux macOS prenne en charge le SSO Kerberos :

- Une infrastructure Kerberos, qui comprend un KDC avec un serveur d'authentification (AS) et un Ticket Granting Service (service d'émission de tickets - TGS).

  Le KDC doit être accessible depuis les terminaux sur lesquels l'application GlobalProtect fonctionne. Dans la plupart des cas, le KDC n'est accessible que depuis l'intérieur du réseau d'entreprise, ce qui signifie que l'application GlobalProtect ne peut utiliser l'authentification Kerberos que lorsque le terminal est interne. Cependant, si le KDC est accessible depuis l'extérieur du réseau d'entreprise (depuis Internet), l'application GlobalProtect peut utiliser l'authentification Kerberos lorsque le terminal est externe.

  Si le magasin de certificats utilisateur contient au moins un certificat délivré par la même CA que le certificat utilisé pour l'établissement du tunnel de préouverture de session, vous pouvez

 ©2026 Palo Alto Networks, Inc.

également utiliser l'authentification Kerberos avec la préouverture de session pour permettre à l'application GlobalProtect d'utiliser l'authentification Kerberos lorsque le terminal est externe.

Lorsqu'un utilisateur final tente d'accéder à des ressources réseau protégées en utilisant l'authentification Kerberos, l'AS accorde à l'utilisateur un Ticket pour obtenir des tickets (Ticket to Get Tickets ,TGT), qui est une demande de service utilisée pour générer des tickets de service à partir du TGS. Le ticket de service est ensuite utilisé pour authentifier l'utilisateur final et établir une session de service.

- Un compte de service Kerberos pour chaque portail et passerelle GlobalProtect.

  Les comptes de service sont nécessaires pour créer des keytabs Kerberos, qui sont des fichiers contenant le nom principal et le mot de passe de chaque portail ou passerelle GlobalProtect.

1. Créez un fichier keytab Kerberos.
   1. Connectez-vous au KDC en utilisant les informations d'identification de votre compte de service Kerberos.
   2. Ouvrez une invite de commande, puis entrez la commande suivante :

      ```
      ktpass /princ <principal_name> /pass <password> /crypto
       <algorithm> /ptype KRB5_NT_PRINCIPAL /out <file_name>.keytab
      ```

      *Le **<principal_name>** et le **<password>** sont le nom principal et le mot de passe du portail ou de la passerelle GlobalProtect. Le **<algorithm>** doit correspondre à l'algorithme dans le ticket de service émis par le TGS, qui est déterminé par l'administrateur Kerberos. Si le portail ou la passerelle GlobalProtect fonctionne en mode FIPS ou CC, l'algorithme doit être **aes128-cts-hmac-sha1-96** ou **aes256-cts-hmac-sha1-96**. Si le portail ou la passerelle ne fonctionne pas en mode FIPS ou CC, vous pouvez également utiliser **des3-cbc-sha1** ou **arcfour-hmac**.*

 ©2026 Palo Alto Networks, Inc.

2. Créez un profil de serveur pour l'authentification Kerberos.

   Le profil de serveur identifie le service d'authentification externe et indique au pare-feu comment se connecter à ce service d'authentification et accéder aux informations d'authentification pour vos utilisateurs.

   1. Choisissez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Device (Périphérique)** > **Server Profiles (Profils serveur)** > **Kerberos**, puis **Add (Ajouter)** un profil de serveur Kerberos.
      - Sur Strata Cloud Manager, suivez les étapes ci-dessous :
        1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma AccessGlobalProtect** > **GlobalProtect**.
        2. Sélectionnez **Identity Services (Services d'identité)Authentication (Authentification)Server Profiles (Profils de serveur)Kerberos**, puis **Add (Ajouter)** un profil de serveur Kerberos.
   2. Saisissez un **Profile Name (Nom de profil)**, par exemple **`GP-User-Auth`**.
   3. S'il s'agit du profil d'un pare-feu pouvant prendre en charge de multiples systèmes virtuels, sélectionnez un système virtuel ou sélectionnez l'option **Shared (Partagé)** en tant que **Location (Emplacement)** où le profil est disponible.
   4. Cliquez sur **Add (Ajouter)** dans la zone **Servers (Serveurs)**, puis saisissez les informations suivantes pour vous connecter au service d'authentification :
      - **Name (Nom)** du serveur
      - Adresse IP ou nom de domaine complet du **Kerberos Server (Serveur Kerberos)**.
      - **Port**
   5. Cliquez sur **OK** pour enregistrer le profil de serveur.

3. (Facultatif) Créez un profil d'authentification.

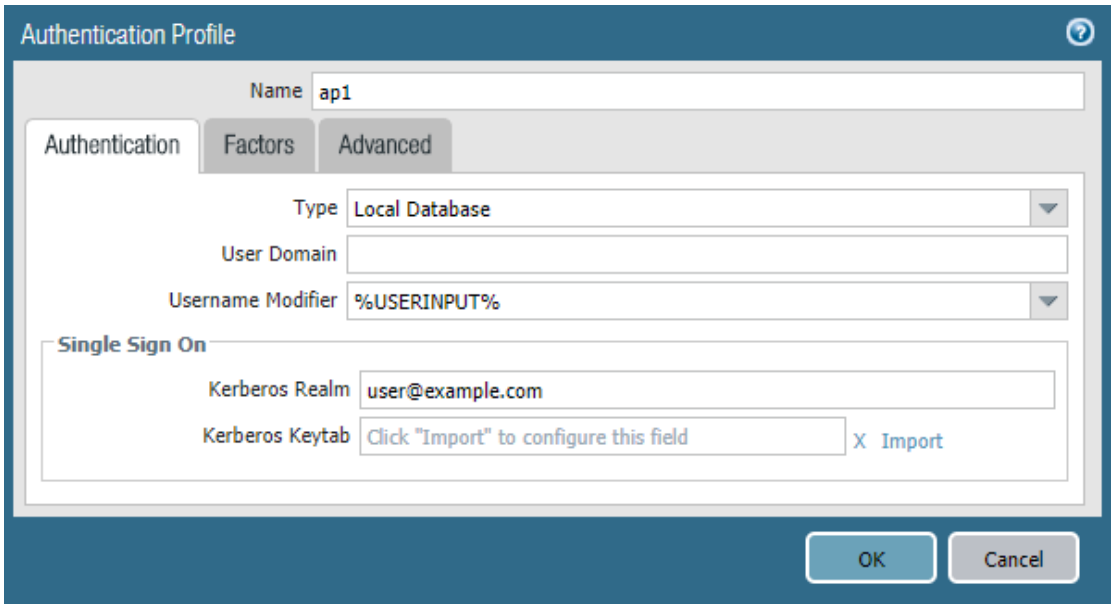
   Le profil d'authentification spécifie le profil du serveur pour le portail ou les passerelles à utiliser lorsqu'ils authentifient les utilisateurs. Sur un portail ou une passerelle, vous pouvez attribuer un ou plusieurs profils d'authentification dans un ou plusieurs profils d'authentification client. Pour obtenir des renseignements sur la façon dont un profil d'authentification dans un profil d'authentification client prend en charge l'authentification

 ©2026 Palo Alto Networks, Inc.

utilisateur granulaire, voir les sections Configurer une passerelle GlobalProtect et Paramétrer l'accès au portail GlobalProtect.

Pour permettre aux utilisateurs de se connecter et de modifier leur mot de passe expiré sans l'intervention d'un administrateur, songez à utiliser un VPN d'accès distant avec pré-connexion.

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis **Add (Ajouter)** un nouveau profil d'authentification.



   - Sur Strata Cloud Manager, suivez les étapes ci-dessous :
     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma AccessGlobalProtect** > **GlobalProtect**.
     2. Sélectionnez **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Authentication Profiles (Profils d'authentification)** puis **Add (Ajouter)** un nouveau profil d'authentification.
2. Donnez un **Name (Nom)** au profil, puis sélectionnez **Kerberos** comme **Type** d'authentification.
3. Sélectionnez le **Server Profile (Profil de serveur)** de l'authentification Kerberos que vous avez créé à l'étape 1.
4. Spécifiez le **User Domain (Domaine d'utilisateur)** et le **Username Modifier (Modificateur d'utilisateur)**. Le point de terminaison combine ces valeurs pour modifier la chaîne domaine / nom d'utilisateur qu'un utilisateur saisit lors de la connexion. Le point de terminaison utilise la chaîne modifiée pour l'authentification et la valeur **User Domain (Domaine utilisateur)** pour le mappage de groupe User-ID. Il s'avère utile de modifier la saisie utilisateur lorsque le service d'authentification demande que la chaîne domaine/ nom d'utilisateur soit indiquée dans un format spécifique ; vous ne voulez toutefois pas

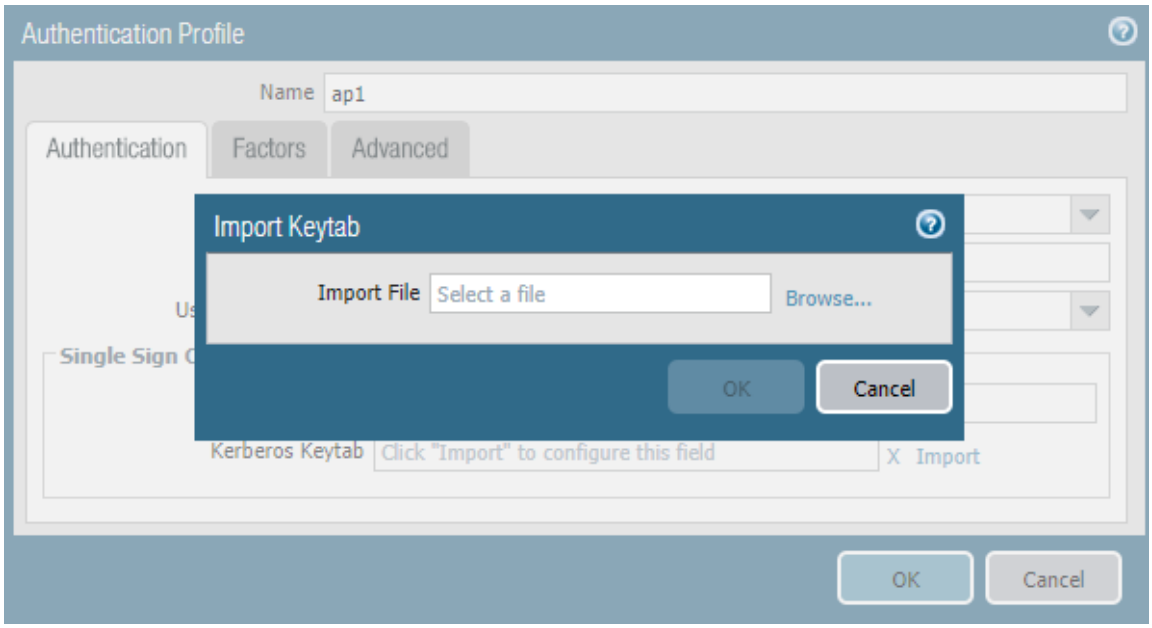
 ©2026 Palo Alto Networks, Inc.

que les utilisateurs aient à saisir correctement le domaine. Vous devez faire une sélection parmi les options suivantes :

- Pour envoyer l'entrée non modifiée de l'utilisateur, laissez le **User Domain (Domaine utilisateur)** vide (par défaut) et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** à la variable **%USERINPUT%** (par défaut).
- Pour ajouter initialement un domaine sur la saisie utilisateur, saisissez un **User Domain (Domaine utilisateur)** et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** sur **%USERDOMAIN%\%USERINPUT% (%DOMAINEUTILISATEUR%\%SAISIEUTILISATEUR%)**.
- Pour ajouter un domaine sur la saisie utilisateur, saisissez un **User Domain (Domaine utilisateur)** et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** sur **%USERINPUT%@%USERDOMAIN% (%SAISIEUTILISATEUR%@ %DOMAINEUTILISATEUR%)**.

  *Si le **Username Modifier (Modificateur du nom d'utilisateur)** inclut la variable **%USERDOMAIN% (%DOMAINEUTILISATEUR%)**, la valeur **User Domain (Domaine utilisateur)** remplace toute chaîne de domaine saisie par l'utilisateur. Si le **User Domain (Domaine utilisateur)** est vide, le périphérique supprime toute chaîne de domaine saisie par l'utilisateur.*

5. Configurez l'authentification unique (SSO) Kerberos, si elle est prise en charge par votre réseau.
   1. Saisissez la **Kerberos Realm (Partition Kerberos)** (maximum de 127 caractères) afin de spécifier la portion nom d'hôte du nom de connexion de l'utilisateur. Par exemple, le nom de compte utilisateur utilisateur@EXEMPLE.LOCAL comporte la partition EXEMPLE.LOCAL.
   2. **Import (Importez)** un fichier **Kerberos Keytab (Keytab Kerberos)**. Lorsque vous y êtes invité, **Browse (Parcourez)** pour trouver le fichier keytab, puis cliquez sur **OK**.



6. À l'onglet **Advanced (Avancé)**, **Add (Ajoutez)** une **Allow List (Liste d'autorisation)** pour sélectionner les utilisateurs et les groupes d'utilisateurs à authentifier au moyen

 ©2026 Palo Alto Networks, Inc.

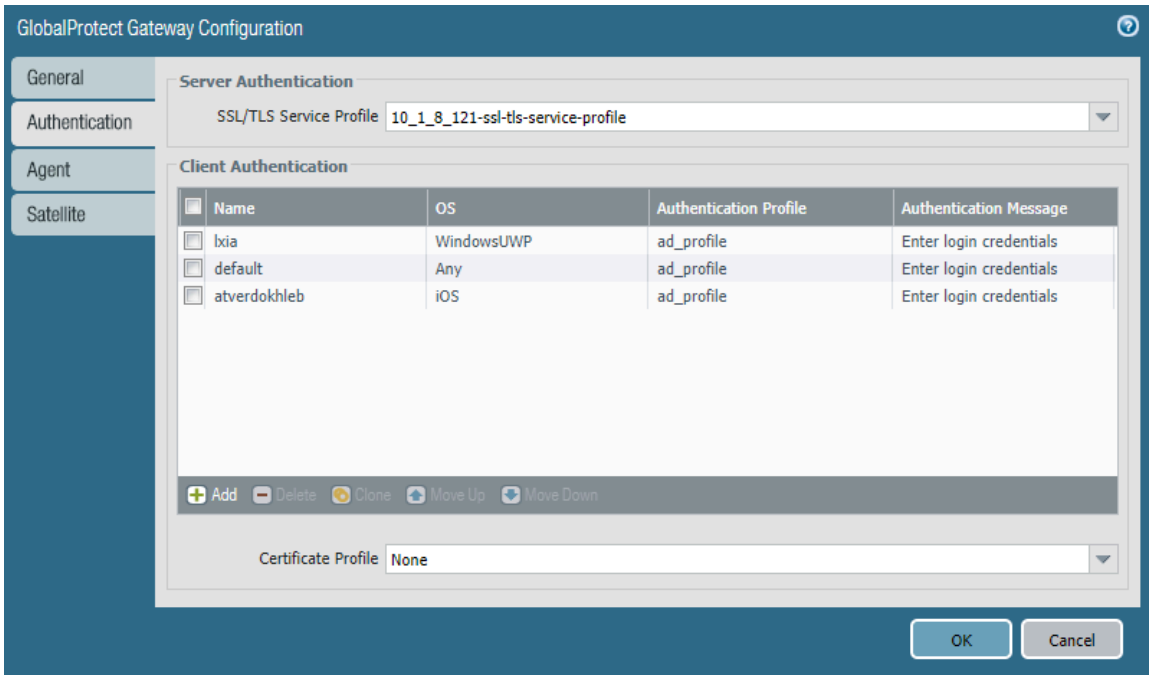
de ce profil. L'option **all (tous)** permet à tous les utilisateurs de s'authentifier à l'aide de ce profil. Par défaut, la liste est vide, ce qui signifie qu'aucun utilisateur ne peut s'authentifier.

Lors de l'authentification, le point de terminaison cherche d'abord à établir une ouverture de session unique en utilisant le keytab. S'il réussit et que l'utilisateur tentant l'accès figure dans la **Allow List (Liste d'autorisations)**, l'authentification réussit immédiatement. Sinon, le processus d'authentification revient à l'authentification manuelle (nom d'utilisateur/mot de passe) en utilisant le **Type** d'authentification spécifié. Le **Type** n'a pas à être Kerberos. Pour modifier ce comportement afin que les utilisateurs puissent s'authentifier uniquement à l'aide de Kerberos, définissez **Use Default Authentication on Kerberos Authentication Failure (Utiliser l'authentification par défaut si échec de l'authentification Kerberos)** sur **No (non)** dans la configuration de l'agent du portail GlobalProtect.

7. Cliquez sur **OK**.

4. Affectez le profil d'authentification à une passerelle :

1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** pour modifier une passerelle existante ou en **Add (Ajouter)** une nouvelle.



2. Sélectionnez un **SSL/TLS Service Profile (Profil de service SSL/TLS)** existant pour sécuriser la passerelle, ou **Add (Ajouter)** un nouveau profil de service (**Network [Réseau]**

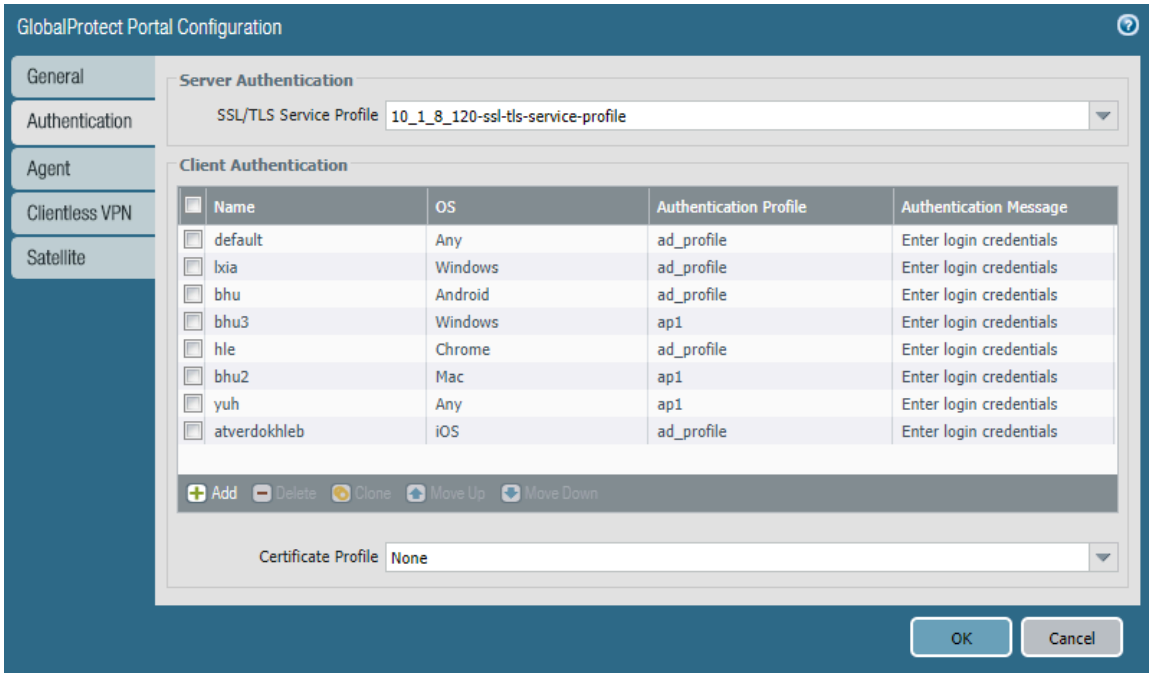
 ©2026 Palo Alto Networks, Inc.

> **GlobalProtect** > **Gateways [Passerelles]** > ***<gateway-config>*** > **Authentication [Authentification]**).

3. Vous devez **Add (Ajouter)** une nouvelle configuration de **Client Authentication (Authentification du client)** (**Network [Réseau]** > **GlobalProtect** > **Gateways [Passerelles]** > ***<gateway-config>*** > **Authentication [Authentification]**), puis configurer les paramètres suivants :
   - **Name (Nom)** : le nom de la configuration de l'authentification client.
   - **OS (Système d'exploitation)** : les systèmes d'exploitation sur lesquels la passerelle est accessible.
   - **Authentication Profile (Profil d'authentification)** : le profil d'authentification dans lequel votre fichier keytab Kerberos a été importé.
   - (Facultatif) **Username Label (Étiquette de nom d'utilisateur)** : une étiquette de nom d'utilisateur personnalisée pour la connexion à la passerelle GlobalProtect.
   - (Facultatif) **Password Label (Étiquette de mot de passe)** : indiquez une étiquette de mot de passe personnalisée pour la connexion à la passerelle GlobalProtect.
   - (Facultatif) **Authentication Message (Message d'authentification)** : message affiché lorsque les utilisateurs finaux s'authentifient à la passerelle.
4. Cliquez sur **OK** pour enregistrer vos modifications.

 ©2026 Palo Alto Networks, Inc.

5. Affectez le profil d'authentification au portail GlobalProtect.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
   2. Sélectionnez un portail existant ou en **Add (Ajouter)** une nouvelle.



   3. Sélectionnez un **SSL/TLS Service Profile (Profil de service SSL/TLS)** existant pour sécuriser la portail, ou **Add (Ajouter)** un nouveau profil de service (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > ***<portal-config>*** > **Authentication [Authentification]**).
   4. Vous devez **Add (Ajouter)** une nouvelle configuration de **Client Authentication (Authentification du client)** (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > ***<portal-config>*** > **Authentication [Authentification]**), puis configurer les paramètres suivants :
      - **Name (Nom)** : le nom de la configuration de l'authentification client.
      - **OS (Système d'exploitation)** : les systèmes d'exploitation sur lesquels le portail est accessible.
      - **Authentication Profile (Profil d'authentification)** : le profil d'authentification dans lequel votre fichier keytab Kerberos est importé.
      - (Facultatif) **Username Label (Étiquette de nom d'utilisateur)** : une étiquette de nom d'utilisateur personnalisée pour la connexion au portail GlobalProtect.
      - (Facultatif) **Password Label (Étiquette de mot de passe)** : indiquez une étiquette de mot de passe personnalisée pour la connexion au portail GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

- (Facultatif) **Authentication Message (Message d'authentification)** : message affiché lorsque les utilisateurs finaux se connectent au portail.

5. Cliquez sur **OK** pour enregistrer vos modifications.

6. Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**.

Configurer l'authentification RADIUS ou TACACS+

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

RADIUS est un protocole client / serveur et un logiciel qui permet aux serveurs d'accès à distance de communiquer avec un serveur central pour authentifier les utilisateurs d'appels entrants et autoriser leur accès au système ou au service demandé. TACACS+ est un protocole d'authentification bien établi commun aux réseaux UNIX qui permet à un serveur d'accès à distance de transférer le mot de passe d'ouverture de session d'un utilisateur à un serveur d'authentification pour déterminer si l'accès peut être autorisé à un système donné.

 ©2026 Palo Alto Networks, Inc.

1. Créez un profil de serveur.

Le profil de serveur identifie le service d'authentification externe et indique au pare-feu comment se connecter à ce service d'authentification et accéder aux informations d'authentification pour vos utilisateurs.

Si vous souhaitez activer la livraison des attributs VSA vers un serveur RADIUS, *vous devez créer un profil de serveur RADIUS.*

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)**, puis sélectionnez le type de profil (**RADIUS** ou **TACACS+**).
   - Sur Strata Cloud Manager, suivez les étapes ci-dessous :
     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma AccessGlobalProtect** > **GlobalProtect**.
     2. Sélectionnez **Identity Services (Services d'identité)Authentication (Authentification)Server Profiles (Profils de serveur)** puis sélectionnez le type de profil (**RADIUS** ou **TACACS+**).
2. **Add (Ajoutez)** un nouveau profil de serveur RADIUS ou TACACS+.
3. Saisissez un **Profile Name (Nom de profil)**, par exemple **`GP-User-Auth`**.
4. S'il s'agit du profil d'un pare-feu pouvant prendre en charge de multiples systèmes virtuels, sélectionnez un système virtuel ou sélectionnez l'option **Shared (Partagé)** en tant que **Location (Emplacement)** où le profil est disponible.
5. Configurez les **Server Settings (Paramètres de serveur)** suivants :
   - **Timeout (sec) (Délai d'attente (sec))** : le nombre de secondes avant qu'une requête de connexion au serveur expire en raison d'un manque de réponse du serveur d'authentification.
   - **Authentication Protocol (Protocole d'authentification)** : le protocole utilisé pour se connecter au serveur d'authentification. Voici certaines des options offertes : **CHAP**, **PAP**, **PEAP-MSCHAPv2**, **PEAP with GTC** ou **EAP-TTLS with PAP**.

     *Si vous configurez **PEAP-MSCHAPv2** (Protected Extensible Authentication Protocol Microsoft Challenge Handshakie Authentication Protocol version 2) en tant que protocole d'authentification, les utilisateurs distants peuvent changer leurs mots de passe RADIUS ou Active Directory (AD) par l'intermédiaire de l'application GlobalProtect à l'expiration de leur mot de passe ou lorsqu'un administrateur RADIUS/AD exige que le mot de passe soit modifié à la prochaine connexion.*
   - (RADIUS uniquement) **Retries (Tentatives)** : le nombre de fois que le pare-feu tente de se connecte au serveur d'authentification avant d'abandonner la demande.
   - (TACACS+ uniquement) **Use single connection for all authentication (Utiliser une connexion unique pour toutes les authentifications)** : option permettant d'autoriser

 ©2026 Palo Alto Networks, Inc.

toutes les requêtes d'authentification TACACS+ à se produire sur une seule session TCP plutôt que des sessions distinctes pour chaque requête.

6. Cliquez sur **Add (Ajouter)** dans la zone **Servers (Serveurs)**, puis saisissez les informations suivantes pour vous connecter au service d'authentification :
   - **Name (Nom)**
   - **Server (Serveur) RADIUS** ou **TACACS+** (Adresse IP ou FQDN du serveur)
   - **Secret** (secret partagé qui permet au service d'authentification d'authentifier le pare-feu.)
   - **Port**
7. Cliquez sur **OK** pour enregistrer le profil de serveur.

2. (Facultatif) Créez un profil d'authentification.

Le profil d'authentification spécifie le profil du serveur pour le portail ou les passerelles à utiliser lorsqu'ils authentifient les utilisateurs. Sur un portail ou une passerelle, vous pouvez attribuer un ou plusieurs profils d'authentification dans un ou plusieurs profils d'authentification client. Pour obtenir des renseignements sur la façon dont un profil d'authentification dans un profil d'authentification client prend en charge l'authentification utilisateur granulaire, voir les sections Configurer une passerelle GlobalProtect et Paramétrer l'accès au portail GlobalProtect.

Pour permettre aux utilisateurs de se connecter et de modifier leur propre mot de passe expiré sans l'intervention d'un administrateur, songez à utiliser un VPN d'accès distant avec pré-connexion.

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis **Add (Ajouter)** un nouveau profil d'authentification.
   - Sur Strata Cloud Manager, suivez les étapes ci-dessous :
     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma AccessGlobalProtect** > **GlobalProtect**.
     2. Sélectionnez **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Authentication Profiles (Profils d'authentification)** puis **Add (Ajouter)** un nouveau profil d'authentification.
2. Saisissez un **Name (Nom)** pour le profil.
3. Sélectionnez le **Authentication Type (Type d'authentification)** (**RADIUS** ou **TACACS+**).
4. Sélectionnez le **Server Profile (Profil de serveur)** de l'authentification RADIUS ou TACACS+ que vous avez créé à l'étape 1 depuis la liste déroulante.
5. (RADIUS uniquement) Activez **Retrieve user group from RADIUS (Récupérer le groupe d'utilisateurs auprès de RADIUS)** si vous souhaitez inclure cette information dans le profil d'authentification.
6. Spécifiez le **User Domain (Domaine d'utilisateur)** et le **Username Modifier (Modificateur d'utilisateur)**. Le point de terminaison combine ces valeurs pour modifier la chaîne domaine / nom d'utilisateur qu'un utilisateur saisit lors de la connexion. Le point de terminaison utilise la chaîne modifiée pour l'authentification et la valeur **User Domain**

 ©2026 Palo Alto Networks, Inc.

(Domaine utilisateur) pour le mappage de groupe User-ID. Il s'avère utile de modifier la saisie utilisateur lorsque le service d'authentification demande que la chaîne domaine/nom d'utilisateur soit indiquée dans un format spécifique ; vous ne voulez toutefois pas que les utilisateurs aient à saisir correctement le domaine. Vous devez faire une sélection parmi les options suivantes :

- Pour envoyer l'entrée non modifiée de l'utilisateur, laissez vide le **User Domaine (Domaine utilisateur)** (par défaut) et définissez le **Username Modifier (Modificateur d'utilisateur)** sur la variable **% USERINPUT%** (la valeur par défaut).
- Pour ajouter initialement un domaine sur la saisie utilisateur, saisissez un **User Domain (Domaine utilisateur)** et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** sur **%USERDOMAIN%\%USERINPUT% (%DOMAINEUTILISATEUR%\%SAISIEUTILISATEUR%)**.
- Pour ajouter un domaine sur la saisie utilisateur, saisissez un **User Domain (Domaine utilisateur)** et définissez le **Username Modifier (Modificateur du nom d'utilisateur)** sur **%USERINPUT%@%USERDOMAIN% (%SAISIEUTILISATEUR%@%DOMAINEUTILISATEUR%)**.

  *Si le **Username Modifier (Modificateur du nom d'utilisateur)** inclut la variable **%USERDOMAIN% (%DOMAINEUTILISATEUR%)**, la valeur **User Domain (Domaine utilisateur)** remplace toute chaîne de domaine saisie par l'utilisateur. Si le **User Domain (Domaine utilisateur)** est vide, le périphérique supprime toute chaîne de domaine saisie par l'utilisateur.*

7. À l'onglet **Advanced (Avancé)**, **Add (Ajoutez)** une **Allow List (Liste d'autorisation)** pour sélectionner les utilisateurs et les groupes d'utilisateurs à authentifier au moyen de ce profil. L'option **all (tous)** permet à tous les utilisateurs de s'authentifier à l'aide de ce profil. Par défaut, la liste est vide, ce qui signifie qu'aucun utilisateur ne peut s'authentifier.
8. Cliquez sur **OK**.

3. **Commit (Validez)** la configuration.

 ©2026 Palo Alto Networks, Inc.

Configurer l'authentification du certificat client

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Avec l'authentification facultative du certificat client, l'utilisateur présente un certificat client ainsi qu'une demande de connexion au portail GlobalProtect ou à la passerelle. Le portail ou la passerelle peut utiliser soit un certificat client partagé ou unique pour valider que l'utilisateur ou le point de terminaison appartient à votre organisation.

- Pour authentifier l'utilisateur, un des champs de certificat, tel que le champ nom du sujet, doit identifier le nom d'utilisateur.
- Pour authentifier le point de terminaison, le champ objet du certificat doit identifier le type de périphérique au lieu du nom d'utilisateur. (avec les méthodes de connexion avant ouverture de session, le portail ou la passerelle authentifie le point de terminaison avant que l'utilisateur ne se connecte.)

  *Si vous configurez le portail ou la passerelle pour l'authentification des utilisateurs au moyen de l'authentification du certificat du client, les utilisateurs n'auront pas l'option de **Sign Out (Se déconnecter)** de l'application GlobalProtect s'ils s'authentifient avec succès à l'aide d'un certificat client uniquement.*

Pour un profil de configuration d'agent qui spécifie les certificats client, chaque utilisateur reçoit un certificat client. Le mécanisme de fourniture des certificats détermine si un certificat est unique à chaque utilisateur ou s'il est identique pour tous les utilisateurs sous cette configuration de l'agent :

- Pour déployer des certificats clients uniques à chaque utilisateur et point de terminaison, utilisez **SCEP**. Lorsqu'un utilisateur se connecte pour la première fois, le portail demande un certificat de l'ICP de l'entreprise. Le portail obtient un certificat unique et le déploie au point de terminaison.
- Pour déployer le même certificat client à tous les utilisateurs qui reçoivent une configuration d'agent, déployez un certificat **Local (Local)** au pare-feu.

Utilisez un profil de certificat facultatif pour vérifier le certificat client qu'un point de terminaison présente avec une demande de connexion. Le profil de certificat spécifie le contenu des champs nom d'utilisateur et domaine utilisateur ; répertorie les certificats d'AC ; critères de blocage d'une session ; et offre des manières de déterminer l'état de révocation des certificats d'AC. Étant donné que le certificat fait partie de l'authentification du point de terminaison ou de l'utilisateur pour une nouvelle session, vous devez pré-déployer les certificats utilisés dans les profils de certificats sur les points de terminaison avant la connexion initiale au portail des utilisateurs.

Le profil de certificat spécifie quel champ de certificat contient le nom d'utilisateur. Si le profil de certificat indique Sujet dans le champ Nom d'utilisateur, le certificat présenté par le point de terminaison doit contenir un nom commun pour que le point de terminaison puisse se connecter.

 ©2026 Palo Alto Networks, Inc.

Si le profil de certificat indique Sujet-Alt avec un Email ou un nom principal pour le champ Nom d'utilisateur, le certificat présenté par le point de terminaison doit contenir les champs correspondants, qui seront utilisés pour le nom d'utilisateur lorsque l'application GlobalProtect s'authentifie sur le portail ou la passerelle.

GlobalProtect prend également en charge l'authentification par les cartes d'accès communes (CAC) et les cartes à puce, qui reposent sur un profil de certificat. Dans ce cas, le profil de certificat doit contenir le certificat AC racine qui a généré le certificat dans la carte à puce intelligente ou CAC.

Si vous précisez l'authentification du certificat client, vous ne devez pas configurer un certificat client dans la configuration du portail, car le point de terminaison le fournit lorsque l'utilisateur se connecte. Pour obtenir un exemple de configuration de l'authentification du certificat client, consultez la section VPN d'accès à distance (profil de certificat).

Les méthodes de déploiement de certificats clients dépendent des exigences de sécurité pour votre organisation :

- Déployer des certificats clients partagés pour l'authentification
- Déployer des certificats d'ordinateur pour l'authentification
- Déployer des certificats clients spécifiques à l'utilisateur pour l'authentification
- Activer la prise en charge du magasin de certificats natif pour GlobalProtect
- Activer la sélection des certificats en fonction de l'OID

Déployer des certificats clients partagés pour l'authentification

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour confirmer qu'un utilisateur de point de terminaison appartient à votre organisation, vous pouvez utiliser le même certificat client pour tous les points de terminaison ou générer des certificats distincts à déployer avec une configuration d'agent spécifique. Utilisez ce workflow pour émettre des certificats clients autosignés et les déployer à partir du portail.

> *Si vous incluez un certificat client dans la configuration du portail pour appareils mobiles, vous ne pouvez utiliser l'authentification par certificat client que dans la configuration de la passerelle car la phrase secrète du certificat client est enregistrée dans la configuration du portail. De plus, le certificat client ne peut être utilisé qu'une fois le certificat récupéré à partir de la configuration du portail.*

 ©2026 Palo Alto Networks, Inc.

1. Générez un certificat à déployer à plusieurs points de terminaison GlobalProtect.
   1. Créer le certificat AC racine pour générer les certificats AC auto-signés pour les composants GlobalProtect.
   2. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Generate (Générez)** un nouveau certificat.
   3. Définissez le **Certificate Type (Type de certificat)** sur **Local** (par défaut).
   4. Saisissez un **Certificate Name (Nom de certificat)**. Ce nom ne peut contenir d'espaces.
   5. Saisissez un **Common Name (Nom commun)** pour identifier ce certificat en tant que certificat d'application (par exemple, **`GP_Windows_App`**). Comme ce certificat sera déployé sur toutes les applications dotées de cette même configuration d'agent, il n'a pas besoin d'identifier de façon unique un utilisateur final ou un système spécifique.
   6. Dans le champ **Signed By (Signé par)**, sélectionnez votre AC racine.
   7. Sélectionnez un **OCSP Responder (répondeur OCSP)** pour vérifier l'état de révocation des certificats.
   8. Cliquez sur **OK** pour générer le certificat.
2. Configurer l'authentification à deux facteurs.

   Configurez les paramètres d'authentification dans une configuration d'agent de portail GlobalProtect pour permettre au portail de déployer de manière transparente le certificat client **Local** au pare-feu pour les applications qui reçoivent la configuration.

Déployer des certificats d'ordinateur pour l'authentification

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour valider le fait que le système client appartienne à votre organisation : utilisez votre propre infrastructure à clés publiques (PKI) pour générer et distribuer les certificats machines sur chaque système client (recommandé) ou générez un certificat de machine auto-signé pour l'exporter. Avec les méthodes de pré-connexion, un certificat de machine est requis et doit être installé sur le point de terminaison avant que les composantes GlobalProtect n'accordent l'accès.

Pour confirmer que le point de terminaison appartient à votre organisation, vous devez également configurer un profil d'authentification pour authentifier l'utilisateur (voir la section Authentification à deux facteurs).

Utilisez le flux de travail suivant pour créer le certificat client et le déployer manuellement dans un point de terminaison. Pour plus d'informations, consultez la rubrique authentification de l'utilisateur GlobalProtect. Pour obtenir un exemple de configuration, consultez accès distant VPN (profil de certificat).

- Déployer des certificats d'ordinateur pour l'authentification – Panorama

 ©2026 Palo Alto Networks, Inc.

- Déployer des certificats d'ordinateur pour l'authentification SCM

Déployer des certificats d'ordinateur pour l'authentification – Panorama

1. Émettez des certificats clients pour les applications GlobalProtect et les points de terminaison.

   Cela permet au portail GlobalProtect et aux passerelles de valider que le point de terminaison appartient à votre organisation.

   1. Créez le certificat CA racine pour générer les certificats auto-signés pour les composants GlobalProtect.
   2. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphériques)**, puis cliquez sur **Generate (Générer)**.
   3. Saisissez un **Certificate Name (Nom de certificat)**. Le nom du certificat ne peut pas contenir d'espaces.
   4. Saisissez l'adresse IP ou le FQDN qui apparaîtra sur le certificat dans le champ **Common Name (Nom commun)**.
   5. Sélectionnez votre AC racine dans la liste déroulante **Signed By (Signé par)**.
   6. Sélectionnez un **OCSP Responder (répondeur OCSP)** pour vérifier l'état de révocation des certificats.
   7. Configurez les **Cryptographic Settings (Paramètres cryptographiques)** du certificat, y compris l'**Algorithm (Algorithme)** de chiffrement, la longueur de clé (**Number of Bits (Nombre de bits)**), le **Digest (Résumé)** de l'algorithme (utilisez SHA1, SHA256 ou SHA384 ou SHA512) et l'**Expiration (expiration)** (en jours) pour le certificat.

      Si le pare-feu est en mode FIPS-CC et que l'algorithme de génération de clé est RSA, les clés RSA doivent comporter 2 048 ou 3 072 bits.
   8. Dans la zone **Certificate Attributes (Attributs du certificat)**, **Add (Ajoutez)** et définissez les attributs qui identifient de façon unique les points de terminaison comme appartenant à votre organisation. N'oubliez pas que si vous ajoutez un attribut **Host Name (Nom d'hôte)** (qui renseigne le champ SAN du certificat), il doit correspondre exactement à la valeur de **Common Name (Nom commun)** que vous avez définie.
   9. Cliquez sur **OK** pour générer le certificat.

 ©2026 Palo Alto Networks, Inc.

2. Installez les certificats dans le magasin de certificats personnel sur les points d'extrémité.

Si vous utilisez des certificats d'utilisateur unique ou des certificats d'ordinateurs uniques, vous devez installer chaque certificat dans le magasin de certificats personnel sur le terminal avant le premier portail ou la connexion de passerelle.

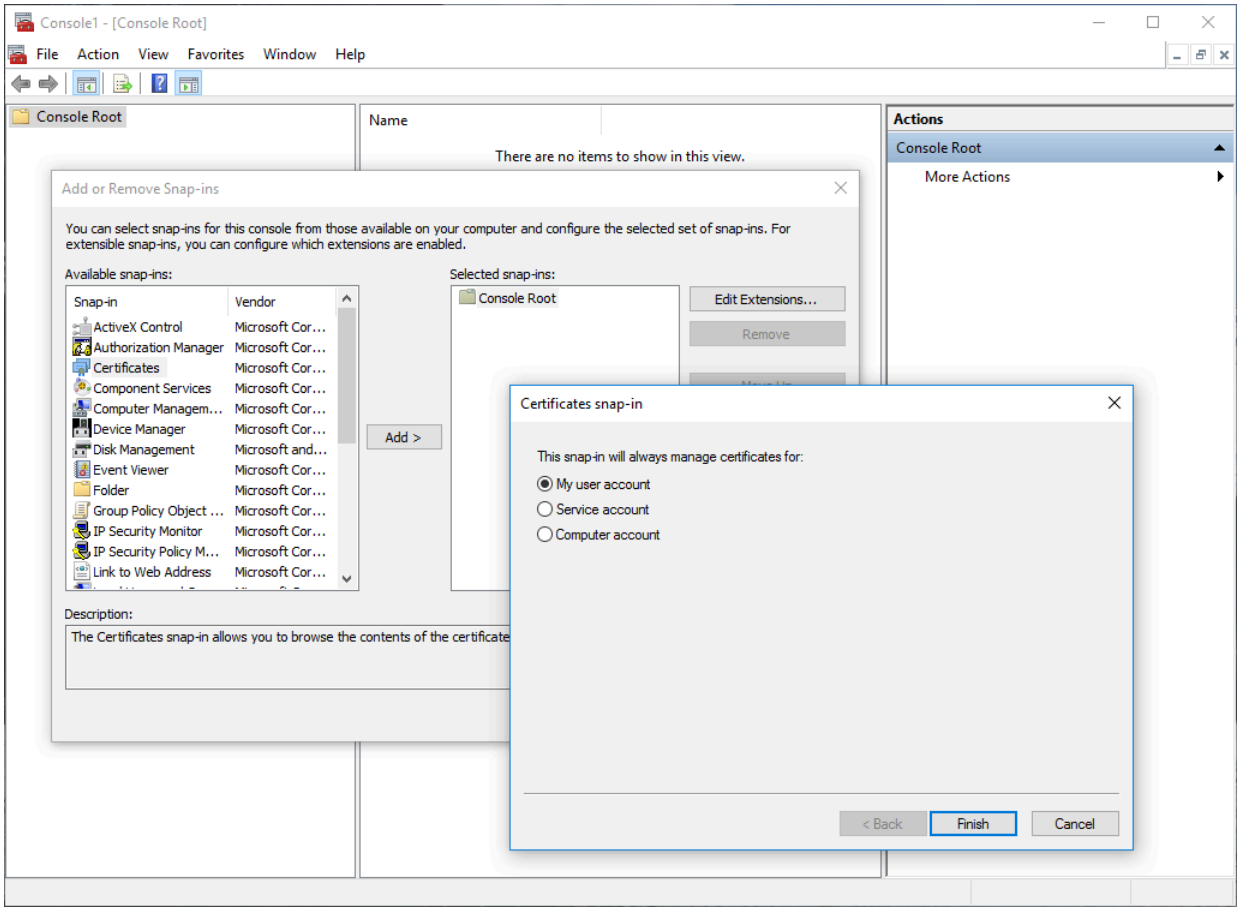
- **Windows** : installez les certificats d'ordinateur dans le magasin de certificats de l'ordinateur local et installez les certificats d'utilisateur dans le magasin de certificats de l'utilisateur actuel.
- **macOS** : installez les certificats d'ordinateur dans le trousseau système et installez les certificats d'utilisateur dans le trousseau sur macOS.
- **Linux** : si vous utilisez le Moteur d'identité sur le cloud pour l'authentification, importez le certificat client dans tous les navigateurs qui accèdent aux pages web nécessitant une authentification.

Par exemple, pour installer un certificat sur un système Windows utilisant la Console de gestion Microsoft :

1. Depuis l'invite de commande, saisissez `mmc` pour lancer la console de gestion de Microsoft.
2. Sélectionnez **File (Fichier)** > **Add/Remove Snap-in (Ajouter / Supprimer un composant logiciel enfichable)**.
3. Dans la liste des **Available snap-ins (Composants logiciels enfichables disponibles)**, sélectionnez **Certificates (Certificats)**, puis **Add (Ajoutez)** et sélectionnez l'un des composants logiciels enfichables de certificat suivants, selon le type de certificat que vous importez :
   - **Computer account (Compte ordinateur)** : Sélectionnez cette option si vous importez un certificat machine.

 ©2026 Palo Alto Networks, Inc.

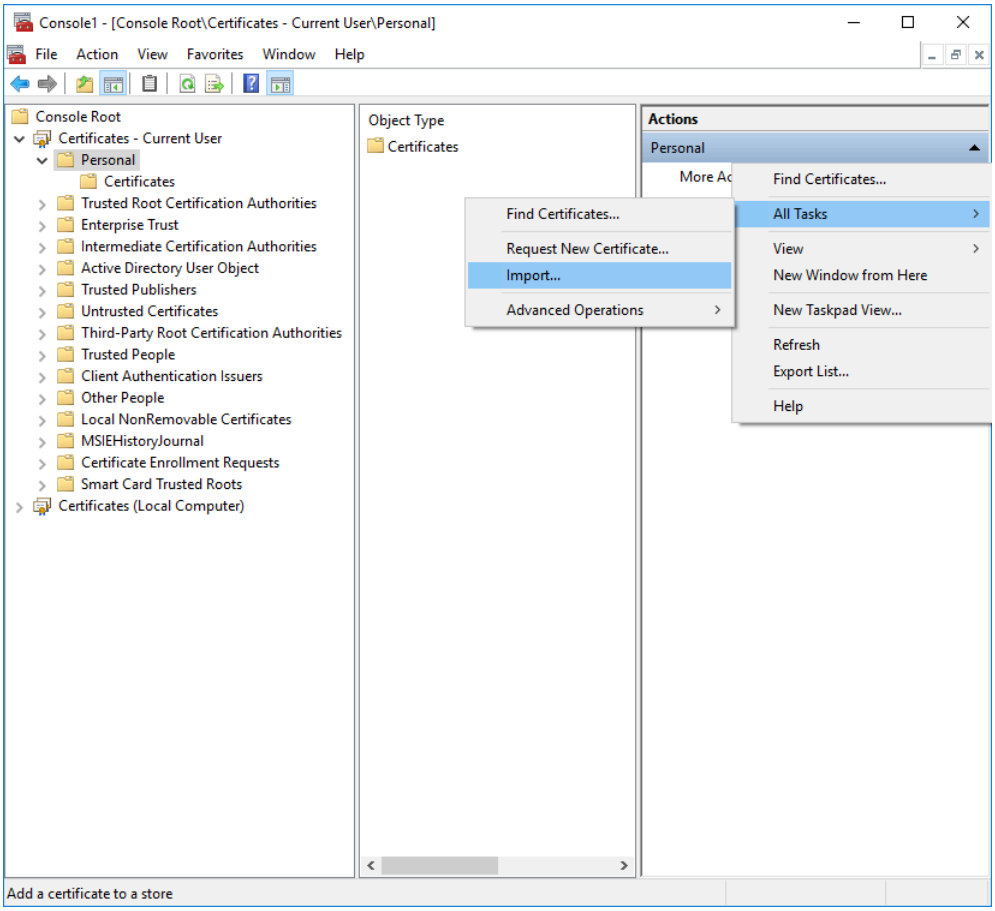
- **My user account (Mon compte utilisateur)** : Sélectionnez cette option si vous importez un certificat utilisateur.



4. À partir de la **Console Root (Racine de la console)**, développez les **Certificates (Certificats)**, puis sélectionnez **Personal (Personnel)**.
5. Dans la colonne **Actions**, sélectionnez **Personal (Personnel)** > **More Actions (Plus d'actions)** > **All Tasks (Toutes les tâches)** > **Import (Importer)** et suivez les étapes de

 ©2026 Palo Alto Networks, Inc.

l'Assistant d'importation de certificats pour importer le fichier PKCS que vous avez reçu de l'autorité de certification.

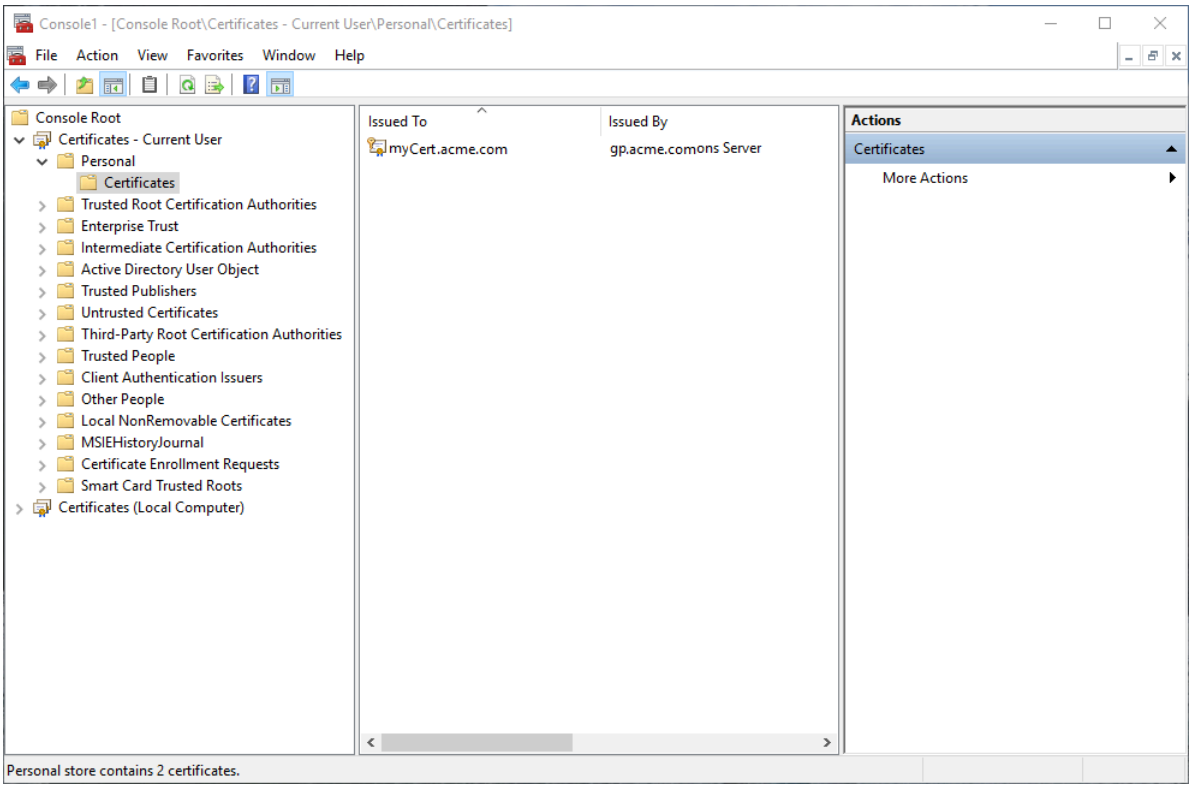


6. **Browse (Naviguez)** jusqu'au fichier de certificat .p12 et sélectionnez-le pour l'importer (sélectionnez **Personal Information Exchange (Échange d'informations personnelles)** pour le type de fichier recherché par la navigation) et saisissez le **Password (Mot de passe)** que vous avez utilisé pour coder la clé privée. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.

 ©2026 Palo Alto Networks, Inc.

3. Vérifiez que le certificat a été ajouté au magasin de certificats personnels.

Accédez au magasin de certificats personnels à partir de la **Console Root (Racine de la console)** (**Certificates (Certifcats)** > **Personal (Personnel)** > **Certificates (Certificats)** :



4. Importez le certificat AC racine utilisé pour générer les certificats clients sur le pare-feu.

Cette étape est requise uniquement si une autorité de certification externe a émis les certificats clients, telles qu'une autorité de certification publique ou une AC CPI d'entreprise.

 ©2026 Palo Alto Networks, Inc.

Si vous utilisez des certificats auto-signés, l'AC racine a déjà été validée par le portail/la passerelle comme AC de confiance.

1. Téléchargez le certificat AC racine utilisé pour générer les certificats clients (au format Base64).
2. Importez le certificat AC racine à partir de l'AC ayant généré les certificats clients sur le pare-feu :
    1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Import (Importer)**.
    2. Définissez le **Certificate Type (Type de certificat)** sur **Local** (par défaut).
    3. Saisissez un **Certificate Name (Nom de certificat)** qui identifie le certificat comme étant votre certificat CA client.
    4. **Browse (Accédez)** au **Certificate File (Fichier du certificat)** que vous avez téléchargé de l'AC, puis sélectionnez-le.
    5. Définissez le **File Format (Format du fichier)** sur **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))**, puis cliquez sur **OK**.
    6. À l'onglet **Device Certificates (Certificats de périphérique)**, sélectionnez le certificat que vous venez d'importer pour ouvrir les Informations sur le certificat.
    7. Sélectionnez **Trusted Root CA (CA racine de confiance)**, puis cliquez sur **OK**.

5. Créer un profil de certificat client.
    1. Sélectionnez **Device (Périphérique)** > **Certificates (Certificats)** > **Certificate Management (Gestion de Certificats)** > **Certificate Profile (Profil de certificat)** pour **Add (Ajouter)** un nouveau profil de certificat.
    2. Saisissez un **Name (Nom)** de profil.
    3. Sélectionnez une valeur de **Username Field (Champ Nom d'utilisateur)** pour indiquer le champ dans le certificat qui contiendra les informations d'identification de l'utilisateur.

        Si vous prévoyez de configurer le portail ou les passerelles pour authentifier les utilisateurs avec des certificats uniquement, vous devez spécifier le **Username Field (Champ Nom d'utilisateur)** . Cela permet à GlobalProtect d'associer un nom d'utilisateur au certificat.

        Si vous prévoyez de configurer le portail ou la passerelle pour l'authentification à deux facteurs, vous pouvez laisser la valeur par défaut de **None (Aucun)**, ou, pour ajouter une couche supplémentaire de sécurité, spécifiez un nom d'utilisateur. Si vous spécifiez un nom d'utilisateur, votre service d'authentification externe vérifie que le nom d'utilisateur du certificat client correspond au nom d'utilisateur que demande l'authentification. Cela garantit que l'utilisateur est celui auquel le certificat a été délivré.

        Les utilisateurs ne peuvent pas modifier le nom d'utilisateur qui est inclus dans le certificat.
    4. Dans la zone **CA Certificates (Certificats AC)**, cliquez sur **Add (Ajouter)**. Sélectionnez le certificat de l'autorité de certification racine de confiance que vous avez importé à l'étape 4 dans le menu déroulant **CA Certificate (Certificat de l'autorité de certification)**, puis cliquez sur **OK**.

 ©2026 Palo Alto Networks, Inc.

6. Enregistrer la configuration.

   Validez les modifications.

Déployer des certificats d'ordinateur pour l'authentification SCM

1. Émettez des certificats clients pour les applications GlobalProtect et les points de terminaison.

   Cela permet au portail GlobalProtect et aux passerelles de valider que le point de terminaison appartient à votre organisation.

   1. Créer le certificat AC racine pour générer les certificats AC auto-signés pour les composants GlobalProtect.
   2. Sélectionnez **Manage Configuration (Gérer la configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)**, puis cliquez sur **Generate (Générer)**.
   3. Saisissez un **Certificate Name (Nom de certificat)**. Le nom du certificat ne peut pas contenir d'espaces.
   4. Sélectionnez votre AC racine dans la liste déroulante **Signed By (Signé par)**.
   5. Configurez les **Cryptographic Settings (Paramètres cryptographiques)** du certificat, y compris l'**Algorithm (Algorithme)** de chiffrement, la longueur de clé (**Number of Bits (Nombre de bits)**), le **Digest (Résumé)** de l'algorithme (utilisez SHA1, SHA256 ou SHA384 ou SHA512) et l'**Expiration (expiration)** (en jours) pour le certificat.

      Si le pare-feu est en mode FIPS-CC et que l'algorithme de génération de clé est RSA, les clés RSA doivent comporter 2 048 ou 3 072 bits.
   6. Dans la zone **Certificate Attributes (Attributs du certificat)**, **Add (Ajoutez)** et définissez les attributs qui identifient de façon unique les points de terminaison comme appartenant à votre organisation. N'oubliez pas que si vous ajoutez un attribut **Host Name (Nom d'hôte)** (qui renseigne le champ SAN du certificat), il doit correspondre exactement à la valeur de **Common Name (Nom commun)** que vous avez définie.
   7. Sélectionnez un **OCSP Responder (répondeur OCSP)** pour vérifier l'état de révocation des certificats.
   8. Cliquez sur **Save (Enregistrer)** pour générer le certificat.

 ©2026 Palo Alto Networks, Inc.

2. Installez les certificats dans le magasin de certificats personnel sur les points d'extrémité.

Si vous utilisez des certificats d'utilisateur unique ou des certificats d'ordinateurs uniques, vous devez installer chaque certificat dans le magasin de certificats personnel sur le terminal avant le premier portail ou la connexion de passerelle.

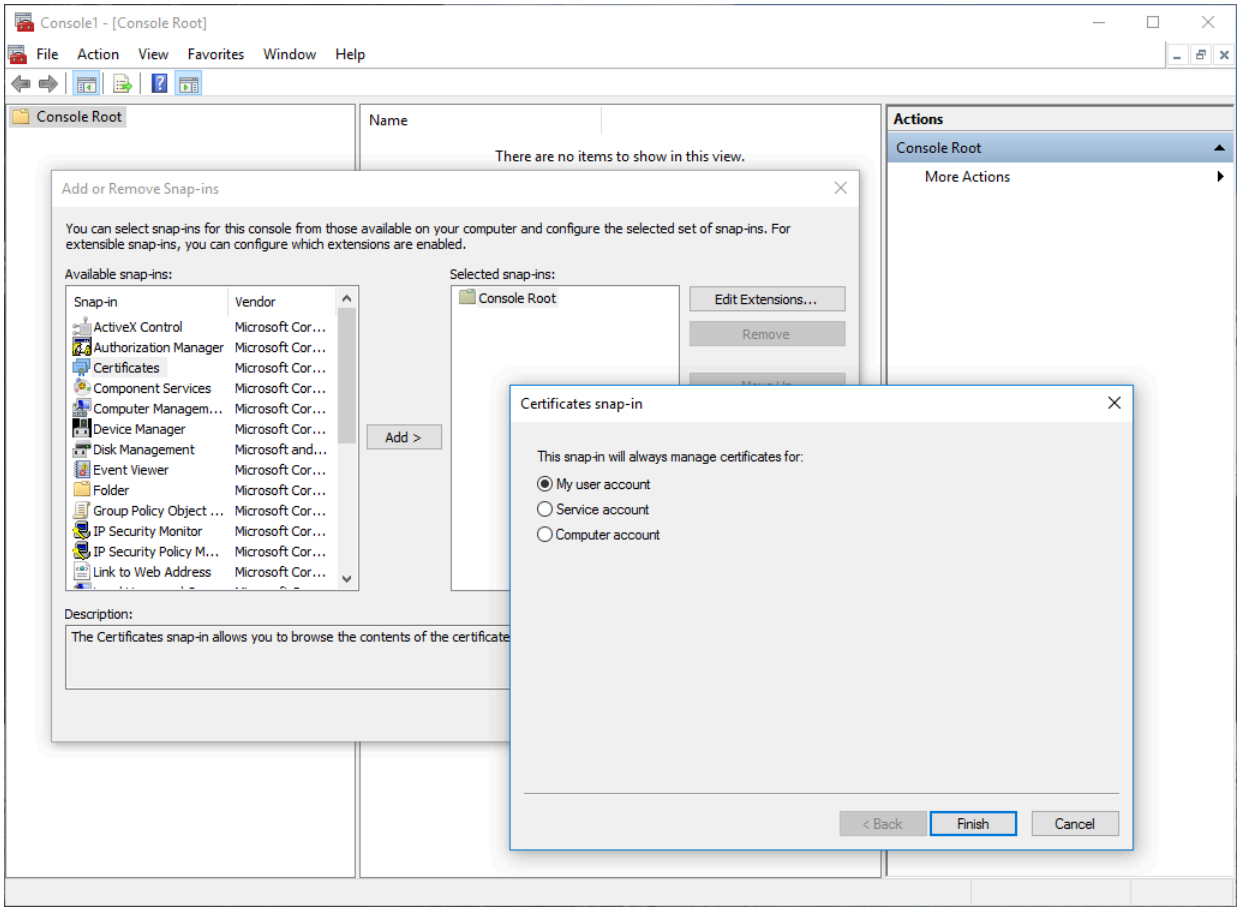
- **Windows** : installez les certificats d'ordinateur dans le magasin de certificats de l'ordinateur local et installez les certificats d'utilisateur dans le magasin de certificats de l'utilisateur actuel.
- **macOS** : installez les certificats d'ordinateur dans le trousseau système et installez les certificats d'utilisateur dans le trousseau sur macOS.
- **Linux** : si vous utilisez le Moteur d'identité sur le cloud pour l'authentification, importez le certificat client dans tous les navigateurs qui accèdent aux pages web nécessitant une authentification.

Par exemple, pour installer un certificat sur un système Windows utilisant la Console de gestion Microsoft :

1. Depuis l'invite de commande, saisissez `mmc` pour lancer la console de gestion de Microsoft.
2. Sélectionnez **File (Fichier)** > **Add/Remove Snap-in (Ajouter / Supprimer un composant logiciel enfichable)**.
3. Dans la liste des **Available snap-ins (Composants logiciels enfichables disponibles)**, sélectionnez **Certificates (Certificats)**, puis **Add (Ajoutez)** et sélectionnez l'un des composants logiciels enfichables de certificat suivants, selon le type de certificat que vous importez :
   - **Computer account (Compte ordinateur)** : Sélectionnez cette option si vous importez un certificat machine.

 ©2026 Palo Alto Networks, Inc.

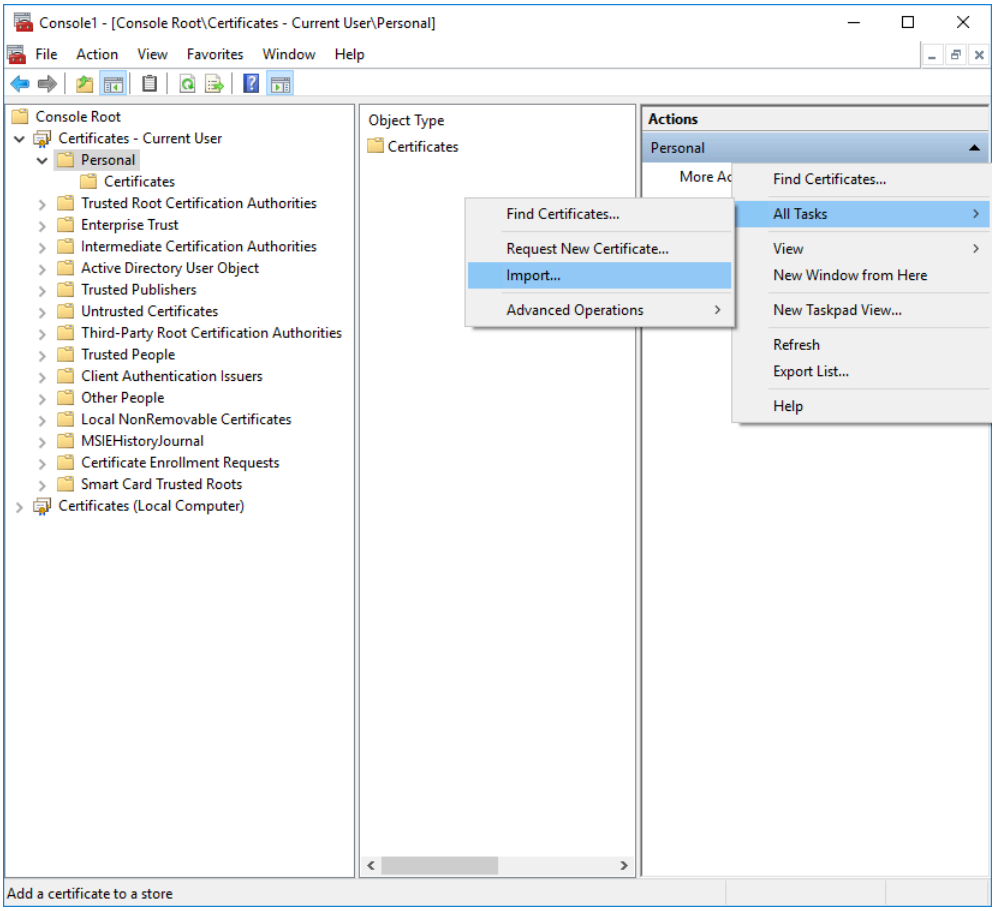
- **My user account (Mon compte utilisateur)** : Sélectionnez cette option si vous importez un certificat utilisateur.



4. À partir de la **Console Root (Racine de la console)**, développez les **Certificates (Certificats)**, puis sélectionnez **Personal (Personnel)**.
5. Dans la colonne **Actions**, sélectionnez **Personal (Personnel)** > **More Actions (Plus d'actions)** > **All Tasks (Toutes les tâches)** > **Import (Importer)** et suivez les étapes de

 ©2026 Palo Alto Networks, Inc.

l'Assistant d'importation de certificats pour importer le fichier PKCS que vous avez reçu de l'autorité de certification.

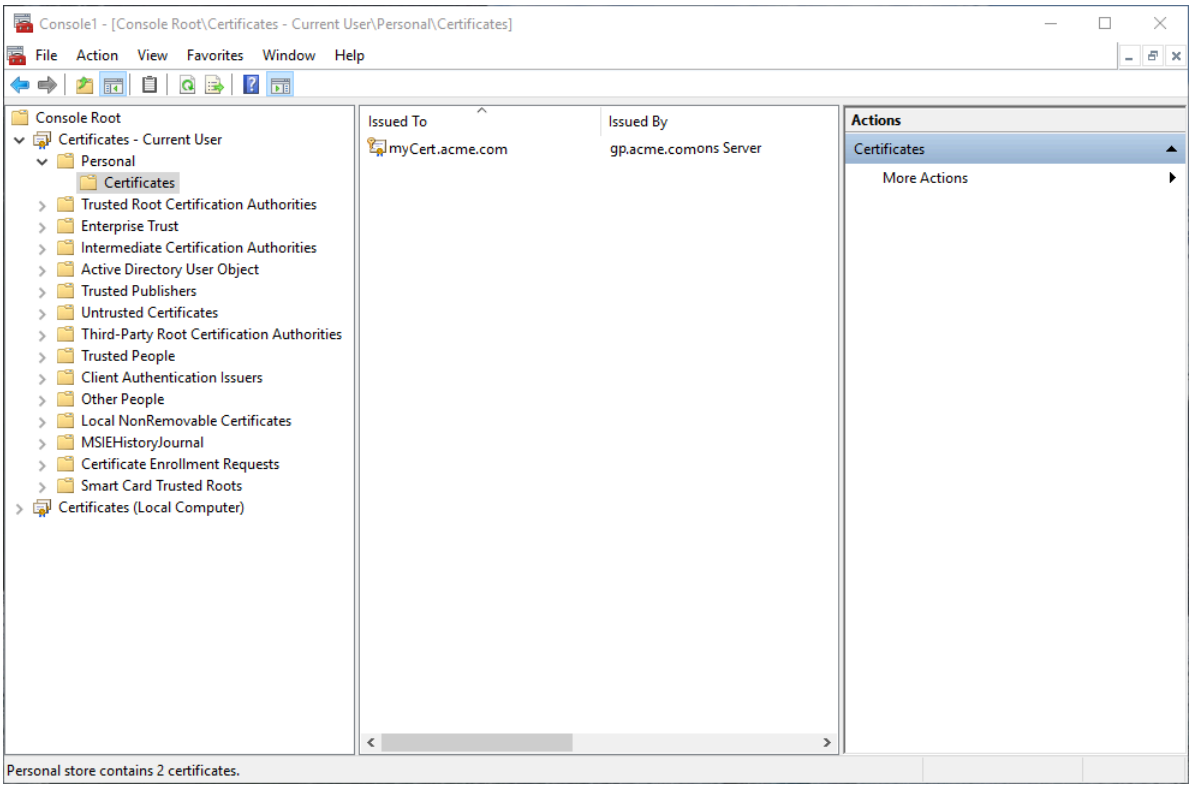


6. **Browse (Naviguez)** jusqu'au fichier de certificat .p12 et sélectionnez-le pour l'importer (sélectionnez **Personal Information Exchange (Échange d'informations personnelles)** pour le type de fichier recherché par la navigation) et saisissez le **Password (Mot de passe)** que vous avez utilisé pour coder la clé privée. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.

 ©2026 Palo Alto Networks, Inc.

3. Vérifiez que le certificat a été ajouté au magasin de certificats personnels.

Accédez au magasin de certificats personnels à partir de la **Console Root (Racine de la console)** (**Certificates (Certifcats)** > **Personal (Personnel)** > **Certificates (Certificats)** :



4. Importez le certificat CA racine utilisé pour générer les certificats clients.

Cette étape est requise uniquement si une autorité de certification externe a émis les certificats clients, telles qu'une autorité de certification publique ou une AC CPI d'entreprise.

 ©2026 Palo Alto Networks, Inc.

Si vous utilisez des certificats auto-signés, l'AC racine a déjà été validée par le portail/la passerelle comme AC de confiance.

1. Téléchargez le certificat AC racine utilisé pour générer les certificats clients (au format Base64).
2. Importez le certificat AC racine à partir de l'AC ayant généré les certificats clients sur le pare-feu :
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis cliquez sur **Import (Importer)**.
   2. Définissez le **Certificate Type (Type de certificat)** sur **Local** (par défaut).
   3. Saisissez un **Certificate Name (Nom de certificat)** qui identifie le certificat comme étant votre certificat CA client.
   4. **Browse (Accédez)** au **Certificate File (Fichier du certificat)** que vous avez téléchargé de l'AC, puis sélectionnez-le.
   5. Définissez le **File Format (Format du fichier)** sur **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))**, puis cliquez sur **OK**.
   6. À l'onglet **Device Certificates (Certificats de périphérique)**, sélectionnez le certificat que vous venez d'importer pour ouvrir les Informations sur le certificat.
   7. Sélectionnez **Trusted Root CA (CA racine de confiance)**, puis cliquez sur **OK**.

5. Créer un profil de certificat client.
   1. Sélectionnez **Manage Configuration (Gérer la configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)**.
   2. Dans la section Profil de certificat, cliquez sur **Add Profile (Ajouter un profil)**.
   3. Saisissez un **Name (Nom)** de profil.
   4. Sélectionnez une valeur de **Username Field (Champ Nom d'utilisateur)** pour indiquer le champ dans le certificat qui contiendra les informations d'identification de l'utilisateur.

      Si vous prévoyez de configurer le portail ou les passerelles pour authentifier les utilisateurs avec des certificats uniquement, vous devez spécifier le **Username Field (Champ Nom d'utilisateur)** . Cela permet à GlobalProtect d'associer un nom d'utilisateur au certificat.

      Si vous prévoyez de configurer le portail ou la passerelle pour l'authentification à deux facteurs, vous pouvez laisser la valeur par défaut de **None (Aucun)**, ou, pour ajouter une couche supplémentaire de sécurité, spécifiez un nom d'utilisateur. Si vous spécifiez un nom d'utilisateur, votre service d'authentification externe vérifie que le nom d'utilisateur du certificat client correspond au nom d'utilisateur que demande l'authentification. Cela garantit que l'utilisateur est celui auquel le certificat a été délivré.

      Les utilisateurs ne peuvent pas modifier le nom d'utilisateur qui est inclus dans le certificat.
   5. Dans la zone **CA Certificates (Certificats AC)**, cliquez sur **Add (Ajouter)**. Sélectionnez le certificat de l'autorité de certification racine de confiance que vous avez importé à l'étape 4 dans le menu déroulant **CA Certificate (Certificat de l'autorité de certification)**, puis cliquez sur **OK**.

 ©2026 Palo Alto Networks, Inc.

6. Enregistrer la configuration.

   Validez les modifications.

Déployer des certificats clients spécifiques à l'utilisateur pour l'authentification

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour authentifier les utilisateurs individuels : Vous devez générer un certificat client unique pour chaque utilisateur GlobalProtect et les déployer sur les systèmes clients avant d'activer GlobalProtect. Pour automatiser la génération et le déploiement de certificats de clients spécifiques à l'utilisateur, vous pouvez configurer votre portail GlobalProtect pour agir en tant que client SCEP (Simple Certificate Enrollment Protocol) vers un serveur SCEP dans votre CPI d'entreprise.

> *Si vous incluez un certificat client dans la configuration du portail pour appareils mobiles, vous ne pouvez utiliser l'authentification par certificat client que dans la configuration de la passerelle car la phrase secrète du certificat client est enregistrée dans la configuration du portail. De plus, le certificat client ne peut être utilisé qu'une fois le certificat récupéré à partir de la configuration du portail.*

L'opération SCEP est dynamique dans la mesure où la CPI d'entreprise génère un certificat spécifique à l'utilisateur lorsque le portail le demande et envoie le certificat au portail. Le portail déploie ensuite le certificat à l'application de manière transparente. Lorsqu'un utilisateur demande l'accès, l'application peut alors présenter le certificat client pour s'authentifier auprès du portail ou de la passerelle.

Le portail ou la passerelle GlobalProtect utilise des informations d'identification sur le point de terminaison et l'utilisateur pour évaluer s'il faut accorder l'accès à l'utilisateur. GlobalProtect bloque l'accès si l'ID d'hôte est sur une liste de blocage de périphériques ou si la session correspond à toutes les options de blocage spécifiées dans un profil de certificat. Si l'authentification échoue en raison d'un certificat de client SCEP non valide, l'application GlobalProtect essaie d'authentifier avec le portail (selon les paramètres du profil d'authentification) et de récupérer le certificat. Si l'application ne parvient pas à récupérer le certificat à partir du portail, le point de terminaison n'est pas en mesure de se connecter.

1. Créez un profil SCEP.
   1. Choisissez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SCEP**, puis **Add (Ajouter)** un nouveau profil SCEP.
      - Sur Strata Cloud Manager, sélectionnez **Manage Configuration (Gérer la configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects**

 ©2026 Palo Alto Networks, Inc.

(Objets) > **Certificate Management (Gestion des certificats)** puis cliquez sur **Add SCEP (Ajouter SCEP)**.

2. .
3. Saisissez un **Name (Nom)** pour identifier le profil.
4. S'il s'agit du profil d'un pare-feu pouvant prendre en charge de multiples systèmes virtuels, sélectionnez un système virtuel ou sélectionnez l'option **Shared (Partagé)** en tant que **Location (Emplacement)** où le profil est disponible.

2. (Facultatif) Pour rendre la génération de certificats basée sur SCEP plus sécurisée, configurez un mécanisme de réponse au défi SCEP entre l'ICP et le portail pour chaque demande de certificat.

Après avoir configuré ce mécanisme, son fonctionnement est invisible et aucune autre intervention n'est nécessaire.

Pour vous conformer à la norme FIPS (U.S. Federal Information Processing Standard (norme de traitement de l'information fédérale ; FIPS), utilisez un **SCEP Challenge (Mécanisme de recrutement SCEP) Dynamic (Dynamique)** et précisez une **Server URL (URL du serveur)** qui utilise HTTPS (reportez-vous à l'étape 7).

Sélectionnez l'une des options de **Défi SCEP** suivantes :

- **None (Aucune)** (par défaut) : le serveur SCEP n'envoie pas de demande d'authentification au portail avant de générer un certificat.
- **Fixed (Fixe)** : entrez le **Password (Mot de passe)** du mécanisme de recrutement auprès du serveur SCEP dans l'infrastructure PKI.
- **Dynamic (Dynamique)** : indiquez un **Username (Nom d'utilisateur)** et un **Password (Mot de passe)** de votre choix (il peut s'agir des informations d'identification de l'administrateur PKI) et le **Server URL (URL du serveur)** SCEP où le portail/client enverra ces informations d'identification. Les informations d'identification sont utilisées pour s'authentifier auprès du serveur SCEP, qui génère de manière transparente un mot de passe OTP pour le portail lors de chaque demande de certificat (vous pouvez afficher ce changement de OTP après un rafraîchissement de l'écran dans le champ `le mot de passe enrollment challenge est` après chaque demande de certificat). L'ICP transmet au portail de manière transparente chaque nouveau mot de passe. Le portail utilise ensuite le mot de passe pour sa demande de certificat.

3. Spécifiez les paramètres de connexion entre le serveur SCEP et le portail pour permettre au portail de demander et de recevoir des certificats clients.

Vous pouvez inclure des informations supplémentaires sur le point de terminaison ou l'utilisateur en spécifiant des jetons dans le nom du **Subject (sujet)** du certificat.

Dans le champ **Subject (Sujet)** de la CSR vers le serveur SCEP, le portail inclut la valeur de jeton en tant que **CN** et l'ID d'hôte en tant que **SerialNumber (Numéro de série)**. L'ID hôte varie selon le type de point de terminaison : GUID (Windows), MAC adresse de l'interface (macOS),

 ©2026 Palo Alto Networks, Inc.

Android ID (points de terminaison Android), UDID (points de terminaison iOS), ou un nom unique qu'assigne GlobalProtect (Chrome).

1. Dans la zone **Configuration**, saisissez la **Server URL (URL du serveur)** que le portail utilise pour atteindre le serveur SCEP dans la PKI (par exemple, `http://10.200.101.1/certsrv/mscep/`).
2. Saisissez un **CA-IDENT Name (Nom AC-IDENT)** (maximum de 255 caractères) pour identifier le serveur SCEP.
3. Saisissez le nom de **Subject (Sujet)** à utiliser pour les certificats générés par le serveur SCEP. Le sujet doit être un nom différent au format **<attribute>=<value>** et doit inclure l'attribut du nom commun (CN) (CN=<**variable**>). Le CN prend en charge les jetons dynamiques suivants :
   - `$USERNAME` : utilisez ce jeton pour permettre au portail de demander des certificats pour un utilisateur spécifique. Pour utiliser cette variable, vous devez également Activer le mappage de groupe. Le nom d'utilisateur saisi par l'utilisateur doit correspondre au nom figurant dans la table de mappage du groupe d'utilisateurs.
   - `$EMAILADDRESS` : utilisez ce jeton pour demander des certificats associés à une adresse e-mail spécifique. Pour utiliser cette variable, vous devez également Activer le mappage de groupe et configurer les **Mail Attributes (Attributs de messagerie)** dans la section des **Mail Domains (Domaines de messagerie)** du profil de serveur. Si GlobalProtect ne peut pas identifier une adresse e-mail pour l'utilisateur, il génère un identifiant unique et remplit le CN avec cette valeur.
   - `$HOSTID` : pour demander des certificats pour le point de terminaison uniquement, spécifiez le jeton ID d'hôte. Lorsqu'un utilisateur tente de se connecter au portail, le point de terminaison envoie des informations d'identification qui incluent sa valeur d'ID d'hôte.

   Lorsque le portail GlobalProtect applique les paramètres SCEP à l'application, la portion CN du nom du sujet est remplacée par la valeur réelle (nom d'utilisateur, ID d'hôte ou adresse e-mail) du propriétaire du certificat (par exemple, **O=acme,CN=johndoe**).
4. Sélectionnez le **Subject Alternative Name Type (Type de nom alternatif de sujet)**.
   - **RFC 822 Name (Nom RFC 822)** : saisissez le nom de la messagerie dans l'objet du certificat ou l'extension alternative du nom de l'objet.
   - **DNS Name (Nom DNS)** : saisissez le nom DNS utilisé pour évaluer les certificats.
   - **Uniform Resource Identifier (Identificateur de ressource uniforme)** : saisissez le nom de la ressource à partir de laquelle l'application obtient le certificat.
   - **None (Aucun)** : ne spécifiez pas d'attributs pour le certificat.

4. (Facultatif) Configurez les **Cryptographic Settings (Paramètres cryptographiques)** du certificat.

- Sélectionnez le **Number of Bits (Nombre de bits)** (longueur de la clé) pour le certificat.

  Si le pare-feu est en mode FIPS-CC et que l'algorithme de génération de clés est RSA. Les clés RSA doivent être de 2.048 bits ou plus.
- Sélectionnez le **Digest for CSR (Résumé pour CSR)** qui indique l'algorithme de synthèse pour la demande de signature de certificat (CSR) : sha1, sha256, sha384 ou sha512.

 ©2026 Palo Alto Networks, Inc.

5. (Facultatif) Configurez les utilisations autorisées du certificat, soit pour la signature ou le chiffrement.
   - Pour utiliser ce certificat pour la signature, activez la case à cocher **Use as digital signature (Utiliser comme signature numérique)**. Cette option permet au point de terminaison d'utiliser la clé privée dans le certificat pour valider une signature numérique.
   - Pour utiliser ce certificat pour le chiffrement, activez la case à cocher **Use for key encipherment (Utiliser pour le chiffrement des clés)**. Cette option permet à l'application d'utiliser la clé privée dans le certificat dans le but de crypter les données échangées par le biais de la connexion HTTPS établie avec les certificats générés par le serveur SCEP.

6. (Facultatif) Pour veiller à ce que le portail se connecte au bon serveur SCEP, saisissez le **CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**. Obtenez cette empreinte du champ **Thumbprint (Empreinte numérique)** de l'interface du serveur SCEP.
   1. Entrez l'URL de l'interface utilisateur du serveur SCEP (par exemple, **`http: // <hostname or IP>/ CertSrv / mscep_admin /`**).
   2. Copiez l'empreinte numérique et saisissez-la dans le champ **CA Certificate Fingerprint (Empreinte du certificat de l'autorité de certification)**.

7. Activer l'authentification SSL mutuelle entre le serveur SCEP et le portail GlobalProtect. C'est nécessaire pour se conformer à la norme FIPS (Federal Information Processing Standard) des États-Unis.

   L'opération FIPS-CC est indiquée sur la page de connexion du pare-feu et dans la barre d'état du pare-feu.

   Sélectionnez le **CA Certificate (Certificat CA)** racine du serveur SCEP. Vous pouvez activer l'authentification SSL mutuelle entre le serveur SCEP et le portail GlobalProtect en sélectionnant **Client Certificate (Certificat client)**.

8. Enregistrez et validez la configuration.
   1. Cliquez sur **OK** pour enregistrer les paramètres.
   2. **Commit (Validez)** la configuration.

   Le portail tente de demander un certificat CA à l'aide des paramètres du profil SCEP, puis l'enregistre sur le pare-feu hébergeant le portail. En cas de succès, le certificat de l'AC est affiché dans **Device (Périphérique)** > **Certificate Management (Gestion de certificat)** > **Certificates (Certificats)**.

 ©2026 Palo Alto Networks, Inc.

9. (Facultatif) Si le portail ne parvient pas à obtenir le certificat après avoir enregistré le profil SCEP, vous pouvez générer manuellement une demande de signature de certificat (CSR) à partir du portail.
   1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Generate (Générez)** un nouveau certificat.
   2. Sélectionnez **SCEP** comme **Certificate Type (Type de certificat)**.
   3. Saisissez un **Certificate Name (Nom de certificat)**. Ce nom ne peut contenir d'espaces.
   4. Sélectionnez le **SCEP Profile (Profil SCEP)** qui doit servir à l'envoi d'une CSR à la PKI de votre entreprise.
   5. Cliquez sur **OK** pour soumettre la demande et générer le certificat.
10. Configurer l'authentification à deux facteurs.

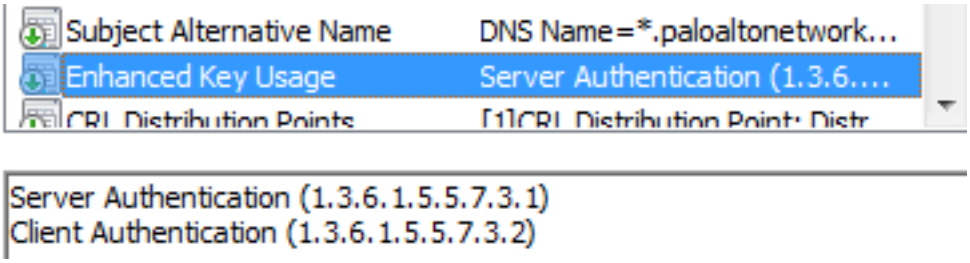
    Attribuez au profil SCEP une configuration d'agent Portail GlobalProtect pour permettre au portail de demander et de déployer des certificats client de manière transparente aux applications qui reçoivent la configuration.

Activer la sélection des certificats en fonction de l'OID

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Si vous déployez plusieurs certificats sur vos périphériques d'utilisateur final pour des cas d'utilisation distincts (par exemple des certificats de machine, des certificats d'utilisateur et des certificats de chiffrement des e-mails tous émis par la même autorité de certification) il peut être difficile de distinguer quel certificat utiliser dans quel cas d'utilisation. Pour vous y aider, vous pouvez désigner un identifiant d'objet (OID) spécifique que vous souhaitez que GlobalProtect utilise pour identifier quel certificat utiliser. Cela simplifie et améliore le processus de sélection des certificats lorsque plusieurs certificats sont installés sur vos terminaux macOS ou Windows.

Un OID est une valeur numérique qui identifie l'application ou le service pour lequel un certificat est utilisé. Lorsque l'autorité de certification (CA) crée le certificat, la CA inclut automatiquement l'IDO dans le champ Utilisation améliorée des clés.



 ©2026 Palo Alto Networks, Inc.

Lorsque vous créez le certificat, vous pouvez spécifier l'IDO pour identifier l'objectif du certificat. Par défaut, GlobalProtect filtre automatiquement les certificats pour ceux qui spécifient un objectif d'authentification client (OID 1.3.6.1.5.5.7.3.2), il n'est donc pas nécessaire de spécifier l'OID associé à l'authentification client. Toutefois, si vous souhaitez utiliser un autre OID pour distinguer le certificat que vous voulez que GlobalProtect sélectionne, vous pouvez spécifier une autre utilisation du certificat lors de sa création, puis demander à GlobalProtect de sélectionner le certificat avec l'OID correspondant. Certains des OID les plus couramment utilisés sont:

- 1.3.6.1.5.5.7.3.1 : Authentification du serveur
- 1.3.6.1.5.5.7.3.3 : Signature de codes
- 1.3.6.1.5.5.7.3.4 : Protection des e-mails
- 1.3.6.1.5.5.7.3.5 : Système terminal IPSec
- 1.3.6.1.5.5.7.3.6 : Tunnel IPsec
- 1.3.6.1.5.5.7.3.7 : Utilisateur IPSec
- 1.3.6.1.5.5.7.3.8 : Horodatage
- 1.3.6.1.5.5.7.3.9 : Signature du PSOC

Par exemple, disons que vos terminaux ont quatre certificats clients installés, mais que celui que vous souhaitez que vos utilisateurs sélectionnent a l'OID 1.3.6.1.5.5.7.3.1. Plutôt que d'avoir l'application GlobalProtect pour présenter les quatre certificats clients à l'utilisateur, vous pouvez spécifier l'**Extended Key Usage OID (OID d'utilisation de clé étendue)** dans la configuration de l'application du portail GlobalProtect pour les utilisateurs dont les terminaux ont plusieurs certificats clients. Gardez à l'esprit que si plusieurs certificats clients sur le terminal ont l'OID correspondant, GlobalProtect invitera l'utilisateur à sélectionner le certificat client dans la liste filtrée.

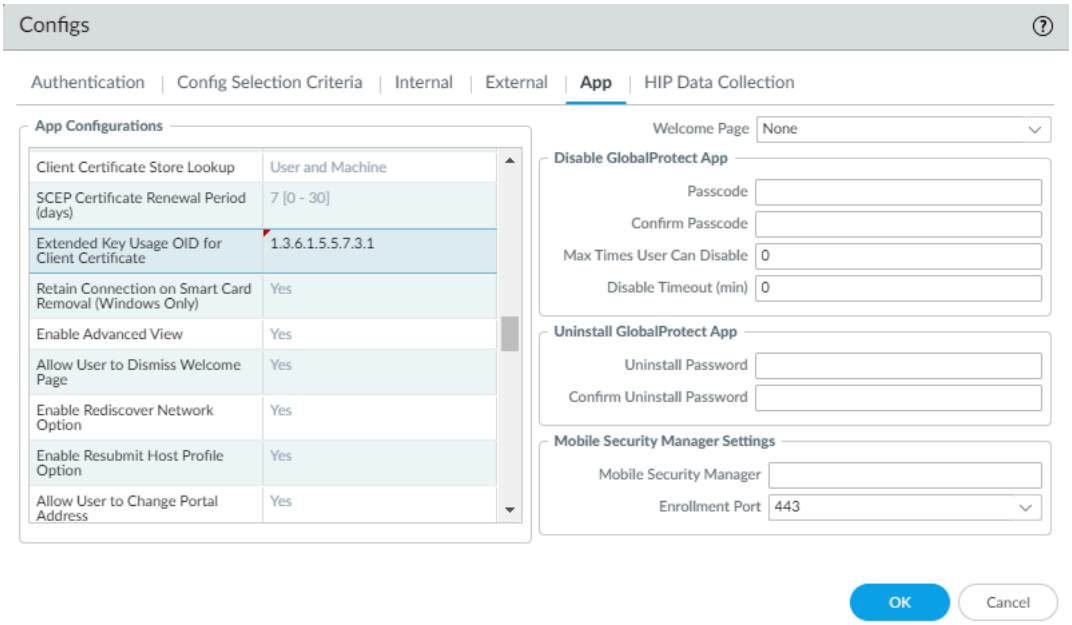
> *GlobalProtect utilise uniquement le champ OID d'utilisation de clé étendue du certificat et n'évalue aucun autre champ de certificat tel que le Nom du sujet pour déterminer si les certificats doivent être présentés. Notez que la valeur de l'OID d'utilisation de clé étendue est différente de l'OID d'informations sur le modèle de certificat. Pour les autres exigences de sélection de certificats, consultez* Comment l'application sait-elle quel certificat elle doit fournir ?

Pour configurer l'OID en tant qu'exigence pour la sélection des certificats :

1. (Facultatif) Créez ou modifiez le certificat client et notez l'OID associé.
   1. Ouvrez le composant logiciel enfichable Modèles de certificat.
   2. Dans le volet Détails, créez ou modifiez le modèle de certificat à modifier, puis cliquez sur Propriétés.
   3. Sous l'onglet **Extensions**, sélectionnez **Application Policies (Politiques d'application)** > **Edit (Modifier)**.
   4. Dans la boîte de dialogue Modifier l'extension des politiques d'application, cliquez sur **Add (Ajouter)**.
   5. Dans Ajouter une stratégie d'application, assurez-vous que l'application que vous créez n'existe pas déjà, puis cliquez sur **New (Nouveau)**.
   6. Dans la boîte de dialogue Nouvelle stratégie d'application, indiquez le nom de la nouvelle stratégie d'application (par exemple Authentification GlobalProtect).
   7. Notez l'identifiant d'objet généré, puis cliquez sur **OK**.

 ©2026 Palo Alto Networks, Inc.

2. Spécifiez l'identifiant d'objet (OID) du certificat dans le champ OID d'utilisation de clé étendue dans le cadre de la configuration d'application appropriée du portail GlobalProtect.



Prise en charge du magasin de certificats natif pour Prisma Access et l'application GlobalProtect sur les terminaux Linux

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Terminaux Linux uniquement	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect 6.2 ou ultérieure

La prise en charge du magasin de certificats natif permet à l'application GlobalProtect installée sur les terminaux Linux d'utiliser des certificats du magasin de certificats pour :

- Authentification par certificat client au portail et à la passerelle
- Rapports sur les journaux de l'application GlobalProtect

Auparavant, l'application GlobalProtect utilisait les certificats clients installés à l'aide de la commande CLI GlobalProtect, qui n'est disponible que dans le répertoire de fichiers `/opt/paloaltonetworks/globalprotect/` sur les terminaux Linux.

Pour configurer l'application GlobalProtect afin d'utiliser le certificat dans le magasin de certificats natif, vous devez :

 ©2026 Palo Alto Networks, Inc.

1. Placez le certificat dans l'emplacement du magasin natif.

   Par exemple :

   ```
   sudo cp xxxxx.cert.pem /etc/ssl/certs
   sudo cp xxxxx.key.pem /etc/ssl/private
   ```

   Les emplacements du magasin de certificats pour diverses plateformes Linux sont :

   - **Ubuntu** :
     - Certificat : `/etc/ssl/certs`
     - Clé : `/etc/ssl/private`
   - **Fedora** :
     - Certificat : `/etc/ssl/certs`
     - Clé : `/etc/ssl/private`
   - **Red Hat**
     - Certificat : `/etc/pki/tls/certs`
     - Clé : `/etc/pki/tls/private`

   Les formats pris en charge sont :

   - `.pem`
   - `.p12`
     - *Lorsque le certificat est au format `.pem`, il sera sur l'emplacement `/etc/ssl/certs` et la clé dans l'emplacement `/etc/ssl/private`. Le fichier clé dans `/etc/ssl/private` peut être au format `.pem` ou `.key`*
     - *Lorsque le certificat est au format `.p12`, le format contient déjà la clé et il n'y aura qu'un certificat contenant la clé dans l'emplacement `/etc/ssl/certs`.*

   L'accès racine est requis pour placer le certificat en utilisant la commande `sudo cp` dans les emplacements mentionnés à l'étape 1 pour diverses plateformes Linux, par exemple, pour Ubuntu :

   ```
   testuser@testuser-virtual-machine:~$ sudo cp www.example.com.cert.pem /etc/ssl/certs/
   testuser@testuser-virtual-machine:~$ sudo cp www.example.com.key.pem /etc/ssl/private/
   testuser@testuser-virtual-machine:~$ ls /etc/ssl/certs/www.example.com.cert.pem
   /etc/ssl/certs/www.example.com.cert.pem
   testuser@testuser-virtual-machine:~$ sudo ls www.example.com.key.pem /etc/ssl/private/
   www.example.com.key.pem
   ```

2. (Facultatif) Stockez la clé dans le `/etc/ssl/private dossier` si le certificat est au format `.pem`.

3. Connectez-vous à GlobalProtect, sélectionnez votre certificat client et procédez aux étapes suivantes. Les utilisateurs finaux doivent entrer le code d'accès pour s'authentifier à l'application pour la première fois. L'application ne demandera pas aux utilisateurs finaux

 ©2026 Palo Alto Networks, Inc.

d'entrer le code d'accès pour les tentatives d'authentification suivantes, sauf si l'application est désinstallée ou si l'utilisateur se déconnecte de GlobalProtect depuis le portail.

Si le format de certificat utilisé est `.pem` et qu'il y a plus d'un certificat correspondant aux critères, l'application GlobalProtect filtre les certificats et affiche la liste des certificats dans la fenêtre contextuelle de sélection de certificat. Pour que la fenêtre contextuelle de sélection de certificat affiche le certificat dans la liste, elle doit ;

- Correspondre à la liste CA
- Correspondre à l'OID d'authentification client
- Ne pas être dans l'état `En attente` ou `Expiré`.

Si le format utilisé est `.p12`, l'application ne filtre pas les certificats et la fenêtre contextuelle de sélection de certificat affiche tous les certificats.

Scénario de mise à niveau :

- Lorsque vous utilisez l'authentification par certificat client et que vous mettez à niveau vers la version 6.2.0 de l'application GlobalProtect, vous devez redémarrer votre système après une mise à niveau réussie.

 ©2026 Palo Alto Networks, Inc.

Configurer l'authentification à deux facteurs

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Si vous avez besoin d'une authentification forte pour protéger les actifs sensibles ou pour respecter des exigences réglementaires, telles que PCI, SOx ou HIPAA, configurez GlobalProtect pour utiliser un service d'authentification qui utilise un schéma d'authentification à deux facteurs. Un schéma d'authentification à deux facteurs implique deux éléments : un élément que l'utilisateur final connaît (tel qu'un numéro d'identification personnel (PIN) ou un mot de passe) et un élément que l'utilisateur final possède (un jeton matériel ou logiciel /MPUU, une carte à puce intelligente, ou un certificat). Vous pouvez également activer l'authentification à deux facteurs à l'aide d'une combinaison de services d'authentification externe et de profils de clients et de certificats.

> *L'authentification à deux facteurs prend en charge le* VPN d'accès à distance avec pré-ouverture de session *avec les versions 5.0 ou ultérieures de l'application GlobalProtect.*

Les sections suivantes fournissent des exemples de la configuration de l'authentification à deux facteurs sur GlobalProtect :

- Activer l'authentification à deux facteurs à l'aide de profils de certificat et d'authentification
- Activer l'authentification à deux facteurs basée sur les mots de passe à usage unique (MPUU)
- Activer l'authentification à deux facteurs basée sur les cartes à puce intelligentes
- Activer l'authentification à deux facteurs basée sur une application de jetons logiciels

Activer l'authentification à deux facteurs à l'aide de profils de certificat et d'authentification

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Le flux de travail suivant décrit comment configurer GlobalProtect pour exiger que les utilisateurs s'authentifient à la fois sur un profil de certificat et sur un profil d'authentification. L'utilisateur doit réussir à s'authentifier en utilisant les deux méthodes pour se connecter au portail/à la passerelle. Pour plus d'informations sur cette configuration, consultez VPN d'accès distant avec authentification à deux facteurs.

 ©2026 Palo Alto Networks, Inc.

Si le profil de certificat spécifie un **Username Field (Champ nom d'utilisateur)** à partir duquel GlobalProtect peut obtenir un nom d'utilisateur, le service d'authentification externe utilise automatiquement le nom d'utilisateur pour authentifier l'utilisateur sur le service d'authentification externe spécifié dans le profil d'authentification. Par exemple, si le **Username Field (Champ nom d'utilisateur)** du profil de certificat est défini comme **Subject (Sujet)**, la valeur dans le champ nom commun du certificat est utilisée comme nom d'utilisateur lorsque le serveur d'authentification essaie d'authentifier l'utilisateur. Si vous ne souhaitez pas forcer les utilisateurs à s'authentifier avec un nom d'utilisateur figurant sur le certificat, veillez à ce que le **Username Field (Champ Nom d'utilisateur)** du profil du certificat soit défini sur **None (Aucun)**. Consultez VPN d'accès distant avec authentification à deux facteurs pour une configuration d'exemple.

1. Créez un profil de serveur de messagerie.

   Le profil du serveur d’authentification détermine la façon dont le pare-feu est connecté à un service d’authentification externe et récupère les informations d’authentification pour vos utilisateurs. Pour plus d’informations sur la création d’un profil de serveur d’authentification, reportez-vous à Configurer l’authentification externe.

2. Créez un profil d'authentification qui identifie le service pour l'authentification des utilisateurs. Vous aurez plus tard l'option d'attribuer le profil sur le portail et sur les passerelles. Pour plus d’informations sur la création d’un profil d’authentification, reportez-vous à Configurer l’authentification externe.

3. Créez un profil de certificat client que le portail utilise pour authentifier les certificats clients qui proviennent de points de terminaison utilisateur.

   Lorsque vous configurez l'authentification à deux facteurs pour utiliser des certificats clients, le service d'authentification externe utilise la valeur UserName pour authentifier l'utilisateur,

 ©2026 Palo Alto Networks, Inc.

s'il est spécifié, dans le certificat client. Cela garantit que l'utilisateur qui ouvre une session est effectivement l'utilisateur pour lequel le certificat a été généré.

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Generate (Générer)** un nouveau certificat.
   - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW et Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** et **Generate (Générer)** un nouveau certificat.
2. Saisissez un **Name (Nom)** pour le profil.
3. Sélectionnez l'une des valeurs de **Usermame Field (Champ Nom d'utilisateur)** suivantes :
   - Si vous souhaitez que le certificat client authentifie les utilisateurs individuels, sélectionnez le champ du certificat qui identifie l'utilisateur.
   - Si vous déployez le certificat client depuis le portail, sélectionnez **None (Aucun)**.
   - Si vous configurez un profil de certificat à utiliser avec la pré-connexion, sélectionnez **None (Aucun)**.
4. **Add (Ajoutez)** les **CA Certificates (Certificats de l'autorité de certification)** que vous voulez affecter au profil, puis configurez les paramètres suivants :
   1. Sélectionnez le **CA certificate (certificat AC)**, soit un certificat d'AC racine approuvée ou le certificat de AC à partir d'un serveur SCEP. Au besoin, importez le certificat.
   2. (Facultatif) Saisissez le **Default OCSP URL (URL OCSP par défaut)**.
   3. (Facultatif) Sélectionnez un certificat pour la **OCSP Verify Certificate (Vérification du certificat par OCSP)**.
   4. (Facultatif – Panorama uniquement) Saisissez un **Template Name (Nom de modèle)** à donner au modèle qui a été utilisé pour signer le certificat.
5. (Facultatif) Sélectionnez les options suivantes pour spécifier le moment où il faut bloquer la session demandée de l'utilisateur :
   1. L'état du certificat est inconnu.
   2. Le composant GlobalProtect ne récupère pas l'état du certificat dans le nombre de secondes dans le délai d'**Certificate Status Timeout (expiration de l'état du certificat)**.
   3. L'attribut de numéro de série dans l'objet d'un certificat client ne correspond pas à l'ID hôte que l'application GlobalProtect signale pour le point de terminaison.
   4. Les certificats sont expirés.
6. Cliquez sur **OK**.

4. (Facultatif) Émettez des certificats clients pour les clients GlobalProtect et les points de terminaison.

Pour déployer de manière transparente les certificats clients, configurez votre portail pour distribuer un certificat de client partagé à vos points de terminaison ou configurez le portail

 ©2026 Palo Alto Networks, Inc.

pour utiliser SCEP afin de demander et de déployer des certificats de clients uniques pour chaque utilisateur.

1. Utilisez votre CPI d'entreprise ou une AC publique pour générer un certificat client unique pour chaque utilisateur GlobalProtect.
2. Pour les méthodes de connexion pré-connexion, installez des certificats dans le magasin de certificats personnel sur le point de terminaison.

5. Enregistrez la configuration GlobalProtect.

Cliquez sur **Commit (Valider)**.

Activer l’authentification à deux facteurs basée sur les mots de passe à usage unique (MPUU)

Utilisez ce workflow pour configurer l'authentification à deux facteurs à l'aide de mots de passe à usage unique (MPUU) sur le portail et les passerelles. Lorsqu'un utilisateur demande l'accès, le portail ou la passerelle invite l'utilisateur à entrer un MPUU. Le service d'authentification envoie le MPUU en guise de jeton au périphérique RSA de l'utilisateur.

La configuration d'un schéma d'authentification à deux facteurs est similaire à la configuration d'autres types d'authentification. Le schéma d’authentification à deux facteurs vous oblige à configurer :

- Un profil serveur (généralement pour un service RADIUS pour l'authentification à deux facteurs) affecté à un profil d'authentification.
- Un profil d'authentification client qui inclut le profil d'authentification pour le service que ces composants utilisent.

Par défaut, l'application fournira les mêmes informations d'identification qu'elle a utilisées pour ouvrir une session sur le portail et la passerelle. Dans le cas de l'authentification basée sur le mot de passe à usage unique, ce comportement provoque initialement l'échec de l'authentification sur la passerelle et, compte tenu du retard que cela cause pour inviter l'utilisateur à effectuer une ouverture de session, le mot de passe à usage unique de l'utilisateur peut expirer. Pour éviter cette situation, vous devez configurer les portails et les passerelles qui demandent le MPUU au lieu d'utiliser les mêmes informations d'identification sur une base de configuration selon l’application.

Vous pouvez également réduire la fréquence à laquelle les utilisateurs sont invités à donner MPUU en configurant une substitution d'authentification. Cela permet aux portails et aux passerelles de générer et d'accepter un cookie crypté sécurisé pour authentifier l'utilisateur pour un laps de temps spécifié. Les portails et/ou passerelles ne nécessitent pas de nouveau MPUU tant que le cookie n’expire pas, ce qui réduit le nombre de fois où les utilisateurs doivent fournir un MPUU.

1. Après avoir configuré le service RADIUS back-end pour générer des jetons pour les MPUU et garantir aux utilisateurs les périphériques nécessaires (comme un jeton matériel), configurez un serveur RADIUS pour interagir avec le pare-feu.

   Pour obtenir des instructions spécifiques, consultez la documentation de votre serveur RADIUS. Dans la plupart des cas, vous devez configurer un agent d'authentification et une configuration client sur le serveur RADIUS pour permettre la communication entre le pare-feu

 ©2026 Palo Alto Networks, Inc.

et le serveur RADIUS. Vous devez également définir le secret partagé à utiliser pour chiffrer des sessions entre le pare-feu et le serveur RADIUS.

2. Sur chaque pare-feu qui héberge les passerelles et / ou le portail, créez un profil de serveur RADIUS. (Pour un petit déploiement, un pare-feu peut héberger le portail et les passerelles.)
   1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils du serveur)** > **RADIUS (RADIUS)**.
   2. **Add (Ajouter)** un nouveau profil.
   3. Saisissez un **Profile Name (nom de profil)** pour ce profil RADIUS.
   4. Dans la zone **Servers (serveurs)**, **Add (ajoutez)** une instance RADIUS, puis entrez les informations suivantes :
      - Un **Name (Nom)** descriptif pour identifier ce Serveur RADIUS.
      - L'adresse IP du **RADIUS Server (Serveur RADIUS)**.
      - Le **Secret** partagé utilisé pour coder les sessions entre le pare-feu et le serveur RADIUS
      - Le numéro du **Port** que le serveur RADIUS utilisera pour l'écoute des demandes d'authentification (par défaut 1812)
   5. Cliquez sur **OK** pour enregistrer le profil.

3. Créez un profil d'authentification.
   1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)** et **Add (ajoutez)** un nouveau profil.
   2. Saisissez un **Name (Nom)** pour le profil. Le nom du certificat ne doit pas contenir d'espace.
   3. Sélectionnez **RADIUS** en tant que **Type** de service d'authentification.
   4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé pour accéder à votre serveur RADIUS.
   5. Saisissez le nom du **User Domain (Domaine utilisateur)**. Le pare-feu utilise cette valeur pour faire correspondre les utilisateurs s'authentifiant aux entrées de la Liste d'autorisations et pour le mappage de groupe User-ID.
   6. Sélectionnez un **Username Modifier (Modificateur du nom d'utilisateur)** pour modifier le format du nom d'utilisateur / domaine attendu par le serveur RADIUS.
   7. Cliquez sur **OK** pour enregistrer le profil d'authentification.

 ©2026 Palo Alto Networks, Inc.

4. Affectez le profil d'authentification à la passerelle et/ou au portail GlobalProtect.

   Vous pouvez configurer plusieurs configurations d'authentification client pour le portail et les passerelles. Pour chaque configuration d'authentification client, vous pouvez spécifier le profil d'authentification à appliquer aux points de terminaison d'un système d'exploitation spécifique.

   Cette étape décrit comment ajouter le profil d'authentification à la configuration de la passerelle ou du portail. Pour plus d'informations sur la configuration de ces composants, voir les sections Portails GlobalProtect et Passerelles GlobalProtect.

   1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** ou **Gateways (Passerelles)**.
   2. Sélectionnez une configuration de portail ou de passerelle existante ou **Add (Ajoutez)**-en une nouvelle. Si vous ajoutez une nouvelle passerelle ou un nouveau portail, spécifiez son nom, son emplacement et ses paramètres réseau.
   3. Sur l'onglet **Authentication (authentification)**, sélectionnez un **SSL/TLS service Profile (Profil de service SSL/TLS)** ou **Add (ajoutez)** un nouveau profil.
   4. Vous devez **Add (Ajouter)** une nouvelle configuration de **Client Authentication (Authentification du client)**, puis configurer les paramètres suivants :
      - Le **Name (Nom)** de la configuration de l'authentification client.
      - Le **OS (Système d'exploitation)** du point de terminaison auquel cette configuration s'applique.
      - Le **Authentication Profile (profil d'authentification)** que vous avez créé à la section Créer un profil d'authentification.
      - (Facultatif) Une **Username Label (Étiquette de nom d'utilisateur)** personnalisée.
      - (Facultatif) Une **Password Label (Étiquette de mot de passe)** personnalisée.
      - (Facultatif) Un **Authentication Message (Message d'authentification)** personnalisé.
   5. Cliquez sur **OK** pour enregistrer la configuration.

5. (Facultatif) Configurez le portail ou la passerelle pour demander un nom d'utilisateur et un mot de passe ou seulement un mot de passe chaque fois que l'utilisateur se connecte. Les mots de passe enregistrés ne sont pas pris en charge avec l'authentification à deux facteurs utilisant des OTP car l'utilisateur doit saisir un mot de passe dynamique chaque fois qu'il s'identifie.

   Cette étape décrit comment configurer le paramètre de mot de passe dans une configuration d'agent Portail. Pour plus d'informations, consultez personnaliser l'application GlobalProtect.

   1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** et sélectionnez une configuration de portail existante.
   2. Dans la boîte de dialogue GlobalProtect Portal Configuration (Configuration du portail GlobalProtect), sélectionnez **Agent**.
   3. Sélectionnez une configuration d'agent existante ou **Add (Ajoutez)**-en une nouvelle.
   4. À l'onglet **Authentication (Authentification)**, définissez l'option **Save User Credentials (Enregistrer les informations)** sur **Save Username Only (Enregistrer le nom d'utilisateur uniquement)** ou sur **No (non)**. Ce paramètre permet à GlobalProtect de demander aux utilisateurs d'indiquer des mots de passe dynamiques pour chaque composant que vous sélectionnez dans l'étape suivante.

 ©2026 Palo Alto Networks, Inc.

5. Cliquez deux fois sur **OK** pour enregistrer la configuration.

6. Sélectionnez les composants GlobalProtect — portail et types de passerelles — qui demandent les mots de passe dynamiques, tels que MPUU.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** et sélectionnez une configuration de portail existante.
   2. Dans la boîte de dialogue GlobalProtect Portal Configuration (Configuration du portail GlobalProtect), sélectionnez **Agent**.
   3. Sélectionnez une configuration d'agent existante ou **Add (Ajoutez)**-en une nouvelle.
   4. À l'onglet **Authentication (authentification)**, sélectionnez les **Components that Require Dynamic Passwords (Two-Factor Authentication) (Composants nécessitant des mots de passe dynamiques (authentification à deux facteurs))**. Lorsqu'il est sélectionné, le portail et / ou les types de passerelles demandent des MPUU.

      Ne sélectionnez pas les Composants nécessitant des mots de passe dynamiques (authentification à deux facteurs).

   5. Cliquez deux fois sur **OK** pour enregistrer la configuration.

7. Si l'authentification unique (SSO) est activée, désactivez-la. Puisque la configuration de l'agent spécifie RADIUS comme service d'authentification, Kerberos SSO n'est pas pris en charge.

   Cette étape décrit comment désactiver SSO. Pour plus d'informations, consultez définir les configurations de l'agent GlobalProtect.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** et sélectionnez une configuration de portail existante.
   2. Dans la boîte de dialogue GlobalProtect Portal Configuration (Configuration du portail GlobalProtect), sélectionnez **Agent**.
   3. Sélectionnez une configuration d'agent existante ou **Add (Ajoutez)**-en une nouvelle.
   4. À l'onglet **App (Application)**, définissez **Use Single Sign-on (Windows Only) (Utiliser l'ouverture de session unique (Windows uniquement))** sur **No (Non)**.
   5. Cliquez deux fois sur **OK** pour enregistrer la configuration.

8. (Facultatif) Pour minimiser le nombre de fois où un utilisateur doit fournir des informations d'identification, configurez une substitution d'authentification.

   Par défaut, le portail ou les passerelles authentifient l'utilisateur avec un profil d'authentification et un profil de certificat facultatif. Avec la substitution d'authentification, le portail ou la passerelle authentifie l'utilisateur avec un cookie crypté qu'il a déployé sur le point de terminaison. Pendant que le cookie est valide, l'utilisateur peut se connecter sans entrer

 ©2026 Palo Alto Networks, Inc.

des informations d'identification régulières ou un MPUU. Pour plus d'informations, consultez Authentification par cookie sur le portail ou la passerelle dans Comment l'application sait-elle quelles sont les informations d'identification elle doit fournir ?.

Si vous devez immédiatement bloquer l'accès à un terminal dont le cookie n'a pas encore expiré (par exemple, si le terminal est perdu ou volé), vous pouvez utiliser Identification et mise en quarantaine du périphérique compromis *en ajoutant ce dernier à une liste de quarantaine.*

Pour plus d'informations, voir Portails GlobalProtect et Passerelles GlobalProtect.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** ou **Gateways (Passerelles)**.
2. Sélectionnez une configuration de portail ou de passerelle existante ou **Add (Ajoutez)**-en une nouvelle.
3. Selon que vous configuriez un portail ou une passerelle, sélectionnez l'une des options suivantes :
   - **Configuration du portail GlobalProtect** : dans la boîte de dialogue GlobalProtect Portal Configuration (Configuration du portail GlobalProtect), sélectionnez **Agent** > ***<agent-config>*** > **Authentication (Authentification)**.
   - **Configuration de la passerelle GlobalProtect** : dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > ***<client-setting>*** > **Authentication Override (Contrôle prioritaire de l'authentification)**.
4. Configurez les paramètres de **Authentication Override (Contrôle prioritaire de l'authentification)** suivants :
   - **Name (Nom)** du contrôle prioritaire de l'authentification.
   - **Generate cookie for authentication override (Générer un cookie pour substituer l'authentification)** : permet au portail ou à la passerelle de générer des cookies chiffrés, spécifiques au point de terminaison. Une fois que les utilisateurs s'authentifient avec succès, le portail ou la passerelle délivre le cookie d'authentification au point de terminaison.

     Le cookie d'authentification comprend les champs suivants :
     - `user (utilisateur)` : le nom d'utilisateur qui est utilisé pour authentifier l'utilisateur.
     - `Domain (Domaine)` : le nom de domaine de l'utilisateur.
     - `os` : le nom de l'application utilisée sur le périphérique.
     - `hostID (ID de l'hôte)` : l'ID unique que GlobalProtect affecte afin d'identifier l'hôte.
     - `gen time (heure de génération)` : la date et l'heure auxquelles l cookie d'authentification a été généré.
     - `ip` : adresse IP du périphérique qui est utilisé pour s'authentifier avec succès sur GlobalProtect et pour obtenir le cookie.
   - **Accept cookie for authentication override (Accepter un cookie pour substituer l'authentification)** : indique au portail ou à la passerelle qu'il ou elle doit

 ©2026 Palo Alto Networks, Inc.

authentifier l'utilisateur avec un cookie crypté valide. Lorsque le point de terminaison présente un cookie valide, le portail ou la passerelle vérifie que le cookie a été crypté par le portail ou la passerelle, décrypte le cookie, puis authentifie l'utilisateur.

L'application GlobalProtect doit connaître le nom d'utilisateur de l'utilisateur qui se connecte afin de faire correspondre et d'extraire les cookies d'authentification associés du point de terminaison de l'utilisateur. Une fois que l'application a extrait les cookies, elle les envoie au portail ou à la passerelle à des fins d'authentification de l'utilisateur.

(Windows uniquement) Si vous réglez l'option Use Single Sign-On (Utiliser l'ouverture de session unique) *sur* ***Yes (Oui)*** *(SSO est activée) dans la configuration d'agent du portail (****Network (Réseau)*** *>* ***GlobalProtect*** *>* ***Portals (Portails)*** *>* ***<portal-config>*** *>* ***Agent*** *>* ***<agent-config>.*** *>* ***App (Appli)****), l'appli GlobalProtect utilise le nom d'utilisateur Windows pour récupérer le cookie d'authentification local pour l'utilisateur. Si vous définissez l'option* ***Use Single Sign-On (Utiliser l'ouverture de session unique)*** *sur* ***No (Non)*** *(la SSO est désactivée), vous devez activer l'application GlobalProtect pour qu'elle* enregistre les informations d'identification de l'utilisateur *pour que l'application retire le cookie d'authentification pour l'utilisateur. Définissez l'option* ***Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)*** *sur* ***Yes (Oui)*** *pour enregistrer le nom d'utilisateur et le mot de passe ou* ***Save Username Only (Enregistrer le nom d'utilisateur uniquement)*** *pour enregistrer uniquement le nom d'utilisateur.*

(macOS uniquement) Comme les points de terminaison macOS ne prennent pas en charge l'ouverture de session unique, vous devez activer l'application GlobalProtect pour qu'elle ***enregistre les informations d'identification de l'utilisateur*** *pour que l'application retire le cookie d'authentification pour l'utilisateur. Définissez l'option* ***Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)*** *sur* ***Yes (Oui)*** *pour enregistrer le nom d'utilisateur et le mot de passe ou* ***Save Username Only (Enregistrer le nom d'utilisateur uniquement)*** *pour enregistrer uniquement le nom d'utilisateur.*

- **Cookie Lifetime (Durée de vie des cookies)** : spécifie les heures, les jours ou les semaines pour lesquelles le témoin est valide. La durée de vie typique est de 24 heures pour les passerelles, qui protègent les informations sensibles, ou 15 jours pour le portail. La plage des heures est de 1 à 72 ; des semaines, 1 – 52 ; et des jours, 1 – 365. Une fois que le cookie expire sur le portail ou sur la passerelle (selon la première occurrence), le portail ou la passerelle invite l'utilisateur à s'authentifier et crypte ultérieurement un nouveau cookie à envoyer au point de terminaison.

  Si vous avez défini la valeur de **Authentication Override Cookie Lifetime (Durée de vie du cookie de remplacement d'authentification)** plus élevée que la **Tunnel Login Lifetime (Durée de vie de la connexion au tunnel)**, examinez les tableaux ci-dessous.

Version PAN-OS	Valeur de durée de vie du cookie
PAN-OS 10.1	Sur les versions PAN-OS 10.1.x, la **Authentication Override Cookie Lifetime (Durée de vie du cookie de remplacement d'authentification)** ne peut pas dépasser la valeur de la **Tunnel Login Lifetime (Durée de vie de la connexion au tunnel)**. Même si vous

 ©2026 Palo Alto Networks, Inc.

Version PAN-OS	Valeur de durée de vie du cookie
	définissez la durée de vie du cookie de remplacement d'authentification comme étant plus élevée, elle restera valide uniquement pendant la durée de vie de la connexion au tunnel.
PAN-OS 10.2	Sur les versions PAN-OS 10.2 à 10.2.13, la **Authentication Override Cookie Lifetime (Durée de vie du cookie de remplacement d'authentification)** peut dépasser la valeur de la **Tunnel Login Lifetime (Durée de vie de la connexion au tunnel)**. Sur les versions PAN-OS 10.2.14 et ultérieures 10.2.x, la **Authentication Override Cookie Lifetime (Durée de vie du cookie de remplacement d'authentification)** ne peut pas dépasser la valeur de la **Tunnel Login Lifetime (Durée de vie de la connexion au tunnel)**. Même si vous définissez la durée de vie du cookie de remplacement d'authentification comme étant plus élevée, elle restera valide uniquement pendant la durée de vie de la connexion au tunnel.
PAN-OS 11.0	Sur les versions PAN-OS 11.0 à 11.0.6, la **Authentication Override Cookie Lifetime (Durée de vie du cookie de remplacement d'authentification)** peut dépasser la valeur de la **Tunnel Login Lifetime (Durée de vie de la connexion au tunnel)**. Sur les versions PAN-OS 11.0.7 et ultérieures 11.0.x, la **Authentication Override Cookie Lifetime (Durée de vie du cookie de remplacement d'authentification)** ne peut pas dépasser la valeur de la **Tunnel Login Lifetime (Durée de vie de la connexion au tunnel)**. Même si vous définissez la durée de vie du cookie de remplacement d'authentification comme étant plus élevée, elle restera valide uniquement pendant la durée de vie de la connexion au tunnel.
PAN-OS 11.1	Sur les versions PAN-OS 11.1.x, la **Authentication Override Cookie Lifetime (Durée de vie du cookie de remplacement d'authentification)** ne peut pas dépasser la valeur de la **Tunnel Login Lifetime (Durée de vie de la connexion au tunnel)**. Même si vous définissez la durée de vie du cookie de remplacement d'authentification comme étant plus élevée, elle restera valide uniquement pendant la durée de vie de la connexion au tunnel.

©2026 Palo Alto Networks, Inc.

- **Certificate to Encrypt/Decrypt Cookie (Certificat pour chiffrer/décrypter le cookie)** : indique le certificat RSA à utiliser pour chiffrer et décrypter le cookie. Vous devez utiliser le même certificat sur le portail et les passerelles.

  Le mieux est de configurer le certificat RSA pour utiliser l'algorithme de synthèse le plus fort que votre réseau prend en charge.

  Le portail et les passerelles utilisent le schéma de remplissage RSA crypte PKCS # 1 V1.5 pour générer le cookie (en utilisant la clé publique du certificat) et décrypter le cookie (en utilisant la clé privée du certificat).

5. Cliquez deux fois sur **OK** pour enregistrer la configuration.

9. **Commit (Validez)** la configuration.

10. Vérifiez la configuration.

Depuis un système client exécutant l'application GlobalProtect, essayez de vous connecter à une passerelle ou à un portail sur lesquels vous avez activé l'authentification par mot de passe à usage unique. Vous devez voir des messages de commande similaires aux suivants s'afficher :

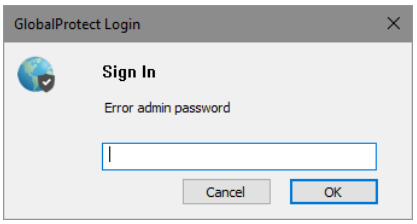


Illustration 1 : Fenêtre contextuelle relative au mot de passe à usage unique

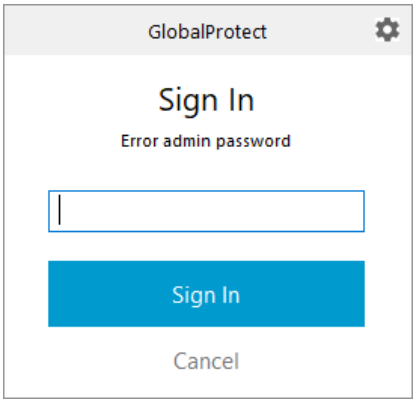


Illustration 2 : Invite relative au mot de passe à usage unique sur le panneau d'état de GlobalProtect

 ©2026 Palo Alto Networks, Inc.

Activer l’authentification à deux facteurs pour GlobalProtect basée sur les cartes à puce intelligentes

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW géré par Panorama • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Terminaux Windows et MacOS uniquement	Licence de passerelle GlobalProtect ou licence Prisma Access avec l’abonnement Utilisateur mobile

Si vous souhaitez que vos utilisateurs finaux s'authentifient à l'aide d'une carte à puce ou d'une carte d'accès commune (CAC), vous devez importer le certificat CA racine qui a délivré les certificats contenus dans la CAC ou les cartes à puce sur le portail et la passerelle. Vous pouvez ensuite créer un profil de certificat qui inclut cette AC racine et l'appliquer à vos configurations de portail et/ou de passerelle pour activer l'utilisation de la carte à puce intelligente dans le processus d'authentification.

1. Configurez votre infrastructure de carte à puce intelligente.

   Cette procédure présume que vous avez déployé les cartes à puce intelligentes et les lecteurs de cartes à puce intelligentes chez vos utilisateurs finaux.

   Pour obtenir des instructions spécifiques, consultez la documentation du logiciel du fournisseur de l'authentification.

   Dans la plupart des cas, la mise en place de l'infrastructure de la carte à puce implique la génération de certificats pour les utilisateurs finaux et pour les serveurs participants, qui sont le portail GlobalProtect et les passerelles dans ce cas d'utilisation.

 ©2026 Palo Alto Networks, Inc.

2. Importez le certificat AC racine qui a généré les certificats clients figurant sur les cartes à puce intelligentes de l'utilisateur final.

   Vérifiez que le certificat est accessible depuis votre système de gestion, puis exécutez les étapes suivantes :

   1. Choisissez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importer)** un nouveau certificat.
      - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW et Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** et **Import (Importer)** un certificat.
   2. Saisissez un **Certificate Name (Nom de certificat)**.
   3. Saisissez le chemin et le nom du **Certificate File (Fichier du certificat)** reçu de la part de l'autorité de certification, ou **Browse (Parcourez)** pour trouver le fichier.
   4. Sélectionnez **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))** dans la liste déroulante **File Format (Format de fichier)**, puis cliquez sur **OK (OK)** pour importer le certificat.

3. Créez le profil de certificat sur chaque portail / passerelle sur lesquels vous envisagez d'utiliser l'authentification activée par la CAC ou la carte à puce intelligente.

   Pour plus d'informations sur les autres champs du profil de certificat, notamment l'utilisation de CRL ou d'OCSP, reportez-vous à l'aide en ligne.

   1. Choisissez l'une des actions suivantes :
      - Dans Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**.
      - Sur Strata Cloud Manager, sélectionnez **Manage(Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Profile (Profil de certificat)**.
   2. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
   3. Sélectionnez un profil de certificat existant ou **Add (Ajoutez)**-en un nouveau.
   4. Donnez un **Name (Nom)** au profil de certificat.
   5. Sélectionnez le champ **Username (Nom d'utilisateur)** du certificat utilisé par PAN-OS pour faire correspondre l'adresse IP pour le User-ID, soit **Subject (Objet)** pour utiliser un nom commun, soit **Subject Alt: (Autre objet :) Email (Autre objet :E-mail)** pour utiliser une adresse électronique, soit **Subject Alt: Principal Name (Autre objet : Nom principal)** pour utiliser le nom principal.
   6. Dans la zone **CA Certificates (Certificats CA)**, **Add (Ajoutez)** le certificat CA racine de confiance que vous avez importé à l'étape 2 au profil du certificat. Lorsque vous y êtes invité, sélectionnez le **CA Certificate (Certificat CA)**, puis cliquez sur **OK**.
   7. Cliquez sur **OK** pour enregistrer le profil de certificat.

4. Affectez le profil de certificat à la passerelle ou au portail. Cette étape décrit comment ajouter le profil de certificat à la configuration de la passerelle ou du portail. Pour

 ©2026 Palo Alto Networks, Inc.

plus d'informations sur la configuration de ces composants, voir les sections Portails GlobalProtect et Passerelles GlobalProtect.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** ou **Gateways (Passerelles)**.
2. Sélectionnez une configuration de portail ou de passerelle existante ou **Add (Ajoutez)**-en une nouvelle.
3. Dans la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect), sélectionnez **Authentication (Authentification)**.
4. Sélectionnez le **Certificate Profile (Profil de certificat)** que vous venez de créer.
5. Cliquez sur **OK** pour enregistrer la configuration.

5. **Commit (Validez)** la configuration.

6. Vérifiez la configuration.

Depuis un point de terminaison exécutant l'application GlobalProtect, essayez de vous connecter à la passerelle ou au portail sur lesquels vous avez configuré l'authentification activée par la carte à puce intelligente. Lorsque vous y êtes invité, insérez votre carte à puce intelligente et vérifiez que vous pouvez vous authentifier sur GlobalProtect.

Réduire les invites de code PIN pour l'authentification par carte à puce sur GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Terminaux Windows uniquement	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Version 6.3.0 ou ultérieure de l'application GlobalProtect

Lorsque la connexion avant identification est configurée pour l'application GlobalProtect, les utilisateurs peuvent désormais s'authentifier avec une carte à puce et le logiciel ActivClient sans être invités à entrer leur code PIN plusieurs fois. Auparavant, les utilisateurs devaient entrer le code PIN de la carte à puce plusieurs fois : une fois par le fournisseur d'identité Windows et encore une fois par ActivClient, lors de l'utilisation de GlobalProtect avec CBL. Cette amélioration élimine les invites redondantes, permettant à l'application GlobalProtect de demander le code PIN de la carte à puce une unique fois, via ActivClient.

Pour utiliser cette fonctionnalité, vous devez répondre aux prérequis suivants :

- Assurez-vous que le portail GlobalProtect est pré-déployé.
- Assurez-vous que le mode Connexion avant identification est configuré pour l'application GlobalProtect.
- Assurez-vous que l'option **Use Single Sign-On for Smart Card PIN (Windows) (Utiliser l'authentification unique pour le code PIN de la carte à puce [Windows])** est **No (Non)** (valeur par défaut) dans les paramètres de l'application de la configuration du portail GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Les utilisateurs finaux doivent réintroduire le code PIN de la carte à puce dans les scénarios suivants car le logiciel ActivClient efface le cache du code PIN lorsque

- L'utilisateur s'est déconnecté du système
- L'utilisateur a changé d'utilisateur sur le périphérique
- Le système a été redémarré par l'utilisateur

Les utilisateurs finaux n'ont pas à réintroduire le code PIN lorsque le système sort du mode veille ou du mode hibernation.

Prise en charge des profils d'authentification avec ou sans PIV

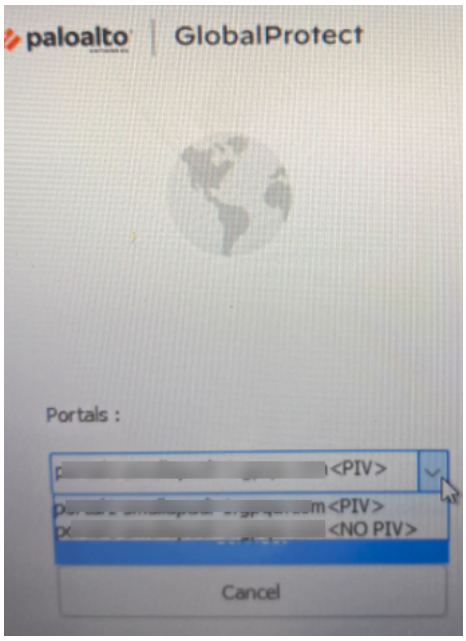
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Terminaux Windows et MacOS uniquement	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Version de l'application GlobalProtect 6.3.0 ou ultérieure pour Windows Version de l'application GlobalProtect 6.3.1 ou ultérieure pour macOS Version du contenu pour la carte intelligente pour macOS : 8890-8951

Si vous avez configuré le mode **On-demand (À la demande)** pour l'application GlobalProtect fonctionnant sur des terminaux Windows ou macOS avec l'authentification par carte à puce comme méthode d'authentification, l'application affiche désormais les options de profil d'authentification avec ou sans la carte à puce PIV.

Si vous avez configuré le mode Se connecter avant identification : **On-demand (À la demande)** pour l'application GlobalProtect avec l'authentification par carte à puce comme méthode d'authentification, l'application offre désormais la flexibilité aux utilisateurs finaux de s'authentifier à l'application soit en utilisant la carte à puce, soit en utilisant leur nom d'utilisateur/mot de passe. Avec cette fonctionnalité activée, l'application GlobalProtect affiche deux profils d'authentification pour l'utilisateur final dans le menu déroulant **Portals (Portails)** sur la page d'accueil de l'application ; un profil avec <PIV> et un autre profil avec <NO PIV>. Parmi les deux options disponibles, les utilisateurs finaux peuvent choisir leur profil d'authentification préféré. Le profil avec l'option PIV permet à l'utilisateur final de s'authentifier à l'application en utilisant la méthode d'authentification par carte à puce, tandis que le profil avec l'option PAS DE PIV leur permet de s'authentifier à l'application en utilisant leur nom d'utilisateur et mot de passe.

Par exemple, si les utilisateurs finaux oublient d'apporter leur carte à puce au travail, ils peuvent choisir le profil d'authentification avec PAS DE PIV dans le menu déroulant **Portals (Portails)** et peuvent utiliser leur nom d'utilisateur et mot de passe pour s'authentifier à l'application. Si la carte à puce est disponible, ils peuvent utiliser le profil avec PIV et s'authentifier en utilisant l'authentification par carte intelligente.

 ©2026 Palo Alto Networks, Inc.



Cette fonctionnalité ne fonctionnera que lorsque le logiciel ActivClient est installé sur l'appareil.

Pour que l'application GlobalProtect affiche les options de profil d'authentification avec ou sans la carte à puce PIV, vous devez :

1. Assurez-vous que Se connecter avant la connexion (CBL) est configuré avec le mode **On-demand (À la demande)** pour l'application GlobalProtect.
2. Sélectionnez l'option Autoriser l'authentification avec les informations d'identification de l'utilisateur OU le certificat client lors de la configuration de la passerelle et du portail GlobalProtect. Cette option définit si les utilisateurs peuvent s'authentifier au portail ou à la passerelle en utilisant des informations d'identification et/ou des certificats clients.

 ©2026 Palo Alto Networks, Inc.

3. Dans le Registre Windows, définissez les paramètres de pré-déploiement pour que l'application affiche les options de profil d'authentification avec `PIV` et `Pas de PIV`.
   1. Lancez l'invite de commande et tapez **`regedit`** pour ouvrir le Registre Windows.
   2. Dans le registre Windows, accédez à : `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`.
   3. Cliquez sur **Edit (Modifier)**, puis sélectionnez **New (Nouveau)** > **String Value (Valeur de chaîne)**.
   4. Lorsque vous êtes invité à le faire, spécifiez le **Name (Nom)** de la nouvelle valeur du registre en tant que **`PIV-profile`**.
   5. Cliquez avec le bouton droit sur la nouvelle valeur du registre et **Modify (Modifiez)**-la.
   6. Définissez la **Value Data (Données de valeur)** sur **`yes (oui)`**
   7. Cliquez sur **OK**.

   Pour pré-déployer le paramètre à partir de Windows Installer (Msiexec), utilisez la syntaxe suivante :

   ```
   msiexec.exe / globalprotect64.msi /i PIVPROFILE=yes
   ```

   Si les clés de registre sont pré-déployées lors de l'installation de l'application GlobalProtect avec l'adresse du portail, un redémarrage n'est pas nécessaire. Cependant, si les clés de registre sont mises à jour après l'installation de l'application GlobalProtect, un redémarrage du service PanGPS est nécessaire pour que les modifications prennent effet.

Améliorations pour l'authentification utilisant des cartes à puce sur les terminaux Windows

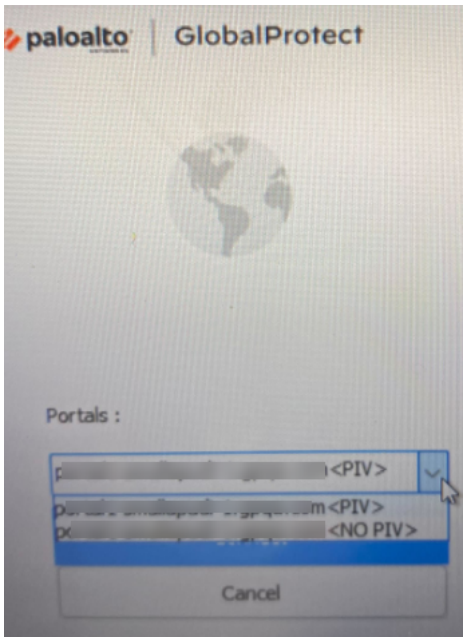
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Licence d'abonnement GlobalProtect	Version 6.3.0 ou ultérieure de l'application GlobalProtect Application GlobalProtect fonctionnant sur des terminaux Windows

Si vous avez configuré le mode Se connecter avant identification : **On-demand (À la demande)** pour l'application GlobalProtect avec l'authentification par carte à puce comme méthode d'authentification, l'application offre désormais la flexibilité aux utilisateurs finaux de s'authentifier à l'application soit en utilisant la carte à puce, soit en utilisant leur nom d'utilisateur/mot de passe. Avec cette fonctionnalité activée, l'application GlobalProtect affiche deux profils d'authentification pour l'utilisateur final dans le menu déroulant **Portals (Portails)** sur la page d'accueil de l'application ; un profil avec `<smartcard>` et un autre profil avec `<no smartcard>`. Parmi les deux options disponibles, les utilisateurs finaux peuvent choisir leur profil d'authentification préféré. Le profil avec l'option `<smartcard>` permet à l'utilisateur final de s'authentifier à l'application en utilisant la méthode d'authentification par carte à puce, tandis que le profil avec l'option `<no smartcard>` permet de s'authentifier à l'application en utilisant le nom d'utilisateur et le mot de passe.

 ©2026 Palo Alto Networks, Inc.

Par exemple, si les utilisateurs finaux oublient d'apporter leur carte à puce au travail, ils peuvent choisir le profil d'authentification avec `<no smartcard>` dans le menu déroulant **Portals (Portails)** et ils peuvent utiliser leur nom d'utilisateur et leur mot de passe pour s'authentifier sur l'application. Si la carte à puce est disponible, ils peuvent utiliser le profil avec `<smartcard>` et s'authentifier en utilisant l'authentification par carte intelligente.

Cette fonctionnalité ne fonctionnera que lorsque le logiciel ActivClient est installé sur le périphérique, si vous avez configuré la méthode Connecter avant identification *pour l'application GlobalProtect.*



*Si la méthode de connexion **Always-on (Toujours active)** est configurée pour l'application GlobalProtect et que les clés de profil d'authentification sont pré-déployées, l'option de profil par défaut `<smartcard>` sera sélectionnée. L'utilisateur final a la possibilité de déconnecter l'application et de changer l'option de profil si nécessaire.*

*Si la méthode de connexion **On-Demand (À la demande)** est configurée pour l'application GlobalProtect et que les clés de profil d'authentification sont pré-déployées, l'utilisateur final peut choisir soit l'option `<smartcard>` soit `<no smartcard>` dans l'interface utilisateur de l'application (menu déroulant **Portals [Portails]**).*

Si vous avez configuré le mode Connecter avant identification : **On-demand (À la demande)** pour l'application GlobalProtect avec l'authentification par carte à puce comme méthode d'authentification, l'application affiche désormais les options de profil d'authentification avec ou sans la carte à puce PIV.

Pour que l'application GlobalProtect affiche les options de profil d'authentification avec ou sans la carte à puce PIV, vous devez :

1. Assurez-vous que Se connecter avant la connexion (CBL) est configuré avec le mode **On-demand (À la demande)** pour l'application GlobalProtect.
2. Sélectionnez l'option Autoriser l'authentification avec les informations d'identification de l'utilisateur OU le certificat client lors de la configuration de la passerelle et du portail

 ©2026 Palo Alto Networks, Inc.

GlobalProtect. Cette option définit si les utilisateurs peuvent s'authentifier au portail ou à la passerelle en utilisant des informations d'identification et/ou des certificats clients.

3. Dans le Registre Windows, définissez les paramètres de pré-déploiement pour que l'application affiche les options de profil d'authentification avec `<smartcard>` et `<no smartcard>`.
   1. Lancez l'invite de commande et tapez **`regedit`** pour ouvrir le Registre Windows.
   2. Dans le registre Windows, accédez à : `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`.
   3. Cliquez sur **Edit (Modifier)**, puis sélectionnez **New (Nouveau)** > **String Value (Valeur de chaîne)**.
   4. Lorsque vous êtes invité à le faire, spécifiez le **Name (Nom)** de la nouvelle valeur du registre en tant que **`PIV-profile`**.
   5. Cliquez avec le bouton droit sur la nouvelle valeur du registre et **Modify (Modifiez)**-la.
   6. Définissez la **Value Data (Données de valeur)** sur **`yes (oui)`**
   7. Cliquez sur **OK**.

   Pour pré-déployer le paramètre à partir de Windows Installer (Msiexec), utilisez la syntaxe suivante :

   ```
   msiexec.exe / globalprotect64.msi /i PIVPROFILE=yes
   ```

   Personnaliser les clés de Registre Windows pour les options de profil

   À partir de la version 6.3.1 de GlobalProtect, vous pouvez pré-déployer les valeurs de clé de registre personnalisées pour les options de profil ; `<PIV>` et `<NO PIV>`.

   - La clé `<PIVString>` est disponible dans le chemin du Registre Windows : `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect \Settings`
   - La clé `<NoPIVString>` est disponible dans le chemin du Registre Windows : `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect \Settings`

Améliorations pour l'authentification utilisant des cartes à puce sur les terminaux macOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Licence d'abonnement GlobalProtect	Version 6.3.1 ou ultérieure de l'application GlobalProtect Version du contenu pour la carte intelligente pour macOS : 8890-8951

Si vous avez configuré le mode **On-demand (À la demande)** pour l'application GlobalProtect fonctionnant sur des terminaux macOS avec l'authentification par carte à puce comme méthode d'authentification, l'application affiche désormais les options de profil d'authentification avec ou sans la carte à puce PIV.

 ©2026 Palo Alto Networks, Inc.

*Si la méthode de connexion **Always-on (Toujours active)** est configurée pour l'application GlobalProtect et que les clés de profil d'authentification sont pré-déployées, l'option de profil par défaut <smartcard> sera sélectionnée. L'utilisateur final a la possibilité de déconnecter l'application et de changer l'option de profil si nécessaire.*

*Si la méthode de connexion **On-Demand (À la demande)** est configurée pour l'application GlobalProtect et que les clés de profil d'authentification sont pré-déployées, l'utilisateur final peut choisir soit l'option <smartcard> soit <no smartcard> dans l'interface utilisateur de l'application (menu déroulant **Portals [Portails]**).*

Pour que l'application GlobalProtect affiche les options de profil d'authentification avec ou sans la carte à puce sur les terminaux macOS, vous devez :

1. Assurez-vous que la méthode de connexion est configurée avec le mode **On-demand (À la demande)** pour l'application GlobalProtect.
2. Sélectionnez l'option Autoriser l'authentification avec les informations d'identification de l'utilisateur OU le certificat client lors de la configuration de la passerelle et du portail GlobalProtect. Cette option définit si les utilisateurs peuvent s'authentifier au portail ou à la passerelle en utilisant des informations d'identification et/ou des certificats clients.

 ©2026 Palo Alto Networks, Inc.

3. Dans le fichier plist GlobalProtect de macOS, définissez les paramètres de pré-déploiement pour que l'application affiche les options de profil d'authentification avec `<smartcard>` et `<n0 smartcard>`.
   1. Ouvrez le fichier plist GlobalProtect et recherchez les paramètres de personnalisation GlobalProtect.
      - Lancez un éditeur de plist, comme Xcode.
      - Dans l'éditeur de plist, ouvrez le fichier de la plist suivant : `/Library/ Preferences/ com.paloaltonetworks.GlobalProtect.settings.plist`.
      - Trouvez le dictionnaire des paramètres GlobalProtect : `/Palo Alto Networks/ GlobalProtect/Settings`. Si le dictionnaire des paramètres n'existe pas, créez-le. Vous pouvez ajouter chaque clé au dictionnaire des paramètres en tant que chaîne.
   2. Dans le dictionnaire des paramètres, ajoutez la paire clé-valeur suivante pour activer le profil d'authentification PIV avec ou sans carte à puce PIV :

```
<key>PIV-profile</key>
<string>yes</string>
                    </dict>
                    <key>Settings</key>
                    <dict>
                            <key>PIV-profile</key>
                            <string>yes</string>
```

Pour pré-déployer les clés personnalisées, utilisez :

- **`<key>PIVString</key>`**
- **`<key>noPIVString</key>`**

Activer l'authentification à deux facteurs basée sur une application de jetons logiciels

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW géré par Panorama • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Terminaux Windows et MacOS uniquement	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Si votre organisation utilise une application de jeton logiciel, comme RSA SecurID, pour mettre en œuvre l'authentification à deux facteurs, les utilisateurs doivent d'abord ouvrir leur application et saisir leur code PIN pour obtenir un code secret, puis saisir le code dans le champ **Mot de passe** dans leur application GlobalProtect. Ce processus en deux étapes complique le processus de connexion.

Pour simplifier le processus de connexion et améliorer l'expérience des utilisateurs, GlobalProtect offre l'authentification par jeton logiciel. L'utilisateur saisit le PIN RSA dans le champ **Mot de**

 ©2026 Palo Alto Networks, Inc.

passe de GlobalProtect, et GlobalProtect extrait le code secret de RSA et procède à la connexion sans que l'utilisateur n'ait à ouvrir l'application RSA.

Cette fonctionnalité est prise en charge pour les trois modes RSA : PinPad Style, Fob Style et mode Pinless. Pour PinPad et Fob Style, l'utilisateur saisit le PIN dans le champ **Mot de passe** et GlobalProtect récupère le code secret. Au mode Pinless, le champ Mot de passe est en gris et les utilisateurs saisissent leur nom d'utilisateur.

1. Modifiez les clés de registre sur les périphériques Windows client pour activer l'authentification par jeton logiciel en toute fluidité.

   Avant de pouvoir activer l'authentification par jeton logiciel en toute fluidité, vous devez modifier le registre Windows sur les périphériques Windows des clients. GlobalProtect récupère l'entrée du registre une seule fois : lors de l'initialisation de l'application GlobalProtect.

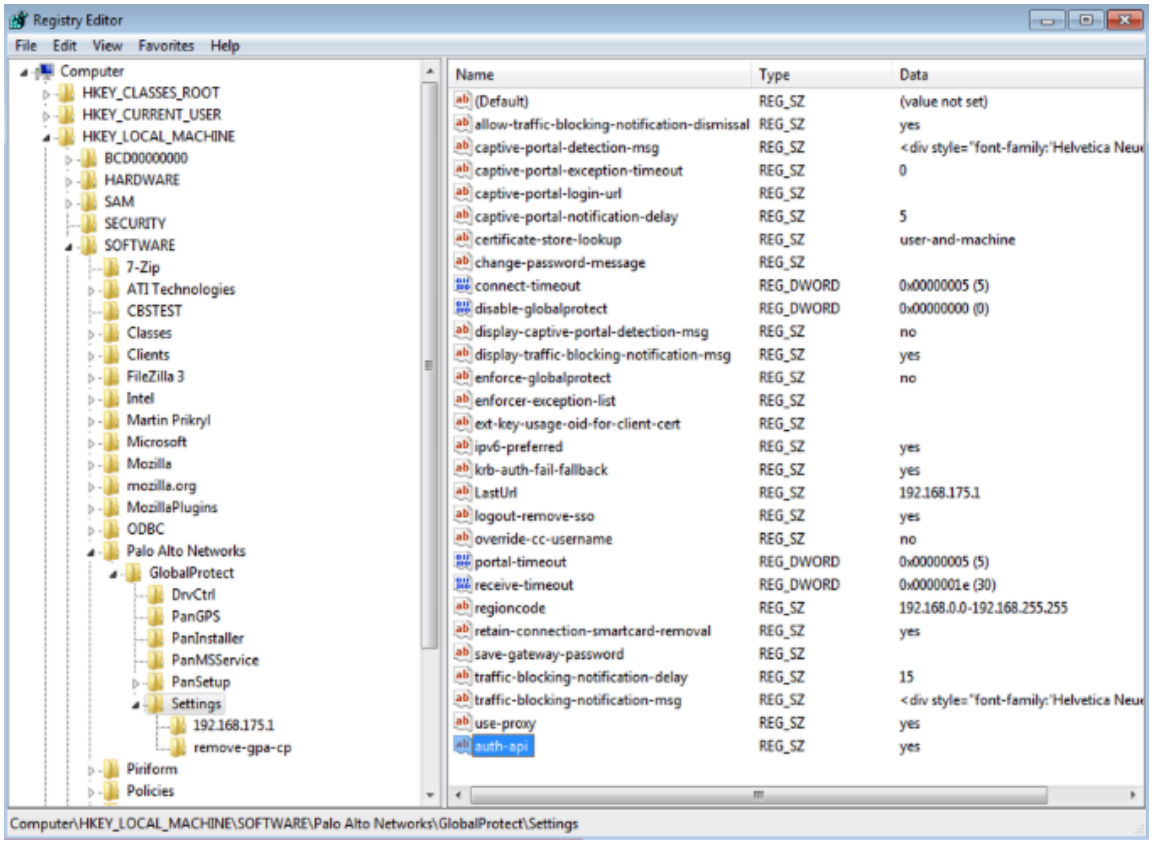
   1. Ouvrez l'éditeur du registre Windows et sélectionnez **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Palo Alto Networks** > **GlobalProtect** > **Settings**.
   2. Changez la valeur **auth-api** à **oui**.

      *Comme auth-api est défini sur **oui** dans la machine du client, vous devriez configurer le portail et les passerelles à l'aide de l'authentification RSA. Aucun autre profil d'authentification n'est pris en charge, car GlobalProtect tentera d'extraire le code secret.*

      Comme le portail et la passerelle utilisent l'authentification RSA, nous vous recommandons d'activer l'authentification «cookie-based» sur les passerelles. Il se peut que le jeton qui a été récupéré pour le portail soit toujours actif lorsque GlobalProtect tente d'obtenir le code secret de la passerelle, et il se peut que l'authentification échoue parce que le code secret a déjà été utilisé. Nous vous suggérons donc de générer un

 ©2026 Palo Alto Networks, Inc.

cookie de réécriture de l'authentification sur le portail et d'accepter le cookie sur la passerelle.



2. Configurez le portail et la passerelle à l'aide de l'authentification RSA.

 ©2026 Palo Alto Networks, Inc.

3. Activez l'authentification basée sur les cookies sur le portail GlobalProtect.

   En permettant à GlobalProtect de réécrire une authentification existante, GlobalProtect peut remplacer un code secret existant par un code secret nouvellement créé.

   1. Effectuez l'une des actions suivantes :

- **Suivez les étapes ci-dessous pour Panorama géré NGFW.**

  1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal-config>***, puis sélectionnez l'onglet **Agent**.
  2. Cliquez sur **OK**.

- **Suivez l'étape ci-dessous pour Prisma Access géré par Panorama.**

  1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **GlobalProtect_Portal** > **Agent** > **Default (Par défaut)** > **App (Application)**.

- **Suivez l'étape ci-dessous pour Strata Cloud géré NGFW et Prisma Access.**

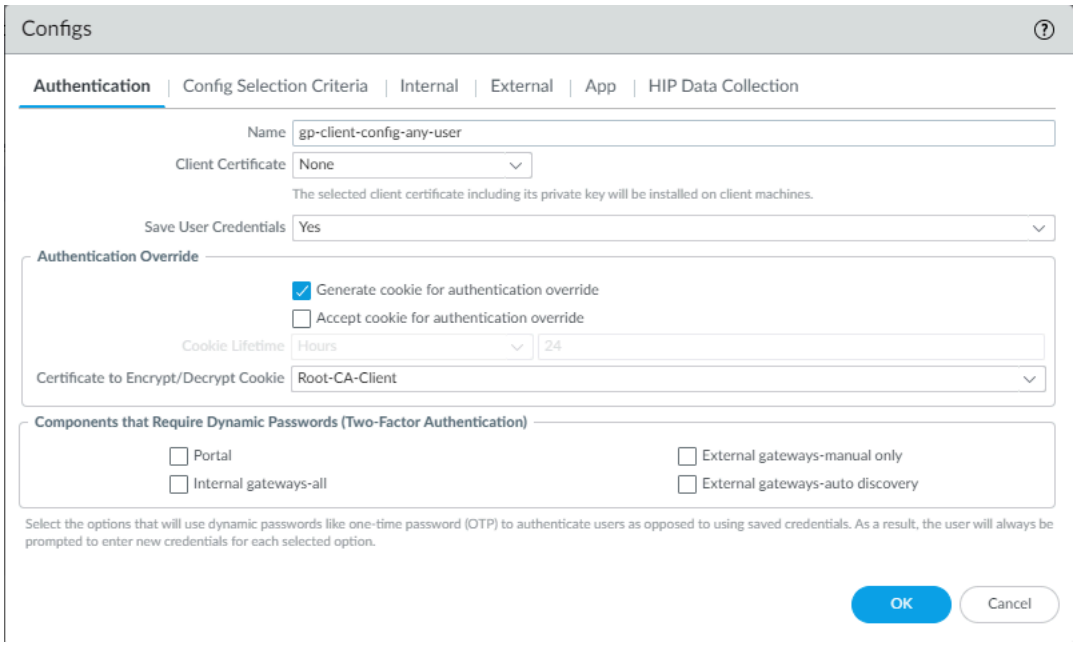
  1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration de Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Application GlobalProtect)**.

1. Sélectionnez **Générer le cookie pour la réécriture de l'authentification**.

   Le cookie d'authentification comprend les champs suivants :

   - `user (utilisateur)` : le nom d'utilisateur qui est utilisé pour authentifier l'utilisateur.
   - `Domain (Domaine)` : le nom de domaine de l'utilisateur.
   - `os` : le nom de l'application utilisée sur le périphérique.
   - `hostID (ID de l'hôte)` : l'ID unique que GlobalProtect affecte afin d'identifier l'hôte.
   - `gen time (heure de génération)` : la date et l'heure auxquelles l cookie d'authentification a été généré.
   - `ip` : adresse IP du périphérique qui est utilisé pour s'authentifier avec succès sur GlobalProtect et pour obtenir le cookie.

 ©2026 Palo Alto Networks, Inc.

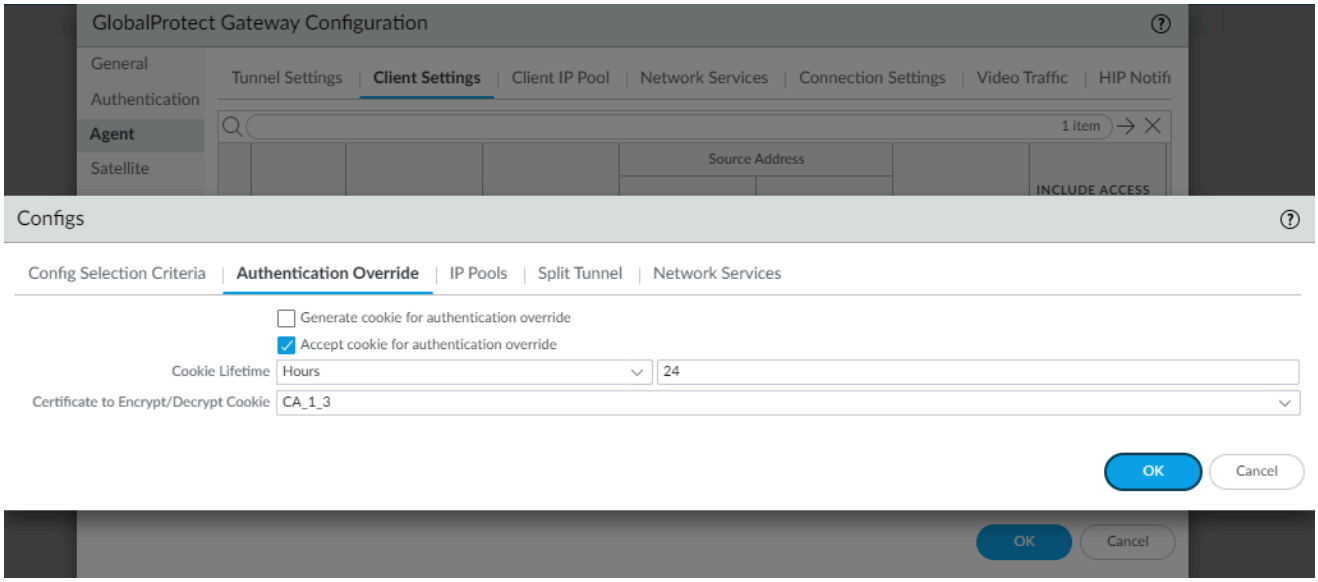


 ©2026 Palo Alto Networks, Inc.

4. Activez l'option Accepter le cookie pour la substitution d'authentification sur la passerelle GlobalProtect.
   1. Sur votre passerelle, sélectionnez l'onglet **Agent**.
   2. Sélectionnez **Paramètres du client**, puis sélectionnez la configuration du client GlobalProtect ou ajoutez-en une nouvelle.
   3. Sélectionnez **Réécriture de d'authentification**; puis sélectionnez **Accepter le cookie pour la réécriture de l'authentification**.

      Le cookie d'authentification comprend les champs suivants :

      - `user (utilisateur)` : le nom d'utilisateur qui est utilisé pour authentifier l'utilisateur.
      - `Domain (Domaine)` : le nom de domaine de l'utilisateur.
      - `os` : le nom de l'application utilisée sur le périphérique.
      - `hostID (ID de l'hôte)` : l'ID unique que GlobalProtect affecte afin d'identifier l'hôte.
      - `gen time (heure de génération)` : la date et l'heure auxquelles l cookie d'authentification a été généré.
      - `ip` : adresse IP du périphérique qui est utilisé pour s'authentifier avec succès sur GlobalProtect et pour obtenir le cookie.



5. Sur votre portail, sélectionnez l'onglet **Authentication (Authentification)**.

6. **Ajoutez** un profil d'authentification client ou sélectionnez-en un qui existe déjà ; puis sélectionnez **Récupérer automatiquement le code secret de l'application de jeton logiciel**.

 ©2026 Palo Alto Networks, Inc.

Configurer l'authentification pour les points de terminaison strongSwan Ubuntu et CentOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Terminaux Windows et macOS uniquement	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour étendre l'accès GlobalProtect aux terminaux strongSwan Ubuntu et CentOS, configurez l'authentification pour ces terminaux.

> *Pour connaître la version GlobalProtect minimale prenant en charge strongSwan sur Ubuntu Linux et CentOS, reportez-vous à la section* Quelles versions d'OS sont prises en charge par GlobalProtect ?.

Pour se connecter à la passerelle GlobalProtect, l'utilisateur doit réussir à s'authentifier. Les flux de travail suivants illustrent comment activer l'authentification pour les points de terminaison strongSwan. Pour obtenir des informations complètes sur strongSwan, reportez-vous au wiki strongSwan.

Activer l'authentification par certificat pour les terminaux strongSwan

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Le flux de travail suivant indique comment activer l'authentification des clients strongSwan à l'aide d'un profil de certificat.

©2026 Palo Alto Networks, Inc.

1. Configurez un tunnel IPsec pour que la passerelle GlobalProtect puisse communiquer avec un client strongSwan.

   L'authentification étendue (X-Auth) n'est pas prise en charge pour les déploiements Prisma Access.

   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**.
   2. Sélectionnez une passerelle existante ou **Add (Ajoutez)**-en une nouvelle.
   3. À l'onglet **Authentication (Authentification)** de la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect), sélectionnez le **Certificate Profile (Profil de certificat)** que vous souhaitez utiliser pour l'authentification.
   4. Sélectionnez **Agent** > **Tunnel Settings (Paramètres de tunnel)** pour activer le **Tunnel Mode (Mode tunnel)**, puis spécifiez les paramètres suivants pour établir le tunnel :
      - Cochez la case qui permet d'**Enable X-Auth Support (Activer la prise en charge X-Auth)**.
      - Si un **Group Name (Nom de groupe)** et un **Group Password (Mot de passe de groupe)** sont déjà configurés, supprimez-les.
      - Cliquez sur **OK** pour enregistrer les paramètres.

2. Vérifiez que les paramètres de connexion par défaut de la section `conn %default` du ficher de configuration du tunnel IPSec (`ipsec.conf`) sont correctement définis pour le client strongSwan.

Le fichier `ipsec.conf` se trouve généralement dans le dossier `/etc`.

Les configurations présentées dans cette procédure ont été testées et vérifiées pour les versions suivantes :

- *Ubuntu 14.0.4 avec strongSwan 5.1.2 et CentOS 6.5 avec strongSwan 5.1.3 pour PAN-OS 6.1.*
- *Ubuntu 14.0.4 avec strongSwan 5.2.1 pour PAN-OS 7.0.*

Les configurations présentées dans cette procédure peuvent être utilisées à titre de référence si vous utilisez une autre version de strongSwan. Pour plus d'informations, consultez strongSwan wiki.

À la section `conn %default` du fichier `ipsec.conf`, modifiez les paramètres suivants afin d'utiliser ces paramètres recommandés.

```
ikelifetime=20m reauth=yes rekey=yes keylife=10m rekeymargin=3m
 rekeyfuzz=0% keyingtries=1 type=tunnel
```

 ©2026 Palo Alto Networks, Inc.

3. Pour utiliser les paramètres recommandés, modifiez le fichier de configuration IPsec (`ipsec.conf`) et le fichier de mot de passe IPsec (`ipsec.secrets`) du client strongSwan.

Le fichier `ipsec.secrets` se trouve généralement dans le dossier `/etc` .

Utilisez le nom d'utilisateur du client strongSwan comme nom commun du certificat.

Modifiez les éléments suivants du fichier `ipsec.conf` afin d'utiliser ces paramètres recommandés.

```
conn <connection name> keyexchange=ikev1 authby=rsasig ike=aes-
sha1-modp1024,aes256 left=<strongSwan/Linux-client-IP-address>
 leftcert=<client certificate with the strongSwan client
 username used as the certificate's common name> leftsourceip=
%config leftauth2=xauth right=<GlobalProtect-Gateway-IP-
address> rightid="CN=<Subject-name-of-gateway-certificate>"
 rightsubnet=0.0.0.0/0 auto=add
```

Modifiez les éléments suivants du fichier `ipsec.conf` afin d'utiliser ces paramètres recommandés.

```
:RSA <private key file> "<passphrase if used>"
```

4. Démarrez les services IPsec strongSwan et connectez-vous au tunnel IPsec que le client strongSwan doit utiliser lorsqu'il s'authentifie sur la passerelle GlobalProtect.

Utilisez la variable `config <name>` pour nommer la configuration de tunnel.

- Ubuntu :

```
ipsec start ipsec up <name>
```

- CentOS :

```
strongSwan start strongswan up <name>
```

 ©2026 Palo Alto Networks, Inc.

5. Vérifiez que le tunnel est configuré correctement et que la connexion VPN est établie avec le client strongSwan et la passerelle GlobalProtect.
   1. Vérifiez les informations d'état détaillées d'une connexion spécifique (en nommant la connexion) ou vérifiez les informations d'état de toutes les connexions du client strongSwan :
      - Ubuntu :

        ```
        ipsec statusall [<connection name>]
        ```

      - CentOS :

        ```
        strongswan statusall [<connection name>]
        ```

   2. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**. Dans la colonne **Info (Informations)**, sélectionnez les **Remote Users (Utilisateurs distants)** de la passerelle configurée pour la connexion au client strongSwan. Le client strongSwan devrait figurer dans la liste des **Current Users (Utilisateurs actuels)**.

Activer la prise en charge X-Auth des terminaux strongSwan

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Le flux de travail suivant indique comment activer l'authentification des clients strongSwan à l'aide d'un profil d'authentification. Le profil d'authentification indique le profil de serveur à utiliser lors de l'authentification des clients strongSwan.

 ©2026 Palo Alto Networks, Inc.

1. Configurez le tunnel IPsec que la passerelle GlobalProtect utilisera pour communiquer avec un client strongSwan.

   L'authentification étendue (X-Auth) n'est pas prise en charge pour les déploiements Prisma Access.

   1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**.
   2. Sélectionnez une passerelle existante ou **Add (Ajoutez)**-en une nouvelle.
   3. À l'onglet **Authentication (Authentification)** de la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect), sélectionnez le **Authentication Profile (Profil d'authentification)** que vous souhaitez utiliser.
   4. Sélectionnez **Agent (Agent)** > **Tunnel Settings (Paramètres de tunnel)** pour activer le **Tunnel Mode (Mode tunnel)**, puis spécifiez les paramètres suivants pour établir le tunnel :
      - Cochez la case qui permet d'**Enable X-Auth Support (Activer la prise en charge X-Auth)**.
      - Saisissez un **Group Name (Nom de groupe)** et un **Group Password (Mot de passe de groupe)**, si ceux-ci ne sont pas déjà configurés.
      - Cliquez sur **OK** pour enregistrer ces paramètres de tunnel.

2. Vérifiez que les paramètres de connexion par défaut de la section `conn %default` du ficher de configuration du tunnel IPSec (`ipsec.conf`) sont correctement définis pour le client strongSwan.

Le fichier `ipsec.conf` se trouve généralement dans le dossier `/etc`.

Les configurations présentées dans cette procédure ont été testées et vérifiées pour les versions suivantes :

- *Ubuntu 14.0.4 avec strongSwan 5.1.2 et CentOS 6.5 avec strongSwan 5.1.3 pour PAN-OS 6.1.*
- *Ubuntu 14.0.4 avec strongSwan 5.2.1 pour PAN-OS 7.0.*

Les configurations présentées dans cette procédure peuvent être utilisées à titre de référence si vous utilisez une autre version de strongSwan. Pour plus d'informations, consultez strongSwan wiki.

À la section `conn %default` du fichier `ipsec.conf`, configurez les paramètres recommandés suivants :

```
ikelifetime=20m reauth=yes rekey=yes keylife=10m rekeymargin=3m
 rekeyfuzz=0% keyingtries=1 type=tunnel
```

 ©2026 Palo Alto Networks, Inc.

3. Pour utiliser les paramètres recommandés, modifiez le fichier de configuration IPsec (`ipsec.conf`) et le fichier de mot de passe IPsec (`ipsec.secrets`) du client strongSwan.

Le fichier `ipsec.secrets` se trouve généralement dans le dossier `/etc` .

Utilisez le nom d'utilisateur du client strongSwan comme nom commun du certificat.

Configurez les paramètres recommandés suivants dans le fichier `ipsec.conf` :

```
conn <connection name> keyexchange=ikev1 ikelifetime=1440m
 keylife=60m aggressive=yes ike=aes-sha1-modp1024,aes256 esp=aes-
sha1 xauth=client left=<strongSwan/Linux-client-IP-address>
 leftid=@#<hex of Group Name configured in the GlobalProtect
 gateway> leftsourceip=%modeconfig leftauth=psk rightauth=psk
 leftauth2=xauth right=<gateway-IP-address> rightsubnet=0.0.0.0/0
 xauth_identity=<LDAP username> auto=add
```

Configurez les paramètres recommandés suivants dans le fichier `ipsec.secrets` :

```
: PSK <Group Password configured in the gateway> <username> : XAUTH
 "<user password>"
```

4. Démarrez les services IPsec strongSwan et connectez-vous au tunnel IPsec que le client strongSwan doit utiliser lorsqu'il s'authentifie sur la passerelle GlobalProtect.

- Ubuntu :

```
ipsec start ipsec up <name>
```

- CentOS :

```
strongSwan start strongswan up <name>
```

5. Vérifiez que le tunnel est configuré correctement et que la connexion VPN est établie avec le client strongSwan et la passerelle GlobalProtect.
   1. Vérifiez les informations d'état détaillées d'une connexion spécifique (en nommant la connexion) ou vérifiez les informations d'état de toutes les connexions du client strongSwan :
      - Ubuntu :

```
ipsec statusall [<connection name>]
```

      - CentOS :

```
strongswan statusall [<connection name>]
```

   2. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**. Dans la colonne **Info (Informations)**, sélectionnez les **Remote Users (Utilisateurs distants)** de la passerelle configurée pour la connexion au client

 ©2026 Palo Alto Networks, Inc.

strongSwan. Le client strongSwan devrait figurer dans la liste des **Current Users (Utilisateurs actuels)**.

Activer l'authentification à deux facteurs par certificat pour les terminaux strongSwan

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Avec l'authentification à deux facteurs, le client strongSwan doit s'authentifier à l'aide d'un profil de certificat et d'un profil d'authentification pour se connecter à la passerelle GlobalProtect. Le flux de travail suivant indique comment activer l'authentification des clients strongSwan à l'aide de l'authentification à deux facteurs.

1. Configurez le tunnel IPsec que la passerelle GlobalProtect utilisera pour communiquer avec un client strongSwan.

   L'authentification étendue (X-Auth) n'est pas prise en charge pour les déploiements Prisma Access.

   1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**.
   2. Sélectionnez une passerelle existante ou **Add (Ajoutez)**-en une nouvelle.
   3. À l'onglet **Authentication (Authentification)** de la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect), sélectionnez le **Certificate Profile (Profil de certificat)** et le **Authentication Profile (Profil d'authentification)** que vous souhaitez utiliser.
   4. Sélectionnez **Agent (Agent)** > **Tunnel Settings (Paramètres de tunnel)** pour activer le **Tunnel Mode (Mode tunnel)**, puis spécifiez les paramètres suivants pour établir le tunnel :
      - Cochez la case qui permet d'**Enable X-Auth Support (Activer la prise en charge X-Auth)**.
      - Si un **Group Name (Nom de groupe)** et un **Group Password (Mot de passe de groupe)** sont déjà configurés, supprimez-les.
      - Cliquez sur **OK** pour enregistrer ces paramètres de tunnel.

 ©2026 Palo Alto Networks, Inc.

2. Vérifiez que les paramètres de connexion par défaut de la section `conn %default` du ficher de configuration du tunnel IPSec (`ipsec.conf`) sont correctement définis pour le client strongSwan.

Le `ipsec.conf` se trouve généralement dans le dossier `/etc`.

Les configurations présentées dans cette procédure ont été testées et vérifiées pour les versions suivantes :

- *Ubuntu 14.0.4 avec strongSwan 5.1.2 et CentOS 6.5 avec strongSwan 5.1.3 pour PAN-OS 6.1.*
- *Ubuntu 14.0.4 avec strongSwan 5.2.1 pour PAN-OS 7.0.*

Utilisez les configurations de cette procédure comme référence si vous utilisez une version différente de strongSwan. Pour plus d'informations, consultez strongSwan wiki.

Configurez les paramètres recommandés suivants dans le fichier `ipsec.conf` :

```
ikelifetime=20m reauth=yes rekey=yes keylife=10m rekeymargin=3m
 rekeyfuzz=0% keyingtries=1 type=tunnel
```

3. Pour utiliser les paramètres recommandés, modifiez le fichier de configuration IPsec (`ipsec.conf`) et le fichier de mot de passe IPsec (`ipsec.secrets`) du client strongSwan.

Le fichier `ipsec.secrets` se trouve généralement dans le dossier `/etc` .

Utilisez le nom d'utilisateur du client strongSwan comme nom commun du certificat.

Configurez les paramètres recommandés suivants dans le fichier `ipsec.conf` :

```
conn <connection name> keyexchange=ikev1 authby=xauthrsasig
 ike=aes-sha1-modp1024 esp=aes-sha1 xauth=client left=<strongSwan/
Linux-client-IP-address> leftcert=<client-certificate-without-
password> leftsourceip=%config right=<GlobalProtect-gateway-
IP-address> rightid=%anyCN=<Subject-name-of-gateway-cert>"
 rightsubnet=0.0.0.0/0 leftauth2=xauth xauth_identity=<LDAP
 username> auto=add
```

Configurez les paramètres recommandés suivants dans le fichier `ipsec.secrets` :

```
<username> :XAUTH "<user password>" ::RSA <private key file>
 "<passphrase if used>"
```

 ©2026 Palo Alto Networks, Inc.

4. Démarrez les services IPsec strongSwan et connectez-vous au tunnel IPsec que le client strongSwan doit utiliser lorsqu'il s'authentifie sur la passerelle GlobalProtect.

   - Ubuntu :

     ```
     ipsec start  ipsec up <name>
     ```

   - CentOS :

     ```
     strongSwan start strongswan up <name>
     ```

5. Vérifiez que le tunnel est configuré correctement et que la connexion VPN est établie avec le client strongSwan et la passerelle GlobalProtect.

   1. Vérifiez les informations d'état détaillées d'une connexion spécifique (en nommant la connexion) ou vérifiez les informations d'état de toutes les connexions du client strongSwan :

      - Ubuntu :

        ```
        ipsec statusall [<connection name>]
        ```

      - CentOS :

        ```
        strongswan statusall [<connection name>]
        ```

   2. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**. Dans la colonne **Info (Informations)**, sélectionnez les **Remote Users (Utilisateurs distants)** de la passerelle configurée pour la connexion au client strongSwan. Le client strongSwan devrait figurer dans la liste des **Current Users (Utilisateurs actuels)**.

 ©2026 Palo Alto Networks, Inc.

Configurer l'authentification du moteur d'identité cloud

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama et Strata Cloud Manager) • Prisma Access (géré par Panorama et Strata Cloud Manager)	Terminaux GlobalProtect fonctionnant sous Windows et macOS Application GlobalProtect 6.2.6 et versions 6.2.x ultérieures pour l'authentification OIDC du moteur d'identité sur le cloud Application GlobalProtect 6.3.0 et versions ultérieures pour le moteur d'identité sur le cloud SAML et l'authentification par certificat client GlobalProtect 6.3.1 et versions ultérieures pour la fonctionnalité de saut de hub SSO à authentification multiple du moteur d'identité sur le cloud PAN-OS 10.2 et versions ultérieures pour l'authentification du moteur d'identité sur le cloud

Le moteur d'identité sur le cloud prend en charge les méthodes d'authentification suivantes pour GlobalProtect :

- SAML
- Certificat client

OIDC

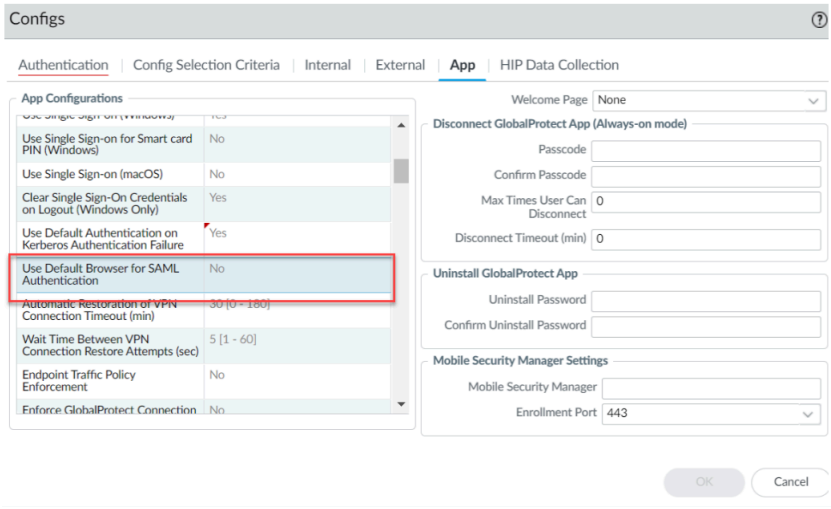
1. Créez un profil d'authentification.
2. Dans votre environnement, accédez à l'écran Ajouter une authentification pour GlobalProtect.
3. Sélectionnez Moteur d'identité sur le cloud comme méthode d'authentification et le profil que vous avez créé à l'étape 1.
4. Suivez les invites à l'écran pour configurer l'authentification de l'identité sur le cloud souhaitée.

Authentification SAML du moteur d'identité sur le cloud avec affichage web intégré

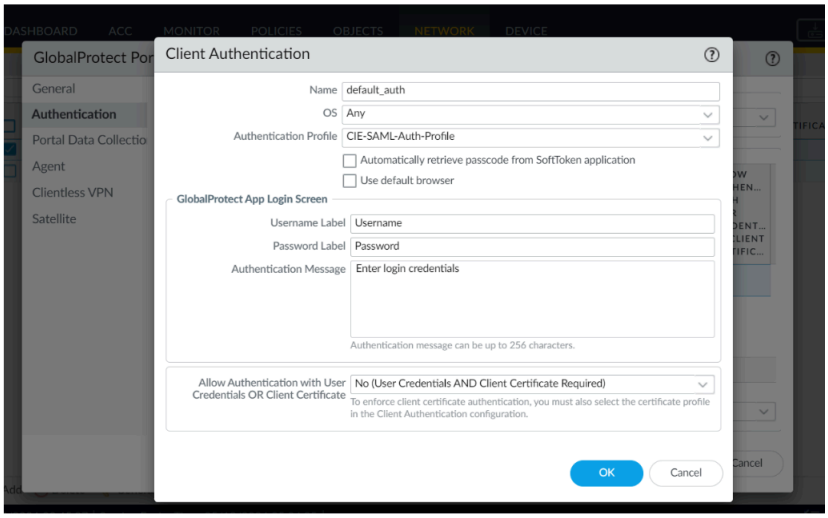
Le navigateur système est le navigateur par défaut pour l'authentification SAML du moteur d'identité sur le cloud. Suivez les étapes ci-dessous pour utiliser l'affichage web intégré :

 ©2026 Palo Alto Networks, Inc.

1. Désactivez l'option **Use Default Browser for SAML Authentication (Utiliser le navigateur par défaut pour l'authentification SAML)** dans les paramètres de l'application de la configuration du portail.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<portal-config>** > **Agent** > **<agent-config>** > **App (Application)**.
   2. Dans la section Configurations d'application, définissez l'option **Use Default Browser for SAML Authentication** (Utiliser le navigateur par défaut pour l'authentification SAML) sur **No (Non)** pour permettre à l'application GlobalProtect d'ouvrir le navigateur intégré pour l'authentification CIE. Après avoir défini l'option sur **No (Non)** et lorsque l'application GlobalProtect tente de se reconnecter, l'application invite les utilisateurs finaux à se réauthentifier en utilisant CIE comme méthode d'authentification.



2. Définissez l'option du navigateur dans les paramètres d'authentification client de la configuration du portail.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<portal-config>** > **Authentication (Authentification)** > **<client-authentication-config>**.
   2. Décochez l'option **Use default browser (Utiliser le navigateur par défaut)** dans la fenêtre **Client Authentication (Authentification client)** pour utiliser le navigateur intégré pour l'authentification CIE.



 ©2026 Palo Alto Networks, Inc.

3. Cliquez sur **OK**.
4. **Commit (Commit)** la configuration.

Multi-authentification du moteur d'identité cloud

Vous pouvez créer un profil d'authentification qui redirige les utilisateurs vers le type d'authentification (un certificat client ou un fournisseur d'identité conforme à SAML 2.0) que vous configurez pour l'authentification. Pour plus d'informations, consultez Configurer l'authentification moteur d'identité sur le cloud sur le pare-feu ou Panorama.

Avec la multi-authentification moteur d'identité sur le cloud, vous pouvez permettre à l'utilisateur final de contourner la page du hub SSO (qui invite l'utilisateur à saisir son nom d'utilisateur SAML) sur les terminaux Windows en prédéployant la clé de registre suivante :

`CASSKIPHUBPAGE` utilisant la syntaxe suivante :

```
msiexec.exe /i globalprotect64.msi CASSKIPHUBPAGE=yes
```

La clé de registre est affichée dans le chemin d'accès du registre Windows `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`.

Cette fonctionnalité est prise en charge sur le navigateur par défaut et l'affichage web intégré pour les actions suivantes :

- L'utilisateur déverrouille le périphérique
- Le périphérique sort du mode veille
- Après un redémarrage du système

  Pour l'application GlobalProtect avec Se connecter avant identification (CBL) installé sur les terminaux Windows, vous devez utiliser le navigateur par défaut pour l'authentification SAML du moteur d'identité sur le cloud.

Avant d'activer cette fonctionnalité, assurez-vous de ce qui suit :

- Le nom d'utilisateur est configuré au format UPN dans CIE ou les terminaux Windows sont joints au domaine Azure (AAD ou Active Directory).
- Le moteur d'identité cloud est configuré sans l'option Forcer l'authentification dans le profil d'authentification.
- La session IDP/SAML est active.

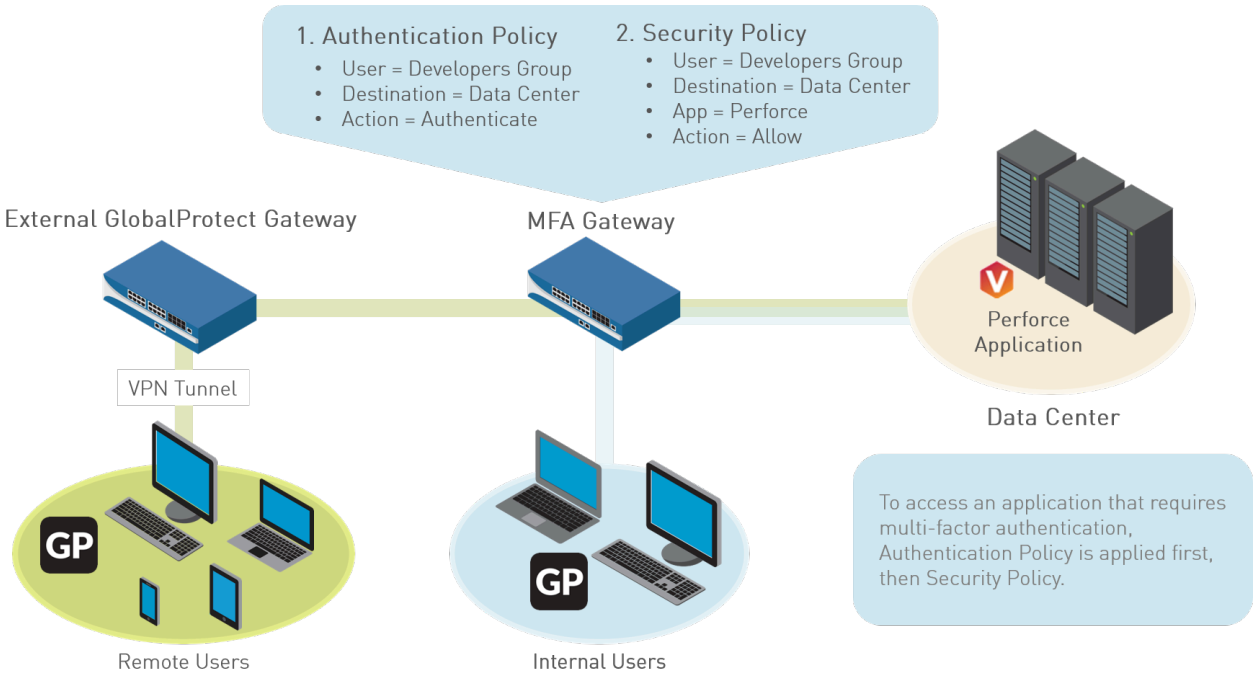
 ©2026 Palo Alto Networks, Inc.

Configurer GlobalProtect pour faciliter les notifications d'authentification multifacteur

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour protéger les applications critiques et empêcher les pirates d'utiliser des informations d'identification volées pour effectuer des mouvements latéraux sur votre réseau, vous pouvez configurer une authentification multifacteur basée sur des politiques. Cela garantit que chaque utilisateur répond à plusieurs demandes d'authentification de différents types (facteurs) avant de pouvoir accéder à des services et applications hautement sensibles.

©2026 Palo Alto Networks, Inc.



 ©2026 Palo Alto Networks, Inc.

Si une session utilisateur correspond à la politique d'authentification, le type d'application ou de service détermine l'expérience utilisateur pour les notifications relatives à la demande d'authentification :

- (Points de terminaison Windows ou MacOS uniquement) **Applications non basées sur un navigateur** : pour faciliter les notifications MFA pour les applications non HTTP (telles que Perforce) sur les points de terminaison Windows ou MacOS, une application GlobalProtect est requise. Lorsqu'une session correspond à une règle de politique d'authentification, le pare-feu envoie une notification UDP à l'application GlobalProtect avec un lien URL intégré vers la page Authentication Portal (Portail d'authentification). L'application GlobalProtect affiche ensuite ce message sous la forme d'une notification contextuelle à l'utilisateur.
- **Applications basées sur un navigateur** : les applications basées sur un navigateur n'exigent pas que GlobalProtect affiche les messages de notification à l'utilisateur. Lorsque le pare-feu identifie une session comme trafic de navigation Web (basé sur App-ID), le pare-feu présente automatiquement à l'utilisateur la page Authentication Portal (Portail d'authentification) (précédemment appelée page Captive Portal (Portail captif) spécifiée dans la règle de politique d'authentification.

Vous ne pouvez pas remplacer manuellement la classification de l'application (basée sur un navigateur ou non basée sur un navigateur). Pour configurer GlobalProtect afin d'afficher les notifications MFA pour les applications non basées sur un navigateur, utilisez le flux de travail suivant :

1. Avant de configurer GlobalProtect, configurez l'authentification multifacteur sur le pare-feu.

   Si vous utilisez l'authentification à deux facteurs avec GlobalProtect pour vous authentifier auprès de la passerelle ou du portail, un profil de serveur RADIUS est requis. Si vous utilisez GlobalProtect pour informer l'utilisateur d'une correspondance de politique d'authentification (message UDP), un profil de serveur d'authentification multifacteur est suffisant.

   Pour utiliser l'authentification multifacteur pour protéger les ressources sensibles, la solution la plus simple consiste à intégrer le pare-feu à un fournisseur MFA déjà installé sur votre réseau. Lorsque votre structure MFA est prête, vous pouvez commencer à configurer les composants de votre politique d'authentification.

   - Activez Captive Portal (Portail captif) pour enregistrer les horodatages d'authentification et mettre à jour les mappages utilisateur.
   - Créez des profils de serveur qui définissent la manière dont le pare-feu se connectera aux services qui authentifient les utilisateurs.
   - Affectez les profils de serveur à un profil d'authentification qui spécifie les paramètres d'authentification.
   - Configurez une règle de politique de sécurité qui autorise les utilisateurs à accéder aux ressources qui exigent une authentification.

 ©2026 Palo Alto Networks, Inc.

2. (Passerelles externes uniquement) Pour que GlobalProtect prenne en charge l'authentification multifacteur sur les passerelles externes, vous devez Configurer une page de réponse pour l'interface de tunnel d'entrée sur le pare-feu :
   1. Sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponses)** > **MFA Login Page (Page de connexion MFA)**.
   2. Sélectionnez puis **Export (Exportez)** le modèle **Predefined (Prédéfini)** à l'emplacement de votre choix.
   3. Sur votre point de terminaison, utilisez un éditeur HTML pour personnaliser la page de réponse téléchargée et enregistrez-la en lui donnant un nom de fichier unique.
   4. Revenez à la boîte de dialogue **MFA Login Page (Page de connexion MFA)** du pare-feu, **Import (Importez)** votre page personnalisée, **Browse (Parcourez)** pour sélectionner le **Import File (Fichier d'importation)**, puis sélectionnez la **Destination** (système virtuel ou emplacement partagé). Cliquez sur **OK**, puis cliquez sur **Close (Fermer)**.
3. (Passerelles externes uniquement) Activez **Response Pages (Pages de réponses)** comme service autorisé sur le profil **Interface Mgmt (Gestion de l'interface)** :
   1. Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **Interface Mgmt (Gestion de l'interface)**, puis sélectionnez le profil.
   2. Dans la zone **Permitted Services (Services autorisés)**, sélectionnez **Response Page (Pages de réponses)** et cliquez sur **OK**.
4. (Passerelles externes uniquement) Attachez le profil **Interface Mgmt (Gestion de l'interface)** à une interface de tunnel :
   1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Tunnel** et l'interface de tunnel sur laquelle vous souhaitez utiliser la page de réponse.
   2. Sélectionnez **Advanced (Avancé)**, puis sélectionnez le profil **Interface Mgmt (Gestion de l'interface)** que vous avez configuré à l'étape précédente en tant que **Management Profile (Profil de gestion)**.
5. (Passerelles externes uniquement) **Enable User Identification (Activer l'identification de l'utilisateur)** sur la zone associée à l'interface de tunnel (**Network (Réseau)** > **Zones** > **<tunnel-zone**).
6. Configurez les clients GlobalProtect pour prendre en charge les notifications d'authentification multifacteur pour les applications non basées sur un navigateur.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**, et sélectionnez une configuration de portail (ou **Add (Ajoutez)**-en une).
   2. Sélectionnez **Agent (Agent)**, puis sélectionnez une configuration d'agent existante ou **Add (Ajoutez)**-en une nouvelle.
   3. À l'onglet **App (Appplication)**, spécifiez les éléments suivants :
      - Définissez **Enable Inbound Authentication Prompts from MFA Gateways (Activer les invites d'authentification entrante des passerelles MFA)** sur **Yes (Oui)**. Pour prendre en charge la Multi-Factor Authentication (authentification multifacteur ; MFA), l'application GlobalProtect doit recevoir et reconnaître les invites d'authentification UDP qui proviennent de la passerelle. Sélectionnez **Yes (Oui)** pour permettre à l'application GlobalProtect de recevoir et d'accepter l'invite. Par défaut,

 ©2026 Palo Alto Networks, Inc.

cette valeur est définie sur **No (Non)**, ce qui signifie que GlobalProtect bloque les invites d'authentification UDP de la passerelle.

- Dans le champ **Network Port for Inbound Authentication Prompts (UDP) (Port réseau pour les invites d'authentification entrante (UDP))**, spécifiez le numéro de port que l'application GlobalProtect utilise pour recevoir les invites d'authentification UDP entrante en provenance des passerelles MFA. Le port par défaut est 4501. Pour changer de port, indiquez un chiffre entre 1 et 65 535.
- Dans le champ **Trusted MFA Gateways (Passerelles MFA de confiance)**, précisez l'adresse de la passerelle et le numéro de port (requis uniquement pour les ports autres que par défaut, comme 6082) de l'URL de redirection auquel l'application GlobalProtect fera confiance pour l'authentification multifacteur. Lorsqu'une application GlobalProtect reçoit une invite d'authentification UDP dotée d'une URL de redirection destinée au port réseau spécifié, GlobalProtect affiche un message d'authentification uniquement si l'URL de redirection est approuvée.
- Configurer le **Default Message for Inbound Authentication Prompts (Message par défaut pour les invites d'authentification entrantes)**. Lorsque les utilisateurs tentent d'accéder à une ressource qui nécessite une authentification supplémentaire, GlobalProtect reçoit un paquet UDP contenant l'invite d'authentification entrante et affiche ce message. Le paquet UDP contient également l'URL vers la page du Portail d'authentification que vous avez précisée lors de la configuration de l'authentification multifacteur. GlobalProtect ajoute automatiquement l'URL au message. Par exemple, pour afficher la notification affichée au début de cette rubrique, entrez le message suivant :

  ```
  Vous avez tenté d'accéder à une ressource protégée qui
  nécessite une authentification supplémentaire. Procédez à
  l'authentification sur :
  ```

4. Enregistrez la configuration de l'agent (cliquez deux fois sur **OK**), puis **Commit (Validez)** vos changements.

 ©2026 Palo Alto Networks, Inc.

Activer la transmission des ASV vers un serveur RADIUS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Lorsqu'ils communiquent avec les passerelles ou les portails, les points de terminaison GlobalProtect envoient des informations qui comprennent leur adresse IP, le système d'exploitation, le nom d'hôte, le nom de domaine ainsi que la version de l'application GlobalProtect. Vous pouvez permettre au pare-feu de transmettre ces informations en tant qu'attributs spécifiques au fournisseur (ASV) à un serveur RADIUS lors de l'authentification (par défaut, le pare-feu ne transmet pas les ASV). Les administrateurs RADIUS peuvent alors effectuer des tâches administratives en fonction de ces ASV. Par exemple, les administrateurs RADIUS pourraient utiliser l'attribut OS pour définir une politique qui exige l'authentification par mot de passe régulière pour les utilisateurs de Microsoft Windows et l'authentification par de mot de passe à usage unique pour les utilisateurs de Google Android.

Voici les tâches préalables qui s'appliquent à cette procédure :

- Importez le dictionnaire RADIUS de Palo Alto Networks dans votre serveur RADIUS.
- Configurez un profil de serveur et affectez-le à un profil d'authentification. Reportez-vous à la section Configuration de l'authentification externe pour obtenir de plus amples précisions.
- Affectez le profil d'authentification à une passerelle ou un portail GlobalProtect. Reportez-vous à la section Paramétrer l'accès au portail GlobalProtect ou Configurer une passerelle GlobalProtect pour obtenir de plus amples précisions.

1. Connectez-vous à l'ILC du pare-feu.
2. Saisissez la commande de chaque ASV que vous souhaitez transmettre :

```
username@hostname> set authentication radius-vsa-on client-source-
ip username@hostname> set authentication radius-vsa-on client-
os username@hostname> set authentication radius-vsa-on client-
hostname username@hostname> set authentication radius-vsa-on user-
domain username@hostname> set authentication radius-vsa-on client-
gp-version
```

Si vous souhaitez ultérieurement empêcher le pare-feu de transmettre certains VSA, exécutez les mêmes commandes, en utilisant l'option ***radius-vsa-off*** *plutôt que l'option* ***radius-vsa-on****.*

 ©2026 Palo Alto Networks, Inc.

Activer le mappage des groupes

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Comme l'agent ou l'application fonctionnant sur les systèmes de vos utilisateurs finaux exige que l'utilisateur se soit authentifié avant d'obtenir l'accès à GlobalProtect, l'identité de chaque utilisateur GlobalProtect est connue. Toutefois, si vous souhaitez avoir la possibilité de définir des configurations GlobalProtect et/ou les politiques de sécurité basées sur l'appartenance à un groupe, le pare-feu doit récupérer la liste des groupes et la liste correspondante des membres sur votre serveur d'annuaires. Cela s'appelle *mappage de groupe*.

Pour activer cette fonctionnalité, vous devez créer un profil de serveur LDAP qui indique au pare-feu comment se connecter et s'authentifier sur le serveur d'annuaires, et comment rechercher les informations relatives à l'utilisateur et au groupe dans l'annuaire. Une fois que le pare-feu se connecte au serveur LDAP et récupère les mappages de groupe, vous pouvez sélectionner des groupes lorsque vous définissez les configurations de l'agent et les stratégies de sécurité. Le pare-feu prend en charge divers serveurs d'annuaires LDAP, notamment Microsoft Active Directory (AD), Novell eDirectory et Sun ONE Directory Server.

Procédez comme suit pour vous connecter à votre annuaire LDAP afin d'activer le pare-feu pour qu'il récupère les informations de mappage utilisateur / groupe :

1. Créez un profil de serveur LDAP qui précise comment se connecter aux serveurs d'annuaires auxquels le pare-feu devra se connecter pour obtenir les informations de mappage de groupe.
   1. Sélectionnez **Device (Périphériques)** > **Server Profiles (Profils Serveur)** > **LDAP (LDAP)** et cliquez sur **Add (Ajouter)**.
   2. Saisissez un **Profile Name (Nom de profil)** pour identifier le profil de serveur.
   3. S'il s'agit du profil d'un pare-feu pouvant prendre en charge de multiples systèmes virtuels, sélectionnez un système virtuel ou sélectionnez l'option **Shared (Partagé)** en tant que **Location (Emplacement)** où le profil est disponible.
   4. Pour chaque serveur LDAP (quatre au maximum), cliquez sur **Add (Ajouter)** et saisissez un **Name (Nom)** (pour identifier le serveur), l'adresse IP du serveur (champ **LDAP Server (Serveur LDAP)** et le **Port** du serveur (par défaut 389).
   5. Sélectionnez le **Type** de serveur dans le menu déroulant : **active-directory**, **e-directory**, **sun** ou **other (autre)**.
   6. Si vous souhaitez que le périphérique utilise le protocole SSL ou TLS pour une connexion plus sécurisée au serveur d'annuaires, cochez la case **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)** (cochée par défaut). Le protocole utilisé par le périphérique varie selon le **Port** de serveur défini :
      - 389 (par défaut) : TLS (le périphérique utilise plus précisément l'opération StartTLS, qui met à niveau la connexion en texte brut initiale en TLS.)

 ©2026 Palo Alto Networks, Inc.

- 636 : SSL.
- Tout autre port : le périphérique tente tout d'abord d'utiliser TLS. Si le serveur d'annuaires ne prend pas en charge TLS, le périphérique fera appel à SSL.

7. Pour renforcer la sécurité, vous pouvez cocher la case **Verify Server Certificate for SSL sessions (Vérifier le certificat du serveur pour les sessions SSL)** afin que le périphérique vérifie le certificat que le serveur d'annuaires présente pour les connexions SSL/TLS. Pour activer cette vérification, vous devez également cocher la case **Require SSL/TLS secured connection (Exiger une connexion sécurisée SSL/TLS)**. Pour une vérification réussie, le certificat doit remplir l'une des conditions suivantes :
   - Il se trouve dans la liste des certificats de périphérique : **Device (Périphérique)** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique).** Au besoin, importez le certificat dans le périphérique.
   - Le signataire du certificat figure dans la liste des autorités de certification de confiance : **Device (Périphérique)** > **Certificate Management (Gestion de Certificats)** > **Certificates (Certificats)** > **Default Trusted Certificate Authorities (Autorités de certificats fiables par défaut)**.
8. Cliquez sur **OK**.

2. Ajoutez le profil de serveur LDAP à la configuration du mappage de groupe Identifiant d'utilisateur.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)**, puis **Add (Ajouter)** une nouvelle configuration de mappage de groupe.
2. Sélectionnez **Server Profile (Profil de serveur)**.
3. Saisissez un **Name (Nom)** à donner à la configuration du mappage de groupe.
4. Sélectionnez le **Server Profile (Profil de serveur)** que vous venez de créer.
5. Indiquez l'**Update Interval (Intervalle de mise à jour)** (en secondes) après lequel le pare-feu établit une connexion au serveur d'annulaire LDAP pour obtenir toutes les mises à jour des groupes que les politiques de pare-feu utilisent (plage comprise entre 60 et 86 400 secondes).
6. Assurez-vous que le profil du serveur est **Enabled (Activé)** pour le mappage de groupe.

3. (Facultatif) Activez la récupération par GlobalProtect des numéros de série à partir du serveur d'annuaire.

GlobalProtect peut identifier l'état des points de terminaison qui se connectent et appliquer les politiques de sécurité basées sur HIP en fonction de la présence du numéro de série des points de terminaison. Si un point de terminaison est géré, vous pouvez lier son numéro de série au compte machine du point de terminaison qui figur dans votre serveur d'annuaire. Le pare-feu peut ensuite précharger les numéros de série de ces points de terminaison gérés lorsqu'il récupère les informations de mappage auprès du serveur d'annuaire.

1. Dans votre configuration de mappage de groupe, sélectionnez **Server Profile (Profil de serveur)**.
2. Activez l'option **Fetch list of managed devices (Récupérer la liste des périphériques gérés)**.

 ©2026 Palo Alto Networks, Inc.

4. (Facultatif) Spécifiez les attributs pour identifier les utilisateurs et les groupes d'utilisateurs.
   1. Dans votre configuration de mappage de groupe, sélectionnez **User and Group Attributes (Attributs des utilisateurs et des groupes)**.
   2. Dans la section User Attributes (Attributs des utilisateurs), indiquez le **Primary Username (Nom d'utilisateur principale)**, le **E-Mail** et le **Alternate Username 1-3 (Nom d'utilisateur alternatif 1-3)** qui servent à identifier les utilisateurs individuels.
   3. Dans la section Group Attributes (Attributs des groupes), indiquez le **Group Name (Nom de groupe)**, le **Group Member (Membre du groupe)** et le **E-Mail** qui servent à identifier les groupes d'utilisateurs.

5. (Facultatif) Limitez les groupes qui peuvent être sélectionnés dans des règles de politique.

   Par défaut, si vous ne spécifiez pas de groupes, tous les groupes sont disponibles dans les règles de politique.

   1. Ajoutez des profils existants du service d'annuaire :
      1. Dans votre configuration de mappage de groupe, sélectionnez **Group Include List (Liste d'inclusion de groupes)**.
      2. Dans la liste Available Groups (Groupes disponibles), sélectionnez les groupes qui doivent apparaître dans les règles de politique, puis cliquez sur l'icône Ajouter (⊕) pour ajouter le groupe à la liste d'inclusion de groupes.
   2. Si vous souhaitez baser des règles de politique sur des attributs utilisateur ne correspondant pas à des groupes d'utilisateurs existants, créez des groupes personnalisés basés sur des filtres LDAP :
      1. Dans votre configuration de mappage de groupe, sélectionnez **Custom Group (Groupe personnalisé)**.
      2. **Add (Ajoutez)** un nouveau groupe personnalisé.
      3. Donnez un **Name (Nom)** unique au groupe dans la configuration du mappage de groupe pour le pare-feu ou le système virtuel actuel. Si le **Name (Nom)** a la même valeur que le nom unique (DN) d'un groupe de domaines AD existant, le pare-feu utilise le groupe personnalisé dans toutes les références à ce nom (par exemple, dans les politiques et les journaux).
      4. Spécifiez un **LDAP Filter (Filtre LDAP)** de 2 048 caractères UTF-8 maximum, puis cliquez sur **OK**. Le pare-feu ne valide pas les filtres LDAP.

         Pour optimiser les recherches LDAP et minimiser l'impact sur les performances du serveur d'annuaires LDAP, utilisez des attributs indexés et réduisez la portée des recherches en n'incluant que les objets d'utilisateurs et de groupes dont vous avez besoin pour la politique ou la visibilité. Vous pouvez également créer des groupes personnalisés en fonction des filtres LDAP.

6. Validez vos modifications.

   Cliquez sur **OK**, puis sur **Commit (Valider)**.

 ©2026 Palo Alto Networks, Inc.

Passerelles GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Les passerelles GlobalProtect permettent la mise en œuvre de la sécurité du trafic depuis les applications GlobalProtect. En outre, si la fonction Host Information Profile (HIP) (Profil d'informations sur l'hôte - HIP) est activée, la passerelle génère un rapport HIP à partir des données brutes sur l'hôte que les terminaux soumettent, lequel il peut utiliser dans la mise en œuvre des politiques.

Configurez une passerelle GlobalProtect sur n'importe quel pare-feu nouvelle génération NGFW Palo Alto Networks ou sur Prisma Access. Sur le NGFW, vous pouvez utiliser à la fois une passerelle et un portail sur le même pare-feu, ou vous pouvez avoir plusieurs passerelles distribuées partout dans votre entreprise. Sur Prisma Access, toutes les passerelles dans vos emplacements Prisma Access sont disponibles pour les utilisateurs. Si vous disposez de passerelles GlobalProtect supplémentaires auxquelles vous souhaitez que vos utilisateurs puissent se connecter, vous pouvez aussi ajouter ces passerelles.

GlobalProtect prend en charge les types de passerelles suivants :

- **Passerelle interne** : une passerelle interne est une interface sur le réseau interne qui est configurée en tant que passerelle GlobalProtect et qui applique des politiques de sécurité pour l'accès aux ressources internes. Lorsqu'elle est utilisée en association avec l'ID utilisateur et/ou les archivages HIP, une passerelle interne peut être utilisée pour fournir une méthode sécurisée et précise d'identification et de contrôle du trafic par utilisateur et/ou état du périphérique. Les passerelles internes sont utiles dans des environnements fragiles où l'accès authentifié aux ressources vitales est requis. Vous pouvez configurer une passerelle interne dans l'un des deux modes de tunnel ou dans le mode non-tunnel. L'application GlobalProtect se connecte à la passerelle interne après avoir effectué une détection d'hôte interne pour déterminer l'emplacement du point de terminaison. Si la détection d'hôte interne n'est pas configurée, l'application GlobalProtect se connecte d'abord à la passerelle interne, suivie de la passerelle externe en cas d'échec de connexion.

  Une passerelle interne et une détection d'hôte interne sont configurées sans passerelle externe et que la détection d'hôte interne échoue, l'application GlobalProtect réessaiera la découverte du réseau si le paramètre **Enable Intelligent Internal Host Detection (Activer la détection intelligente d'hôte interne)** est défini sur oui. Cette fonctionnalité s'applique lorsque les utilisateurs utilisent l'application GlobalProtect en mode de détection d'hôte interne pour l'User-ID tout en utilisant un VPN tiers pour accéder aux applications de parties privées. Lorsque la détection d'hôte interne a lieu avant que le VPN tiers n'établisse un tunnel, il échoue à établir l'User-ID. Avec le paramètre **Enable Intelligent Internal Host Detection (Activer la détection intelligente d'hôte interne)**, l'application GlobalProtect peut maintenant détecter la détection d'hôte interne en présence d'un agent VPN tiers en relançant la découverte réseau

jusqu'à ce que la détection d'hôte interne soit réussie. Pour des informations sur l'endroit où définir ce paramètre, voir l'étape 18 dans Personnaliser l'application GlobalProtect.

*Le paramètre **Enable Intelligent Internal Host Detection (Activer la détection intelligente d'hôte interne)** est disponible uniquement pour l'application GlobalProtect 6.3.1 et les versions ultérieures. La version minimale requise de la version du contenu est 8890-8951.*

- **Passerelle externe (détection automatique)** : une passerelle externe réside en dehors du réseau de l'entreprise et fournit une mise en œuvre de la sécurité et/ou un accès au réseau privé virtuel (VPN) à vos utilisateurs distants. Par défaut, l'application GlobalProtect se connecte automatiquement à la passerelle externe **Best Available (La meilleure qui est disponible)** en fonction de la priorité que vous attribuez à la passerelle, de la région source et du temps de réponse (voir Priorité de passerelle dans une configuration de passerelle multiple).
- **Passerelle externe (manuelle)** : une passerelle manuelle externe réside également en dehors du réseau de l'entreprise et fournit une mise en œuvre de la sécurité et/ou un accès VPN à vos utilisateurs distants. La différence entre la passerelle externe à détection automatique et la passerelle externe manuelle est que l'application GlobalProtect se connecte uniquement à une passerelle externe manuelle lorsque l'utilisateur initie une connexion. Vous pouvez également configurer différentes exigences d'authentification pour les passerelles externes manuelles. Pour configurer une passerelle manuelle, vous devez identifier la passerelle **Manual (Manuelle)** lorsque vous définissez les configurations de l'agent GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Priorité de passerelle dans une configuration de passerelle multiple

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour permettre un accès sécurisé à votre main-d'œuvre mobile, peu importe où ils se trouvent, vous pouvez déployer stratégiquement des pare-feu de nouvelle génération de Palo Alto Networks et les configurer comme passerelles GlobalProtect. Pour déterminer la passerelle privilégiée à laquelle vos applications se connectent, ajoutez les passerelles à une configuration d'agent Portail, puis affectez à chaque passerelle une priorité de connexion. Voir Définir les configurations de l'agent GlobalProtect.

Si une configuration d'agent de portail GlobalProtect contient plusieurs passerelles, l'application tente de communiquer avec toutes les passerelles répertoriées dans sa configuration d'agent. L'application utilise ensuite les règles de priorité et le temps de réponse pour déterminer à quelle passerelle il doit se connecter. Avec l'application GlobalProtect 4.0.2 et les versions antérieures, l'application se connecte à une passerelle de priorité faible uniquement si le temps de réponse pour la passerelle de priorité élevée est supérieur au temps de réponse moyen entre toutes les passerelles.

Par exemple, considérez les temps de réponse suivants pour GW1 et GW2 :

Name (Nom)	Priorité	Temps de réponse
gw1	La plus élevée	80 ms
gw2	Élevée	25 ms

L'application détermine que le temps de réponse pour la passerelle avec la priorité la plus élevée (le nombre le plus élevé) est supérieur au temps de réponse moyen pour les deux passerelles (52,5 ms) et, par conséquent, se connecte à GW2. Dans cet exemple, l'application ne s'est pas connectée à GW1 même si elle avait une priorité plus élevée parce qu'un temps de réponse de 80 ms était plus élevé que la moyenne pour les deux.

Considérez maintenant les délais de réponse suivants pour GW1, GW2 et une troisième passerelle, GW3 :

Name (Nom)	Priorité	Temps de réponse
gw1	La plus élevée	30 ms

©2026 Palo Alto Networks, Inc.

Name (Nom)	Priorité	Temps de réponse
gw2	Élevée	25 ms
gw3	Moyenne	50 ms

Dans cet exemple, le temps de réponse moyen pour toutes les passerelles est de 35 ms. L'application évaluera alors quelles passerelles répondent plus rapidement que le temps de réponse moyen et constatera que GW1 et GW2 ont des temps de réponse plus rapides. L'application se connectera alors à n'importe quelle passerelle qui avait la priorité la plus élevée. Dans cet exemple, l'application se connecte à GW1 parce que GW1 a la priorité la plus élevée de toutes les passerelles avec les temps de réponse au-dessous de la moyenne.

En plus de la priorité des passerelles, vous pouvez ajouter une ou plusieurs régions source à une configuration de passerelle externe. GlobalProtect reconnaît la région source et permet aux utilisateurs de se connecter uniquement aux passerelles configurées pour cette région. En ce qui concerne les choix, la région source est considérée en premier, suivie par la passerelle.

Dans les versions 4.0.3 et ultérieures de l'application GlobalProtect, l'application GlobalProtect privilégie les passerelles auxquelles est attribuée la priorité la plus élevée, élevée ou moyenne plutôt que les passerelles ayant une priorité faible ou la plus faible, quel que soit le temps de réponse. L'application GlobalProtect ajoute ensuite les passerelles affectées d'une priorité faible ou la plus faible à la liste des passerelles. Cela garantit que l'application tente d'abord de se connecter aux passerelles que vous configurez avec une priorité plus élevée.

Critères de sélection de la passerelle avec TLSv 1.3

Lorsque plusieurs passerelles sont dotées d'une priorité égale, l'application GlobalProtect détermine la meilleure passerelle en mesurant le temps de réponse de l'établissement de la connexion SSL/TLS. Ce comportement peut être impacté par la version de TLS qui est utilisée. TLSv 1.3 a une latence inférieure à celle de TLSv 1.2 en raison d'un établissement de la connexion plus efficace, qui nécessite seulement un aller-retour au lieu de deux. Les passerelles configurées pour TLSv 1.3 rapporteront intrinsèquement des temps de poignée de main plus rapides que les passerelles utilisant une version non-TLSv 1.3, même si la passerelle non-TLSv 1.3 est géographiquement plus proche. Cela peut amener la passerelle TLSv 1.3 à être sélectionnée comme la meilleure passerelle disponible, ce qui peut pousser l'application GlobalProtect à se connecter à une passerelle qui n'est pas la plus proche géographiquement. Si vous souhaitez vous connecter à la passerelle géographiquement la plus proche indépendamment de la version de TLS, vous pouvez attribuer manuellement des priorités de passerelle en fonction de la région.

Alternativement, si vous utilisez la version 6.3.1 ou ultérieure de l'application GlobalProtect, vous pouvez modifier le paramètre meilleurs critères de sélection de passerelle dans le portail en changeant la valeur par défaut, **Load & response time (Temps de chargement et de réponse)**, à **Response time (Temps de réponse)**.

 ©2026 Palo Alto Networks, Inc.

Meilleurs critères de sélection de passerelle

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile GlobalProtect 6.3.1 ou versions ultérieures Terminaux GlobalProtect fonctionnant sous Windows et macOS Version du contenu : 8903-9009

GlobalProtect utilise une méthode de découverte de réseau pour sélectionner la meilleure passerelle disponible parmi les multiples options de passerelle disponibles. GlobalProtect essaie de communiquer avec toutes les passerelles et utilise des critères tels que la priorité de la passerelle, la charge et le temps de réponse de la passerelle pour déterminer la meilleure passerelle disponible pour se connecter. Des conditions sous-optimales des terminaux, telles qu'une charge élevée et une utilisation intensive du processeur, peuvent avoir un impact sur le temps de réponse et entraîner une sélection incorrecte de la passerelle.

La fonctionnalité de Meilleurs critères de sélection de passerelle de GlobalProtect empêche les effets des conditions sous-optimales des terminaux sur la découverte de réseau de GlobalProtect, ce qui permet une sélection fiable de la meilleure passerelle GlobalProtect disponible dans un environnement sous-optimal des terminaux.

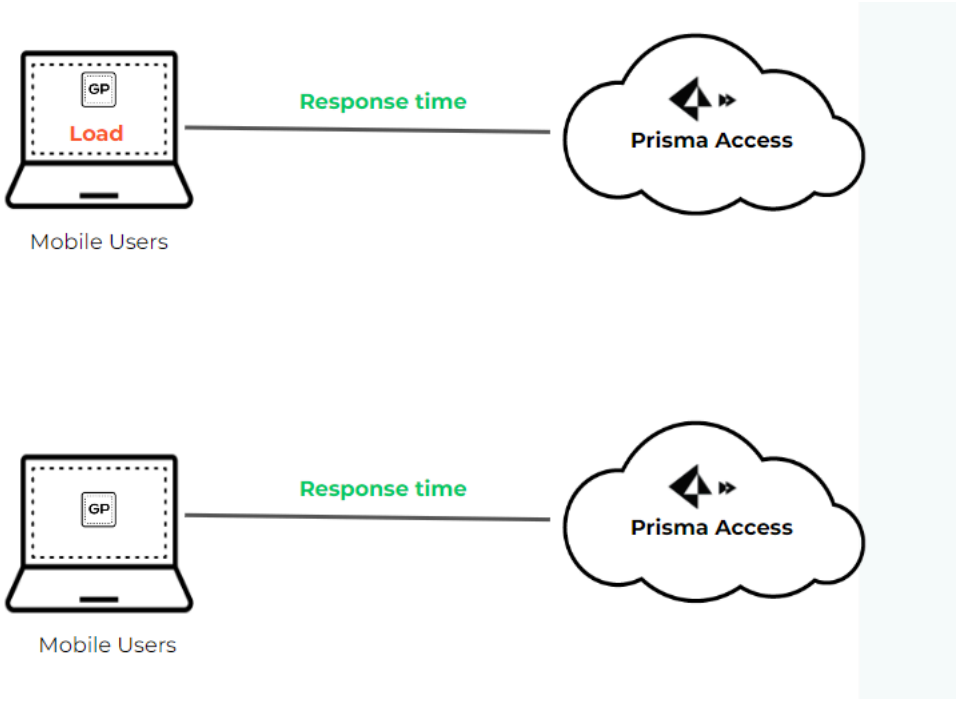
Il est désormais possible de configurer les meilleurs critères de sélection de passerelle dans les paramètres de l'application de la configuration du portail GlobalProtect pour les terminaux afin de sélectionner la meilleure passerelle disponible lorsque les utilisateurs finaux se connectent à partir d'un réseau externe.

Lorsque l'utilisateur final se connecte à partir d'un réseau externe, l'application GlobalProtect tente d'abord de se connecter aux passerelles externes répertoriées dans sa configuration client, puis établit une connexion avec la passerelle ayant la priorité la plus élevée et le temps de réponse le plus court.

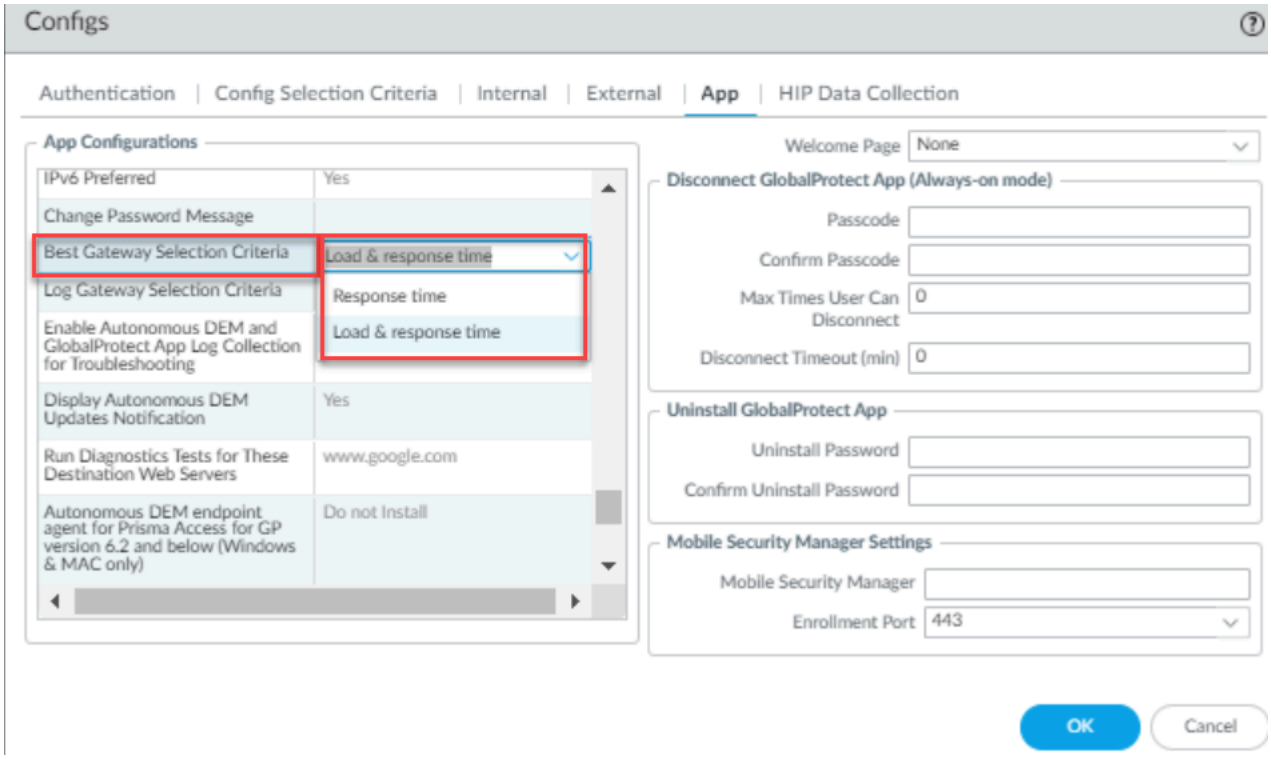
Auparavant, le temps nécessaire pour un établissement de liaison TLS réussi (**Load & response time [Temps de chargement et de réponse]**) était utilisé par l'application pour mesurer le temps nécessaire à l'établissement d'une connexion de passerelle externe.

Avec cette fonctionnalité activée, vous pouvez configurer l'application pour utiliser le temps nécessaire pour une connexion TCP réussie (**Response Time [Temps de réponse]**) comme critère de mesure de la passerelle externe. Lorsque vous sélectionnez l'option **Best Gateway Selection Criteria (Meilleurs critères de sélection de passerelle)** comme **Response Time (Temps de réponse)** dans les paramètres de l'application de la configuration du portail, la durée de l'établissement de connexion TCP est utilisée par l'application pour mesurer le temps nécessaire à l'établissement d'une connexion de passerelle externe.

 ©2026 Palo Alto Networks, Inc.

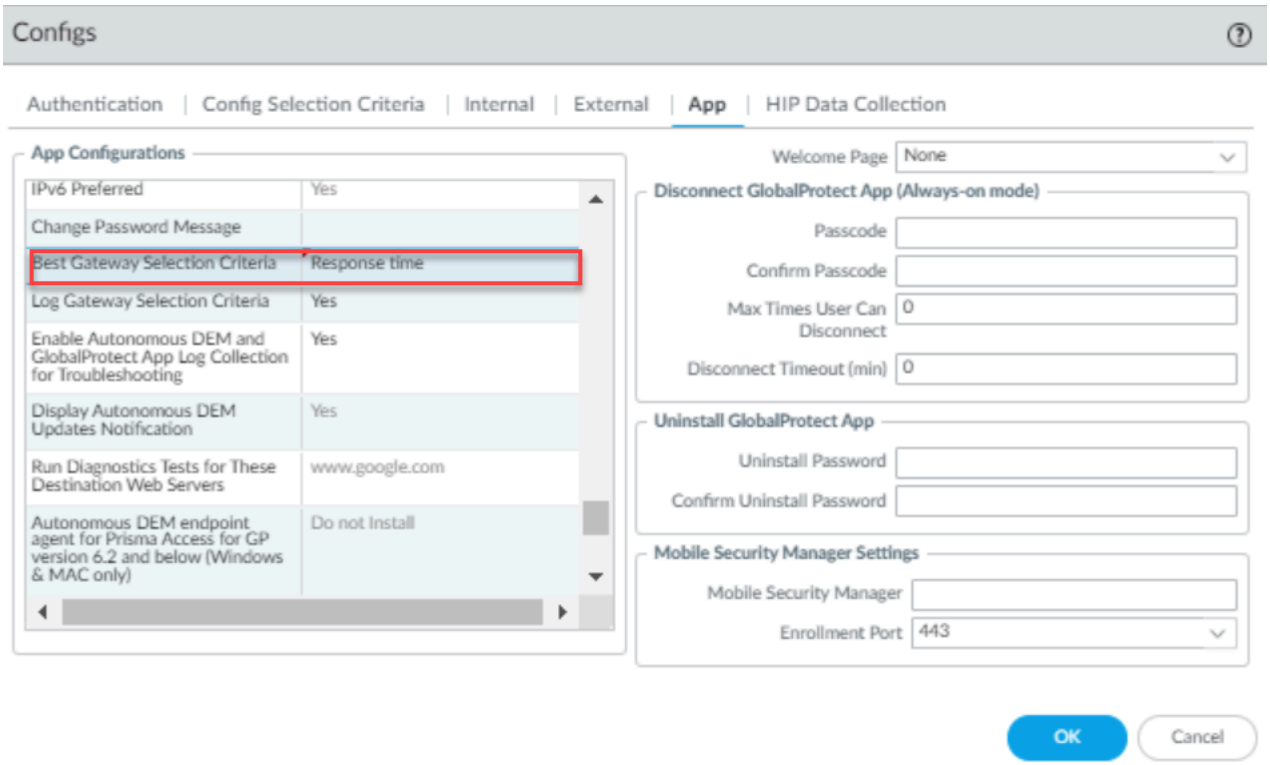


Par défaut, les meilleurs critères de sélection de passerelle sont considérés comme le ***Load & response time (Temps de chargement et de réponse)*** *(durée de l'établissement de connexion) dans les paramètres de l'application de la configuration du portail. Il s'agit du comportement par défaut et, auparavant,* ***Load & response time (Temps de chargement et de réponse)*** *était utilisé par l'application pour mesurer le temps nécessaire à l'établissement d'une connexion de passerelle externe.*



 ©2026 Palo Alto Networks, Inc.

1. Configurez le Portail GlobalProtect.
2. Configurez la Passerelle GlobalProtect.
3. Configurez l'application GlobalProtect pour utiliser les meilleurs critères de sélection de passerelle lors de la connexion à la passerelle externe.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<portal-config>** > **Agent** > **<agent-config>** > **App (Application)**.
   2. Dans la zone des configurations de l'application, sélectionnez l'option **Best Gateway Selection Criteria (Meilleurs critères de sélection de passerelle)** comme **Response Time (Temps de réponse)** pour que l'application GlobalProtect utilise la durée du temps de l'établissement de connexion TCP comme critère de mesure de la passerelle externe. Par défaut, la fonctionnalité **Best Gateway Selection Criteria (Meilleurs critères de sélection de passerelle)** est sélectionnée comme le **Load & response time (Temps de chargement et de réponse)**, qui est la durée d'établissement de connexion TLS pour mesurer le temps nécessaire à une connexion de passerelle externe.



4. Cliquez sur **OK**.
5. **Commit (Validez)** la configuration.

 ©2026 Palo Alto Networks, Inc.

Configurer une passerelle GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager) *Le protocole IKEv2 n'est pris en charge que sur NGFW géré par Panorama*	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile *Le protocole IKEv2 nécessite la licence GlobalProtect Gateway* GlobalProtect 6.4.1 ou version ultérieure et PAN-OS 12.1.5 ou version ultérieure pour le protocole IKEv2

Puisque la configuration du portail GlobalProtect qui est transmise aux applications comprend la liste des passerelles auxquelles le point de terminaison peut se connecter, il est recommandé de configurer les passerelles avant de configurer le portail.

Les passerelles GlobalProtect sont configurées de sorte à fournir deux fonctions principales :

- Mise en œuvre d'une stratégie de sécurité pour les applications GlobalProtect qui se connectent aux paserelles. Vous pouvez aussi activer la collecte de données HIP sur la passerelle pour affiner la granularité de la politique de sécurité.
- Accès du réseau privé virtuel (VPN) au réseau interne de l'entreprise. L'accès VPN est établi via un tunnel IPSec ou SSL entre le terminal et l'interface de tunnel sur le pare-feu qui héberge la passerelle.

Sur NGFW géré par Panorama, les passerelles GlobalProtect prennent en charge les protocoles IPSec et Internet Key Exchange version 2 (IKEv2) standardisés. Contrairement aux méthodes propriétaires ou personnalisées, IKEv2 utilise des protocoles d'échange de clés standard de l'industrie pour établir plus efficacement des tunnels sécurisés, nécessitant seulement quatre échanges de messages au lieu de huit. Ce protocole fournit une Network Address Translation (traduction d'adresse réseau - NAT) intégrée et une résilience améliorée contre les attaques par Denial-of-Service (déni de service - DoS).

1. Avant de commencer à configurer la passerelle, assurez-vous d'avoir :

   Créé des interfaces (et des zones) du pare-feu sur lequel vous envisagez de configurer chaque passerelle. Pour les passerelles qui exigent des connexions en tunnel, vous devez configurer à la fois l'interface physique et l'interface virtuelle de tunnel.

   Configuration des certificats de serveur de passerelle et du profil de service SSL/TLS requis pour que l'application GlobalProtect puisse établir une connexion SSL avec la passerelle.

   Définis des profils d'authentification et/ou des profils de certificat qui seront utilisés pour authentifier les utilisateurs GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

2. **Add (Ajouter)** une passerelle.
   1. Pour ajouter une nouvelle passerelle, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Tunnel Settings (Paramètres de Tunnel)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feux)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)** et puis **Add Gateway (Ajouter passerelle)**.
      - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**.
   2. Cliquez sur **Add (Ajouter)**.
   3. **Name (Donnez un nom)** à la passerelle.

      Le nom de la passerelle ne peut contenir d'espaces et doit être unique pour chaque système virtuel. Il est recommandé d'inclure l'emplacement ou d'autres informations descriptives qui permettront aux utilisateurs et administrateurs d'identifier la passerelle.
   4. (Facultatif) Sélectionnez le **Location (Emplacement)** du système virtuel auquel la passerelle appartient.

3. Spécifiez les informations sur le réseau permettant aux points de terminaison de se connecter à la passerelle.

Si elle n'existe pas déjà, créez l'interface réseau de la passerelle.

- Définissez le **IP Address Type (Type d'adresse IP)** sur **IPv4 Only (IPv4 seulement)**, **IPv6 Only (IPv6 seulement)** ou sur **IPv4 and IPv6 (IPv4 et IPv6)**. Utilisez **IPv4 and IPv6 (IPv4 et IPv6)** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps.
- L'adresse IP doit être compatible avec le type d'adresse IP. Par exemple, `172.16.1.0` pour les adresses IPv4 ou `21DA:D3:0:2F3b` pour les adresses IPv6. Pour les configurations en double pile, saisissez une adresse IPv4 ainsi qu'une adresse IPv6.

N'attachez pas de profil de gestion d'interface qui autorise HTTP, HTTPS, Telnet ou SSH sur l'interface où vous avez configuré ; cela permet d'accéder à votre interface de gestion depuis Internet. Suivez les Meilleures pratiques pour sécuriser l'accès administratif *afin de vous assurer que vous sécurisez l'accès administratif à vos pare-feux d'une manière qui empêchera la réussite des attaques.*

 ©2026 Palo Alto Networks, Inc.

4. Configuration des paramètres de journalisation de décryptage

Vous pouvez journaliser les communications TLS/SSL réussies et avortées et vous pouvez transférer les journaux de décryptage aux Collecteurs de journaux, aux autres périphériques de stockage et aux administrateurs spécifiques.

- Par défaut, le pare-feu ne journalise que les communications TLS avortées. Il est conseillé de journaliser les communications réussies également afin d'avoir une visibilité sur autant de trafic décrypté que les resources (ressources)l'autorisent (mais ne décryptent pas le trafic privé ou sensible; respectez les decryption best practices (bonnes pratiques du décryptage) et décryptez autant de trafic que possible).
- Si vous ne l'avez pas déjà fait, créez un Log Forwarding profile (profil de transfert des journaux) pour transférer les journaux de décryptage et indiquez le dans la configuration de la passerelle.
- Si vous journalisez des communications TLS réussies en plus des communications TLS avortées, configurez un quota d'espace de stockage de journaux plus important pour les journaux de décryptage (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de rapports)** > **Log Storage (stockage des journaux)**). Le quota par défaut (attribution) est de un pour cent de la capacité de stockage des journaux du périphérique pour les journaux de décryptage et de un pour cent pour le résumé de décryptage général. Il n'y a pas d'attribution par défaut pour les résumés de décryptage horaires, quotidiens ou hebdomadaires. Configure Decryption Logging (Configurer la journalisation du décryptage) donne plus d'informations sur la façon d'attribuer un espace de journaux de pare-feu aux journaux de décryptage.

5. Spécifiez comment la passerelle authentifie les utilisateurs.

Si aucun profil de service SSL/TLS existe pour la passerelle, déployez les certificats de serveur sur les composants GlobalProtect.

Si les profils d'authentification ou les profil de certificat n'existent pas déjà, utilisez la tâches de configuration de l'authentification pour configurer ces profils pour la passerelle.

Configurez n'importe lequel des paramètres d'**Authentication** de passerelle suivants :

- Pour sécuriser la communication entre la passerelle et l'application GlobalProtect, sélectionnez le **SSL/TLS Service Profile (Profil de service SSL/TLS)** de la passerelle.

  *La **Max Version (Version max)** de TLS dans le**profil de service SSL/TLS** est **TLSv1.2**. **TLSv1.3** n'est actuellement pas compatible pour les connexions de l'application GlobalProtect et Clientless VPN.*

  *Pour une sécurité renforcée, définissez la **Min Version (Version minimale)** du profil de service SSL/TLS sur **TLSv1.2**.*

- Pour authentifier les utilisateurs avec une base de données utilisateur locale ou un service d'authentification externe, tel que LDAP, Kerberos, TACACS +, SAML ou RADIUS (y compris OTP), **Add (Ajoutez)** une configuration de **Client Authentication (Authentification client)** avec les paramètres suivants :
  - Précisez un **Name (Nom)** pour identifier la configuration de l'authentification client.
  - Identifiez le type de **OS (Système d'exploitation)** auquel cette configuration s'applique. Par défaut, la configuration s'applique à **Any (Tout)** système d'exploitation.

 ©2026 Palo Alto Networks, Inc.

- Sélectionnez ou ajoutez un **Authentication Profile (Profil d'authentification)** pour authentifier des points de terminaison recherchant l'accès à la passerelle.
- Saisissez une **Username Label (Étiquette de nom d'utilisateur)** pour la connexion à la passerelle (par exemple, **`Adresse électronique (nom_d'utilisateur@domaine)`**.
- Saisissez une **Password Label (Étiquette de mot de passe)** personnalisée pour la connexion à la passerelle (par exemple, un **`Passcode (Code secret)`** pour l'authentification basée sur jeton à deux facteurs).
- Saisissez un **Authentication Message (Message d'authentification)** pour aider les utilisateurs finaux à comprendre les informations d'identification à utiliser lors de la connexion. Ce message peut comporter jusqu'à 256 caractères (par défaut, il s'agit de `Enter login credentials`).
- Sélectionnez l'une des options suivantes pour définir si les utilisateurs peuvent authentifier la passerelle à l'aide des identifiants de connexion et/ou des certificats clients :
  - Pour exiger que les utilisateurs s'authentifient à la passerelle à l'aide des identifiants de connexion ET d'un certificat client, définissez l'option **Allow Authentication with User Credentials OR Client Certificate (Autoriser l'authentification à l'aide des informations d'identification des utilisateurs OU du certificat client)** sur **No (User Credentials AND Client Certificate Required) [Non (Les informations d'identification des utilisateurs ET le certificat client sont requis]** (par défaut).
  - Pour autoriser les utilisateurs s'authentifient à la passerelle à l'aide des identifiants de connexion OU d'un certificat client, définissez l'option **Allow Authentication with User Credentials OR Client Certificate (Autoriser l'authentification à l'aide des informations d'identification des utilisateurs OU du certificat client)** sur **Yes (User Credentials OR Client Certificate Required) [Oui (Les informations d'identification des utilisateurs OU le certificat client sont requis]**.

    Lorsque vous définissez cette option sur **Yes (Oui)**, la passerelle vérifie d'abord si un certificat client se trouve sur le point de terminaison. Si le point de terminaison ne dispose pas d'un certificat client ou que vous ne configurez pas de profil de certificat pour votre configuration d'authentification client, l'utilisateur du point de terminaison peut ensuite s'authentifier auprès de la passerelle à l'aide de ses informations d'identification d'utilisateur.

    *Si vous prévoyez d'utiliser l'authentification SAML, ne configurez pas le **Username Field (Champ de nom d'utilisateur)** dans le **Certificate Profile (Profil de certificat)**.*

- Pour authentifier les utilisateurs par un certificat client ou une carte à puce intelligente/CAC, sélectionnez le **Certificate Profile (Profil de certificat)** correspondant. Vous devez prédéployer le certificat client ou Déployer des certificats clients spécifiques à l'utilisateur pour l'authentification au moyen du Simple Certificate Enrollment Protocol (Protocole de recrutement de certificat simple ; SCEP).
  - Si vous souhaitez que les utilisateurs s'authentifient à la passerelle à l'aide de leurs informations d'identification d'utilisateur et d'un certificat client, vous devez spécifier un **Certificate Profile (Profil de certificat)** et un profil d'authentification.
  - Si vous souhaitez permettre aux utilisateurs de s'authentifier auprès de la passerelle à l'aide de leurs informations d'identification d'utilisateur ou d'un certificat client et que

 ©2026 Palo Alto Networks, Inc.

vous spécifiez un **Authentication Profile (Profil d'authentification)** pour l'authentification des utilisateurs, puis le **Certificate Profile (Profil de certificat)** est facultatif.

- Si vous souhaitez permettre aux utilisateurs de s'authentifier auprès de la passerelle à l'aide de leurs informations d'identification d'utilisateur ou d'un certificat client et que vous ne sélectionnez pas de **Authentication Profile (Profil d'authentification)** pour l'authentification des utilisateurs, le **Certificate Profile (Profil de certificat)** est alors obligatoire.
- Si vous ne configurez pas de **Authentication Profile (Profil d'authentification)** qui correspond à un système d'exploitation spécifique, le **Certificate Profile (Profil de certificat)** est alors obligatoire.

*Si vous autorisez les utilisateurs à s'authentifier à la passerelle à l'aide des informations d'identification d'utilisateur ou d'un certificat client, ne sélectionnez pas de **Certificate Profile (Profil de certificat)** où le **Username Field (Champ Nom d'utilisateur)** est configuré en tant que **None (Aucun)**.*

- Pour utiliser l'authentification à deux facteurs, sélectionnez à la fois un **Authentication Profile (Profil d'authentification)** et un **Certificate Profile (Profil de certificat)**. L'utilisateur doit alors s'authentifier par les deux méthodes pour obtenir l'accès.

  (Chrome uniquement) Si vous configurez la passerelle pour qu'elle utilise les certificats clients et LDAP pour l'authentification à deux facteurs, les Chromebook qui exécutent Chrome 47 ou des versions ultérieures font face à des invites excessives pour sélectionner le certificat client. Pour empêcher les invites excessives, configurez une politique pour spécifier le certificat client dans la console Google Admin, puis déployez cette politique à vos Chromebook gérés.

  1. *Connectez-vous à la console Google Admin, puis sélectionnez **Device management (Gestion de périphériques)** > **Chrome management (Gestion de Chrome)** > **User settings (Paramètres des utilisateurs)**.*
  2. *Dans la section Client Certificates (Certificats clients), saisissez le modèle d'URL suivant sous **Automatically Select Client Certificate for These Sites (Sélectionner automatiquement un certificat client pour ces sites)** :*

     ```
     {"pattern": "https://[*.]","filter":{}}
     ```

  3. *Cliquez sur **Save (Enregistrer)**. La console Google Admin déploie la politique à tous les périphériques en quelques minutes.*
  4. *Pour empêcher les utilisateurs GlobalProtect de logging in from quarantined devices (se connecter depuis des périphériques en quarantaine) à la passerelle GlobalProtect, sélectionnez **Block login for quarantine devices (bloquer la connexion depuis les périphériques en quarantaine).***

 ©2026 Palo Alto Networks, Inc.

6. Activez la tunnellisation, puis configurez les paramètres du tunnel.

Les paramètres du tunnel sont obligatoires pour une passerelle externe ; ils sont facultatifs pour une passerelle interne.

Pour forcer l'utilisation du mode tunnel VPN-SSL, décochez (supprimez) l'option **Enable IPSec (Activer IPSec)**. Par défaut, VPN-SSL n'est utilisé que si le client n'arrive pas à établir de tunnel IPSec.

*L'authentification étendue (X-Auth) est prise en charge uniquement sur les tunnels IPSec. Si vous **Enable X-Auth Support (activez le support x-auth)**, les profils Crypto GlobalProtect IPSec ne sont pas utilisés.*

L'application GlobalProtect n'est pas en mesure de se connecter à la passerelle GlobalProtect via un tunnel IPSec si la NAT source est configurée sur le même pare-feu pour l'adresse IP publique du client GlobalProtect. Dans ce cas, la connexion du tunnel reviendra à SSL.

Pour obtenir de plus amples informations sur les algorithmes cryptographiques, reportez-vous à la section Fonctions cryptographiques de l'application GlobalProtect.

1. Cliquez sur l'onglet **Agent** et activez le **Tunnel Mode (Mode tunnel)** pour activer la segmentation des tunnels.
2. Sélectionnez la **Tunnel Interface (Interface de tunnel)** que vous avez définie lors de la création de l'interface réseau de la passerelle.
3. (Facultatif) Précisez le nombre maximum d'utilisateurs (**Max User**) pouvant accéder à la passerelle simultanément, pour l'authentification, les mises à jour HIP et de l'application GlobalProtect. La plage de valeurs s'affiche lorsque le champ est vide ; elle varie selon la plateforme.
4. **Enable IPSec (Activez IPSec)**, puis sélectionnez un profil **GlobalProtect IPSec Crypto (Crypto IPSec GlobalProtect)** pour sécuriser les tunnels VPN entre l'application et la passerelle GlobalProtect. Le profil **default (par défaut)** utilise le cryptage AES-128-CBC et l'authentification sha1.

   IPSec n'est pas pris en charge sur les terminaux Windows 10 UWP.

   Vous pouvez également créer un **New GlobalProtect IPSec Crypto (Nouveau profil Crypto IPSec GlobalProtect)** (liste déroulante **GlobalProtect IPSec Crypto (Crypto IPSec GlobalProtec)**), puis configurez les paramètres suivants :

   1. Spécifiez un **Name (Nom)** pour identifier le profil.
   2. **Add (Ajoutez)** les algorithmes d'**Authentication (Authentification)** et de **Encryption (Chiffrement)** que les homologues VPN peuvent utiliser pour négocier les clés pour sécuriser les données dans le tunnel :

      - **Encryption (Chiffrement)** : en cas de doute sur les algorithmes de chiffrement pris en charge par les homologues VPN, vous pouvez en ajouter plusieurs dans l'ordre du plus sécurisé au moins sécurisé, comme suit : **aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**. Les homologues négocieront l'algorithme le plus renforcé pour établir le tunnel.
      - **Authentication** : sélectionnez l'algorithme d'authentification (**sha1**) pour assurer l'intégrité des données et la protection d'authenticité. Bien que l'algorithme d'authentification soit requis pour le profil, ce paramètre s'applique uniquement au chiffrement AES-CBC (**AES-128-CBC (AES-128-CBC)**). Si vous utilisez un

 ©2026 Palo Alto Networks, Inc.

algorithme de chiffrement AES-GCM (**AES-256-GCM (AES-256-GCM)** ou **AES-128-GCM (AES-128-GCM)**), le paramètre est ignoré parce que ces codes fournissent une protection d'intégrité ESP native.

3. Cliquez sur **OK** pour enregistrer le profil.

5. (Facultatif) **Enable x-auth support (Activez le support x-auth)** si un point de terminaison doit se connecter à la passerelle en utilisant un VPN tiers (par exemple, un client VPNC fonctionnant sous Linux). Si vous activez X-Auth, vous devez fournir le nom de **Group (Groupe)** et le **Group Password (Mot de passe de groupe)** (si le point de terminaison l'exige). Par défaut, l'utilisateur ne doit pas se ré-authentifier si la clé qui établit le tunnel IPsec expire. Pour obliger les utilisateurs à se ré-authentifier, désactivez l'option **Skip Auth on IKE Rekey (Ignorer l'authentification lors du renouvellement de la clé)**.

   L'authentification étendue (X-Auth) n'est pas prise en charge pour les déploiements Prisma Access.

   *Pour **Enable X-Auth Support (Activer la prise en charge X-Auth)** des points de terminaison strongSwan, vous devez également décocher l'option **Skip Auth on IKE Rekey (Abandonner l'authentification en cas de refrappe IKE)**, car ces points de terminaison exigent la réauthentification lors de la négotiation IKE SA. De plus, vous devez ajouter le paramètre **`closeaction=restart`** à la section `conn %default` du fichier de configuration strongSwan IPSec. (Reportez-vous à la section Configurer l'authentification pour les points de terminaison strongSwan Ubuntu et CentOS pour obtenir de plus amples informations sur la configuration StrongSwan IPSec.)*

   Même si l'accès X-Auth est pris en charge sur les périphériques iOS et Android, il offre des fonctionnalités GlobalProtect limitées. Utilisez plutôt l'application GlobalProtect pour un accès simplifié à toutes les fonctionnalités de sécurité que GlobalProtect fournit sur les points de terminaison iOS et Android. L'app GlobalProtect pour iOS est disponible sur l'Apple App Store. L'app GlobalProtect pour Android est disponible sur Google Play.

7. NGFW géré par Panorama uniquement, GlobalProtect 6.4.1 et versions ultérieures, uniquement pour les terminaux Windows et macOS Pour prendre en charge le protocole

 ©2026 Palo Alto Networks, Inc.

IKEv2 standardisé sur le tunnel, cliquez sur **Enable IKEv2 (Activer IKEv2)** et indiquez les paramètres suivants.

1. Sélectionnez le mode IKEv2 :
   - Sélectionnez **IKEv2 Only (IKEv2 uniquement)** pour permettre au client de se connecter uniquement via IKEv2. Si le réseau de l'utilisateur bloque IKEv2 ou si le client est trop ancien pour le prendre en charge, la connexion échoue complètement
   - Sélectionnez **IKEv2 Preferred (IKEv2 préféré)** pour permettre au client de revenir à un tunnel SSL/TLS si IKEv2 échoue. Cette option permet également aux anciens clients de se connecter.
2. Sélectionnez le profil de crypto IKE et le profil crypto IPSec associés au profil réseau.
3. Sélectionnez une des méthodes d'authentification suivantes :
   - Utilisez une clé pré-partagée.
     1. Sélectionnez **Pre-Shared Key (Clé pré-partagée)** et saisissez la longueur de la clé principale en caractères.

        La longueur de la clé principale doit être comprise entre 32 et 128 caractères.
     2. Cliquez sur **Generate Strong Master Key (Générer une clé principale forte)**.
     3. Copiez la clé principale générée et collez-la dans les champs **Master Key (clé principale)** et **Confirm Master Key (Confirmer la clé principale)**.

        Vous pouvez également entrer directement une clé principale au lieu de générer une clé. La clé doit contenir un nombre pair de caractères et doit suivre le format HEX.
   - Pour réutiliser le profil de certificat spécifié dans l'onglet d'authentification de la passerelle, sélectionnez **Certificate (Certificat)** comme méthode d'authentification.

Pour afficher les événements détaillés concernant l'établissement du tunnel IKEv2, les échecs et les basculements (d'IKEv2 à SSL), accédez à **Monitor (Surveiller)** > **System (Système)**.

Le tableau suivant décrit le comportement de l'application GlobalProtect en fonction du protocole de tunnel sélectionné (IPSec ou IKEv2) et du mode IKEv2.

Protocole sélectionné	Mode IKEv2 sélectionné	Version de l'application GlobalProtect antérieure à 6.4.1	Version de l'application GlobalProtect 6.4.1 et ultérieure
Aucun sélectionné	N/A	TLS	TLS
Enable IPSec (Activer IPSec)	N/A	IPSec Peut revenir à TLS	IPSec Peut revenir à TLS
Enable IPSec (Activer IPSec) et **Enable IKEv2 (Activer IKEv2)**	**IKEv2 Only (IKEv2 uniquement)**	IPSec Peut revenir à TLS	IKEv2 Pas de retour en arrière

 ©2026 Palo Alto Networks, Inc.

Protocole sélectionné	Mode IKEv2 sélectionné	Version de l'application GlobalProtect antérieure à 6.4.1	Version de l'application GlobalProtect 6.4.1 et ultérieure
Activer IPSec et **Activer IKEv2**	**IKEv2 préféré**	IPSec Peut revenir à TLS	IKEv2 Peut revenir à TLS
Enable IKEv2 (Activer IKEv2)	**IKEv2 Only (IKEv2 uniquement)**	Aucun tunnel IPSec Pas de retour en arrière	IKEv2 Pas de retour en arrière
Enable IKEv2 (Activer IKEv2)	**IKEv2 Preferred (IKEv2 préféré)**	TLS	IKEv2 Peut revenir à TLS

8. (Mode tunnel uniquement) Spécifiez les critères de sélection des configurations des paramètres de vos clients.

La passerelle utilise les critères de sélection pour déterminer la configuration qui doit être fournie aux applications GlobalProtect qui se connectent. Si vous avez plusieurs configurations, vous devez vous assurer de bien les classer. Dès que la passerelle trouve une correspondance (en fonction du **Source User (Utilisateur source)**, du **OS (Système d'exploitation)** et de la **Source Address (Adresse source)**), elle transmet la configuration associée à l'utilisateur. Ainsi, les configurations plus spécifiques doivent précéder les configurations plus générales. Reportez-vous à l'étape 13 pour obtenir des instructions sur le classement de la liste des configurations des paramètres du client.

*Vous ne pouvez pas **Enable X-Auth Support (activer la prise en charge X-Auth)** lorsque vous spécifiez les critères de sélection pour vos configurations de paramètres client.*

1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)**.
2. Sélectionnez une configuration des paramètres client existante ou **Add (Ajoutez)**-en une nouvelle. Vous pouvez ajouter jusqu'à 64 entrées de configuration client pour une seule passerelle.
3. Configurez les **Config Selection Criteria (Critères de sélection de la configuration)** suivants :
   - Pour déployer cette configuration à des utilisateurs ou groupes d'utilisateurs spécifiques, **Add (Ajoutez)** le **Source User (Utilisateur source)** (ou le groupes d'utilisateurs). Pour déployer cette configuration uniquement aux utilisateurs disposant d'applications en mode préouverture de session, sélectionnez **pre-logon (préouverture de session)** dans le menu déroulant **Source User (Utilisateur source)**. Pour déployer cette configuration à tous les utilisateurs, sélectionnez **any (indifférent)**.

     Pour déployer la configuration à des groupes spécifiques, vous devez d'abord mapper les utilisateurs à des groupes comme décrit lorsque vous avez Activé le mappage de groupe.

 ©2026 Palo Alto Networks, Inc.

- Pour déployer cette configuration en fonction du système d'exploitation du point de terminaison, **Add (Ajoutez)** un **OS (Système d'exploitation)** (comme Android ou Chrome). Pour déployer cette configuration à tous les systèmes d'exploitation, sélectionnez **Any (Indifférent)**.
- Pour déployer cette configuration selon l'emplacement de l'utilisateur, **Add (Ajoutez)** une **Region** source ou une **IP Address (Adresse IP)** (IPv4 et IPv6). Pour déployer cette configuration à tous les emplacements d'utilisateurs, ne précisez aucune **Region (Région)** ou **IP Address (Adresse IP)**.

4. Cliquez sur **OK** pour enregistrer vos critères de sélection de configuration.

9. (Mode tunnel uniquement) Configurez les paramètres de substitution d'authentification pour permettre à la passerelle de générer et d'accepter des cookies sécurisés et chiffrés pour authentifier l'utilisateur.

Cette fonctionnalité permet à l'utilisateur de fournir des informations d'identification uniquement une seule fois pendant la période spécifiée (par exemple, toutes les 24 heures).

Par défaut, les passerelles authentifient les utilisateurs avec un profil d'authentification et un profil de certificat facultatif. Lorsque la substitution d'authentification est activée, GlobalProtect met en cache le résultat d'une connexion réussie et utilise le cookie pour authentifier l'utilisateur au lieu de demander à l'utilisateur des informations d'identification. Pour plus d'informations, voir Authentification par cookie sur le portail ou la passerelle. Si les certificats clients sont requis, le point de terminaison doit également fournir un certificat valide pour obtenir l'accès.

Si vous devez immédiatement bloquer l'accès à un périphérique dont le cookie n'a pas expiré (par exemple, si le périphérique est perdu ou volé), vous pouvez immédiatement utiliser Identification et mise en quarantaine du périphérique compromis *en ajoutant ce dernier à une liste de quarantaine.*

1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)**.
2. Sélectionnez une configuration des paramètres client existante ou **Add (Ajoutez)**-en une nouvelle.
3. Configurez les paramètres de **Authentication Override (Contrôle prioritaire de l'authentification)** suivants :
   - **Name (Nom)** : identifie la configuration.
   - **Generate cookie for authentication override (Générer un cookie pour remplacer l'authentification)** : permet à la passerelle de générer des cookies chiffrés, spécifiques

 ©2026 Palo Alto Networks, Inc.

au point de terminaison et d'émettre les cookies d'authentification au point de terminaison.

Le cookie d'authentification comprend les champs suivants :

- `user (utilisateur)` : le nom d'utilisateur qui est utilisé pour authentifier l'utilisateur.
- `Domain (Domaine)` : le nom de domaine de l'utilisateur.
- `os` : le nom de l'application utilisée sur le périphérique.
- `hostID (ID de l'hôte)` : l'ID unique que GlobalProtect affecte afin d'identifier l'hôte.
- `gen time (heure de génération)` : la date et l'heure auxquelles l cookie d'authentification a été généré.
- `ip` : adresse IP du périphérique qui est utilisé pour s'authentifier avec succès sur GlobalProtect et pour obtenir le cookie.

- **Accept cookie for authentication override (Accepter un cookie pour remplacer l'authentification)** : permet à la passerelle d'authentifier les utilisateurs au moyen d'un cookie chiffré qui est valide. Lorsque l'application présente un cookie valide, la passerelle vérifie que le cookie a été chiffré par le portail ou la passerelle, déchiffre le cookie, puis authentifie l'utilisateur.

  L'application GlobalProtect doit connaître le nom d'utilisateur de l'utilisateur qui se connecte afin de faire correspondre et d'extraire les cookies d'authentification associés du point de terminaison de l'utilisateur. Une fois que l'application a extrait les cookies, elle les envoie au portail ou à la passerelle à des fins d'authentification de l'utilisateur.

  (Windows uniquement) Si vous réglez l'option Use Single Sign-On (Utiliser l'ouverture de session unique) *sur **Yes (Oui)** (SSO est activée) dans la configuration d'agent du portail (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<portal-config>** > **Agent** > **<agent-config>.** > **App (Appli)**), l'appli GlobalProtect utilise le nom d'utilisateur Windows pour récupérer le cookie d'authentification local pour l'utilisateur. Si vous définissez l'option **Use Single Sign-On (Utiliser l'ouverture de session unique)** sur **No (Non)** (la SSO est désactivée), vous devez activer l'application GlobalProtect pour qu'elle* enregistre les informations d'identification de l'utilisateur *pour que l'application retire le cookie d'authentification pour l'utilisateur. Définissez l'option **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)** sur **Yes (Oui)** pour enregistrer le nom d'utilisateur et le mot de passe ou **Save Username Only (Enregistrer le nom d'utilisateur uniquement)** pour enregistrer uniquement le nom d'utilisateur.*

- **Cookie Lifetime (Durée de vie des cookies)** : spécifie les heures, les jours ou les semaines pendant lesquelles le cookie est valide (la valeur par défaut est 24 heures). La plage des heures est de 1 à 72 ; des semaines, de 1 à 52 ; et des jours, de 1 à 365. Après l'expiration du cookie, l'utilisateur doit entrer de nouveau ses informations d'identification, puis le portail chiffre ensuite un nouveau cookie à envoyer à l'application. Cette valeur peut être identique ou différente de la **Cookie Lifetime (durée de vie des cookies)** que vous configurez pour le portail.

 ©2026 Palo Alto Networks, Inc.

- **Certificate to Encrypt/Decrypt Cookie (Certificat pour chiffrer/décrypter le cookie)** : sélectionnez le certificat RSA utilisé pour chiffrer et décrypter le cookie. Vous devez utiliser le même certificat sur le portail et la passerelle.

  Le mieux est de configurer le certificat RSA pour utiliser l'algorithme de synthèse le plus fort que votre réseau prend en charge.

  Le portail et la passerelle utilisent le schéma de remplissage RSA crypte PKCS # 1 V1.5 pour générer le cookie (en utilisant la clé publique du certificat) et décrypter le cookie (en utilisant la clé privée du certificat).

10. (En mode tunnel uniquement) (Facultatif) Configurez les pools d'adresses IP au niveau du client qui sont utilisés pour affecter des adresses IPv4 ou IPv6 aux cartes réseau virtuel sur tous les points de terminaison qui se connectent à la passerelle.

    Les paramètres des pools d'adresses IP et des tunnels segmentés ne sont pas requis dans les configurations de passerelle interne en mode non-tunnel parce que les applications utilisent les paramètres réseau assignés à la carte réseau physique.

    L'utilisation d'objets d'adresse lors de la configuration de pools d'adresses IP pour la passerelle n'est pas pris en charge.

    1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)**.
    2. Sélectionnez une configuration des paramètres client existante ou **Add (Ajoutez)**-en une nouvelle.
    3. Configurez n'importe lequel des paramètres des **IP Pools (Pools d'adresses IP)** :
       - Pour indiquer le pool d'adresses IP du serveur d'authentification pour les points de terminaison qui nécessitent des adresses IP fixes, activez l'option **Retrieve Framed-IP-Address attribute from authentication server (Récupérer l'attribut Adresse IP tramée auprès du serveur d'authentification)**, puis **Add (Ajoutez)** le sous-réseau ou la plage d'adresses IP au **Authentication Server IP Pool (Pool d'adresses IP du serveur d'authentification)**. Lorsque le tunnel est établi, une interface est créée sur l'ordinateur de l'utilisateur distant avec une adresse dans le sous-réseau ou la plage IP qui correspond à l'attribut Framed-IP du serveur d'authentification.

         La réserve d'adresses IP du serveur d'authentification doit être suffisamment importante pour prendre en charge toutes les connexions simultanées. L'attribution d'adresse IP est fixe et est conservée même après la déconnexion de l'utilisateur.

       - Pour préciser le **Pool d'adresses IP** utilisé pour affecter les adresses IPv4 ou IPv6 aux terminaux qui se connectent à la passerelle, **Ajoutez** le sous-réseau ou la plage d'adresses IP. Vous pouvez ajouter des sous-réseaux ou des plages d'adresses IPv4 ou IPv6, ou les deux.

         Pour garantir un routage approprié de retour vers la passerelle, vous devez utiliser une plage d'adresses IP différentes de celles assignées aux pools d'adresses IP existants sur la passerelle (le cas échéant) et aux points de terminaison qui sont physiquement connectés à votre LAN. Nous vous recommandons d'utiliser un modèle d'adressage IP privé.
    4. Cliquez sur **OK** pour enregistrer la configuration du pools d'adresses IP.

 ©2026 Palo Alto Networks, Inc.

11. (Mode tunnel uniquement—Facultatif) Désactivez le tunnel séparé pour garantir que tout le traficy compris le trafic du sous-réseau local) passe par le tunnel VPN à des fins d'inspection et d'application de la politique.

12. (Mode tunnel uniquement) (Facultatif) Configurez les paramètres de séparation des tunnels selon l'itinéraire d'accès.

13. (Mode tunnel uniquement) (Facultatif) Configurez les paramètres de séparation des tunnels selon le domaine de destination.

14. (Mode tunnel uniquement) (Facultatif) Configurez les paramètres de séparation des tunnels selon l'application.

15. (Mode tunnel uniquement—Facultatif) Configurez les paramètres DNS d'une configuration des paramètres du client.

    *Si vous configurez au moins un serveur DNS ou suffixe DNS dans la configuration des paramètres du client (**Network [Réseau])** > **GlobalProtect** > **Gateways [Passerelles]** > **<gateway-config>** > **Agent** > **Client Settings [Paramètres du client]** > **<client-settings-config>** > **Network Services [Services réseaux]**), la passerelle envoie la configuration du serveur DNS et du suffixe DNS au terminal. Cela se produit lorsque vous configurez des serveurs DNS et des suffixes DNS globaux (niveau de la passerelle).*

    *Si vous ne configurez aucun serveur DNS ou suffixe DNS dans la configuration des paramètres du client, la passerelle envoie les serveurs DNS et les suffixes DNS globaux au terminal, s'ils sont configurés (**Network [Réseau]** > **GlobalProtect** > **Gateways [Passerelles]** > **<gateway-config>** > **Agent** > **Network Services [Services réseaux]**)*

    1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)**.
    2. Sélectionnez une configuration des paramètres client existante ou **Add (Ajoutez)**-en une nouvelle.
    3. Configurez n'importe lequel des paramètres des **Network Services (Services réseau)** :
        - Précisez l'adresse IP du **DNS Server (Serveur DNS)** auquel l'application GlobalProtect disposant de cette configuration de paramètres du client envoie des requêtes DNS. Vous pouvez ajouter un maximum de dix serveurs DNS en séparant chaque adresse IP avec une virgule.
        - Spécifiez le **DNS Suffix (Suffixe DNS)** que le point de terminaison doit utiliser lorsqu'il se trouve en présence d'un nom d'hôte non qualifié, que le point de terminaison ne peut pas résoudre.

16. (Mode tunnel uniquement) Organisez les configurations de l'agent de passerelle afin que la configuration adéquate soit déployée pour chaque application GlobalProtect.

    Dès qu'une application se connecte, la passerelle compare les informations sources dans le paquet aux configurations d'agent que vous avez définies (**Agent** > **Client Settings (Paramètres du client)**). Comme avec l'évaluation des règles de sécurité, le portail recherche une correspondance en commençant par le sommet de la liste. Lorsqu'il trouve une correspondance, il fournit la configuration correspondante à l'application.

    - Pour faire remonter une configuration de passerelle dans la liste de configurations, sélectionnez la configuration, puis cliquez sur **Move Up (Remonter)**.

 ©2026 Palo Alto Networks, Inc.

- Pour faire descendre une configuration de passerelle dans la liste de configurations, sélectionnez la configuration, puis cliquez sur **Move Down (Descendre)**.

17. (En mode tunnel uniquement) (Facultatif) Configurez les pools d'adresses IP globaux utilisés pour affecter des adresses IPv4 ou IPv6 aux cartes réseau virtuel sur tous les terminaux qui se connectent à la passerelle.

Cette option vous permet de simplifier la configuration en définissant les pools d'adresses IP au niveau de la passerelle plutôt que de définir les pools d'adresses IP pour chacun des paramètres client dans la configuration de la passerelle.

*Vous devez configurer les pools d'adresses IP à un seul niveau, soit au niveau de la passerelle (**Network [Réseau]** > **GlobalProtect** > **Gateways [Passerelles]** > **<gateway-config>** > **Agent** > **Client IP Pool [Pools d'adresses IP du client]**) ou au niveau du client (**Network [Réseau]** > **GlobalProtect** > **Gateways [Passerelles]** > **<gateway-config>** > **Agent** > **Client Settings [Paramètres du client]** > **<client-setting>** > **IP Pools [Pools d'adresses IP]**).*

*Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feux)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)** et puis **Add Gateway (Ajouter passerelle)**. Sur la page Ajouter une passerelle, ajoutez **Client IP Pool (Pools d'adresses IP du client)**.*

L'utilisation d'objets d'adresse lors de la configuration de pools d'adresses IP pour la passerelle n'est pas pris en charge.

1. Pour configurer les pools d'adresses IP globaux utilisés pour affecter des adresses IPv4 ou IPv6 aux cartes réseau virtuel sur tous les terminaux qui se connectent à la passerelle, effectuez l'une des actions suivantes :
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feux)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)** et puis **Add Gateway (Ajouter passerelle)**. Sur la page Ajouter une passerelle, ajoutez **Client IP Pool (Pools d'adresses IP du client)**.
   - Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **<gateway-config>** > **Agent** > **Client IP Pool (Pool d'adresses IP du client)**.
2. **Ajoutez** la plage ou le sous-réseau d'adresses IP utilisé pour affecter les adresses IPv4 ou IPv6 à tous les terminaux qui se connectent à la passerelle. Vous pouvez ajouter des sous-réseaux ou des plages d'adresses IPv4 ou IPv6, ou les deux.

   Pour garantir un routage approprié de retour vers la passerelle, vous devez utiliser une plage d'adresses IP différentes de celles assignées aux pools d'adresses IP existants sur la passerelle (le cas échéant) et aux points de terminaison qui sont physiquement connectés à votre LAN. Nous vous recommandons d'utiliser un modèle d'adressage IP privé.

 ©2026 Palo Alto Networks, Inc.

18. (Mode tunnel uniquement) Spécifiez les paramètres de configuration du réseau pour le point de terminaison.

    Les paramètres réseau ne sont pas requis dans les configurations de passerelle interne en mode non-tunnel parce que l'application GlobalProtect utilise les paramètres réseau assignés à la carte réseau physique.

    Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Network Services (Services réseau)**, puis configurez l'un des paramètres de configuration réseau suivants :

    - Si le pare-feu comprend une interface qui est configurée comme un client DHCP, définissez la **Inheritance Source (Source d'héritage)** pour cette interface de sorte que l'application GlobalProtect se voit assigner les mêmes paramètres que le client DHCP. Vous pouvez également cocher l'option **Inherit DNS Suffixes (hériter des suffixes DNS)** de la source d'héritage.
    - Affectez manuellement le serveur **Primary DNS (DNS principal)**, le serveur **Secondary DNS (DNS secondaire)**, le serveur **Primary WINS (WINS principal)**, le serveur **Secondary WINS (WINS Secondaire)** et le **DNS Suffix (Suffixe DNS)**. Vous pouvez saisir plusieurs suffixes DNS (maximum de 100) en séparant chaque suffixe par une virgule.

      *Le **DNS Suffix (Suffixe DNS)** ne peut contenir de caractère non-ASCII.*

19. (Facultatif) Modifiez les paramètres de temporisation par défaut pour les points de terminaison.

    - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **NGFW and Prisma Access (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)**. Sur la page Paramètres généraux, sélectionnez **General (Général)** > **Timeout (Délai d'expiration)** pour modifier les paramètres de délai d'expiration.
    - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)** puis **Add Gateway (Ajouter une passerelle)**. Sur la page Ajouter une passerelle, sélectionnez **Advanced Settings (Paramètres avancés)** > **Connection Settings (Paramètres de connexion)** pour modifier les paramètres.

 ©2026 Palo Alto Networks, Inc.

- Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **Agent** > **Connection Settings (Paramètres de connexion)**.
- Modifiez les paramètres de délai d'expiration de session de terminaux pour Délai de connexion et déconnexion d'inactivité.

  À partir de la version 6.2 de GlobalProtect, vous pouvez prolonger la durée de vie de la session de connexion de l'application GlobalProtect avant son expiration afin que les utilisateurs puissent éviter une déconnexion soudaine de la session de l'application. Vous pouvez configurer la fonctionnalité Prolonger la session utilisateur GlobalProtect via les Personnaliser l'application GlobalProtectparamètres de l'application sur le portail GlobalProtect.

  L'application affiche une notification à l'utilisateur final lors de l'expiration de la session selon les paramètres de notification sur la passerelle. Ces notifications informent les utilisateurs finaux à l'avance lorsque leurs sessions d'application sont sur le point d'expirer en raison de l'expiration de la durée de connexion. Avec l'introduction de la fonctionnalité Prolonger la session utilisateur GlobalProtect, la fenêtre contextuelle de notification d'expiration offre la possibilité d'étendre la durée de la session utilisateur afin que les utilisateurs ne soient pas déconnectés brusquement de leur session de manière.
- Définissez et planifiez l'affichage des notifications des utilisateurs finaux concernant la déconnexion de la session GlobalProtect pour la durée de connexion, la déconnexion par inactivité et la déconnexion initiée par l'administrateur.

  Pour la durée de connexion, l'application affiche également le compte à rebours pour la session dans l'onglet Connexions sous Paramètres de l'application.

  > *La notification des utilisateurs finaux concernant la déconnexion de la session GlobalProtect est prise en charge à partir de la version 6.1 de l'application GlobalProtect™.*
- (Facultatif) Modifiez la notification d'expiration par défaut et créez des messages personnalisés pour l'expiration de la durée de connexion, la déconnexion par inactivité et la déconnexion par l'administrateur que vous souhaitez afficher aux utilisateurs lorsque leurs sessions utilisateur sont sur le point d'expirer.

20. (Facultatif) Configurez la restauration automatique des tunnels VPN SSL.

Si la connexion à GlobalProtect est perdue en raison de l'instabilité du réseau ou d'un changement dans l'état du point de terminaison, vous pouvez autoriser l'application GlobalProtect à rétablir automatiquement le tunnel VPN pour les passerelles spécifiques en configurant la restauration automatique des tunnels VPN SSL ou les empêcher de le faire.

1. Pour configurer la restauration automatique des tunnels SSL VPN, effectuez l'une des actions suivantes :
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)** puis **Add Gateway (Ajouter une passerelle)**. Sur la page Ajouter une passerelle, sélectionnez **Advanced Settings (Paramètres avancés)** > **Connection Settings (Paramètres de connexion)** > **Authentication Cookie Usage Restrictions (Restrictions d'utilisation de l'authentification par cookie)**.

 ©2026 Palo Alto Networks, Inc.

- Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **NGFW and Prisma Access (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)**. Sur la page Paramètres globaux, sélectionnez **General (Général)** > **Authentication Cookie Usage Restrictions (Restrictions d'utilisation de l'authentification par cookie)**.
- Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **Agent** > **Connection Settings (Paramètres de connexion)**.

2. Configurez l'une des options suivantes pour les Restrictions d'utilisation des cookies d'authentification :
   - Pour empêcher l'application GlobalProtect de rétablir automatiquement le tunnel VPN pour cette passerelle, **Disable Automatic Restoration of SSL VPN (Désactivez la restauration automatique de VPN SSL)**.
   - Pour autoriser l'application GlobalProtect à rétablir automatiquement le tunnel VPN pour cette passerelle, désactivez (supprimez) l'option de **Disable Automatic Restoration of SSL VPN (Désactiver la restauration automatique de VPN SSL)** (par défaut).

21. (Facultatif) Configurez l'application de l'adresse IP source pour les cookies d'authentification.

Vous pouvez configurer la passerelle ou le portail GlobalProtect pour qu'ils acceptent les cookies des points de terminaison uniquement lorsque l'adresse IP du point de terminaison correspond aux adresses IP source d'origine pour lesquelles le cookie a été émis ou lorsque l'adresse IP du point de terminaison correspond à une plage d'adresses IP de réseau spécifique. Vous pouvez définir la plage d'adresses IP de réseau à l'aide d'un masque de sous-réseau CIDR, comme /24 ou /32. Par exemple, si un cookie d'authentification a été initialement émis à un point de terminaison possédant une adresse IP source de 201.109.11.10 et que le masque de sous-réseau de la plage d'adresses IP de réseau est défini sur /24, le cookie d'authentification est ensuite valide sur les points de terminaison disposant d'adresses IP source publiques de la plage d'adresses IP de réseau 201.109.11.0/24.

1. Pour configurer l'application de l'adresse IP source pour les cookies d'authentification, effectuez l'une des actions suivantes :
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)** puis **Add Gateway (Ajouter une passerelle)**. Sur la page **Add Gateway (Ajouter une passerelle)**, sélectionnez **Advanced Settings (Paramètres avancés)** > **Connection Settings (Paramètres de connexion)** > **Authentication Cookie Usage Restrictions (Restrictions d'utilisation de l'authentification par cookie)**.
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **NGFW and Prisma Access (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)**. Sur la page Paramètres globaux, sélectionnez **General (Général)** > **Authentication Cookie Usage Restrictions (Restrictions d'utilisation de l'authentification par cookie)**.

 ©2026 Palo Alto Networks, Inc.

- Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **Agent** > **Connection Settings (Paramètres de connexion)**.

2. À la section Authentication Cookie Usage Restrictions (Restrictions d'utilisation des cookies d'authentification), **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override) [Restreignez l'utilisation des cookies d'authentification (pour la restauration automatique du tunnel VPN ou la substitution d'authentification]**, puis configurez l'une des conditions suivantes :

   - Si vous sélectionnez **The original Source IP for which the authentication cookie was issued (La IP source d'origine pour laquelle le cookie d'authentification a été émis)**, le cookie d'authentification n'est valide que si l'adresse IP source publique du point de terminaison qui tente d'utiliser le cookie est identique à l'adresse IP source publique du point de terminaison pour laquelle le cookie a initialement été émis.
   - Si vous sélectionnez **The original Source IP network range (La plage réseau de l'IP source d'origine)**, le cookie d'authentification n'est valide que si l'adresse IP source publique du point de terminaison qui tente d'utiliser le cookie se situe dans la plage désignée d'adresses IP de réseau. Saisissez un **Source IPv4 Netmask (Masque réseau IPv4 source)** ou un **Source IPv6 Netmask (Masque réseau IPv6 source)** pour définir le masque de sous-réseau de la plage d'adresses IP de réseau pour laquelle le cookie d'authentification est valide (par exemple **32** ou **128**).

22. (Mode tunnel uniquement) Exclure le trafic de diffusion vidéo HTTP/HTTPS du tunnel VPN.

23. (Facultatif) Ce sous-onglet vous permet de définir les messages de notification destinés aux utilisateurs finaux lorsqu'une règle de sécurité dotée d'un profil d'informations sur l'hôte (HIP) est mise en œuvre.

Cette étape s'applique uniquement si vous avez créé des profils d'informations sur l'hôte et les avez ajoutés à vos politiques de sécurité. Reportez-vous à la section Informations sur l'hôteInformations sur l'hôte pour obtenir plus d'informations sur la configuration de la fonction HIP et pour obtenir des informations sur la création des messages de notification HIP.

1. Pour créer une notification HIP, effectuez l'une des actions suivantes :

   - Sur Strata Cloud Manager (NGFW) :

     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)**.
     2. Sur la page Ajouter une passerelle, sélectionnez **Advanced Settings (Paramètres avancés)** > **HIP Notifications (Notifications HIP)**.

     .

   - Sur Strata Cloud Manager (Prisma Access) :

     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access (Prisma Access)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)**.

 ©2026 Palo Alto Networks, Inc.

2. Sur la page Paramètres généraux, sélectionnez **Add HIP Notification (Ajouter une notification HIP)**.

- Sur le pare-feu (ou Panorama) qui héberge votre ou vos passerelles GlobalProtect, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**. Dans la boîte de dialogue Configuration des passerelles GlobalProtect, sélectionnez **Agent** > **HIP Notification (Notification HIP)**.

2. Sélectionnez une configuration de notification HIP existante ou **Add (Ajoutez)**-en une nouvelle.
3. Configurez les paramètres suivants'A0;:
   - Sélectionnez l'oobjet ou le profil des **Host Information (informations sur l'hôte)** auquel ce message s'applique.
   - Selon que vous souhaitiez afficher le message lorsque le profil HIP correspondant est mis en correspondance dans une politique ou lorsqu'il ne l'est pas, sélectionnez **Match Message (Faire correspondre le message)** ou**Not Match Message (Ne pas faire correspondre le message)**, puis **Enable (Activez)** les notifications. Vous pouvez créer des messages à la fois pour une correspondance et une non-correspondance, selon les objets faisant l'objet d'une correspondance et vos objectifs pour la politique. Pour l'option **Match Message (Faire correspondre le message)**, vous pouvez également activer l'option **Include Mobile App List (Inclure la liste des applications mobiles)** pour indiquer les applications qui ont déclenché la correspondance HIP.
   - Sélectionnez si vous souhaitez afficher le message sous la forme d'un **System Tray Balloon (système de ballon de plateau)** ou en tant que **Pop Up Message (message contextuel)**.
   - Saisissez et format le texte de votre message (**Template (Modèle)**), puis cliquez sur **OK**.
   - Répétez ces étapes pour chaque message que vous souhaitez définir.

24. Enregistrez la configuration de la passerelle.
    1. Cliquez sur **OK** pour enregistrer les paramètres.
    2. **Validez** les modifications.

25. (Facultatif) Pour configurer l'application GlobalProtect pour qu'elle affiche une étiquette qui identifie l'emplacement de cette passerelle lorsque les utilsateurs finaux sont connectés, spécifiez l'emplacement physique du pare-feu sur lequel vous avez configuré cette passerelle.

    Lorsque les utilisateurs finaux constatent un comportement inhabituel, comme une piètre performance du réseau, ils peuvent donner les informations de cet emplacement à leur service d'assistance ou aux professionnels du Centre d'assistance pour qu'ils les aident avec la résolution du problème. Ils peuvent également utiliser ces informations sur l'emplacement pour

 ©2026 Palo Alto Networks, Inc.

déterminer leur proximité à la passerelle. Selon leur proximité, ils peuvent évaluer s'ils doivent passer à une passerelle plus près.

Si vous ne spécifiez pas l'emplacement de la passerelle, l'application GlobalProtect affiche un champ d'emplacement vide.

- **Dans la CLI** : Utilisez la commande de la CLI suivante pour spécifier l'emplacement physique du pare-feu sur lequel vous avez configuré la passerelle :

```
<username@hostname> définir le paramètre deviceconfig global-
protect location <location>
```

- **Dans l'API XML** : Utilisez la commande de l'API XML suivante pour spécifier l'emplacement physique du pare-feu sur lequel vous avez configuré la passerelle :
  - **périphériques** : nom du pare-feu sur lequel vous avez configuré la passerelle;
  - **emplacement** : emplacement du pare-feu sur lequel vous avez configuré la passerelle.

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

 ©2026 Palo Alto Networks, Inc.

Attribution et gestion d'adresses IP basées sur DHCP pour GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect PAN-OS 11.2 (ou une version ultérieure de PAN-OS) Application GlobalProtect 6.0.8, 6.2.1 ou versions ultérieures Terminaux GlobalProtect fonctionnant sous Windows, macOS, Android, iOS et Linux

À partir de PAN-OS 11.2.1, la fonctionnalité d'affectation d'adresses IP basées sur DHCP est prise en charge pour les plateformes de pare-feu virtuel VM-Series et de pare-feu de nouvelle génération matériel.

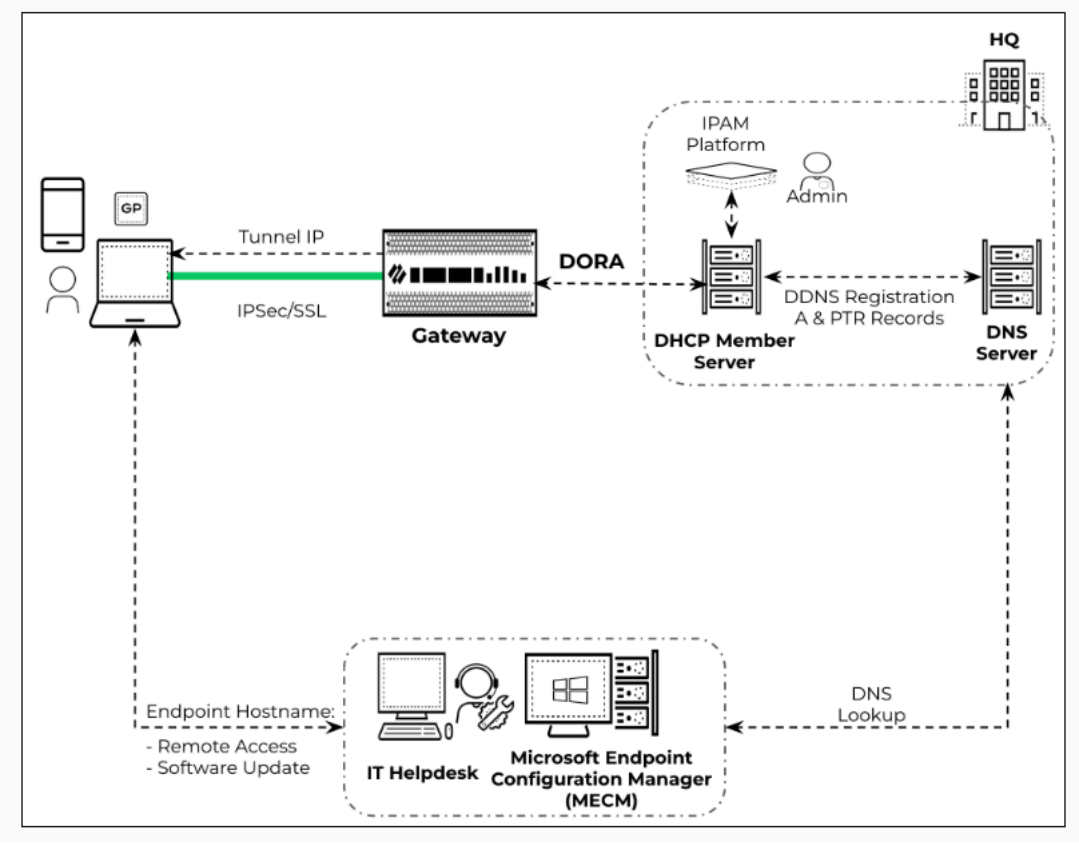
La fonctionnalité d'affectation d'adresses IP basées sur DHCP dans la version PAN OS 11.2.0 est prise en charge uniquement pour les pare-feu virtuels VM-Series. La fonctionnalité n'est pas prise en charge pour les plateformes de pare-feu de nouvelle génération matériel.

Vous pouvez maintenant configurer un profil de serveur DHCP sur la passerelle GlobalProtect pour utiliser le serveur DHCP pour gérer et attribuer des adresses IP aux terminaux connectés à distance via l'application GlobalProtect. Les utilisateurs qui utilisent des serveurs DHCP d'entreprise peuvent activer cette fonctionnalité pour une gestion centralisée des IP et des affectations d'adresses IP.

Lorsque vous configurez un profil de serveur DHCP sur la passerelle GlobalProtect et après une communication réussie entre la passerelle et le serveur DHCP, la passerelle obtient des adresses IP DHCP d'un serveur membre DHCP. La passerelle GlobalProtect attribue ensuite les adresses IP comme IP de tunnel pour les terminaux qui sont connectés à distance via l'application GlobalProtect. Tout d'abord, vous devez configurer un profil de serveur DHCP sur la passerelle GlobalProtect. Après une communication réussie entre la passerelle et le serveur DHCP, la passerelle obtient des adresses IP DHCP d'un serveur membre DHCP. La passerelle GlobalProtect attribue ensuite les adresses IP comme IP de tunnel pour les terminaux qui sont connectés à distance via l'application GlobalProtect.

Lorsque la passerelle GlobalProtect attribue les adresses IP DHCP aux terminaux, vous pouvez configurer leur serveur DHCP pour créer des enregistrements DNS dynamiques (enregistrement d'adresse et d'indice) pour les utilisateurs connectés à GlobalProtect. Les DDNS sont utiles pour les administrateurs de terminaux pour effectuer des dépannages sur les terminaux des utilisateurs distants connectés à GlobalProtect. Les adresses IP sont enregistrées sur le serveur DDNS uniquement lorsque vous configurez la gestion des adresses IP (IPAM) sur Windows Server, le serveur DDNS ou sur le serveur Infoblox.

 ©2026 Palo Alto Networks, Inc.



Lorsque vous créez un profil DHCP sur le pare-feu et activez le serveur DHCP sur la passerelle GlobalProtect, la passerelle utilise le serveur DHCP pour gérer et attribuer les adresses IP pour les terminaux au lieu d'attribuer les adresses IP à partir du pool d'adresses IP privées de la passerelle. Si le serveur DHCP ne répond pas à la passerelle dans le délai d'expiration de communication et la période de temps de nouvelle tentative définis, la passerelle revient au pool d'adresses IP statiques privées pour l'attribution d'adresses IP aux terminaux.

- *La fonctionnalité d'affectation d'adresses IP basée sur DHCP est uniquement prise en charge pour l'affectation d'adresses IPv4 et non pour IPv6.*
- *La configuration d'un pool d'adresses IP statiques sur la passerelle GlobalProtect est optionnelle lorsque vous configurez une fonctionnalité d'affectation d'adresses IP basée sur DHCP.*

Configurer le serveur DHCP sur la passerelle GlobalProtect pour attribuer des adresses IP DHCP aux terminaux

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect PAN-OS 11.2 (ou une version ultérieure de PAN-OS) Application GlobalProtect 6.0.8, 6.2.1 ou versions ultérieures

 ©2026 Palo Alto Networks, Inc.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	Terminaux GlobalProtect fonctionnant sous Windows, macOS, Android, iOS et Linux

La fonctionnalité d'affectation d'adresses IP basées sur DHCP dans la version PAN OS 11.2.0 est prise en charge uniquement pour les pare-feu virtuels VM-Series. La fonctionnalité n'est pas prise en charge pour les plateformes de pare-feu de nouvelle génération matériel.

Utilisez la procédure suivante pour configurer le serveur DHCP sur la passerelle GlobalProtect pour attribuer des adresses IP DHCP aux terminaison :

- Configurer un serveur DHCP sur le serveur Windows ou sur le serveur Infoblox
- Configurer le portail GlobalProtect
- Créer Créer des profils DHCP sur le pare-feu
- Configurer la passerelle GlobalProtect
- Activer le serveur DHCP sur la passerelle GlobalProtect
- Consulter et Vérifier l'attribution d'adresses IP basée sur DHCP
- Configurer les itinéraires de service pour les requêtes DHCP

Configurer un serveur DHCP sur le serveur Windows ou sur le serveur Infoblox

Configurez un serveur DHCP sur le serveur Windows avec desoptions de sous-réseau de sélection DHCP ou un serveur DHCP sur le serveur Infoblox / Configurez des réseaux partagés IPv4..

Le temps du bail DHCP que vous configurez sur le serveur DHCP ne doit pas être inférieur à 5 minutes.

Consultez Configurer le serveur DHCP sur le serveur Infoblox et Configurer le serveur DHCP sur Windows Server pour en savoir plus sur la configuration du serveur DHCP sur le serveur Windows ou Infoblox :

Configurer le portail GlobalProtect

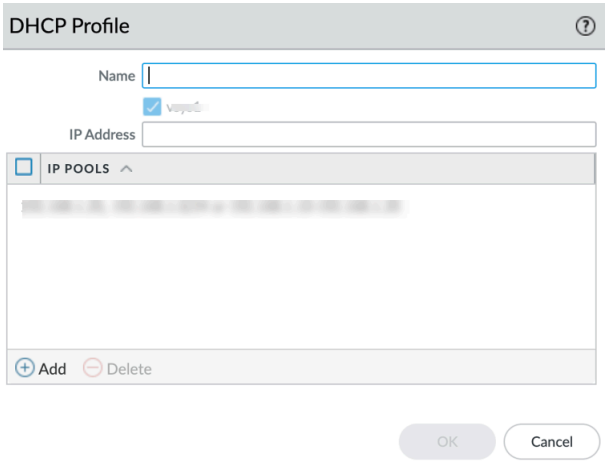
Configurez le portail GlobalProtect.

Créer des profils DHCP sur le pare-feu

1. Pour créer un profil DHCP, effectuez l'une des actions suivantes :
   - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **DHCP Profile (Profil DHCP)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Profiles (Profils)** > **DHCP Profile (Profil DHCP)** puis **Add Profil (Ajouter un profil)**.

 ©2026 Palo Alto Networks, Inc.

2. Saisissez un **Name (Nom)** descriptif pour le profil DHCP.

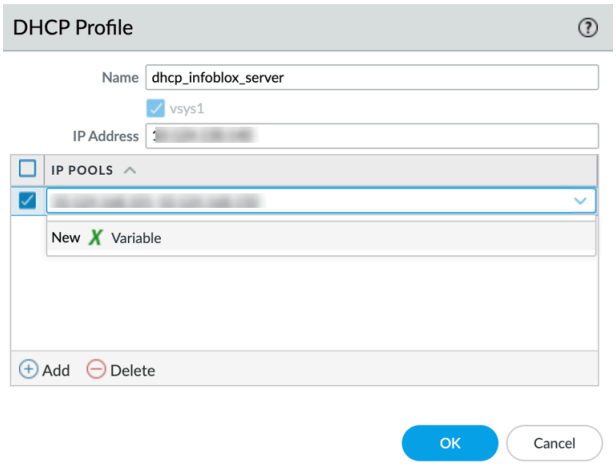


Vous pouvez créer un maximum de cinq profils DHCP.

3. Spécifiez l'adresse IP du serveur DHCP que vous souhaitez configurer sur la passerelle GlobalProtect.

4. Sélectionnez la plage d'adresses IP DHCP que vous souhaitez que la passerelle GlobalProtect utilise et attribue aux terminaux.

Le pool d'adresses IP DHCP que vous configurez sur la passerelle GlobalProtect doit correspondre au pool IP dans le serveur DHCP. Si vous configurez de façon incorrecte les adresses IP DHCP sur la passerelle GlobalProtect, le trafic ne circulera pas comme prévu.



5. Cliquez sur **OK** pour enregistrer le profil DHCP.

Configurer la passerelle GlobalProtect

Configurez la Passerelle GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Activer le serveur DHCP sur la passerelle GlobalProtect

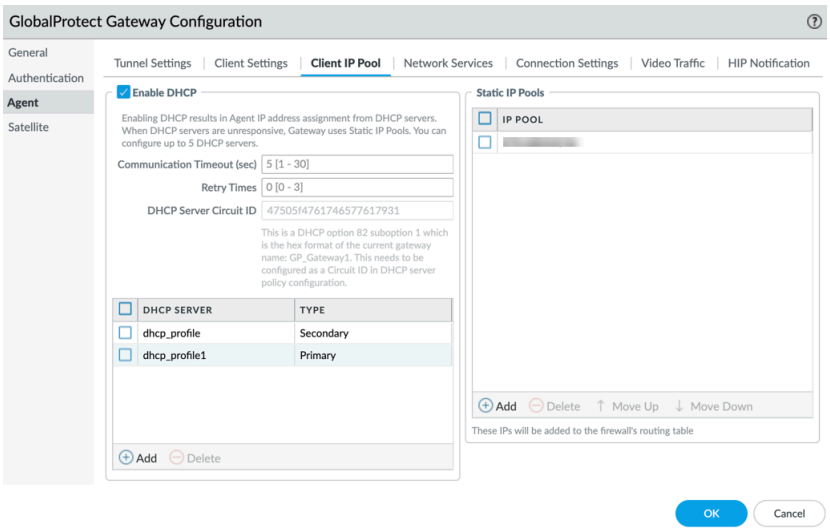
1. Pour activer le serveur DHCP sur la passerelle GlobalProtect, effectuez l'une des actions suivantes :
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Add Gateway (Ajouter une passerelle)**. Sur la page Ajouter une passerelle, sous **Client IP Pool (Pool d'adresses IP du client)**, activez le DHCP.
   - Sur Panorama, sélectionnez **Networks (Réseaux)** > **GlobalProtect** > **Gateways (Passerelles)** > **<gateway config>** > **Agent** > **Client IP Pool (Pool d'adresses IP du client)**.
2. Dans l'onglet **Client Pool (Pool client)**, activez **DHCP**.
3. Spécifiez le **Communication Timeout (Délai d'expiration de la communication** (en secondes) pour définir le nombre de secondes que la passerelle GlobalProtect et le serveur DHCP prennent pour communiquer et le processus d'affectation des adresses IP. La valeur par défaut est de 5 secondes. Le **Communication Timeout (sec) (Délai d'expiration de réception TCP [sec])** que vous configurez dans les paramètres de l'application de la configuration du portail GlobalProtect doit être égal ou supérieur au **Communication Timeout (Délai d'expiration de la communication)** DHCP.
4. Spécifiez le nombre de fois que la passerelle GlobalProtect doit renouveler sa tentative de connexion au serveur DHCP lorsque le délai d'expiration de la communication est dépassé entre la passerelle et le serveur DHCP. La valeur par défaut est de 0.
5. **DHCP Server Circuit ID (ID de circuit du serveur DHCP)** est prérempli pour configurer la passerelle GlobalProtect en tant qu'agent de relais et pour permettre à la passerelle de recevoir des adresses IP du serveur DHCP et de les transmettre aux terminaux lorsqu'ils

 ©2026 Palo Alto Networks, Inc.

sont connectés à l'application GlobalProtect. L'ID de circuit du serveur DHCP est le format hexadécimal du nom actuel de la passerelle GlobalProtect.

L'**ID de circuit du serveur DHCP (ID de circuit du serveur DHCP)** doit être configuré comme l'ID de circuit lors de la configuration de la politique du serveur DHCP.

L'ID de circuit du serveur DHCP doit être configuré comme l'ID de circuit lors de la configuration de la politique du serveur DHCP.



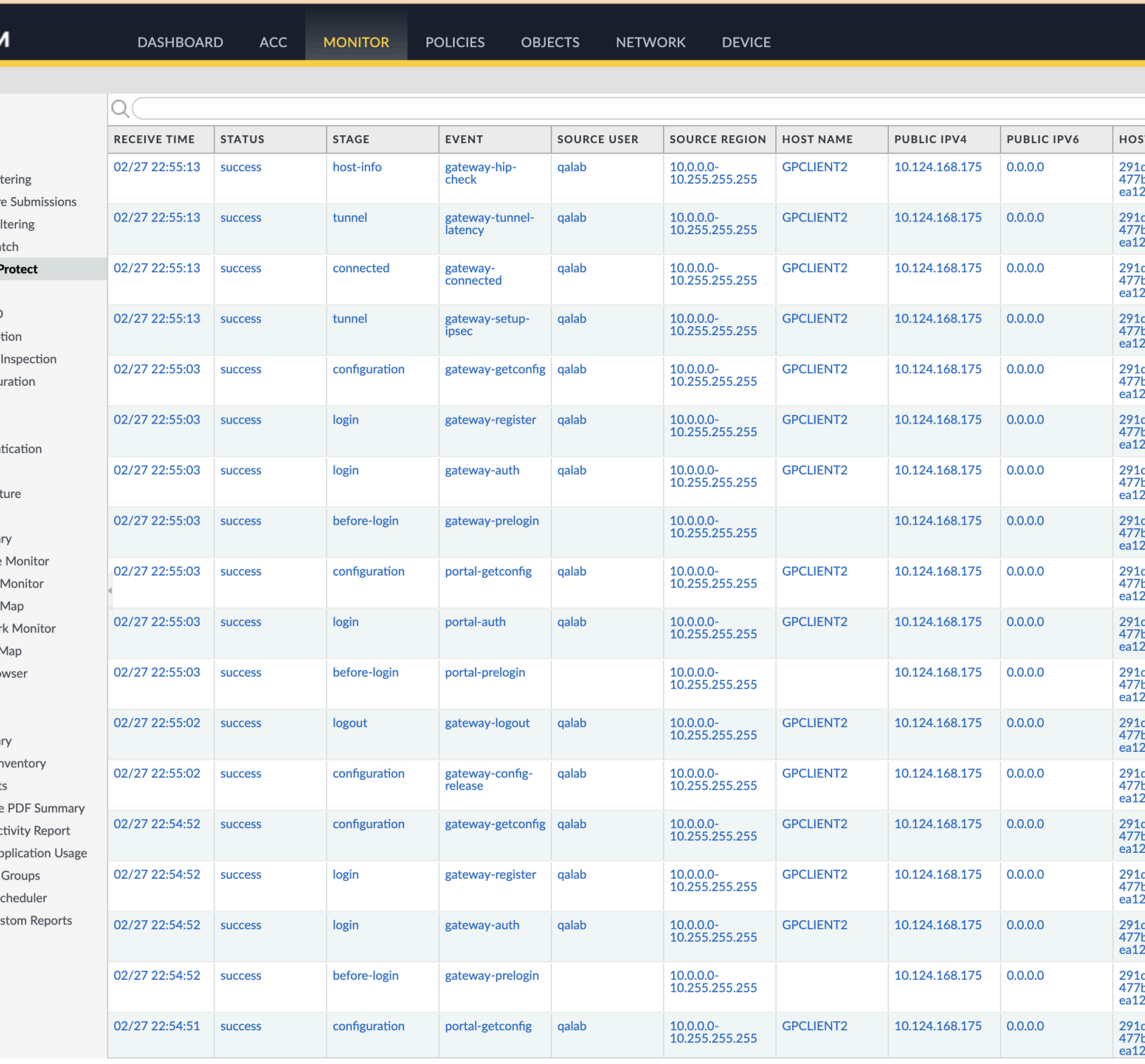
6. Sélectionnez le type de serveur DHCP dans la liste affichée des serveurs DHCP que vous avez configurés. Vous pouvez sélectionner des serveurs comme **Primary (Principal)** et **Secondary (Secondaire)**. Lorsque vous définissez un serveur DHCP comme secondaire, il agira comme le serveur de secours pour le serveur DHCP principal. Si le serveur principal tombe en panne, le serveur secondaire sera utilisé pour les requêtes DHCP après expiration du délai d'expiration et du nombre de tentatives. Si les deux serveurs DHCP sont principaux, alors la requête DHCP sera envoyée aux deux serveurs et la réponse reçue en premier sera prise en compte.

7. Cliquez sur **OK** et validez les modifications.

Afficher et vérifier les journaux d'affectation d'adresses IP basés sur DHCP

Consultez les journaux GlobalProtect (page **Monitor (Surveiller)** > **Logs (Journaux)** > **GlobalProtect**) pour vérifier et dépanner l'affectation d'adresses IP de la passerelle GlobalProtect utilisant le serveur DHCP.

 ©2026 Palo Alto Networks, Inc.



RECEIVE TIME	STATUS	STAGE	EVENT	SOURCE USER	SOURCE REGION	HOST NAME	PUBLIC IPV4	PUBLIC IPV6	HOST
02/27 22:55:13	success	host-info	gateway-hip-check	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:13	success	tunnel	gateway-tunnel-latency	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:13	success	connected	gateway-connected	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:13	success	tunnel	gateway-setup-ipsec	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:03	success	configuration	gateway-getconfig	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:03	success	login	gateway-register	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:03	success	login	gateway-auth	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:03	success	before-login	gateway-prelogin		10.0.0.0-10.255.255.255		10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:03	success	configuration	portal-getconfig	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:03	success	login	portal-auth	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:03	success	before-login	portal-prelogin		10.0.0.0-10.255.255.255		10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:02	success	logout	gateway-logout	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:55:02	success	configuration	gateway-config-release	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:54:52	success	configuration	gateway-getconfig	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:54:52	success	login	gateway-register	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:54:52	success	login	gateway-auth	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:54:52	success	before-login	gateway-prelogin		10.0.0.0-10.255.255.255		10.124.168.175	0.0.0.0	291c 477b ea12
02/27 22:54:51	success	configuration	portal-getconfig	qalab	10.0.0.0-10.255.255.255	GPCLIENT2	10.124.168.175	0.0.0.0	291c 477b ea12

Vous pouvez voir les journaux suivants pour DHCP en utilisant Command Line Interface (interface de ligne de commande - CLI).

- moins mp-log gpsvc.log
- moins mp-log rasmgr.log
- moins mp-log gp_broker.log

 ©2026 Palo Alto Networks, Inc.

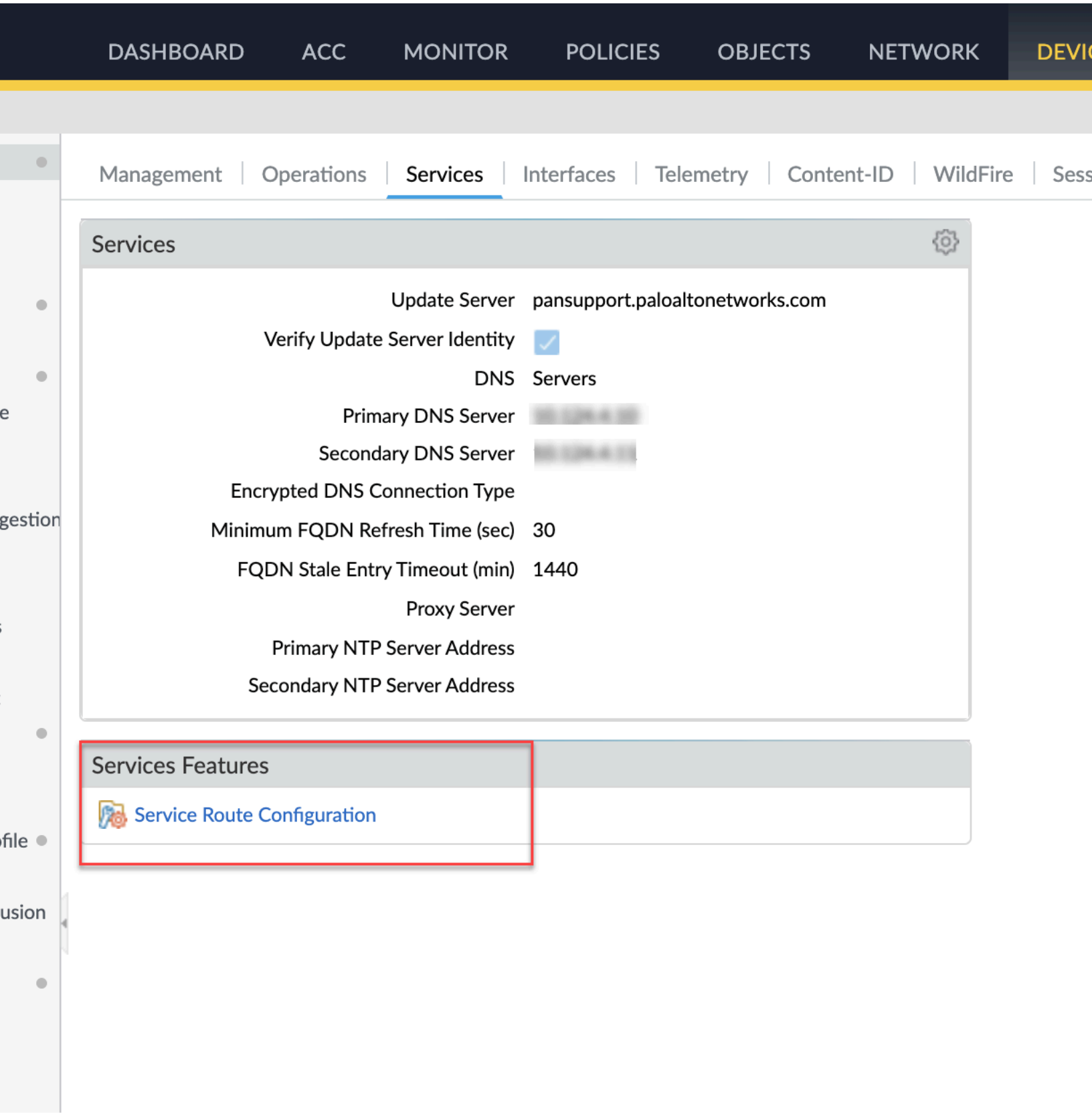
Configurer les itinéraires de service pour les requêtes DHCP

Vous pouvez configurer votre plan de données personnalisé comme un itinéraire de service pour envoyer des demandes DHCP, si vous ne souhaitez pas utiliser l'interface de gestion par défaut pour envoyer des requêtes DHCP.

Utilisez la procédure suivante pour configurer un itinéraire de service pour les requêtes DHCP :

 ©2026 Palo Alto Networks, Inc.

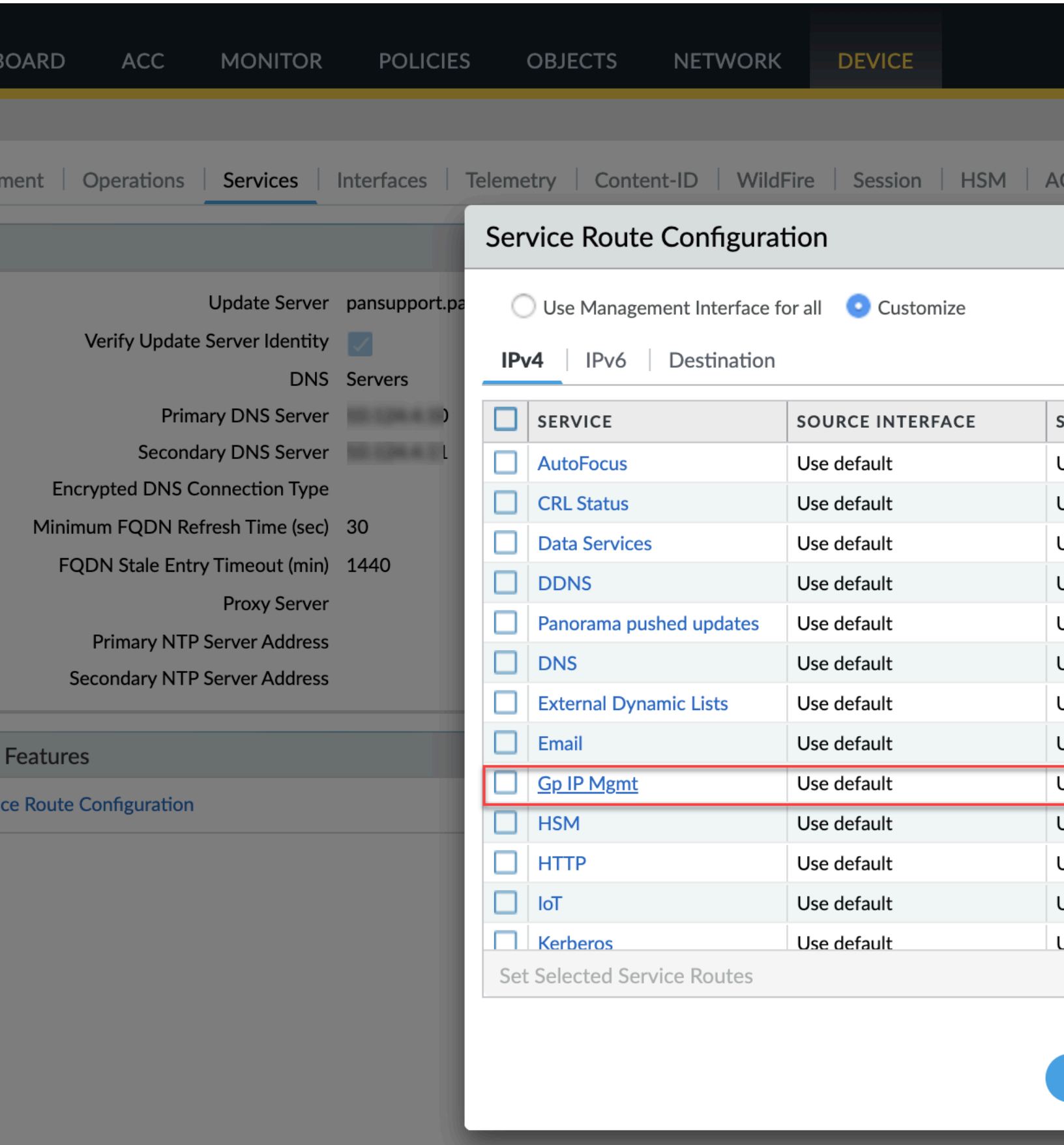
1. Allez sur **Device (Périphérique)** > **Setup (Configuration)** > **Services.**



 ©2026 Palo Alto Networks, Inc.

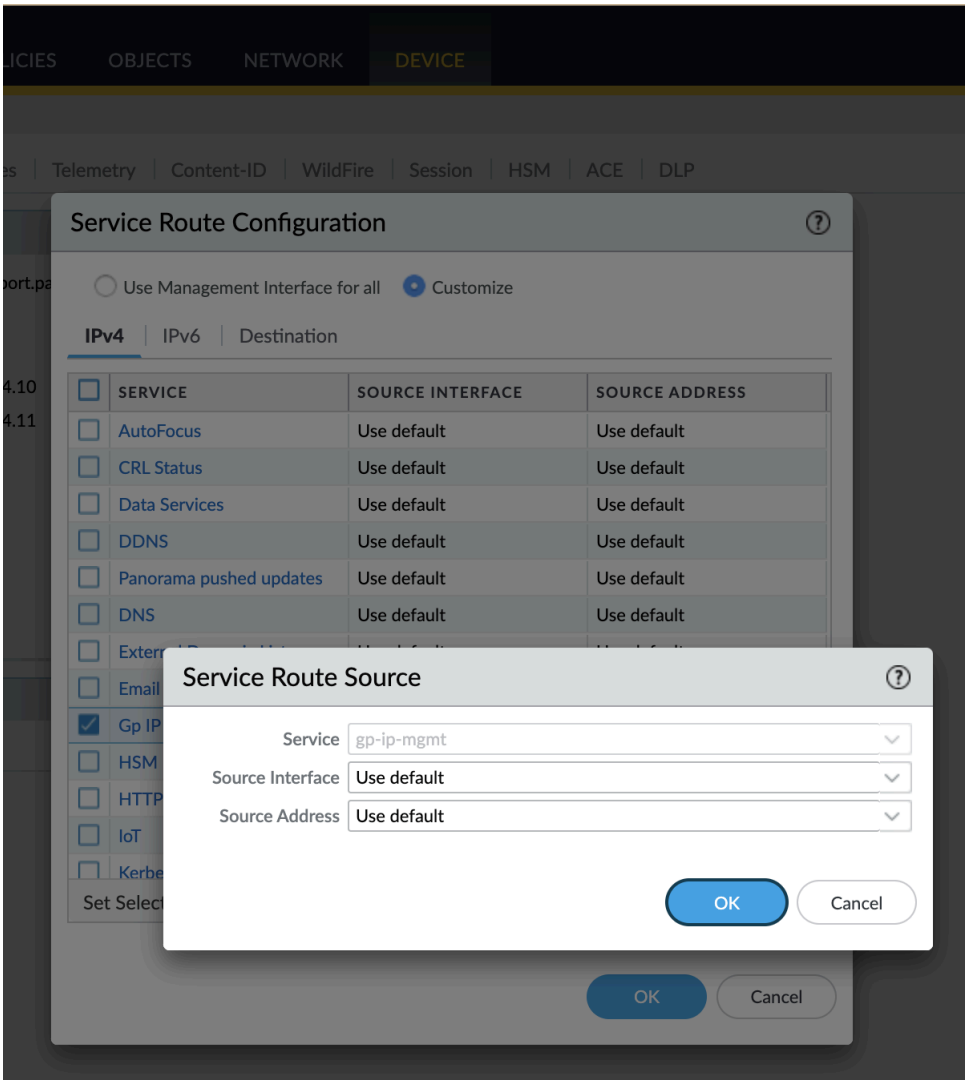
2. Cliquez sur le lien **Services Route Configuration (Configuration de l'itinéraire de service)**.

 ©2026 Palo Alto Networks, Inc.



©2026 Palo Alto Networks, Inc.

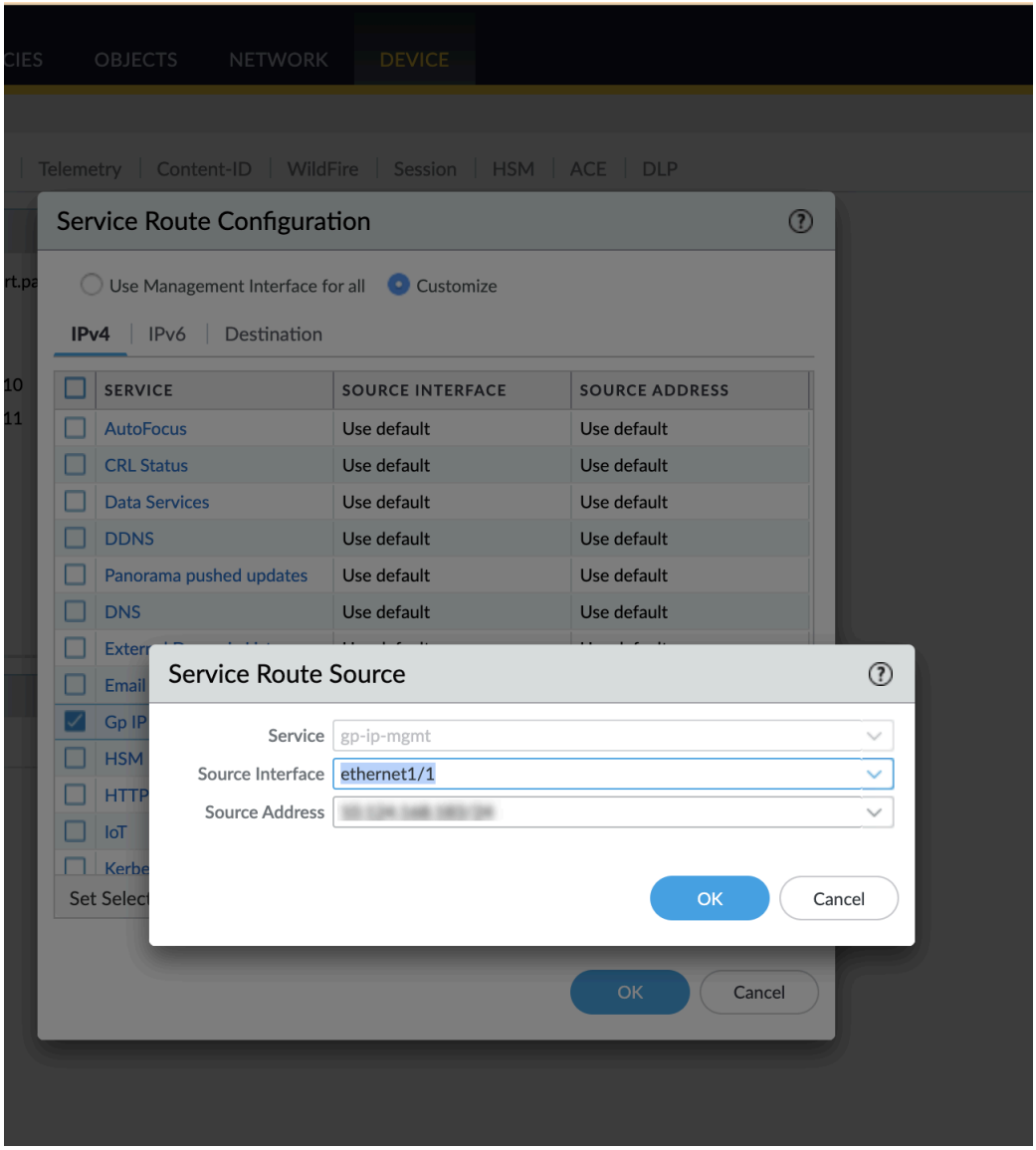
3. Sélectionnez **Gp IP Mgmt** et cliquez sur **OK**. La fenêtre contextuelle Source de l'itinéraire de service affiche les valeurs par défaut.



4. Spécifiez la **Source Interface (Interface Source)** et la **Source IP Address (Adresse IP source)** que vous souhaitez configurer pour envoyer les demandes DHCP si vous ne souhaitez pas

 ©2026 Palo Alto Networks, Inc.

utiliser l'interface de gestion. Par exemple, vous pouvez spécifier l'interface source comme Ethernet et les adresses IP associées comme l'interface.



*Vous ne pouvez pas sélectionner **Any (Toute)** comme interface source lors de la configuration des routes de service pour les demandes DHCP.*

5. Cliquez sur **OK** pour enregistrer la configuration.

6. **Commit (Validez)** les modifications.

Configurer un serveur DHCP sur le serveur Windows ou sur le serveur Infoblox

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

 ©2026 Palo Alto Networks, Inc.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	PAN-OS 11.2 (ou une version ultérieure de PAN-OS) Application GlobalProtect 6.0.8, 6.2.1 ou versions ultérieures Terminaux GlobalProtect fonctionnant sous Windows, macOS, Android, iOS et Linux

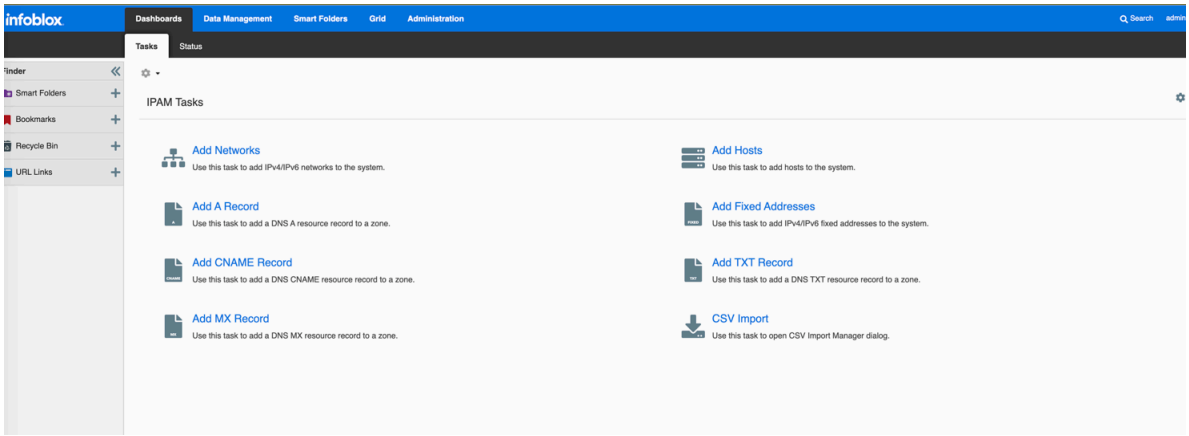
Vous pouvez configurer un serveur DHCP sur le serveur Windows ou sur le serveur Infoblox

- Windows Server
- Serveur Infloblox

Configurer le serveur DHCP sur le serveur Infoblox

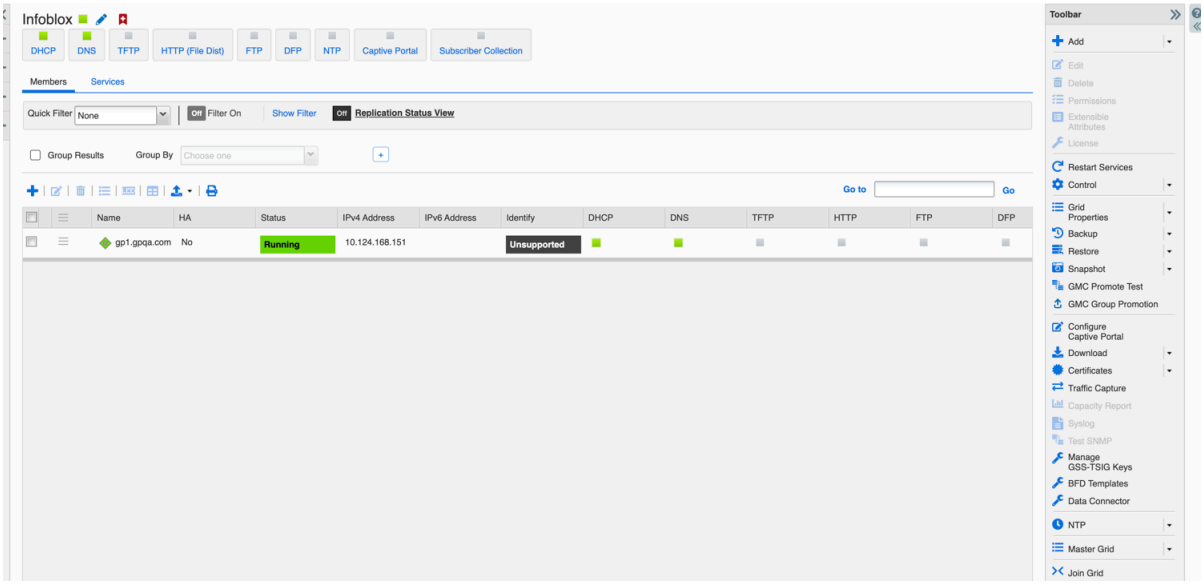
Pour obtenir les dernières informations sur la configuration du serveur DHCP, reportez-vous à la documentation Infoblox, telle que serveur DHCP sur le serveur Infoblox.

1. Connectez-vous au Gestionnaire de grille Infoblox.
2. Cliquez sur **Add Networks (Ajouter des réseaux)** pour ajouter un nouveau réseau.

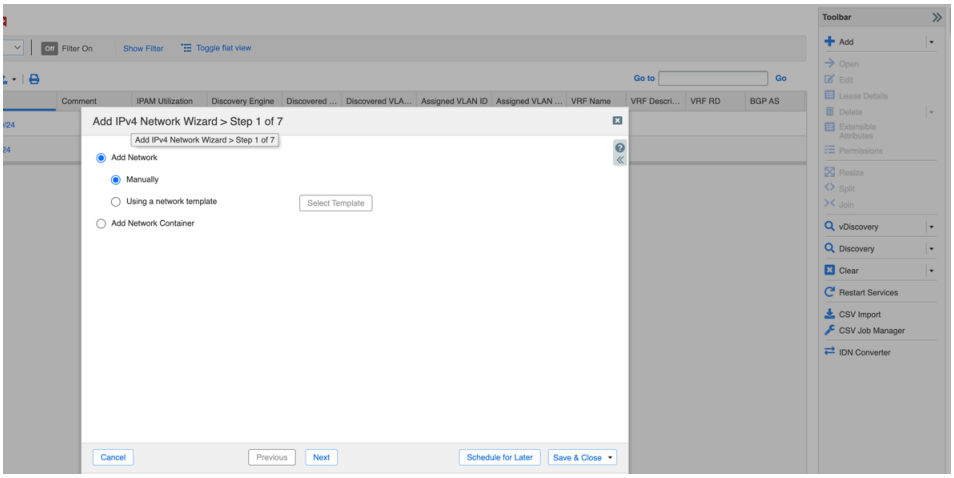


 ©2026 Palo Alto Networks, Inc.

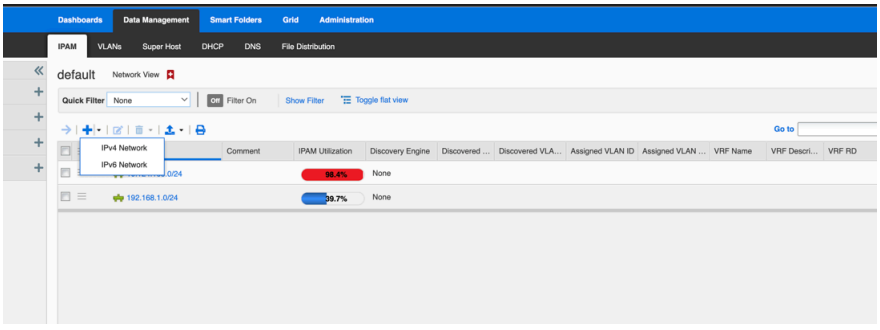
3. Assurez-vous que DHCP et DNS sont activés et exécutés sur la Grille.



4. Cliquez sur **Add (Ajouter)** sous **Toolbar (Barre d'outils)** pour ajouter un réseau IPv4.

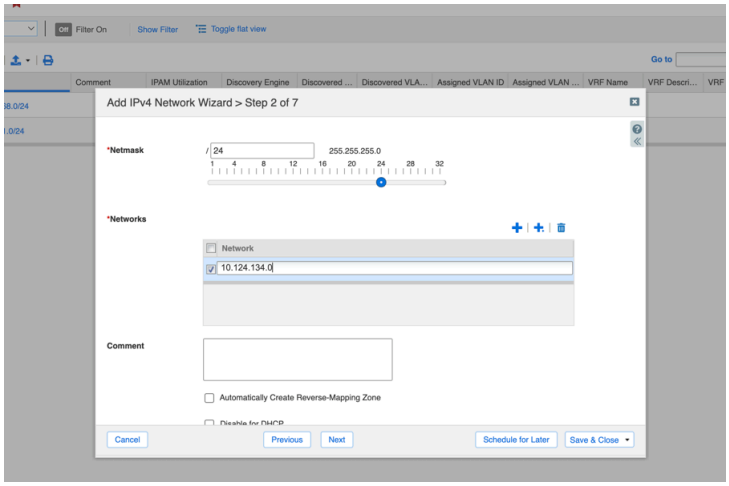


5. Cliquez sur **Next (Suivant)** pour ajouter un réseau IPv4.

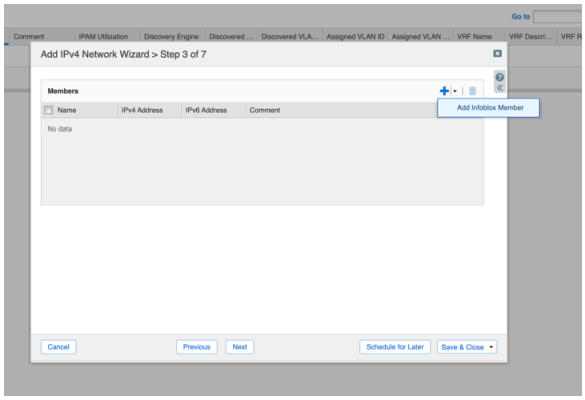


 ©2026 Palo Alto Networks, Inc.

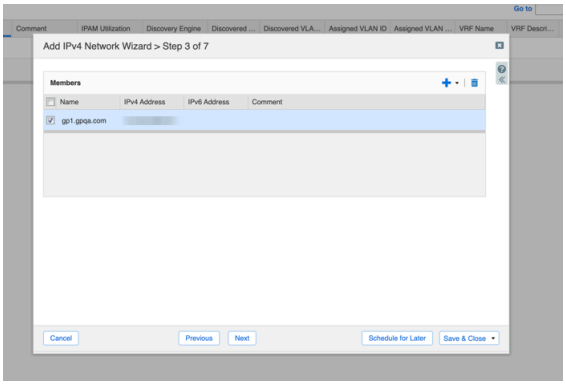
6. Ajoutez l'adresse IP du réseau et cliquez sur **Next (Suivant)**.



7. Ajoutez des membres Infoblox.

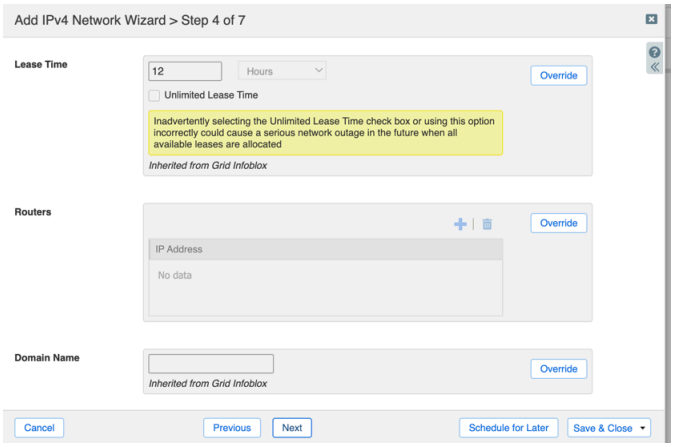


8. Après avoir ajouté le membre, cliquez sur **Next (Suivant)**.

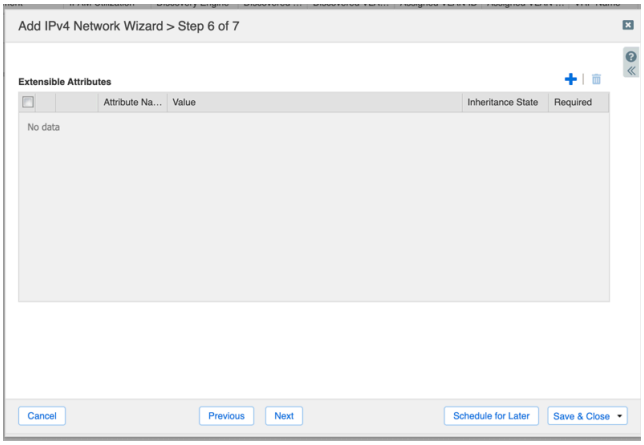


 ©2026 Palo Alto Networks, Inc.

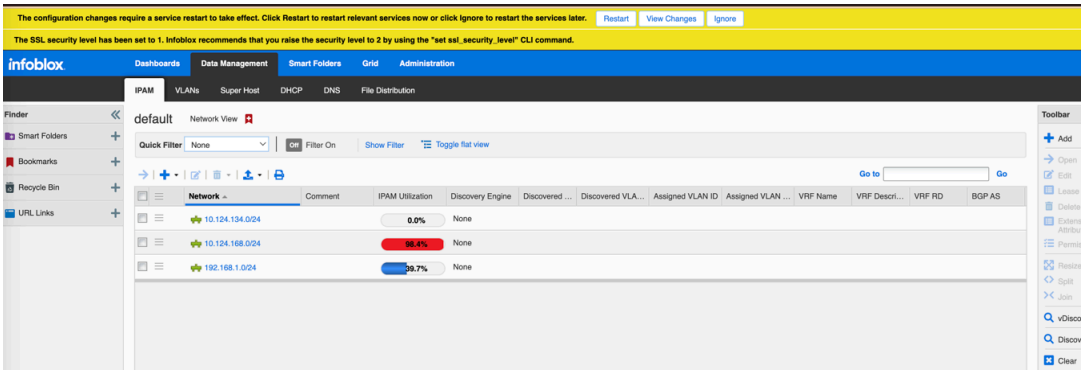
9. (Facultatif) Modifiez la durée du bail par défaut et cliquez sur **Next (Suivant)**.



10. Cliquez sur **Next (Suivant)**.

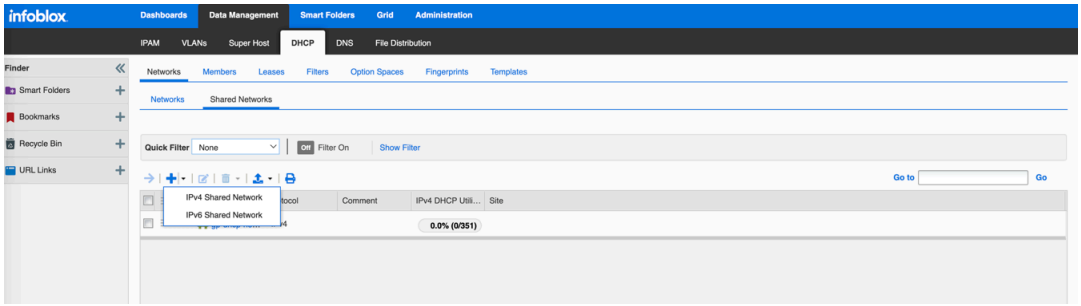


11. Redémarrez le service pour refléter les configurations ajoutées pour le nouveau réseau.

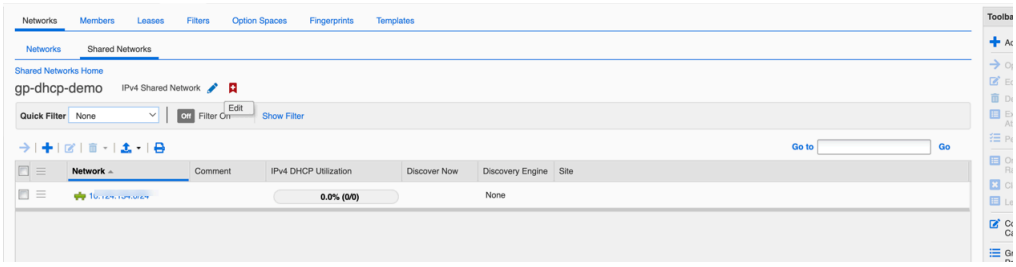


 ©2026 Palo Alto Networks, Inc.

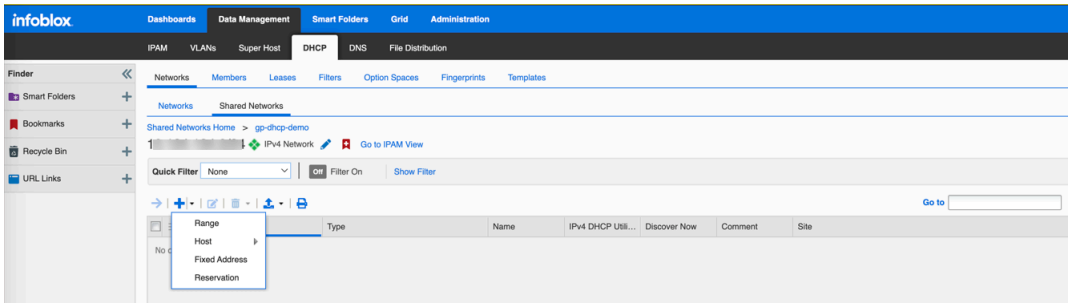
12. Pour ajouter un **Shared Network (Réseau partagé)**, accédez à **DHCP (DHCP)** > **Networks (Réseaux)** > **Shared Network (Réseau partagé)**.



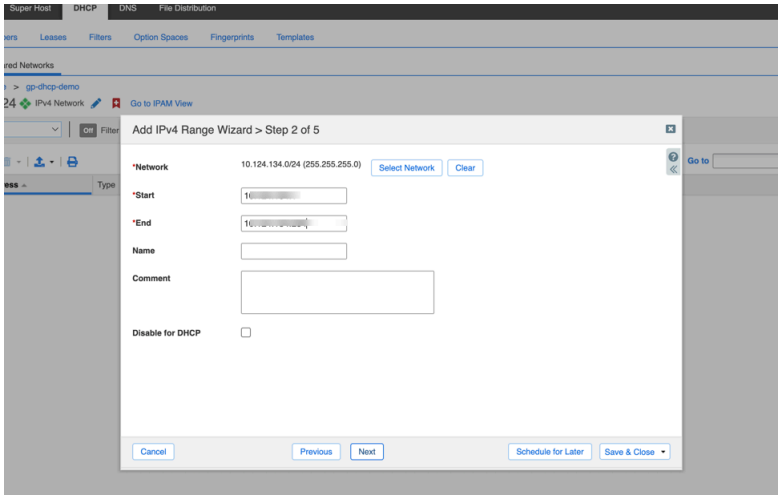
13. Créez tous vos réseaux sous un seul Shared Network (Réseau partagé).



14. Cliquez sur le réseau partagé pour ajouter une plage d'adresses IP.

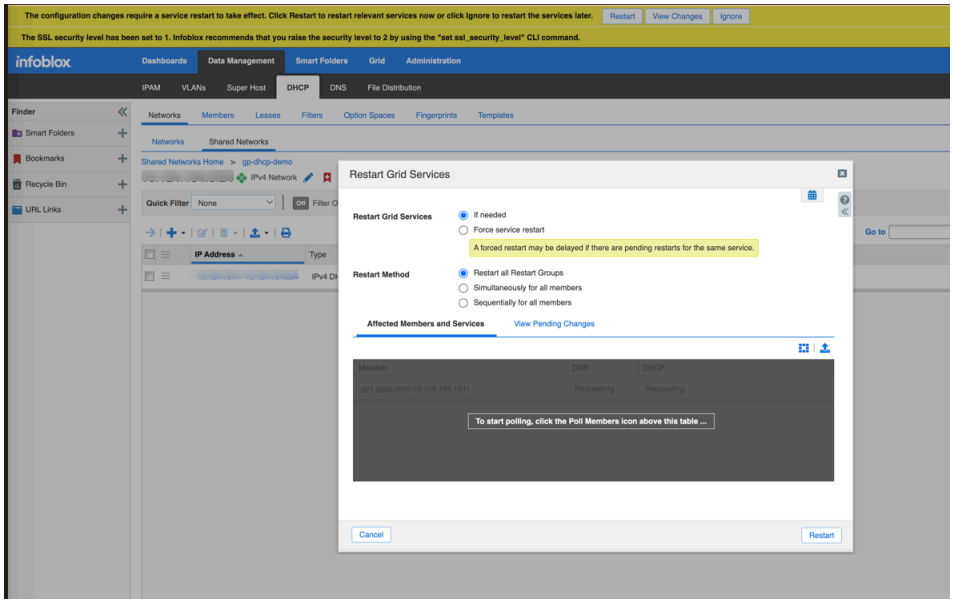


15. Cliquez sur plage pour ajouter une plage d'adresses IP et cliquez sur **Next (Suivant)**.

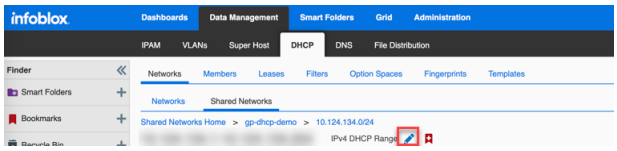


 ©2026 Palo Alto Networks, Inc.

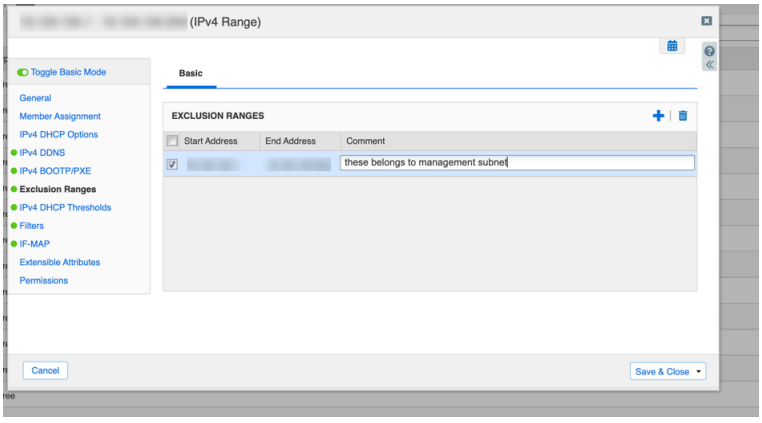
16. Cliquez sur **Next (Suivant)** pour ajouter d'autres détails et continuer jusqu'à ce que l'écran de redémarrage apparaisse. Redémarrez la grille pour refléter les nouvelles configurations ajoutées.



17. Après avoir ajouté les plages IPv4, les adresses IP de la plage s'affichent sous l'onglet **Shared Networks (Réseaux partagés)**. Cliquez sur **Edit (Modifier)** pour modifier les informations.



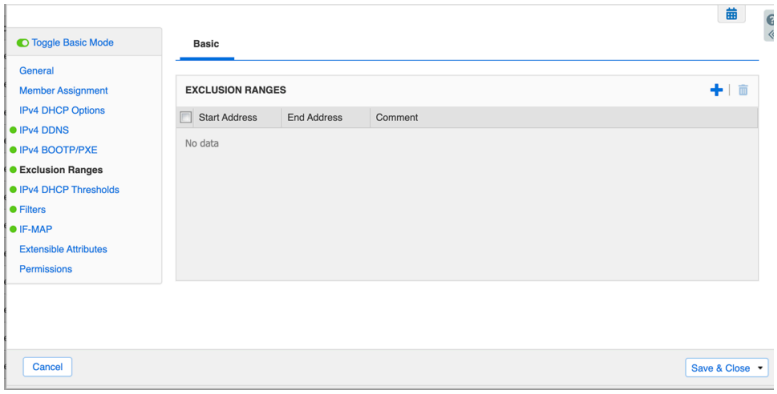
18. (Facultatif)Saisissez la plage d'adresses IP que vous souhaitez exclure de la plage. Cliquez sur le signe **Add (Ajouter)** pour ajouter les **Exclusion Ranges (Plages d'exclusion)**.



19. Cliquez sur **Save & Close (Enregistrer et fermer)**.

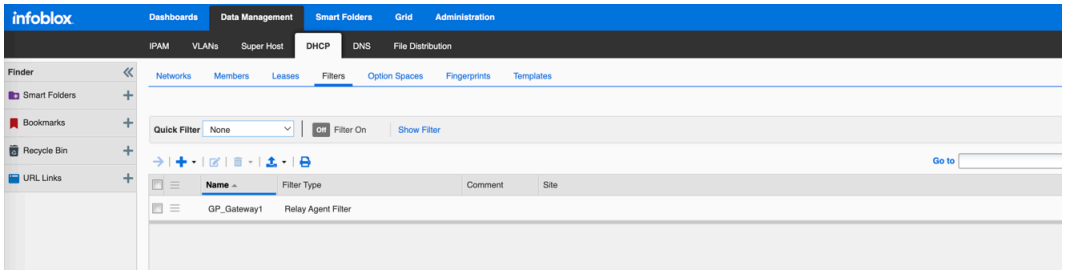
 ©2026 Palo Alto Networks, Inc.

20. Vous pouvez laisser la plage d'exclusion vide si vous ne souhaitez exclure aucune adresse IP.

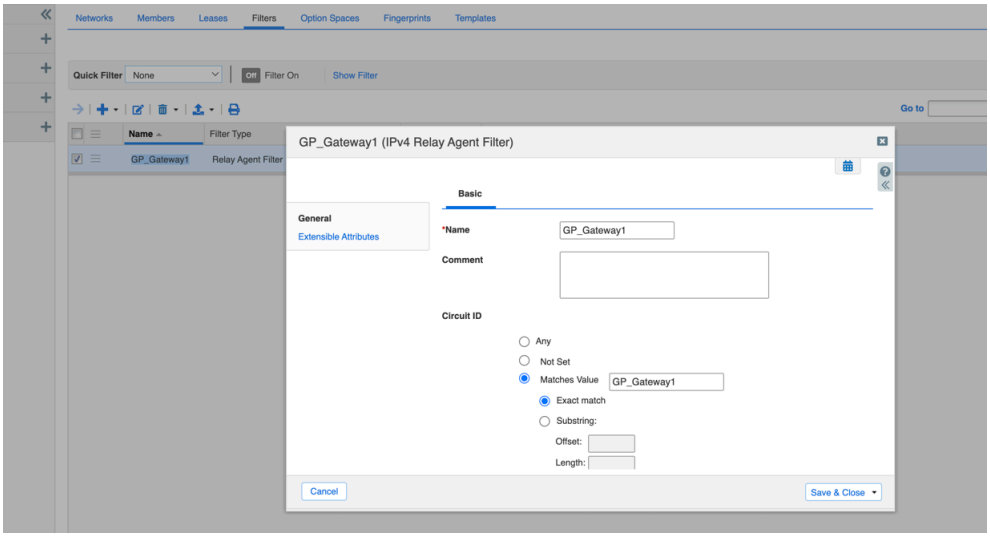


21. Cliquez sur **Next (Suivant)** pour continuer et saisissez les détails tels que le membre de la grille, le changement de calendrier, etc., jusqu'à **Save and Close (Enregistrer et fermer)** les configurations.

22. Après avoir créé la configuration DHCP, vous pouvez créer des filtres avec Nom de passerelle.



23. Vous pouvez afficher les détails de l'agent de relais de la passerelle GlobalProtect.



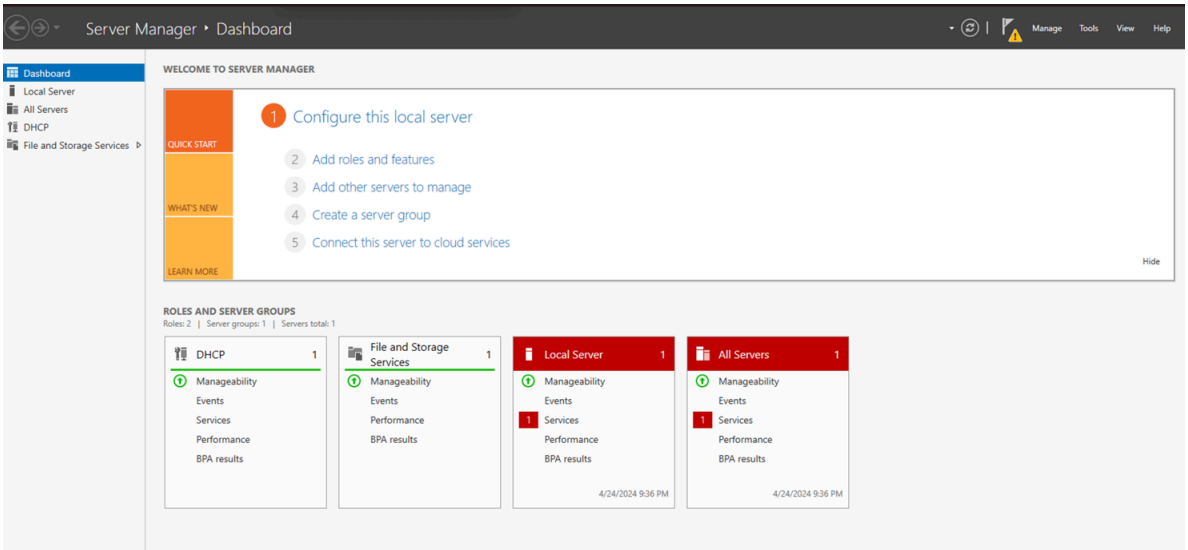
Configurer le serveur DHCP sur Windows Server

 ©2026 Palo Alto Networks, Inc.

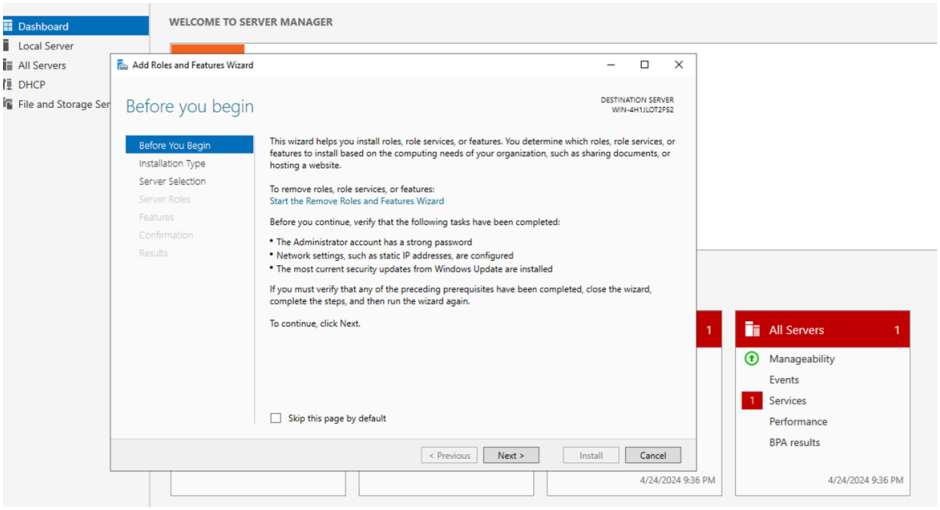
1. Connectez-vous au gestionnaire de Microsoft Server.

   Pour les dernières informations sur la configuration du serveur DHCP, consultez la documentation Microsoft

2. Sur le **Microsoft Server Manager Dashboard (Tableau de bord du gestionnaire de Microsoft Server)**, sélectionnez **Add roles and features (Ajouter des rôles et des fonctionnalités)**.

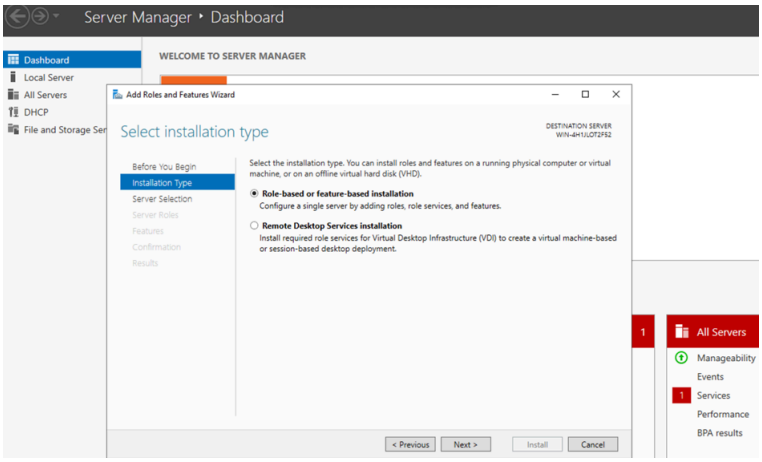


3. Sur l'écran **Before you begin (Avant de commencer)**, cliquez sur **Next (Suivant)**.

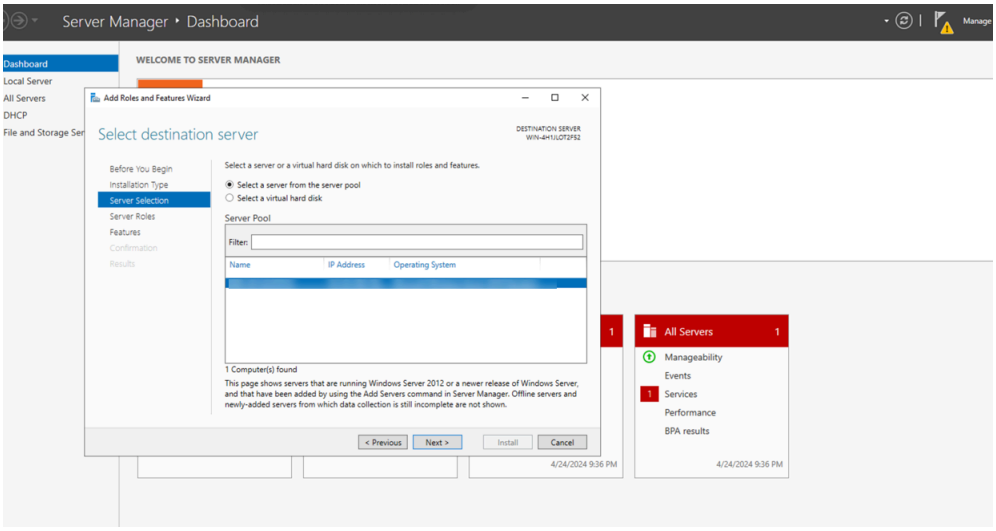


 ©2026 Palo Alto Networks, Inc.

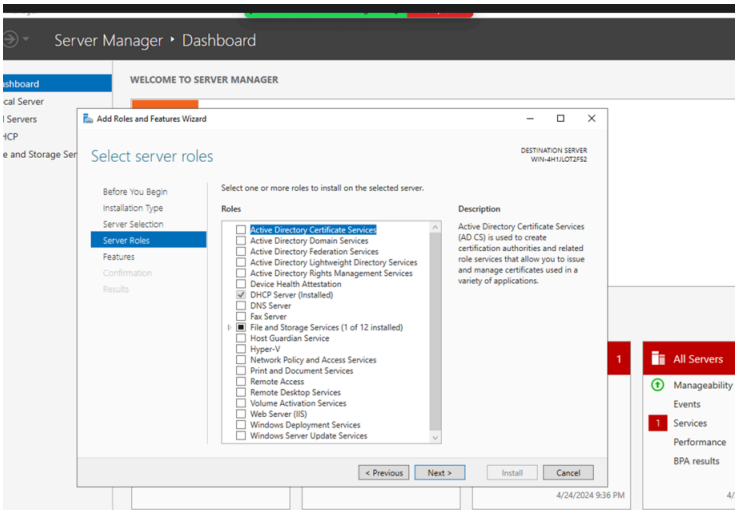
4. Sélectionnez le type d'installation et cliquez sur **Next (Suivant)**.



5. Sélectionnez le serveur de destination dans la zone de pool de serveurs et cliquez sur **Next (Suivant)**.

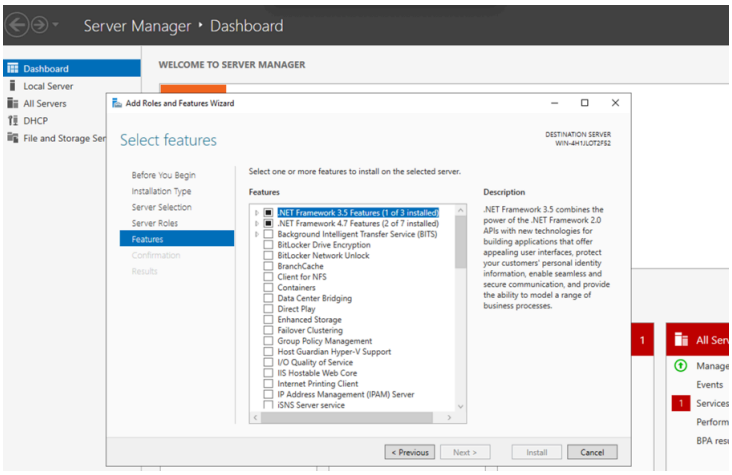


6. Sélectionnez les **Server Roles (Rôles de serveur)** et cliquez sur **Next (Suivant)**.

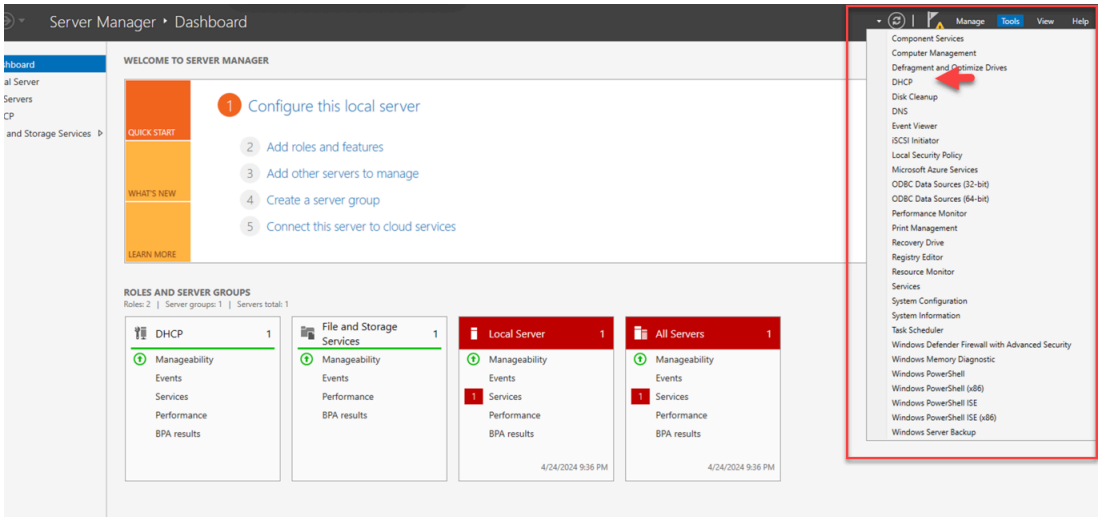


 ©2026 Palo Alto Networks, Inc.

7. Sélectionnez les fonctionnalités et cliquez sur **Next (Suivant)**.

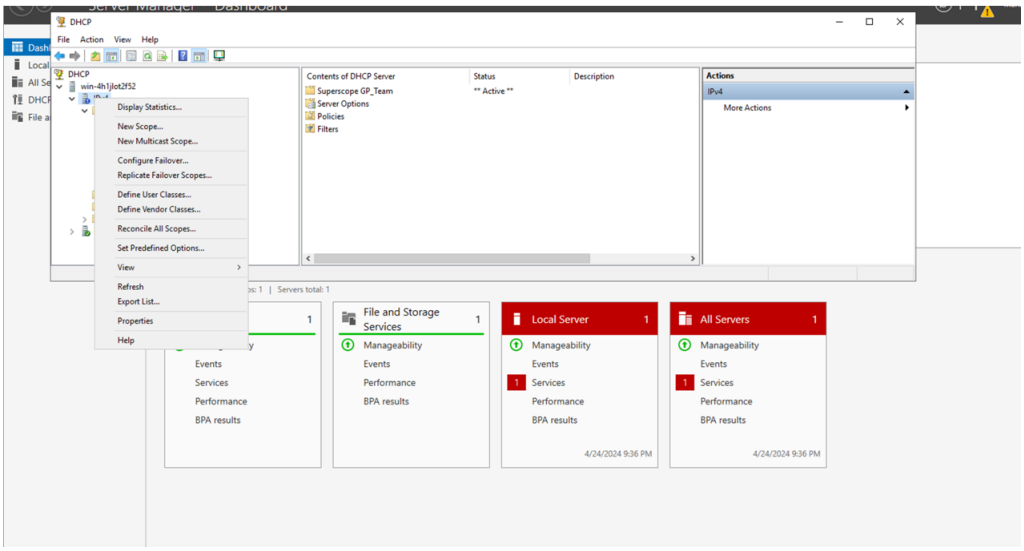


8. Cliquez sur **Tools (Outils)** et sélectionnez **DHCP**.

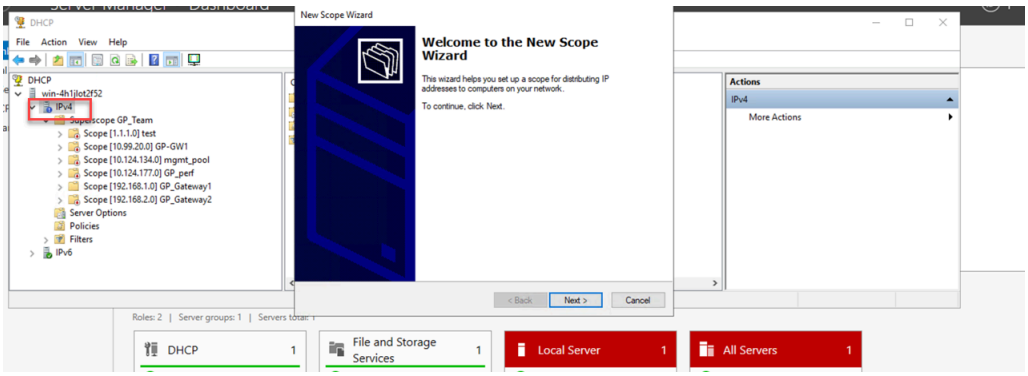


 ©2026 Palo Alto Networks, Inc.

9. Sélectionnez IPv4, faites un clic droit et sélectionnez l'option **New Scope (Nouvelle portée)**.

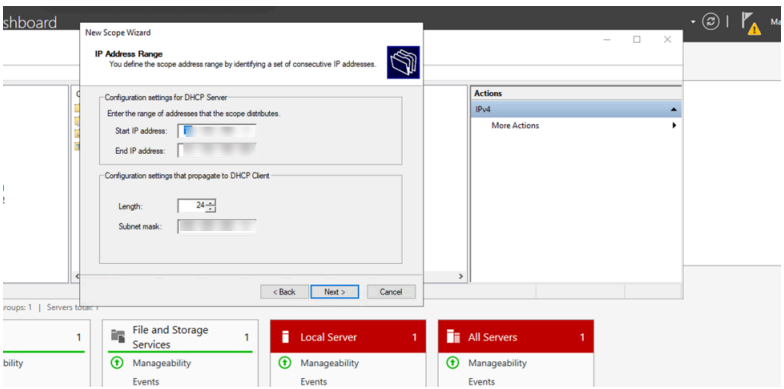


10. Cliquez sur **Suivant (Next)** dans l'assistant Nouvelle portée.



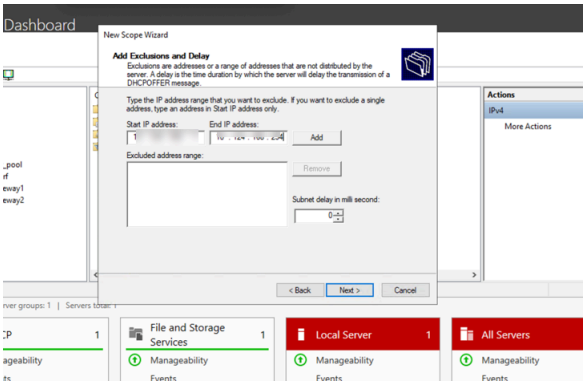
11. Entrez la plage d'adresses IP que la nouvelle portée utilisera pour la distribution.

La plage d'adresses IP du pool DHCP que vous configurez sur le serveur DHCP doit correspondre aux adresses IP de l'interface de gestion dans la passerelle GlobalProtect. Si vous configurez incorrectement les adresses IP DHCP sur le serveur DHCP, le trafic ne circulera pas comme prévu.

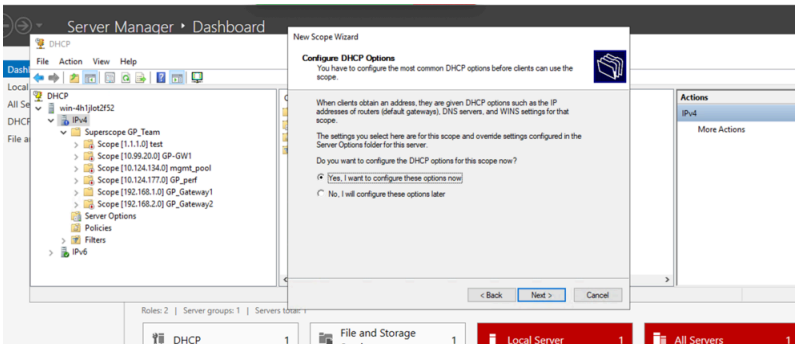


 ©2026 Palo Alto Networks, Inc.

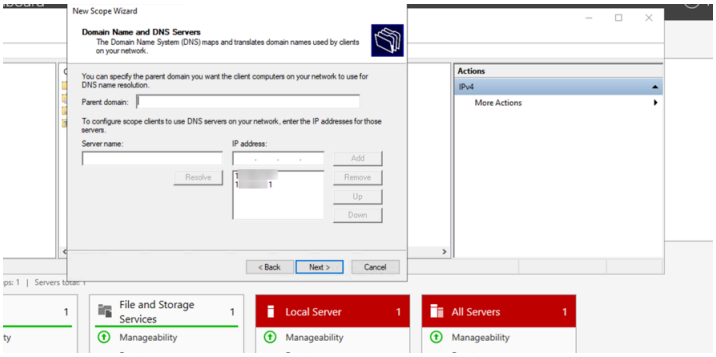
12. (Facultatif) Entrez la plage d'adresses IP que vous souhaitez exclure et qui ne seront pas distribuées par le serveur.



13. Configurez les **DHCP options (Options DHCP)** et cliquez sur **Next (Suivant)**.

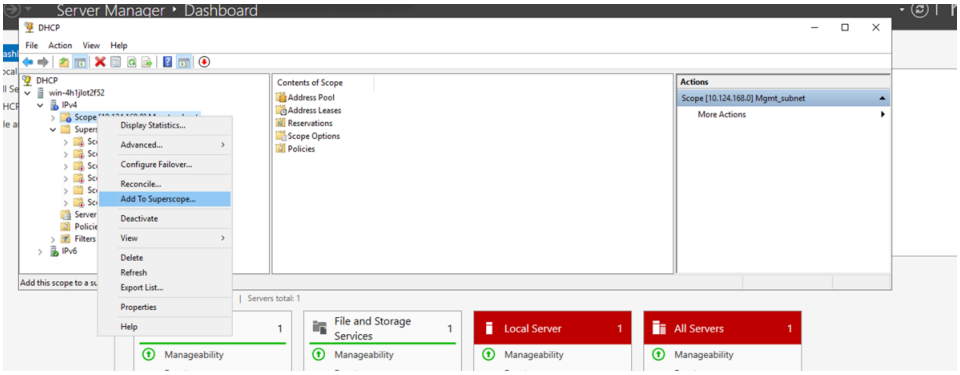


14. Cliquez sur **Next (Suivant)** dans la fenêtre **Domain Name and DNS server (Nom de domaine et serveur DNS)**.

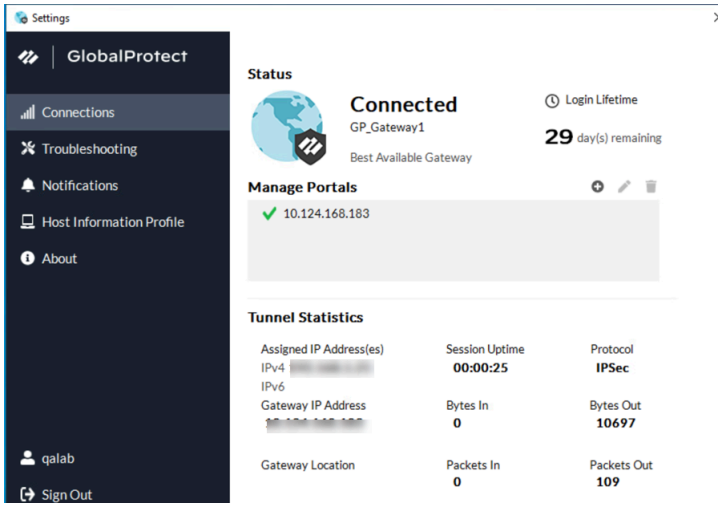


 ©2026 Palo Alto Networks, Inc.

15. La nouvelle portée d'adresses IP est ajouté sous **IPv4**. Cliquez avec le bouton droit de la souris sur la nouvelle portée et sélectionnez **Add to SuperScope (Ajouter à la super portée)**.

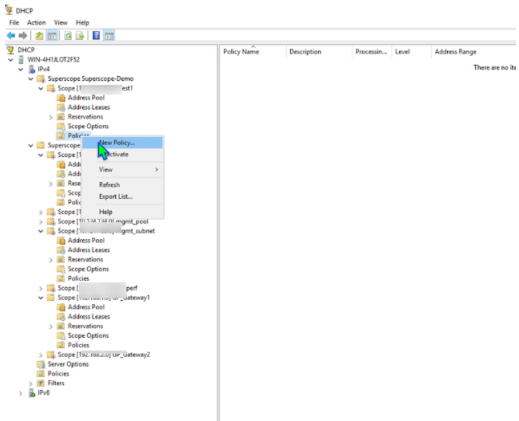


16. Les adresses IP ajoutées seront affichées sous l'onglet **Connections (Connexions)** de l'application GlobalProtect.



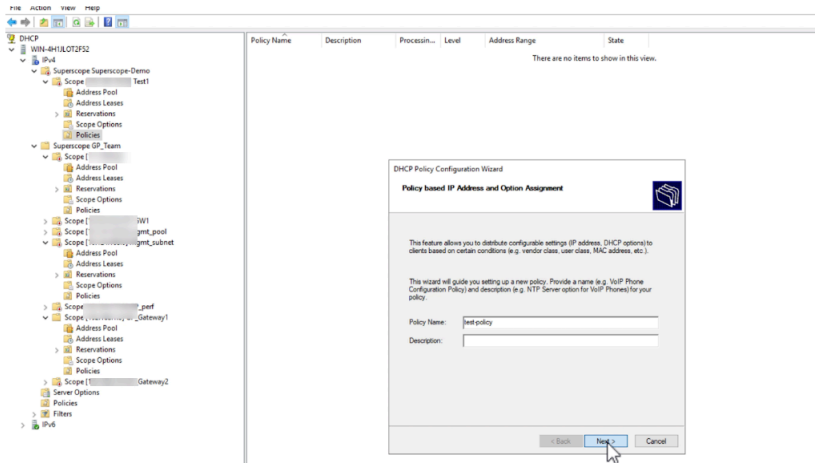
Configurer la politique DHCP sur la nouvelle portée

1. Sous **Scope (Portée)**, cliquez sur la **Policy (Politique)** et sélectionnez **New Policy (Nouvelle politique)**.

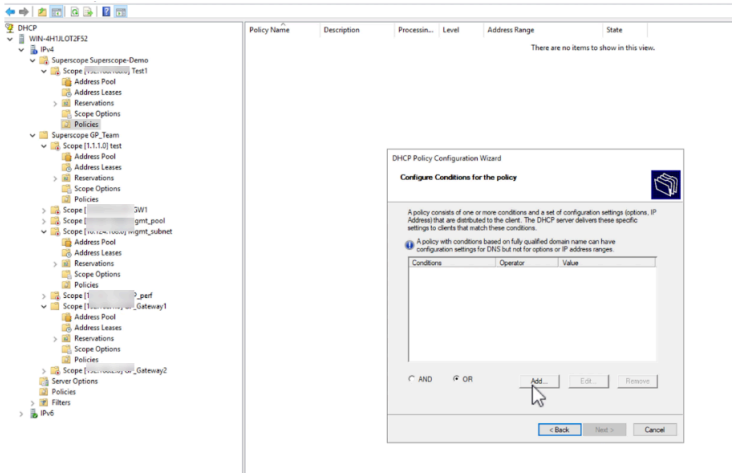


 ©2026 Palo Alto Networks, Inc.

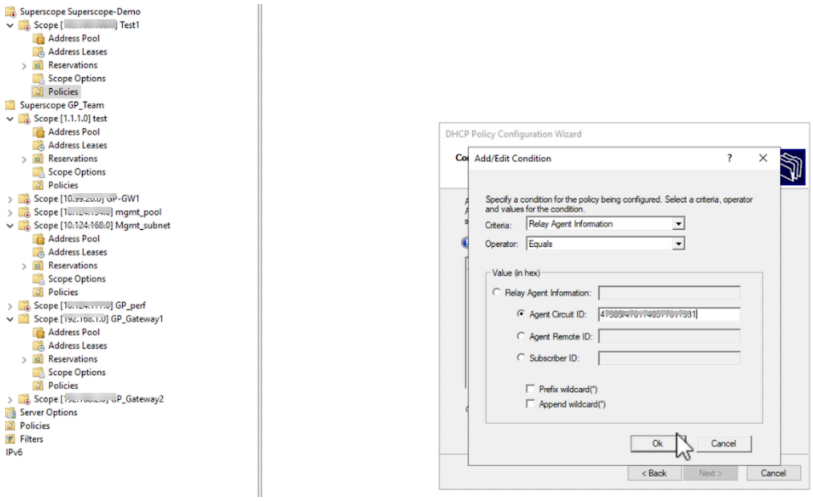
2. Entrez le nom et la description de la politique.



3. Cliquez sur **Add (Ajouter)** pour ajouter l'ID de circuit dans la règle de politique.



4. Sélectionnez **Context (Contexte)** comme **Relay Agent Information (Informations sur l'agent de relais)** et **Operator (Opérateur)** comme **Equals (Égal)**.

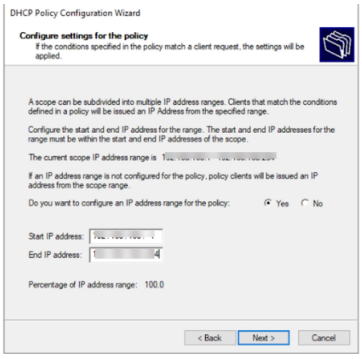


 ©2026 Palo Alto Networks, Inc.

5. Sélectionnez **Agent Circuit ID ID de circuit de l'agent)** et entrez l'ID de circuit de GlobalProtect depuis le pare-feu (**Network (Réseau)** > **GlobalProtect** > **GlobalProtect Gateway (Passerelle GlobalProtect)** > **<globalprotect-gateway-config>** > **Agent** > **Client IP Pool (Pool d'adresses IP du client)** > **DHCP Server Circuit ID (ID de circuit du serveur DHCP).**)

6. Cliquez sur **OK**.

7. Ajoutez la plage d'adresses IP de la portée dans la politique et cliquez sur **Next (Suivant)**.



8. Cliquez sur **Next (Suivant)** à nouveau, puis cliquez sur **Finish (Terminer)** pour enregistrer les configurations.

 ©2026 Palo Alto Networks, Inc.

Personnaliser les paramètres de délai d'expiration de la session du terminal

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Version de l'application GlobalProtect 6.2 ou ultérieure et version PAN-OS 11.0.2 ou ultérieure pour étendre la session utilisateur Prise en charge du système d'exploitation : Windows et Mac Version de publication de contenu : 8692-16961 Version de l'application GlobalProtect 6.1 ou ultérieure et version PAN-OS 11.0 ou ultérieure pour la notification de l'utilisateur final concernant la déconnexion de la session GlobalProtect Prise en charge du système d'exploitation : Linux, Windows 10, Windows 10 basé sur ARM64, macOS 11 et versions ultérieures, et macOS basé sur ARM 11 et versions ultérieures

Les sessions utilisateur GlobalProtect sont créées lorsqu'un utilisateur se connecte à la passerelle GlobalProtect et réussit à s'authentifier. La session est ensuite attribuée à une passerelle spécifique qui détermine le trafic à mettre en tunnel en fonction des règles définies du tunnel fractionné. La session peut être personnalisée de plusieurs manières, y compris les suivantes :

- Définir la durée de validité de la session.
- Configurer les types d'applications qui peuvent être utilisées pendant la session.
- Définir les politiques de sécurité qui s'appliquent à la session.
- Planifier l'affichage des notifications utilisateur concernant la déconnexion de la session GlobalProtect.
- Créer des messages personnalisés que vous souhaitez afficher aux utilisateurs lorsque les sessions sont sur le point d'expirer.
- Prolonger la durée de vie de la session utilisateur pour les utilisateurs de GlobalProtect.

En personnalisant les sessions utilisateur, vous pouvez vous assurer que les utilisateurs ont l'accès dont ils ont besoin pour accomplir leur travail, tout en protégeant votre réseau contre les accès non autorisés.

 ©2026 Palo Alto Networks, Inc.

Modifier les paramètres de délai d'expiration de la session du terminal

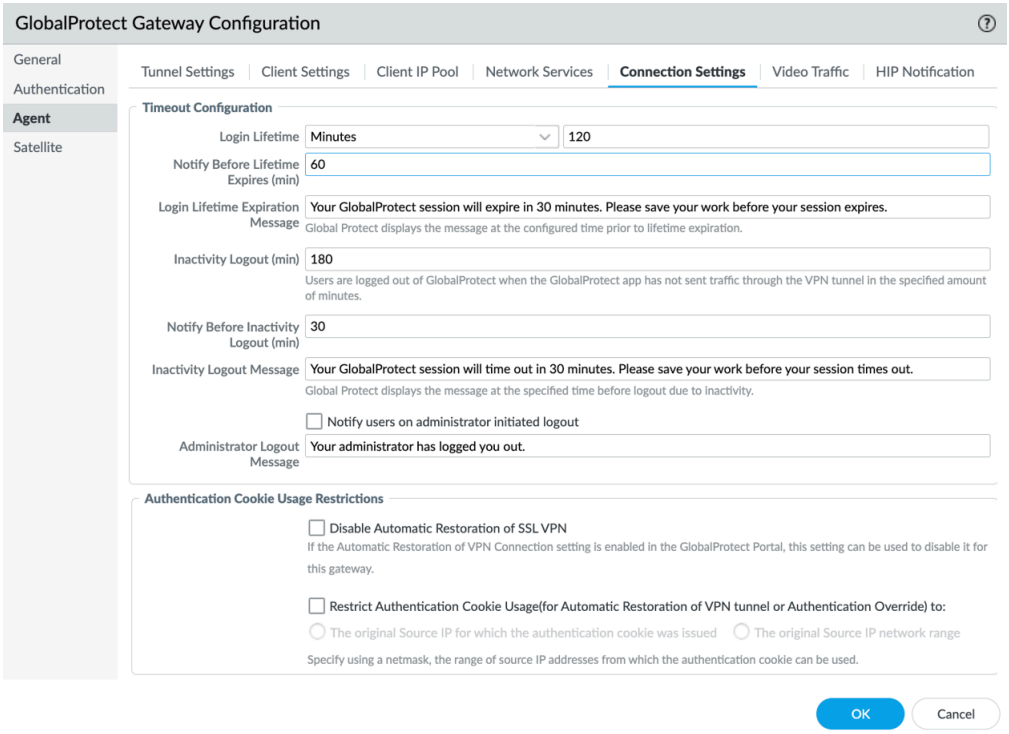
Apprenez à modifier la configuration du délai d'expiration.

1. Pour modifier les paramètres de délai d'expiration de la session du terminal, effectuez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **Agent** > **Connection Settings (Paramètres de connexion)**.
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **NGFW and Prisma Access (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)**. Sur la page des paramètres globaux, sélectionnez **General (Général)** > **Timeout (Délai d'expiration)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)** puis **Add Gateway (Ajouter une passerelle)**. Sur la page **Add Gateway (Ajouter une passerelle)**, sélectionnez **Advanced Settings (Paramètres avancés)** > **Connection Settings (Paramètres de connexion)**.
2. Dans la zone de configuration du délai d'expiration :
   1. Modifiez la **Login Lifetime (Durée de vie de connexion)** maximale d'une session de connexion d'une seule passerelle (la valeur par défaut est de 30 jours). Pendant la durée de vie, l'utilisateur reste connecté tant que la passerelle reçoit un contrôle HIP à partir du point de terminaison dans la période de **Inactivity Logout (Déconnexion d'inactivité)**. Après cette période, la session de connexion se termine automatiquement.
   2. Modifiez la période de **Inactivity Logout (Déconnexion d'inactivité)** pour spécifier la durée après laquelle les utilisateurs inactifs sont déconnectés de GlobalProtect. Vous pouvez appliquer une politique de sécurité pour surveiller le trafic des points de terminaison lorsque vous êtes connecté à GlobalProtect et pour vous déconnecter rapidement des sessions GlobalProtect inactives. Vous pouvez imposer une période de déconnexion d'inactivité plus courte. Les utilisateurs sont déconnectés de GlobalProtect si l'application GlobalProtect n'a pas acheminé le trafic via le tunnel VPN ou si la passerelle ne reçoit pas de vérification HIP du point de terminaison au cours de la période configurée.

      La période de **Inactivity Logout (Déconnexion d'inactivité)** est supérieure au Automatic Restoration of VPN Connection Timeout (délai d'expiration de la restauration automatique de la connexion VPN) pour permettre à GlobalProtect de tenter de rétablir la connexion après la déconnexion du tunnel (la plage est de 0 à 180 minutes ; la valeur par défaut est de 30 minutes). Lorsque vous configurez une passerelle interne en mode non tunnel, la période de **Inactivity Logout (déconnexion d'inactivité)** doit

 ©2026 Palo Alto Networks, Inc.

être supérieure à la valeur actuelle de l'intervalle de vérification HIP que l'application GlobalProtect attend avant d'envoyer le rapport HIP.



3. (Facultatif) Activez les notifications des utilisateurs finaux concernant la session GlobalProtect et créez des messages personnalisés.
4. Cliquez sur **OK** pour enregistrer les paramètres de délai d'expiration de session.
5. **Commit (Validez)** les modifications.

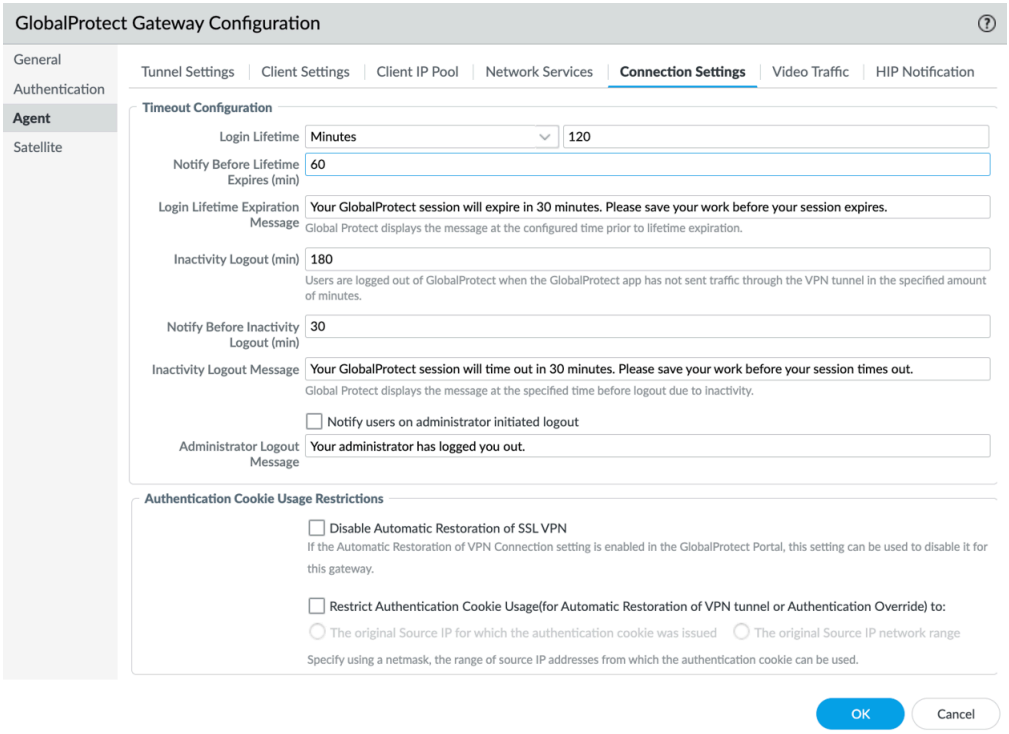
Activer les notifications des utilisateurs finaux concernant la déconnexion de la session GlobalProtect

Pour activer les notifications des utilisateurs finaux concernant la déconnexion de la session GlobalProtect et créer des messages personnalisés :

1. Pour activer les notifications des utilisateurs finaux concernant la déconnexion de la session GlobalProtect, effectuez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **Agent** > **Connection Settings (Paramètres de connexion)**.
   - Dans Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **GlobalProtect App Settings (Paramètres de l'application GlobalProtect)**. Sur la page des paramètres globaux, sélectionnez **General (Général)** > **Timeout (Délai d'expiration)**.

 ©2026 Palo Alto Networks, Inc.

- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)** puis **Add Gateway (Ajouter une passerelle)**. Sur la page Ajouter une passerelle, sélectionnez **Advanced Settings (Paramètres avancés)** > **Connection Settings (Paramètres de connexion)**.



2. Dans la zone de configuration du délai d'expiration, vous pouvez planifier l'affichage des notifications des utilisateurs finaux concernant la déconnexion de la session GlobalProtect et créer des messages personnalisés :
   1. Définissez le temps en minutes (la valeur par défaut est de 30 minutes) de la **Notify Before Lifetime Expires (Notification avant l'expiration de la durée de vie)** pour programmer l'affichage des notifications d'expiration de la durée de vie de la connexion sur l'application GlobalProtect. La **Notify Before Lifetime Expires (notification avant l'expiration de la durée de vie)** doit être inférieure à la **Login Lifetime (durée de vie de la connexion)**. Par exemple, si vous définissez **Notify Before Lifetime Expires (Notification avant l'expiration de la durée de vie)** à 120 minutes, l'application affichera la notification à l'utilisateur 2 heures avant l'expiration de la durée de vie de la connexion. Si vous ne souhaitez pas que la notification soit affichée, définissez la valeur sur 0. Si vous configurez la fonction d'extension de session utilisateur via les paramètres de l'application du portail GlobalProtect, la fenêtre contextuelle de notification d'expiration de la durée de vie de la connexion affiche l'option d'étendre la durée de la session utilisateur afin que les utilisateurs ne soient pas brusquement déconnectés de leur session.
   2. (Facultatif) Modifiez le message par défaut avec **Login Lifetime Expiration Message (Message d'expiration de la durée de vie de la connexion)** pour créer un message d'expiration de durée de vie de connexion personnalisé. La longueur du message est de 127 caractères maximum.

 ©2026 Palo Alto Networks, Inc.

3. Définissez le temps en minutes (la valeur par défaut est de 30 minutes) de la **Notify Before Inactivity Logout (Notification avant la déconnexion en cas d'inactivité)** pour programmer l'affichage de la notification de déconnexion en cas d'inactivité sur l'application. La période **Notify Before Inactivity Logout (Notification avant la déconnexion en cas d'inactivité)** doit être inférieure à la **Inactivity Logout period (Période de déconnexion en cas d'inactivité)**. Par exemple, si vous définissez la **Notify Before Inactivity Logout (Notification avant la déconnexion en cas d'inactivité)** à 20 minutes, l'application affichera la notification à l'utilisateur 20 minutes avant l'expiration de la session inactive. Si vous ne souhaitez pas que la notification soit affichée, définissez la valeur sur 0.
4. (Facultatif) Modifiez le message **Inactivity Logout Message (Message de déconnexion pour inactivité)** par défaut et de créer un message personnalisé que vous souhaitez afficher aux utilisateurs lorsque leurs sessions inactives sont sur le point d'expirer. La longueur du message est de 127 caractères maximum.
5. Activez **Notify users on administrator initiated logout (Avertir les utilisateurs lors de la déconnexion initiée par l'administrateur)** si vous souhaitez que l'application affiche une notification aux utilisateurs après que la déconnexion initiée par l'administrateur se soit produite.
6. (Facultatif) Modifiez le **Administrator Logout Message (Message de déconnexion de l'administrateur)** pour créer un message personnalisé que vous souhaitez afficher aux utilisateurs après la déconnexion initiée par l'administrateur. La longueur du message est de 127 caractères maximum.
7. Cliquez sur **OK** pour enregistrer les paramètres de notification.
8. **Commit (Validez)** les modifications.

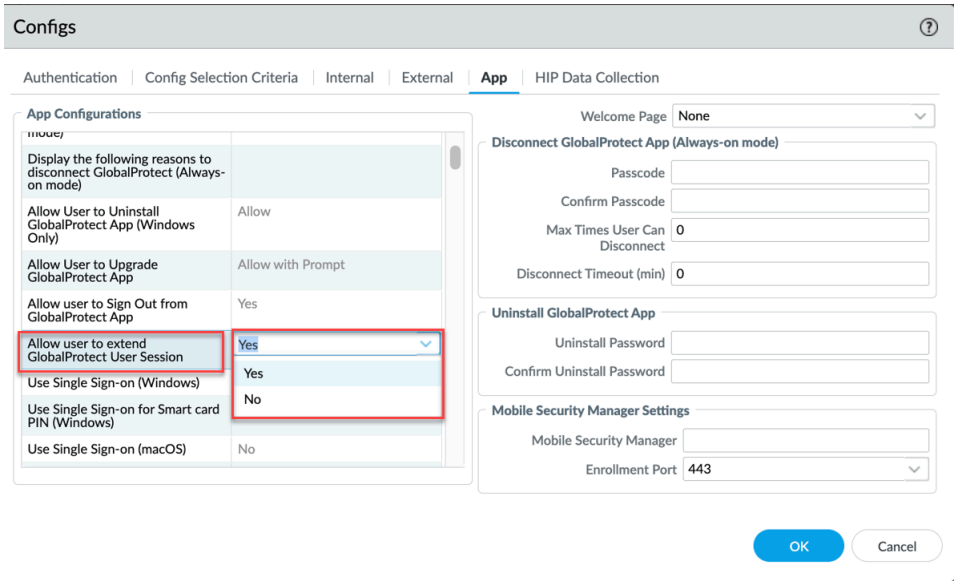
Configurer l'extension de session utilisateur

Pour configurer Étendre la session utilisateur pour les utilisateurs de GlobalProtect :

1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez la configuration du portail à laquelle vous ajoutez la configuration de l'agent, puis sélectionnez l'onglet **Agent**.
3. Dans l'onglet **Agent**, sélectionnez **App (Application)**.
4. Dans la zone des configurations d'application, définissez **Allow User to Extend GlobalProtect User Session (Autoriser l'utilisateur à prolonger la session utilisateur GlobalProtect)** sur **Yes (Oui)** pour permettre aux utilisateurs d'étendre la durée de vie de la session de connexion de l'application GlobalProtect avant qu'elle n'expire afin d'éviter une déconnexion abrupte de la session de l'application. Sélectionnez **No (Non)** (par défaut) si vous ne souhaitez pas que

 ©2026 Palo Alto Networks, Inc.

les utilisateurs puissent prolonger la durée de vie de la session de connexion de l'application GlobalProtect avant son expiration.



5. Définissez le temps en minutes avec **Notify Before Lifetime Expires (Notification avant l'expiration de la durée de vie)** pour programmer l'affichage des notifications d'expiration de la durée de vie de la connexion sur l'application GlobalProtect.

6. (Facultatif) Modifiez le message par défaut avec **Login Lifetime Expiration Message (Message d'expiration de la durée de vie de la connexion)** pour créer un message d'expiration de durée de vie de connexion personnalisé.

7. Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.

Après avoir configuré les paramètres de l'application **Extend GlobalProtect User Session (Prolonger la session utilisateur GlobalProtect)** via le portail GlobalProtect, la notification de l'utilisateur final pour l'expiration de la durée de vie de la connexion affiche l'option **Extend GlobalProtect User Session (Prolonger la session utilisateur GlobalProtect)** dans la fenêtre contextuelle de notification. L'utilisateur final peut sélectionner **Extend GlobalProtect User Session (Prolonger la session utilisateur GlobalProtect)** pour étendre la durée de vie de la session de connexion.

 ©2026 Palo Alto Networks, Inc.

Séparation du trafic tunnel sur les passerelles GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	• Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile • Terminaux macOS et Windows exécutant n'importe quelle version actuellement prise en charge de l'application GlobalProtect. • Terminaux Linux exécutant l'application GlobalProtect 6.1 ou ultérieure. Les terminaux Linux prennent en charge la segmentation de tunnel basée sur le domaine et la route d'accès uniquement ; la segmentation de tunnel basée sur l'application n'est pas pris en charge sur Linux.

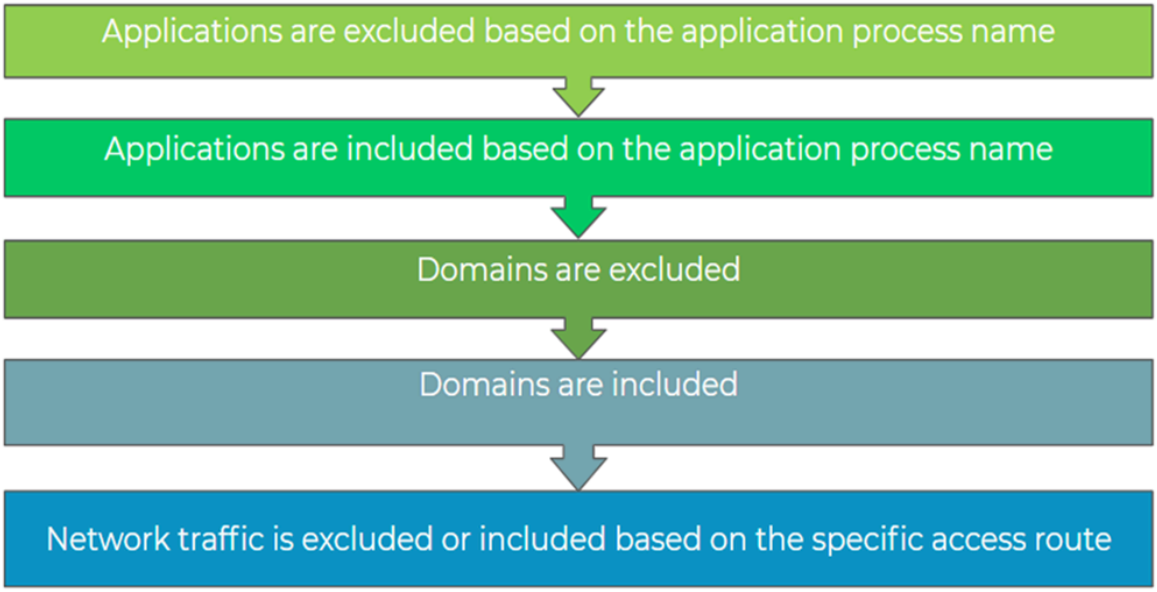
Vous pouvez configurer la séparation du trafic tunnel en fonction de l'itinéraire d'accès, du domaine de destination, de l'application ou de l'application de diffusion vidéo en continu HTTP/HTTPS.

La capacité de séparation du tunnel vous permet de préserver la bande passante et d'acheminer le trafic vers :

- Tunnelisez les applications du cloud public et SaaS de l'entreprise pour obtenir une visibilité et un contrôle total des applications SaaS et ainsi éliminer les risques associés au Shadow IT dans des environnements où il n'est pas possible de tunneliser tout le trafic.
- Envoyez le trafic sensible à la latence, comme VoIP, à l'extérieur du tunnel VPN, et le reste du trafic via le VPN à des fins d'inspection et d'application de la politique par la passerelle GlobalProtect.
- Exclure le trafic de diffusion vidéo HTTP/HTTPS du tunnel VPN. Les applications de diffusion vidéo, comme YouTube et Netflix, consomment de grandes quantités de bande passante. Exclure la diffusion vidéo à faible risque du tunnel VPN, vous pouvez diminuer la consommation de bande passante sur la passerelle.

Les règles de la segmentation de tunnel sont appliquées dans l'ordre suivant :

 ©2026 Palo Alto Networks, Inc.



Sur les terminaux Linux, seules les règles de domaine et de route d'accès sont appliquées.

Configuration d'un tunnel séparé en fonction de l'itinéraire d'accès

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Si vous n'incluez ou n'excluez pas d'itinéraires, chaque demande est acheminée à travers le tunnel GlobalProtect (sans une segmentation du tunnel). Vous pouvez inclure ou exclure un trafic du sous-réseau IP de destination spécifique de l'envoi par le tunnel GlobalProtect. Vous pouvez définir les itinéraires à envoyer via le tunnel comme des itinéraires à inclure dans le tunnel, ou comme des itinéraires à exclure du tunnel, ou les deux. Par exemple, vous pouvez paramétrer une séparation des tunnels pour permettre aux utilisateurs distants d'accéder à Internet sans recourir au tunnel VPN. Les itinéraires plus spécifiques sont prioritaires par rapport aux itinéraires moins spécifiques.

Lorsque vous définissez du trafic de tunnel séparé pour inclure les itinéraires d'accès, ce sont les itinéraires que la passerelle applique aux terminaux des utilisateurs distants afin de spécifier le trafic que les terminaux des utilisateurs peuvent envoyer via le tunnel VPN. Lorsque vous définissez le trafic du tunnel séparé de sorte à exclure les itinéraires d'accès, ces itinéraires sont transmis via la carte physique du terminal plutôt que par le tunnel VPN GlobalProtect via la carte virtuelle (le tunnel). En excluant le trafic du tunnel séparé par itinéraires d'accès, vous pouvez envoyer le trafic sensible à la latence ou très exigeant au niveau de la bande passante à l'extérieur du tunnel VPN, tandis que tous les autres types de trafic sont acheminés par le VPN à des fins d'inspection et d'application de la politique par la passerelle GlobalProtect. Vous pouvez forcer tout le trafic à transiter par le tunnel VPN à des fins d'inspection et d'application de la politique dès que des utilisateurs sont connectés à GlobalProtect, en désactivant la segmentation du tunnel.

 ©2026 Palo Alto Networks, Inc.

Les itinéraires locaux ont priorité sur les itinéraires envoyés à partir de la passerelle. Lorsque vous activez le tunnel séparé, les utilisateurs peuvent joindre les proxys et les ressources locales (comme les imprimantes locales) directement sans envoyer le trafic de sous-réseau local par l'intermédiaire du tunnel VPN. Pour empêcher les terminaux d'envoyer et de recevoir du trafic sur le sous-réseau local afin de contourner l'application de la politique au lieu de l'envoyer via le tunnel, vous pouvez activer le paramètre No direct access to local network (Pas d'accès direct au réseau local) sur les terminaux Windows, macOS et Linux (les terminaux Linux doivent exécuter la version 6.0.0 ou ultérieure de l'application GlobalProtect). Le trafic de la segmentation du tunnel en fonction de l'itinéraire d'accès, du domaine de destination et de l'application fonctionne toujours comme prévu lorsqu'aucun accès direct au réseau local n'est activé.

Activez le paramètre No direct access to local network (Aucun accès direct au réseau local) pour réduire les risques dans les réseaux non approuvés tels que les points d'accès Wi-Fi malveillants.

Tenez compte du comportement du trafic IPv4 et IPv6 selon que vous avez activé ou désactivé l'accès direct aux réseaux locaux.

Tableau 1 : Comportement du trafic IPv4

Le trafic IPv4 vers le sous-réseau local	Aucun accès direct au réseau local est activé		Aucun accès direct au réseau local est désactivé	
	Avant l'établissement du tunnel	Après l'établissement du tunnel	Avant l'établissement du tunnel	Après l'établissement du tunnel
Nouveau trafic entrant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	(Windows 10 only (Windows 10 uniquement)) Lorsque le tunneling fractionné basé sur le domaine et l'application de destination n'est pas activé, le trafic adhérant à la table de routage est envoyé via le tunnel VPN. Certaines applications peuvent toujours se lier directement à une interface spécifique et acheminer	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.

 ©2026 Palo Alto Networks, Inc.

Le trafic IPv4 vers le sous-réseau local	Aucun accès direct au réseau local est activé		Aucun accès direct au réseau local est désactivé	
		le trafic via une interface physique en ignorant la table de routage. Lorsque vous activez le tunnel séparé sur la base du domaine de destination et de l'application, le trafic est autorisé sur le réseau secondaire local via l'adaptateur physique. (macOS and Linux (macOS et Linux)) Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.		
Nouveau trafic sortant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est envoyé au tunnel VPN.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.
Trafic existant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	(Windows) Le trafic est terminé. (macOS and Linux (macOS et Linux)) Le trafic est autorisé à entrer	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.

©2026 Palo Alto Networks, Inc.

Le trafic IPv4 vers le sous-réseau local	Aucun accès direct au réseau local est activé		Aucun accès direct au réseau local est désactivé	
		sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.		

Tableau 2 : Comportement du trafic IPv6

Le trafic IPv6 vers le sous-réseau local	Aucun accès direct au réseau local est activé		Aucun accès direct au réseau local est désactivé	
	Avant l'établissement du tunnel	Après l'établissement du tunnel	Avant l'établissement du tunnel	Après l'établissement du tunnel
Nouveau trafic entrant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.
Nouveau trafic sortant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic (sauf les adresses locales de liaison fe80::/10) est envoyé via le tunnel VPN.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.
Trafic existant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.

Suivez les étapes suivantes pour configurer un tunnel séparé en fonction des itinéraires d'accès.

 ©2026 Palo Alto Networks, Inc.

1. Avant de commencer :
   1. Configurez une passerelle GlobalProtect.
   2. Pour modifier une passerelle existante ou en ajouter une nouvelle.
      - Dans Panorama, sélectionnez **Network (réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > ***<gateway-config>***.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Tunnel Settings (Paramètres de Tunnel)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access** > **Device (Périphérique)** > **GlobalProtect** > **Portals and** > **Gateways (Passerelles)** > **Add Gateway (Ajouter une passerelle)**.
2. Activez un tunnel séparé.
   1. Pour activer la segmentation du tunnel, effectuez l'une des actions suivantes :
      - Sur Panorama, dans la boîte de dialogue **GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect)**, sélectionnez **Agent** > **Tunnel Settings (Paramètres de tunnel)** pour activer le **Tunnel Mode (Mode Tunnel)**.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default (Par défaut)** et indiquez les paramètres de segmentation du tunnel.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling (Segmentation de tunnel)**.
   2. Configurez les paramètres de tunnel pour l'application GlobalProtect.
3. (Mode tunnel uniquement) Désactivez la séparation de tunnel pour garantir que tout le trafic (y compris le trafic du sous-réseau local) passe par le tunnel VPN à des fins d'inspection et d'application de la politique. Effectuez l'une des actions suivantes :
   1. Dans la boîte de dialogue **GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect)**, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > ***<client-setting-config>*** pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.

      Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default**

 ©2026 Palo Alto Networks, Inc.

(Par défaut) et indiquez les paramètres de segmentation du tunnel. Sous **Split Tunneling (Segmentation de tunnel)**, activez l'option **Block direct access to local network (Bloquer l'accès direct au réseau local)**.

- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access** > **Device** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres de l'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**. Sélectionnez ensuite **Agent Tunnel Settings (Paramètres de tunnel de l'agent)** > **Split Tunneling (Segmentation du tunnel)** et activez l'option **No direct access to local network (Aucun accès direct au réseau local)**.

2. Sélectionnez **Split Tunnel (Segmentation du tunnel)** > **Access Route (Itinéraire d'accès)**, puis activez l'option **No direct access to local network (Aucun accès direct au réseau local)**.

   Si vous activez cette option, l'accès direct au réseau local est désactivé et les utilisateurs ne peuvent envoyer de trafic directement à des proxys ou à des ressources locales lorsqu'ils sont connectés à GlobalProtect. Le trafic de tunnel divisé en fonction de l'itinéraire d'accès, du domaine de destination et de l'application fonctionne toujours comme prévu.

4. (Mode tunnel uniquement) Configurez les paramètres de tunnel séparé selon l'itinéraire d'accès.

Ces paramètres sont assignés à la carte réseau virtuel des terminaux lorsque l'application GlobalProtect établit un tunnel avec la passerelle.

Évitez de spécifier le même itinéraire d'accès en tant qu'itinéraire d'accès d'inclusion et d'exclusion. Cela entraîne une mauvaise configuration.

Vous pouvez acheminer certain trafic pour qu'il soit inclus ou exclu du tunnel en spécifiant les sous-réseaux de destination ou l'objet d'adresse (du type **Masque réseau IP**).

1. Dans la boîte de dialogue **GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect)**, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > ***<client-setting-config>*** pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.

   Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default (Par défaut)** et indiquez les paramètres de segmentation du tunnel. Sous **Split Tunneling (Segmentation du tunnel)**, ajoutez les options **Exclude Access Route (Exclure l'itinéraire d'accès)** ou **Include Access Route (Inclure l'itinéraire d'accès)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis sélectionnez **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling**

 ©2026 Palo Alto Networks, Inc.

(Segmentation de tunnel). Ajoutez **Exclude Access Route (Exclure l'itinéraire d'accès)** ou **Include Access Route (Inclure l'itinéraire d'accès)** du trafic.

2. Configurez n'importe lequel des paramètres de **Split Tunnel (Segmentation de tunnels)** basée sur l'itinéraire d'accès (**Split Tunnel (Segmentation de tunnels)** > **Access Route (Itinéraire d'accès)**) :

   - (Facultatif) Dans la section **Inclut**, **Ajoutez** les sous-réseaux de destination ou l'objet d'adresse de type **Masque de réseau IP**) pour acheminer uniquement certain trafic destiné à votre LAN vers GlobalProtect. Vous pouvez inclure des sous-réseaux IPv6 ou IPv4.

     Sur PAN-OS 8.0.2 et les versions ultérieures, un maximum de 100 itinéraires d'accès peuvent être utilisés pour inclure le trafic dans une configuration de passerelle de tunnel séparé. En combinaison avec la version 4.1.x de l'application GlobalProtect ou une version ultérieure, jusqu'à 1 000 itinéraires d'accès peuvent être utilisés.

   - (Facultatif) Dans la section **Exclut**, **Ajoutez** les sous-réseaux de destination ou l'objet d'adresse (de type **Masque de réseau IP**) que vous souhaitez que l'application exclut. Les itinéraires exclus doivent être plus spécifiques que les itinéraires inclus. Sinon, vous risqueriez d'exclure plus de trafic que prévu. Vous pouvez exclure des sous-réseaux IPv6 ou IPv4. Le pare-feu prend en charge un maximum de 100 itinéraires d'accès exclus dans une configuration de passerelle de tunnel séparé. En combinaison avec la version 4.1 de l'application GlobalProtect ou une version ultérieure, jusqu'à 200 itinéraires d'accès exclus peuvent être utilisés.

     Vous ne pouvez exclure les itinéraires d'accès des terminaux exécutant Android sur Chromebook. Seuls les itinéraires IPv4 sont pris en charge sur les Chromebook.

3. Cliquez sur **OK** pour enregistrer la configuration de segmentation des tunnels.

5. Enregistrez la configuration de la passerelle.
   1. Cliquez sur **OK** pour enregistrer les paramètres.
   2. **Validez** les modifications.

Configuration d'un tunnel séparé en fonction du domaine et de l'application

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Licence Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence GlobalProtect Gateway ou licence Prisma Access avec l'abonnement Utilisateur mobile

Lorsque vous configurez la segmentation du tunnel pour inclure tout le trafic (IPv4 et IPv6) basé sur le domaine et le port de destination (facultatif) ou l'application, tout le trafic allant vers ce domaine ou cette application spécifique est envoyé via le tunnel VPN pour inspection et application de politique. Par exemple, vous pouvez autoriser tout le trafic Salesforce à passer par le tunnel VPN à l'aide du domaine de destination ***Salesforce.com**. En autorisant (incluant) tout le trafic Salesforce à passer par le tunnel VPN, vous pouvez fournir un accès sécurisé à tous

 ©2026 Palo Alto Networks, Inc.

les domaines et sous-domaines Salesforce. Vous pouvez configurer une séparation de tunnel sans avoir à spécifier de sous-réseau d'adresse IP de destination, ce qui étend la capacité de la séparation du tunnel aux domaines et aux applications qui possèdent des adresses IP publiques dynamiques, comme les applications SaaS et les applications de cloud public.

Lorsque vous configurez un tunnel séparé pour qu'il exclut le trafic (IPv4 et IPv6) en fonction du domaine de destination et du port (facultatif) ou de l'application, tout le trafic qui se rend à cette application ou à ce domaine est transmis directement à la carte physique du terminal, sans inspection. Par exemple, vous pouvez exclure tout le trafic Skype du tunnel VPN à l'aide du nom de processus **C:\Program Files (x86)\Skype\Phone\Skype**.

Suivez ces recommandations lors de la configuration d'un tunnel divisé en fonction du domaine et de l'application de destination :

- *Avec une licence GlobalProtect, vous pouvez appliquer ou appliquer des règles de tunnel fractionné en fonction du domaine et de l'application de destination aux points de terminaison Windows et macOS.*
- *Sur les terminaux Linux exécutant l'application GlobalProtect 6.1 ou version ultérieure, vous pouvez appliquer des règles de la segmentation du tunnel en fonction du domaine ou de la voie d'accès uniquement. La segmentation du tunnel en fonction de l'application n'est pas prise en charge sur les terminaux Linux.*
- *Sur les périphériques Windows, la tunnel basée sur le domaine prend en charge le trafic TCP uniquement ; le trafic UDP n'est pas pris en charge dans la tunnellisation segmenté basée sur le domaine sous Windows.*
- *Les demandes ICMP telles que la latence, la gigue, les tests de route de trace ne sont pas prises en charge pour le tunneling fractionné en fonction du domaine de destination.*
- *Pris en charge sur les postes de travail dotés de Windows 7 Service Pack 2 et des versions ultérieures de même que de macOS 10.10 et des versions ultérieures.*

Suivez les étapes suivantes pour configurer un tunnel séparé pour inclure ou exclure le trafic en fonction du domaine de destination ou du nom du processus de l'application.

1. Avant de commencer :
   1. Configurez une passerelle GlobalProtect.
   2. Pour modifier une passerelle existante ou en ajouter une nouvelle.
      - Dans Panorama, sélectionnez **Network (réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > ***<gateway-config>***.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Tunnel Settings (Paramètres de Tunnel)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access** > **Device (Périphérique)** > **GlobalProtect** > **Portals and** > **Gateways (Passerelles)** > **Add Gateway (Ajouter une passerelle)**.

 ©2026 Palo Alto Networks, Inc.

2. Activez un tunnel séparé.
   1. Pour activer la segmentation du tunnel, effectuez l'une des actions suivantes :
      - Sur Panorama, dans la boîte de dialogue **GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect)**, sélectionnez **Agent** > **Tunnel Settings (Paramètres de tunnel)** pour activer le **Tunnel Mode (Mode Tunnel)**.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default (Par défaut)** et indiquez les paramètres de segmentation du tunnel.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis sélectionnez **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling (Segmentation de tunnel)** et indiquez les paramètres du tunnel.
   2. Configurez les paramètres de tunnel pour l'application GlobalProtect.

3. (Mode tunnel uniquement) Configurez les paramètres de séparation des tunnels selon le domaine de destination. Ces paramètres sont assignés à la carte réseau virtuel des points de terminaison lorsque l'application GlobalProtect établit un tunnel avec la passerelle.

Vous pouvez appliquer leDNS traffic (trafic DNS) en plus du trafic de réseau si vous avez déjà précisé **Both Network Traffic and DNS (Trafic réseau et trafic DNS)** comme **Split-Tunnel Option (option de tunnel séparé)** dans la zone **App Configurations (Configurations des appli)** de votre portail GlobalProtect.

1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > ***<client-setting-config>*** pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.

   Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default (Par défaut)** et indiquez les paramètres de segmentation du tunnel. Sous **Split Tunneling (Segmentation de tunnel)**, ajoutez les options **Exclude Traffic (Exclure le trafic)** ou **Include Traffic (Inclure le trafic)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis sélectionnez **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling (Segmentation de tunnel)**. Ajoutez les options **Exclude Traffic (Exclure le trafic)** ou **Include Traffic (Inclure le trafic)**.

 ©2026 Palo Alto Networks, Inc.

2. (Facultatif) **Ajoutez** les applications SaaS ou de cloud public que vous souhaitez acheminer vers GlobalProtect via la connexion VPN en utilisant le domaine et le port de destination (**Séparation de tunnel** > **Domaine et application** > **Inclure le Domaine**). Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez **`*.gmail.com`** pour autoriser tout le trafic Gmail à passer par le tunnel VPN.
3. (Facultatif) **Add (Ajoutez)** les applications SaaS ou de cloud public que vous souhaitez exclure du tunnel VPN en utilisant le domaine et le port de destination (**Split Tunnel (Segmentation de tunnel)** > **Domain and Application (Domaine et application)** > **Exclude Domain (Exclure un Domaine)**). Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez **`*.target.com`** pour exclure tout le trafic Target du tunnel VPN.
4. Cliquez sur **OK** pour enregistrer les paramètres de segmentation des tunnels.

4. (Mode tunnel uniquement) Configurez les paramètres de tunnel séparé selon l'application.

   Le trafic Safari ne peut être ajouté à la règle de tunnel séparé selon l'application sur les terminaux macOS.

   Vous pouvez utiliser des variables d'environnements pour configurer une segmentation du selon l'application sur les terminaux Windows et macOS.

   1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > ***<client-setting-config>*** pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.

      Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default (Par défaut)** et indiquez les paramètres de segmentation du tunnel. Sous **Split Tunneling (Segmentation de tunnel)**, ajoutez les options **Exclude Traffic (Exclure le trafic)** ou **Include Traffic (Inclure le trafic)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis sélectionnez **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling (Segmentation de tunnel)**. Ajoutez les options **Exclude Traffic (Exclure le trafic)** ou **Include Traffic (Inclure le trafic)**.
   2. (Facultatif) **Add (Ajoutez)** les applications SaaS ou de cloud public que vous souhaitez acheminer vers GlobalProtect via la connexion VPN en utilisant le nom de processus de l'application (**Split Tunnel (Segmentation de tunnel)** > **Domain and Application (Domaine et application)** > **Include Client Application Process Name (Inclure le Nom de processus de l'application cliente)**). Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez **`/Applications/RingCentral for Mac.app/Contents/MacOS/Softphone`** pour autoriser tout le trafic RingCentral à passer par le tunnel VPN sur les terminaux MacOS.

 ©2026 Palo Alto Networks, Inc.

3. (Facultatif) **Add (Ajoutez)** les applications SaaS ou de cloud public que vous exclure du tunnel VPN en utilisant le nom de processus de l'application (**Split Tunnel (Segmentation de tunnel)** > **Domain and Application (Domaine et application)** > **Exclude Client Application Process Name (Exclure le Nom de processus de l'application client)**). Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez **`/Applications/Microsoft Lync.app/Contents/MacOS/Microsoft Lync`** pour exclure tout le trafic de l'application Microsoft Lync du tunnel VPN.
4. Cliquez sur **OK** pour enregistrer les paramètres de segmentation des tunnels.

5. Enregistrez la configuration de la passerelle.
   1. Cliquez sur **OK** pour enregistrer la configuration de la passerelle.
   2. **Commit (Validez)** vos modifications.

Support des caractères génériques pour les paramètres de segmentation du tunnel basés sur l'application

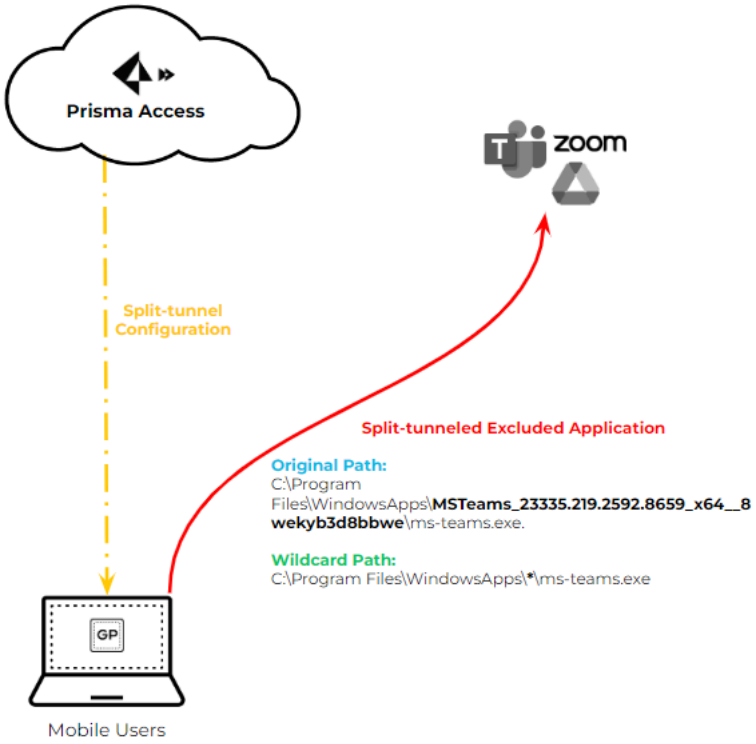
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect fonctionnant sur des terminaux Windows et macOS

À partir de la version 6.3.1 de l'application GlobalProtect, vous pouvez configurer le chemin de l'application de terminal en utilisant le caractère générique (*) lors de la configuration de segmentation du tunnel basé sur l'application, tant pour le trafic à exclure que pour le trafic à inclure. Vous pouvez ajouter jusqu'à 200 entrées à la liste pour exclure ou inclure le trafic via le tunnel VPN.

Lorsque vous utilisez le caractère générique dans le chemin de l'application et que vous l'ajoutez à la liste d'exclusion ou d'inclusion pour la segmentation du tunnel, GlobalProtect contourne la vérification de l'application pour ce chemin d'application particulier même lorsque le chemin de l'application change après une mise à jour logicielle ou de correctif.

Par exemple, lorsque vous appliquez le caractère générique au chemin des applications tierces telles que le Service de Sécurité Web Symantec (WSS) ou Microsoft Teams, vous n'avez pas besoin de mettre à jour manuellement la liste d'exclusion pour l'application dans la configuration de segmentation du tunnel chaque fois que le chemin de l'application tierce change après une mise à jour logicielle.

 ©2026 Palo Alto Networks, Inc.



Pour configurer le chemin de l'application de terminal en utilisant le caractère générique (*) lors de la configuration de segmentation du tunnel basé sur l'application, vous devez :

1. Assurez-vous que le portail GlobalProtect est configuré.
2. Assurez-vous que la Passerelle GlobalProtect est configurée.
3. Assurez-vous que la segmentation du tunnel basée sur l'application est configuré pour la passerelle GlobalProtect.
4. Configurez les paramètres de segmentation du tunnel selon l'application.
   1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > **<client-setting-config>** pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.
   2. **Ajouter (Add)** les applications SaaS ou de cloud public que vous exclure du tunnel VPN en utilisant le nom de processus de l'application (**Split Tunnel (Segmentation de tunnel)** > **Domain and Application (Domaine et application)** > **Exclude Client Application Process Name (Exclure le nom de processus de l'application client)**). Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez `/Applications/Microsoft`

 ©2026 Palo Alto Networks, Inc.

`Lync.app/*/MacOS/Microsoft Lync` pour exclure tout le trafic de l'application Microsoft Lync du tunnel VPN.

Auparavant, les chemins étaient ajoutés sans caractères génériques :

```
:\Program Files\WindowsApps
\MSTeams_23335.219.2592.8659_x64__8wekyb3d8bbwe\ms-teams.exe.
```

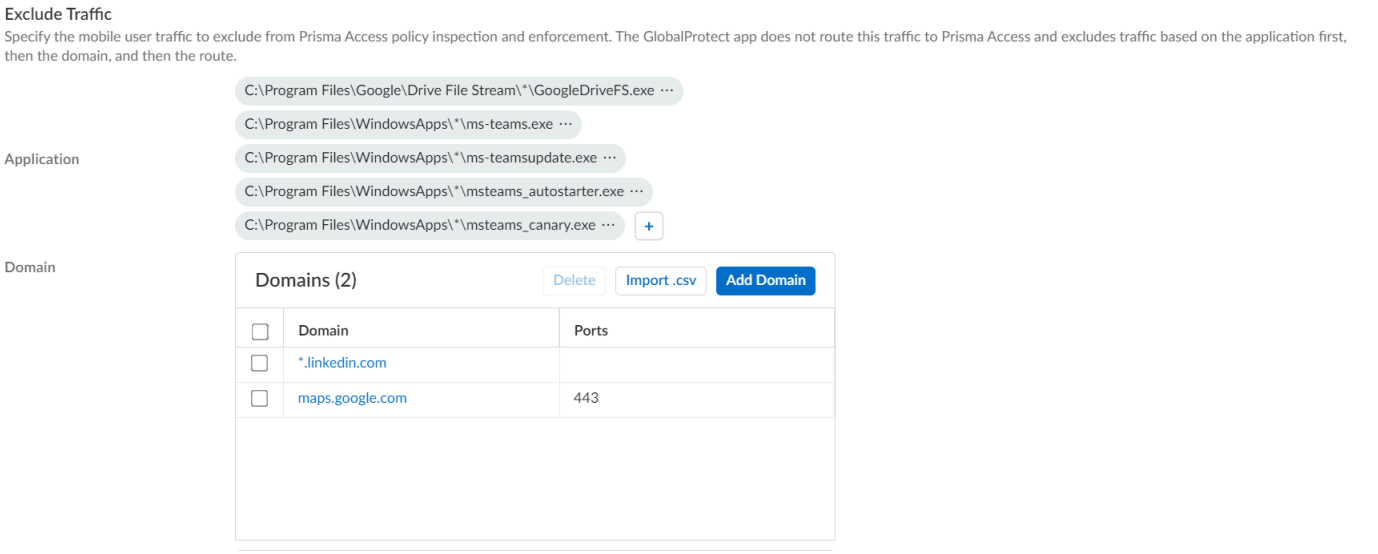
Après avoir activé la fonctionnalité de support des caractères génériques, vous pouvez ajouter le chemin avec (*) :

```
:\Program Files\WindowsApps\*\ms-teams.exe
```

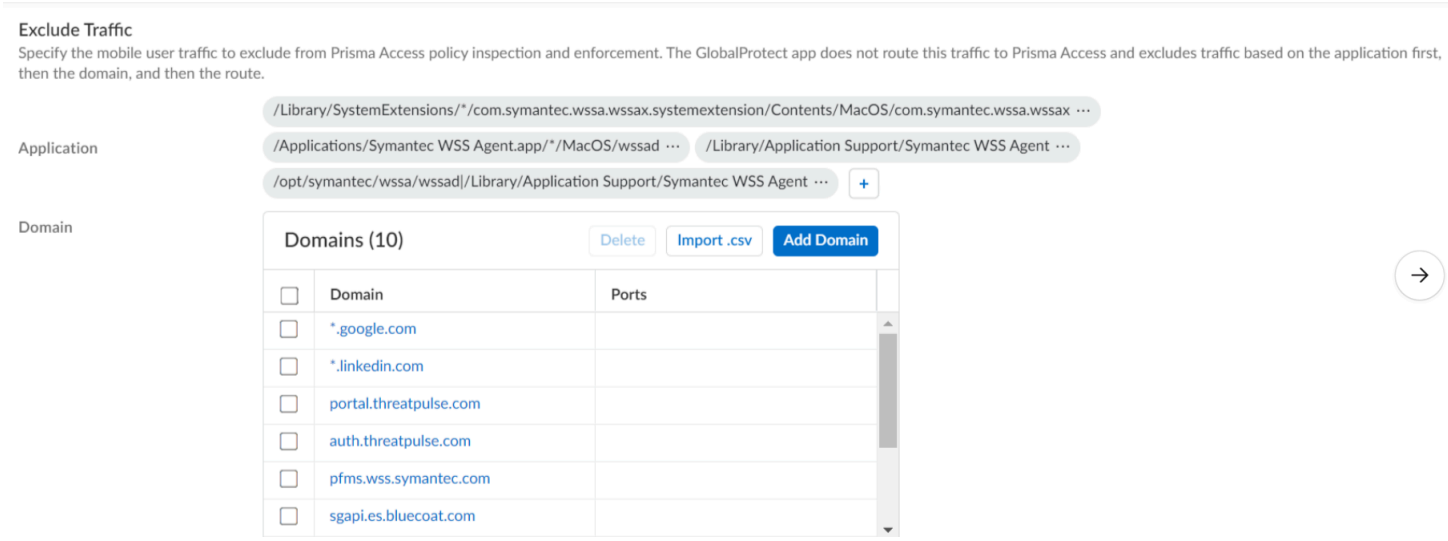
 ©2026 Palo Alto Networks, Inc.

3. Cliquez sur **OK** pour enregistrer les paramètres de segmentation des tunnels.

Windows



macOS



- *Vous pouvez utiliser un caractère générique pour tout chemin d'application dans la configuration de segmentation du tunnel.*
- *Un seul caractère générique est pris en charge dans un chemin d'application. Par exemple, `Applications/Microsoft Lync.app/*/MacOS/Microsoft Lync`. Le chemin d'application avec plus d'un caractère générique n'est pas pris en charge. Par exemple, `C:\Users\user1\AppData\Roaming\*\*\Zoom_launcher.exe`*
- *Le nom du chemin de l'application doit se terminer par le nom de l'application et non par le nom du dossier. Par exemple : `C:\Program Files\WindowsApps\*\ms-teams.exe`. Cela ne peut pas être `C:\Program Files\WindowsApps\*`*

 ©2026 Palo Alto Networks, Inc.

Configurer le DNS segmenté

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect 5.2 et versions ultérieures pour Windows et macOS avec version de contenu 8284-6139 ou ultérieure Application GlobalProtect 6.1.6 ou versions ultérieures pour iOS avec version du contenu : 8911-9049 Windows et macOS exécutant macOS Catalina 10.15.4 ou version ultérieure, et iOS

Vous pouvez désormais permettre aux utilisateurs d'accéder aux applications ou aux ressources locales en spécifiant des exclusions ou des inclusions et d'envoyer des requêtes DNS à un serveur DNS local à l'aide de l'adaptateur physique sur le terminal. Avec un DNS partagé, vous pouvez configurer quels domaines sont résolus par les serveurs DNS attribués au VPN et quels sont ceux qui sont résolus par les serveurs DNS locaux.

- Terminaux Windows et MacOS
- Terminaux iOS

Configurer la segmentation du DNS pour l'application GlobalProtect sur les terminaux Windows et macOS

1. Avant de commencer :
   1. Lancez l'interface web.
   2. Configurer une passerelle GlobalProtect
   3. Pour modifier une passerelle existante ou en ajouter une nouvelle.
      - Dans Panorama, sélectionnez **Network (réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > ***<gateway-config>***.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Tunnel Settings (Paramètres de Tunnel)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feux)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)**.
   4. Configurez la segmentation de tunnel en fonction de la route d'accès.

 ©2026 Palo Alto Networks, Inc.

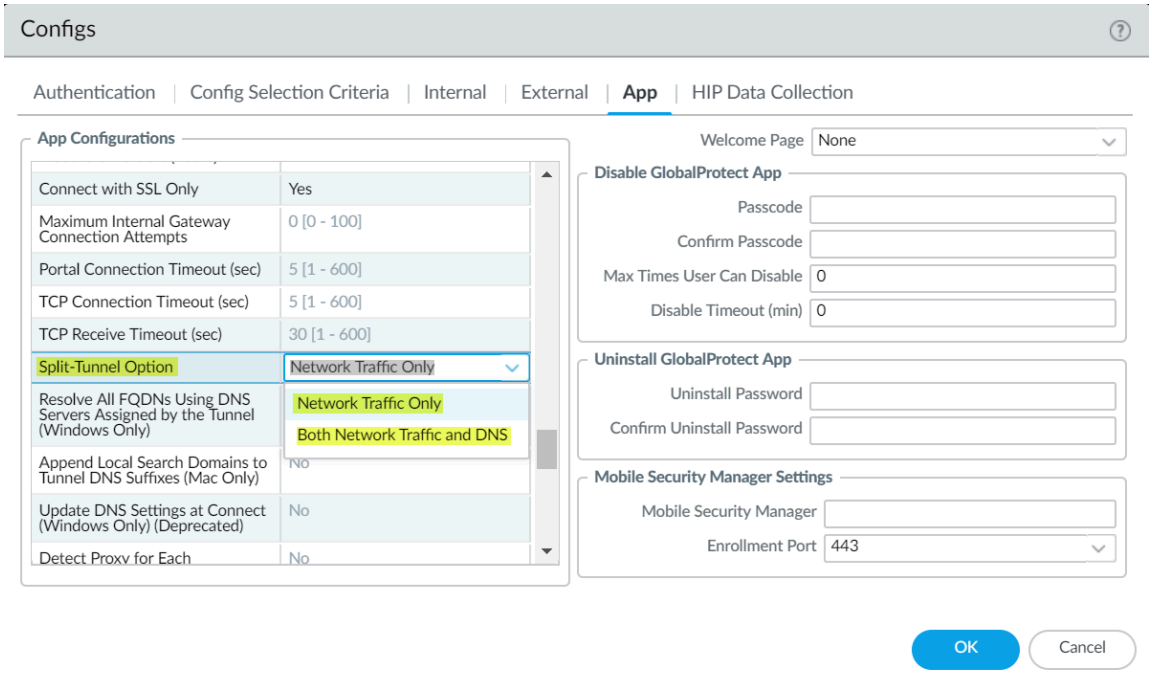
2. Activer le trafic réseau ou à la fois le trafic réseau et DNS.

Vous pouvez activer la segmentation du DNS pour autoriser les utilisateurs à diriger leurs requêtes DNS vers les applications et les ressources via le tunnel VPN ou en dehors du tunnel VPN en plus du trafic réseau.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **(Portals) Portails** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **Application** > **Split Tunnel Option (Option de segmentation de tunnel)**.

- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis sélectionnez **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling (Segmentation de tunnel)**.

1. Sélectionnez **Network Traffic Only (Uniquement le trafic du réseau)** pour inclure et exclure les règles qui sont appliquées uniquement au trafic de l'application sur le réseau et non au trafic DNS. Tout le trafic DNS passe par le tunnel VPN quel que soit le tunnel partagé sur la base du destination domain (domaine de destination) que vous avez indiqué pour les inclusions et les exclusions. Lorsque vous sélectionnez **Both Network Traffic and DNS (Trafic de réseau et DNS)**, la segmentation de tunnel sur la base du domaine de destination que vous avez indiqué pour les inclusions et les exclusions est appliqué au trafic DNS et au trafic de l'application du réseau associé pour ce domaine.



3. Cliquez deux fois sur **OK**.

4. **Commit (Validez)** la configuration.

 ©2026 Palo Alto Networks, Inc.

Configurer la segmentation du DNS pour l'application GlobalProtect sur les terminaux iOS

GlobalProtect étend désormais la fonctionnalité d'inclusion Split DNS (Segmentation du DNS) aux plateformes iOS, en plus de Linux, Windows et macOS.

La fonctionnalité d'exclusion DNS segmenté n'est pas prise en charge sur les plateformes iOS.

Avec Split DNS (Segmentation du DNS), vous pouvez configurer quels domaines sont résolus par les serveurs DNS attribués à la passerelle GlobalProtect et quels sont ceux qui sont résolus par les serveurs DNS locaux. Ceci est applicable lorsque vous avez configuré la méthode de connexion **On-demand (À la demande)** et **Always-On (Toujours actif)** pour l'application GlobalProtect. Si la configuration VPN par application est définie, seuls le trafic réseau et le trafic DNS de l'application spécifique configurée seront acheminés dans le tunnel.

La Segmentation du DNS sera appliquée quelle que soit la méthode de connexion **On-demand (À la demande)** ou **Always-On (Toujours actif)**. Il ne sera pas appliqué lorsque vous avez configuré Par application à l'aide du MDM.

Tenez compte des éléments suivants lors de la configuration de la fonctionnalité de segmentation du DNS pour les terminaux iOS :

- Par défaut, tous les DNS sont pris par le tunnel quel que soit le paramètre **Split-Tunnel Option (Option de segmentation du tunnel)** de l'application configuré en **Network Traffic Only (Trafic réseau uniquement)** ou **Both Network Traffic and DNS (Trafic réseau et DNS)**.
- Pour les terminaux Windows et macOS, le trafic correspondant pour les requêtes DNS est automatiquement envoyé à l'adaptateur virtuel s'il y a été envoyé initialement. De même, le trafic pour les requêtes DNS envoyées à l'adaptateur physique est envoyé à l'adaptateur physique.
- Pour les terminaux iOS et Android, les routes d'accès IP contrôlent le trafic tunnelisé et les règles de domaine contrôlent les requêtes DNS tunnelisées. Si vous souhaitez que DNS et trafic pour un même site soient inclus ou exclus dans le tunnel VPN, vous devez configurer des règles IP et Domaine distinctes en conséquence.
- Si vous souhaitez configurer DNS segmenté sur des terminaux iOS, vous devez :
  - Ajouter un itinéraire d'accès IP (Inclusion), afin que GlobalProtect ne soit plus l'itinéraire par défaut
  - Vous devez définir l'option **Resolve all FQDNs using theTunnel DNS Server (Résoudre tous les FQDN via les DNS de tunnel)** sur **No (Non)** dans les paramètres de l'application des configurations du portail. (La valeur par défaut est **Yes (Oui)**.

    Sur Strata Cloud Manger (NGFW), sélectionnez

    - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres de l'agent)** > **Agent App Settings (Paramètres de l'application de l'agent)** > **App Configuration (Configuration d'application)** > **Show Advanced Options (Afficher les options avancées)** et sous **DNS**, sélectionnez **Resolve All FQDNs Using the Tunnel DNS Server (iOS only) (Résoudre tous les FQDN via les serveurs DNS de tunnel [iOS uniquement])**.
  - Vous devez configurer les règles d'inclusion du domaine pour tout trafic DNS que vous souhaitez résoudre par le serveur DNS tunnel.

 ©2026 Palo Alto Networks, Inc.

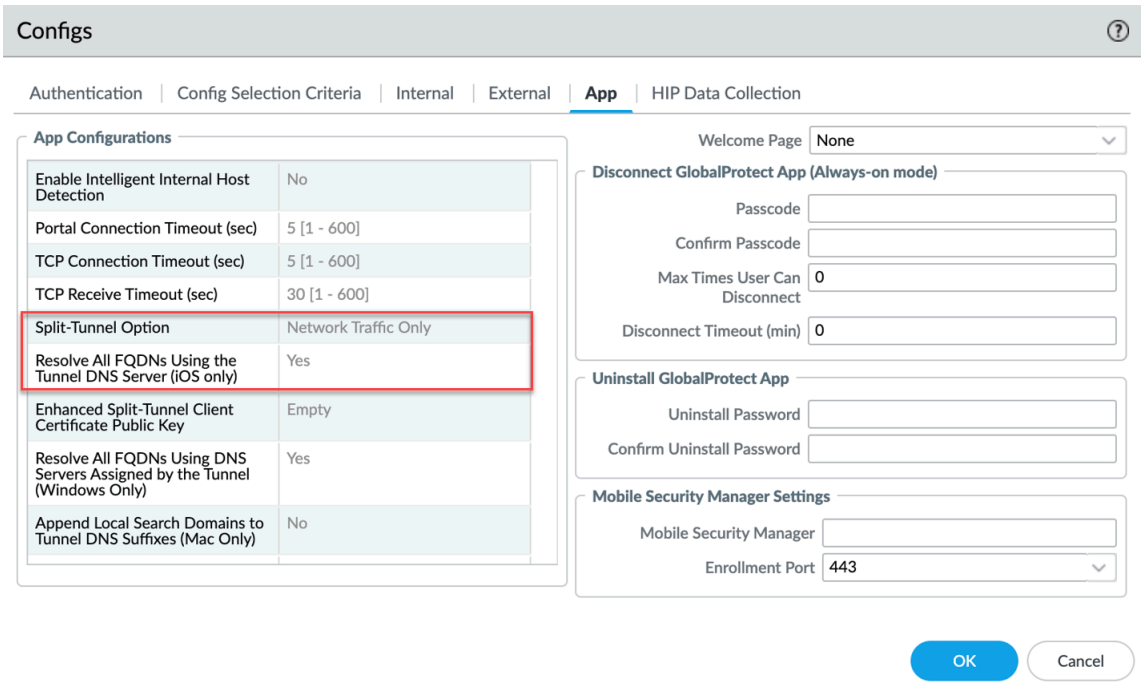
- Le paramétrage de **Split-Tunnel Option (Option de segmentation du tunnel)** sur les paramètres d'application des configurations du portail n'a aucun impact sur la segmentation du DNS.

Utilisez les procédures suivantes pour activer la fonctionnalité de segmentation du DNS pour les terminaux iOS :

1. Assurez-vous que le portail GlobalProtect est configuré.

   Pour vous assurer que le portail GlobalProtect est configuré, veuillez confirmer que les valeurs par défaut suivantes des paramètres de l'application sur les configurations du portail sont utilisées :

   - **Split-Tunnel Option (Option de segmentation du tunnel)** - Trafic réseau uniquement
   - **Resolve All FQDNS Using the Tunnel DNS Server (iOS only) (Résoudre tous les FQDNs via les serveurs DNS de tunnel ([iOS uniquement])** -Oui



2. Assurez-vous que la passerelle GlobalProtect est configurée.

3. Configurez les paramètres de segmentation de tunnel en fonction des DNS et du trafic réseau pour la passerelle GlobalProtect. Ces paramètres sont assignés à la carte réseau virtuel des points de terminaison lorsque l'application GlobalProtect établit un tunnel avec la passerelle.

   1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > **<client-setting-config>**pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.

      Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs**

 ©2026 Palo Alto Networks, Inc.

mobiles) > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default (Par défaut)** et indiquez les paramètres de segmentation du tunnel.

- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis sélectionnez **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling (Segmentation de tunnel)** et indiquez les paramètres de segmentation du tunnel.

2. Ajoutez l'itinéraire d'accès et le domaine que vous souhaitez acheminer vers GlobalProtect via la connexion VPN. Vous pouvez ajouter jusqu'à 200 entrées à la liste de la passerelle GlobalProtect. Vous pouvez ajouter certains trafics et DNS à inclure dans le tunnel en spécifiant les sous-réseaux de destination ou l'objet d'adresse et le domaine de destination.

   Vous pouvez configurer la fonctionnalité de segmentation de tunnel pour l'application GlobalProtect sur les terminaux iOS pour spécifier comment le DNS et le trafic réseau doivent être traités au sein du tunnel :

   - Seuls certains trafics et certains DNS doivent être tunnelisés par GlobalProtect

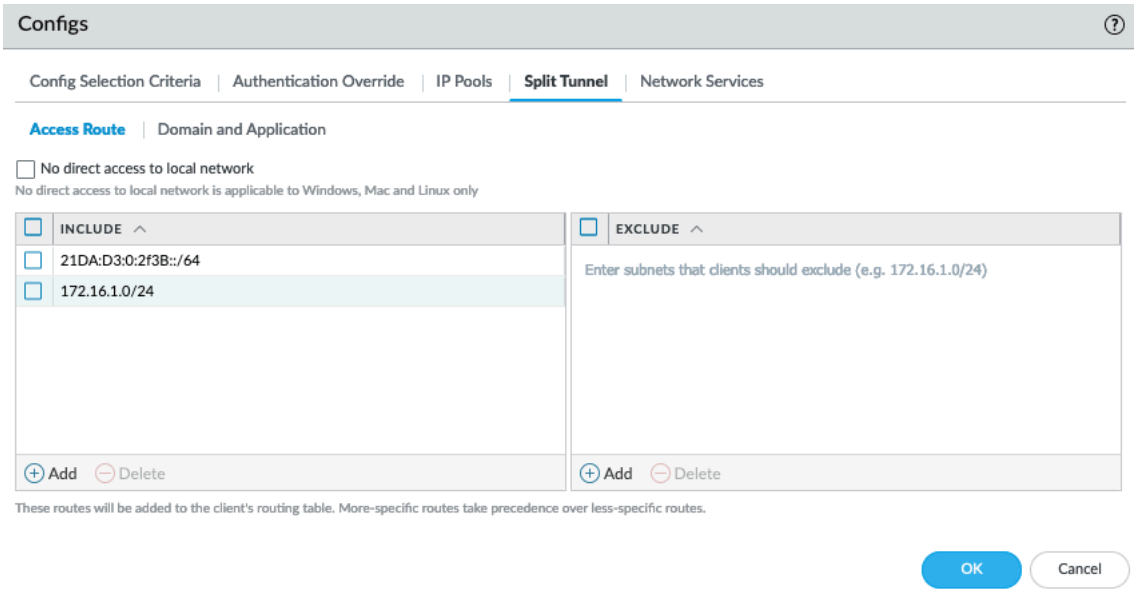
 ©2026 Palo Alto Networks, Inc.

- Seuls certains trafics sont inclus dans le tunnel et excluent tous les DNS

Pour inclure uniquement certains trafics et certains DNS à tunneliser via la connexion VPN

1. Configurez les paramètres basés sur l'itinéraire d'accès **Split Tunnel (Segmentation de tunnel)** (**Split Tunnel [Segmentation de tunnel]** > **Access Route [Itinéraire d'accès]**).

   Dans la section **Inclusion**, ajoutez les sous-réseaux de destination ou l'objet d'adresse (de type masque de réseau IP) pour acheminer uniquement certain trafic destiné à votre LAN vers GlobalProtect. Vous pouvez inclure des sous-réseaux IPv6 ou IPv4.

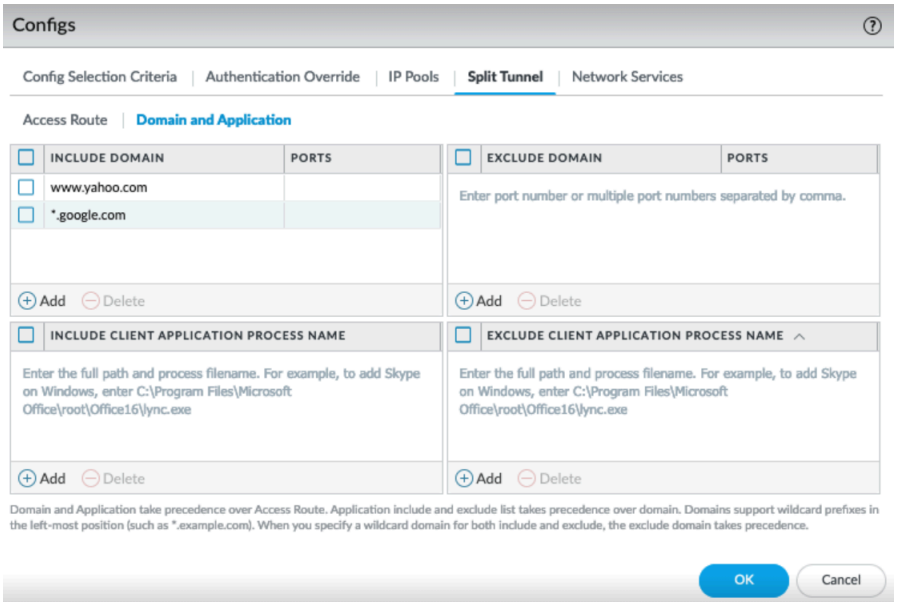


2. Configurez les paramètres **Split Tunnel (Segmentation de tunnel)** basés sur le domaine (**Split Tunnel [Segmentation de tunnel]** > > **Domain and Application [Domaine et application]**).

   Dans la zone **Include (Inclusion)**, ajoutez le domaine privé et les applications SaaS ou cloud public dont vous souhaitez acheminer le trafic DNS vers GlobalProtect via la connexion VPN à l'aide du domaine et du port de destination. Ces règles de domaine ne s'appliquent qu'aux requêtes DNS et non au trafic. Vous pouvez ajouter jusqu'à 200 entrées à la liste de la passerelle GlobalProtect. Par exemple, ajoutez ***.google.com** pour permettre à toutes les requêtes DNS de Google de passer par le tunnel VPN. Vous pouvez utiliser un caractère générique (*) au début du nom de

 ©2026 Palo Alto Networks, Inc.

domaine. Vous ne pouvez pas utiliser le caractère générique (*) au milieu ou à la fin du nom de domaine.



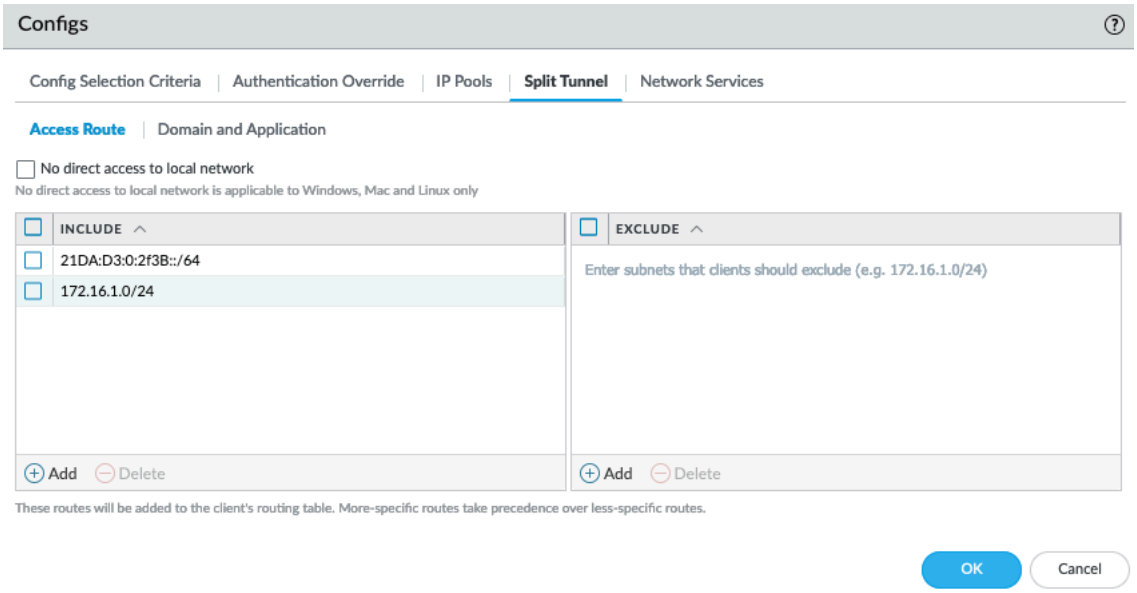
 ©2026 Palo Alto Networks, Inc.

3. Configurez le serveur DNS du tunnel.
   - Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > **<client-setting-config>** > **Network Services (Services du réseau)**.
   - Entrez dans le **DNS Server (Serveur DNS)**.
   - (Facultatif)Entrez le **DNS Suffix (Suffixe DNS)**.
   - Cliquez sur **OK**.

Pour inclure seulement certains trafics dans le tunnel et exclure tous les DNS

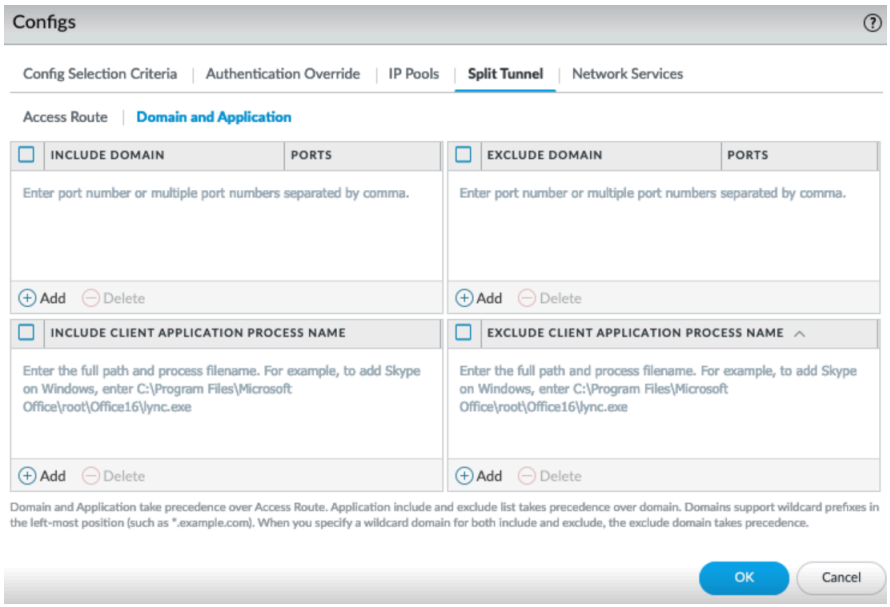
1. Configurez les paramètres basés sur l'itinéraire d'accès **Split Tunnel (Segmentation de tunnel)** (**Split Tunnel [Segmentation de tunnel]** > **Access Route [Itinéraire d'accès]**).

   Dans la section **Inclusion**, ajoutez les sous-réseaux de destination ou l'objet d'adresse (de type masque de réseau IP) pour acheminer uniquement certain trafic destiné à votre LAN vers GlobalProtect. Vous pouvez inclure des sous-réseaux IPv6 ou IPv4.



2. Pour exclure tous les DNS du tunnel, laissez la zone d'inclusion vide (zone **Split Tunnel [Segmentation de tunnel]** > **Domain and Application [Domaine et application]** > **Include [Inclusion]**). Dans ce cas, aucun DNS ne sera tunnelisé via la connexion VPN

 ©2026 Palo Alto Networks, Inc.



4. Cliquez sur **OK** et validez vos modifications.

5. Affichez le PanGPS.log pour afficher les paramètres DNS : Par exemple,

```
DNSSettings = { protocol = cleartext server = ( x.x.x.x, )
 searchDomains = () matchDomains = ( paloaltonetworks.com,
 *.paloaltonetworks.com, ) matchDomainsNoSearch = YES }
 IPv4Settings = { configMethod = manual addresses =
 ( xxx.xx.xx.xx, ) subnetMasks = ( xxx.xxx.xxx.xxx, )
 includedRoutes = ( { destinationAddress = 0.0.0.0
 destinationSubnetMask = 0.0.0.0 }, { destinationAddress
 = x.x.x.x destinationSubnetMask = xxx.xxx.xxx.xxx }, )
 excludedRoutes = ( { destinationAddress = xxx.xx.xx.xxx
 destinationSubnetMask = xxx.xxx.xxx.xxx }, ) overridePrimary
 = NO } IPv6Settings = { configMethod = manual addresses =
 ( fc00::4f, ) networkPrefixLengths = ( 128, ) includedRoutes
 = ( { destinationAddress = :: destinationNetworkPrefixLength =
 0 }, { destinationAddress = :: destinationNetworkPrefixLength =
 128 }, )
```

```
  Débogage (13251) : split-tunnel-option est network-traffic
Débogage (13262) : split-tunnel-option-mobile est oui
```

split-tunnel-option peut avoir les valeurs **network-traffic** ou **network traffic and DNS** et **split-tunnel-option-mobile** peuvent avoir la valeur **oui** ou **non**.

 ©2026 Palo Alto Networks, Inc.

Exclusion du trafic vidéo à partir du tunnel VPN GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez configurer un tunnel séparé pour qu'il exclut l'envoi par le tunnel VPN du trafic de diffusion vidéo HTTP/HTTPS provenant d'un domaine donné, ce qui permet au trafic vidéo de passer directement des interfaces physiques du terminal. La fonctionnalité App-ID sur le pare-feu identifie la diffusion vidéo avant que le trafic puisse être segmenté. En excluant la diffusion vidéo à faible risque (comme YouTube et Netflix) du tunnel VPN, vous pouvez diminuer la consommation de bande passante sur la passerelle.

> *Avec une licence GlobalProtect, vous pouvez appliquer ou appliquer des règles de tunnel fractionné pour exclure le trafic de streaming vidéo du tunnel VPN sur les points de terminaison Windows et macOS.*

Tous les types de trafic vidéo sont redirigés pour les applications de diffusion vidéo suivantes :

- YouTube
- Dailymotion
- Netflix

Si vous excluez les autres applications de diffusion vidéo du tunnel VPN, seuls les types de trafic vidéo suivants sont redirigés pour ces applications :

- MP4
- WebM
- MPEG

Utilisez les étapes suivantes pour configurer un tunnel séparé afin d'exclure le trafic de diffusion vidéo du tunnel VPN.

1. Avant de commencer :
   1. Suivez les prérequis suivants :
      - Pris en charge uniquement sur les postes de travail dotés de Windows 7 Service Pack 2 et des versions ultérieures de même que de macOS 10.10 et des versions ultérieures.
      - Vous devez vous assurer que les pool d'adresses IP utilisés pour attribuer des adresses IP aux cartes du réseau virtuel sur ces points de terminaison n'incluent aucune adresse IPv6. Si la carte physique des points de terminaison Windows ou macOs ne prend en charge que les adresses IPv4, l'utilisateur du point de terminaison ne peut accéder aux applications de diffusion vidéo que vous excluez du tunnel VPN lorsque vous configurez la passerelle GlobalProtect pour qu'elle attribue des adresses IPv6 aux cartes du réseau virtuel sur les points de terminaison qui se connectent à la passerelle.

 ©2026 Palo Alto Networks, Inc.

- Si vous excluez le trafic de diffusion vidéo du tunnel VPN, n'incluez pas les applications de navigateur Web, comme Firefox ou Chrome, dans le tunnel VPN. Ainsi, vous vous assurez qu'il n'y a aucune logique conflictuelle dans la configuration de segmentation de tunnel et que vos utilisateurs peuvent visionner des vidéos à partir des navigateurs Web.
- Pour exclure le trafic de l'application Sling TV du tunnel VPN, configurez un tunnel séparé basé sur une application.

2. Configurez une passerelle GlobalProtect.
3. Pour modifier une passerelle existante ou en ajouter une nouvelle.
   - Dans Panorama, sélectionnez **Network (réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > ***<gateway-config>***.
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Tunnel Settings (Paramètres de Tunnel)** > ***<tunnel-config>***
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)**.

2. Activez un tunnel séparé.

1. Pour activer la segmentation du tunnel, effectuez l'une des actions suivantes :
   - Sur Panorama, dans la boîte de dialogue **GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect)**, sélectionnez **Agent** > **Tunnel Settings (Paramètres de tunnel)** pour activer le **Tunnel Mode (Mode Tunnel)**.
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default (Par défaut)** et indiquez les paramètres de segmentation du tunnel.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis sélectionnez **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling (Segmentation de tunnel)**.
2. Configurez les paramètres de tunnel pour l'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

3. (Mode tunnel uniquement) Excluez le trafic de diffusion vidéo HTTP/HTTPS du tunnel VPN.
   1. Dans la boîte de dialogue **Configuration de la passerelle GlobalProtect**, sélectionnez **Agent** > **Video Traffic (Trafic vidéo)**.
   2. Activez l'option visant à **Exclude video applications from the tunnel (Exclure les applications vidéo du tunnel)**.

      Si vous activez cette option, mais que vous n'excluez pas d'applications de diffusion vidéo spécifiques du tunnel VPN, tout le trafic de diffusion vidéo est exclu.

      Le trafic vidéo exclu ne prendra pas en compte la configuration de segmentation de tunnel pour les flux vidéo.
   3. (Facultatif) **Browse (Parcourez)** la liste des **Applications** pour consulter toutes les applications de diffusion vidéo que vous pouvez exclure du tunnel VPN. Cliquez sur l'icône d'ajout en regard des applications que vous souhaitez exclure. Par exemple, cliquez sur l'icône d'ajout de **directv** pour exclure le trafic de diffusion vidéo provenant de DIRECTV du tunnel VPN.
   4. **Ajoutez** les applications de diffusion vidéo que vous voulez exclure du tunnel VPN en utilisant la liste déroulante **Applications** une version plus brève de la liste des **Applications**. Vous pouvez ajouter un maximum de 200 entrées d'applications vidéo à la liste. Par exemple, sélectionnez **youtube-streaming** pour exclure du tunnel VPN tout le trafic de diffusion vidéo provenant de YouTube.

4. Enregistrez la configuration de la passerelle.
   1. Cliquez sur **OK** pour enregistrer la configuration de la passerelle.
   2. **Commit (Validez)** vos modifications.

 ©2026 Palo Alto Networks, Inc.

Héberger un fichier de configuration pour la segmentation de tunnel sur un serveur web

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	• Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile • Version de l'application GlobalProtect 6.2 ou ultérieure pour Windows et macOS • Version de publication de contenu 8699-7991 ou ultérieure

Vous pouvez soit définir votre segmentation de tunnel sur la passerelle GlobalProtect, soit l'héberger dans un fichier de configuration pour segmentation de tunnel que vous hébergez sur un serveur web de votre environnement. Afin de pousser la configuration de la segmentation du tunnel vers le terminal :

- Votre fichier de configuration de la segmentation du tunnel doit être analysé comme XML valide
- Le serveur web doit être accessible par tous les terminaux configurés pour aller chercher le fichier de configuration de la segmentation du tunnel
- Le serveur et le client doivent pouvoir s'authentifier mutuellement

Si l'application GlobalProtect ne peut pas aller chercher le fichier de configuration de la segmentation du tunnel, il revient à la configuration de la segmentation du tunnel que vous avez configurée sur la passerelle.

Le tableau suivant indique les limites de configuration de la segmentation du tunnel lorsque la configuration est hébergée sur GlobalProtect ou lorsqu'elle est hébergée dans un fichier de configuration de la segmentation du tunnel dans votre environnement :

Segmentation du tunnel par...		Configurer une passerelle GlobalProtect	Hébergé sur un serveur web
Accéder à l'itinéraire	Inclure	1000	1000
	Exclure	200	1000
Domaine	Inclure	200	1000
	Exclure	200	1000
Application	Inclure	200	200

 ©2026 Palo Alto Networks, Inc.

Segmentation du tunnel par…		Configurer une passerelle GlobalProtect	Hébergé sur un serveur web
	Exclure	200	200

 ©2026 Palo Alto Networks, Inc.

1. Créez et signez le fichier de configuration de la segmentation du tunnel.
   1. Créez votre fichier de configuration de la segmentation du tunnel au format XML, comme dans l'exemple suivant.

```
File    Edit    View

    <access-routes>
        <member>0.0.0.0</member>
    </access-routes>
    <exclude-access-routes>
        <member>18.0.0.0/8</member>
    </exclude-access-routes>
    <include-split-tunneling-domain>
        <member>*.kohls.com</member>
        <member>*.target.com</member>
    </include-split-tunneling-domain>
    <exclude-split-tunneling-domain>
        <member>*.cnn.com</member>
        <member>*.barnesandnoble.com</member>
    </exclude-split-tunneling-domain>
    <exclude-split-tunneling-application>
        <member>C:\Users\admin\AppData\Roaming\Zoom\bin\Zoom.exe</member>
        <member>C:\Users\admin\AppData\Roaming\Zoom\bin\Zoom_launcher.exe</m
    </exclude-split-tunneling-application>
    <include-split-tunneling-application>
        <member>/Applications/TV.app/Contents/MacOS/TV</member>
    </include-split-tunneling-application>
```

   2. Signez le fichier de configuration.

      Par exemple, si le nom du fichier de signature est config_signature.sha256:

      openssl dgst -sha256 -sign private_key.pem -out config_signature.sha256 config.txt

      Vous pouvez éventuellement vérifier la signature :

      openssl dgst -sha256 -verify public_key.pem -signature config_signature.sha256 config.txt

      Fichier de signature d'encodage Base64 (sans encapsulation) :

      openssl base64 -A -in config_signature.sha256 -out encoded_signature.txt

   3. Ajoutez le résumé codé au fichier de configuration.
      1. Ajoutez le résumé codé en première ligne dans le fichier de configuration. Il doit être sur une seule ligne.
      2. Ajoutez la configuration de la segmentation du tunnel comme deuxième ligne.
      3. Si vous souhaitez que le trafic soit acheminé par défaut via GlobalProtect, ajoutez une section <access-routes> avec l'itinéraire par défaut 0.0.0.0/0.

 ©2026 Palo Alto Networks, Inc.

Le contenu du fichier ne doit pas être terminé par un caractère NULL (ASCII '\0', ou ^@)").

```
YV8z+cr0f6qnjbRoptUuSiCsZeucNVdMCXdD4UrgQAX1faI3TwknO/Vuglo35mUi1RULuDyhuVq+
0HKI2DjHgqjiVCydFZqMFflMQY0Zng4VtmI9GYksXNtA5vtjQ0yBhEExNqfA7iS1b4os+BjGEoAXKQr
Gu1WOSpddGKnxS23DF84bR1ajrl75P6IRdoCMFZ0f4BJ7DQqPwtqOT4I3aBT8dxow0J6mCY5JPVLrRD
      <access-routes>
            <member>0.0.0.0</member>
      </access-routes>
      <exclude-access-routes>
            <member>18.0.0.0/8</member>
      </exclude-access-routes>
      <include-split-tunneling-domain>
            <member>*.kohls.com</member>
            <member>*.target.com</member>
      </include-split-tunneling-domain>
      <exclude-split-tunneling-domain>
            <member>*.cnn.com</member>
            <member>*.barnesandnoble.com</member>
      </exclude-split-tunneling-domain>
      <exclude-split-tunneling-application>
            <member>C:\Users\admin\AppData\Roaming\Zoom\bin\Zoom.exe</member>
            <member>C:\Users\admin\AppData\Roaming\Zoom\bin\Zoom_launcher.exe</
      </exclude-split-tunneling-application>
      <include-split-tunneling-application>
            <member>/Applications/TV.app/Contents/MacOS/TV</member>
      </include-split-tunneling-application>
```

4. Hébergez le fichier de configuration de la segmentation du tunnel que vous venez de créer sur un serveur web accessible par vos terminaux GlobalProtect.
5. Activez l'authentification mutuelle.

   Vous aurez besoin du certificat de clé publique que vous utilisez pour l'authentification mutuelle pour la configuration GlobalProtect.

   Par exemple, pour héberger le fichier de configuration de la segmentation du tunnel dans AWS derrière les équilibreurs de charge réseau protégés par le pare-feu réseau AWS, vous procédez comme suit :

   1. Fournissez des instances EC2 aux serveurs hôtes.
   2. - Créez des équilibreurs de charge réseau (NLB) et configurez les écouteurs sur le port TCP 443.

 ©2026 Palo Alto Networks, Inc.

- Créez des groupes cibles avec le port 443 et associez des instances EC2 aux groupes cibles.
- Configurez le pare-feu réseau et deux groupes de règles sans état et associez-les aux pare-feu configurés que vous avez provisionnés. Configurez la règle 1 pour supprimer les paquets vers tous les ports et protocoles à partir d'une adresse IP ou d'un sous-réseau spécifique. Configurez la règle 2 pour autoriser les paquets sur le port TCP 443.
- Configurez les tables de routage VPC pour transférer le trafic provenant d'Internet vers le NLB via le pare-feu réseau.

2. Ajoutez le certificat de clé publique que vous avez utilisé sur votre serveur web à la configuration du portail.

Dans la zone Configurations d'application, collez le certificat de clé publique dans le champ **Enhanced Split Tunnel Client Certificate Public Key (Clé publique du certificat client de segmentation du tunnel amélioré)**.

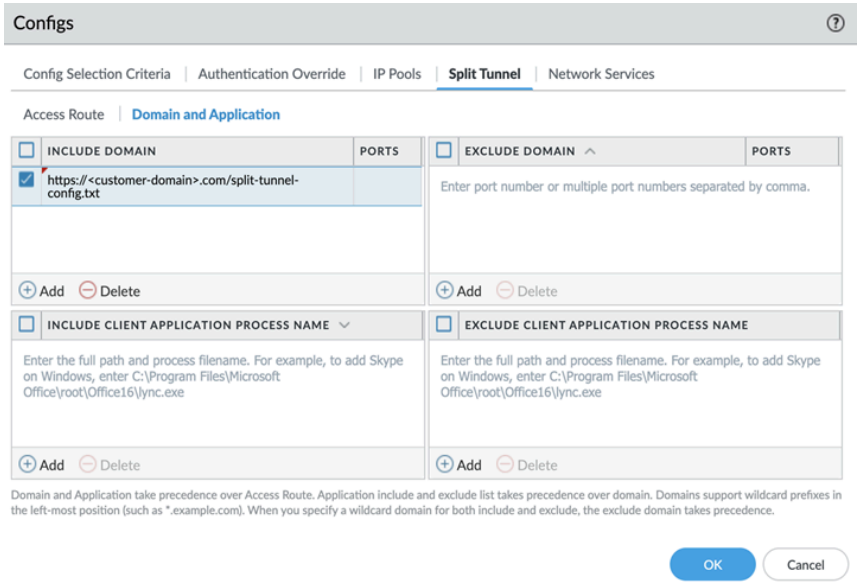
Enhanced Split-Tunnel Client Certificate Public Key	-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQEFA... Sp6bmLQ3DjporGzz428VVdBal... ct6GRRmDI7RtWsyRWO2QF+... f5NkFfAFJBK8TOkwhGIfjRBt8o... GqCKgiveZJmY54EyelQWxnOY... Z7AOOSGuTK9c+U8oSvAOp3I... VwIDAQAB -----END PUBLIC KEY-----

3. Enable split tunneling (Activer la segmentation de tunnel) et ajoutez l'URL de votre fichier de configuration de la segmentation du tunnel.
   1. Pour activer la segmentation du tunnel, effectuez l'une des actions suivantes :
      - Sur Panorama, dans la boîte de dialogue **GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect)**, sélectionnez **Agent** > **Tunnel Settings (Paramètres de tunnel)** pour activer le **Tunnel Mode (Mode Tunnel)**.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Container Mobile Users (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)**. Dans Tunnel Settings (Paramètres du tunnel), sélectionnez **Default (Par défaut)** et indiquez les paramètres de segmentation du tunnel.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Agent Settings (Paramètres d'agent)** > **Agent Tunnel Settings (Paramètres de tunnel de l'agent)**, puis sélectionnez **Add Agent Tunnel Settings (Ajouter les paramètres de tunnel d'agent)** > **Split Tunneling (Segmentation de tunnel)**.
   2. Configurez les paramètres de tunnel pour l'application GlobalProtect.
   3. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)** et sélectionnez une configuration de paramètres client existante ou en ajouter une nouvelle.

 ©2026 Palo Alto Networks, Inc.

4. Sélectionnez **Split Tunnel (Segmentation du tunnel)** et dans la section Inclure un domaine, ajoutez l'URL de votre fichier de configuration de la segmentation du tunnel comme première entrée dans la section Inclure un domaine.

   Seules les URL HTTPS sont supportées.



5. Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.

   Sur Strata Cloud Manager (NGFW), pour héberger un profil :

   1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Profiles (Profils)** > **Gateway Agent Profiles (Profil de l'agent de passerelle)**.
   2. Cliquez sur **Add Profile (Ajouter un profil)**.
   3. Dans la page Ajouter un profil de l'agent de passerelle, sous la section Paramètres du tunnel d'agent, ajoutez des itinéraires d'accès.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect MIB support

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Les points de terminaison de Palo Alto Networks prennent en charge les bases d'informations de gestion standard et d'entreprise (MIB) qui vous permettent de surveiller l'état physique, les statistiques d'utilisation, les pièges et d'autres informations utiles sur les points de terminaison. La plupart des MIB utilisent des groupes d'objets pour décrire les caractéristiques du point de terminaison à l'aide du protocole SNMP (Simple Network Management Protocol). Vous devez charger ces MIB dans votre gestionnaire SNMP pour surveiller les objets (statistiques et pièges des terminaux) définis dans les MIB (pour plus de détails, consultez Utilisation d'un gestionnaire SNMP pour explorer les MIB et les objets).

Le PAN-COMMON-MIB - qui est inclus avec les MIB de l'entreprise - utilise le groupe d'objets panGlobalProtect. Le tableau suivant décrit les objets qui composent le groupe d'objets panGlobalProtect.

object	Description
panGPGWUtilizationPct	Utilisation (en pourcentage) de la passerelle GlobalProtect
panGPGWUtilizationMaxTunnels	Nombre maximum de tunnels autorisés
panGPGWUtilizationActiveTunnels	Nombre de tunnels actifs

Utilisez ces objets SNMP pour surveiller l'utilisation des passerelles GlobalProtect et apporter des modifications au besoin. Par exemple, si le nombre de tunnels actifs atteint 80% ou est supérieur au nombre maximal de tunnels autorisés, vous devriez envisager d'ajouter des passerelles supplémentaires.

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

Portails GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Le portail GlobalProtect fournit les fonctions de gestion de votre infrastructure GlobalProtect. Chaque système client qui fait partie du réseau GlobalProtect reçoit des informations de configuration du portail, notamment des informations sur les passerelles disponibles et sur les certificats clients pouvant être requis pour se connecter aux passerelles. De plus, le portail contrôle le comportement et la distribution du logiciel de l'application GlobalProtect à la fois sur les terminaux Windows et MacOS.

> *Le portail ne distribue pas l'application GlobalProtect à utiliser sur les terminaux mobiles. Pour obtenir l'application GlobalProtect pour les terminaux mobiles, les utilisateurs finaux doivent la télécharger depuis le magasin du périphérique. App Store pour iOS, Google Play pour Android, Chrome Web Store pour Chromebooks, ou Microsoft Store pour Windows 10 UWP. Toutefois, les configurations de l'agent qui sont déployées pour les utilisateurs de l'App mobile contrôlent la ou les passerelles auxquelles les terminaux ont accès. Consultez* quels systèmes d'exploitation de terminal sont pris en charge sur chaque version de l'application GP.

En plus de distribuer le logiciel GlobalProtect, vous pouvez configurer le portail GlobalProtect pour fournir un accès distant sécurisé aux applications web d'entreprise courantes qui utilisent les technologies HTML, HTML5 et JavaScript à l'aide du VPN sans client GlobalProtect. Les utilisateurs ont l'avantage d'un accès sécurisé à partir de navigateurs Web sur lesquels SSL est activé sans installer le logiciel de l'application GlobalProtect. Cela est utile lorsque vous devez activer l'accès à ces applications pour des partenaires ou des entrepreneurs et pour activer de manière sécurisée les actifs non gérés, y compris les points de terminaison personnels.

Paramétrer l'accès au portail GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Configurez le portail GlobalProtect de la façon suivante :

1. Avant de commencer à configurer le portail, assurez-vous d'avoir :

   Création des interfaces (et des zones) pour le pare-feu sur laquelle vous envisagez de configurer le portail.

   Configuration du certificat de serveur du portail, du certificat de serveur de passerelle, des profils de service SSL/TLS et, facultativement, de certains certificats clients à déployer pour les utilisateurs finaux afin d'activer les connexions SSL/TLS mutuelles avec les services GlobalProtect™.

   Définition des profils d'authentification et des profils de certificats que le portail peut utiliser pour authentifier les utilisateurs GlobalProtect.

   Configuration d'une passerelle GlobalProtect et comprendre Priorité de passerelle dans une configuration de passerelle multiple.

2. Ajoutez le portail.
   1. Pour ajouter un nouveau portail, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** et ajoutez des configurations de portail.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Portals (Portails)** puis **Add Portal (Ajouter un portail)**.
      - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**. Sélectionnez une configuration de portail existante que vous souhaitez modifier ou en **Add (Ajouter)** une nouvelle pour déployer sur les utilisateurs/groupes de test.
   2. Saisissez un **Name (Nom)** à donner au portail.

      Le nom de la passerelle ne peut contenir d'espaces et doit être unique pour chaque système virtuel.
   3. (Facultatif) Sélectionnez le système virtuel auquel ce portail appartient dans le champ **Location (Emplacement)**.

 ©2026 Palo Alto Networks, Inc.

3. Spécifiez les paramètres réseau pour permettre à l'application GlobalProtect de communiquer avec le portail.

Si vous n'avez pas encore créé d'interface réseau pour le portail, consultez la section Créer des interfaces et des zones pour GlobalProtect. Si vous n'avez pas encore créé de profil de service SSL/TLS pour le portail, consultez Déployer des certificats de serveur sur les composants GlobalProtect.

N'attachez pas de profil de gestion d'interface qui autorise HTTP, HTTPS, Telnet ou SSH sur l'interface où vous avez configuré un portail ou une passerelle GlobalProtect, car cela permet d'accéder à votre interface de gestion depuis Internet. Suivez les Meilleures pratiques pour sécuriser l'accès administratif afin de vous assurer que vous sécurisez l'accès administratif à vos pare-feu d'une manière qui empêchera la réussite des attaques.

1. Sélectionnez **General (Général)**.
2. Dans la section Network Settings (Paramètres réseau), sélectionnez une **Interface**.
3. Spécifiez le **IP Address Type (Type d'adresse IP)** et la **IP address (Adresse IP)** pour le service Web du portail :
   - L'adresse IP peut être de type **IPv4 Only (IPv4 uniquement)**, **IPv6 Only (IPv6 uniquement)** ou **IPv4 and IPv6 (IPv4 et IPv6)**. Utilisez **IPv4 and IPv6 (IPv4 et IPv6)** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps.
   - L'adresse IP doit être compatible avec le type d'adresse IP. Par exemple, `172.16.1.0` pour les adresses IPv4 ou `21DA:D3:0:2F3b` pour les adresses IPv6. Pour les configurations en double pile, saisissez une adresse IPv4 ainsi qu'une adresse IPv6.
4. Sélectionnez un **SSL/TLS Service Profile (profil de service SSL/TLS)**.

4. SélectionnezGeneral (Généralités) et configurez les paramètres de journal de décryptage.

Vous pouvez journaliser les communications TLS/SSL réussies et avortées et vous pouvez transférer les journaux de décryptage aux Collecteurs de journaux, aux autres périphériques de stockage et aux administrateurs spécifiques.

- Par défaut, le pare-feu ne journalise que les communications TLS avortées. Il est conseillé de journaliser les communications réussies également afin d'avoir une visibilité sur autant de trafic décrypté que les resources (ressources)l'autorisent (mais ne décryptent pas le trafic privé ou sensible; respectez les decryption best practices (bonnes pratiques du décryptage) et décryptez autant de trafic que possible).
- Si vous ne l'avez pas déjà fait, créez un Log Forwarding profile (profil de transfert des journaux) pour transférer les journaux de décryptage et indiquez le dans la configuration de la passerelle.

 ©2026 Palo Alto Networks, Inc.

- Si vous journalisez des communications TLS réussies en plus des communications TLS avortées, configurez un quota d'espace de stockage de journaux plus important pour les journaux de décryptage.
- Sur Panorama, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)** > **Log Storage (Stockage des journaux)**.
- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Portals (Portails)** > **Add Portal (Ajouter un portail)** > **Advanced Settings (Paramètres avancés)** > **Log Settings (Paramètres des journaux)**.

Le quota par défaut (attribution) est de un pour cent de la capacité de stockage des journaux du périphérique pour les journaux de décryptage et de un pour cent pour le résumé de décryptage général. Il n'y a pas d'attribution par défaut pour les résumés de décryptage horaires, quotidiens ou hebdomadaires. Configure Decryption Logging (Configurer la journalisation du décryptage) donne plus d'informations sur la façon d'attribuer un espace de journaux de pare-feu aux journaux de décryptage.

5. Sélectionnez des pages d'aide et de connexion personnalisées ou désactivez ces pages complètement. Reportez-vous à la section Personnaliser les pages d'accès, de bienvenue et d'aide du Portail GlobalProtect pour obtenir de plus amples précisions sur la création d'une page d'aide et d'une page de connexion personnalisées.

Utilisez l'une des plateformes pour configurer les pages de connexion et d'aide personnalisées :

- Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **Response Pages (Pages de réponse)**.
- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Portals (Portails)** > **Add Portal (Ajouter un portail)**. Sur la page Ajouter un portail, sous **Advanced Settings (Paramètres avancés)**, sélectionnez **Appearance (Apparence)**.
- Sur Panorama, sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.
  1. Sélectionnez **General (Général)**.
  2. Dans la section Appearance (Apparence), configurez l'un des paramètres suivants :
     - Pour établir la **Portal Login Page (Page de connexion au portail)** pour l'accès des utilisateurs au portail, sélectionnez la page de connexion **factory-default (par défaut de l'usine)**, **Import (Importez)** une page de connexion personnalisée ou **Disable (Désactivez)** l'accès à la page de connexion.
     - Pour établir la **App Help Page (Page d'aide de l'application)** dans le but de fournir de l'aide aux utilisateurs relativement à l'application GlobalProtect, sélectionnez la page d'aide **factory-default (par défaut de l'usine)**, **Import (Importez)** une page d'aide personnalisée ou sélectionnez **None (Aucune)** pour supprimer l'option **Help (Aide)** du menu des **Settings (Paramètres)** du panneau d'état de GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

6. Spécifiez comment le portail authentifie les utilisateurs.

- Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Identity Services (Services d'identité)** > **Authentication** > **Authentication Profiles (Profils d'authentification)** > **Add Profile (Ajouter un profil)**.
- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Profiles (Profils)** > **GP Authentication Profiles (Profil d'authentification GP)** > **Add Profil (Ajouter un profil)**.

1. Sur Panorama, sélectionnez **Authentication (Authentification)**.
2. Configurez n'importe lequel des paramètres d'authentification du portail suivants :

   Si vous n'avez pas encore créé de certificat de serveur pour le portail et émis des certificats de passerelle, consultez la section Déployer des certificats de serveur sur les composants GlobalProtect.

   - Pour sécuriser la communication entre la passerelle et l'application GlobalProtect, sélectionnez le **SSL/TLS Service Profile (profil de service SSL/TLS)** que vous avez configuré pour le portail.
   - Pour authentifier les utilisateurs en ayant recours à une base de données d'utilisateurs locaux ou un service d'authentification externe, tel que LDAP, Kerberos, TACACS +, SAML ou RADIUS (incluant le mot de passe à usage unique), définissez les configurations d'authentification client GlobalProtect.
   - Pour authentifier les utilisateurs par un certificat client ou une carte à puce intelligente/CAC, sélectionnez le **Certificate Profile (Profil de certificat)** correspondant. Vous devez prédéployer le certificat client ou Déployer des certificats clients spécifiques à l'utilisateur pour l'authentification au moyen du Simple Certificate Enrollment Protocol (Protocole de recrutement de certificat simple ; SCEP).
     - Si vous souhaitez exiger que les utilisateurs s'authentifient auprès du portail à l'aide de leurs informations d'identification d'utilisateur ET d'un certificat client, un **Certificate Profile (Profil de certificat)** et un Profil d'authentification sont tous deux requis.
     - Si vous souhaitez permettre aux utilisateurs de s'authentifier auprès du portail à l'aide de leurs informations d'identification d'utilisateur OU d'un certificat client et que vous sélectionnez un Profil d'authentification pour l'authentification des utilisateurs, le **Certificate Profile (Profil de certificat)** est alors facultatif.
     - Si vous souhaitez permettre aux utilisateurs de s'authentifier auprès du portail à l'aide de leurs informations d'identification d'utilisateur OU d'un certificat client et que vous ne sélectionnez pas de Authentication Profile (Profil d'authentification) pour l'authentification des utilisateurs, le **Certificate Profile (Profil de certificat)** est alors obligatoire.

 ©2026 Palo Alto Networks, Inc.

- Si vous ne configurez pas de Authentication Profile (Profil d'authentification) qui correspond à un système d'exploitation spécifique, le **Certificate Profile (Profil de certificat)** est alors obligatoire.

*Si vous autorisez les utilisateurs à s'authentifier au portail à l'aide des informations d'identification d'utilisateur OU d'un certificat client, sélectionnez un **Certificate Profile (Profil de certificat)** où le **Username Field (Champ Nom d'utilisateur)** est configuré en tant que **Subject (Sujet)** ou **Subject Alt (Sujet alt.)**.*

7. Définissez les données que l'application GlobalProtect collecte auprès des points de terminaison se connectant après que les utilisateurs s'authentifient avec succès au portail.

L'application GlobalProtect envoie ces données au portail pour les mettre en correspondance avec les critères de sélection que vous définissez pour la configuration de l'agent de chaque portail. Selon ces critères, le portail transmet une configuration d'agent spécifique aux applications GlobalProtect qui se connectent.

1. Sélectionnez **Portail Data Collection (Collecte de données auprès du portail)**.
2. Configurez n'importe lequel des paramètres de collecte de données suivants :
   - Si vous voulez que l'application GlobalProtect collecte les certificats machine auprès des points de terminaison se connectant, sélectionnez le **Certificate Profile (Profil de certificat)** qui spécifie les certificats machine que vous aimeriez collecter.
   - Si vous voulez que l'application GlobalProtect collecte les informations sur l'hôte personnalisées auprès des points de terminaison se connectant, définissez les données du registre ou de la plist suivants dans la section Custom Checks (Vérifications personnalisées) :
     - Pour collecter les données du registre auprès des points de terminaison Windows, sélectionnez **Windows**, puis **Add (Ajoutez)** la **Registry Key (Clé de registre)** et la **Registry Value (Valeur du registre)** correspondante.
     - Pour collecter les données du fichier plist auprès des points de terminaison macOS, sélectionnez **Mac**, puis **Ajoutez** la clé de la **Plist** et la **Valeur** correspondante.

   Si vous utilisez Strata Cloud Manager (NGFW) pour collecter des informations d'hôte personnalisées à partir des terminaux, alors :

   1. Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)**.
   2. Sur la page Ajouter des paramètres d'application de l'agent, sous **HIP Data Collection (Collecte de données HIP)** > **Afficher les options avancées (Show Advanced Options)**

 ©2026 Palo Alto Networks, Inc.

> **Vérifications personnalisées (Custom Checks)** puis modifiez les vérifications personnalisées.

3. Cliquez sur **Add (Ajouter)** pour ajouter Windows (Clé de registre), Mac (Plist) ou Linux (Liste des processus).

Si vous utilisez Strata Cloud Manager (Prisma Access) pour collecter des informations d'hôtes personnalisées à partir des terminaux, alors :

1. Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **<default>**.
2. Sur la page par défaut, sélectionnez **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Custom Checks (Vérifications personnalisées)** puis modifiez les vérifications personnalisées.
3. Cliquez sur **Add (Ajouter)** pour ajouter Windows (Clé de registre), Mac (Plist) ou Linux (Liste des processus).

8. Enregistrez la configuration du portail.
   1. Cliquez sur **OK** pour enregistrer les paramètres.
   2. **Validez** les modifications.

 ©2026 Palo Alto Networks, Inc.

Définir les configurations d'authentification client GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Chaque configuration d'authentification du client GlobalProtect spécifie les paramètres qui permettent à l'utilisateur de s'authentifier auprès du portail GlobalProtect. Vous pouvez personnaliser les paramètres pour chaque système d'exploitation ou vous pouvez configurer les paramètres à appliquer à tous les points de terminaison. Par exemple, vous pouvez configurer les utilisateurs Android pour utiliser l'authentification RADIUS et les utilisateurs Windows pour utiliser l'authentification LDAP. Vous pouvez également personnaliser l'authentification du client pour les utilisateurs qui accèdent au portail à partir d'un navigateur Web (pour télécharger l'application GlobalProtect) ou pour l'accès VPN (X-Auth) IPsec tiers à des passerelles GlobalProtect.

1. Paramétrer l'accès au portail GlobalProtect.
2. Spécifiez comment le portail authentifie les utilisateurs.

   Vous pouvez configurer le portail GlobalProtect pour authentifier les utilisateurs à l'aide d'une base de données utilisateur locale ou d'un service d'authentification externe, tel que LDAP, Kerberos, TACACS+, SAML ou RADIUS (y compris le mot de passe à usage unique). Si vous n'avez pas encore configuré les profils d'authentification et/ou les profils de certificat, reportez-vous à la section GlobalProtect User Authentification (Authentification de l'utilisateur GlobalProtect) pour obtenir les instructions.

   Utilisez l'une des actions suivantes :

   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Identity Services (Services d'identité)** > **Authentication** > **Authentication Profiles (Profils d'authentification)**. Sur la page Ajouter un profil d'authentification, ajoutez des informations d'authentification.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Profiles (Profils)** > **GP Authentication Profiles (Profil d'authentification GP)** > **Add Profil (Ajouter un profil)**. Sur la page Ajouter une authentification, ajoutez **Client Authentication (Authentification du client)**.
   - Sur Panorama, dans la boîte de dialogue Configuration des portails GlobalProtect (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > ***<portal-config>***), sélectionnez

 ©2026 Palo Alto Networks, Inc.

Authentication (Authentification) pour **Add (Ajouter)** une nouvelle configuration de **Client Authentication (Authentification du client)** qui comporte les paramètres suivants :

- Entrez un **Name (Nom)** pour identifier la configuration de l'authentification client.
- Spécifiez les points de terminaison auxquels vous souhaitez déployer cette configuration. Pour appliquer cette configuration à tous les points de terminaison, acceptez le **OS (Système d'exploitation)** par défaut, qui est défini sur **Any (N'importe lequel)**. Pour appliquer cette configuration aux points de terminaison exécutant un système d'exploitation spécifique, sélectionnez un **OS (système d'exploitation)** comme **Android**. Vous pouvez également appliquer cette configuration aux points de terminaison qui se connectent à un portail VPN sans client à partir d'un **Browser (Navigateur)** Web.
- Pour permettre aux utilisateurs de s'authentifier auprès du portail ou de la passerelle à l'aide de leurs informations d'identification d'utilisateur, sélectionnez un **Authentication Profile (Profil d'authentification)** ou ajoutez-en un.
  - Si vous souhaitez exiger que les utilisateurs s'authentifient auprès du portail ou de la passerelle à l'aide de leurs informations d'identification d'utilisateur ET d'un certificat client, le **Authentication Profile (Profil d'authentification)** et le Certificate Profile (Profil de certificat) sont tous deux requis.
  - Si vous souhaitez permettre aux utilisateurs de s'authentifier auprès du portail ou de la passerelle à l'aide de leurs informations d'identification d'utilisateur OU d'un certificat client et que vous sélectionnez un Profil de certificat pour l'authentification des utilisateurs, le **Authentication Profile (Profil d'authentification)** est alors facultatif.
  - Si vous souhaitez permettre aux utilisateurs de s'authentifier auprès du portail ou de la passerelle à l'aide de leurs informations d'identification d'utilisateur OU d'un certificat client et que vous ne sélectionnez pas de Profil de certificat pour l'authentification des utilisateurs (ou que vous définissez le **Certificate Profile [Profil de certificat]** sur **None [Aucun]**), un **Profil d'authentification** est alors requis.
- (Facultatif) Saisissez une **Username Label (Étiquette de nom d'utilisateur)** pour la connexion au portail GlobalProtect (par exemple, **Email Address (username@domain (Adresse électronique (nom_d'utilisateur@domaine))**.
- (Facultatif) Saisissez une **Password Label (Étiquette de mot de passe)** personnalisée pour la connexion au portail GlobalProtect (par exemple, un **Passcode (Code secret)** pour l'authentification basée sur jeton à deux facteurs).
- (Facultatif) Saisissez un **Authentication Message (Message d'authentification)** pour aider les utilisateurs finaux à comprendre les informations d'identification à utiliser lors de la connexion. Ce message peut comporter jusqu'à 256 caractères (par défaut, il s'agit de `Enter login credentials`).
- Sélectionnez l'une des options suivantes pour définir si les utilisateurs peuvent authentifier le portail à l'aide des identifiants de connexion et/ou des certificats clients :
  - Pour exiger que les utilisateurs s'authentifient au portail à l'aide des identifiants de connexion ET d'un certificat client, définissez l'option **Allow Authentication with User Credentials OR Client Certificate (Autoriser l'authentification à l'aide des informations d'identification des utilisateurs OU du certificat client)** sur **No (User Credentials AND Client Certificate Required) [Non (Les informations d'identification des utilisateurs ET le certificat client sont requis]** (par défaut).

 ©2026 Palo Alto Networks, Inc.

- Pour autoriser les utilisateurs s'authentifient au portail à l'aide des identifiants de connexion OU d'un certificat client, définissez l'option **Allow Authentication with User Credentials OR Client Certificate (Autoriser l'authentification à l'aide des informations d'identification des utilisateurs OU du certificat client)** sur **Yes (User Credentials OR Client Certificate Required) [Oui (Les informations d'identification des utilisateurs OU le certificat client sont requis]**.

  Lorsque vous définissez cette option sur **Yes (Oui)**, le portail GlobalProtect cherche d'abord si un certificat client se trouve sur le point de terminaison. Si le point de terminaison ne dispose pas d'un certificat client ou que vous ne configurez pas de profil de certificat pour votre configuration d'authentification client, l'utilisateur final doit ensuite s'authentifier auprès du portail à l'aide de ses informations d'identification d'utilisateur.

3. Organisez les configurations d'authentification du client avec des configurations spécifiques au système d'exploitation en haut de la liste et des configurations qui s'appliquent à **Any (n'importe quel)** système d'exploitation en bas de la liste (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > **<portal-config>** > **Authentication [Authentification]**). Comme avec l'évaluation des règles de sécurité, le portail recherche une correspondance en commençant par le début de la liste. Lorsqu'il trouve une correspondance, il fournit la configuration correspondante à l'application.

- Pour faire remonter une configuration de client dans la liste des configurations, sélectionnez la configuration et cliquez sur **Move Up (Remonter)**.
- Pour faire descendre une configuration de client dans la liste des configurations, sélectionnez la configuration et cliquez sur **Move Down (Descendre)**.

4. (Facultatif) Pour activer l'authentification à deux facteurs à l'aide d'un profil d'authentification et d'un profil de certificat, configurez les deux dans cette configuration du portail.

Le portail doit authentifier le point de terminaison en utilisant les deux méthodes avant que l'utilisateur puisse y avoir accès.

(Chrome uniquement) Si vous configurez le portail pour qu'il utilise les certificats clients et LDAP pour l'authentification à deux facteurs, les Chromebook qui exécutent Chrome 47 ou des versions ultérieures font face à des invites excessives pour sélectionner le certificat client. Pour empêcher les invites excessives, configurez une politique pour spécifier le certificat client dans la console Google Admin, puis déployez cette politique à vos Chromebook gérés :

1. *Connectez-vous à la console Google Admin, puis sélectionnez **Device management (Gestion de périphériques)** > **Chrome management (Gestion de Chrome)** > **User settings (Paramètres des utilisateurs)**.*
2. *Dans la section Client Certificates (Certificats clients), saisissez le modèle d'URL suivant sous **Automatically Select Client Certificate for These Sites (Sélectionner automatiquement un certificat client pour ces sites)** :*

   ```
   {"pattern": "https://[*.]","filter":{}}
   ```

3. *Cliquez sur **Save (Enregistrer)**. La console Google Admin déploie la politique à tous les périphériques en quelques minutes.*

À la boîte de dialogue Configuration des portails GlobalProtect (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > ***<portal-config>***), sélectionnez **Authentication**

 ©2026 Palo Alto Networks, Inc.

(Authentification) pour choisir le **Certificate Profile (Profil du certificat)** pour authentifier les utilisateurs en fonction d'un certificat client ou d'une carte à puce intelligente.

Le champ Nom commun (NC) et, le cas échéant, le champ Autre nom de l'objet (ANO) du certificat doivent correspondre exactement à l'adresse IP ou au nom de domaine complet (FQDN) de l'interface sur laquelle vous configurez le portail. Sinon, les connexions HTTPS au portail ne pourront pas être établies.

5. Enregistrez la configuration du portail.
   1. Cliquez sur **OK** pour enregistrer votre configuration.
   2. **Validez** les modifications.

 ©2026 Palo Alto Networks, Inc.

Définir les configurations de l'agent GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Une fois qu'un utilisateur GlobalProtect se connecte au portail et est authentifié par le portail GlobalProtect, le portail envoie la configuration d'agent à l'application, en fonction des paramètres que vous définissez. Si vous avez des rôles différents pour les utilisateurs ou les groupes nécessitant des configurations spécifiques, vous pouvez créer une configuration d'agent distincte pour chaque type d'utilisateur ou groupe d'utilisateurs. Le portail utilise l'OS du point de terminaison et le nom d'utilisateur ou de groupe pour déterminer la configuration de l'agent à déployer. Comme pour d'autres évaluations de règles de sécurité, le portail commence à rechercher une correspondance en haut de la liste. Lorsqu'il détecte une correspondance, le portail envoie la configuration à l'application.

La configuration peut inclure les éléments suivants :

- Une liste des passerelles auxquelles le point de terminaison peut se connecter.
- Parmi les passerelles externes, toute passerelle que l'utilisateur peut sélectionner manuellement pour la session.
- Le certificat AC racine requis pour activer l'application pour établir une connexion SSL avec les passerelles GlobalProtect.
- Le certificat racine AC pour le déchiffrement SSL en mode proxy direct.
- Le certificat client que le point de terminaison doit présenter à la passerelle lorsqu'il se connecte. Cette configuration n'est requise que si l'authentification mutuelle entre l'application et le portail ou la passerelle est requise.
- Un cookie crypté sécurisé que le point de terminaison doit présenter au portail ou à la passerelle lorsqu'il se connecte. Le cookie n'est inclus que si vous activez le portail pour en générer un.
- Les paramètres que l'agent utilise pour déterminer s'il est connecté au réseau local ou à un réseau externe.
- Le comportement de l'application, tel que ce que les utilisateurs finaux peuvent voir dans leur affichage, qu'ils puissent enregistrer leur mot de passe GlobalProtect, et s'ils sont invités à mettre à niveau leur logiciel.

  Si le portail est arrêté ou inaccessible, l'application utilise la version mise en cache de sa configuration client de sa dernière connexion au portail pour obtenir les paramètres, notamment les passerelles auxquelles se connecter, les certificats racines CA à utiliser pour établir une communication sécurisée avec les passerelles, et la méthode de connexion à utiliser.

Utilisez la procédure suivante pour créer une configuration client.

 ©2026 Palo Alto Networks, Inc.

1. Ajoutez un ou plusieurs certificats racines CA approuvés à la configuration de l'agent de portail pour permettre à l'application GlobalProtect de vérifier l'identité du portail et des passerelles.

   Le portail déploie le certificat dans un fichier de certificat lu uniquement par GlobalProtect.

   1. Pour ajouter un ou plusieurs certificats CA racine de confiance à la configuration de l'agent du portail, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **NGFW and Prisma Access (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Configuration** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)** > **Trusted Certificate Distribution (Distribution de certificats fiables)** > **Add Trusted Certificate Distribution (Ajouter une distribution de certificats fiables)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Portals (Portails)** puis . Sur la page Ajouter un portail, sélectionnez **Advanced Settings (Paramètres avancés)** > **Trusted Certificate Distribution (Distribution de certificats fiables)** et **Add (Ajouter)** une distribution de certificats fiables.
      - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
   2. Sélectionnez la configuration du portail à laquelle vous ajoutez la configuration de l'agent, puis sélectionnez l'onglet **Agent**.
   3. Dans le champ **Trusted Root CA (CA racine de confiance)**, cliquez sur **Add (Ajouter)**, et sélectionnez le certificat CA qui a été utilisé pour générer les certificats de serveur de passerelle et/ou de portail.

      L'interface Web présente une liste des certificats CA importés sur le pare-feu servant de portail GlobalProtect. L'interface Web exclut également les certificats d'entité finale, parfois appelés certificats feuille, de la liste des certificats que vous pouvez sélectionner. Vous pouvez aussi **Import (Importer)** un nouveau certificat CA.

      Utilisez les meilleures pratiques suivantes lors de la création et de l'ajout de certificats :

      - *Utilisez le même émetteur de certificat pour émettre des certificats pour toutes vos passerelles.*
      - *Ajoutez la chaîne de certificats complète (CA racine de confiance et certificats CA intermédiaires) à la configuration de l'agent de portail.*
   4. (Facultatif) Déployez des certificats CA supplémentaires à des fins autres que GlobalProtect (par exemple, déchiffrement proxy de transfert SSL).

      Cette option vous permet d'utiliser le portail pour déployer des certificats sur le point de terminaison et l'agent pour les installer dans le magasin de certificats racine local. Cela peut être utile si vous n'avez pas d'autre méthode pour distribuer ces certificats de serveur ou si vous préférez utiliser le portail pour la distribution de certificats.

      Pour le déchiffrement proxy de transfert SSL, vous indiquez le certificat de confiance de transfert que le pare-feu utilise (sur les points de terminaison Windows et MacOS

 ©2026 Palo Alto Networks, Inc.

uniquement) pour mettre fin à la connexion HTTPS, inspecter le trafic de conformité des stratégies et rétablir la connexion HTTPS pour transférer le trafic chiffré.

1. Ajoutez le certificat comme décrit dans l'étape précédente.
2. Activez l'option visant la **Install in Local Root Certificate Store (Installation dans la boutique des certificats racines locaux)**.

   Le portail envoie automatiquement le certificat lorsque l'utilisateur se connecte au portail et l'installe dans le magasin local du point de terminaison, éliminant ainsi la nécessité d'installer le certificat manuellement.

2. Ajoutez une configuration d'agent.

La configuration de l'agent spécifie les paramètres de configuration GlobalProtect à déployer sur les applications de connexion. Vous devez définir au moins une configuration agent. Vous pouvez ajouter jusqu'à 512 entrées de configuration d'agent pour chaque portail.

1. À partir de la configuration du portail (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > ***<portal-config>***), **Add (Ajouter)** une nouvelle configuration de l'agent.
2. Saisissez un **Name (Nom)** pour identifier la configuration d'agent. Si vous envisagez de créer plusieurs configurations, veillez à ce que le nom que vous définissez pour chaque configuration est suffisamment explicite pour permettre de les distinguer.

3. (Facultatif) Configurez les paramètres pour spécifier comment les utilisateurs ayant cette configuration s'authentifient au portail.

Si la passerelle authentifie les points de terminaison à l'aide d'un certificat client, vous devez sélectionner la source qui distribue le certificat.

Configurez n'importe lequel des paramètres d'**Authentication (Authentification)** suivants :

- Pour permettre aux utilisateurs de s'authentifier auprès du portail à l'aide de certificats clients, sélectionnez la source de **Client Certificate (certificat client)** (**SCEP**, **Local** ou **None (Aucun)**) qui distribue le certificat et sa clé privée à un point de terminaison. Si vous utilisez une autorité de certification interne pour distribuer les certificats aux points de terminaison, sélectionnez **None (Aucun)** (par défaut). Pour permettre au portail de générer et d'envoyer un certificat de machine à l'application pour le stockage dans le magasin de certificats local et utiliser le certificat pour l'authentification du portail et de la passerelle, sélectionnez **SCEP** et le profil SCEP associé. Ces certificats sont spécifiques au périphérique et ne peuvent être utilisés que sur le point de terminaison auquel il a été délivré. Pour utiliser le même certificat pour tous les points de terminaison, sélectionnez un certificat qui est **Local** sur le portail. Lorsque **None (Aucun)** est sélectionné, le portail ne transmet pas de certificat au point de terminaison, mais vous pouvez utiliser d'autres manières d'obtenir un certificat au point de terminaison.

  Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

  - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Identity Services (Services d'identité)** > **Authentication** > **Authentication Profiles (Profils d'authentification)** > **Add Profile (Ajouter un profil)**.
  - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All**

 ©2026 Palo Alto Networks, Inc.

Firewalls (Tous les pare-feu) > **Device (Périphérique)** > **GlobalProtect** > **Profiles (Profils)** > **GP Authentication Profiles (Profil d'authentification GP)** > **Add Profil (Ajouter un profil)**.

- Spécifiez s'il faut **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**. Sélectionnez **Oui** pour enregistrer le nom d'utilisateur et le mot de passe (par défaut), **Enregistrer uniquement le nom d'utilisateur** pour n'enregistrer que le nom d'utilisateur, **Uniquement avec l'empreinte digitale de l'utilisateur** pour enregistrer les données biométriques (empreinte digitale) de l'utilisateur ou, sur les terminaux iOS X uniquement, les identifiants Face ID. Vous pouvez également sélectionner **Non** pour ne jamais enregistrer les informations d'identification.

  *Lorsque vous réglez **Save User Credentials (enregistrer les informations d'identification de l'utilisateur)** sur **No (non)**, et si le portail et la passerelle sont configurés pour utiliser les mêmes méthodes d'authentification, l'application GlobalProtect peut authentifier vers la passerelle de façon transparente en utilisant les informations d'identification fournies par l'utilisateur pour s'authentifier sur le portail. L'utilisateur n'a pas besoin de saisir à nouveau ses informations d'identification pour s'authentifier sur la passerelle.*

  Si vous configurez le portail ou les passerelles pour demander un mot de passe dynamique tel qu'un mot de passe unique (ANP), l'utilisateur doit entrer un nouveau mot de passe à chaque connexion. Dans ce cas, l'application GlobalProtect ignore la sélection pour enregistrer à la fois le nom d'utilisateur et le mot de passe, s'il est spécifié, et enregistre uniquement le nom d'utilisateur. Pour plus d'informations, consultez Activer l'authentification à deux facteurs à l'aide de mots de passe uniques (OTP).

  Si vous optez pour que GlobalProtect **enregistre les identifiants de connexion de l'utilisateur Uniquement à partir de ses empreintes digitales**, GlobalProtect peut exploiter les fonctionnalités du système d'exploitation de l'application pour valider l'utilisateur avant d'autoriser l'authentification auprès de GlobalProtect. Les utilisateurs finaux doivent fournir une empreinte digitale qui correspond à un modèle d'empreinte digitale sur le terminal pour utiliser un mot de passe enregistré à des fins d'authentification auprès du portail et des passerelles GlobalProtect. Sur iOS X, GlobalProtect prend également en charge la reconnaissance faciale avec Face ID. GlobalProtect ne stocke pas le modèle d'empreinte digitale ou facial utilisé aux fins d'authentification, mais se fie aux fonctionnalités de numérisation du système d'exploitation pour déterminer la validité d'une correspondance.

4. Si le point de terminaison GlobalProtect ne requiert pas de connexions de tunnel lorsqu'il est sur le réseau interne, configurez la détection interne de l'hôte.
   1. Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal-config>*** > **Agent** > **Internal (Interne)**.

      Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **Internal Host Detection (Détection d'hôte interne)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent**

 ©2026 Palo Alto Networks, Inc.

Settings (Paramètres de l'agent) > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)** > **Internal Host Detection (Détection d'hôte interne)**.

2. Activez la **Internal Host Detection (Détection d'hôte interne)**(**IPv4** ou **IPv6**).
3. Saisissez l'**IP Address (Adresse IP)** d'un hôte qui peut être trouvé uniquement depuis le réseau interne. L'adresse IP que vous indiquez doit être compatible avec le type d'adresse IP (**IPv4** ou **IPv6**). Par exemple, 172.16.1.0 pour IPv4 ou 21DA:D3:0:2F3b pour IPv6.
4. Saisissez le **Hostname (Nom d'hôte)** DNS pour l'adresse IP que vous saisissez. Les points de terminaison qui essaient de se connecter à GlobalProtect tentent de faire une recherche DNS inversée sur l'adresse spécifiée. Si la recherche échoue, le point de terminaison détermine qu'il se trouve sur le réseau externe, puis déclenche une connexion tunnel à une passerelle sur sa liste de passerelles externes.
5. (Facultatif) Entrez une plage d'adresses source pour le terminaux. Lorsque les utilisateurs se connectent, GlobalProtect reconnaît l'adresse source du périphérique. Seules les applications GlobalProtect dont les adresses IP sont incluses dans le pool d'adresses source peuvent s'authentifier via la passerelle et envoyer des rapports HIP.

   Le sous-réseau IPv4 doit être /30 ou plus grand. Sinon, une plage d'IP spécifique doit être spécifiée. Par exemple, 192.168.1.0/30 ou 192.168.2.6-192.168.2.7

5. Configurez l'accès à un système tiers de gestion des points de terminaison mobiles.

Cette étape est nécessaire si les points de terminaison mobiles utilisant cette configuration seront gérés par un système de gestion de points de terminaison mobiles tiers. Tous les points de terminaisons se connectent initialement au portail et, si un système de gestion de points de terminaison mobiles tiers est configuré sur la configuration correspondante de l'agent du portail, le point de terminaison sera redirigé vers lui pour l'inscription.

1. Saisissez l'adresse IP ou le FQDN de l'interface d'archivage de point de terminaison associée à votre gestionnaire de points de terminaison mobiles. La valeur que vous saisissez ici doit correspondre exactement à la valeur du certificat de serveur associé à l'interface d'archivage de point de terminaison. Vous pouvez indiquer une adresse IPv6 ou IPv4.
2. Définissez le **Enrollment Port (Port d'inscription)** pour l'écoute des demandes de recrutement par le gestionnaire de points de terminaison mobiles. Cette valeur doit correspondre à la valeur définie sur le gestionnaire de sécurité mobile (par défaut = 443).

6. Spécifiez les critères de sélection de votre configuration de l'agent du portail.

Le portail utilise les critères de sélection que vous spécifiez pour déterminer la configuration qui doit être fournie aux applications GlobalProtect qui se connectent. Par conséquent, si vous avez plusieurs configurations, vous devez vous assurer de les commander conformément. Dès que le portail trouve une correspondance, il fournit la configuration. Ainsi, les configurations

 ©2026 Palo Alto Networks, Inc.

plus spécifiques doivent précéder les configurations plus générales. Reportez-vous à l'étape 12 pour obtenir des instructions sur le classement de la liste des configurations de l'agent.

Sélectionnez **Config Selection Criteria (Configuration des critères de sélection)**, puis configurez l'une des options suivantes :

- Pour spécifier l'utilisateur, le groupe d'utilisateurs et/ou le système d'exploitation auxquels cette configuration s'applique, sur Panorama, sélectionnez **User/User Group (Utilisateur/ Groupe d'utilisateurs)**, puis configurez l'une des options suivantes :

  Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

  1. Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs et groupes locaux)**.
  2. Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs et groupes locaux)**.
- Pour fournir cette configuration aux applications fonctionnant sur un système d'exploitation spécifique, **Add (Ajoutez)** le **OS (système d'exploitation)** (**Android**, **Chrome**, **iOS**, **Linux**, **Mac**, **Windows** ou **WindowsUWP**) auquel cette configuration s'applique et sélectionnez-le. Définissez le **OS (Système d'exploitation)** sur **Any (N'importe lequel)** pour déployer la configuration sur tous les systèmes d'exploitation.
- Pour restreindre cette configuration à un utilisateur ou à un groupe précis, **Add (Ajoutez)** le **User/User Group (Utilisateur/Groupe d'utilisateurs)** qui doit recevoir cette configuration et sélectionnez-le. Répétez cette étape pour chaque utilisateur/groupe que vous souhaitez ajouter. Pour restreindre la configuration aux utilisateurs qui ne sont pas encore connectés à leurs points de terminaison, sélectionnez **pre-logon (connexion pré-ouverte)** dans la liste déroulante **User/User Group (Utilisateur / groupe d'utilisateurs)**. Pour déployer la configuration à tout utilisateur, indépendamment de l'état de connexion, (à la fois à la connexion pré-ouverture de session et aux utilisateurs enregistrés), sélectionnez **any (chaque)**du menu déroulant **User/User Group (utilisateur/groupe d'utilisateur)**.

  Avant de pouvoir restreindre la configuration à des groupes spécifiques, vous devez mapper les utilisateurs à des groupes comme décrit dans Activer le mappage de groupe.
- Pour transmettre cette configuration aux applications en fonction d'attributs de périphériques spécifiques, sélectionnez **Device Checks (Vérifications du périphérique)**, puis configurez l'une des options suivantes :

  - Pour transmettre cette configuration en fonction de la présence du numéro de série du point de terminaison dans Active Directory ou Azure AD, sélectionnez une option dans la liste déroulante **Machine account exists with device serial number (Le compte machine existe avec le numéro de série du périphérique)**. Si vous définissez cette option sur **Yes (Oui)**, la configuration de l'agent s'applique uniquement aux points de terminaison pour lesquels un numéro de série existe (points de terminaison gérés). Si vous définissez cette option sur **No (Non)**, la configuration de l'agent s'applique uniquement aux points de terminaison pour lesquels aucun numéro de série existe (points de terminaison non gérés). Si vous définissez cette option sur **None (Aucun)**, la configuration n'est pas transmise aux applications en fonction de la présence du numéro de série du point de terminaison.

 ©2026 Palo Alto Networks, Inc.

- Pour transmettre cette configuration en fonction du certificat machine du point de terminaison, sélectionnez un **Certificate Profile (Profil de certificat)** à faire correspondre au certificat machine installé sur le point de terminaison.

  Les vérifications du périphérique sont prises en charge sur les systèmes d'exploitation Windows et Mac.

- Pour transmettre cette configuration aux applications en fonction des informations sur l'hôte personnalisées, sélectionnez **Custom Checks (Vérifications personnalisées)**, effectuez l'une des actions suivantes :

  Sur Strata Cloud Manager (NGFW) :

  1. Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)**.
  2. Sur la page Ajouter les paramètres de l'application de l'agent, sous **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Custom Checks (Vérifications personnalisées)**, modifiez les vérifications personnalisées.
  3. Cliquez sur **Add (Ajouter)** pour ajouter Windows (Clé de registre), Mac (Plist) ou Linux (Liste des processus).

  Sur Strata Cloud Manager (Prisma Access) :

  1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **<default>**.
  2. Sur la page par défaut, sélectionnez **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Custom Checks (Vérifications personnalisées)** et modifiez les vérifications personnalisées.
  3. Cliquez sur **Add (Ajouter)** pour ajouter Windows (Clé de registre), Mac (Plist) ou Linux (Liste des processus).

  Sur Panorama, activez **Custom Checks (Vérifications personnalisées)**, puis définissez les dates du registre ou de la plist suivantes :

  - Pour vérifier si les points de terminaison Windows possèdent une clé de registre spécifique, utilisez les étapes suivantes :

    1. **Add (Ajoutez)** une nouvelle clé de registre (**Custom Checks (Vérifications personnalisées)** > **Registry Key (Clé de registre)**).
    2. Lorsque vous êtes invité, entrez la **Registry Key (Clé de registre)** pour la mise en correspondance.
    3. (Facultatif) Pour transmettre cette configuration uniquement si le point de terminaison ne dispose pas de la clé de registre spécifiée ou de la valeur de la clé,

 ©2026 Palo Alto Networks, Inc.

sélectionnez l'option **Key does not exist or match the specified value data (La clé n'existe pas ou ne correspond pas aux données de la valeur définies)**.

4. (Facultatif) Pour transmettre cette configuration en fonction des valeurs du registre spécifiques, **Add (Ajoutez)** la **Registry Value (Valeur du registre)** et les **Value Data (Données de valeur)** correspondantes. Pour transmettre cette configuration uniquement aux points de terminaison qui n'ont pas de **Registry Value (Valeur du registre)** ou de **Value Data (Données de valeur)** spécifiées, sélectionnez **Negate (Refuser)**.

- Pour vérifier si les points de terminaison MacOS possèdent une entrés spécifique dans la plist, utilisez les étapes suivantes :

1. **Add (Ajoutez)** une nouvelle plist (**Custom Checks (Vérifications personnalisées)** > **Plist**).
2. Lorsque vous êtes invité à le faire, saisissez le nom de la **Plist**.
3. (Facultatif) Pour transmettre cette configuration uniquement s le point de terminaison ne dispose pas de la plist spécifiée, sélectionnez **Plist does not exist (La plist n'existe pas)**.
4. (Facultatif) Pour transmettre cette configuration en fonction de paires valeur-clé spécifiques dans la plist, cliquez sur **Add (Ajouter)**, puis saisissez la **Key (Clé)** et la **Value (Valeur)** correspondante. Pour la mise en correspondance uniquement des points de terminaison qui ne disposent pas de la clé ou de la valeur spécifiée, cochez la case **Negate (Ignorer)**

7. Spécifiez les passerelles externes auxquelles les utilisateurs possédant cette configuration peuvent se connecter.

Considérez les meilleures pratiques suivantes lorsque vous configurez les passerelles :

- *Si vous ajoutez des passerelles internes et externes à la même configuration, assurez-vous d'activer la **Internal Host Detection (Détection interne de l'hôte** (étape 4).*
- *Pour en savoir plus sur la façon dont l'application GlobalProtect détermine la passerelle vers laquelle il doit se connecter, voir la section* Priorité de la passerelle dans une configuration de passerelle multiple.

1. Ajoutez une passerelle interne ou externe, effectuez l'une des actions suivantes :
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **Gateways (Passerelles)** > **External Gateway (Passerelles externes)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)** > **Gateways (Passerelles)** > **External Gateway (Passerelles externes)**.
   - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal-config>*** > **Agent** > **External (Externe)**.

 ©2026 Palo Alto Networks, Inc.

2. **Add (Ajoutez)** les **External Gateways (Passerelles externes)** auxquelles les utilisateurs peuvent se connecter.
3. Donnez un **Name (Nom)** descriptif à la passerelle. Le nom que vous saisissez ici doit correspondre au nom que vous avez défini lorsque vous avez configuré la passerelle et doit être suffisamment descriptif pour que les utilisateurs sachent l'emplacement de la passerelle à laquelle ils sont connectés.
4. Saisissez le nom de domaine complet ou l'adresse IP de l'interface sur laquelle la passerelle est configurée dans le champ **Address (Adresse)**. Vous pouvez configurer une adresse IPv4 ou IPv6. L'adresse que vous spécifiez doit correspondre exactement au nom commun (NC) dans le certificat de serveur de passerelle.
5. **Add (Ajoutez)** une ou plusieurs **Source Regions (Régions sources)** pour la passerelle, ou sélectionnez **Any (Tout)** pour rendre la passerelle accessible à toutes les régions. Lorsque les utilisateurs se connectent, GlobalProtect reconnaît la région et permet aux utilisateurs de se connecter uniquement aux passerelles configurées pour cette région. En ce qui concerne les choix, la région source est considérée en premier, suivie par la passerelle.
6. Définissez la **Priority (Priorité)** de la passerelle en cliquant dans le champ et en sélectionnant l'une des valeurs suivantes :
   - Si vous avez une seule passerelle externe, vous pouvez laisser la valeur définie sur **Highest (La plus grande)** (valeur par défaut).
   - Si vous avez de multiples passerelles externes, vous pouvez modifier les valeurs de priorité (allant de **Highest (La plus grande)** à **Lowest (La plus basse)**) pour indiquer une préférence pour le groupe d'utilisateurs spécifique auquel cette configuration s'applique. Par exemple, si vous préférez que le groupe d'utilisateurs se connecte à une passerelle locale, vous devez définir la priorité à un niveau plus élevé que celui des passerelles plus éloignées géographiquement. La valeur de priorité est ensuite utilisée pour pondérer l'algorithme de sélection de passerelle de l'agent.
   - Si vous ne souhaitez pas que les applications établissent automatiquement des connexions avec la passerelle, sélectionnez **Manual only (Manuelle uniquement)**. Ce paramètre est utile pour tester les environnements.
7. Cochez la case **Manual (Manuelle)** pour autoriser les utilisateurs à passer manuellement sur la passerelle.

8. Spécifiez les passerelles internes auxquelles les utilisateurs possédant cette configuration peuvent se connecter.

   Veillez à ne pas utiliser l'option à la demande comme méthode de connexion si votre configuration inclut des passerelles internes.

   1. Ajoutez une passerelle interne ou externe, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **Gateways (Passerelles)** > **Internal Gateway (Passerelles internes)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)**

 ©2026 Palo Alto Networks, Inc.

> **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)** > **Gateways (Passerelles)** Activez **Passerelle interne (Passerelle interne)** et spécifiez les détails de la passerelle.

- Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal-config>*** > **Agent** > **Internal (Interne)**.

2. **Add (Ajoutez)** les **Internal Gateways (Passerelles internes)** auxquelles les utilisateurs peuvent se connecter.
3. Donnez un **Name (Nom)** descriptif à la passerelle. Le nom que vous saisissez ici doit correspondre au nom que vous avez défini lorsque vous avez configuré la passerelle et doit être suffisamment descriptif pour que les utilisateurs sachent l'emplacement de la passerelle à laquelle ils sont connectés.
4. Saisissez le nom de domaine complet ou l'adresse IP de l'interface sur laquelle la passerelle est configurée dans le champ **Address (Adresse)**. Vous pouvez configurer une adresse IPv4 ou IPv6. L'adresse que vous spécifiez doit correspondre exactement au nom commun (NC) dans le certificat de serveur de passerelle.
5. (Facultatif) **Add (Ajoutez)** une ou plusieurs **Source Addresses (Adresses sources)** à la configuration de la passerelle. L'adresse source peut être un sous-réseau IP, une plage ou une adresse prédéfinie. GlobalProtect prend en charge les adresses IPv6 et IPv4. Lorsque les utilisateurs se connectent, GlobalProtect reconnaît l'adresse source du point de terminaison et permet aux utilisateurs de se connecter uniquement aux passerelles configurées pour cette adresse.
6. Cliquez sur **OK** pour enregistrer vos modifications.
7. (Facultatif) **Add (Ajoutez)** un **DHCP Option 43 Code (Code d'option DHCP 43)** à la configuration de la passerelle. Vous pouvez inclure un ou plusieurs codes de sous-option associés aux informations spécifiques au fournisseur (option 43) que le serveur DHCP a été configuré pour offrir au client. Par exemple, vous pouvez avoir un code de sous-option 100 associé à une adresse IP 192.168.3.1.

   Lorsqu'un utilisateur se connecte, le portail GlobalProtect envoie la liste des codes d'option dans la configuration du portail à l'application GlobalProtect, et l'application sélectionne les passerelles indiquées par ces options.

   Lorsque l'adresse source et les options DHCP sont configurées, la liste des passerelles disponibles présentées au point de terminaison se base sur la combinaison (union) des deux configurations.

   Les options DHCP sont prises en charge uniquement sur les points de terminaison Windows et MacOS. Les options DHCP ne peuvent pas être utilisées pour sélectionner des passerelles utilisant l'adressage IPv6.
8. (Facultatif) Sur Panorama, sélectionnez **Internal Host Detection (Détection d'hôte interne)** pour permettre à l'application GlobalProtect de déterminer si elle est à l'intérieur du réseau d'entreprise. Lorsqu'un utilisateur tente de se connecter, l'application effectue une recherche DNS inversée du **Hostname (Nom d'hôte)** à l'**IP Address (Adresse IP)** spécifiée.

   Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée**

 ©2026 Palo Alto Networks, Inc.

de la configuration) > Prisma Access > GlobalProtect > Setup (Configuration) > GlobalProtect App (Application GlobalProtect) > App Settings (Paramètres de l'application) > Internal Host Detection (Détection d'hôte interne).

- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration > NGFW and Prisma Access (NGFW et Prisma Access) > Configuration Scope (Portée de la configuration) > All Firewalls (Tous les pare-feu) > Device (Périphérique) > GlobalProtect > Agent Settings (Paramètres de l'agent) > Add Agent App Settings (Ajouter les paramètres de l'application de l'agent) > Internal Host Detection (Détection d'hôte interne)**.

L'hôte sert de point de référence qui est accessible si le terminal est à l'intérieur du réseau d'entreprise. Si l'application trouve l'hôte, le point de terminaison est à l'intérieur du réseau et l'application se connecte à une passerelle interne ; si l'application ne parvient pas à trouver l'hôte interne, le point de terminaison est en dehors du réseau et l'application se connecte à l'une des passerelles extérieures.

Vous pouvez configurer un adressage **IPv4** ou **IPv6** pour **Internal Host Detection (Détection d'hôte interne)**. L'adresse IP que vous indiquez doit être compatible avec le type d'adresse IP. Par exemple, 172.16.1.0 pour IPv4 ou 21DA:D3:0:2F3b pour IPv6.

9. Personnalisez le comportement de l'application GlobalProtect pour les utilisateurs disposant de cette configuration.

Modifiez les paramètres de **App (l'application)** selon vos besoins. Pour plus d'informations sur chaque option, voir la section Personnaliser l'application GlobalProtect.

10. (Facultatif) Définissez toutes les données de profil d'informations personnalisées sur l'hôte (HIP) que l'application devra collecter et/ou exclure de la collecte.

Cette étape s'applique uniquement si vous envisagez d'utiliser la fonction HIP et qu'il existe des informations que vous souhaitez collecter qui ne peuvent pas être collectées en utilisant les objets HIP standard ou s'il existe des informations que vous ne souhaitez pas collecter. Pour plus d'informations sur la configuration et l'utilisation de la fonction HIP, reportez-vous à la section Informations de l'hôte.

Reportez-vous à la section Collecter des données d'application et de processus sur des points de terminaison *pour obtenir de plus amples informations sur la collecte des données HIP personnalisées.*

1. Sélectionnez **HIP Data Collection (Collecte de données HIP)**.
2. Activez l'option **Collect HIP Data (Collecter les données HIP)** sur l'application GlobalProtect.
3. Indiquez le **Max Wait Time (sec) (délai d'attente max (sec))** que l'application doit rechercher des données HIP avant de soumettre les données disponibles (plage comprise entre 10 et 60 secondes ; 20 secondes par défaut).
4. Sélectionnez le **Certificate Profile (Profil de certificat)** que le portail GlobalProtect utilise pour apparier le certificat de machine envoyé par l'application GlobalProtect.
5. Sélectionnez **Exclude Categories (exclure les catégories)** pour exclure les catégories spécifiques et/ou les vendeurs, les applications ou les versions dans une catégorie. Pour

 ©2026 Palo Alto Networks, Inc.

plus de détails, reportez-vous à la section Configurer l'application des stratégies basées sur HIP.

6. Sélectionnez **Custom Checks (Vérifications personnalisées)** pour définir toutes les données personnalisées que vous souhaitez collecter auprès des hôtes dotés de cette configuration de l'agent.

11. Enregistrez la configuration d'agent.

Cliquez sur **OK** pour enregistrer la configuration client.

12. Organisez les configurations de l'agent afin que la configuration adéquate soit déployée pour chaque application.

Dès qu'une application se connecte, le portail compare les informations sources dans le paquet aux configurations d'agent que vous avez définies. Comme avec l'évaluation des règles de sécurité, le portail recherche une correspondance en commençant par le début de la liste. Lorsqu'il trouve une correspondance, il fournit la configuration correspondante à l'application.

- Pour faire remonter une configuration de passerelle dans la liste de configurations, sélectionnez la configuration, puis cliquez sur **Move Up (Monter)**.
- Pour descendre une configuration de satellite dans la liste de configurations, sélectionnez la configuration, puis cliquez sur **Move Down (Déplacer vers le bas)**.

13. Enregistrez la configuration du portail.

1. Cliquez sur **OK** pour enregistrer la configuration de client.
2. **Validez** les modifications.

 ©2026 Palo Alto Networks, Inc.

Configurer la sélection intelligente du portail

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence pour utilisateurs mobiles de Prisma Access (à utiliser avec Prisma Access) Licence de passerelle GlobalProtect (à utiliser avec PAN-OS) Application GlobalProtect 6.3 et versions ultérieures Prise en charge du système d'exploitation : Windows et macOS Version du contenu : 8833-8679 et versions ultérieures

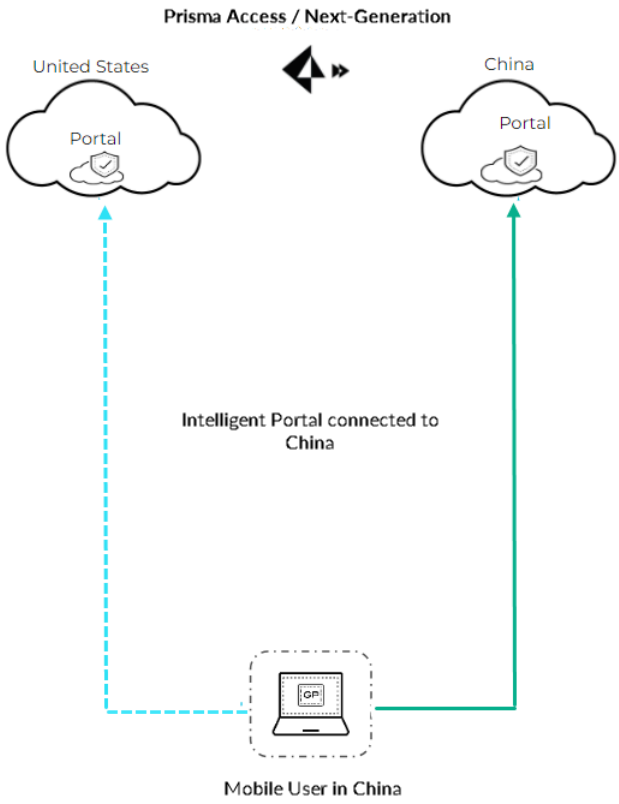
La fonctionnalité de sélection intelligente du portail permet la sélection automatique du portail approprié lorsqu'un utilisateur voyage à travers plusieurs pays pour une connectivité transparente et sécurisée. Après avoir configuré le portail intelligent dans votre environnement, vous êtes automatiquement acheminé vers le portail Prisma Access approprié en fonction de l'emplacement de votre pays. Par exemple, lorsque vous voyagez en Chine, vous êtes redirigé vers le portail Prisma Access Chine et vers le portail Amérique du Nord lorsque vous êtes aux États-Unis. Ce système élimine la nécessité de sélectionner manuellement les portails et améliore l'expérience utilisateur.

La fonctionnalité de portail intelligent est prise en charge pour les modes suivants.

- Toujours actif et Toujours actif (préouverture de session)
- Se connecter avant identification s'il n'y a pas de liste de portails supplémentaire pour Se connecter avant identification

Le portail intelligent n'est pas pris en charge pour Se connecter avant identification si une liste de portails est définie et pour le mode à la demande.

 ©2026 Palo Alto Networks, Inc.



Suivez les étapes ci-dessous pour configurer et utiliser la fonctionnalité de portail intelligent dans votre environnement.

1. Configurez le portail intelligent.

Environnement actuel	Étapes de déploiement
Nouvelle installation de GlobalProtect 6.3 et versions ultérieures sur Windows et macOS	Déployez GlobalProtect avec une option de ligne de commande pour ajouter la fonctionnalité de portail intelligent : msiexec.exe /i "GlobalProtect64.msi" PORTALCOUNTRYMAP="*portal1_address*(*country1_code*);p Par exemple, la commande suivante déploie GlobalProtect avec un portail intelligent et définit les portails pour les États-Unis et la Chine. Vous pouvez définir plusieurs portails pour un pays. `msiexec.exe /i "GlobalProtect64.msi" PORTALCOUNTRYMAP="xxx.com(US);yyy.com(CN)"`
Installation existante de GlobalProtect 6.3 et versions ultérieures pour Windows	Si GlobalProtect 6.3 ou versions ultérieures est déjà installé dans votre environnement, vous pouvez ajouter les

 ©2026 Palo Alto Networks, Inc.

Environnement actuel	Étapes de déploiement
	clés suivantes au Registre Windows (chemin HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\). • (Obligatoire) `REG ADD "HKLM \Software\Palo Alto Networks \GlobalProtect\Settings" /v portal-country-map /t REG_SZ /d` *portal_1* (*country1_code*);*portal_2* (*country2_code*) La carte du portail ne doit pas dépasser 255 caractères. • (Facultatif) `REG ADD "HKLM \Software\Palo Alto Networks \GlobalProtect\Settings" /v intelligent-portal /t REG_SZ /d yes` Cette entrée active la fonctionnalité de portail intelligent la première fois que l'utilisateur final se connecte à l'application GlobalProtect. • (Facultatif) `REG ADD "HKLM \Software\Palo Alto Networks \GlobalProtect\Settings" / v intelligent-portal-service /t REG_SZ /d "geoip.gpcloudservice.com/ getIPLocation"` Ajoutez cette entrée si vous souhaitez héberger le service API pour fournir l'emplacement de l'utilisateur.
Installation existante de GlobalProtect 6.3 et versions ultérieures pour macOS	Si GlobalProtect 6.3 ou versions ultérieures est déjà installé dans votre environnement, vous pouvez définir les entrées suivantes dans la plist MacOS. 1. Type `sudo vi / Library/Preferences/ com.paloaltonetworks.GlobalProtect.setting` 2. Accédez au dictionnaire `/Palo Alto Networks/GlobalProtect/Settings`. 3. Ajoutez les entrées suivantes. `<key>intelligent-portal</ key> <string>yes</ string> <key>portal-`

 ©2026 Palo Alto Networks, Inc.

Environnement actuel	Étapes de déploiement
	country-map</key> <string>*portal1_address*(*country1_code*); string> <key>intelligent- portal-service</key> <string>geoip.gpcloudservice.com/ getIPLocation</string>
Mise à niveau vers GlobalProtect 6.3 et versions ultérieures	Si vous désinstallez la version précédente de GlobalProtect et effectuez une nouvelle installation, suivez la nouvelle procédure d'installation décrite ci-dessus. Si vous mettez à niveau GlobalProtect via le portail, ajoutez les paramètres du portail intelligent au Registre Windows ou à la plist MacOS.

Pour plus d'informations sur les paramètres de l'application, consultez Paramètres d'application personnalisables.

2. Activez la fonctionnalité de portail intelligent sur le portail. Reportez-vous à l'étape 6 de la section Personnaliser l'application GlobalProtect.

   Vous devez activer le portail intelligent sur le portail même si vous avez défini la clé comme facultative `REG ADD "HKLM\Software\Palo Alto Networks\GlobalProtect \Settings" /v intelligent-portal /t REG_SZ /d yes` dans le Registre Windows ou la plist MacOS.

La section suivante décrit le fonctionnement du portail intelligent après sa configuration.

- Lorsque l'utilisateur final se connecte à l'application GlobalProtect, GlobalProtect sélectionne automatiquement le portail défini dans la carte des pays du portail pour cet emplacement. Si plusieurs portails sont définis pour un pays, GlobalProtect sélectionne le premier portail pour ce pays.
- Si l'utilisateur sélectionne manuellement un autre portail pour ce pays dans la carte du portail, GlobalProtect dirige l'utilisateur vers ce portail pour les sessions suivantes. Le portail est conservé lorsque l'application est actualisée ou que l'ordinateur se met en mode veille.
- Si l'utilisateur sélectionne manuellement un portail qui n'est pas défini dans la carte des pays, ce portail est conservé pour la session. Lorsque l'application GlobalProtect est actualisée ou que l'ordinateur sort du mode veille, GlobalProtect les dirige automatiquement vers le portail défini dans la carte des pays du portail pour cet emplacement. Si plusieurs portails sont définis pour ce portail, GlobalProtect sélectionne le premier portail pour ce pays.

Les journaux de la fonctionnalité de portail intelligent sont inclus dans le fichier `GlobalProtectLogs.tgz`. Consultez les lignes surlignées dans la capture d'écran ci-dessous.

 ©2026 Palo Alto Networks, Inc.

```
(P5424-T7364)Debug(5439): 04/23/24 09:52:26:295 PanIntelligentPortal: intelligent portal & always on portal
(P5424-T7364)Debug(5452): 04/23/24 09:52:26:295 PanIntelligentPortal: CountryMapKeyExists true ; Not ManualChangePortal true
(P5424-T7364)Debug(5457): 04/23/24 09:52:26:295 PanIntelligentPortal: Start Intelligent Portal
(P5424-T7364)Debug(2432): 04/23/24 09:52:26:295 pan_get_gp_user_agent szGpUserAgent ua is PAN GlobalProtect/6.3.0-5 (Microsoft Windows 10 Home , 64-bit).
(P5424-T3000)Debug(6269): 04/23/24 09:52:26:310 NotificationTimerThread: notification timer thread starts.
(P5424-T3000)Debug(6440): 04/23/24 09:52:26:310 NotificationTimerThread: wait (-1 ms) for notification timer event.
(P5424-T8792)Debug(6486): 04/23/24 09:52:26:310 CaptivePortalDetectionThread: captive portal detection thread starts.
(P5424-T8792)Debug(6706): 04/23/24 09:52:26:310 CaptivePortalDetectionThread: wait (-1 ms) for captive portal detection event.
(P5424-T7116)Debug(6887): 04/23/24 09:52:26:310 NetworkDiscoverThread: network discover thread starts.
(P5424-T7116)Debug(6900): 04/23/24 09:52:26:310 Start NetworkDiscoverThread
(P5424-T3012)Debug(7670): 04/23/24 09:52:26:310 HipReportThread: HipReportThread starts up.
(P5424-T3012)Debug(7696): 04/23/24 09:52:26:310 HipReportThread: wait for HIP report ready event.
(P5424-T620)Debug(7969): 04/23/24 09:52:26:310 NetworkConnectionMonitorThread: network connection monitor thread starts.
(P5424-T3500)Debug( 168): 04/23/24 09:52:26:310 Start HipCheckThread
```

Pour plus d'informations sur l'accès au fichier journal, reportez-vous à la section Afficher et collecter les journaux d'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Personnaliser l'application GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

La configuration de l'agent de portail vous permet de personnaliser la façon dont vos utilisateurs finaux interagissent avec les applications GlobalProtect installées sur leurs points de terminaison. Vous pouvez personnaliser l'affichage et le comportement de l'application et définir des paramètres d'application distincts pour les différentes configurations d'agent GlobalProtect que vous créez. Par exemple, vous pouvez spécifier les éléments suivants :

- Les menus et les affichages auxquels les utilisateurs peuvent accéder.
- Si les utilisateurs peuvent désinstaller ou désactiver l'application (méthode de pré-connexion de l'utilisateur uniquement).
- Si une page d'accueil doit être affichée dès l'ouverture de session. Dans vos configurations, vous pouvez aussi décider si l'utilisateur peut ignorer la page d'accueil ou non et personnaliser les pages Ouverture de session, Bienvenue et Aide de GlobalProtect pour orienter vos utilisateurs sur l'utilisation de GlobalProtect au sein de votre environnement.
- Si l'application GlobalProtect se met automatiquement à niveau ou si les utilisateurs sont invités à procéder manuellement à sa mise à niveau.
- S'il faut indiquer aux utilisateurs si une authentification multifacteur est nécessaire pour accéder aux ressources réseau sensibles.

Vous pouvez également définir les paramètres d'application dans le registre Windows, dans Windows Installer (Msiexec) et dans la plist MacOS globale. Les paramètres qui sont définis dans l'interface Web (configuration d'agent du portail) ont priorité sur les paramètres définis dans le registre Windows, dans Msiexec ou dans la Plist MacOS. Pour plus d'informations, consultez la séction Déployer les paramètres d'application de façon transparente.

> *Certains paramètres n'ont pas de paramètres de configuration de portail correspondants sur l'interface Web, et doivent être configurés à l'aide du Registre Windows, MsiExec ou de la plist macOS. Ces paramètres sont listés comme « Pas sur le portail ».*

Les paramètres supplémentaires qui ne sont disponibles que via le Registre Windows, Msiexec, ou plist macOS vous permettent de personnaliser des options y compris, mais sans s'y limiter, les suivantes :

- indiquer si l'application demande à l'utilisateur final les informations d'identification si le SSO de Windows échoue.
- indiquer l'adresse IP du portail par défaut (ou le nom d'hôte).
- autoriser GlobalProtect à initier une connexion avant que l'utilisateur ne se connecte au point de terminaison.

 ©2026 Palo Alto Networks, Inc.

- déployer des scripts qui s'exécutent avant ou après que GlobalProtect établisse une connexion ou après que GlobalProtect se déconnecte.
- Configurer l'application GlobalProtect pour qu'elle englobe des informations d'identification indépendantes sur les points de terminaison Windows, permettant ainsi l'ouverture de session unique lorsqu'un fournisseur d'informations d'identification indépendantes est utilisé.

1. Sélectionnez la configuration d'agent que vous souhaitez personnaliser.

   Vous pouvez également configurer la plupart des paramètres d'application dans le registre Windows, dans Windows Installer (Msiexec) et dans la plist macOS. Cependant, les paramètres qui sont définis dans l'interface Web ont priorité sur les paramètres définis dans le registre Windows, dans Msiexec ou dans la Plist MacOS. Reportez-vous à la section Déployer les paramètres d'application de façon transparente *pour plus de détails.*

   1. Pour personnaliser l'application GlobalProtect, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)** > **App Configuration (Configuration de l'application)**.
      - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
   2. Sélectionnez le portail sur lequel vous voulez ajouter la configuration d'agent ou **Add (Ajoutez)**-en un nouveau.
   3. À l'onglet **Agent (Agent)**, sélectionnez la configuration de l'agent que vous souhaitez modifier (ou **Add (ajoutez)**-en une nouvelle).
   4. Sélectionnez l'onglet **App (Applications)**.

      La zone configurations de l'App affiche les paramètres d'application avec les valeurs par défaut que vous pouvez personnaliser pour chaque configuration d'agent. Lorsque vous modifiez le comportement par défaut, la couleur du texte passe de gris à la couleur par défaut.

2. Spécifiez la **Connect Method (méthode de connexion)** qu'une application utilise pour sa connexion GlobalProtect.

   Utilisez la méthode de connexion ***Pre-logon (Always On) (Pré-ouverture de session (Toujours activée))***, ***Pre-logon then On-demand (Pré-ouverture de session puis À la demande)***, *ou* ***Connexion-utilisateur (Toujours Activée)*** *pour accéder au réseau en utilisant une passerelle interne.*

   Dans la zone App Configurations (Configurations de l'app), sélectionnez l'une des options de **Connect Method (Méthode de connexion)** suivantes :

   - **User-logon (Always On) (Connexion utilisateur (Toujours activée))** : l'application GlobalProtect se connecte automatiquement au portail dès que l'utilisateur se connecte au point de terminaison (ou au domaine). Lorsqu'elle est utilisée en association avec l'ouverture

 ©2026 Palo Alto Networks, Inc.

de session unique (points de terminaison Windows uniquement), l'ouverture de session sur GlobalProtect est transparente pour l'utilisateur final.

Sur les points de terminaison iOS, ce paramètre empêche les applications de mot de passe à usage unique (OTP) de fonctionner, car GlobalProtect force tout le trafic à traverser le tunnel.

- **Pre-logon (Always On) (Pré-ouverture de session (Toujours activée))** : l'application GlobalProtect authentifie l'utilisateur et établit un tunnel VPN vers la passerelle GlobalProtect avant que l'utilisateur ne se connecte au point de terminaison. Cette option requiert que vous utilisiez une solution PKI externe pour pré-déployer un certificat de machine à chaque point de terminaison qui reçoit cette configuration. Voir VPN d'accès distant avec pré-connexion pour plus de détails sur la connexion préalable.
- **On-demand (Manual user initiated connection) (À la demande (connexion manuelle initiale de l'utilisateur))** : les utilisateurs doivent lancer manuellement l'application pour se connecter à GlobalProtect. Utilisez cette méthode de connexion pour les passerelles externes uniquement.
- **Pre-logon then On-demand (Pré-ouverture de session puis à la demande)** - Semblable à la méthode de connexion **Pre-logon (Always On) (pré-connexion (toujours activée))**, cette méthode de connexion (qui nécessite la version de version de contenu 590-3397 ou ultérieure) permet à l'application GlobalProtect d'authentifier l'utilisateur et d'établir un tunnel VPN à la passerelle GlobalProtect avant que l'utilisateur ne se connecte au point de terminaison. Contrairement à la méthode de connexion avant ouverture de session, une fois que l'utilisateur se connecte au point de terminaison, les utilisateurs doivent lancer manuellement l'application pour se connecter à GlobalProtect si la connexion est terminée pour une raison quelconque. L'avantage de cette option est que vous pouvez permettre aux utilisateurs de spécifier un nouveau mot de passe après expiration du mot de passe ou s'ils oublient leur mot de passe, mais que l'on exige toujours des utilisateurs d'initier manuellement la connexion après qu'ils se connectent.
- **Conditional Connect Method Based on Network Type (Using Windows Registry/macOS Plist) (Méthode de connexion conditionnelle basée sur le type de réseau [Utilisation du Registre Windows/plist macOS])** : en utilisant le Registre Windows/plist macOS, vous pouvez changer dynamiquement la méthode de connexion de **Always-On (Toujours actif)** à **On-demand (À la demande)** et vice versa en fonction du type de réseau (interne ou externe) auquel l'utilisateur final est connecté. Pour utiliser cette fonctionnalité, vous devez activer la détection des hôtes internes et définir la méthode de connexion pour les terminaux sur À la demande.

3. (Windows 10, Windows 10 basé sur ARM64, macOS 11 et versions ultérieures, et macOS 11 et versions ultérieures basé sur ARM ; version de contenu 8450-6909 ou ultérieure ; Nécessite l'application GlobalProtect 6.0) Configurez l'application de la politique de trafic

 ©2026 Palo Alto Networks, Inc.

des terminaux pour bloquer les connexions entrantes malveillantes à l'aide de l'adaptateur physique sur le terminal distant.

En appliquant la politique de trafic du point de terminaison sur le point de terminaison GlobalProtect, vous pouvez exécuter les fonctions suivantes :

- Bloquez les connexions entrantes malveillantes en dehors du tunnel VPN pour vous protéger contre l'exfiltration de données.
- Empêchez les applications de contourner le tunnel GlobalProtect en liant leurs connexions directement à l'adaptateur physique sur le point de terminaison distant.
- Empêchez les utilisateurs finaux de falsifier la table de routage pour contourner le tunnel GlobalProtect.

Lorsqu'il est utilisé en conjonction avec l'option**No direct access to local network (Pas d'accès direct au réseau local)**, vous pouvez également contrôler l'accès au réseau local. Par défaut, l'application de la stratégie de trafic du point de terminaison est désactivée.

Dans la zone **App Configurations (Configurations de l'application)**, sélectionnez l'une des options de **Endpoint Traffic Policy Enforcement (application de la stratégie de trafic des points de terminaison)** suivantes :

- **No (Non)** : spécifie que la fonctionnalité d'application de la stratégie de trafic des points de terminaison est désactivée et que cette fonctionnalité n'est pas appliquée. Ceci est l'option par défaut.
- **TCP/UDP Traffic Based on Tunnel IP Address Type (Trafic TCP/UDP basé sur le type d'adresse IP du tunnel)** : active l'application de la stratégie de trafic des points de terminaison pour le trafic TCP/UDP. Cette fonctionnalité est activée pour le trafic en fonction du type d'adresse IP du tunnel. Si le tunnel est IPv4, cette fonctionnalité s'applique uniquement au trafic IPv4. Si le tunnel est IPv6, cette fonctionnalité s'applique uniquement au trafic IPv6.
- **All TCP/UDP Traffic (Tout le trafic TCP/UDP)** : active l'application de la politique de trafic des points de terminaison pour tout le trafic TCP/UDP, quel que soit le type d'adresse IP du tunnel. Si le type d'adresse IP du tunnel est IPv4, l'application de la stratégie de trafic du point de terminaison s'applique à tout le trafic TCP/UDP (IPv4 ou IPv6). Si le type d'adresse IP du tunnel est IPv6, l'application de la stratégie de trafic du point de terminaison s'applique à tout le trafic TCP/UDP (IPv4 ou IPv6).
- **All Traffic (Tout le trafic)** : active l'application de la politique de trafic des points de terminaison pour tous les protocoles TCP, UDP, ICMP et tous les autres protocoles, quel que soit le type d'adresse IP du tunnel.

4. Spécifiez s'il faut appliquer les connexions GlobalProtect pour l'accès au réseau.

(Windows 10 uniquement) Lorsque **Enforce GlobalProtect Connection for Network Access (Appliquer la connexion GlobalProtect pour l'accès au réseau)** est activée, les types

 ©2026 Palo Alto Networks, Inc.

d'application suivants sont contournés et toutes les autres connexions sortantes et entrantes sont bloquées.

- L'agent GlobalProtect (**PanGPA.exe**), le service GlobalProtect (**PanGPS.exe**), et le service sous-système de l'autorité de sécurité locale (**lsass.exe**) se lancent
- Protocoles DHCP, DNS, NetBIOS (Network Basic Input/Output System), et Link-Local Multicast Name Resolution (LLMNR)
- Trafic d'interface en boucle

(macOS only (macOS uniquement)) Lorsque **Enforce GlobalProtect Connection for Network Access (Appliquer la connexion GlobalProtect pour l'accès au réseau)** est activée, les types d'application suivants sont contournés et toutes les autres connexions sortantes et entrantes sont bloquées.

- L'application GlobalProtect et le service GlobalProtect (PanGPS) :
- Protocoles DHCP et DNS
- Trafic d'interface en boucle
- Processus `ocspd`, `syspolicyd`, `ntpd`, `apsd`, et `trustd`

*Pour appliquer GlobalProtect pour l'accès au réseau, nous vous recommandons d'activer cette fonctionnalité uniquement pour les utilisateurs qui se connectent en mode d'**User-logon (ouverture de session utilisateur)** ou de **Pre-logon (pré-connexion)**. Les utilisateurs qui se connectent en mode **On-demand (à la demande)** peuvent ne pas être en mesure d'établir une connexion dans les délais autorisés.*

Dans la zone configurations de l'app, configurez l'une des options suivantes :

- Pour forcer tout le trafic réseau à parcourir un tunnel GlobalProtect, définissez **Enforce GlobalProtect Connection for Network Access (appliquer la connexion GlobalProtect pour l'accès au réseau)** sur **Yes (Oui)**. Par défaut, GlobalProtect n'est pas requis pour l'accès au réseau, signifiant que les utilisateurs peuvent toujours accéder à Internet lorsque GlobalProtect est désactivé ou déconnecté. Pour fournir des instructions aux utilisateurs avant le blocage du trafic, configurez GlobalProtect pour qu'il **Displays Traffic Blocking Notification Message (Affiche un message de notification de blocage du trafic)** et spécifiez éventuellement le moment d'afficher le message (**Traffic Blocking Notification Delay (Retard de notification de blocage du trafic)**).

  *Quand **Enforce GlobalProtect Connection for Network Access (Appliquer la connexion GlobalProtect pour l'accès au réseau)** est activé, vous pouvez envisager de permettre aux utilisateurs de désactiver l'application GlobalProtect avec un mot de passe. La fonctionnalité **Enforce GlobalProtect Connection for Network Access (Appliquer la connexion GlobalProtect pour l'accès au réseau)** améliore la sécurité du réseau en exigeant une connexion GlobalProtect pour l'accès au réseau. En de rares occasions, les points de terminaison peuvent ne pas se connecter au VPN et nécessiter une connexion administrative à distance pour le dépannage. En désactivant l'application GlobalProtect (pour Windows ou MacOS) en utilisant le mot de passe fourni par l'administrateur lors de la session de dépannage, vous pouvez autoriser les administrateurs à se connecter à distance à votre point de terminaison.*
- Configurez les exclusions de certaines adresses IP locales ou certains segments de réseau pour l'accès au réseau en saisissant ces adresses IP pour **autoriser le trafic vers les hôtes/réseaux spécifiés lorsque l'application de la connexion GlobalProtect pour l'accès au**

 ©2026 Palo Alto Networks, Inc.

réseau est activée et que la connexion à GlobalProtect n'est pas établie. Spécifiez un maximum de vingt adresses IP ou segments de réseau pour lesquels vous souhaitez autoriser l'accès lorsque vous appliquez GlobalProtect pour l'accès au réseau et que GlobalProtect ne peut établir de connexion.

Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.

*Si vous utilisez Connect Before Logon (Connexion avant authentification) en conjonction avec l'applicateur pour l'authentification par carte à puce ou l'authentification par nom d'utilisateur/mot de passe pour la connexion utilisateur à l'aide d'un service d'authentification tel que LDAP, RADIUS ou OTP, vous devez configurer des exclusions pour des adresses IP ou des segments de réseau spécifiques pour le portail et la passerelle en les saisissant sur **Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established (Autoriser le trafic vers le nom de domaine complet spécifié lorsque Enforce GlobalProtect Connection for Network Access est activé et que la connexion GlobalProtect n'est pas établie)**.*

En configurant des exclusions, vous pouvez améliorer l'expérience utilisateur en permettant aux utilisateurs d'accéder aux ressources locales lorsque GlobalProtect est déconnecté. Par exemple, lorsque GlobalProtect n'est pas connecté, GlobalProtect peut autoriser l'accès aux adresses locales de liaison. L'utilisateur peut ainsi accéder à un segment de réseau local ou à un domaine de diffusion.

- (Windows 10 et macOS utilisant macOS Catalina 10.15.4 ou une version ultérieure uniquement ; Nécessite GlobalProtect™ app 5.2 ou versions ultérieures) Configurez les exclusions pour des noms de domaine entièrement qualifiés spécifiques pour lesquels vous souhaitez autoriser l'accès lorsque vous appliquez les connexions GlobalProtectpour l'accès au réseau en saisissant ces noms de domaines entièrement qualifiés pour **Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established (Autoriser le trafic vers le FQDN indiqué lorsque Appliquer la connexion GlobalProtect pour l'accès au réseau est activé et que la connexion GlobalProtect n'est pas établie)**.

  Spécifiez un maximum de 40 noms de domaine entièrement qualifiés pour lesquels vous souhaitez autoriser l'accès lorsque vous appliquez les connexions GlobalProtect pour l'accès au réseau et que GlobalProtect ne peut établir de connexion.

  *Si vous utilisez Connect Before Logon (Connexion avant authentification) en conjonction avec l'applicateur pour l'authentification par carte à puce ou l'authentification par nom d'utilisateur/mot de passe pour la connexion utilisateur à l'aide d'un service d'authentification tel que LDAP, RADIUS ou OTP, vous devez configurer des exclusions pour des noms de domaine complètement qualifiés spécifiques pour le portail et la passerelle en les saisissant sur **Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established (Autoriser le trafic vers le nom de domaine complet spécifié lorsque Enforce GlobalProtect Connection for Network Access est activé et que la connexion GlobalProtect n'est pas établie)**.*

  Les noms de domaines entièrement qualifiés que vous fournissez ne sont utilisés que lorsque **Enforce GlobalProtect Connection for Network Access (Appliquer la connexion GlobalProtect à l'accès au réseau)** est réglé sur **Yes (Oui)**. Utilisez des virgules pour séparer plusieurs noms de domaine entièrement qualifiés (par exemple google.com,

 ©2026 Palo Alto Networks, Inc.

gmail.com). Utilisez le caractère de remplacement (*) pour les noms de domaine (par exemple, *.gmail.com). La longueur est de 1 024 caractères maximum.

Cette option nécessite la version de contenu 8284-6139 ou toute version ultérieure.

En configurant des exclusions FQDN, vous pouvez améliorer l'expérience utilisateur en permettant aux utilisateurs d'accéder aux ressources spécifiques lorsque GlobalProtect est déconnecté. Par exemple, le terminal peut communiquer avec un fournisseur d'identité hébergé sur le cloud (IdP) pour des besoins d'authentification ou avec un serveur de gestion de périphérique à distance même lorsque l'option Appliquer GlobalProtect pour l'accès au réseau est activée.

- Si vos utilisateurs doivent se connecter à un portail captif pour accéder à l'Internet, précisez un **Captive Portal Exception Timeout (sec) (Délai d'envoi d'une exception dans le portail captif (secondes))** pour indiquer la période de temps (en secondes) au cours de laquelle les utilisateurs peuvent se connecter au portail captif (la plage est comprise entre 0 et 3 600 secondes ; la valeur par défaut est de 0 seconde). Si les utilisateurs ne se connectent pas au cours de cette période, la page de connexion au portail captif expire et les utilisateurs ne peuvent pas utiliser le réseau.

  Pour que l'application GlobalProtect affiche un message de notification lorsqu'elle détecte un portail captif, définissez l'option **Display Captive Portal Detection Message (Afficher le message de détection du portail captif)** sur **Yes (Oui)**. Dans le champ **Captive Portal Notification Delay (sec) (Délai de notification du portail captif (secondes))**, saisissez la période de temps (en secondes) à l'issue de laquelle l'application GlobalProtect affiche ce message (la plage est comprise entre 0 et 120 secondes ; la valeur par défaut est de 5 secondes). GlobalProtect lance la minuterie après que le portail captif a été détecté, mais avant que l'Internet devienne accessible. Vous pouvez également fournir des instructions supplémentaires en configurant un **Captive Portal Detection Message (message de détection de portail captif)**.

  (Terminal Windows uniquement ; Nécessite la version GlobalProtect 6.2.8-c223 ou ultérieure ou 6.3.3 ou ultérieure et la version de contenu 8966-9398)

  Par défaut, GlobalProtect utilise le navigateur par défaut pour le portail captif. Avec le support du navigateur intégré pour le portail captif, GlobalProtect offre une expérience utilisateur améliorée et une sécurité renforcée comme expliqué dans les points suivants.

  - **Improved Security (Sécurité améliorée) :** L'option **Enforce GlobalProtect Connection for Network Access (Appliquer la connexion GlobalProtect pour l'accès au réseau.)** n'a plus besoin d'être désactivée lorsque le portail captif est détecté. Le trafic du portail captif du navigateur intégré est implicitement autorisé car un navigateur intégré est le propre processus de GlobalProtect. Pour le temps pendant lequel l'authentification du portail captif est complétée, seul le trafic du navigateur intégré GlobalProtect est autorisé (sauf pour les exceptions dans l'étape 4), ce qui entraîne une sécurité améliorée.

    Optimized Configuration (Configuration optimisée) : Vous n'avez pas besoin de définir des exceptions **Enforce GlobalProtect Connection for Network Access (Appliquer la connexion GlobalProtect pour l'accès au réseau.)** (basées sur l'IP ou basées sur le FQDN) pour le trafic lié au portail captif du navigateur intégré ou aux pages associées. Cela permet également d'économiser le nombre d'entrées (limitées) pour les exceptions **Enforce GlobalProtect Connection for Network Access (Appliquer la connexion GlobalProtect pour l'accès au réseau.)**.

 ©2026 Palo Alto Networks, Inc.

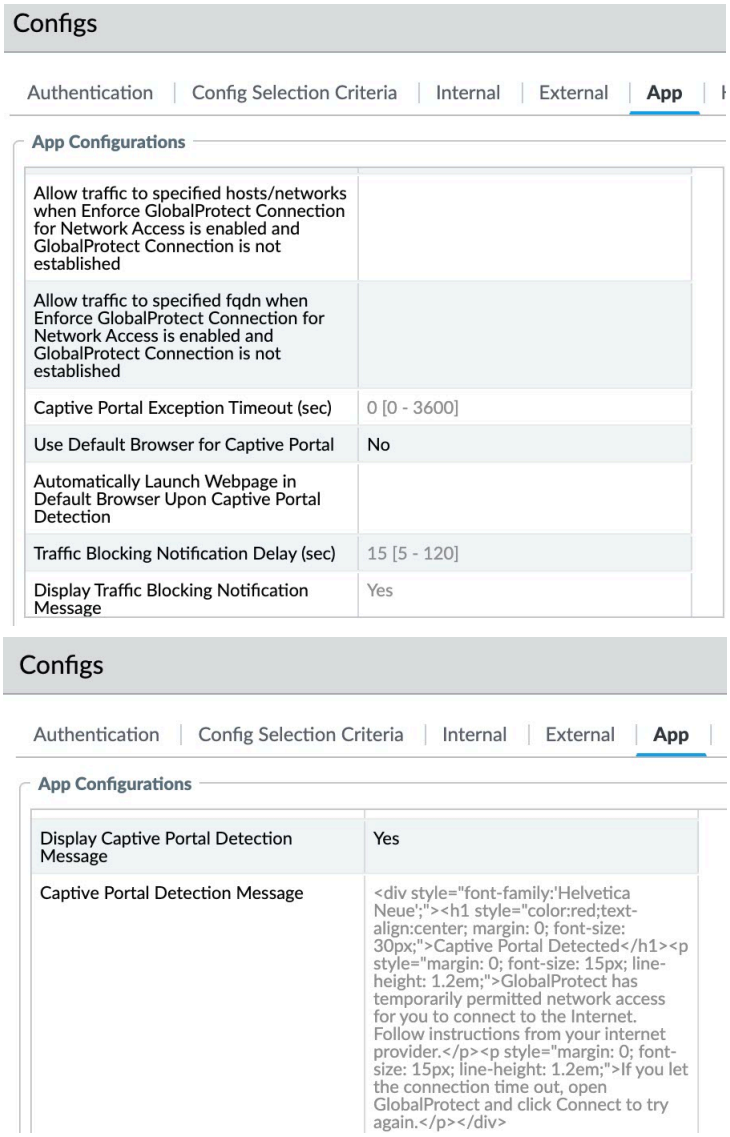
- **Meilleure expérience utilisateur :** Le navigateur intégré se lance en tant que fenêtre au premier plan, demandant immédiatement à l'utilisateur de s'authentifier contrairement à un navigateur par défaut qui pourrait ouvrir la page dans un nouvel onglet dans le navigateur. Lors de l'utilisation d'un navigateur intégré, il n'y a pas de souci concernant l'expiration du délai d'exception du portail captif et la nécessité de compléter l'authentification dans l'intervalle préconfiguré.

Pour utiliser le navigateur intégré GlobalProtect pour l'authentification du portail captif, vous devez :

1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**. Dans l'onglet Agent, sélectionnez la configuration de l'agent que vous souhaitez modifier. Sélectionnez l'onglet **App (Applications)**.
2. Définissez le **Use Default Browser for Captive Portal (Utiliser le navigateur par défaut pour le portail captif)** sur **No (Non)**. Vous pouvez également utiliser le paramètre de pré-déploiement `CPUSINGDEFBROWSER` pour ce paramètre. Pour plus d'informations, consultez Options de comportement de l'application.
3. Définissez **Display Captive Portal Detection Message (Afficher le message de détection du portail captif)** sur **Yes (Oui)**.

 ©2026 Palo Alto Networks, Inc.

4. Définissez **Captive Portal Exception Timeout (sec) (Expiration de l'exception du portail captif [sec])** sur **0**.



(Version GlobalProtect antérieure à 6.2.4 et 6.3.1) Pour lancer votre navigateur web par défaut, lorsqu'un portail captif est détecté, vous devez configurer ce qui suit :

- Dans le champ **Automatically Launch Webpage in Default Browser Upon Captive Portal Detection Lancer automatiquement la page web dans le navigateur par défaut lors de la détection du portail captif**, spécifiez l'URL avec le protocole défini : HTTP://<IP/FQDN>. Nous recommandons d'utiliser le protocole HTTP:// et une page HTTP pour éviter les

 ©2026 Palo Alto Networks, Inc.

invites de certificat non fiable et les problèmes avec les sites web utilisant la sécurité de transport strict HTTP (HSTS).

Si le champ est vide (par défaut), GlobalProtect ne lance pas automatiquement le navigateur Web par défaut lors de la détection du portail captif.

À partir des versions GlobalProtect 6.2.4 ou ultérieures et 6.3.1 ou ultérieures, spécifier l'URL n'est pas nécessaire pour lancer automatiquement le navigateur web lorsqu'un portail captif est détecté.

Ces options nécessitent la version 607-3486 ou toute version ultérieure. Le ***Délai de notification du portail captif*** *exige la version de contenu 8118-5277 ou toute version ultérieure. L'option* ***Lancer automatiquement la page Web dans le navigateur par défaut lors de la détection du portail captif*** *exige la version de contenu lancée le 8 juillet 2019 ou plus tard.*

5. Spécifiez des paramètres supplémentaires de connexion GlobalProtect .

   Lorsque l'ouverture de session unique est activée (par défaut), l'application GlobalProtect utilise les informations d'identification de connexion Windows de l'utilisateur pour s'authentifier et se connecter automatiquement au portail GlobalProtect et à la passerelle. Cela permet à GlobalProtect d'englober les informations d'identification indépendantes pour veiller à ce que les utilisateurs Windows puissent s'authentifier et se connecter même lorsqu'un fournisseur d'informations d'identification indépendantes est utilisé.

   Dans la zone configurations de l'app, configurez l'une des options suivantes :

   - (Windows et macOS uniquement ; la prise en charge de macOS exige la version de contenu 8196-5685 ou toute version ultérieure) Définissez **Utiliser l'ouverture de session unique (Windows)** ou **Utiliser l'ouverture de session unique (macOs)** sur **Non** pour désactiver l'ouverture de session unique.

     Si vous configurez la passerelle GlobalProtect pour qu'elle authentifie les utilisateurs au moyen de l'authentification SAML et pour qu'elle génère et accepte les cookies pour le contrôle prioritaire de l'authentification, vous devez définir l'option ***Use Single Sign-On (Utiliser l'ouverture de session unique)*** *sur* ***No (Non)*** *lorsque le nom d'utilisateur Windows de l'utilisateur diffère de son nom d'utilisateur SAML (par exemple, le nom d'utilisateur Windows est « user » et le nom d'utilisateur SMAL est « user123 ») ou si un nom d'utilisateur contient un nom de domaine complet (par exemple, le nom d'utilisateur Windows est « user » et le nom d'utilisateur SMAL est « user@example.com »).*

   - (Windows 10 uniquement ; version de contenu 8451-6911 ou ultérieure ; nécessite l'application GlobalProtect 6.0 ou ultérieure) Définissez **Use Single Sign-On for Smart Card PIN (Windows) (Utiliser l'authentification unique pour le code PIN de la carte à puce [Windows])** sur **Yes (Oui)** pour permettre à l'application GlobalProtect d'utiliser l'authentification unique pour le code PIN de la carte à puce. La valeur par défaut est **No (Non)**.

     Si vous avez configuré le portail GlobalProtect pour authentifier les utilisateurs finaux via l'authentification unique (SSO) à l'aide de l'authentification par carte à puce, les utilisateurs finaux peuvent se connecter sans avoir à ressaisir leur numéro d'identification personnel (PIN) de carte à puce dans l'application GlobalProtect pour une Expérience

 ©2026 Palo Alto Networks, Inc.

d'authentification unique. Les utilisateurs finaux peuvent utiliser le même code PIN de carte à puce pour GlobalProtect avec leur point de terminaison Windows. Cela améliore l'expérience utilisateur en réduisant le nombre de fois où les utilisateurs finaux doivent saisir le code PIN de leur carte à puce lorsqu'ils se connectent. Une fois que l'utilisateur final s'est connecté avec succès au point de terminaison Windows, l'application GlobalProtect acquiert et mémorise le code PIN de sa carte à puce pour s'authentifier auprès du portail et de la passerelle GlobalProtect.

Vous devez définir le pre-deployed setting (paramètre prédéployé) sur les points de terminaison de l'utilisateur final avant de pouvoir activer l'authentification unique pour le code PIN de la carte à puce. GlobalProtect récupère l'entrée du registre une seule fois : lors de l'initialisation de l'application GlobalProtect.

Si la valeur **USESSOPIN** est définie sur **yes (oui)** dans le paramètre prédéployé de l'ordinateur client et que l'option **Use Single Sign-On for Smart Card PIN (Windows) (Utiliser l'authentification unique pour le code PIN de la carte à puce (Windows))** est définie sur **no (non)** dans la configuration du portail, les utilisateurs finaux n'auront pas le meilleur utilisateur vivre. L'option **Use Single Sign-On for Smart Card PIN (Windows) (Utiliser l'authentification unique pour le code PIN de la carte à puce (Windows))** du portail GlobalProtect et le paramètre prédéployé sur la machine de l'utilisateur final doivent avoir la même valeur pour offrir la meilleure expérience utilisateur.

> *Si vous définissez les options**Use Single Sign-On (Windows) (Utiliser l'authentification unique (Windows))** et **Use Single Sign-On for Smart Card PIN (Windows) (Utiliser l'authentification unique pour le code PIN de la carte à puce (Windows))** sur **yes (oui)** dans la configuration du portail, l'option **Use Single Sign-On for Smart Card PIN (Windows) (Utiliser l'authentification unique pour le code PIN de la carte à puce (Windows))** est prioritaire sur l'option **Use Single Sign-On (Windows) (Utiliser l'authentification unique (Windows))**.*

- (Version de publication de contenu 8284-6139 version ultérieure ; nécessite GlobalProtect app 5.2 ou ultérieure) Réglez **Use Default Browser for SAML Authentication (Utiliser le navigateur par défaut pour l'authentification SAML)** sur **Yes (Oui)** pour que l'application GlobalProtect s'ouvre sur le navigateur du système par défaut pour l'authentification SAML. La valeur par défaut est **No (Non)**. L'application s'ouvrira dans le navigateur intégré.

  Si vous avez configuré le portail GlobalProtect pour authentifier les utilisateurs via l'authentification Security Assertion Markup Language (SAML), les utilisateurs finaux peuvent se connecter à l'application ou à d'autres applications activées par SAML sans avoir besoin de saisir à nouveau leurs informations d'identification, pour une expérience Single Sign-On (ouverture de session unique - SSO) sans problème. Vous pouvez activer l'application GlobalProtect afin que les utilisateurs finaux puisse exploiter la même connexion pour GlobalProtect et utiliser leur navigateur système par défaut pour l'authentification SAML comme Chrome, Firefox, ou Safari.
- Précisez la période de temps (en heures) pendant laquelle vous voulez que l'application GlobalProtect **Automatically Use SSL When IPSec Is Unreliable (Utilise automatiquement SSL lorsque IPSec est peu fiable)** (la plage est comprise entre 0 et 168 heures). Si vous configurez cette option, l'application GlobalProtect ne tente pas d'établir de tunnel IPSec

 ©2026 Palo Alto Networks, Inc.

au cours de la période de temps spécifiée. Ce minuteur est lancé chaque fois qu'un tunnel IPSec devient indisponible en raison d'un délai d'expiration keepalive du tunnel.

Si vous acceptez la valeur par défaut de **0**, l'application ne recommence pas à établir un tunnel SSL si elle peut établir un tunnel IPSec. Elle revient à l'établissement d'un tunnel SSL uniquement lorsque le tunnel IPSec ne peut être établi.

Cette option nécessite la version de contenu lancée le 8 juillet 2019 ou plus tard.

- (Version de contenu 8387-6595 ou ultérieure ; nécessite l'application GlobalProtect 5.2.6 ou ultérieure) Définissez **Display IPSec to SSL Fallback Notification (Afficher IPSec sur la notification de secours SSL)** sur **Yes (Oui)** pour permettre à l'application GlobalProtect d'afficher une notification de secours SSL uniquement lorsque GlobalProtect utilise de nouveau SSL après avoir tenté IPSec. Définissez **Display IPSec to SSL Fallback Notification (Afficher les notification de basculement d'IPSec vers SSl)** sur **No (Non)** pour empêcher l'application d'afficher la notification. Par défaut, cette option est définie sur **Yes (Oui)**. Si vous spécifiez la durée (en heures) pendant laquelle vous souhaitez que l'application GlobalProtect **Automatically Use SSL When IPSec Is Unreliable (utilise automatiquement SSL lorsque IPSec n'est pas fiable)**, par exemple 5 heures, l'application n'affichera pas cette notification pendant la période spécifiée car elle ne tentera pas de établissez un tunnel IPSec et établissez à la place un tunnel SSL.
- Choisissez les options de connexion SSL pour l'application GlobalProtect. Vous pouvez choisir d'appliquer les connexions SSL uniquement, d'interdire les connexions SSL ou d'autoriser l'utilisateur à choisir SSL ou IPSec (par défaut) selon l'emplacement géographique et les performances réseaux, et ce, afin d'offrir la meilleure expérience utilisateur qui soit.

  À la section configuration de l'application, choisissez les options **Se connecter au moyen de SSL uniquement** que vous souhaitez autoriser.

  Cette option nécessite la version de contenu 8207-5750 ou toute version ultérieure.

  - **Oui** : Cette option exige que tous les clients GlobalProtect se connectent à l'aide de SSL uniquement.
  - **Non** : Les clients se connectent à l'aide du protocole configuré sur la passerelle pour la connexion VPN. Si l'IPSec est activé dans la configuration de la passerelle, c'est alors IPSec qui sera utilisé pour la connexion VPN. Si SSL est activé dans la configuration de la passerelle, c'est alors SSL qui sera utilisé pour la connexion VPN.
  - **L'utilisateur peut procéder à la modification** : Cette option autorise l'utilisateur à opter pour SSL ou à conserver IPSec, sur l'application GlobalProtect.

    Sur l'application, l'utilisateur peut sélectionner **Settings (Paramètres)** > **General (Général)** pour activer **Connect with SSL Only (Se connecter au moyen de SSL uniquement)** et **Settings (Paramètres)** > **Connection (Connexion)** pour vérifier que le **Protocol (Protocol)** est défini sur **SSL**.

 ©2026 Palo Alto Networks, Inc.

- Choisissez le protocole de connexion réseau pour l'application GlobalProtect.

  Dans la zone de configuration de l'application, choisissez les options **Advanced Control for Tunnel Mode Behavior (Contrôle avancé du comportement en mode tunnel)** que vous souhaitez autoriser.

  Cette option nécessite l'application GlobalProtect 6.3 ou ultérieure.

  - **No (Non)** : les clients se connectent par défaut avec IPSec si IPSec est activé sur la passerelle et passent à SSL si IPSec n'est pas activé sur la passerelle. Il s'agit de la sélection par défaut.
  - **Connect with SSL Only (Se connecter au moyen de SSL uniquement)** : cette option exige que tous les clients GlobalProtect se connectent à l'aide de SSL uniquement.
  - **Connect with SSL Only - User can Change (Se connecter au moyen de SSL uniquement - L'utilisateur peut changer)** : les clients GlobalProtect se connectent en utilisant SSL mais l'utilisateur peut changer s'il souhaite utiliser IPSec ou rester avec SSL sur l'application GlobalProtect.

    Sur l'application, l'utilisateur peut naviguer sur **Settings (Paramètres)** > **Preferences (Préférences)** pour activer **Connect with SSL Only (Se connecter au moyen de SSL uniquement)** et **Settings (Paramètres)** > **Connection (Connexion)** pour vérifier que le **Protocol (Protocol)** est défini sur **SSL**.
  - Cette option est disponible avec la version de publication de contenu 8846-8732 ou ultérieure ; nécessite l'application GlobalProtect 6.3 ou ultérieure**IPSec uniquement** : exige que tous les clients GlobalProtect se connectent uniquement en utilisant IPSec. Si IPSec n'est pas activé sur la passerelle, GlobalProtect reste déconnecté et ne passera pas à SSL.

    Sur l'application, l'utilisateur peut sélectionner **Settings (Paramètres)** > **Connection (Connexion)** pour vérifier que le **Protocol (Protocole)** utilisé.

    Le tableau suivant décrit le comportement de mise à niveau pour cette fonctionnalité.

Option Connect with SSL Only (Se connecter au moyen de SSL uniquement) sélectionnée dans l'environnement pré-6.3	Option par défaut Advanced Control for Tunnel Mode Behavior (Contrôle avancé du comportement en mode tunnel) après la mise à niveau vers 6.3
Oui	SSL
Non	None

 ©2026 Palo Alto Networks, Inc.

Option Connect with SSL Only (Se connecter au moyen de SSL uniquement) sélectionnée dans l'environnement pré-6.3	Option par défaut Advanced Control for Tunnel Mode Behavior (Contrôle avancé du comportement en mode tunnel) après la mise à niveau vers 6.3
L'utilisateur peut changer	SSL – L'utilisateur peut changer

Le tableau suivant décrit le comportement de rétrogradation pour cette fonctionnalité.

Option Advanced Control for Tunnel Mode Behavior (Contrôle avancé du comportement en mode tunnel) sélectionnée dans l'environnement 6.3	Option par défaut Connect with SSL Only (Se connecter au moyen de SSL uniquement) après rétrogradation
None	Non
SSL	Oui
SSL – L'utilisateur peut changer	L'utilisateur peut changer
IPSec	3 L'utilisateur peut sélectionner manuellement l'option appropriée.

- (Version de contenu de publication 8346-6423 ou version ultérieure ; nécessite l'application GlobalProtect 5.2.4 ou version ultérieure) Saisissez la valeur de la**GlobalProtect Connection MTU (bytes) (MTU de connexion GlobalProtect [octets])** qui est utilisée par l'application pour les connexions à la passerelle. Vous pouvez indiquer une plage MTU de 1 000 à 1 420 octets au lieu de la valeur MTU défini par défaut de 1 400 octets. La valeur par défaut est 1400 octets.

  (Windows UWP only (Windows UWP uniquement)) Après avoir manuellement configuré la valeur **GlobalProtect Connection MTU (bytes) (MTU de connexion GlobalProtect (octets))** à l'aide de la commande **`netsh`**, le client GlobalProtect client n'est pas en mesure de régler la valeur**GlobalProtect Connection MTU (bytes) (MTU de connexion GlobalProtect (octets))** de la configuration du portail au-delà de la valeur configurée manuellement.

  > *Si la valeur MTU est inférieure à 1280 octets et que IPv6 est activé, l'adaptateur GlobalProtect modifie automatiquement la valeur sur 1280 octets selon le besoin en MTU minimum compatible pour IPv6.*

  Vous pouvez optimiser l'expérience de connexion pour les utilisateurs finaux se connectant par des réseaux qui nécessitent des valeurs d'unité de transmission maximale (MTU) inférieures à la norme de 1500 octets en configurant la valeur MTU qui est utilisée par l'application GlobalProtect pour se connecter à la passerelle. En réduisant la taille de MTU, vous pouvez éliminer les problèmes de performance et connectivité qui se produisent du fait de la fragmentation lorsque les connexions de tunnel VPN passent par plusieurs Internet Service Providers (fournisseur d'accès à Internet - ISP) et des chemins d'accès de réseau avec une MTU inférieure à 1500 octets. Par exemple, vous pouvez ajuster la valeur MTU pour un groupe spécifique d'utilisateurs d'une région sur une valeur MTU inférieure

 ©2026 Palo Alto Networks, Inc.

en utilisant une configuration de portail différente avec un besoin en valeur MTU inférieur. La valeur MTU que vous avez configurée pour un portail spécifique s'applique à toutes les connexions du tunnel de la passerelle figurant sur la liste pour ce portail pour les protocoles de tunnel IPSec et SSL.

*Dans les déploiements de pré-ouverture de session (toujours activé), GlobalProtect doit recréer le tunnel utilisateur pour que la nouvelle valeur MTU configurée dans la configuration du portail de l'utilisateur prenne effet. Ce déploiement nécessite que la valeur **Pre-logon Tunnel Rename Timeout (Délai de renommage du tunnel de pré-ouverture de session)** soit définie sur **0** dans la configuration du portail GlobalProtect.*

- Entrez les **Maximum Internal Gateway Connection Attempts (tentatives maximales de connexion de passerelle interne)** pour spécifier le nombre de fois où l'application GlobalProtect peut réessayer la connexion à une passerelle interne après la première tentative échouée (la plage est de 0 à 100; 4 ou 5 est recommandé; la valeur par défaut de 0 indique que l'application GlobalProtect ne réessaye pas la connexion). En augmentant cette valeur, vous pouvez permettre à l'application de se connecter à une passerelle interne qui est temporairement indisponible ou inaccessible, mais redevient disponible avant que le nombre spécifié de tentatives soit épuisé. L'augmentation de la valeur assure également que la passerelle interne reçoit les informations de l'utilisateur et de l'hôte les plus à jour.
- Entrez l' **GlobalProtect App Config Refresh Interval (Intervalle de rafraîchissement de configuration de l'application GlobalProtect)** pour spécifier le nombre d'heures que le portail GlobalProtect attend avant d'initialiser la prochaine actualisation de la configuration d'un client (la plage est de 1 à 168 ; la valeur par défaut est 24).
- (Windows uniquement) Selon vos exigences de sécurité, spécifiez si vous **Retain Connection on Smart Card Removal (Maintenez la connexion lors du retrait de la carte à puce intelligente)**. Par défaut, cette option est définie sur **Yes (Oui)**, ce qui signifie que GlobalProtect conserve le tunnel lorsqu'un utilisateur retire une carte à puce contenant un certificat client. Pour fermer le tunnel, réglez cette option sur **No (Non)**.

  Cette fonction requiert la version 590-3397 ou une version ultérieure.
- Configurez une **Automatic Restoration of VPN Connection Timeout (Délai d'expiration de la restauration automatique de la connexion VPN)** pour spécifier l'action que GlobalProtect prend lorsque le tunnel est déconnecté. Définissez cette option sur une valeur autre que zéro pour autoriser GlobalProtect à tenter de rétablir la connexion après la déconnexion du tunnel. Si le temps d'arrêt du tunnel dépasse la valeur de délai d'attente configurée (la plage est de 0 à 180 minutes ; la valeur par défaut est de 30), la restauration du tunnel ne sera pas effectuée et le résultat est le même que si vous définissez cette option sur **0**. Définissez cette option sur **0** pour empêcher GlobalProtect de tenter de rétablir la connexion après la déconnexion du tunnel. Si vous configurez le paramètre de connexion sur **Always-On (toujours activé)**, GlobalProtect effectuera à nouveau la découverte du réseau. Si vous configurez le paramètre de connexion sur **On-Demand (À la demande)**, l'utilisateur doit se reconnecter manuellement. Configurez le **Wait Time Between VPN Connection Restore Attempts (Délai d'attente entre les tentatives de restauration de la connexion VPN)** pour ajuster la durée de temps (en secondes) que GlobalProtect attend entre des tentatives de restaurer la connexion (plage entre 1 et 60 secondes ; la valeur par défaut est 5). Le client GlobalProtect essaie plusieurs fois de restaurer la connexion et utilise ce temps d'attente comme valeur de délai d'expiration de la connexion.

  Avec une méthode de connexion toujours activée, si un utilisateur passe d'un réseau externe à un réseau interne avant l'expiration du délai d'attente, GlobalProtect n'effectue

 ©2026 Palo Alto Networks, Inc.

*aucune détection de réseau. Par conséquent, GlobalProtect restaure la connexion à la dernière passerelle externe connue. Pour déclencher la détection d'hôte interne, l'utilisateur doit sélectionner **Refresh Connection (Actualiser la connexion)** dans le menu des paramètres qui se trouve dans le panneau d'état de GlobalProtect.*

6. Configurez les menus et les affichages de l'interface utilisateur qui sont disponibles pour les utilisateurs possédant cette configuration d'agent.

Dans la zone configurations de l'app, configurez l'une des options suivantes :

- Si vous souhaitez que les utilisateurs ne voient que les informations d'état de base dans l'application, définissez **Enable Advanced View (Activer la vue avancée)** sur **No (Non)**. Lorsque vous désactivez cette option, les utilisateurs peuvent voir des informations des onglets suivants :
  - **General (Général)** : affiche le nom d'utilisateur et le ou les portails associés au compte GlobalProtect.
  - **Notification** : affiche les notifications GlobalProtect.

  Le mode par défaut est**Yes (Oui)**. Lorsque vous activez cette option, les utilisateurs peuvent voir les onglets supplémentaires suivants :
  - **Connection (Connexion)** : liste les passerelles configurées pour l'application GlobalProtect et les informations sur chaque passerelle.
  - **Host Profile (Profil d'hôte)** : affiche les données sur les postes de travail que GlobalProtect utilise pour la surveillance et l'application des politiques de sécurité par l'intermédiaire du HIP.
  - **Résolution de problèmes** : affiche les informations concernant la configuration du réseau, les paramètres d'itinéraire, les connexions actives et les journaux. Vous pouvez également collecter les journaux générés par GlobalProtect et définir le niveau de journalisation.

    Pour que l'application GlobalProtect envoie des journaux de dépannage, des journaux de diagnostic ou les deux au Strata Logging Service pour une analyse plus approfondie, vous devez configurer le portail GlobalProtect pour activer la Collecte de journaux d'application GlobalProtect pour le dépannage. De plus, vous pouvez configurer les paramètres de collecte des journaux d'application sur le portail GlobalProtect. qui peut contenir des adresses IP ou des noms de domaine entièrement qualifiés des serveurs/web ressources que vous souhaitez interroger, et pour déterminer des problèmes tels que la latence ou la performance réseau sur le terminal de l'utilisateur final.
- Si vous souhaitez masquer l'icône de bac de système GlobalProtect sur les points de terminaison, définissez **Display GlobalProtect Icon (Afficher l'icône GlobalProtect** sur **No (Non)**. Lorsque l'icône est masquée, les utilisateurs ne peuvent pas effectuer de tâches telles que la modification des mots de passe enregistrés, la redécouverte du réseau, la remise des informations de l'hôte, l'affichage des informations de dépannage ou l'initiation de connexions à la demande. Cependant, les messages de notification HIP, les invitations de connexion et les dialogues de certificats continuent de s'afficher au besoin.
- Pour empêcher les utilisateurs d'effectuer une découverte du réseau, réglez l'**Enable Rediscover Network Option (Activer l'option d'activation de la redécouverte du réseau)** sur

 ©2026 Palo Alto Networks, Inc.

No (Non). Lorsque vous désactivez cette option, l'option d'**Actualisation de la connexion** est grisée dans le menu des paramètres du panneau de l'état de GlobalProtect.

- (Windows et macOS uniquement) Nécessite l'application GlobalProtect 6.4 ou ultérieure Pour activer la détection de transition réseau, définissez le paramètre **Enable GlobalProtect Discovery for Network Transition (Activer la découverte GlobalProtect pour la transition réseau)** sur oui. Lorsqu'il est activé, ce paramètre permet à GlobalProtect de détecter automatiquement les changements de réseau et de rétablir une connectivité optimale en supprimant le tunnel existant et en effectuant une découverte réseau pour les modes à la demande et toujours actif sur les réseaux internes et externes.

  Lorsqu'une nouvelle connexion réseau est détectée, GlobalProtect identifie de nouvelles adresses IP sur les interfaces réseau : celles commençant par « ethernet » sur les terminaux Windows et celles commençant par « en » sur les terminaux macOS. Lors de la détection, GlobalProtect met en œuvre un processus de stabilisation en deux phases : il attend 3 secondes pour la stabilisation du réseau, puis ignore les événements d'adresses IP supplémentaires pendant 5 secondes. Cette fenêtre de 8 secondes prend en compte les scénarios où plusieurs adresses (comme IPv4 et IPv6) sont attribuées simultanément lors de la connexion d'une connexion filaire, empêchant plusieurs cycles de découverte réseau inutiles.

  Ce paramètre est désactivé par défaut.
- Pour empêcher les utilisateurs de renvoyer manuellement les données HIP à la passerelle, définissez **Enable Resubmit Host Profile Option (Activer Réintroduire l'option de profil d'hôte)** sur **No (Non)**. Cette option, qui est activée par défaut, s'avère utile dans les cas où la politique de sécurité basée sur HIP empêche les utilisateurs d'accéder aux ressources, parce qu'elle autorise l'utilisateur à régler les problèmes liés à la conformité sur l'ordinateur afin de renvoyer les données HIP.
- (Windows et macOS uniquement) Nécessite l'application GlobalProtect 6.3 et la version de publication de contenu 8833-8679 ou ultérieure Pour permettre à GlobalProtect de diriger automatiquement les utilisateurs vers le portail Prisma Access approprié en fonction de leur emplacement, définissez **Enable Intelligent Portal Selection (Activer la sélection intelligente du portail)** sur **Yes (Oui)**. La valeur par défaut pour ce champ est **No (Non)**.
- (Windows uniquement) Pour permettre à GlobalProtect d'afficher des notifications dans le bac système, définissez **Show System Tray Notifications (Afficher les notifications de bac système)** sur **Yes (Oui)**.
- Pour créer un message personnalisé à afficher aux utilisateurs lorsque leurs mots de passe sont sur le point d'expirer, saisissez un **Custom Password Expiration Message (LDAP Authentication Only) (message d'expiration du mot de passe personnalisé (authentification LDAP uniquement))**. La longueur du message est de 200 caractères maximum.
- Pour créer un message personnalisé visant la définition des exigences ou des politiques en matière de mots de passe lorsque les utilisateurs modifient leur mot de passe Active Directory (répertoire actif ; AD), saisissez un **Change Password Message (Message de modification de mot de passe)**. La longueur du message est de 255 caractères maximum.

7. Définissez ce que les utilisateurs finaux avec cette configuration peuvent faire dans leur application.

- Réglez **Allow User to Change Portal Address (Autoriser l'utilisateur à modifier l'adresse du portail)** sur **No (Non)** pour désactiver le champ **Portal (Portail)** dans le panneau d'état

 ©2026 Palo Alto Networks, Inc.

de l'application GlobalProtect. Étant donné que l'utilisateur ne sera pas en mesure de spécifier un portail auquel se connecter, vous devez fournir l'adresse par défaut du portail dans le registre Windows (`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` avec la clé `Portal`) ou la plist MacOS (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist` avec la clé `Portal` sous le dictionnaire `PanSetup`). Pour plus d'informations, consultez la séction Déployer les paramètres d'application de façon transparente.

- Pour empêcher les utilisateurs de rejeter la page d'accueil, réglez **Allow User to Dismiss Welcome Page (autoriser l'utilisateur à renvoyer la page de bienvenue)** sur **No (Non)**. Lorsque cette option est réglée sur **Yes (Oui)**, l'utilisateur peut rejeter la page d'accueil et empêcher GlobalProtect d'afficher la page après les connexions ultérieures.
- Pour obliger l'utilisateur final à accepter les conditions d'utilisation afin de se conformer aux politiques de l'entreprise et pour afficher une page pour consulter les conditions d'utilisation de votre entreprise avant de se connecter à GlobalProtect, définissez **Have User Accept Terms of Use Before Creating Tunnel (Faire accepter les conditions d'utilisation par l'utilisateur avant de créer un tunnel)** sur **Yes (Oui)**. Lorsque cette option est définie sur **No (Non)**, l'utilisateur final n'est pas tenu d'accepter les conditions d'utilisation pour se conformer aux politiques de l'entreprise avant de se connecter à GlobalProtect.

8. Spécifiez si les utilisateurs peuvent désactiver l'application GlobalProtect.

L'option **Allow User to Disable GlobalProtect (autoriser l'utilisateur à désactiver GlobalProtect)** s'applique aux configurations d'agent disposant de la **Connect Method (Méthode de connexion) User-Logon (Always On) (ouverture de session utilisateur (Toujours activée))**. En mode de connexion utilisateur, l'application se connecte automatiquement dès que l'utilisateur se connecte au point de terminaison. Ce mode est parfois appelé «toujours activé», c'est pourquoi l'utilisateur doit remplacer ce comportement pour désactiver l'application GlobalProtect.

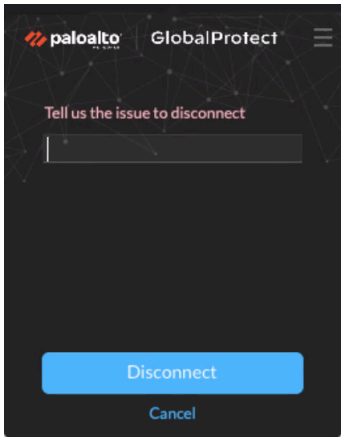
Par défaut, cette option est définie sur **Allow (Autoriser)**, ce qui permet aux utilisateurs de désactiver GlobalProtect sans fournir de commentaire, de code ou de numéro de ticket. Cependant,

Si l'icône du bac système GlobalProtect n'est pas visible, les utilisateurs ne peuvent pas désactiver l'application GlobalProtect. Pour plus d'informations, reportez-vous à l'étape 6.

- Pour éviter que les utilisateurs avec la méthode de connexion connexion-utilisateur ne désactivent GlobalProtect, réglez **Autoriser l'utilisateur à désactiver l'application GlobalProtect** sur **interdire**.
- Pour permettre aux utilisateurs de désactiver GlobalProtect uniquement s'ils doivent répondre à une ou plusieurs raisons telles que **Internet speed slow (vitesse Internet lente)** ou **App not working (application ne fonctionnant pas)** (si nécessaire). Les raisons de la déconnexion ne s'affichent que si vous configurez **Display the following reasons to disconnect GlobalProtect (Always-on mode) (Afficher les raisons suivantes pour déconnecter GlobalProtect (mode toujours activé))**. Si vous n'avez pas configuré

 ©2026 Palo Alto Networks, Inc.

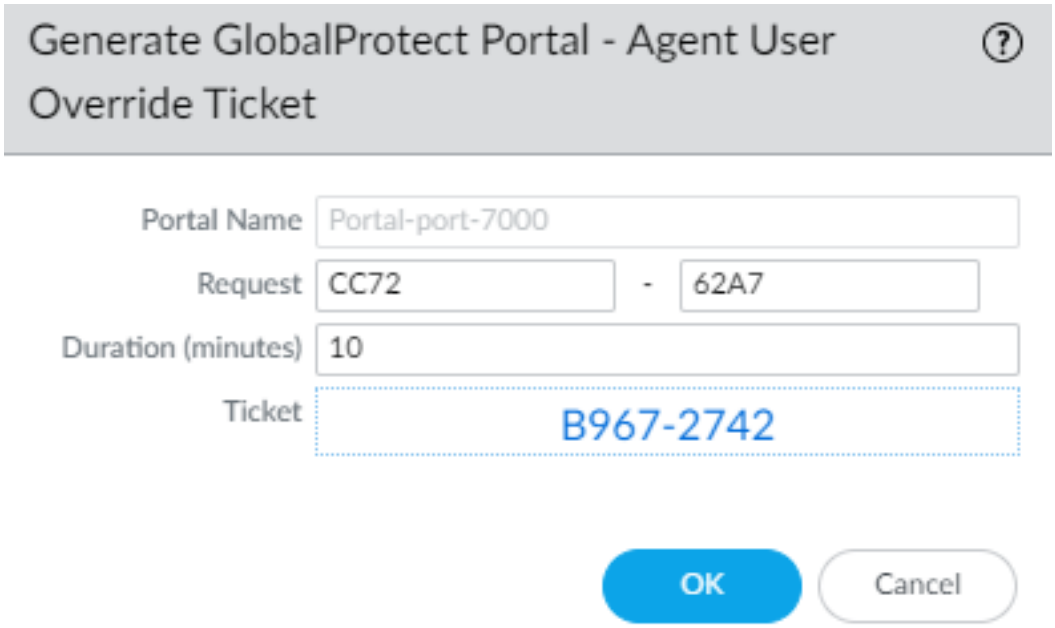
l'application GlobalProtect pour afficher les raisons de la déconnexion, les utilisateurs finaux sont invités à fournir une raison pour se déconnecter de l'application.



- Pour permettre aux utilisateurs finaux de fournir une raison de déconnexion, définissez **Allow User to Disable GlobalProtect App (Autoriser l'utilisateur à désactiver l'application GlobalProtect)** sur **Allow with Comment (Autoriser avec commentaire)**. Avec cette option, les utilisateurs finaux peuvent sélectionner **Other reason (Autre raison)** dans l'application GlobalProtect pour fournir une raison de déconnexion.
- Pour permettre aux utilisateurs de désactiver GlobalProtect uniquement s'ils fournissent un code d'authentification, définissez **Autoriser l'utilisateur à désactiver l'application GlobalProtect** sur **Autoriser avec le code**. Ensuite, dans la zone désactiver GlobalProtect App, entrez (et confirmez) le **Passcode (Code d'authentification)** que les utilisateurs finaux doivent fournir.
- Pour permettre aux utilisateurs de désactiver GlobalProtect uniquement s'ils fournissent un ticket, définissez **Allow User to Disable GlobalProtect (Autoriser l'utilisateur à désactiver GlobalProtect)** sur **Allow with Ticket (Autoriser avec un ticket)**. Avec cette option, l'action de désactivation pousse l'application à générer un numéro de requête, que l'utilisateur final doit fournir à l'administrateur. L'administrateur clique ensuite sur **Generate Ticket (Générer un ticket)** sur la page **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** et entre le numéro de demande de l'utilisateur pour générer le ticket. L'administrateur fournit le ticket

 ©2026 Palo Alto Networks, Inc.

à l'utilisateur final, qui le saisit dans la boîte de dialogue Désactiver GlobalProtect afin de désactiver l'application.



- Pour limiter le nombre de fois où les utilisateurs peuvent désactiver l'application GlobalProtect, précisez une valeur dans le champ **Max Times User Can Disable (Maximum de Fois où l'Utilisateur peut Désactiver)**, à la section Désactiver l'application GlobalProtect. Une valeur de 0 (par défaut) indique qu'il n'y a aucune limite quant au nombre de fois que les utilisateurs peuvent désactiver l'application.

  Ce paramètre n'est applicable qu'avec les options de désactivation ***Allow (Autoriser)***, ***Allow with Comment (Autoriser avec un commentaire)*** *et* ***Allow with Passcode (Autoriser avec un code secret)***.

  Si vous utilisateurs désactivent l'application GlobalProtect le nombre maximal de fois et qu'ils doivent continuer d'avoir la possibilité de désactiver l'application par la suite :

  - Vous pouvez accroître la valeur de **Max Times User Can Disable (Nombre max. de fois qu'un utilisateur peut désactiver)** dans la configuration de l'agent du portail GlobalProtect (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **App [Application]**). L'utilisateur doit ensuite **Refresh Connection (Actualiser la connexion)** à partir du menu des paramètres du panneau d'état GlobalProtect ou établir une nouvelle connexion GlobalProtect pour que la nouvelle valeur prenne effet.
  - Les utilisateurs peuvent réinitialiser le compteur en réinstallant l'application.
- Pour restreindre le nombre de fois que l'application peut être désactivée, saisissez une valeur de **Disable Timeout (min) (Délai d'expiration de désactivation (min.)** dans la zone Disable GlobalProtect App (Désactiver l'application GlobalProtect). Une valeur de 0 (par

 ©2026 Palo Alto Networks, Inc.

défaut) signifie qu'il n'y a aucune restriction quant à la durée pendant laquelle l'utilisateur peut garder l'application désactivée.

*Ce paramètre n'est applicable qu'avec les options de désactivation **Allow (Autoriser)**, **Allow with Comment (Autoriser avec un commentaire)** et **Allow with Passcode (Autoriser avec un code secret)**.*

9. Spécifiez si les utilisateurs peuvent désinstaller l'application GlobalProtect.

Utilisez l'option **Autoriser l'utilisateur à désinstaller l'application GlobalProtect** pour autoriser les utilisateurs à désinstaller l'application GlobalProtect, pour leur interdire de désinstaller l'application GlobalProtect ou pour les autoriser à la désinstaller spécifiquement au travers d'un mot de passe que vous créez.

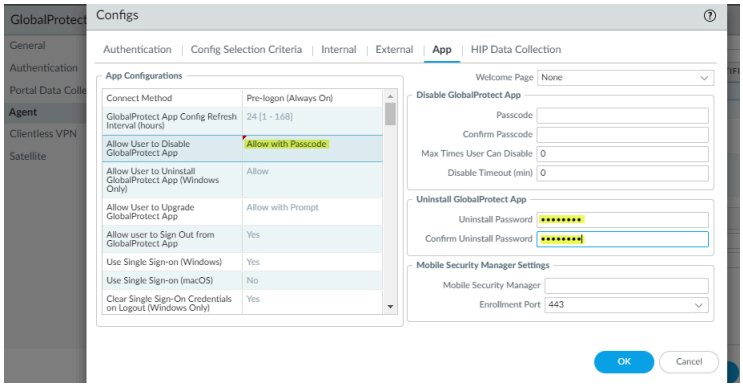
Ce paramètre est transmis au registre du terminal lors de sa première connexion au portail. Il est enregistré pour chaque portail auquel il se connecte.

Cette option nécessite la version de contenu 8207-5750 ou toute version ultérieure.

- Pour permettre aux utilisateurs de désinstaller l'application GlobalProtect sans aucune restriction, sélectionnez **Autoriser**.

  Lorsque vous activez **Allow (Autoriser)** dans le registre Windows, la valeur de ce portail est définie sur 0 sous `Computer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Palo Alto Networks\\GlobalProtect\\Settings\\<portal> 'Uninstall = 0'`.
- Pour empêcher les utilisateurs de désinstaller l'application GlobalProtect, sélectionnez **Interdire**.

  Lorsque vous activez **Interdire** dans le registre Windows, la valeur de ce portail est définie sur 1 sous `Computer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Palo Alto Networks\\GlobalProtect\\Settings\\<portal> 'Uninstall = 1'`.
- Pour permettre aux utilisateurs de désinstaller l'application GlobalProtect à l'aide d'un mot de passe, sélectionnez **Autoriser avec un code** ; puis, à la section Désinstaller l'application GlobalProtect, saisissez un **Mot de passe de désinstallation** et **Confirmez le mot de passe de désinstallation**.



10. Spécifiez si les utilisateurs peuvent se déconnecter de l'application GlobalProtect.

Dans la section configuration de l'application, définissez **Autoriser l'utilisateur à se déconnecter de l'application GlobalProtect** sur **Non** pour empêcher les utilisateurs de se

 ©2026 Palo Alto Networks, Inc.

déconnecter de l'application GlobalProtect ; définissez **Autoriser l'utilisateur à se déconnecter de l'application GlobalProtect** sur **Oui** pour les autoriser à le faire.

Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.

11. Configurez les paramètres de certificat et le comportement des utilisateurs qui reçoivent cette configuration.

Dans la zone configurations de l'app, configurez l'une des options suivantes :

- **Client Certificate Store Lookup (Vérification du magasin de certificat client)** : sélectionnez le magasin que l'application devrait utiliser pour rechercher les certificats clients. Les certificats d'**User (utilisateur)** sont stockés dans le magasin des certificats Current User sous Windows et dans le Personal Keychain sur macOS. Les certificats **Machine (machine)** sont stockés dans le magasin d'attestation de l'ordinateur local sous Windows et dans le System Keychain sur macOS. Par défaut, l'application recherche des certificats **User and machine (d'utilisateur et de machine)** dans les deux endroits.
- **SCEP Certificate Renewal Period (days) (Période de renouvellement du certificat SCEP (jours))** — avec SCEP, le portail peut demander un nouveau certificat client avant l'expiration du certificat. Cette période avant l'expiration du certificat est la *période de renouvellement du certificat SCEP optionnel*. Au cours d'un nombre de jours configurable avant l'expiration d'un certificat client, le portail peut demander un nouveau certificat à partir du serveur SCEP dans votre ICP (Infrastructure de clé publique) d'Enterprise (la plage est 0-30; par défaut est 7). Une valeur de 0 signifie que le portail ne renouvelle pas automatiquement le certificat du client quand il actualise une configuration de client.

  Pour que l'application GlobalProtect obtienne le nouveau certificat pendant la période de renouvellement, l'utilisateur doit se connecter à l'application. Par exemple, si un certificat de client a une durée de vie de 90 jours, la période de renouvellement du certificat est de 7 jours et l'utilisateur se connecte pendant les 7 derniers jours de la durée de validité du certificat, le portail acquiert un nouveau certificat et le déploie avec un nouveau produit de configuration de l'agent. Pour plus d'informations, consultez déployer des certificats clients spécifiques à l'utilisateur pour l'authentification.
- **Extended Key Usage OID for Client Certificate (OID d'utilisation de clé étendue pour le certificat client)** (Points de terminaison Windows et macOS uniquement) - Utilisez cette option uniquement si vous avez activé l'authentification client, attendez la présence de plusieurs certificats clients sur le point de terminaison et avez identifié un objectif secondaire par lequel vous pouvez filtrer les certificats clients. Cette option vous permet de spécifier un objectif secondaire pour un certificat client à l'aide de l'identificateur d'objet associé (OID). Par exemple, pour afficher uniquement les certificats clients ayant également un objectif d'authentification du serveur, entrez l'OID 1.3.6.1.5.5.7.3.1. Lorsque l'application GlobalProtect trouve un seul certificat client correspondant à l'objectif secondaire, GlobalProtect le sélectionne et s'authentifie automatiquement à l'aide de ce certificat. Sinon, GlobalProtect invite l'utilisateur à sélectionner le certificat client dans la liste des certificats clients filtrés correspondant aux critères. Pour plus d'informations, notamment une liste des objectifs de certificat communs et des OID, consultez la section Activer la sélection des certificats en fonction de l'OID.
- Si vous ne souhaitez pas que l'application établisse une connexion avec le portail lorsque le certificat du portail n'est pas valide, réglez **Allow User to Continue with Invalid Portal Server Certificate (autoriser l'utilisateur à continuer avec le certificat du serveur de portail non valide)** sur **No (Non)**. N'oubliez pas que le portail ne fournit que la configuration de

 ©2026 Palo Alto Networks, Inc.

l'agent ; il ne fournit pas d'accès au réseau. Par conséquent, la sécurité du portail est moins critique que la sécurité de la passerelle. Toutefois, si vous avez déployé un certificat de serveur de confiance pour le portail, décocher cette option peut aider à empêcher les attaques de l'homme du milieu (MITM).

12. Indiquez si les utilisateurs reçoivent des invites de connexion lorsqu'une authentification multifacteur est requise pour accéder aux ressources réseau sensibles.

Pour les connexions de passerelle interne, les ressources réseau sensibles (par exemple, les applications financières ou les applications de développement de logiciels) peuvent nécessiter une authentification supplémentaire. Vous pouvez Configurer GlobalProtect pour faciliter les notifications d'authentification multifacteur qui sont requises pour accéder à ces ressources.

Dans la zone configurations de l'app, configurez l'une des options suivantes :

- Définissez **Enable Inbound Authentication Prompts from MFA Gateways (Activer les invites d'authentification entrante des passerelles MFA)** sur **Yes (Oui)**. Pour prendre en charge la Multi-Factor Authentication (authentification multifacteur ; MFA), l'application GlobalProtect doit recevoir et reconnaître les invites UDP qui proviennent de la passerelle. Sélectionnez **Yes (Oui)** pour permettre aux applications GlobalProtect de recevoir et d'accepter l'invite. Par défaut, la valeur est définie sur **No (Non)**, ce qui signifie que GlobalProtect bloque les invites UDP de la passerelle.
- Précisez le **Network Port for Inbound Authentication Prompts (UDP) (Port réseau pour les invites d'authentification entrante (UDP))** que l'application GlobalProtect utilise pour recevoir les invites d'authentification entrante en provenance des passerelles MFA. Le port par défaut est 4501. Pour changer de port, indiquez un chiffre entre 1 et 65 535.
- Spécifiez les **Trusted MFA Gateways (Passerelles MFA de confiance)** auxquelles l'application GlobalProtect peut confiance pour l'authentification multifacteur. Lorsqu'une application GlobalProtect reçoit un message UDP sur le port réseau spécifié, GlobalProtect affiche un message d'authentification uniquement si l'invite UDP provient d'une passerelle de confiance.
- Configurez le **Message d'authentification entrant** ; (par exemple, `Vous avez tenté d'accéder à une ressource protégée qui nécessite une authentication supplémentaire. Procédez à l'authentification sur :.` Lorsque les utilisateurs tentent d'accéder à une ressource nécessitant une authentification supplémentaire, GlobalProtect reçoit un message d'authentification entrant et l'affiche. GlobalProtect ajoute automatiquement l'URL de la page du portail d'authentification que vous spécifiez lorsque vous configurez l'authentification multifacteur dans le message d'authentification entrante.

13. (Windows uniquement) Configurez les paramètres des points de terminaison Windows qui reçoivent cette configuration.

- **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only) (Résoudre tous les FQDN utilisant des serveurs DNS attribués par le tunnel) (Windows uniquement)** - Configurez les préférences de résolution DNS pour le tunnel GlobalProtect. Sélectionnez **No (Non)** pour permettre aux points de terminaison Windows d'envoyer les requêtes DNS au serveur DNS établi sur l'adaptateur physique si la requête initiale envoyée au serveur DNS configuré sur la passerelle n'est pas résolue. Cette option conserve le comportement natif de Windows pour interroger tous les serveurs DNS sur tous les adaptateurs de manière récursive, ce qui peut toutefois se traduire par de longues périodes d'attente pour

 ©2026 Palo Alto Networks, Inc.

résoudre certaines requêtes DNS. Sélectionner **Yes (Oui)** (par défaut) pour permettre aux points de terminaison Windows de résoudre toutes les requêtes DNS avec les serveurs DNS que vous configurez sur la passerelle au lieu de permettre au point de terminaison d'envoyer des requêtes DNS aux serveurs DNS définis sur la carte physique.

Cette fonctionnalité ne prend pas en charge DNS sur TCP.

- **Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Envoyer le rapport HIP immédiatement si les modifications d'état du Centre de sécurité Windows (WSC) changent)** : sélectionnez **No (Non)** pour empêcher l'application GlobalProtect d'envoyer des données HIP lorsque l'état du Centre de sécurité Windows (WSC) change. Sélectionnez **Yes (Oui)** (par défaut) pour envoyer immédiatement les données HIP lorsque le statut du WSC change.
- **Clear Single Sign-On Credentials on Logout (Effacer les informations d'authentification uniques à la déconnexion)** : sélectionnez **No (Non)** pour conserver les informations d'authentification uniques lorsque l'utilisateur se déconnecte. Sélectionnez **Yes (Oui)** (par défaut) pour les supprimer et forcer les utilisateurs à entrer leurs informations d'identification lors de la prochaine connexion.
- **Use Default Authentication on Kerberos Authentication Failure (Utilisez l'authentification par défaut en cas d'échec d'authentification Kerberos)** : sélectionnez **No (Non)** pour utiliser uniquement l'authentification Kerberos. Sélectionnez **Yes (Oui)** (par défaut) pour réessayer à l'aide de la méthode d'authentification par défaut après l'échec de l'authentification à l'aide de Kerberos.

14. (À partir de l'application GlobalProtect™ 6.1) Spécifiez **Proxy Auto-Configuration (PAC) File URL (URL du fichier PAC [Proxy d'auto-configuration])** que vous souhaitez envoyer au terminal pour configurer les paramètres de proxy via le portail GlobalProtect. Vous pouvez déployer différentes URL de PAC à différents terminaux en fonction du nom d'utilisateur ou de l'appartenance à un groupe. Une fois que le terminal a les paramètres de proxy, il utilise le serveur proxy pour accéder à Internet. La longueur maximale de l'URL est de 256 caractères. Les méthodes d'URL de fichier PAC (Proxy Auto-Configuration) suivantes sont prises en charge :

    - Norme PAC (Proxy Auto-Config) (par exemple, http://pac.<hostname or IP>/proxy.pac).
    - Norme WPAD (Web Proxy Auto-Discovery Protocol) (par exemple, http://wpad.<hostname or IP>/wpad.dat).

15. (Windows uniquement) Configurez l'application GlobalProtect pour les points de terminaison Windows pour qu'elle **Detect Proxy for Each Connection (Détecte le proxy pour chaque connexion)**.

    Pour obtenir plus d'informations sur le comportement du trafic réseau en fonction de l'utilisation d'un proxy, reportez-vous à la rubrique Connexions de tunnels via des proxys.

    - Sélectionnez **No (Non)** pour détecter automatiquement le proxy pour la connexion de portail et utiliser ce proxy pour les connexions ultérieures.
    - Sélectionnez **Yes (Oui)** (par défaut) pour détecter automatiquement le proxy à chaque connexion.

16. (Windows et macOS uniquement ; macOS pris en charge sur l'application GlobalProtect™ 6.3.3-h3 et ultérieure) Configurez l'application GlobalProtect pour les

 ©2026 Palo Alto Networks, Inc.

terminaux Windows pour **Detect Proxy for Each Connection (Détecter le proxy pour chaque connexion)**.

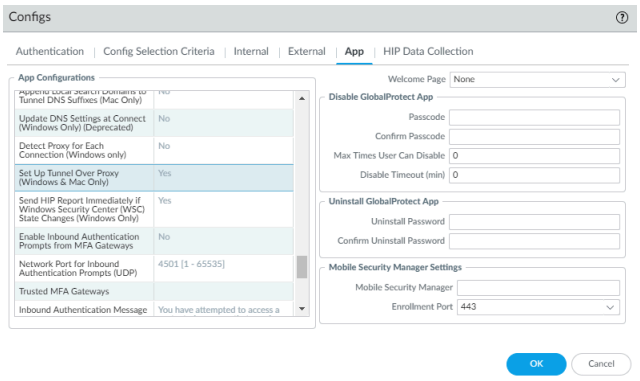
Pour obtenir plus d'informations sur le comportement du trafic réseau en fonction de l'utilisation d'un proxy, reportez-vous à la rubrique Connexions de tunnels via des proxys.

- Sélectionnez **No (Non)** pour détecter automatiquement le proxy pour la connexion de portail et utiliser ce proxy pour les connexions ultérieures.
- Sélectionnez **Yes (Oui)** (par défaut) pour détecter automatiquement le proxy à chaque connexion.

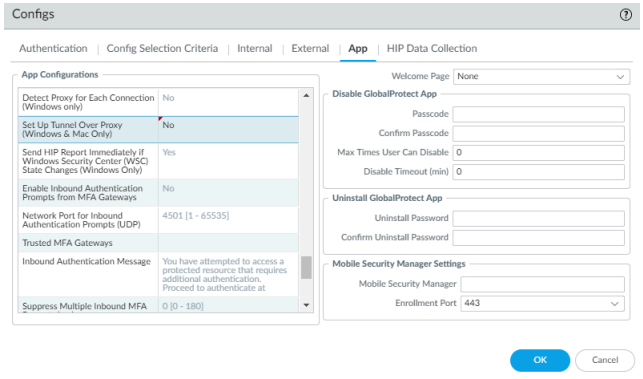
17. (Windows et macOS uniquement) Spécifiez si GlobalProtect doit utiliser les proxys ou les contourner.

Ce paramètre vous permet de configurer le comportement du trafic réseau en fonction de l'utilisation des proxys GlobalProtect. Pour plus d'informations, reportez-vous à la section Connexions de tunnel via des proxys.

- Pour forcer GlobalProtect à utiliser des proxys, définissez l'option **Set Up Tunnel Over Proxy (Windows & Mac only) [Configurer le tunnel sur le proxy (Windows et Mac uniquement)]** sur **Yes (Oui)**.



- Pour forcer GlobalProtect à contourner les proxys, définissez l'option **Set Up Tunnel Over Proxy (Windows & Mac only) [Configurer le tunnel sur le proxy (Windows et Mac uniquement)]** sur **No (Non)**.



18. (À partir de l'application GlobalProtect™ 6.1) Définissez **Enable Advance Host Detection (Activer la détection avancée des hôtes)** sur **Yes (Oui)** pour ajouter une couche de sécurité supplémentaire lors de la détection des hôtes internes par l'application. Avec la détection

 ©2026 Palo Alto Networks, Inc.

avancée de l'hôte interne, l'application valide le certificat de serveur des passerelles internes en plus d'effectuer une recherche DNS inversée de l'hôte interne pour déterminer si l'application se trouve à l'intérieur du réseau d'entreprise. Sélectionnez **No (Non)** (par défaut) pour que l'application GlobalProtect effectue une détection d'hôte interne sans valider le certificat de serveur des passerelles internes.

19. (À partir de l'application GlobalProtect 6.3.1 ou ultérieure et de la version de publication de contenu 8890-8951 ou ultérieure) Définissez **Enable Advance Host Detection (Activer la détection avancée des hôtes)** sur **Yes (Oui)** pour permettre à GlobalProtect de réessayer la découverte réseau si la détection des hôtes internes échoue. Ce paramètre s'applique si une passerelle interne et une détection des hôtes internes sont configurées sans passerelle externe. Par défaut, le paramètre est défini sur **No (Non)**.

20. (Windows et macOS uniquement ; à partir de l'application GlobalProtect 6.3.3-h6 [6.3.3-c842] ou version ultérieure) Définissez **Enable Unified User-ID in Internal Networks (Activer l'User-ID unifié dans les réseaux internes)** sur **Yes (Oui)** pour maintenir une correspondance d'User-ID cohérente lorsque les utilisateurs se connectent simultanément à des passerelles externes et internes. Cela garantit une application cohérente des politiques pour le trafic à la fois tunnelé et acheminé localement. Utilisez ce paramètre lorsque GlobalProtect doit toujours acheminer le trafic Internet via un tunnel, mais acheminer le trafic interne localement pour des performances optimales sur le réseau d'entreprise. Par défaut, le paramètre est défini sur Non. Pour plus d'informations sur le fonctionnement de cette fonctionnalité, consultez Configurer l'application cohérente des politiques.

Vous pouvez également activer cette fonctionnalité via le `registre Windows unified-user-id-hybrid-deployment` dans le fichier `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`.

21. Si vos points de terminaison éprouvent fréquemment une latence ou une lenteur lors de la connexion au portail GlobalProtect ou aux passerelles, envisagez d'ajuster les valeurs du portail et du délai d'expiration TCP.

Pour donner plus de temps à vos points de terminaison de se connecter ou de recevoir des données du portail ou de la passerelle, augmentez les valeurs de temporisation, au besoin. Gardez à l'esprit que l'augmentation des valeurs peut entraîner des délais d'attente plus longs si l'application GlobalProtect n'est pas en mesure d'établir la connexion. En revanche, la diminution des valeurs peut empêcher l'application GlobalProtect d'établir une connexion lorsque le portail ou la passerelle ne répond pas avant l'expiration du délai d'attente.

Dans la zone App Configurations (Configurations de l'application), configurez l'une des options de temporisation suivantes :

- **Portal Connection Timeout (sec) (Délai d'expiration de connexion au portail (sec.))** : le nombre de secondes (entre 1 et 600) avant qu'une requête de connexion au portail n'expire en raison de l'absence de réponse du portail. Lorsque votre pare-feu utilise des versions de contenu Applications et menaces antérieures à 777-4484, la valeur par défaut est 30. À partir de la version de contenu 777-4484, la valeur par défaut est 5.
- **TCP Connection Timeout (sec) (Temporisation de connexion TCP (sec))** : le nombre de secondes (entre 1 et 600) avant qu'une demande de connexion TCP n'expire en raison de la non-réponse de l'une ou l'autre extrémité de la connexion. Lorsque votre pare-feu utilise des versions de contenu Applications et menaces antérieures à 777-4484, la valeur par défaut est 60. À partir de la version de contenu 777-4484, la valeur par défaut est 5.

 ©2026 Palo Alto Networks, Inc.

- **TCP Receive Timeout (sec) (Temporisation de réception TCP (sec))** : le nombre de secondes avant qu'une connexion TCP s'éteigne en raison de l'absence de réponse partielle d'une requête TCP (la plage est de 1 à 600, la valeur par défaut est 30).

22. (Windows 10 et macOS utilisant macOS Catalina 10.15.4 ou une version ultérieure ; Nécessite l'application GlobalProtect™ 5.2 ou une version ultérieure) Précisez s'il faut activer le DNS partagé pour permettre aux utilisateurs d'envoyer leurs requêtes DNS pour les applications et les ressources par le tunnel VPN tunnel ou en dehors du tunnel VPN en plus du trafic sur le réseau en cochant l'option **Split-Tunnel Option (Option de segmentation de tunnel)**.

    Sélectionnez **Network Traffic Only (Uniquement le trafic du réseau)** pour inclure et exclure les règles qui sont appliquées uniquement au trafic de l'application sur le réseau et non au trafic DNS. Tout le trafic DNS passe par le tunnel VPN quel que soit le tunnel partagé sur la base du destination domain (domaine de destination) que vous avez indiqué pour les inclusions et les exclusions, dans la mesure du possible.. Sur les terminaux Windows, la fonctionnalité de segmentation du DNS peut être utilisée avec **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only) (Résoudre tous les FQDN à l'aide des serveurs DNS assignés par le tunnel [Windows uniquement])** pour appliquer et résoudre toutes les requêtes DNS via le tunnel. Lorsque vous sélectionnez **Both Network Traffic and DNS (trafic de réseau et DNS)**, le tunnel partagé sur la base du destination domain (domaine de destination) que vous avez indiqué pour les inclusions et les exclusions est appliqué au trafic DNS et au trafic de l'application du réseau associé pour ce domaine.

    - (Application GlobalProtect 6.2 et ultérieure) Vous pouvez optionnellement pousser lesconfigurations de segmentation de tunnel vers les terminaux via la passerelle en utilisant un fichier de configuration de segmentation de tunnel hébergé sur un serveur web, ce qui vous permet d'ajouter plus de domaines, d'applications ou de routes exclus ou inclus à la fonctionnalité de tunnel fractionné sans modifier manuellement la configuration de la passerelle.

      *Si vous avez sélectionné **Both Network Traffic and DNS (Trafic réseau et DNS)**, vous devez ajouter au moins un faux domaine à la liste d'exclusion.*

    Avec un DNS partagé, vous pouvez configurer quels domaines sont résolus par les serveurs DNS attribués au VPN et quels sont ceux qui sont résolus par les serveurs DNS locaux.

    Cette option nécessite la version de contenu 8284-6139 ou toute version ultérieure.

23. (Facultatif : nécessite l'application GlobalProtect 6.2) Définissez le **HIP Remediation Process Timeout (sec) (Délai d'expiration du processus de correction HIP [sec])** dans lequel l'application GlobalProtect exécutera un script pour compléter le processus de remédiation HIP. Après que vous Configurer la correction du processus HIP, l'application GlobalProtect fournit une période de délai d'expiration spécifiée dans laquelle le terminal peut exécuter un script de remédiation si un terminal échoue à un contrôle de processus. Après l'expiration du délai d'expiration, l'application GlobalProtect soumet à nouveau le rapport HIP.

24. (Facultarif : nécessite l'application GlobalProtect 6.2) Définissez le **Allow User to Extend GlobalProtect User Session (Autoriser l'utilisateur à prolonger la session utilisateur GlobalProtect)** sur **Yes (Oui)** pour prolonger la durée de vie de la session de connexion de l'application GlobalProtect avant qu'elle n'expire.

 ©2026 Palo Alto Networks, Inc.

25. Spécifiez si les connexions de bureau à distance sont autorisées sur les tunnels VPN existants en spécifiant le **User Switch Tunnel Rename Timeout (délai d'expiration du changement de tunnel utilisateur)**. Lorsqu'un nouvel utilisateur se connecte à un ordinateur Windows en utilisant le protocole RDP (Remote Desktop Protocol), la passerelle ré-assigne le tunnel VPN au nouvel utilisateur. La passerelle peut ensuite appliquer des stratégies de sécurité au nouvel utilisateur.

    Permettre des connexions de bureau à distance via des tunnels VPN peut être utile dans les situations où un administrateur informatique doit accéder à un système d'utilisateur final distant à l'aide de RDP.

    Par défaut, la valeur **User Switch Tunnel Rename Timeout (Délai d'attente pour renommer le tunnel de commutation d'utilisateur)** est définie sur 0, ce qui signifie que la passerelle GlobalProtect met fin à la connexion si un nouvel utilisateur s'authentifie via le tunnel VPN. Pour modifier ce comportement, configurez un délai d'expiration compris entre 1 et 7 200 secondes. Si le nouvel utilisateur ne se connecte pas à la passerelle avant l'expiration de la valeur de timeout, la passerelle GlobalProtect termine le tunnel VPN assigné au premier utilisateur.

    *La modification de la valeur du **User Switch Tunnel Rename Timeout (Délai d'attente pour renommer le tunnel de commutation d'utilisateur)** n'affecte que le tunnel RDP et, lorsqu'elle est configurée, ne renomme pas les tunnels de pré-ouverture de session.*

26. (Windows uniquement) Pour limiter la durée pendant laquelle un utilisateur peut renommer un tunnel VPN existant avant une connexion réussie, spécifiez une valeur de **Pre-Logon Tunnel Rename Timeout (sec) (Windows Only) (Délai d'expiration pour renommer le tunnel de pré-ouverture de session (s) [Windows uniquement])**. La valeur par défaut est -1, ce qui permet de renommer à tout moment.

    (Windows uniquement ; nécessite la version GlobalProtect 6.2.8-h5 (6.2.8-c416) et ultérieure ou 6.3.3-h4 (6.3.3-c828) et ultérieure) Sélectionnez **Enable Cache Portal Configuration in Absence of Pre-logon Tunnel (Activer la configuration du portail de cache en l'absence de tunnel de préouverture de session)** pour activer l'utilisation de la configuration de portail local la plus récemment stockée sur le périphérique si un tunnel de préouverture de session n'est pas disponible.

27. Pour que GlobalProtect puisse conserver le tunnel VPN existant après la déconnexion des utilisateurs de leur terminal, spécifiez un **Délai de conservation du tunnel après la déconnexion de l'utilisateur** (plage comprise entre 0 et 600 secondes ; valeur par défaut : 0 seconde). Si vous acceptez la valeur par défaut (**0**), GlobalProtect ne conserve pas le tunnel lorsque l'utilisateur se déconnecte.

    Cette option nécessite la version de contenu lancée le 8 juillet 2019 ou plus tard.

    Tenez compte des comportements de connexion GlobalProtect suivants lorsque vous configurez GlobalProtect pour qu'il conserve le tunnel VPN :

    - Si le même utilisateur se déconnecte et se reconnecte au terminal au cours du délai d'expiration spécifié (en mode toujours actif ou à la demande), GlobalProtect demeure connecté sans aucune interaction avec l'utilisateur (y compris l'authentification au portail et à la passerelle). Si l'utilisateur ne se reconnecte pas au cours de la même période, le tunnel est déconnecté et l'utilisateur doit rétablir la connexion à GlobalProtect.
    - Si un utilisateur se déconnecte d'un poste de travail et qu'un autre utilisateur se connecte à ce même poste de travail au mode toujours actif ou à la demande, le tunnel existant

 ©2026 Palo Alto Networks, Inc.

est renommé pour le nouvel utilisateur uniquement si le nouvel utilisateur réussit à s'authentifier à GlobalProtect au cours du délai d'expiration spécifié. Si le nouvel utilisateur n'arrive pas à se connecter et à s'authentifier au cours du délai d'expiration spécifié, le tunnel existant se déconnecte et une nouvelle connexion à GlobalProtect doit être établie. Si le nouvel utilisateur est en mode Toujours actif, GlobalProtect tente automatiquement d'établir une nouvelle connexion. Si le nouvel utilisateur est en mode à la demande, il doit établir une nouvelle connexion manuellement.

28. Indiquez comment les mises à niveau de l'application GlobalProtect sont effectuées.

Si vous souhaitez contrôler la mise à niveau des utilisateurs, vous pouvez personnaliser la mise à niveau de l'application en fonction de la configuration. Par exemple, si vous souhaitez tester une version sur un petit groupe d'utilisateurs avant de la déployer sur l'ensemble de votre base d'utilisateurs, vous pouvez créer une configuration s'appliquant uniquement aux utilisateurs de votre groupe informatique, leur permettant ainsi de mettre à niveau et de tester tout en désactivant la mise à niveau dans toutes les autres configurations utilisateur / groupe. Après avoir complètement testé la nouvelle version, vous pouvez modifier les configurations logicielles pour le reste de vos utilisateurs et les autoriser à procéder à la mise à niveau.

Par défaut, l'option **Allow User to Upgrade GlobalProtect App (Permettre à l'utilisateur de mettre à niveau l'application GlobalProtect)** est définie sur **Allow with Prompt (Autoriser avec invite)**, ce qui signifie que les utilisateurs finaux sont invités à procéder à la mise à niveau lorsqu'une nouvelle version de l'application est activée sur le pare-feu. Pour modifier ce comportement, sélectionnez l'une des options suivantes :

- **Allow Transparently (Autoriser de manière transparente)** : les mises à jour ont lieu automatique sans aucune interaction avec l'utilisateur. Les mises à niveau peuvent avoir lieu lorsque l'utilisateur travaille à distance ou est connecté dans le réseau de l'entreprise.
- **Internal (Interne)** : les mises à jour se font automatiquement sans interaction avec l'utilisateur, à condition que l'utilisateur soit connecté depuis le réseau de l'entreprise. Ce paramètre est recommandé pour éviter les mises à niveau lentes dans les situations à faible bande passante. Lorsqu'un utilisateur se connecte en dehors du réseau d'entreprise, la mise à niveau est différée et réactivée lorsque l'utilisateur se connecte à partir du réseau d'entreprise. Vous devez configurer les passerelles internes et la détection d'hôte interne pour utiliser cette option.
- **Disallow (Ne pas autoriser)** : cette option empêche les mises à niveau de l'application.
- **Allow Manually (Autoriser manuellement)** : les utilisateurs finaux initient eux-mêmes les mises à niveau de l'application. Dans ce cas, l'utilisateur doit sélectionner **Check Version (Vérifier la version)** dans le menu des paramètres du panneau d'état de GlobalProtect pour déterminer s'il existe une nouvelle version de l'application, puis procéder à la mise à niveau le cas échéant. Notez que cette option ne fonctionnera pas si l'application GlobalProtect est masquée pour l'utilisateur. Consultez l'étape 6 pour obtenir plus de détails sur les paramètres **Display GlobalProtect Icon (Afficher l'icône GlobalProtect)**.

  *Les mises à niveau pour **Allow Transparently (Permettre avec transparence)** et **Internal (Interne)** se font uniquement si la version du logiciel GlobalProtect sur le portail est plus récente que la version du logiciel GlobalProtect sur le point de terminaison. Par exemple, un agent GlobalProtect 6.0.3 connecté à un portail GlobalProtect 6.0.1 n'est pas mis à niveau.*

  *À partir de l'application GlobalProtect 6.0, les configurations définies sur **Allow with Prompt (Autoriser avec message)** ne demandent pas aux utilisateurs de rétrograder leur version*

 ©2026 Palo Alto Networks, Inc.

d'application lorsque la version d'application activée sur le portail est une version antérieure. Pour voir l'invite de rétrogradation, les utilisateurs doivent ***Check for Updates (Rechercher des mises à jour)*** *dans l'onglet* ***About (À propos)****.*

29. Ajoutez un **Change Password Message (Message de changement de mot de passe)** pour préciser les politiques ou les exigences relatives aux mots de passe que vos utilisateurs doivent respecter lorsqu'ils modifient leurs mots de passe (par exemple, les mots de passe doivent contenir au moins un chiffre et une lettre majuscule).

30. Précisez si vous souhaitez que l'application GlobalProtect envoie des journaux de critères de sélection de passerelle au pare-feu en cochant l'option **Log Gateway Selection Criteria (journaliser les critères de sélection de la passerelle)**.

Sélectionnez **Yes (oui)** pour activer l'application GlobalProtect et envoyer les journaux de critères de sélection de passerelle au pare-feu. La valeur par défaut est **No (non)**. L'application n'envoie pas les journaux améliorés au pare-feu.

Pour vous aider à identifier les détails de la raison pour laquelle l'application GlobalProtect choisit de se connecter à une passerelle spécifique, l'application GlobalProtect collecte et transmet les informations d'identification des critères de sélection de passerelle et la latence entre la passerelle et le terminal. Les informations sur les critères de sélection de la passerelle peuvent vous aider à identifier la priorité et le délai de réponse de la passerelle sélectionnée, la liste des tentatives de connexion à la passerelle et les statistiques relatives à la latence du réseau avant et après le tunnel. Les champs des journaux améliorés pour les critères de sélection de la passerelle ont été ajoutés aux GlobalProtect logs (journaux GlobalProtect) dans **Monitor (surveiller)** > **Logs (Journaux)** > **GlobalProtect**.

31. Indiquez s'il faut afficher une page d'accueil lors de la connexion réussie.

Une page d'accueil peut être une étape utile pour diriger les utilisateurs vers les ressources internes auxquelles ils peuvent accéder uniquement lorsqu'ils sont connectés à GlobalProtect, telles que votre Intranet ou d'autres serveurs internes.

Par défaut, l'indication « uniquement lorsque la connexion de l'application est établie » est un message bulle qui s'affiche dans la zone de notification/barre de menus.

Pour afficher une page d'accueil après une connexion réussie, sélectionnez **factory-default (d'usine par défaut)** dans la liste déroulante **Welcome Page (Page de bienvenue)**. GlobalProtect affiche la page d'accueil dans l'application GlobalProtect. Toutefois, vous pouvez définir une ou plusieurs pages d'accueil personnalisées qui fournissent des informations spécifiques à vos utilisateurs, ou à un groupe spécifique d'utilisateurs (en fonction de la configuration du portail qui sera déployée). Pour plus de détails sur la création de pages personnalisées, voir Personnaliser les pages d'accès, de bienvenue et d'aide du portail GlobalProtect.

32. Configurez les paramètres de collecte de journaux d'applications GlobalProtect.

Vous pouvez configurer l'application GlobalProtect pour envoyer des journaux de dépannage, des journaux de diagnostic ou les deux à Strata Logging Service. Consultez Liste de vérification Collecte de journaux de l'application GlobalProtect pour le dépannage pour plus de détails sur la configuration des composants pour activer la collecte des journaux de l'application

 ©2026 Palo Alto Networks, Inc.

GlobalProtect pour le dépannage et pour afficher les détails dans les journaux de dépannage et de diagnostic de l'application GlobalProtect sur l'application Explore.

- (Version de contenu 8350-14191 ou ultérieure ; nécessite l'application GlobalProtect 5.2.5) Définissez **Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting (Activer la collecte de journaux d'applications DEM et GlobalProtect pour le dépannage)** sur **Yes (Oui)** pour permettre à l'application GlobalProtect d'afficher l'option **Report an issue (Signaler un problème)** sur l'application GlobalProtect pour permettre aux utilisateurs finaux pour envoyer les journaux de dépannage et de diagnostic directement au service de journalisation Strata. Vous devez configurer le certificat Strata Logging Service qui est poussé depuis le portail en tant que certificat client pour afficher l'option **Report an issue (Signaler un problème)**. Ce certificat est utilisé pour que le client s'authentifie auprès de Strata Logging Service lors de l'envoi des journaux. Lorsque ce paramètre est défini sur **No (Non)** (par défaut), l'application GlobalProtect n'affiche pas l'option **Report an issue (Signaler un problème)** et les utilisateurs finaux ne peuvent pas envoyer les journaux de dépannage et de diagnostic à Strata Logging Service.
- (Content Release version 8350-14191 or later; Requires GlobalProtect app 5.2.5 (Content Release version 8350-14191 ou ultérieure ; Nécessite l'application GlobalProtect 5.2.5)) Saisissez jusqu'à dix URL de destination HTTPS pouvant contenir des adresses IP ou des noms de domaine complets (par exemple, https://10.10.10.10/resource. html, https://webserver/file.pdf ou https://google.com) pour **Run Diagnostics Tests for These Destination Web Servers (exécuter des tests de diagnostic pour ces serveurs Web de destination)** sur le portail GlobalProtect. Pour vous aider à identifier avec précision les résultats de vitesse de téléchargement, vous pouvez spécifier un emplacement de fichier de téléchargement ayant la taille appropriée. Par exemple, la taille du fichier peut aller de 10 Mo à 50 Mo pour calculer la vitesse de téléchargement suffisante. Cependant, ce calcul n'est pas vrai pour la limitation de taille de la page Web pour récupérer et télécharger le fichier qui peut prendre moins d'une seconde, ce qui n'est pas une taille d'échantillon suffisante pour déterminer des résultats de vitesse de téléchargement élevés. Ce champ est vide par défaut.

  Les URL de destination HTTPS qui peuvent contenir des adresses IP ou des noms de domaine complets que vous fournissez sont utilisées uniquement lorsque **Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting (Activer DEM autonome et Collecte de journaux de l'application GlobalProtect App pour le dépannage)** est défini sur **Yes (Oui)** et lorsque les diagnostics sont effectués. Ces URL de destination basées sur HTTPS ne sont pas utilisées lorsque l'application GlobalProtect crée des rapports de dépannage en cas de problème. Utilisez des virgules, des points-virgules ou des lignes distinctes pour séparer plusieurs noms de domaine complets (par exemple, google.com, gmail.com).

 ©2026 Palo Alto Networks, Inc.

33. Spécifiez si vous souhaitez installer l'agent de point de terminaison Autonomous DEM (ADEM) pendant l'installation de l'application GlobalProtect et autorisez les utilisateurs finaux à activer ou désactiver les tests d'expérience utilisateur à partir de l'application.

- (Windows 10 et macOS uniquement ; version de publication de contenu 8845-8731 ou ultérieure) Les options disponibles dépendent de la version de GlobalProtect dans votre environnement.

Version de GlobalProtect	Nom de la configuration	Valeurs de configuration
GlobalProtect 6.2 et antérieur	Agent de terminal DEM autonome pour Prisma Access pour la version GP 6.2 et inférieure	• **Install and user cannot enable/disable agent from GlobalProtect (Installer et l'utilisateur ne peut pas activer/désactiver l'agent depuis GlobalProtect)** • **Install and user can enable/disable agent from GlobalProtect (Installer et l'utilisateur peut activer/ désactiver l'agent depuis GlobalProtect)** • **Do not install (Ne pas installer)** Ceci est la valeur par défaut.
GlobalProtect 6.3 et ultérieur	Expérience d'accès (ADEM, Accélération d'application, Coaching utilisateur final) pour GP 6.3 et supérieur (Windows et MAC uniquement)	• **Install the Agent (Installer l'agent)** • **Uninstall the Agent (Désinstaller l'agent)** • **No action (The agent state remains as is) (Aucune action [l'état de l'agent reste tel quel])** Ceci est la valeur par défaut.

- (Windows 10 et macOS uniquement ; version de publication du contenu antérieure à 8845-8731) Sélectionnez **Install and user can enable/disable agent from GlobalProtect (Installer et l'utilisateur peut activer/désactiver l'agent de GlobalProtect)** pour installer l'agent du terminal ADEM lors de l'installation de l'application GlobalProtect et autoriser les utilisateurs finaux à activer ou désactiver les tests d'expérience utilisateur à partir de l'application GlobalProtect. Sélectionnez **Install and user cannot enable/disable agent from GlobalProtect (Installer et l'utilisateur ne peut pas activer/désactiver l'agent de GlobalProtect)** pour installer l'agent de point de terminaison ADEM lors de l'installation de l'application GlobalProtect, et ne pas autoriser les utilisateurs finaux à activer ou désactiver les tests d'expérience utilisateur à partir de l'application GlobalProtect. Sélectionnez **Do Not**

 ©2026 Palo Alto Networks, Inc.

Install (Ne pas installer) (par défaut) pour ne pas installer l'agent de point de terminaison ADEM lors de l'installation de l'application GlobalProtect.

Pour des détails sur le démarrage avec ADEM, consultez Premiers pas avec DEM autonome.

34. (Windows uniquement) Spécifiez si vous voulez que l'application GlobalProtect **Display Status Panel at Startup (Afficher le panneau d'état lors du démarrage)**.
    - Pour supprimer le panneau d'état lorsque les utilisateurs établissent une connexion à GlobalProtect pour la première fois, sélectionnez **No (Non)**.
    - Pour afficher automatiquement le panneau d'état GlobalProtect lorsque les utilisateurs établissent une connexion à GlobalProtect pour la première fois, sélectionnez **Yes (Oui)**. Si cette option est activée, les utilisateurs doivent cliquer à l'extérieur du panneau d'état pour le fermer manuellement.

35. (Windows 10 and macOS only; Content Release version 8450-6909 or later; Requires GlobalProtect app 6.0 (Windows 10 et macOS uniquement ; version de contenu 8450-6909 ou ultérieure ; Nécessite l'application GlobalProtect 6.0)) Définissez **Allow GlobalProtect UI to Persist for User Input (Autoriser l'interface utilisateur GlobalProtect à persister pour l'entrée de l'utilisateur)** sur **Yes (Oui)** pour permettre au panneau d'état de continuer à s'afficher à l'écran pendant que l'utilisateur final est entrant leurs informations d'identification lors de la connexion ou annule la demande. Lorsque ce paramètre est défini sur **No (Non)** (par défaut) et que l'utilisateur final doit saisir ses informations d'identification, il doit cliquer en dehors du panneau d'état pour le réduire manuellement.

36. Enregistrez la configuration d'agent.
    1. Si vous avez fini de personnaliser vos configurations d'agent, cliquez sur **OK** pour les enregistrer. Sinon, revenez à la section Définir les configurations de l'agent GlobalProtect pour terminer la configuration de l'agent.
    2. Cliquez sur **OK** pour enregistrer votre configuration de portail.
    3. **Validez** les modifications.

Configurer l'application cohérente des politiques

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Terminaux Windows et MacOS uniquement	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Version GlobalProtect 6.3.3-h6 (6.3.3-c842) ou ultérieure

Vous pouvez maintenir des mappages User-ID cohérents pour les utilisateurs qu'ils travaillent à distance ou connectés au réseau d'entreprise. Pour utiliser cette fonctionnalité, définissez **Enable Unified User-ID in Internal Networks (Activer l'User-ID unifié dans les réseaux internes)** sur **Yes (Oui)** dans l'application GlobalProtect. Pour plus d'informations, consultez Personnaliser l'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Votre environnement doit répondre aux pré-requis suivants pour que cette fonctionnalité fonctionne :

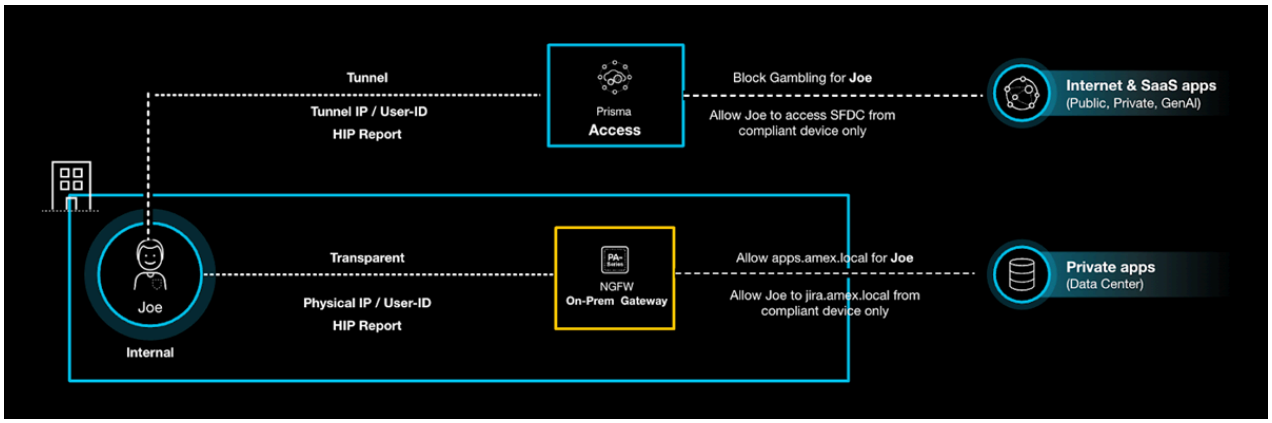
- GobalProtect est configuré en mode toujours actif avec la méthode de connexion est ouverture de session utilisateur ou préouverture de session.
- La Segmentation de tunnel est configurée avec des routes d'accès incluses/exclues pour les passerelles internes afin que l'authentification et les rapports HIP vers les passerelles internes ne passent pas par le tunnel. Pour ce faire, créez une politique de tunnel afin que le trafic du sous-réseau interne soit exclu du tunnel lorsque l'utilisateur est sur le réseau d'entreprise.
- La détection d'hôte interne est configurée et résout vers le réseau interne.

Lorsque les utilisateurs travaillent à distance, l'agent GlobalProtect se lance automatiquement lorsqu'ils allument leur périphérique Windows ou macOS. L'agent authentifie l'utilisateur et établit un tunnel VPN complet vers la passerelle externe configurée (Prisma Access). Un mappage User-ID est créé sur Prisma Access, liant l'utilisateur à son adresse IP virtuelle assignée. Tout le trafic réseau du périphérique est acheminé à travers le tunnel. Prisma Access inspecte tout le trafic et applique les politiques de sécurité basées sur l'utilisateur pertinentes.

Lorsque les utilisateurs sont au bureau sur le réseau interne, l'agent GlobalProtect effectue une double authentification :

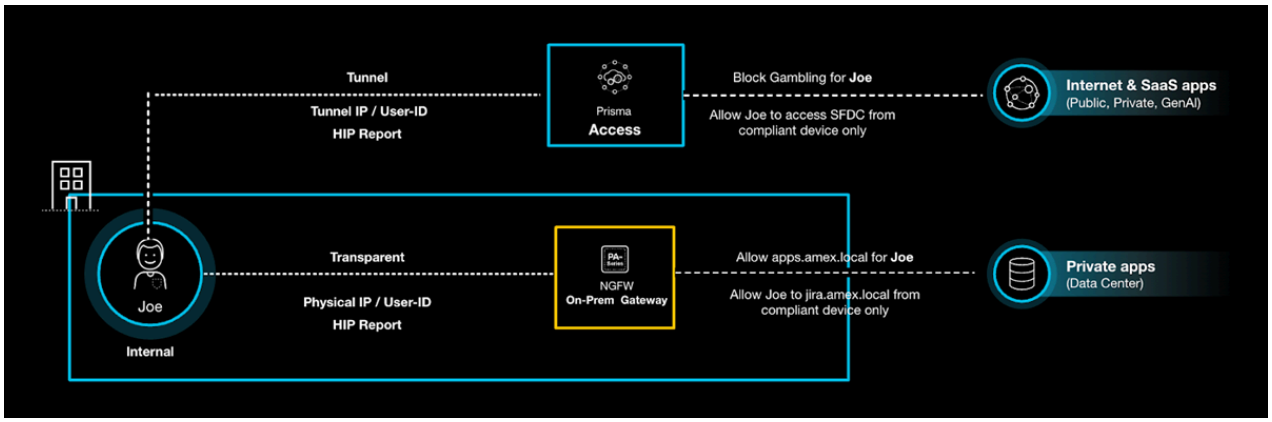
- Authentification externe : Elle s'authentifie avec la passerelle externe (Prisma Access) et établit le tunnel VPN principal, ce qui crée un mappage User-ID sur Prisma Access.
- Authentification interne : Elle s'authentifie également directement avec les passerelles sur site configurées pour créer un mappage User-ID sur les pare-feu sur site. Aucun tunnel n'est établi avec les passerelles internes.

  Le trafic de segmentation du tunnel vers les ressources internes utilise le mappage IP physique tandis que le trafic en tunnel vers les ressources externes utilise le mappage IP virtuel. L'agent collecte des données de profil d'information d'hôte (HIP) de tous les terminaux.



L'agent soumet le rapport HIP à Prisma Access. Prisma Access applique des politiques basées sur HIP à tout le trafic en tunnel. Lorsque l'utilisateur est sur le réseau interne, l'agent soumet le rapport HIP à la fois à la passerelle externe (Prisma Access) et aux passerelles internes lors de l'authentification respective. Prisma Access utilise le rapport pour appliquer des politiques sur tout trafic qui est en tunnel. Les passerelles sur site utilisent le rapport pour appliquer des politiques sur le trafic en tunnel fractionné pour les ressources locales. L'organisation peut ainsi garantir la conformité constante des périphériques des terminaux (par exemple, vérification de l'antivirus actif, du chiffrement du disque) pour tout le trafic, quel que soit l'emplacement de l'utilisateur ou la destination du trafic.

 ©2026 Palo Alto Networks, Inc.



Configurer la détection du portail captif en mode proxy et hybride

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (géré par Panorama ou Strata Cloud Manager) • Terminaux Windows et MacOS	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect 6.3.3-h2 (6.3.3-c679) et versions ultérieures

Le portail captif est une implémentation de sécurité réseau dans laquelle les utilisateurs se connectant à un réseau (généralement Wi-Fi) sont d'abord redirigés vers une page Web pour authentification avant d'être autorisés à établir une connexion sécurisée GlobalProtect pour accéder aux ressources de l'entreprise. Cette approche offre un niveau de sécurité supplémentaire en garantissant que les utilisateurs s'authentifient via le portail du réseau local avant que le client GlobalProtect puisse établir un tunnel sécurisé vers l'infrastructure réseau de l'organisation. Pour plus d'informations sur l'activation et la configuration du portail captif pour les utilisateurs finaux, reportez-vous à Personnaliser l'application GlobalProtect.

Lorsque les utilisateurs sont en mode proxy ou tunnel et proxy (hybride), la page de connexion au portail captif peut ne pas se charger lors de la connexion Wi-Fi, car le proxy intercepte et bloque l'accès des paquets au portail captif. Pour garantir la connectivité du portail captif dans ces modes, il est recommandé de définir **Captive Portal Exception Timeout (sec) (Expiration de l'exception du portail captif [sec])** sur 600 secondes. En outre, vous devez autoriser l'accès direct à Internet (en contournant tout proxy ou filtrage) pour les URL du terminal de vérification de connectivité :

- Sur Panorama, ajoutez ces URL à votre fichier PAC (Proxy Auto-Configuration) :

```
if ( shExpMatch(host, "captive.apple.com") || shExpMatch(host,
 "edge-http.microsoft.com") || shExpMatch(host,
 "detectportal.firefox.com") ) { return "DIRECT"; }
```

 ©2026 Palo Alto Networks, Inc.

- Sur Strata Cloud Manager, ajoutez ces URL à votre fichier PAC ou à un profil de transfert :
  - captive.apple.com
  - clients3.google.com
  - msftconnecttest.com

  Pour plus d'informations, consultez Explicit Proxy Forwarding Profiles (Profils de transfert de proxy explicite).

Connexions de tunnel via des proxys

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

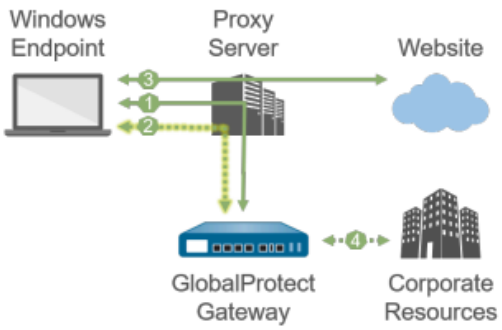
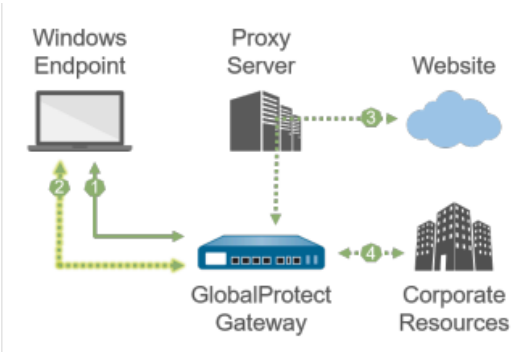
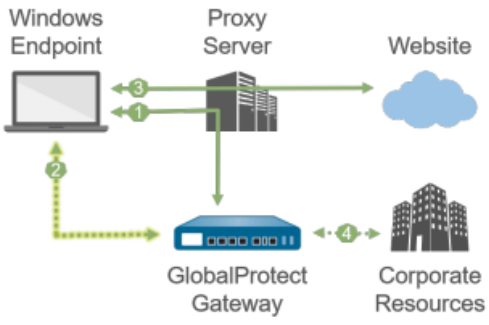
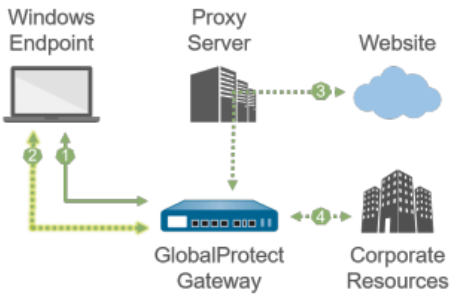
Sur les plateformes Windows et macOS, vous pouvez configurer GlobalProtect pour contourner les proxys afin que tout le trafic HTTP/HTTPS correspondant aux règles du fichier proxy/PAC doive traverser le tunnel VPN GlobalProtect avant d'atteindre la destination prévue. En contournant les proxys, vous pouvez empêcher les utilisateurs de configurer un proxy personnel pour accéder aux ressources web sans passer par le tunnel pour inspection et application des politiques.

Si vous activez GlobalProtect pour utiliser des proxys sur les terminaux Windows, seul le trafic HTTP/HTTPS correspondant aux règles du fichier proxy/PAC passe directement par le proxy après que les utilisateurs aient établi la connexion GlobalProtect. Tout autre trafic correspondant aux itinéraires d'accès configurés sur la passerelle GlobalProtect passe par le tunnel établi via le proxy. Sur les terminaux macOS, les proxys sont désactivés après que les utilisateurs aient établi la connexion GlobalProtect. Cela se produit parce que les paramètres du proxy ne sont pas copiés de l'adaptateur réseau physique du terminal vers l'adaptateur réseau virtuel du terminal, et l'adaptateur réseau virtuel devient l'adaptateur principal à partir duquel le terminal macOS reçoit les paramètres du proxy.

Les tableaux suivants décrivent le comportement du trafic réseau en fonction du système d'exploitation du terminal, du type de tunnel et de l'utilisation du proxy GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

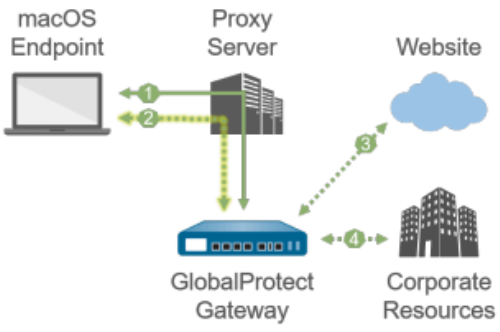
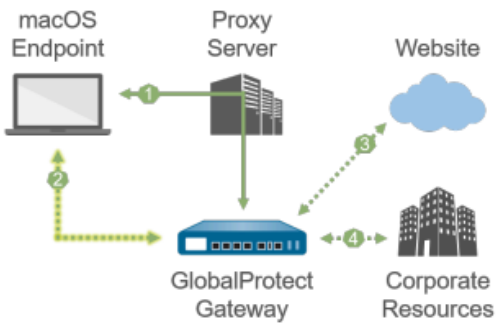
Tableau 3 : Comportement du trafic réseau sur les terminaux Windows

Type de tunnel	GlobalProtect utilise des proxys	GlobalProtect contourne les proxys
SSL		
	1 : toutes les demandes de connexion passent par le proxy.	**1** : toutes les demandes de connexion contournent le proxy et vont directement à la passerelle.
	2 : la configuration du tunnel SSL passe par le proxy.	**2** : la configuration du tunnel SSL contourne le proxy et va directement à la passerelle.
	3 : le trafic HTTP/HTTPS correspondant aux règles du fichier proxy/PAC passe par le proxy et contourne le tunnel SSL.	**3** : le trafic HTTP/HTTPS correspondant aux règles du fichier proxy/PAC passe par le tunnel SSL puis par le proxy. *Si le proxy est inaccessible depuis la passerelle, le trafic HTTP/HTTPS est abandonné, et les utilisateurs ne peuvent pas accéder à la destination prévue.*
	4 : autre trafic qui correspond aux itinéraires d'accès configurés sur la passerelle passe par le tunnel SSL construit sur le proxy.	**4** : autre trafic qui correspond aux itinéraires d'accès configurés sur la passerelle contourne le proxy et passe par le tunnel SSL.
IPSec		

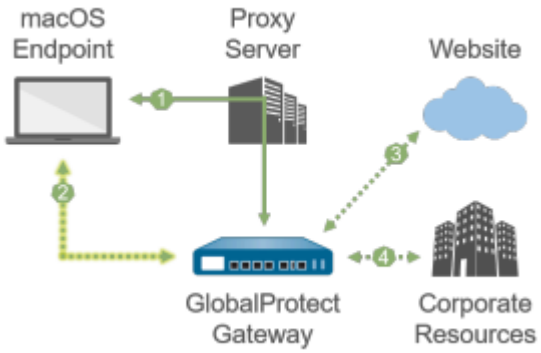
 ©2026 Palo Alto Networks, Inc.

Type de tunnel	GlobalProtect utilise des proxys	GlobalProtect contourne les proxys
	Vous ne pouvez pas configurer un tunnel IPSec à travers un proxy car les proxys ne prennent pas en charge le trafic UDP.	
	1 : toutes les demandes de connexion passent par le proxy.	**1** : toutes les demandes de connexion contournent le proxy et vont directement à la passerelle.
	2 : la configuration du tunnel IPSec contourne le proxy et va directement à la passerelle.	**2** : la configuration du tunnel IPSec contourne le proxy et va directement à la passerelle.
	3 : le trafic HTTP/HTTPS qui correspond aux règles du fichier proxy/PAC passe par le proxy et contourne le tunnel IPSec.	**3** : le trafic HTTP/HTTPS qui correspond aux règles du fichier proxy/PAC passe par le tunnel IPSec puis par le proxy. *Si le proxy est inaccessible depuis la passerelle, le trafic HTTP/HTTPS est abandonné, et les utilisateurs ne peuvent pas accéder à la destination prévue.*
	4 : autre trafic qui correspond aux itinéraires d'accès configurés sur la passerelle contourne le proxy et passe par le tunnel IPSec.	**4** : autre trafic qui correspond aux itinéraires d'accès configurés sur la passerelle contourne le proxy et passe par le tunnel IPSec.

Tableau 4 : Comportement du trafic réseau sur les terminaux Mac

Type de tunnel	GlobalProtect utilise des proxys	GlobalProtect contourne les proxys
SSL		

 ©2026 Palo Alto Networks, Inc.

Type de tunnel	GlobalProtect utilise des proxys	GlobalProtect contourne les proxys
	1 : toutes les demandes de connexion passent par le proxy.	**1** : toutes les demandes de connexion passent par le proxy.
	2 : la configuration du tunnel SSL passe par le proxy.	**2** : la configuration du tunnel SSL contourne le proxy et va directement à la passerelle.
	3 : le trafic HTTP/HTTPS qui correspond aux règles du fichier proxy/PAC passe par le tunnel SSL construit sur le proxy.	**3** : le trafic HTTP/HTTPS qui correspond aux règles du fichier proxy/PAC contourne le proxy et passe par le tunnel SSL.
	4 : autre trafic qui correspond aux itinéraires d'accès configurés sur la passerelle passe par le tunnel SSL construit sur le proxy.	**4** : autre trafic qui correspond aux itinéraires d'accès configurés sur la passerelle contourne le proxy et passe par le tunnel SSL.
IPSec	 *Vous ne pouvez pas configurer un tunnel IPSec à travers un proxy car les proxys ne prennent pas en charge le trafic UDP.*	
	1 : toutes les demandes de connexion passent par le proxy.	
	3 : la configuration du tunnel IPSec contourne le proxy et va directement à la passerelle.	
	3 : le trafic HTTP/HTTPS qui correspond aux règles du fichier proxy/PAC contourne le proxy et passe par le tunnel IPSec.	
	4 : autre trafic qui correspond aux itinéraires d'accès configurés sur la passerelle contourne le proxy et passe par le tunnel IPSec.	

 ©2026 Palo Alto Networks, Inc.

Personnaliser les pages d'accès, de bienvenue et d'aide du Portail GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect fournit les pages Ouverture de session, Accueil, et/ou Aide par défaut. Toutefois, vous pouvez créer vos propres pages personnalisées avec votre marque d'entreprise, les politiques d'utilisation acceptables, et les liens vers vos ressources internes.

Vous pouvez alternativement désactiver l'accès au navigateur à la page de connexion du portail afin d'empêcher les tentatives non autorisées de s'authentifier au portail GlobalProtect.

- *Sur Panorama, configurez l'option* ***Portal Login Page (Page de connexion du portail)*** *>* ***Disable (Désactiver)*** *à partir de* ***Network (Réseau)*** *>* ***GlobalProtect*** *>* ***Portals (Portails)*** *>* ***<portal_config*** *>* ***General (Général)****.*
- *Sur Strata Cloud Manager (NGFW), sélectionnez* ***Configuration*** *>* ***NGFW and Prisma Access (NGFW et Prisma Access)*** *>* ***Configuration Scope (Portée de configuration)*** *>* ***All Firewalls (Tous les pare-feu)*** *>* ***Device (Périphérique)*** *>* ***GlobalProtect*** *>* ***Portals and Gateways (Portails et passerelles)*** *>* ***Portals (Portails) Add Portal (Ajouter un portail)****. Sur la page Ajouter un portail, sous* ***Advanced Settings (Paramètres avancés)*** *>* ***Appearance (Apparence)*** *>* ***Portal Login Page (Page de connexion du portail)*** *et sélectionnez* ***Disable (Désactiver)****.*

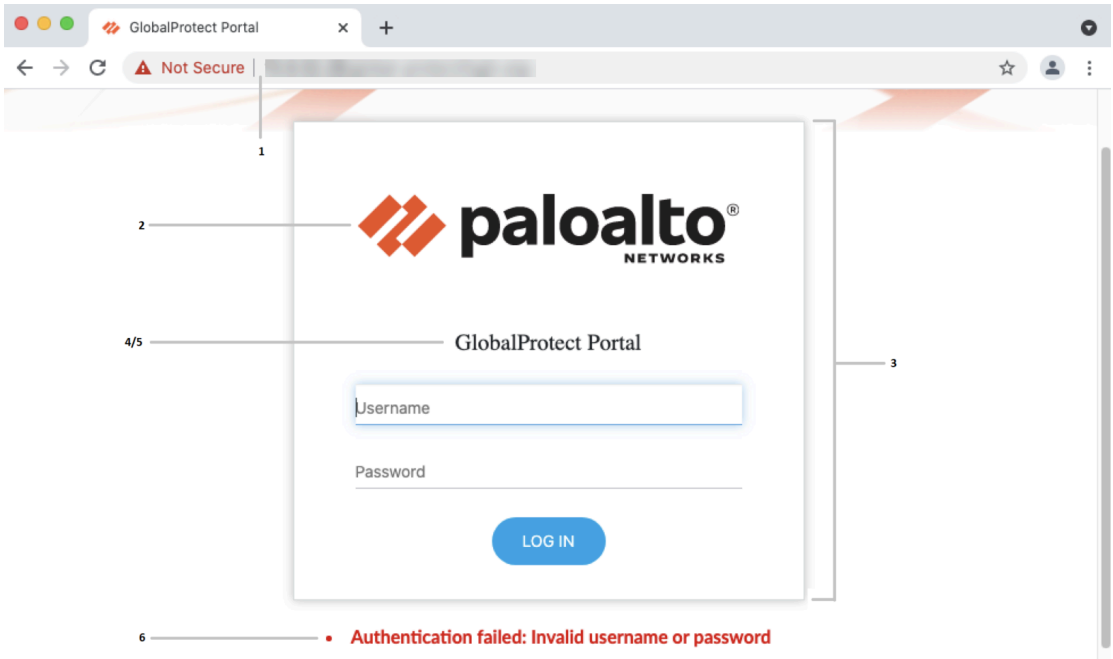
Lorsque la page d'ouverture de session du portail est désactivée, vous pouvez alors utiliser un outil de distribution logicielle tel que System Center Configuration Manager (SCCM) de Microsoft, pour permettre aux utilisateurs de télécharger et d'installer l'application GlobalProtect.

1. Exportez le portail par défaut, la page d'accueil, la page de bienvenue ou la page d'aide.
   1. Pour exporter la page de connexion par défaut du portail, la page d'accueil, la page de bienvenue ou la page d'aide, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **Response Pages (Pages de réponse)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Portals (Portails)** > **Add Portal (Ajouter un portail)**. Sur la page Ajouter un portail, dans le **Advanced Settings (Paramètres avancés)**, sélectionnez l'option **Appearance (Apparence)**.
      - Sur Panorama, sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.

 ©2026 Palo Alto Networks, Inc.

2. Sélectionnez le lien de la page du portail GlobalProtect correspondante, par exemple **GlobalProtect Portal Login Page (Page de connexion au portail GlobalProtect)**.
3. Sélectionnez la page prédéfinie **Default (Par défaut)** et cliquez sur **Export (Exporter)**.

2. Modifiez la page exportée.
   1. À l'aide d'un éditeur de texte HTML de votre choix pour ouvrir et modifier la page.
   2. Pour modifier la page d'accueil ou de connexion, configurez l'une des variables suivantes :
      - **GlobalProtect Portal Login Page (Page de connexion du portail GlobalProtect)** :



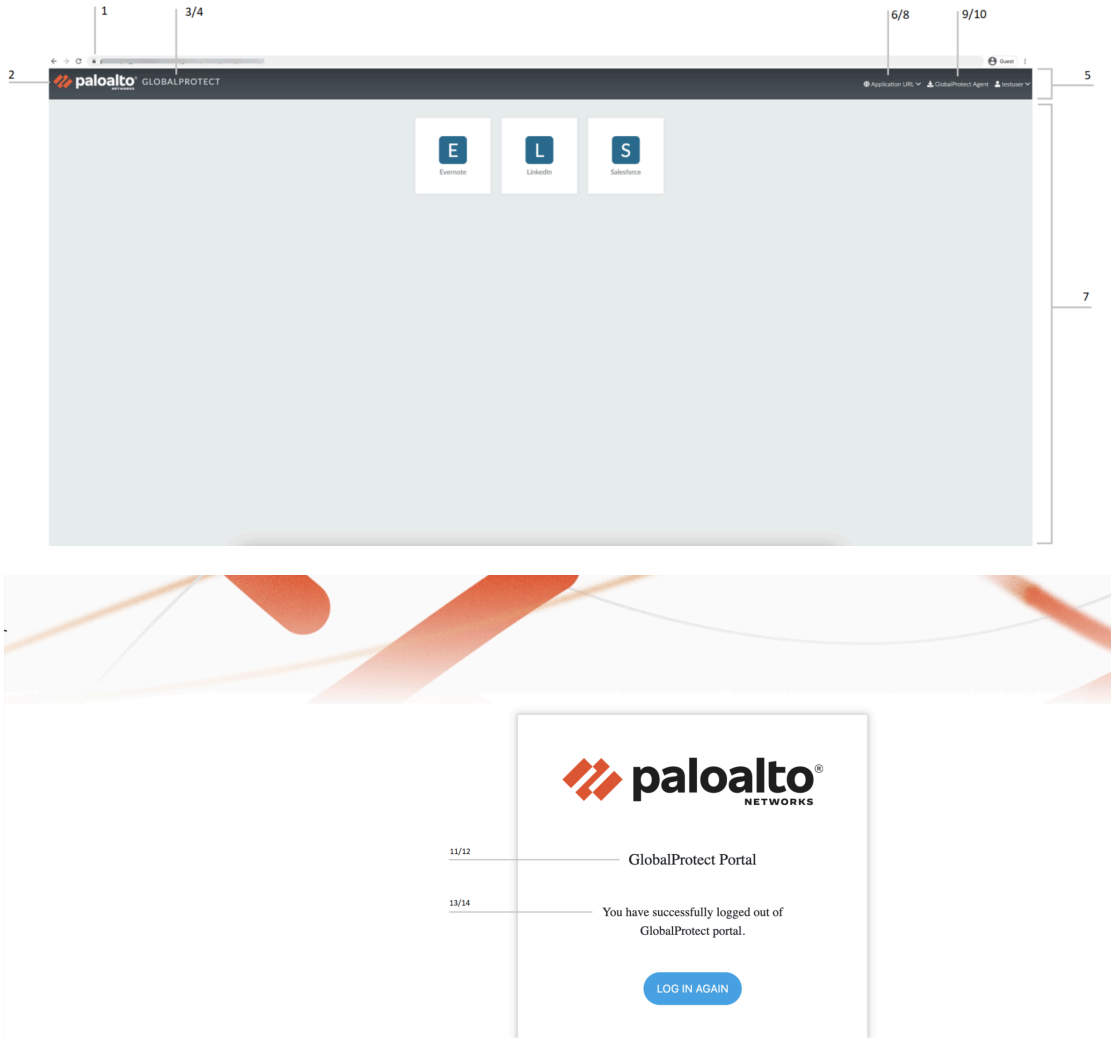
Numéro de l'étiquett	Variable	Description	Exemple
1	`favicon`	URL de l'icône qui s'affiche dans la barre d'adresse du navigateur Web.	`var favicon = 'ht tp:// cdn.slidesh arecdn. com/logo- 24x24. jpg?397576 2018';`
2	`logo`	URL du logo de l'entreprise.	`var logo = 'http: // cdn.slideshare cdn. com/logo-96x 96. jpg?138272258 8';`

 ©2026 Palo Alto Networks, Inc.

Numéro de l'étiquett	Variable	Description	Exemple
3	`bg_color`	Couleur d'arrière-plan de la page de connexion.	`var bg_color = '#D3D3D3';`
4	`gp_portal_name`	Texte qui s'affiche sous le logo de l'entreprise.	`var gp_portal_name = 'GlobalProtect Portal';`
5	`gp_portal_name_color`	Couleur du texte qui s'affiche sous le logo de l'entreprise.	`var gp_portal_name_ color = '#000000';`
6	`error_text_color`	Couleur du texte des messages d'échec de connexion.	`var error_text_ color = '#196390';`

©2026 Palo Alto Networks, Inc.

- **GlobalProtect Portal Home Page (Page d'accueil du portail GlobalProtect) :**



Numéro de l'étiquett	Variable	Description	Exemple
1	`favicon`	URL de l'icône qui s'affiche dans la barre d'adresse du navigateur Web.	`var favicon = 'ht tp:// cdn.slidesh arecdn. com/logo- 24x24. jpg?397576 2018';`
2	`logo`	URL du logo de l'entreprise.	`var logo = 'http: // cdn.slideshare cdn. com/logo-96x`

 ©2026 Palo Alto Networks, Inc.

Numéro de l'étiquett	Variable	Description	Exemple
			96. jpg?138272258 8';
3	navbar_text	Texte de la barre de navigation.	var navbar_text = 'GlobalProtect';
4	navbar_text_color	Couleur du texte de la barre de navigation.	var navbar_text_ color = '#D3D3D3' ;
5	navbar_bg_color	Couleur d'arrière-plan de la barre de navigation.	var navbar_bg_col or = '#A9A9A9';
6	dropdown_bg_color	Couleur d'arrière-plan de la liste déroulante.	var dropdown_bg_ color = '#FFFFFF' ;
7	bg_color	Couleur d'arrière-plan de la page d'accueil.	var bg_color = '# D3D3D3';
8	label_custom_app_url	Étiquette des URL d'application personnalisées/internes.	var label_custom_ app_url = 'Appli cation URL';
9	display_ globalprotect_agent	Option d'afficher ou de masquer le bouton de téléchargement de l'application GlobalProtect. Saisissez **1** pour afficher le bouton de téléchargement. Saisissez **0** pour masquer le bouton de téléchargement.	var display_ glob alprotect_agent = 1;
10	label_globalprotect_ agent	Étiquette du bouton de téléchargement	var label_ global protect_agent = '

 ©2026 Palo Alto Networks, Inc.

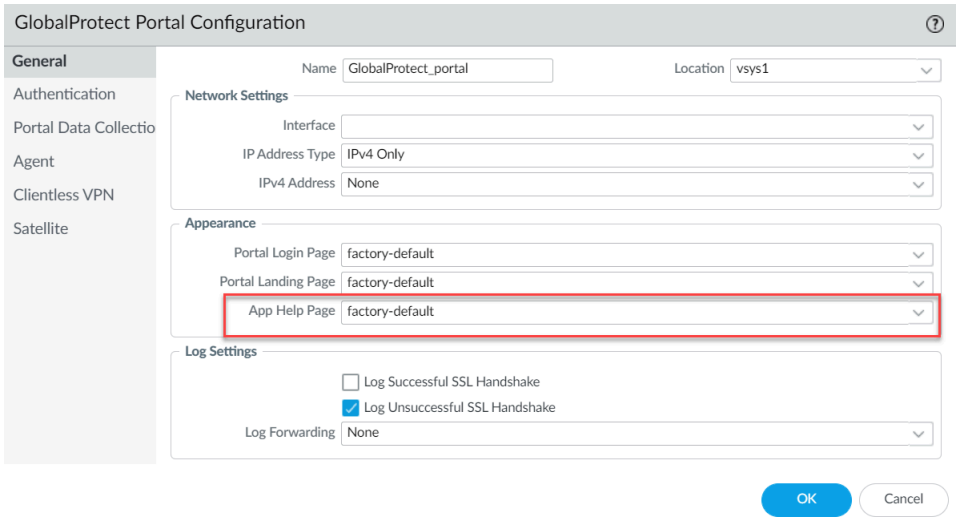
Numéro de l'étiquett	Variable	Description	Exemple
		de l'application GlobalProtect.	`GlobalProtect Agent';`
11	`gp_portal_name`	Texte qui s'affiche sous le logo de l'entreprise sur la page de déconnexion du portail.	`var gp_portal_name = 'GlobalProtect Portal';`
12	`gp_portal_name_color`	Couleur du texte qui s'affiche sous le logo de l'entreprise sur la page de déconnexion du portail.	`var gp_portal_name_ color = '#000000';`
13	`logout_text_array`	Messages qui s'affichent sur la page de déconnexion du portail après que les utilisateurs se sont déconnectés du portail. *Vous ne pouvez modifier que les messages existants ; vous ne pouvez ajouter de nouveaux messages ou supprimer les messages existants.*	`var logout_text_ array = ["You have successfully logged out of GlobalProtect portal.", "GlobalProtect Gateway is not licensed. Contact system administrator.", "User not authenticated to GlobalProtect portal.", "System error, contact system administrator.", "System error, failed to delete user session. Contact system administrator.", "Cannot create user session. Max-capacity reached. Contact system administrator."];`
14	`logout_text_color`	Couleur du texte des messages qui s'affichent sur la page de déconnexion du portail après que les utilisateurs se sont déconnectés du portail.	`var logout_text_ color = '#000000';`

©2026 Palo Alto Networks, Inc.

3. Enregistrez la page modifiée avec un nouveau nom de fichier. Veillez à ce que la page conserve son codage UTF-8.

Pour définir la **GlobalProtect App Help Page (Page d'aide de l'application GlobalProtect)** afin de fournir de l'aide aux utilisateurs de l'application GlobalProtect :

1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**, puis **Add (Ajouter)** un portail.
2. Sélectionnez **General (Général)**.
3. Dans la section Apparence, sélectionnez la page d'aide **factory-default (Par défaut de l'usine)**, **Import (Importer)** une page d'aide personnalisée, ou sélectionnez **None (Aucune)** pour retirer l'option **Help (Aide)** du menu **Settings (Paramètres)** du panneau d'état GlobalProtect.



4. Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.

3. Importez la ou les nouvelles pages.
   1. Sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.
   2. Sélectionnez le lien pour la page du portail GlobalProtect correspondante.
   3. **Import (Importez)** la nouvelle page du portail. Saisissez le chemin et le nom de fichier dans le champ **Import File (Importer le fichier)** ou **Browse (Naviguez)** pour trouver le fichier et sélectionnez-le.
   4. (Facultatif) Sélectionnez le système virtuel sur lequel cette page d'ouverture de session sera utilisée dans la liste déroulante **Destination** ou sélectionnez **shared (Partagée)** (par défaut) pour la rendre disponible pour tous les systèmes virtuels.
   5. Cliquez sur **OK** pour importer le fichier.

©2026 Palo Alto Networks, Inc.

4. Configurez le portail pour utiliser la ou les nouvelles pages.

   - **Portal Login Page (Page de connexion au portail)**, **Portal Landing Page (Page d'accueil du portail)** et **App Help Page (Page d'aide de l'application)** :

     1. sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
     2. Sélectionnez le portail auquel vous souhaitez ajouter la page de connexion, la page d'accueil ou la page d'aide de l'application.
     3. Dans la section Apparence de l'onglet **General (Général)**, sélectionnez la nouvelle page à partir de la liste déroulante correspondante.

   - **Custom Welcome Page (Page d'accueil personnalisée)** :

     1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
     2. Sélectionnez le portail auquel vous souhaitez ajouter la page d'accueil.
     3. Sous l'onglet **Agent**, sélectionnez la configuration de l'agent à laquelle vous souhaitez ajouter la page d'accueil.
     4. À l'onglet **App (Applications)**, sélectionnez la nouvelle page dans la liste déroulante **Welcome Page (Page de bienvenue)**.
     5. Cliquez sur **OK** pour enregistrer la configuration client.

5. Enregistrez la configuration du portail.

   Cliquez sur **OK (OK)** pour enregistrer la configuration du portail, puis sur **Commit (Valider)** pour valider vos modifications.

6. Vérifiez que la nouvelle page de réponse s'affiche.

   - **Testez la page de connexion** : dans le navigateur Web, accédez à l'URL de votre portail (n'ajoutez pas le numéro de port 4443 à la fin de l'URL ; sinon, vous serez dirigé vers l'interface Web pour le pare-feu). Par exemple, saisissez **`https://myportal`** plutôt que **`https://myportal:4443`**. La page d'ouverture de session du portail s'affiche.
   - **Testez la page d'accueil** : dans le navigateur Web, accédez à l'URL de votre portail (n'ajoutez pas le numéro de port 4443 à la fin de l'URL ; sinon, vous serez dirigé vers l'interface Web pour le pare-feu). Par exemple, saisissez **`https://myportal`** plutôt que **`https://myportal:4443`**. Saisissez votre **Username (Nom d'utilisateur)** et le **Password (Mot de passe)**, puis **LOG IN (CONNECTEZ)**-vous au portail. La nouvelle page d'accueil du portail s'affiche.
   - **Testez la page d'aide** : cliquez sur l'icône du bac système GlobalProtect pour lancer l'application GlobalProtect. Lorsque le panneau d'état s'ouvre, cliquez sur l'icône des paramètres ( ) pour ouvrir le menu des paramètres. Sélectionnez **Help (Aide)** pour afficher la nouvelle page d'aide.
   - **Testez la page d'accueil** : cliquez sur l'icône du bac système GlobalProtect pour lancer l'application GlobalProtect. Lorsque le panneau d'état s'ouvre, cliquez sur l'icône des paramètres ( ) pour ouvrir le menu des paramètres. Sélectionnez **Welcome Page (Page d'accueil)** pour afficher la nouvelle page d'accueil.

 ©2026 Palo Alto Networks, Inc.

Application de GlobalProtect pour l'accès au réseau

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour réduire le risque de sécurité de votre entreprise lorsqu'un utilisateur se trouve hors site, vous pouvez obliger les utilisateurs sur les terminaux fonctionnant sous Windows 7 ou macOS 10.9 et versions ultérieures à se connecter à GlobalProtect pour accéder au réseau.

Lorsque cette fonctionnalité est activée, GlobalProtect bloque tout le trafic jusqu'à ce que l'agent soit interne ou se connecte à une passerelle externe. Une fois que l'agent a établi une connexion, GlobalProtect autorise le trafic réseau interne et externe conformément à votre politique de sécurité, soumettant ainsi le trafic à l'inspection du pare-feu et à l'application de la politique de sécurité. Cette fonctionnalité empêche également l'utilisation de proxys pour contourner le pare-feu et accéder à Internet.

Si les utilisateurs doivent se connecter au réseau via un portail captif (comme dans un hôtel ou un aéroport), vous pouvez également configurer un délai de grâce qui leur laisse suffisamment de temps pour se connecter au portail captif, puis à GlobalProtect.

Étant donné que GlobalProtect bloque le trafic à moins que l'agent GlobalProtect ne puisse se connecter à une passerelle, nous vous recommandons d'activer cette fonctionnalité uniquement pour les utilisateurs qui se connectent en mode connexion utilisateur. Gardez à l'esprit que si vous configurez l'application pour utiliser le mode connexion utilisateur et que l'utilisateur désactive ou se déconnecte de GlobalProtect, il pourra se connecter au réseau car la fonctionnalité d'application ne fonctionne que lorsque GlobalProtect est activé. Pour empêcher les utilisateurs d'accéder au réseau sans connexion GlobalProtect, veillez à ne pas autoriser les utilisateurs en mode connexion utilisateur à désactiver ou à déconnecter GlobalProtect.

1. Configurez le portail GlobalProtect.

2. Créez ou modifiez une configuration d'agent.
   1. Pour créer ou modifier une configuration d'agent, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)** Sur la page Ajouter des paramètres d'application Agent, sélectionnez **App Configuration (Configuration d'application)** > **Show Advanced Options (Afficher les options avancées)** > **Enforcement (Application)**.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de**

 ©2026 Palo Alto Networks, Inc.

l'application) > **<Default>** Sur la page par défaut, sélectionnez **App Configuration (Configuration d'application** > **Show Advanced Options (Afficher les options avancées)** > **Enforcement (Application)**.

- Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** et sélectionnez la configuration de portail pour laquelle vous souhaitez ajouter une configuration client ou **Add (Ajouter)** une nouvelle.

2. À l'onglet **Agent (Agent)**, sélectionnez la configuration de l'agent que vous souhaitez modifier ou **Add (Ajouter)** une nouvelle.
3. Sélectionnez l'onglet **App (Applications)**.

3. Configurez GlobalProtect pour contraindre la totalité du trafic réseau à traverser un tunnel GlobalProtect.

Dans la zone de configuration d'application, définissez **Enforce GlobalProtect Connection for Network access (Appliquer la connexion GlobalProtect pour l(accès au réseau)** sur **Yes (Oui)**. Par défaut, cette option est définie sur **No (Non)**, ce qui signifie que les utilisateurs peuvent toujours accéder à Internet si GlobalProtect est désactivé ou déconnecté.

4. (Facultatif) Pour fournir des informations supplémentaires, configurez un message de notification de blocage du trafic.

Le message peut indiquer la raison du blocage du trafic et fournir des instructions sur la façon de se connecter, telles que `Pour accéder au réseau, vous devez d'abord vous connecter à GlobalProtect`. Si vous activez un message, GlobalProtect affichera ce message lorsque GlobalProtect est déconnecté mais détecte que le réseau est accessible.

1. Dans la zone de configuration d'application, assurez-vous que **Display Captive Portal Detection Message (Afficher le message de détection du portail captif)** est défini sur **Yes (Oui)**. La valeur par défaut est **No (Non)**.
2. Spécifiez le texte du message dans le champ **Display Captive Portal Detection Message (Message de détection du portail captif)**. Le message doit contenir un maximum de 512 caractères.
3. Pour spécifier la durée pendant laquelle l'utilisateur doit s'authentifier avec un portail captif, entrez la **Captive Portal Exception Timeout (Expiration de l'exception du portail captif)** en secondes (par défaut 0 ; plage de 0 à 3 600). Par exemple, une valeur de 60 signifie que l'utilisateur doit se connecter au portail captif dans un délai d'une minute après que GlobalProtect l'ait détecté. Une valeur de 0 signifie que GlobalProtect ne permet pas aux utilisateurs de se connecter à un portail captif et bloque immédiatement l'accès.
4. Si vous activez un **Captive Portal Detection Message (Message de détection de portail captif)**, le message apparaît 85 secondes avant la **Captive Portal Exception Timeout(Expiration de l'exception du portail captif)**. Donc, si la **Capture Portal Exception Timeout (Expiration de l'exception du portail de capture)** est de 90 secondes ou moins, le message apparaît 5 secondes après la détection d'un portail captif.

5. Cliquez deux fois sur **OK** pour enregistrer la configuration du portail, puis sur **Commit (Valider)** pour valider vos modifications.

 ©2026 Palo Alto Networks, Inc.

Application de la stratégie de trafic des points de terminaison

Support logiciel : À partir de l'application GlobalProtect™ version 6.0 avec la version de publication de contenu 8450-6909 ou ultérieure.

Prise en charge du système d'exploitation : Windows 10, Windows 10 basé sur ARM64, macOS 11 et versions ultérieures, et macOS basé sur ARM 11 et versions ultérieures

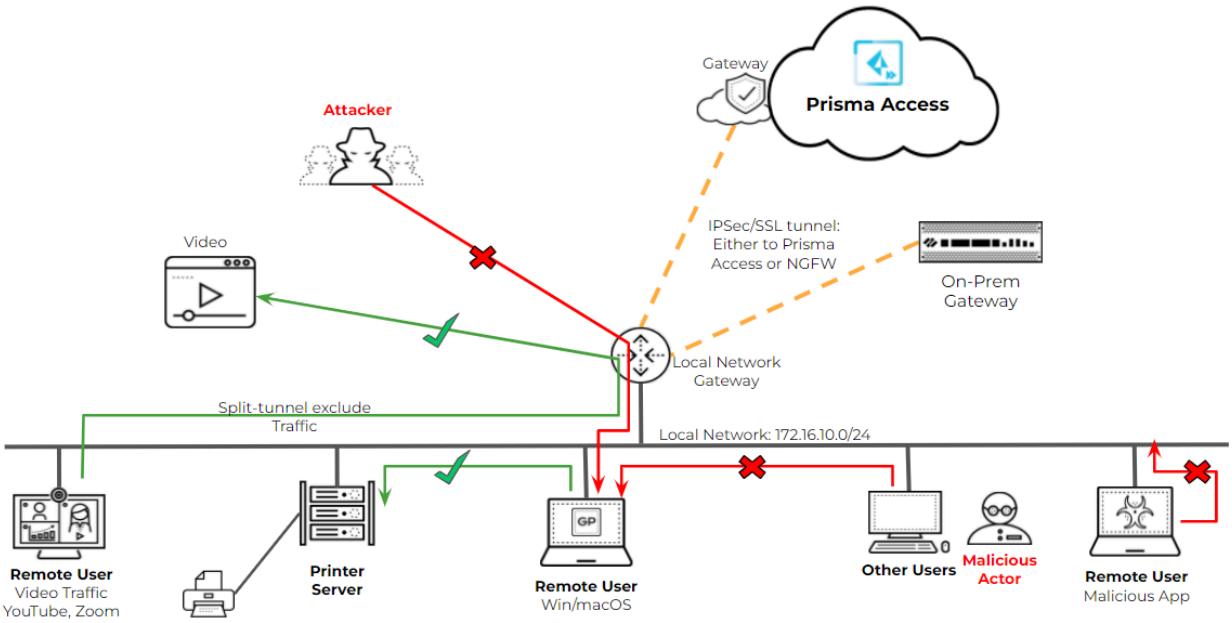
Avec la fonctionnalité d'application de la politique de trafic des terminaux, GlobalProtect offre désormais une sécurité supplémentaire pour protéger votre main-d'œuvre à distance. En appliquant la politique de trafic du terminal sur le terminal GlobalProtect, vous pouvez désormais exécuter les fonctions suivantes :

- Bloquez les connexions entrantes malveillantes en dehors du tunnel VPN pour vous protéger contre l'exfiltration de données.
- Empêchez les applications de contourner le tunnel GlobalProtect en liant leurs connexions directement à l'adaptateur physique sur le point de terminaison distant.
- Empêchez les utilisateurs finaux de falsifier la table de routage pour contourner le tunnel GlobalProtect.

Le diagramme suivant illustre les scénarios d'application de la politique de trafic des terminaux pour bloquer les connexions entrantes malveillantes et empêcher le contournement du tunnel IPSec ou SSL que GlobalProtect construit vers Prisma Access ou vers une passerelle sur le NGFW :

- L'attaquant peut tenter d'établir des connexions entrantes malveillantes vers le terminal distant.
- Un acteur malveillant peut tenter d'effectuer un acte au sein du même réseau local que le terminal GlobalProtect distant.
- Une application peut tenter de lier la connexion directement à l'adaptateur physique sur le terminal de l'utilisateur distant.

 ©2026 Palo Alto Networks, Inc.



Configurer l'application de la politique de trafic des terminaux

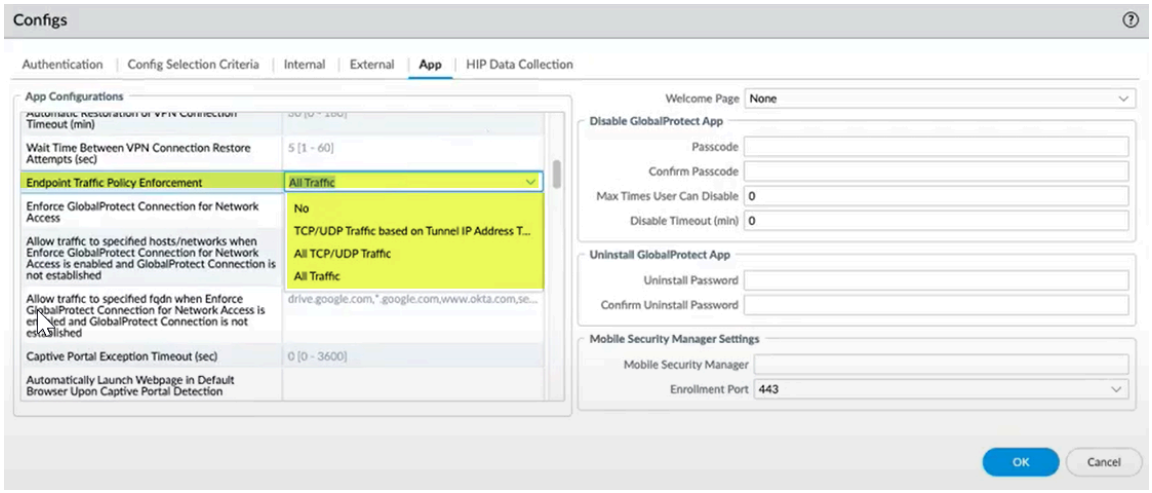
Configurez l'application de la politique de trafic des terminaux pour bloquer les connexions entrantes malveillantes en utilisant l'adaptateur physique sur le terminal distant et empêcher les utilisateurs d'accéder à des applications ou ressources non autorisées après l'établissement du tunnel GlobalProtect.

1. Application de la politique de trafic des terminaux
   1. Lancez l'interface web.
   2. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **App (Application)** > **Endpoint Traffic Policy Enforcement (Application de la politique de trafic des terminaux)**.
   3. Sélectionnez l'une des options suivantes pour l'application de la politique de trafic des terminaux :

Option	Description
Non	Spécifie que la fonctionnalité d'application de la politique de trafic des terminaux est désactivée et que cette fonctionnalité n'est pas appliquée. Ceci est l'option par défaut.
Trafic TCP/UDP basé sur le type d'adresse IP du tunnel	Active l'application de la politique de trafic des terminaux pour le trafic TCP/UDP. Cette fonctionnalité est activée pour le trafic en fonction du type d'adresse IP du tunnel. Si le tunnel est IPv4, cette fonctionnalité s'applique uniquement au trafic IPv4. Si le tunnel est IPv6,

 ©2026 Palo Alto Networks, Inc.

Option	Description
	cette fonctionnalité s'applique uniquement au trafic IPv6.
Tout le trafic TCP/UDP	Active l'application de la politique de trafic des terminaux pour tout le trafic TCP/UDP, quel que soit le type d'adresse IP du tunnel. Si le type d'adresse IP du tunnel est IPv4, l'application de la stratégie de trafic du point de terminaison s'applique à tout le trafic TCP/UDP (IPv4 ou IPv6). Si le type d'adresse IP du tunnel est IPv6, l'application de la stratégie de trafic du point de terminaison s'applique à tout le trafic TCP/UDP (IPv4 ou IPv6).
Tout le trafic	Active l'application de la politique de trafic des terminaux pour tous les protocoles TCP, UDP, ICMP et tous les autres protocoles, quel que soit le type d'adresse IP du tunnel.



2. Enregistrer la configuration.
   1. Cliquez deux fois sur **OK**.
   2. **Commit (Validez)** la configuration.

 ©2026 Palo Alto Networks, Inc.

3. Vérifiez la configuration de l'application de la politique de trafic des terminaux.

   Vous pouvez vérifier l'option d'application de la politique de trafic des terminaux dans le fichier journal du service GlobalProtect (PanGPS).

   L'exemple suivant montre l'entrée dans le fichier journal PanGPS :

   ```
   <traffic-enforcement>tcp-udp-with-tunnel-address-type</traffic-enforcement>
   ```

   Pour vérifier que la fonctionnalité fonctionne comme prévu générer une capture de paquet à la fois sur l'adaptateur physique et l'adaptateur GlobalProtect depuis la machine client tout en étant connecté à GlobalProtect, puis essayez d'accéder à des sites web ou des ressources pour vérifier que le trafic est appliqué comme prévu en fonction de votre configuration.

Application de la politique de trafic des terminaux sans accès direct au réseau local

Vous pouvez utiliser l'application de la politique de trafic des terminaux en conjonction avec le support d'accès direct au réseau local pour contrôler l'accès au réseau local. Le tableau suivant montre le comportement du trafic et l'interaction entre les fonctionnalités.

Trafic IPv4 et IPv6	Stratégie de trafic des terminaux appliquée Aucun accès direct au réseau local est désactivé		Stratégie de trafic des terminaux appliquée Aucun accès direct au réseau local est activé	
	Avant l'établissement du tunnel	Après l'établissement du tunnel	Avant l'établissement du tunnel	Après l'établissement du tunnel
Nouveau trafic entrant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic du sous-réseau local est exclu. Le trafic de retour du sous-réseau local ne sera pas supprimé sur l'interface non tunnel.	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic de retour est supprimé sur l'adaptateur physique à moins que la segmentation du tunnel ne soit configurée pour exclure le trafic en fonction des conditions suivantes : • Itinéraires d'accès • (Windows uniquement) Applications

 ©2026 Palo Alto Networks, Inc.

Trafic IPv4 et IPv6	Stratégie de trafic des terminaux appliquée Aucun accès direct au réseau local est désactivé		Stratégie de trafic des terminaux appliquée Aucun accès direct au réseau local est activé	
				• Exclure le trafic de diffusion vidéo
Nouveau trafic sortant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est envoyé à travers le tunnel VPN à moins que l'adresse IP de destination ne corresponde aux exclusions suivantes pour la segmentation du tunnel : • Itinéraires d'accès • Domaines et applications de destination • Exclure le trafic de diffusion vidéo • Destiné au sous-réseau local qui est récupéré lorsque le tunnel est établi	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est envoyé via le tunnel VPN sauf si l'adresse IP de destination correspond aux exclusions suivantes pour la segmentation du tunnel : • Itinéraires d'accès • Domaines de destination et applications • Exclure le trafic de diffusion vidéo
Trafic existant	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est interrompu sauf si l'adresse IP de destination correspond aux exclusions suivantes pour la segmentation du tunnel : • Itinéraires d'accès • Domaines de destination [1]	Le trafic est autorisé à entrer sur le sous-réseau local par l'intermédiaire de l'adaptateur physique.	Le trafic est interrompu sauf si l'adresse IP de destination correspond aux exclusions suivantes pour la segmentation du tunnel : • Itinéraires d'accès • Domaines de destination [1]

 ©2026 Palo Alto Networks, Inc.

Trafic IPv4 et IPv6	Stratégie de trafic des terminaux appliquée Aucun accès direct au réseau local est désactivé		Stratégie de trafic des terminaux appliquée Aucun accès direct au réseau local est activé	
		• (Windows uniquement) Applications • Exclure le trafic de diffusion vidéo • Destiné au sous-réseau local qui est récupéré lorsque le tunnel est établi.		• (Windows uniquement) Applications • Exclure le trafic de diffusion vidéo

[1] Les domaines de destination ne fonctionneront pas pour les connexions existantes qui ont commencé avant l'établissement de la connexion GlobalProtect car GlobalProtect n'a pas de visibilité associée au DNS. Cependant, ce comportement de trafic fonctionnera pour les connexions existantes lors des reconnexions GlobalProtect car GlobalProtect peut surveiller le DNS lors de l'intervalle de reconnexion.

Cas pratiques de l'application de la politique de trafic des terminaux

L'application de la politique de trafic des terminaux prend en charge les cas d'utilisation suivants :

Empêcher tout le trafic de contourner le tunnel

Aucun trafic ne peut contourner le tunnel après l'établissement de connexions entrantes ou sortantes. Lorsque la fonctionnalité d'accès direct aux réseaux locaux est désactivée en conjonction avec la fonctionnalité d'application de la politique de trafic des terminaux, les utilisateurs mobiles ne peuvent pas accéder directement aux proxys et aux ressources locales (telles que les imprimantes locales) lorsque le trafic passe par le tunnel VPN pour inspection et application de la politique tout en étant activé sur GlobalProtect.

1. Activez **No direct access to local network (Aucun accès direct au réseau local)** (**Agent** > **Client Settings (Paramètres client)** <***client-setting-config***> > **Split Tunnel (Segmentation de tunnel)** > **Access Route (Itinéraire d'accès)**).
2. Définissez **Endpoint Traffic Policy Enforcement (Application de la politique de trafic des terminaux)** sur **All Traffic (Tout le trafic)**.

Exclure les domaines consommant beaucoup de bande passante tout en empêchant le trafic du sous-réseau local

En activant la fonctionnalité d'accès direct aux réseaux locaux en conjonction avec l'application de la politique de trafic des terminaux, vous pouvez exclure les domaines consommant beaucoup de

 ©2026 Palo Alto Networks, Inc.

bande passante du tunnel tout en bloquant le trafic du sous-réseau local. Dans ce cas d'utilisation, les utilisateurs mobiles ne peuvent pas accéder directement aux proxys et aux ressources locales (telles que les imprimantes locales) lorsque le trafic passe par le tunnel VPN pour inspection et application de la politique tout en étant connectés à GlobalProtect. En excluant le trafic de segmentation de tunnel basé sur le domaine, tout le trafic pour ce domaine spécifique est envoyé directement à l'adaptateur physique sur le terminal sans inspection.

1. Activez **No direct access to local network (Aucun accès direct au réseau local)** (**Agent** > **Client Settings (Paramètres client)** <***client-setting-config***> > **Split Tunnel (Segmentation de tunnel)** > **Access Route (Itinéraire d'accès)**).
2. Configurez la segmentation de tunnel pour exclure le trafic à forte bande passante tel que la vidéo du tunnel.
3. Définissez **Endpoint Traffic Policy Enforcement (Application de la politique de trafic des terminaux)** sur **All Traffic (Tout le trafic)**.

Autoriser le trafic local tout en empêchant le trafic sur l'adaptateur physique

Le trafic est envoyé via le tunnel VPN et les utilisateurs finaux peuvent accéder directement aux ressources locales (telles que les imprimantes). Lorsque la fonctionnalité Aucun accès direct au support réseau local est désactivée et que la fonctionnalité Application de la politique de trafic des terminaux est activée, les utilisateurs mobiles peuvent accéder directement aux proxys et aux ressources locales (telles que les imprimantes locales) lorsque tout le trafic passe par le tunnel VPN pour inspection et application de la politique lorsqu'ils sont connectés à GlobalProtect. Si un acteur malveillant tente d'effectuer un acte au sein du même réseau local que le terminal GlobalProtect distant, des connexions entrantes malveillantes peuvent être envoyées directement à l'adaptateur physique sur le terminal de l'utilisateur mobile.

1. Désactivez **No direct access to local network (Aucun accès direct au réseau local)** dans **Agent** > **Client Settings (Paramètres client)** <***client-setting-config***> > **Split Tunnel (Segmentation de tunnel)** > **Access Route (Itinéraire d'accès)**.
2. Définissez **Endpoint Traffic Policy Enforcement (Application de la politique de trafic des terminaux)** sur **All Traffic (Tout le trafic)**.

Exclure les domaines consommant beaucoup de bande passante et permettre l'accès aux ressources locales tout en empêchant le trafic sur l'adaptateur physique

Les domaines consommant beaucoup de bande passante sont exclus mais les utilisateurs finaux peuvent accéder directement aux ressources locales (telles que les imprimantes locales) et certains trafics sont envoyés via le tunnel VPN. Lorsque la fonctionnalité Aucun accès direct au support réseau local est désactivée en conjonction avec l'Application de la politique de trafic des terminaux, qu'elle soit activée ou désactivée, les utilisateurs mobiles peuvent accéder directement aux proxys et aux ressources locales (telles que les imprimantes locales) lorsque le trafic vers le réseau de l'entreprise passe par le tunnel VPN pour inspection et application de la politique tout en étant activé sur GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

1. Désactivez **No direct access to local network (Aucun accès direct au réseau local)** dans **Agent** > **Client Settings (Paramètres client)** <***client-setting-config***> > **Split Tunnel (Segmentation de tunnel)** > **Access Route (Itinéraire d'accès)**.
2. Configurez la segmentation du tunnel pour exclure les domaines et applications consommant beaucoup de bande passante, comme la vidéo.
3. Définissez **Endpoint Traffic Policy Enforcement (Application de la stratégie de trafic des points de terminaison)** pour empêcher **All TCP/UDP Traffic (Tout le trafic TCP/UDP)**, **TCP/UDP Traffic Based on Tunnel IP Address Type (Trafic TCP/UDP basé sur le type d'adresse IP du tunnel)**, ou **All Traffic (Tout le trafic)** sur l'adaptateur physique.

Limitations des fonctionnalités

Ls limites suivantes s'appliquent :

- Les requêtes ICMP ne sont pas prises en charge pour le tunnel fractionné basé sur le domaine ou l'application ou pour l'application de la politique de trafic des terminaux.
- Vous ne pouvez pas exclure le trafic de segmentation de tunnel en fonction des applications côté serveur pour les connexions entrantes.
- Les paquets d'établissement de la connexion TCP sont contournés. Certains paquets TCP ACK sans données peuvent être vus dans les données de capture de paquet.
- Les exclusions pour les domaines de destination peuvent ne pas fonctionner pour les nouvelles connexions entrantes sans la requête DNS ou la réponse DNS car GlobalProtect ne connaîtra pas l'adresse IP du domaine de destination.
- (macOS uniquement) Les exclusions pour les applications ne fonctionneront pas pour les nouvelles connexions entrantes et les connexions existantes.
- (macOS uniquement) Le trafic est autorisé sur les ports TCP 53 et 5353.
- (Windows uniquement) Le trafic DHCP (port distant UDP 67) et DNS (port distant UDP 53) est autorisé.
- La fonctionnalité ne peut pas être utilisée pour le réseau en mode pont ou pour les contrôles de Couche 2. Vous pouvez interdire l'utilisation du mode pont pour les applications de machine virtuelle sur vos terminaux pour contourner cette limitation ou utiliser un réseau standard de Couche 3 avec NAT.

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

Applications GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

L'application GlobalProtect™ fonctionne sur les terminaux de vos utilisateurs (ordinateur de bureau, ordinateur portable, tablette ou smartphone) pour étendre la politique de sécurité que vous utilisez sur votre réseau d'entreprise à vos utilisateurs mobiles afin de garantir que leur trafic est sécurisé, qu'ils accèdent à des ressources dans votre centre de données, votre cloud privé, votre cloud public ou sur Internet.

En plus de fournir une connectivité sécurisée et un accès à distance comme les produits VPN traditionnels, l'application GlobalProtect :

- Protège vos réseaux internes
- Fournit un contrôle au niveau des applications et des services
- Sécurise les périphériques IdO
- Protège contre la perte de données et le vol d'identifiants
- Assure une prévention avancée des menaces
- Permet la mise en quarantaine automatique des périphériques compromis

Pour voir quels systèmes d'exploitation de terminal sont pris en charge par chaque version de l'application GlobalProtect, consultez la Matrice de compatibilité. Après avoir décidé quelles versions d'application vous souhaitez prendre en charge pour vos utilisateurs, vous pouvez Déployer l'application GlobalProtect sur les ordinateurs de bureau. Vous pouvez aussi personnaliser le comportement de l'application lorsque vous configurez la passerelle, ou vous pouvez Déployer les paramètres d'application de façon transparente.

Déployer l'application GlobalProtect sur les ordinateurs de bureau

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Pour se connecter à GlobalProtect™, un terminal doit exécuter l'application GlobalProtect. Utilisez la matrice de compatibilité de l'application GlobalProtect pour déterminer quelle version de l'application GlobalProtect vous souhaitez que vos utilisateurs exécutent sur leurs terminaux. Parce que la version que l'utilisateur final doit télécharger et installer pour permettre une connectivité réussie à votre réseau dépend de votre environnement, il n'y a pas de lien de téléchargement direct pour l'application GlobalProtect sur le site de Palo Alto Networks.

La méthode de déploiement de l'application dépend des types de terminaux suivants :

Platform (Plateforme)	Options de déploiement
postes de travail macOS et Windows	Plusieurs options s'offrent à vous pour distribuer et installer le logiciel sur les postes de travail macOS et Windows : • **Directement via le portail** : Téléchargez le logiciel de l'application sur le pare-feu hébergeant le portail, puis activez-le pour que les utilisateurs finaux puissent installer les mises à jour logicielles lorsqu'ils se connectent au portail. Cette option procure une grande flexibilité en vous autorisant à contrôler comment et à quel moment les utilisateurs finaux reçoivent les mises à jour basées sur les paramètres de configuration de client que vous définissez pour chaque utilisateur, groupe, et/ou système d'exploitation. Toutefois, si un grand nombre d'applications exigent des mises à jour, cela pourrait alourdir la charge confiée à votre portail. Consultez les mises à jour de l'application hôte sur le portail pour obtenir des instructions. • **Sur un serveur Web** : Si un grand nombre de vos points de terminaison ont besoin de mettre à niveau l'application simultanément, songez à héberger les mises à jour logicielles sur un serveur Web pour réduire la charge confiée au pare-feu. Consultez les mises à jour de l'application hôte sur un serveur Web pour obtenir des instructions. • **Mode transparent depuis la ligne de commande** : Pour les points de terminaison Windows, vous pouvez déployer automatiquement les paramètres de l'application dans le programme d'installation Windows (Msiexec). Toutefois, pour mettre à niveau vers une version ultérieure de l'application à l'aide de Msiexec, vous devez d'abord désinstaller l'application existante. En outre, Msiexec autorise le déploiement des paramètres de l'application directement sur les points de

 ©2026 Palo Alto Networks, Inc.

Platform (Plateforme)	Options de déploiement
	terminaison en définissant les valeurs dans le registre Windows. De même, vous pouvez également déployer les paramètres d'application sur des postes de travail macOS en configurant les paramètres dans la plist macOS. Voir la section Déployer les paramètres de l'application de manière transparente. • **Utilisation de règles de politique de groupe** : dans les environnements Active Directory, l'application GlobalProtect peut aussi être distribuée chez les utilisateurs finaux, en ayant recours à une stratégie de groupe Active Directory. Les stratégies de groupe Active Directory permettent la modification automatisée des paramètres et du logiciel des points de terminaison Windows. Consultez l'article disponible à l'adresse http://support.microsoft.com/kb/816102 pour obtenir d'autres informations sur l'utilisation des stratégies de groupe AD pour distribuer automatiquement des programmes à des points de terminaison ou à des utilisateurs. • **À partir d'un système de gestion de terminaux mobiles**, si vous utilisez un système de gestion mobile comme un MDM ou un EMM pour gérer vos points de terminaison mobiles, vous pouvez utiliser le système pour déployer et configurer l'application GlobalProtect. Reportez-vous à la section Aperçu de la gestion des périphériques mobiles.
Téléphone Windows 10 et terminaux UWP Windows 10	• **À partir d'un système de gestion de terminaux mobiles**, si vous utilisez un système de gestion mobile, comme un MDM ou un EMM, qui prend en charge les points de terminaison Windows 10, vous pouvez utiliser le système pour déployer et configurer l'application GlobalProtect. Consultez Aperçu de la gestion des périphériques mobiles.. • **À partir du Microsoft Store** : l'utilisateur final peut également télécharger et installer l'application GlobalProtect GlobalProtect directement à partir du Microsoft Store. Pour obtenir des instructions sur la façon de télécharger et de tester l'installation de l'application GlobalProtect, reportez-vous à la section Télécharger et installer l'application mobile GlobalProtect.
Points de terminaison iOS et Android	• **À partir d'un système de gestion de terminaux mobiles**, si vous utilisez un système de gestion mobile, comme un MDM ou un EMM, vous pouvez utiliser le système pour déployer et configurer l'application GlobalProtect. Consultez Aperçu de la gestion des périphériques mobiles.. • **À partir d'un app store** : l'utilisateur final peut également télécharger et installer l'application GlobalProtect directement à partir de l'Apple App Store (points de terminaison iOS) ou de Google Play (points de terminaison Android). Pour obtenir des instructions sur la façon de télécharger et de tester l'installation

 ©2026 Palo Alto Networks, Inc.

Platform (Plateforme)	Options de déploiement
	de l'application GlobalProtect, reportez-vous à la section Télécharger et installer l'application mobile GlobalProtect.
Chromebooks	• **À partir de la console Google Admin** : La console Google Admin vous permet de gérer les paramètres et les applications Chromebook à partir d'un emplacement central et basé sur le Web. Pour déployer l'application GlobalProtect pour Android sur des Chromebooks gérés en utilisant la console d'administration Google, consultez Déployer l'application GlobalProtect pour Android sur les Chromebooks gérés à l'aide de la console Google Admin.. *L'application GlobalProtect pour Android n'est prise en charge que sur certains Chromebooks. Les Chromebooks qui ne prennent pas en charge les applications Android doivent continuer à exécuter l'application GlobalProtect pour Chrome, qui n'est pas prise en charge à partir de l'application GlobalProtect 5.0 et versions ultérieures.* • **Depuis Workspace ONE** : vous pouvez déployer l'application GlobalProtect pour Android sur les Chromebooks gérés qui sont inscrits auprès de Workspace ONE. Après avoir déployé l'application, configurez et déployez un profil VPN pour configurer automatiquement l'application GlobalProtect pour les utilisateurs finaux. Pour déployer l'application GlobalProtect pour Android sur des Chromebooks gérés en utilisant Workspace ONE, consultez Déployer l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide de Workspace ONE..
Linux	Après avoir téléchargé l'application GlobalProtect pour Linux sur le Site de support, vous pouvez la distribuer et l'installer : • **En utilisant les outils de distribution de l'application Linux** : la distribution de l'application pour Linux est généralement gérée au moyen d'outils tiers (comme Chef et Puppet) ou à l'aide d'un référentiel local pour le système d'exploitation Linux (par exemple, référentiels Ubuntu et référentiels RHEL). Consultez la documentation relative à votre système d'exploitation Linux pour obtenir de plus amples informations. • **Installation manuelle** : si vous mettez le logiciel à la disposition de vos utilisateurs finaux, ces derniers peuvent l'installer manuellement en utilisant les outils Linux, comme **`apt`** ou **`dpkg`**. Pour obtenir des instructions sur l'installation de l'application GlobalProtect pour Linux, consultez le Guide de l'utilisateur de l'application GlobalProtect.

Au lieu de déployer le logiciel de l'application GlobalProtect, vous pouvez configurer le portail GlobalProtect pour fournir un accès distant sécurisé aux applications Web d'entreprise communes qui utilisent les technologies HTML, HTML5 et JavaScript. Les utilisateurs ont

 ©2026 Palo Alto Networks, Inc.

l'avantage d'un accès sécurisé à partir de navigateurs Web sur lesquels SSL est activé sans installer le logiciel de l'application GlobalProtect. Reportez-vous à VPN sans client GlobalProtect.

Configuration matérielle minimale requise pour l'application GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

L'application GlobalProtect fonctionne avec une variété de systèmes d'exploitation. Pour déterminer la version minimale de l'application GlobalProtect requise pour un système d'exploitation spécifique, reportez-vous à la matrice de compatibilité. La configuration matérielle requise pour chaque système d'exploitation de terminal est détaillée dans les sections suivantes :

- Configuration matérielle minimale requise pour l'application GlobalProtect sur Windows
- Configuration matérielle minimale requise pour l'application GlobalProtect sur macOS
- Configuration matérielle minimale requise pour l'application GlobalProtect sur Linux

Configuration matérielle minimale requise pour l'application GlobalProtect sur Windows

Vous pouvez installer l'application GlobalProtect sur les terminaux Windows qui répondent aux exigences matérielles suivantes :

Exigence	Spécification
Processeur	• Intel Pentium 4 ou ultérieur avec prise en charge de jeu d'instructions SSE2 • AMD Opteron/Athlon 64 ou ultérieur avec prise en charge de jeu d'instructions SSE2 • Processeur double cœur (minimum)
Mémoire RAM	2 Go minimum
Espace disque	200 Mo minimum (pour le stockage des journaux)

Configuration matérielle minimale requise pour l'application GlobalProtect sur macOS

Vous pouvez installer l'application GlobalProtect sur les terminaux macOS qui répondent aux exigences matérielles suivantes :

Exigence	Spécification
Processeur	• Intel Pentium 4 ou ultérieur avec prise en charge de jeu d'instructions SSE2

 ©2026 Palo Alto Networks, Inc.

Exigence	Spécification
	• AMD Opteron/Athlon 64 ou ultérieur avec prise en charge de jeu d'instructions SSE2 • Périphériques basés sur macOS avec Apple Silicon M1
Mémoire RAM	512 Mo minimum ; 2 Go recommandés
Espace disque	200 Mo minimum (pour le stockage des journaux)

Configuration matérielle minimale requise pour l'application GlobalProtect sur Linux

Vous pouvez installer l'application GlobalProtect sur les terminaux macOS qui répondent aux exigences matérielles suivantes :

La prise en charge des terminaux Linux nécessite également une licence GlobalProtect Gateway.

Exigence	Spécification
Processeur	Ensemble d'instructions x86 avec processeur 64 bits
Mémoire RAM	256 Mo minimum
Espace disque	100 Mo minimum

Télécharger le package logiciel de l'application GlobalProtect pour l'hébergement sur le portail

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Palo Alto Networks ne fournit pas de lien de téléchargement direct pour l'application GlobalProtect pour les utilisateurs finaux. Pour bien se connecter à votre réseau, les utilisateurs finaux doivent exécuter une version de l'application qui est compatible avec votre environnement. *Après avoir décidé quelle version de l'application vous allez prendre en charge pour chaque système d'exploitation, vous pouvez* Déployer l'application GlobalProtect sur les ordinateurs de bureau. *Si vous êtes un utilisateur final, veuillez contacter votre administrateur TI pour obtenir la version la plus récente du logiciel GlobalProtect.*

Avant de pouvoir déployer l'application GlobalProtect auprès de vos utilisateurs finaux, vous devez télécharger la nouvelle offre groupée d'installation de l'application sur le pare-feu qui héberge votre portail, puis activer le logiciel pour le télécharger sur les applications qui se connectent au portail. Ce mode de déploiement est offert pour toutes les versions de l'application qui ne sont pas conçues pour les appareils mobiles. Pour télécharger la version pour mobile de l'application GlobalProtect, accédez au magasin d'applications de votre périphérique mobile

 ©2026 Palo Alto Networks, Inc.

(pour de plus amples informations, reportez-vous à la section Télécharger et installer l'application mobile GlobalProtect).

Pour télécharger la dernière version de l'application directement sur le pare-feu, le pare-feu doit avoir un itinéraire de service qui l'autorise à accéder au serveur de mise à jour Palo Alto Networks (reportez-vous à la section Déployer l'application GlobalProtect sur les ordinateurs de bureau). Si le pare-feu n'a pas accès à Internet, vous pouvez télécharger le progiciel de l'application sur le site de support Mises à jour logicielles de Palo Alto Networks en utilisant un ordinateur connecté à Internet puis manuellement le transférer sur le pare-feu.

Pour télécharger manuellement le progiciel de l'application :

1. Connectez-vous au portail de support client de Palo Alto Networks (https://support.paloaltonetworks.com/).

   Vous devez disposer d'un compte valide sur le portail du support client de Palo Alto Networks pour vous connecter et télécharger des logiciels à partir de la page Mises à jour logicielles.

2. Sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.

3. Sélectionnez la version de l'application GlobalProtect par système d'exploitation.

4. Passez en revue les Notes de version de la version de l'application, puis sélectionnez le lien de téléchargement pour procéder au téléchargement.

5. Déployer l'application GlobalProtect sur les ordinateurs de bureau.

   Reportez-vous à la Grille de compatibilité Palo Alto Networks pour connaître les systèmes d'exploitation sur lesquels vous pouvez installer chaque version de l'application GlobalProtect.

Mises à jour de l'application hôte

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Le moyen le plus simple pour déployer le logiciel de l'application GlobalProtect consiste à télécharger la nouvelle offre groupée d'installation de l'application sur le pare-feu qui héberge votre portail puis à activer le logiciel pour le télécharger sur les applications qui se connectent au portail. Pour procéder automatiquement, le pare-feu doit avoir un itinéraire de service qui l'autorise à accéder au serveur de mise à jour Palo Alto Networks. Si le pare-feu n'a pas accès à Internet, vous pouvez Télécharger le package logiciel de l'application GlobalProtect pour l'hébergement sur le portail le progiciel de l'application sur le site de support Mises à jour logicielles de Palo Alto Networks en utilisant un ordinateur connecté à Internet puis manuellement le transférer sur le pare-feu.

Si un grand nombre de vos points de terminaison doivent installer et/ou mettre à jour le logiciel de l'application GlobalProtect, songez à héberger les images du logiciel de l'application GlobalProtect sur un serveur Web externe. Cela permet de réduire la charge confiée au pare-feu quand les utilisateurs se connectent pour télécharger l'application.

- Portail

 ©2026 Palo Alto Networks, Inc.

- Serveur web

Héberger les mises à jour de l'application sur le portail

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Vous définissez les conditions selon lesquelles les mises à jour logicielles de l'application sont déployées dans la configuration de l'agent que vous définissez sur le portail : si elles doivent arriver automatiquement quand l'application se connecte au portail, si l'utilisateur doit être invité à mettre à niveau l'application, ou si l'utilisateur final peut manuellement vérifier et télécharger une nouvelle version de l'application. Pour plus d'informations sur la création d'une configuration d'agent, consultez définir les configurations de l'agent GlobalProtect.

1. Sur le pare-feu hébergeant le portail GlobalProtect, vérifiez la présence de nouvelles images du logiciel de l'application.

   Sélectionnez **Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)** pour afficher la liste des images de logiciel de l'application qui sont disponibles.

   - Si le pare-feu a accès au serveur de mises à jour, cliquez sur **Check Now (Vérifier maintenant)** pour rechercher les dernières mises à jour. Si la valeur figurant dans la colonne **Action** est **Download (Télécharger)**, une nouvelle version de l'application est disponible.
   - Si le pare-feu n'a pas accès au serveur de mises à jour, vous devez manuelle télécharger l'image du logiciel à partir du site de support Mises à jour logicielles de Palo Alto Networks, comme décrit à l'étape 2.

2. Téléchargez l'image du logiciel de l'application.

   - Si le serveur a accès au serveur de mises à jour, repérez la version de l'application que vous voulez, puis cliquez sur **Download (Télécharger)**. Une fois le téléchargement terminé, la valeur figurant dans la colonne **Action** passe à **Activate (Activer)**.
   - Si le pare-feu n'a pas accès au serveur de mises à jour, Télécharger le package logiciel de l'application GlobalProtect pour l'hébergement sur le portail. Après avoir téléchargé l'image du logiciel, revenez à la page **Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)** du pare-feu pour la **Upload (Charger)**.

3. Activez l'image du logiciel de l'application pour que les utilisateurs finaux puissent la télécharger depuis le portail.

   Une seule version de l'image du logiciel de l'application peut être activée à la fois. Si vous activez une nouvelle version, mais que certains de vos applications exigent une version précédemment activée, vous devez activer la version requise afin d'autoriser son téléchargement.

   - Si l'image du logiciel a automatiquement été téléchargée depuis le serveur de mises à jour, cliquez sur **Activate (Activer)**.
   - Si vous avez téléchargé manuellement l'image du logiciel sur le pare-feu, cliquez sur **Activate From File (Activer depuis le fichier)**, puis sélectionnez le **GlobalProtect Client File (Client de fichier GlobalProtect)** que vous avez téléchargé depuis la liste déroulante. Cliquez

 ©2026 Palo Alto Networks, Inc.

sur **OK** pour activer l'image sélectionnée. Vous aurez peut-être besoin de rafraîchir la page avant que la version s'affiche comme étant **Currently Activated (Actuellement activée)**.

Héberger les mises à jour de l'application sur un serveur Web

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

1. Téléchargez et activez la version de l'application GlobalProtect que vous envisagez d'héberger sur le serveur Web sur le pare-feu.

   Suivez les étapes de téléchargement et d'activation de l'application sur le pare-feu comme décrit dans les mises à jour de l'application hôte sur le portail.

2. Téléchargez l'image du logiciel de l'application GlobalProtect que vous souhaitez héberger sur votre serveur Web.

   Téléchargez cette même image que vous avez activée sur le portail.

   À partir d'un navigateur web, Télécharger le package logiciel de l'application GlobalProtect pour l'hébergement sur le portail.

3. Publiez l'image du logiciel sur votre serveur Web.

4. Redirigez les utilisateurs finaux vers le serveur Web.

   Sur le pare-feu hébergeant le portail, saisissez les commandes CLI suivantes en mode opérationnel :

   ```
   > définir la redirection global-protect activée > définir
    l'emplacement de redirection global-protect <path>
   ```

   où <*path*> est le chemin de l'URL jusqu'au dossier hébergeant l'image (par exemple **`https://acme/GP`**).

5. Testez la redirection.

   1. À partir d'un navigateur Web, accédez à l'URL suivante :

      ```
      https://<portal address or name>
      ```

      Par exemple, **`https://gp.acme.com`**.

   2. Sur la page d'ouverture de session du portail, saisissez vos **Name (Nom)** et **Password (Mot de passe)** d'utilisateur puis cliquez sur **LOGIN (Ouvrir une session)**. Dès l'ouverture de la session, le portail doit vous rediriger pour le téléchargement.

 ©2026 Palo Alto Networks, Inc.

Tester l'installation de l'application

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Utilisez la procédure suivante pour tester l'installation de l'application GlobalProtect.

1. Créez une configuration d'agent pour tester l'installation de l'application.

   Lors de l'installation initiale de l'application logicielle GlobalProtect sur le point de terminaison, l'utilisateur final doit être connecté au système en utilisant un compte doté de privilèges administratifs. Les mises à jour logicielles ultérieures n'exigent pas de privilèges administratifs.

   Idéalement, créez une configuration d'agent qui est limitée à un petit groupe d'utilisateurs, tels que les administrateurs du service informatique responsables de l'administration du pare-feu.

   1. Pour ajouter un nouveau portail ou modifier un portail existant, effectuez l'une des actions suivantes :
      - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**. Sélectionnez une configuration de portail existante que vous souhaitez modifier ou en **Add (Ajouter)** une nouvelle pour déployer sur les utilisateurs/groupes de test.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Portals (Portails)** puis **Add Portal (Ajouter un portail)**.
   2. À l'onglet **Agent**, sélectionnez une configuration existante ou **Add (Ajoutez)**-en une nouvelle à déployer sur les utilisateurs / le groupe de test.
   3. Ajoutez le **User/User Group (Utilisateur/Groupe d'utilisateurs)** qui testera l'application.
      - Sur Panorama, dans l'onglet **User/User Group (Utilisateur/Groupe d'utilisateurs)**, **Add (Ajouter)** le **User/User Group (Utilisateur/Groupe d'utilisateurs)**.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs et groupes locaux)**
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs et groupes locaux)**.
   4. À l'onglet **App**, définissez l'option **Allow User to Upgrade GlobalProtect App (Autoriser l'utilisateur à mettre à jour l'application GlobalProtect)** sur **Allow with Prompt (Autoriser avec invite)**. Cliquez sur **OK** pour enregistrer la configuration.

 ©2026 Palo Alto Networks, Inc.

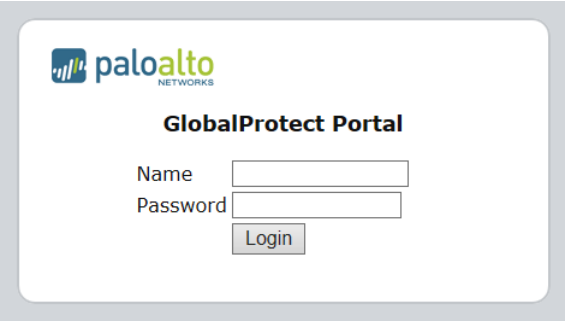
5. (Facultatif) À l'onglet **Agent**, sélectionnez la configuration d'agent que vous venez de créer ou de modifier, puis cliquez sur **Move Up (Déplacer vers le haut)** afin qu'il figure, dans la liste, avant toute configuration plus générique que vous avez créée.

   Dès qu'une application GlobalProtect se connecte, le portail compare les informations sources dans le paquet aux configurations d'agent que vous avez définies. Comme avec l'évaluation des règles de sécurité, les portails recherchent une correspondance en commençant par le début de la liste. Lorsqu'il trouve une correspondance, il fournit la configuration correspondante à l'application.
6. **Commit (Validez)** les modifications.

2. Connectez-vous au portail GlobalProtect.
   1. Lancez votre navigateur Web et accédez à l'URL suivante :

      ```
      https://<portal address or name>
      ```

      Par exemple, **`https://gp.acme.com`**.
   2. Sur la page d'ouverture de session du portail, saisissez vos **Name (Nom)** et **Password (Mot de passe)** d'utilisateur puis cliquez sur **LOG IN (Ouvrir une session)**.



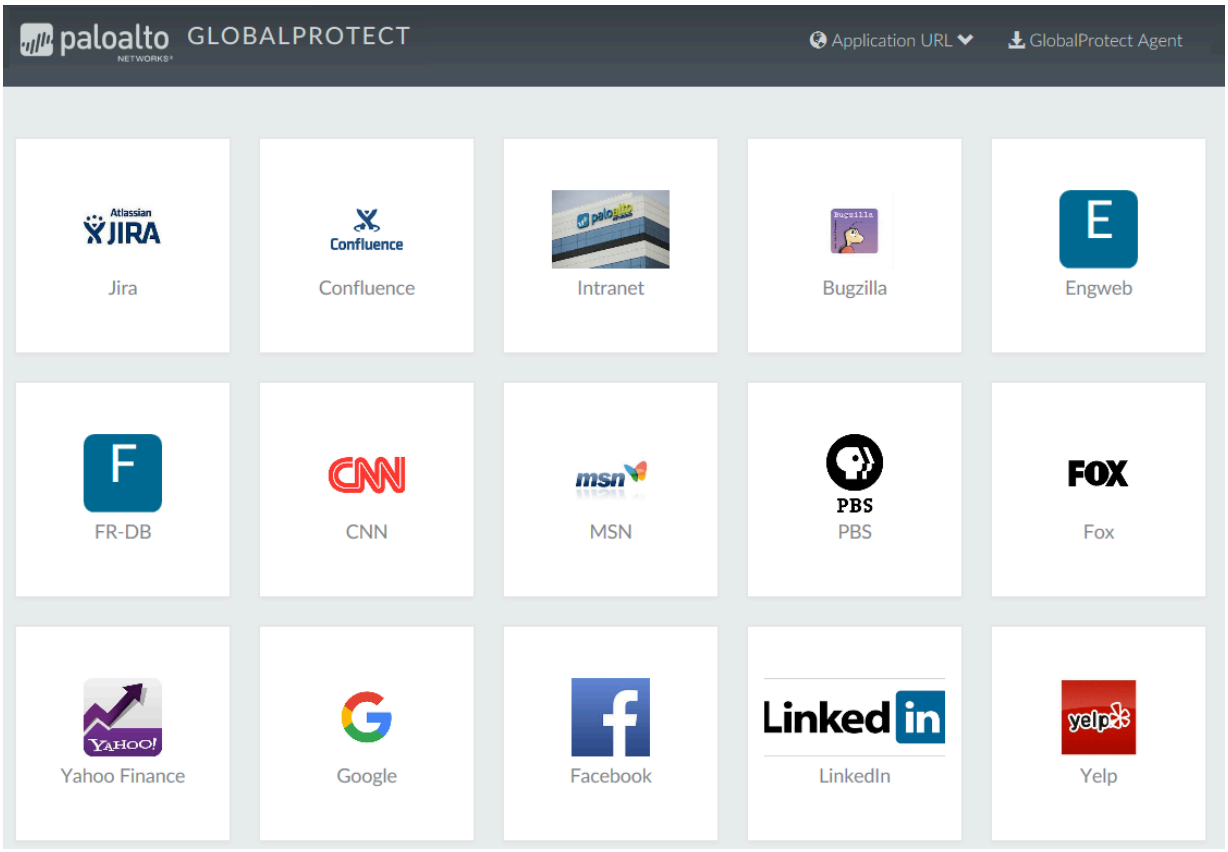
 ©2026 Palo Alto Networks, Inc.

3. Accédez à la page de téléchargement de l'application.

   Dans la plupart des cas, la page de téléchargement de l'application apparaît immédiatement après que vous vous soyez connecté au portail. Utilisez cette page pour télécharger le dernier package logiciel de l'application.

   Si vous avez activé l'accès VPN sans client GlobalProtect, la page d'applications s'ouvre lorsque vous vous connectez au portail (au lieu de la page de téléchargement de l'agent). Sélectionnez **GlobalProtect Agent (Agent GlobalProtect)** pour ouvrir la page de téléchargement.

 ©2026 Palo Alto Networks, Inc.



 ©2026 Palo Alto Networks, Inc.

4. Téléchargez l'application.
   1. Pour commencer le téléchargement, cliquez sur le lien qui correspond au systèmes d'exploitation qui s'exécute sur votre ordinateur.

   2. Ouvrez le fichier d'installation du logiciel.
   3. Lorsque vous êtes invité à utiliser ou enregistrer le logiciel, cliquez sur **Run (Utiliser)**.
   4. Lorsque vous y êtes invité, cliquez sur **Run (Utiliser)** pour lancer l'Assistant de configuration GlobalProtect.

      Lors de l'installation initiale de l'application logicielle GlobalProtect sur le point de terminaison, l'utilisateur final doit être connecté au système en utilisant un compte doté de privilèges administratifs. Les mises à jour logicielles ultérieures n'exigent pas de privilèges administratifs.

5. Terminez la configuration de l'application logicielle GlobalProtect.
   1. Dans l'Assistant de configuration GlobalProtect, cliquez sur **Next (Suivant)**.
   2. Cliquez sur **Next (Suivant)** pour accepter le dossier d'installation par défaut (C:\Program Files\Palo Alto Networks\GlobalProtect), puis cliquez sur **Next (Suivant)** deux fois.

      *Bien que vous puissiez utiliser **Browse (Parcourir)** pour sélectionner un autre emplacement où installer l'application GlobalProtect, la meilleure pratique consiste à l'installer à l'emplacement par défaut. L'emplacement d'installation par défaut est en lecture seule pour les utilisateurs non privilégiés et par conséquent, l'installation à cet emplacement protège contre les accès malveillants à l'application.*
   3. Une fois l'installation terminée, **Close (Fermer)** l'assistant.

 ©2026 Palo Alto Networks, Inc.

6. Ouvrez une session sur GlobalProtect.
   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
   2. Saisissez le nom de domaine complet (FQDN) ou l'adresse IP du portail), puis cliquez sur **Connect (Connexion)**.
   3. (Facultatif) Par défaut, vous êtes automatiquement connecté à la **Best Available (Meilleure passerelle disponible)** selon la configuration que l'administrateur définit et les temps de réponse des passerelles disponibles. Pour vous connecter à une autre passerelle, sélectionnez la passerelle dans le menu déroulant **Gateway (Passerelle)** (pour les passerelles externes uniquement).

      Cette option n'est disponible que si vous activez la sélection manuelle de la passerelle.
   4. (Facultatif) Selon le mode de connexion, cliquez sur **Connect (Connecter)** pour initier la connexion.
   5. (Facultatif) Si vous y êtes invité, entrez votre **Username (Nom d'utilisateur)** et votre **Password (Mot de passe)**, et cliquez sur **Sign In (Ouvrir une session)**.

   Si l'authentification réussit, vous êtes connecté à votre réseau d'entreprise et le panneau d'état afficher l'état **Connected (Connecté)** ou **Connected - Internal (Connecté - Interne)**. Si vous établissez une page d'accueil pour GlobalProtect, elle s'affiche lorsque vous avez ouvert une session.

Télécharger et installer l'application mobile GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

L'application GlobalProtect fournit un moyen simple d'élargir les politiques de sécurité d'entreprise aux périphériques mobiles. Comme pour les autres points de terminaison distants exécutant l'application GlobalProtect, l'application mobile offre un accès sécurisé à votre réseau d'entreprise sur un tunnel IPsec ou SSL VPN. L'application se connecte automatiquement à la passerelle qui est la plus proche de l'emplacement actuel de l'utilisateur final. En outre, le trafic vers et depuis le point de terminaison est automatiquement soumis à la mise en œuvre de la même politique de sécurité que les autres hôtes sur votre réseau d'entreprise. L'application GlobalProtect mobile collecte également des informations sur la configuration de l'hôte et peut utiliser ces informations pour la mise en œuvre d'une politique de sécurité basée sur une HIP renforcée.

Il existe deux méthodes principales pour installer l'application GlobalProtect : Vous pouvez déployer l'application à partir d'un MDM (système de gestion de périphériques mobiles) et insérer de manière transparente l'application sur vos points de terminaison gérés ; vous pouvez également installer l'application directement depuis le magasin officiel de votre point de terminaison :

- Points de terminaison iOS : App Store

 ©2026 Palo Alto Networks, Inc.

- Terminaux Android et Chromebook : Google Play

  À partir de la version 5.0 de l'application GlobalProtect, l'application GlobalProtect pour Chrome n'est pas prise en charge ; utilisez plutôt l'application GlobalProtect pour Android.
- Téléphones Windows 10 et points de terminaison UWP Windows 10 : Microsoft Store

Ce flux de travail décrit comment installer l'application GlobalProtect directement sur le point de terminaison. Pour des instructions sur la façon de déployer l'application GlobalProtect depuis Workspace ONE, consultez Déployer l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide de Workspace ONE.

1. Créez une configuration d'agent pour tester l'installation de l'application.

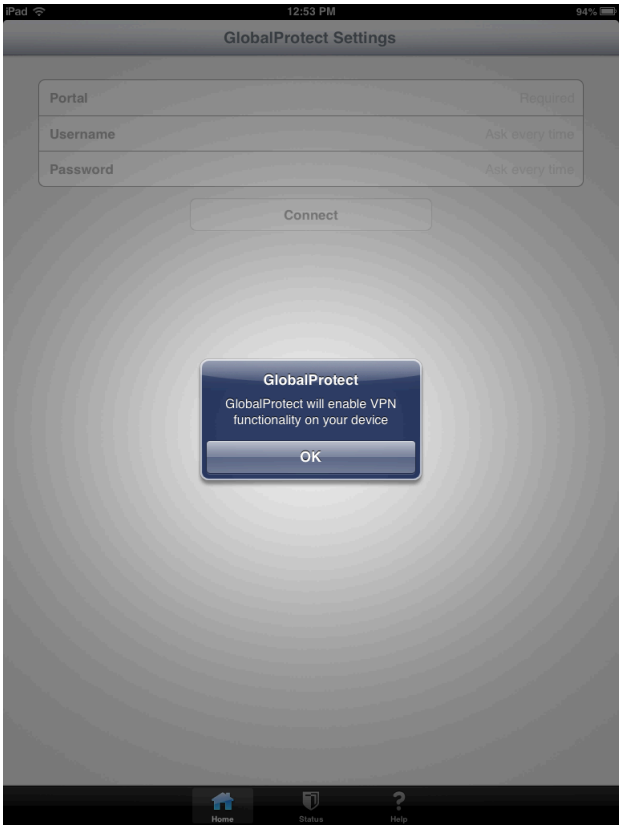
   Idéalement, créez une configuration d'agent qui est limitée à un petit groupe d'utilisateurs, tels que les administrateurs du service informatique responsables de l'administration du pare-feu.

   1. Pour ajouter un nouveau portail ou modifier un portail existant, effectuez l'une des actions suivantes :
      - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**. Sélectionnez une configuration de portail existante que vous souhaitez modifier ou **Add (Ajouter)** une nouvelle.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)**.
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Portals (Portails)** puis **Add Portal (Ajouter un portail)**.
   2. À l'onglet **Agent**, sélectionnez une configuration existante ou **Add (Ajoutez)**-en une nouvelle à déployer sur les utilisateurs /le groupe de test.
   3. Ajoutez le **User/User Group (Utilisateur/Groupe d'utilisateurs)** qui testera l'application.
      - Sur Panorama, dans l'onglet **User/User Group (Utilisateur/Groupe d'utilisateurs)**, **Add (Ajouter)** le **User/User Group (Utilisateur/Groupe d'utilisateurs)**.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs et groupes locaux)**
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs et groupes locaux)**.
   4. Sélectionnez le **OS (Système d'exploitation)** pour l'application que vous testez (**iOS**, **Android** ou **WindowsUWP**).
   5. (Facultatif) Sélectionnez la configuration d'agent que vous venez de créer ou de modifier, puis cliquez sur **Move Up (Déplacer vers le haut)** afin qu'elle figure, dans la liste, avant toute configuration plus générique que vous avez créée.
   6. **Commit (Validez)** les modifications.

 ©2026 Palo Alto Networks, Inc.

2. Depuis le point de terminaison, suivez les invites de commande pour télécharger et installer l'application.
   - Sur les points de terminaison Android, cherchez l'application sur Google Play.
   - Sur les points de terminaison iOS, cherchez l'application sur l'App Store.
   - Sur les points de terminaison UWP Windows 10, cherchez l'application dans le Microsoft Store.
3. Lancez l'application.

Dès la fin de l'installation, l'icône de l'application GlobalProtect s'affiche sur l'écran d'accueil du point de terminaison. Pour lancer l'application, touchez l'icône. Lorsque vous êtes invité à activer la fonctionnalité VPN GlobalProtect, appuyez sur **OK**.



 ©2026 Palo Alto Networks, Inc.

4. Connectez-vous au portail.
   1. Lorsque vous y êtes invité, saisissez le nom ou l'adresse du **Portal (Portail)**, le **Username (Nom d'utilisateur)**, et le **Password (Mot de passe)**. Le nom du portail doit être un FQDN et il ne doit pas inclure https://au début.

   2. Tapez **Connect (Connexion)** et vérifiez que l'application établit une connexion à GlobalProtect avec succès.

      Si un système de gestion de point d'extrémité mobile tiers est configuré, l'application vous invite à vous inscrire.

Lanceur CLI pour GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Terminaux GlobalProtect fonctionnant sous Windows 10 ou Windows 11

Le lanceur CLI GlobalProtect permet d'initier des connexions, de se déconnecter et d'exécuter d'autres fonctions sans utiliser l'interface utilisateur graphique (GUI). Ceci est particulièrement utile pour :

- L'automatisation des connexions à l'aide de scripts.
- L'intégration de GlobalProtect dans des applications tierces.

L'exécutable CLI GlobalProtect `pangpcli.exe` se trouve dans `C:\Program Files\Palo Alto Networks\GlobalProtect`. L'exécutable est installé dans le cadre de l'installation GlobalProtect MSI.

Les journaux de pangpcli.exe sont stockés dans PanGpCli.log dans le dossier `/User/AppData/Local/Palo Alto Networks/GlobalProtect/`. Pour les journaux liés aux fonctionnalités globales de GlobalProtect, reportez-vous à Surveillance et dépannage de GlobalProtect.

Vous pouvez utiliser le lanceur CLI pour les fonctionnalités suivantes :

- VPN IPSec et VPN SSL

 ©2026 Palo Alto Networks, Inc.

- Mode à la demande et toujours actif
- Passerelles NGFW, Prisma Access : Passerelles MU, EP
- Authentification du certificat client, SAML, Authentification locale
- Adressage IPv4 et IPv6
- Tunnel segmenté et tunnel complet
- Rapports HIP et notifications HIP

Prérequis

GlobalProtect doit être installé dans votre environnement à l'aide du fichier MSI.

Syntaxe

```
pangpcli.exe [-help] [-status] [-start {-portal <portal>|-gateway
 <gateway>}] [-start -clientcert <cert_name>] [-disconnect] | [-
disconnect -passcode <disconnect_passcode>] [-logs -level <dump|
debug>]
```

Tableau 5 :

Nom	Exigence	Description
pangpcli.exe	Obligatoire	Lance CLI GlobalProtect. Affiche l'assistance lorsqu'il est utilisé seul.
[-help]	En option	Affiche les options d'utilisation des commandes.
[-start {-portal <portal>|-gateway <gateway>}]	En option	Se connecte au portail et/ou à la passerelle GlobalProtect spécifiés.
[-start -clientcert <cert_name>]	En option	Sélectionne le certificat spécifié lors de la connexion http. Si un nom de certificat incorrect est fourni, GlobalProtect invite l'utilisateur à sélectionner un certificat. Cette commande doit être utilisée en combinaison avec les commandes de portail et de passerelle. Si le nom du certificat inclut un espace, indiquez le cert_name entre " ".
[-status]	En option	Affiche l'état de la connexion de l'agent GlobalProtect. L'état peut être connecté, déconnecté ou non en cours d'exécution.

 ©2026 Palo Alto Networks, Inc.

Nom	Exigence	Description
[-logs -level <dump|debug>]	En option	Définit le niveau de journal GlobalProtect.
[-pangpcli -logs]		Collecte le groupe de journaux GLobalProtect.
[-disconnect]	En option	Déconnecte la session GlobalProtect.
-disconnect -passcode <disconnect_passcode>	En option	Déconnecte la session GlobalProtect. Ce paramètre est utilisé lorsque GlobalProtect est configuré pour avoir besoin d'un code secret distinct pour permettre aux utilisateurs finaux de se déconnecter.
[-signout]	En option	Se déconnecte de GlobalProtect.

Afficher et collecter les journaux d'application GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Vous disposez de deux options pour collecter les journaux d'applications GlobalProtect™ à partir des points de terminaison des utilisateurs finaux :

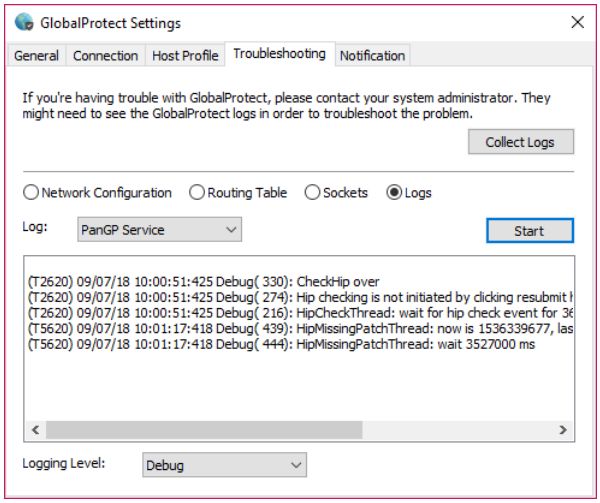
- Collecter les journaux : les utilisateurs finaux doivent collecter manuellement les journaux de l'application GlobalProtect. Ils peuvent également contrôler le nombre de fichiers journaux rotatifs maintenus sur les terminaux Windows et macOS. Pour plus d'informations, consultez Configurer le nombre de fichiers journaux de l'application GlobalProtect.
- Signaler un problème : les utilisateurs finaux signalent un problème directement au Service de journalisation Strata auquel l'administrateur peut accéder lorsqu'ils rencontrent un comportement inhabituel tel qu'une mauvaise performance du réseau ou qu'une connexion n'est pas établie avec le portail et la passerelle.

  Pour que l'application GlobalProtect envoie des journaux de dépannage, des journaux de diagnostic ou les deux à des Strata Logging Service pour une analyse plus approfondie, vous devez configurer le portail GlobalProtect pour activer la configuration des paramètres de collecte de journaux de l'application sur le portail GlobalProtect. En outre, vous pouvez configurer les URL de destination HTTPS qui peuvent contenir des adresses IP ou des noms de domaine complets des serveurs/ressources web que vous souhaitez sonder, et pour déterminer des problèmes tels que la latence ou les performances réseau sur le terminal de l'utilisateur final.

Utilisez les étapes suivantes pour afficher ou collecter les journaux GlobalProtect :

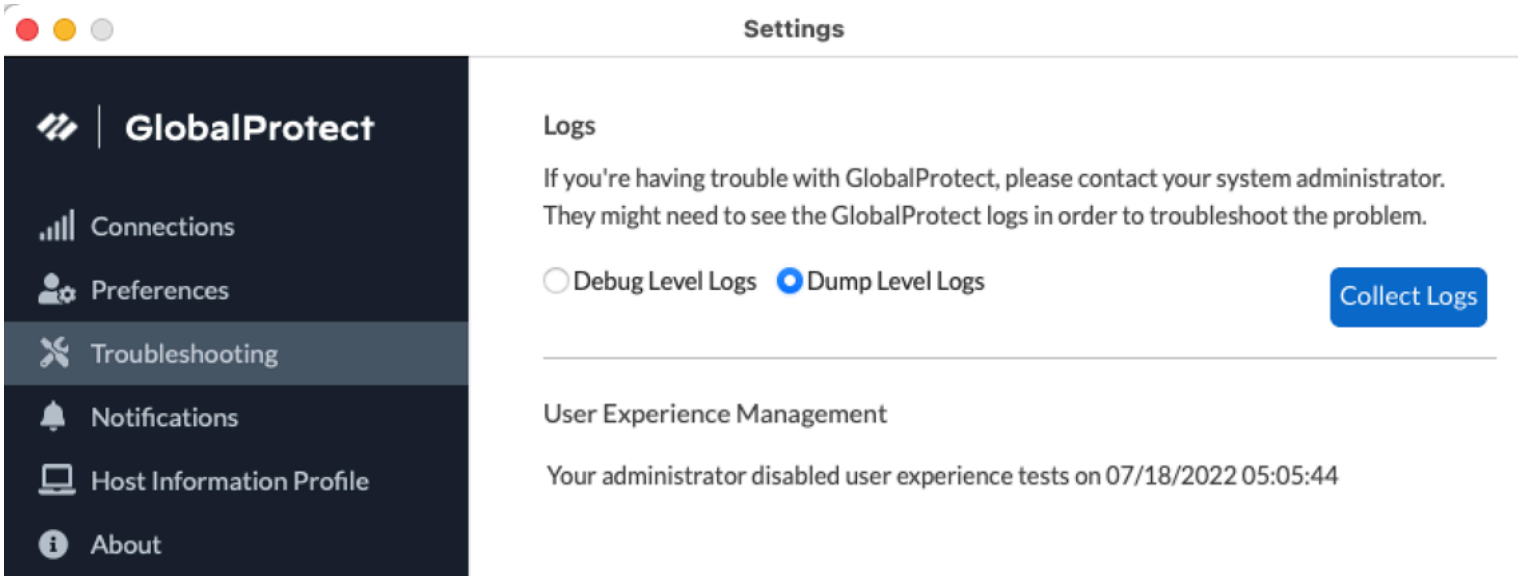
 ©2026 Palo Alto Networks, Inc.

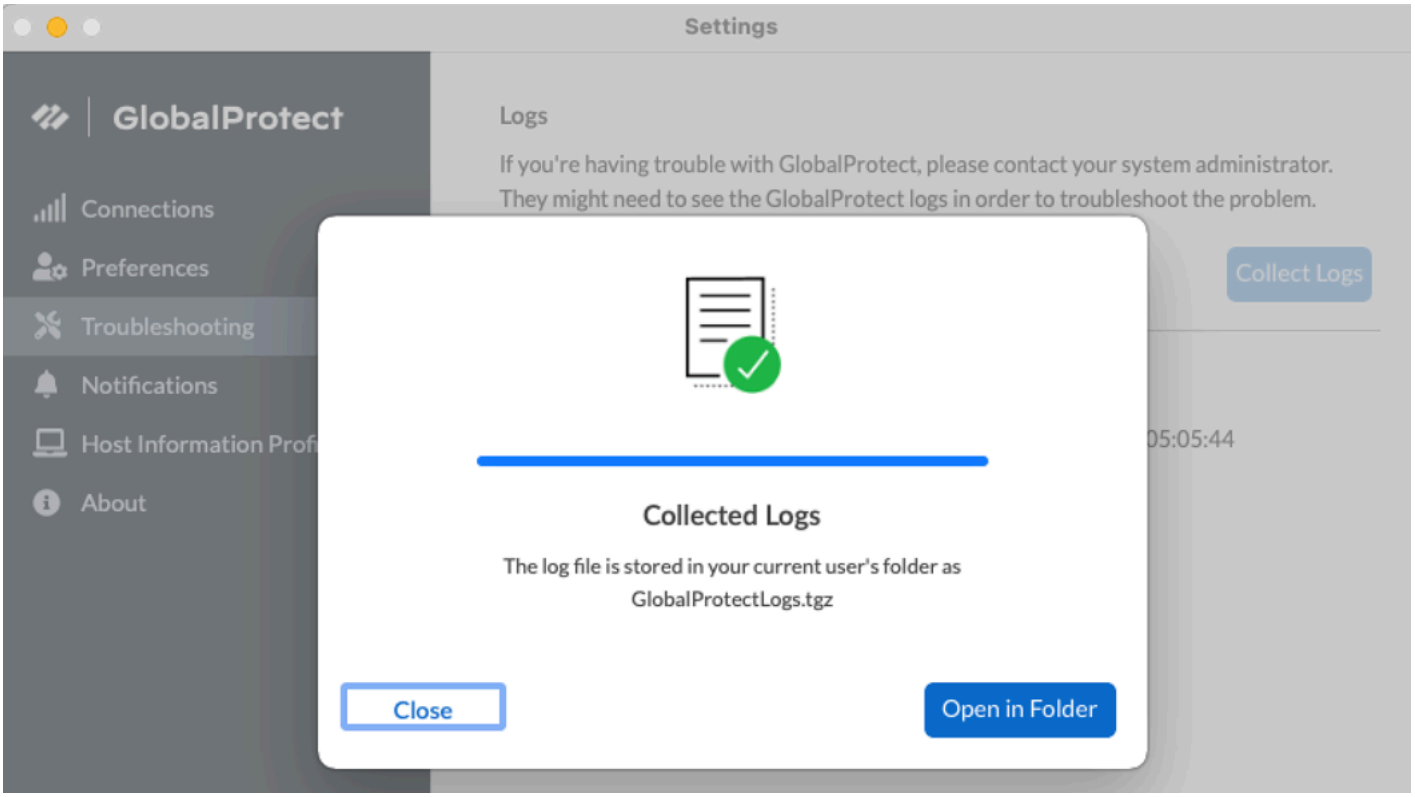
1. Lancez l'application GlobalProtect.
2. À partir du panneau d'état, ouvrez le dialogue des paramètres ( ).
3. Sélectionnez **Settings (Paramètres)**.
4. À partir du panneau des paramètres GlobalProtect, sélectionnez **Troubleshooting (Résolution de problèmes)**.
5. Sélectionnez **Debug (déboguer)** ou **Dump (jeter)** dans la liste déroulante **Logging Level (niveau de connexion)**.
6. (Facultatif—Windows uniquement) Affichez vos journaux GlobalProtect :
   1. Sélectionnez **Logs (Journaux)**.
   2. Choisissez un type de **Log (Journal)**.
   3. **Start (Commencez)** à afficher les journaux.



 ©2026 Palo Alto Networks, Inc.

7. (Facultatif) **Collect Logs (Collectez les journaux)** à envoyer à votre adminstrateur GlobalProtect à des fins de résolution de problèmes.





Configurer le nombre de fichiers journaux de l'application GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	GlobalProtect version 6.2.8-h5 (6.2.8-c416) et ultérieures ou 6.3.3-h4 (6.3.3-c828) et ultérieures

©2026 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Windows et MacOS uniquement	Licence de passerelle GlobalProtect

Pour améliorer la profondeur et l'analyse du dépannage, les administrateurs GlobalProtect peuvent désormais contrôler le nombre de fichiers journaux rotatifs maintenus sur les terminaux Windows et macOS. Cet historique de journaux enrichi vous aide à examiner plus en détail les problèmes complexes. Vous pouvez contrôler le nombre total de fichiers journaux sur les périphériques Windows et macOS à l'aide de paramètres spécifiques dans le Registre Windows ou la plist des fichiers macOS. À noter que ces clés de registre ne sont pas disponibles sur Windows UWP ou si l'application GlobalProtect est en mode FIPS-CC.

Clé	Contrôle le nombre de fichiers journaux pour	Gamme de valeurs	Taille du fichier individuel
PanGPSLogFileCount	Processus PanGPS.exe	2-20 Si une valeur est définie en dehors de cette plage, le client la traitera comme la limite la plus proche (2 ou 20) Si cette clé n'existe pas, 10 fichiers sont enregistrés	5 Mo
LogFileCount	Processus PanGPA, PanGpHip et PanGpHipMp	2-20 Si une valeur est définie en dehors de cette plage, le client la traitera comme la limite la plus proche (2 ou 20) Si cette clé n'existe pas, 2 fichiers sont enregistrés	5 Mo

Les fichiers journaux sont numérotés séquentiellement. Pour un réglage de *N* fichiers, les noms de fichiers sont les suivants :

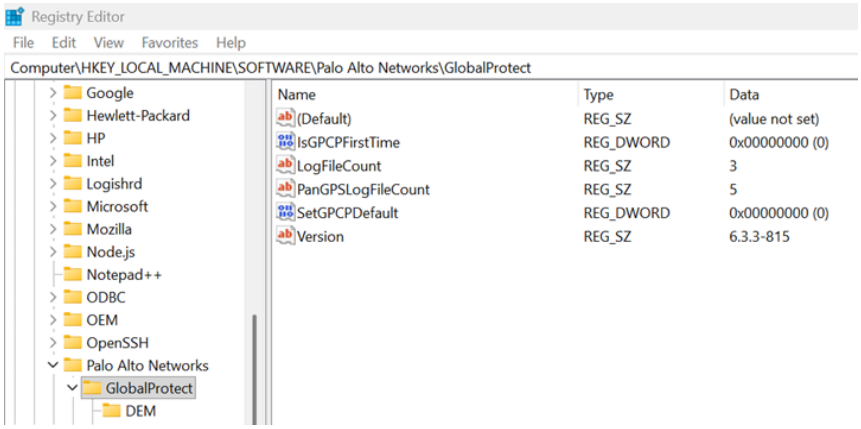
- `[ProcessName].log` (le journal actuel)
- `[ProcessName].1.log`
- `[ProcessName].2.log`
- ... jusqu'à `[ProcessName].[N-1].log`

 ©2026 Palo Alto Networks, Inc.

Par exemple, si `PanGPSLogFileCount` est défini sur **5**, les journaux seront `PanGPS.log`, `PanGPS.1.log`, `PanGPS.2.log`, `PanGPS.3.log` et `PanGPS.4.log`. Le dernier fichier (`PanGPS.4.log` dans notre exemple) contient les derniers journaux.

Définir les clés de Registre sur les terminaux Windows

1. Ouvrez l'éditeur du Registre (regedit) en tant qu'administrateur.
2. Accédez à `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`.
3. Cliquez avec le bouton droit sur la touche `GlobalProtect`, sélectionnez **New (Nouveau)**, puis choisissez **DWORD (32-bit) Value (Valeur DWORD ([32 bits])**.
4. Créez les clés suivantes et définissez leur valeur décimale entre 2 et 20 :
   - `PanGPSLogFileCount`
   - `LogFileCount`



5. Redémarrez votre périphérique Windows après avoir défini les touches pour que les modifications prennent effet. Ces paramètres persistent après la mise à niveau de l'application GlobalProtect.

Définir les clés de Registre sur les terminaux macOS

1. Utilisez un éditeur de listes ou une commande terminale pour modifier le fichier `Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`.

 ©2026 Palo Alto Networks, Inc.

2. Ajoutez les clés suivantes comme valeurs entières et définissez leur valeur entre 2 et 20 :
   - `PanGPSLogFileCount`
   - `LogFileCount`

```
            <key>Prelogon</key>
            <string>1</string>
            <key>PreviousVersion</key>
            <string></string>
        </dict>
        <key>Settings</key>
        <dict>
            <key>LogFileCount</key>
            <integer>3</integer>
            <key>PanGPSLogFileCount</key>
            <integer>5</integer>
            <key>access-gateway-from-agent-only</key>
            <string>no</string>
            <key>agent-user-override</key>
            <string>allowed</string>
            <key>allow-extend-session</key>
            <string>no</string>
            <key>allow-traffic-blocking-notification-dismissal</key>
            <string>no</string>
            <key>captive-portal-detection-msg</key>
            <string>&lt;div style="font-family:'Helvetica Neue';"&gt;&lt;h1 style="co
le="margin: 0; font-size: 15px; line-height: 1.2em;"&gt;GlobalProtect has temporarily permitted network a
t;p style="margin: 0; font-size: 15px; line-height: 1.2em;"&gt;If you let the connection time out, open G
            <key>captive-portal-exception-timeout</key>
            <string>0</string>
            <key>captive-portal-login-url</key>
            <string>http://google.com</string>
            <key>captive-portal-notification-delay</key>
            <string>5</string>
```

3. Redémarrez votre périphérique macOS après avoir défini les touches pour que les modifications prennent effet. Ces paramètres persistent après la mise à niveau de l'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Déployer l'application GlobalProtect sur les périphériques mobiles

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Les terminaux mobiles nécessitent l'application GlobalProtect pour se connecter à GlobalProtect™. Utilisez la matrice de compatibilité de l'application GlobalProtect pour déterminer quelle version de l'application GlobalProtect vous souhaitez que vos utilisateurs exécutent sur leurs terminaux. La version qu'un utilisateur final doit télécharger et installer pour une connectivité réseau réussie dépend de votre environnement.

La méthode de déploiement de l'application dépend des types de terminaux suivants :

Platform (Plateforme)	Options de déploiement
Points de terminaison iOS et Android	• **À partir d'un système de gestion de terminaux mobiles**, si vous utilisez un système de gestion mobile, comme un MDM ou un EMM, vous pouvez utiliser le système pour déployer et configurer l'application GlobalProtect. Consultez Aperçu de la gestion des périphériques mobiles.. • **À partir d'un app store** : l'utilisateur final peut également télécharger et installer l'application GlobalProtect directement à partir de l'Apple App Store (points de terminaison iOS) ou de Google Play (points de terminaison Android). Pour obtenir des instructions sur la façon de télécharger et de tester l'installation de l'application GlobalProtect, reportez-vous à la section Télécharger et installer l'application mobile GlobalProtect.
Chromebooks	• **À partir de la console Google Admin** : La console Google Admin vous permet de gérer les paramètres et les applications Chromebook à partir d'un emplacement central et basé sur le Web. Pour déployer l'application GlobalProtect pour Android sur des Chromebooks gérés en utilisant la console d'administration Google, consultez Déployer l'application GlobalProtect pour Android sur les Chromebooks gérés à l'aide de la console Google Admin.. *L'application GlobalProtect pour Android n'est prise en charge que sur certains Chromebook. Les Chromebook qui ne prennent pas en charge les applications Android doivent continuer d'exécuter l'application GlobalProtect pour Chrome,*

 ©2026 Palo Alto Networks, Inc.

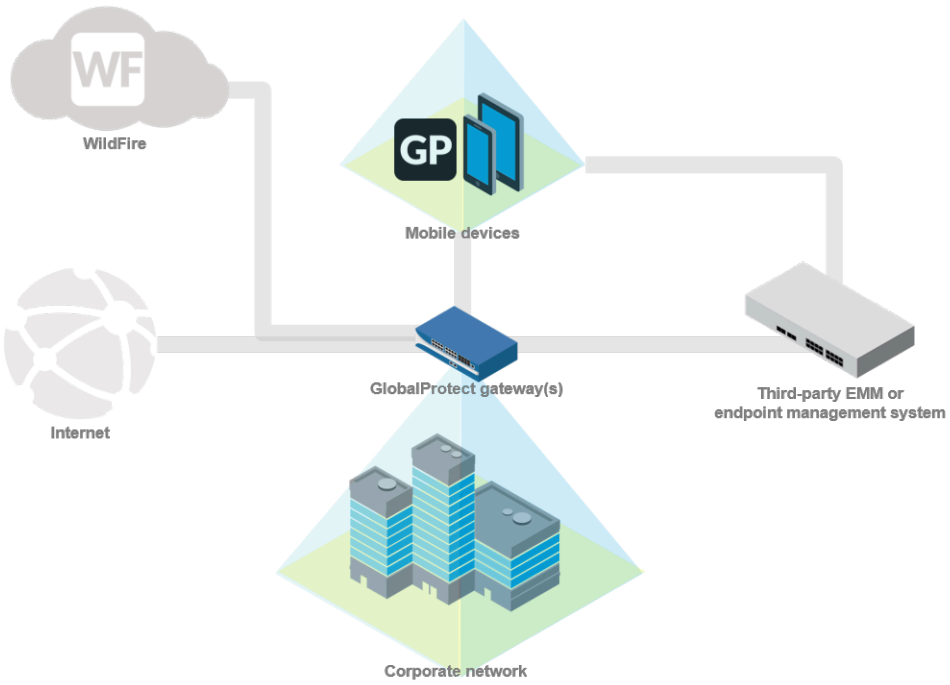
Platform (Plateforme)	Options de déploiement
	qui n'est pas prise en charge à partir de la version 5.0 de l'application GlobalProtect. • **Depuis Workspace ONE** : vous pouvez déployer l'application GlobalProtect pour Android sur les Chromebooks gérés qui sont inscrits auprès de Workspace ONE. Après avoir déployé l'application, configurez et déployez un profil VPN pour configurer automatiquement l'application GlobalProtect pour les utilisateurs finaux. Pour déployer l'application GlobalProtect pour Android sur des Chromebooks gérés en utilisant Workspace ONE, consultez Déployer l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide de Workspace ONE..

Aperçu de la gestion des périphériques mobiles

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

À l'heure où les périphériques mobiles sont de plus en plus performants, les utilisateurs finaux comptent de plus en plus sur eux pour exécuter les tâches de l'entreprise. Toutefois, ces mêmes points de terminaison qui accèdent à votre réseau d'entreprise se connectent également à Internet sans protection contre les menaces et les vulnérabilités.

 ©2026 Palo Alto Networks, Inc.



Un système de gestion des périphériques mobiles (MDM) ou système EMM (Enterprise Mobility Management) simplifie l'administration des points de terminaison mobiles en vous permettant de déployer automatiquement vos paramètres de configuration de compte d'entreprise et de VPN vers des points de terminaison conformes. Vous pouvez également utiliser votre système de gestion de périphériques mobiles pour l'assainissement des violations de sécurité en interagissant avec un point de terminaison qui a été compromis. Cela protège les données d'entreprise ainsi que les données personnelles de l'utilisateur final. Par exemple, si un utilisateur final perd un point de terminaison, vous pouvez verrouiller à distance le point de terminaison à partir du système de gestion des périphériques mobiles ou même effacer le point de terminaison (complètement ou sélectivement).

En plus des fonctions de provisionnement et de gestion des périphériques distants qu'un système de gestion de périphériques mobiles peut fournir, lorsqu'il est intégré à votre infrastructure VPN GlobalProtect™ existante, vous pouvez utiliser des informations d'hôte que les points de terminaison signalent pour appliquer des stratégies de sécurité pour l'accès aux applications via la passerelle GlobalProtect. Vous pouvez également utiliser les outils de surveillance qui sont intégrés dans le pare-feu de la prochaine génération de Palo Alto pour surveiller le trafic de points de terminaison mobile.

Intégration GlobalProtect avec un système MDM ou EMM

Vous pouvez intégrer votre déploiement MDM avec un système MDM ou EMM à l'aide de l'une des méthodes suivantes :

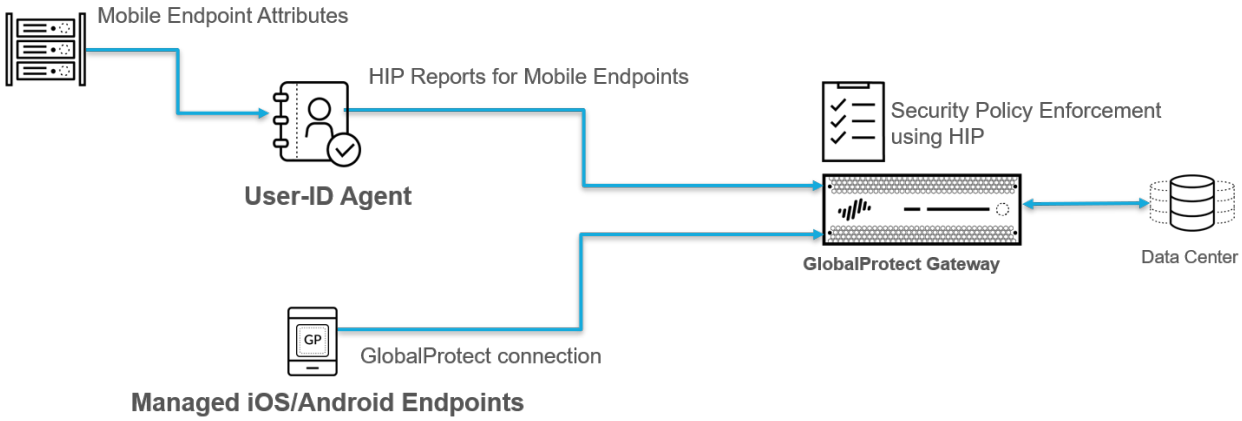
Intégration du pare-feu avec un système MDM ou EMM (Workspace ON uniquement)

Vous pouvez configurer l'agent Windows User-ID pour qu'il communique avec le serveur MDM de Workspace ON pour collecter des informations sur l'hôte auprès des terminaux se connectant. L'agent User-ID envoi ces informations sur l'hôte à la passerelle GlobalProtect dans le cadre du rapport HIP à des fins d'utilisation dans l'application de la politique basée sur HIP.

 ©2026 Palo Alto Networks, Inc.

L'intégration du pare-feu est prise en charge par la version 8.0 de PAN-OS ou toute version ultérieure.

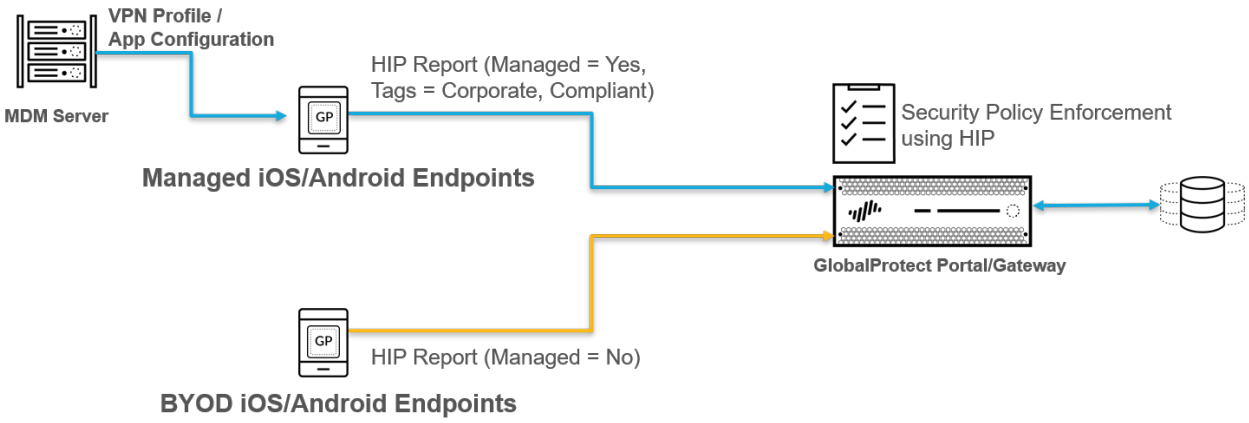
L'intégration du pare-feu est prise en charge uniquement avec VMware Workspace ON.



Intégration de l'application GlobalProtect avec un système MDM ou EMM

À compter de la version 5.0, l'application GlobalProtect pour les points de terminaison iOS et Android peut obtenir les étiquettes et les attributs de données du fournisseur auprès des systèmes MDM. Pour les points de terminaison iOS, les systèmes MDM envoient ces attributs à l'application GlobalProtect dans le cadre du profil VPN. Pour les points de terminaison Android, les systèmes MDM envoient ces attributs dans le cadre de la configuration des restrictions d'applications. L'application GlobalProtect peut ensuite envoyer ces attributs et étiquettes à la passerelle GlobalProtect dans le cadre du rapport HIP à des fins d'utilisation dans l'application de la politique basée sur HIP.

 ©2026 Palo Alto Networks, Inc.



L'intégration de l'application GlobalProtect est possible avec VMware Workspace ON, MobileIron et Microsoft Intune. Cependant, cette méthode d'intégration est également prise en charge avec n'importe quel système MDM ou EMM qui prend en charge les attributs des données de fournisseur dans le profil VPN.

Le tableau suivant décrit les attributs des données de fournisseur prises en charge :

Attribut MDM	Attribut de rapport HIP	Catégorie de rapport HIP	Description
`mobile_id`	**ID d'hôte**	**Général**	Unique device identifier (UDID ; Identificateur de périphérique unique) du point de terminaison.
`managed`	**Géré**	**Général**	Valeur qui indique si le point de terminaison est géré. Si la valeur est **Yes (Oui)**, le point de terminaison est géré. Si la valeur est **No (Non)**, le point de terminaison n'est pas géré.
`compliance`	**Étiquette**	**Périphérique mobile**	État de conformité qui indique si le point de terminaison est conforme aux politiques de conformité MDM que vous avez définies (par exemple, **Compliant (Conforme)**). Cette valeur est annexée à l'attribut **Tag (Étiquette)** indiqué dans le rapport HIP.

 ©2026 Palo Alto Networks, Inc.

Attribut MDM	Attribut de rapport HIP	Catégorie de rapport HIP	Description
`ownership`	**Étiquette**	**Périphérique mobile**	Catégorie d'appartenance du point de terminaison (par exemple, **Employee Owned (appartient à l'employé)**). Cette valeur est annexée à l'attribut **Tag (Étiquette)** indiqué dans le rapport HIP.
`Etiquette`	**Étiquette**	**Périphérique mobile**	Étiquettes à faire correspondre aux autres attributs fondés sur MDM.

Paramétrer l'intégration MDM avec GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour configurer l'intégration MDM avec GlobalProtect, utilisez le workflow suivant :

1. Configurez l'infrastructure GlobalProtect.
   1. Créer des interfaces et des zones pour GlobalProtect.
   2. Activer SSL entre les composants GlobalProtect.
   3. Configurez l'authentification de l'utilisateur GlobalProtect. Reportez-vous à la section Authentification de l'utilisateur GlobalProtect.
   4. Activer le mappage des groupes.
   5. Configurer une passerelle GlobalProtect.
   6. Activez les licences pour chaque pare-feu exécutant une (des) passerelle (s) qui prend en charge l'app GlobalProtect sur les points de terminaison mobiles.
   7. Paramétrer l'accès au portail GlobalProtect.
2. Configurez le système de gestion des périphériques mobiles et décidez s'il faut prendre en charge uniquement les points de terminaison émis par les entreprises ou les deux points de terminaison personnels émis par l'entreprise.

   Reportez-vous aux instructions de votre système de gestion des périphériques mobiles (MDM) ou système EMM (Enterprise Mobility Management).
3. Obtenez l'application GlobalProtect pour les points de terminaison mobiles.

   Vous pouvez installer l'application directement à partir de l'App Store sur votre terminal (voir Télécharger et installer l'application mobile GlobalProtect) ; ou déployez l'application à partir

 ©2026 Palo Alto Networks, Inc.

d'un système de gestion de périphériques mobiles (tel que Workspace ONE) et transmettez de manière transparente l'application à vos terminaux gérés.

- App Store – Télécharger et installer l'application mobile GlobalProtect
- Systèmes de gestion des périphériques mobiles pris en charge : consultez les instructions suivantes sur la manière de déployer des applications sur les terminaux gérés :
  - Déployer l'application mobile GlobalProtect à l'aide de Workspace ONE
  - Déployer l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide de Workspace ONE
  - Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune
  - Déployez l'application mobile GlobalProtect à l'aide de MobileIron
  - Déployer l'application GlobalProtect pour Android sur les Chromebooks gérés à l'aide de la console Google Admin
- Autre système tiers de gestion des périphériques mobiles — consultez les instructions de votre fournisseur sur la façon de déployer des applications vers des points de terminaison gérés.

4. Configurez l'intégration MDM.

Utilisez l'une des méthodes suivantes pour modifier l'intégration MDM :

- Intégration du pare-feu avec un système MDM ou EMM :
  - Configurer l'agent User-ID Windows pour collecter des informations d'hôte
- Intégration de l'application GlobalProtect avec un système MDM ou EMM :
  - Gérer l'application GlobalProtect à l'aide de Workspace ONE
  - Gérer l'application GlobalProtect à l'aide de Microsoft Intune
  - Gérer l'application GlobalProtect à l'aide de MobileIron
  - Gérer l'application GlobalProtect à l'aide de la console Google Admin
  - Gérer l'application GlobalProtect à l'aide d'autres MDM tiers

5. Configurez les stratégies qui ciblent les points de terminaison mobiles à l'aide de l'information d'hôte.

Configurer la mise en œuvre des politiques basées sur HIP pour les terminaux gérés.

Fournisseurs MDM qualifiés

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

Le tableau suivant indique les fournisseurs MDM qualifiés que vous pouvez utiliser pour configurer, déployer et gérer l'application GlobalProtect par système d'exploitation. A – indique que le système d'exploitation n'est pas pris en charge.

Si vous voulez utiliser un fournisseur MDM qui n'' pas été qualifié, Gérer l'application GlobalProtect à l'aide d'autres MDM tiers.

Fournisseur MDM pris en charge	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Workspace ONE (anciennement AirWatch)	√ (Configuration de VPN par application uniquement)	√	–	–	√	–	–
Microsoft Intune	√ (Toujours actif, accès à distance, et configuration VPN uniquement par application)	√	–	–	√ (Configuration de VPN toujours active et Configuration de VPN par application uniquement	–	–
MobileIron	√ (Configuration de VPN toujours active)	√	–	–	–	–	–
Console Google Admin	√ (Pour la prise en charge de l'application Android sur les Chromebook ; déploiement	–	√ (déploiement d'application uniquement)	–	–	–	–

 ©2026 Palo Alto Networks, Inc.

Fournisseur MDM pris en charge	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
	d'application uniquement)						
	Vous pouvez utiliser la console Google Admn uniquement pour déployer l'application GlobalProtect ; vous ne pouvez utiliser la console pour configurer les configurations VPN. Vous devez configurer la configuration VPN via le portail GlobalProtect avant de pouvoir déployer l'application au moyen de la console Google Admin.						
Jamf Pro	—	√	—	—	—	√ (déploiement d'applications et déploiement de profils de configuration uniquement)	—
	Pour les terminaux macOS, vous pouvez utiliser Jamf Pro uniquement pour déployer l'application GlobalProtect et les profils de configuration ; vous ne pouvez pas utiliser Jamf pour configurer les configurations VPN. Vous devez configurer la configuration VPN via le portail GlobalProtect avant de pouvoir déployer l'application au moyen de la console Jamf.						

Gérer l'application GlobalProtect à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Workspace ONE est une plateforme de gestion de mobilité d'entreprise qui vous permet de gérer des points d'extrémité mobiles, à partir d'une console centrale. L'application GlobalProtect offre une connexion sécurisée entre le pare-feu et les terminaux mobiles gérés par Workspace ONE au niveau du périphérique ou de l'application. L'utilisation de GlobalProtect en tant que connexion sécurisée assure l'homogénéité de l'inspection du trafic et de l'application des règles de sécurité du réseau pour la prévention des menaces sur les points de terminaison mobiles.

 ©2026 Palo Alto Networks, Inc.

Si vous n'utilisez pas de système MDM de tiers qualifié, vous pouvez Gérer l'application GlobalProtect à l'aide d'autres MDM tiers.

Déployer l'application mobile GlobalProtect à l'aide de Workspace ONE

Vous pouvez déployer l'application GlobalProtect vers des terminaux gérés qui sont inscrits à Workspace ONE. Les terminaux exécutant iOS ou Android doivent télécharger l'agent Workspace ONE pour s'inscrire auprès du MDM Workspace ONE. Les terminaux Windows 10 ne nécessitent pas l'agent Workspace ONE, mais vous obligent à configurer l'inscription sur le terminal. Après avoir déployé l'application, configurez et déployez un profil VPN pour configurer automatiquement l'application GlobalProtect pour les utilisateurs finaux.

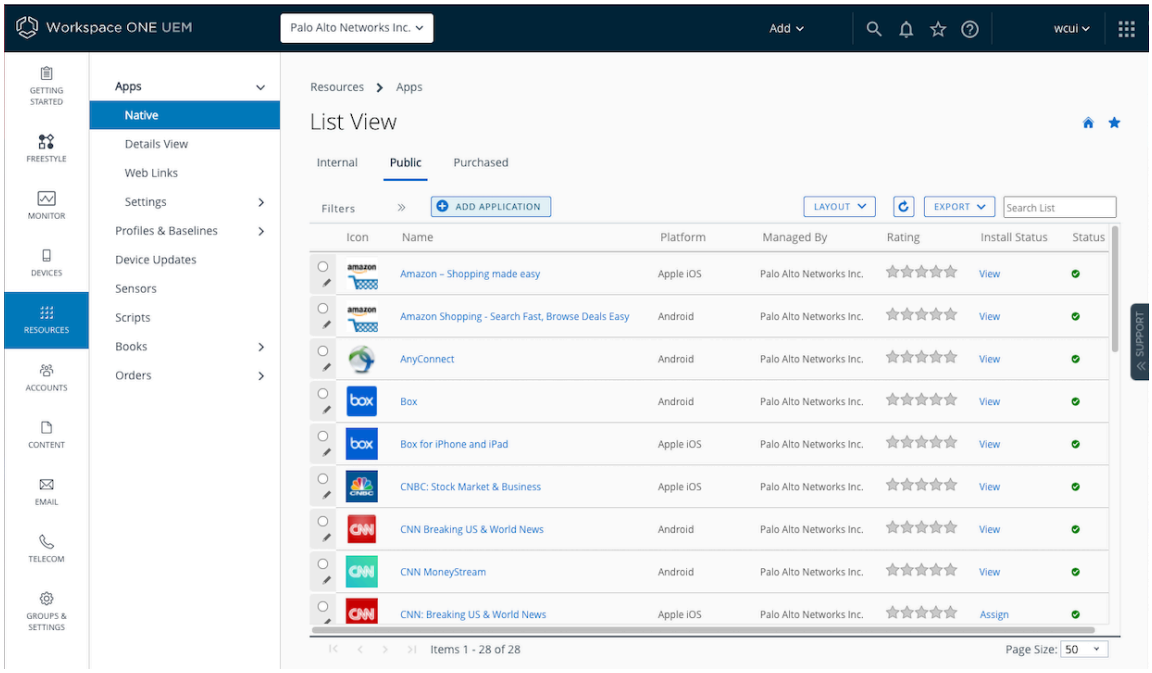
Si vous souhaitez exécuter l'application GlobalProtect pour Android sur des Chromebooks gérés, vous pouvez Déployer l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide de Workspace ONE.

1. Avant de commencer, assurez-vous que les terminaux auxquels vous souhaitez déployer l'application GlobalProtect sont inscrits à Workspace ONE :
   - **Android et iOS** : téléchargez l'agent Workspace ONE et suivez les invites pour vous inscrire.
   - **Windows Phone et Windows 10 UWP** : configurez le terminal UWP de Windows 10 pour s'inscrire à Workspace ONE (à partir du terminal, sélectionnez **Settings (Paramètres)** > **Accounts (Comptes)** > **Work access (Accès au travail)** > **Connect (Connexion)**).

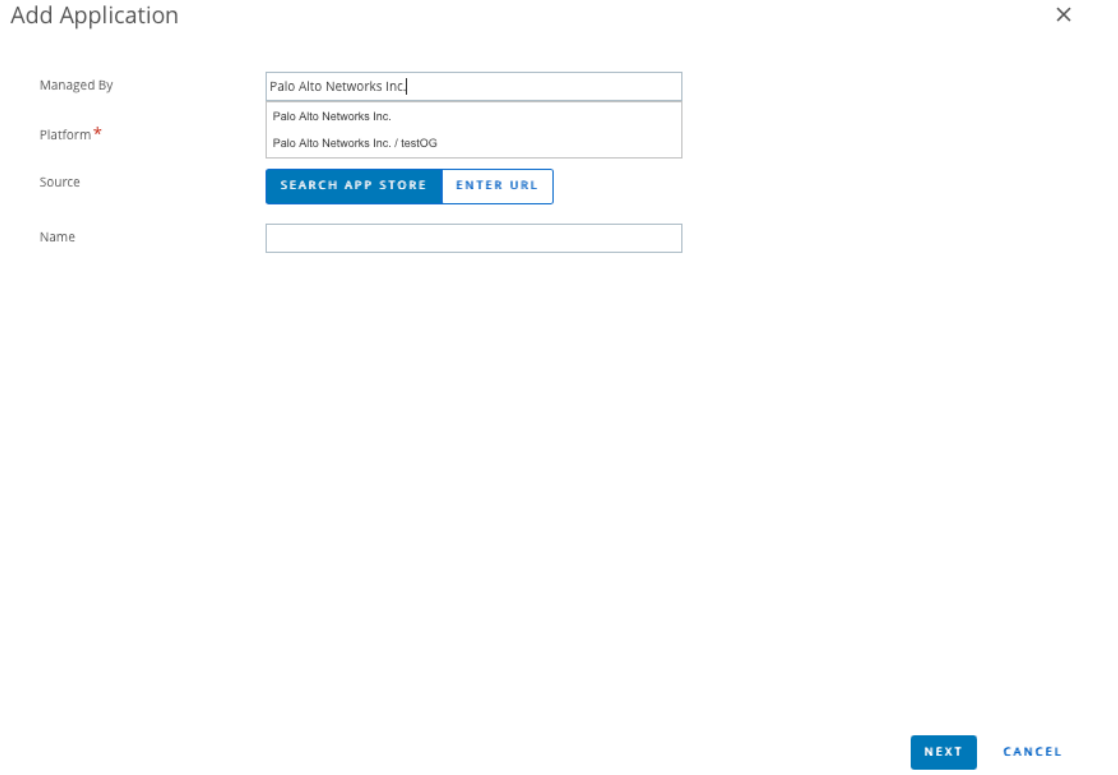
 ©2026 Palo Alto Networks, Inc.

2. Ajoutez l'application GlobalProtect à Workspace ONE :

1. Depuis Workspace ONE, sélectionnez **Resources (Ressources)** > **Applications** > **Native** > **Public (Publique)** > **Add Application (Ajouter une application)**.

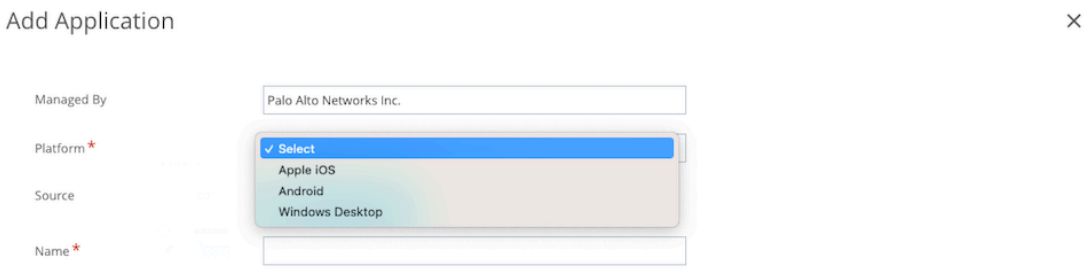


2. Dans le champ **Managed By (Géré par)**, sélectionnez le groupe de l'entreprise qui gérera cette application.



 ©2026 Palo Alto Networks, Inc.

3. Sélectionnez la **Platform (Plateforme)** (**Apple iOS**, **Android** ou **Windows Desktop**).



4. Recherchez l'application GlobalProtect dans l'App Store du point de terminaison ou saisissez l'une des URL suivantes pour la page de l'application GlobalProtect :
   - **Apple iOS** : https://apps.apple.com/us/app/globalprotect/id1400555706
   - **Android** — https://play.google.com/store/apps/details?id=com.paloaltonetworks.globalprotect
   - **Windows Phone et Windows 10 UWP** : https://www.microsoft.com/en-us/p/globalprotect/9nblggh6bzl3
5. Cliquez sur **Next (Suivant)**. Si vous avez recherché l'application dans le magasin d'applications du terminal, vous devez également **Select (Sélectionner)** l'application dans une liste de résultats de recherche, puis **SAVE & ASSIGN (ENREGISTRER ET ASSIGNER)** pour configurer les options de déploiement.

   Si vous avez cherché l'application GlobalProtect pour Android et que vous ne l'avez pas vue dans la liste, contactez votre administrateur de la version professionnelle d'Android (Android for Work) pour ajouter GlobalProtect à la liste des applications approuvées par l'entreprise ou utilisez l'URL de l'application dans le Google Play Store.

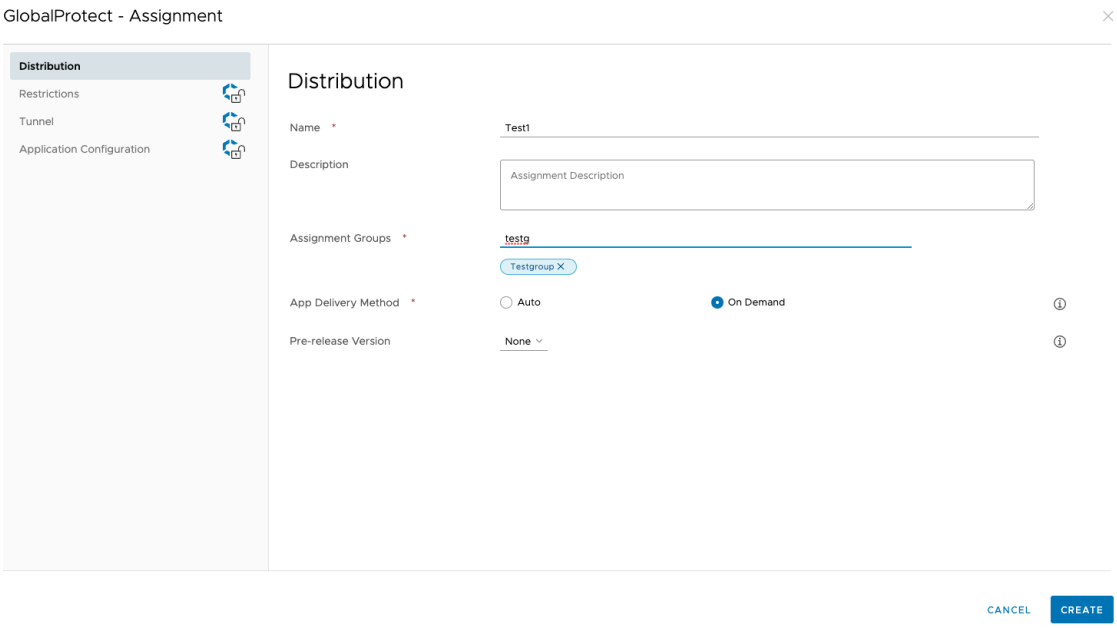
3. Configurez les options de déploiement pour l'application GlobalProtect :

   *Si vous avez ajouté l'application précédemment mais n'avez pas assigné l'application à des groupes intelligents, sélectionnez le lien GlobalProtect dans la liste des applications (**Resources [Ressources]** > **Applications** > **Native** > **Public [Publique]**). Dans la section*

 ©2026 Palo Alto Networks, Inc.

Afficher les détails, sélectionnez ***Assign (Assigner)*** *>* ***Add Assignment (Ajouter une affectation)****.*

1. Dans l'onglet **Distribution**, spécifiez les informations suivantes :
   1. Entrez un **Name (Nom)** pour l'affectation.
   2. Sélectionnez un ou plusieurs **Assignment Groups (Groupes d'affectation)** qui auront accès à l'application GlobalProtect.
   3. Choisissez la **App Delivery Method (Méthode de livraison de l'application)**, soit **Auto (Automatique)**, qui transmet l'application automatiquement sur le périphérique, ou **On Demand (À la demande)** ce qui déploie l'application lorsque cela est nécessaire.



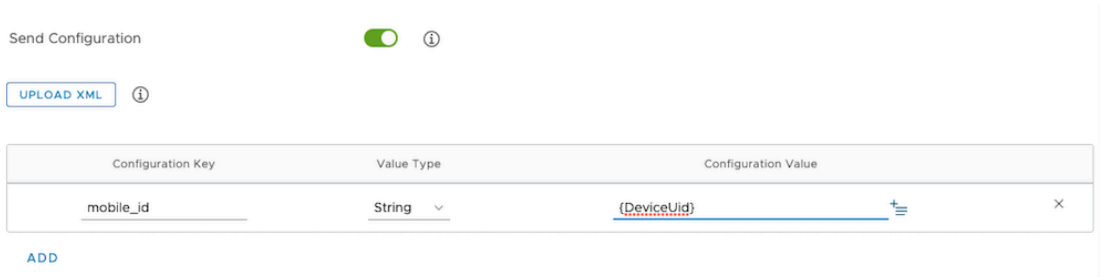
2. (Application GlobalProtect pour iOS ou Android uniquement) Dans l'onglet **Application Configuration (Configuration des applications)**, activez la configuration des applications pour utiliser l'UDID afin d'identifier le terminal.
   - **iOS** : pour utiliser intégration HIP avec MDM pour votre déploiement GlobalProtect sur les appareils iOS, vous pouvez spécifier l'attribut UDID (Unique Device Identifier).

 ©2026 Palo Alto Networks, Inc.

Pour plus d'informations, reportez-vous à la section Configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide de Workspace ONE.

Activez **Send Configuration (Envoyer la configuration)** et ajoutez les paires clé-valeur suivantes :

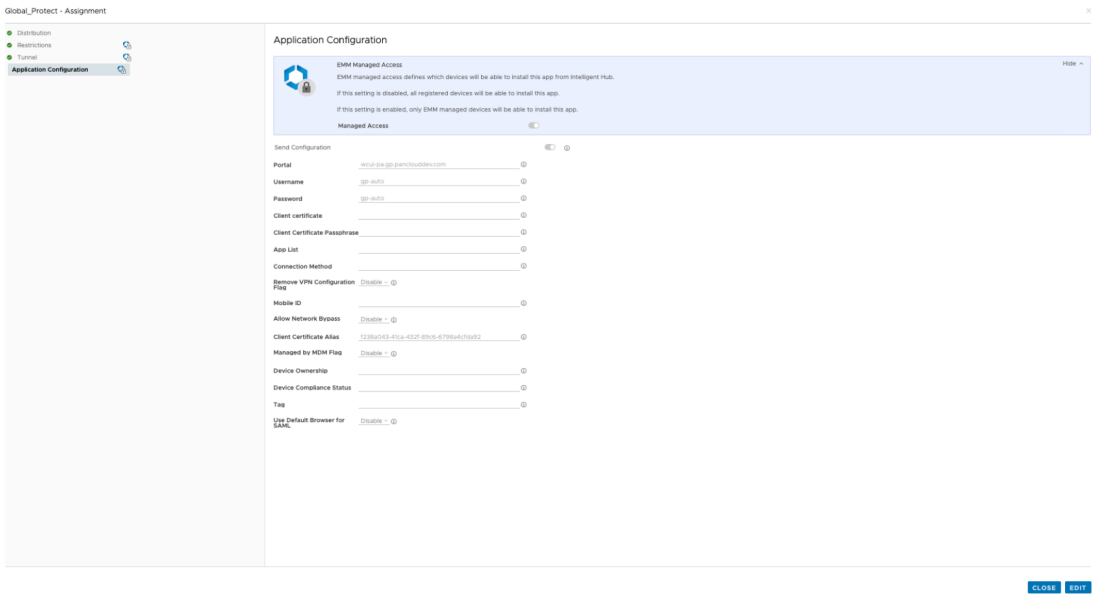
- **Configuration Key (Clé de configuration)**–**`mobile_id`**
- **Value Type (Type de valeur)**–**`String (Chaîne)`**
- **Configuration Value (Valeur de configuration)**–**`{DeviceUid}`**



- **Android** : activez l'option **Send Configuration (Envoyer la configuration)** et spécifiez les paramètres de la configuration de l'application qui sont pertinents pour votre entreprise :
  - **Portal (portail)**: Adresse IP ou nom de domaine complet (FQDN) du portail.
  - **Username (Nom d'utilisateur)**: nom d'utilisateur pour l'authentification de portail.
  - **Password (mot de passe)**: Mot de passe pour l'authentification de portail.
  - **Client Certificate (Certificat client)** : certificat client pour l'authentification du portail.
  - **Client Certificate Passphrase (Phrase secrète du certificat client)** : phrase de passe pour le certificat client.
  - **App List (Liste des applications)**: commencez la chaîne par le mot-clé **allowlist (liste d'autorisations)** ou le mot-clé **blocklist(liste de blocages)** suivi d'un signe deux-points, puis suivez-la avec un tableau de noms d'application séparés par des points-virgules. La liste de blocage ou la liste d'autorisation vous permet de contrôler quel trafic d'application peut passer par le tunnel VPN dans une configuration VPN par application (par exemple, **`allowlist| blocklist: com.google.calendar; com.android.email; com.android.chrome (liste d'autorisation| liste de blocage : com.google.calendar ; com.android.email ; com.android.chrome)`**).
  - **Connection Method (Méthode de connexion)** : méthode de connexion VPN (par exemple, **`user-logon | on-demand (ouverture de session utilisateur | à la demande)`**).
  - **Remove VPN Configuration Flag (Supprimer l'indicateur de configuration VPN)**: indicateur pour supprimer la configuration VPN.
  - **Mobile ID (ID mobile)**: Identifiant unique utilisé pour identifier les points de terminaison mobiles, selon la configuration d'un système MDM tiers.

 ©2026 Palo Alto Networks, Inc.

- **Allow Network Bypass (Autoriser le contournement du réseau)**: indicateur pour permettre au trafic d'application de contourner le tunnel VPN.
- **Client Certificate Alias (pseudo du certificat client)**: Nom unique utilisé pour identifier le certificat client lors de l'authentification au portail ou à la passerelle.
- Spécifiez le**Managed by MDM Flag (indicateur Géré par MDM)** pour indiquer si l'appareil est inscrit auprès d'un serveur MDM.
- **Device ownership (appartenance du périphérique)** : Catégorie d'appartenance du périphérique (par exemple, **`Employee Owned (appartient à l'employé)`**).
- **Device Compliance Status (État de conformité du périphérique)**: état de conformité qui indique si le périphérique est conforme aux politiques de conformité que vous avez définies.
- **Tag (étiquette)**: les étiquettes vous permettent d'identifier les périphériques. Chaque tag doit être séparée par une virgule.
- **Use Default Browser for SAML (Utiliser le navigateur par défaut pour SAML)**: pour activer ou désactiver le navigateur système par défaut pour l'authentification SAML.



4. Cliquez sur **Create (Créer)** puis **Save (Enregistrer)** pour prévisualiser les appareils assignés.

5. Cliquez sur **Publish (Publier)** pour pousser le catalogue d'applications vers les terminaux dans les groupes intelligents que vous avez assignés.

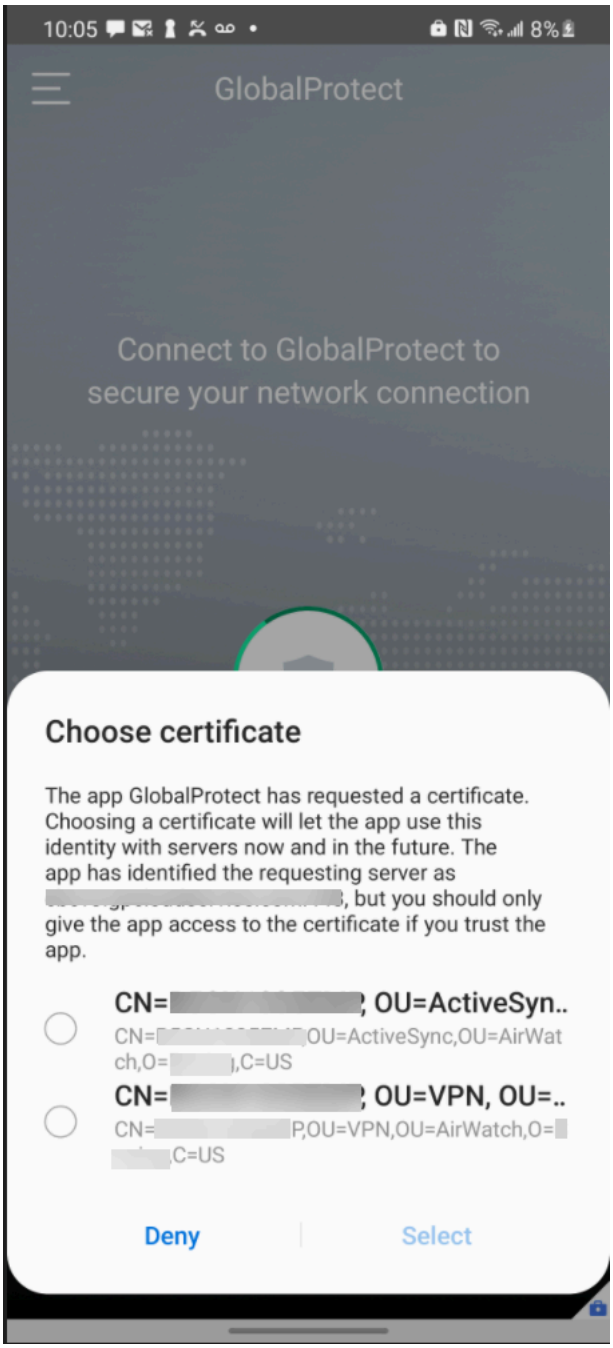
 ©2026 Palo Alto Networks, Inc.

Déléguer des certificats GlobalProtect pour les points de terminaison Android à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Lorsque plusieurs certificats client sont disponibles pour l'authentification client GlobalProtect sur les terminaux Android, l'invite contextuelle Choisir un certificat apparaît, invitant les utilisateurs de l'application GlobalProtect à sélectionner manuellement un certificat client spécifique.

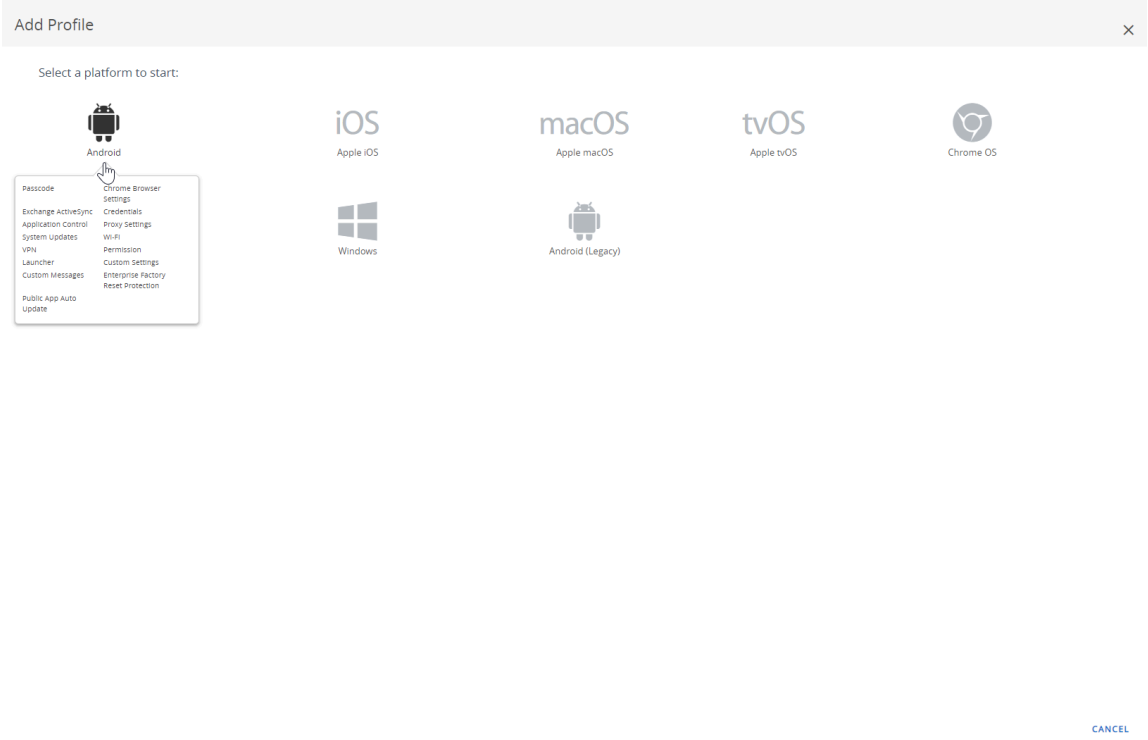
 ©2026 Palo Alto Networks, Inc.



À partir d'Android 8 ou d'une version ultérieure, vous pouvez déléguer la sélection de certificats à l'application GlobalProtect 5.2.5 ou une version ultérieure. Vous pouvez utiliser Workspace ONE pour accorder l'autorisation à l'application GlobalProtect pour la délégation de certificats dans le cadre du profil VPN qui est poussé depuis le serveur Mobile Device Management (gestion des appareils mobiles - MDM). Cela permet à l'application GlobalProtect de sélectionner un certificat client en fonction de l'alias du certificat client sans inviter d'abord les utilisateurs de l'application GlobalProtect à sélectionner manuellement un certificat sur leur point de terminaison Android. Par conséquent, l'invite contextuelle Choisir un certificat n'apparaît pas sur le point de terminaison Android. Si vous déployez des certificats de client à partir du serveur MDM au moyen d'une tout autre méthode, les certificats ne peuvent être utilisés par l'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

1. Téléchargement de l'application GlobalProtect pour Android
   - Déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   - Téléchargez l'app GlobalProtect directement à partir de Google Play.
2. Depuis la console Workspace ONE, modifiez un profil Android existant ou ajoutez-en un nouveau.
   1. Sélectionnez **Resources (Ressources)** > **Profiles & Baselines (Profils et Références)** > **Profiles (Profils)**, puis **ADD (AJOUTER)** un nouveau profil.
   2. Sélectionnez **Android** dans la liste des plateformes.



3. Configurez l'un des **General settings (paramètres généraux)** appropriés pour votre entreprise.

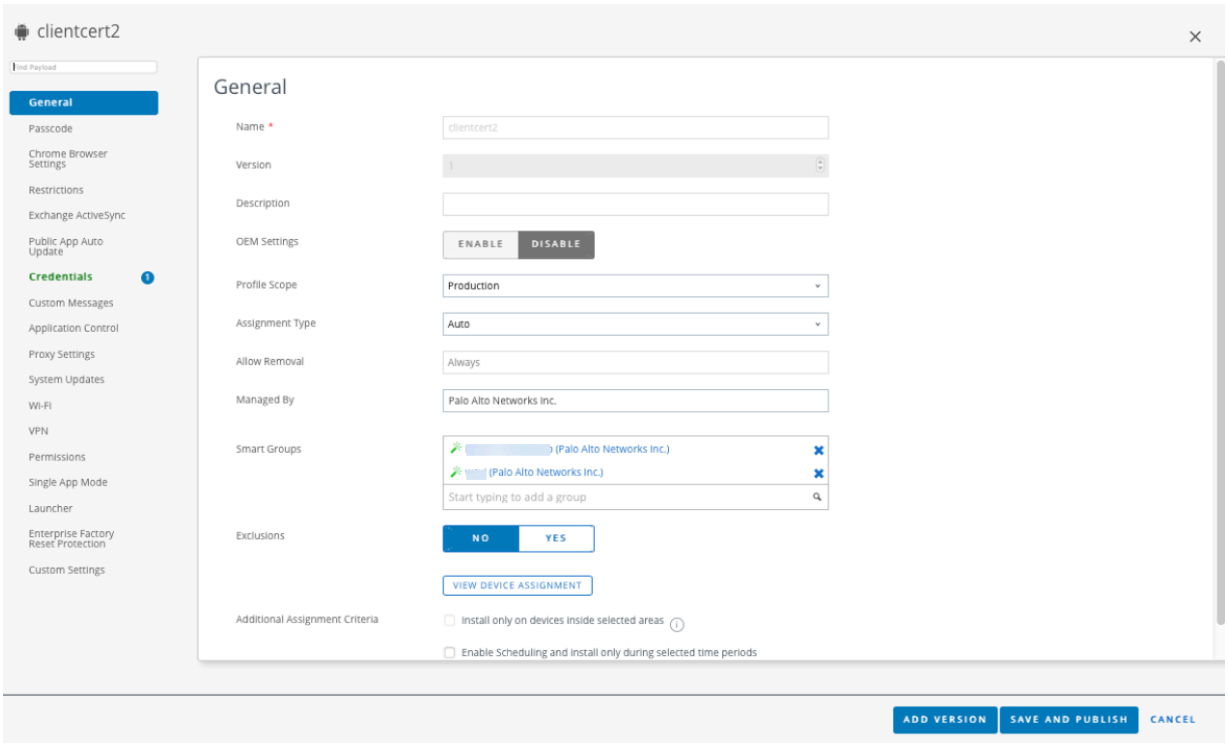
Paramètre	Description
Nom	Saisissez le nom du profil.
Description	Saisissez une brève description du profil qui indique son but.
Paramètres OEM	Spécifiez s'il faut activer ou désactiver les **OEM Settings (paramètres OEM)**.
Profile Scope (portée du profil)	Sélectionnez soit **Production**, **Staging (Mise en scène)** ou **Both (Les deux)**.

 ©2026 Palo Alto Networks, Inc.

Paramètre	Description
Assignment Type (Type d'affectation)	Déterminez comment le profil est déployé sur les points de terminaison. Sélectionnez **Auto** pour déployer automatiquement le profil sur tous les points de terminaison, **Optional (Optionnel)** pour permettre à l'utilisateur final d'installer le profil à partir du portail SSP (portail libre-service) ou de déployer manuellement le profil sur des points de terminaison individuels, ou **Compliance (Conformité)** pour déployer le profil lorsqu'un utilisateur final enfreint une politique de conformité applicable au point de terminaison.
Allow Removal (Autoriser la suppression)	Déterminez s'il faut supprimer le profil de l'utilisateur final. Sélectionner **Always (Toujours)** pour permettre à l'utilisateur final de supprimer manuellement le profil à tout moment, **Never (Jamais)** pour empêcher l'utilisateur final de supprimer le profil, ou **With Authorization (Avec autorisation)** pour permettre à l'utilisateur final de supprimer le profil avec l'autorisation de l'administrateur. Le choix de **With Authorization (Avec autorisation)** ajoute un champ Password (Mot de passe) qui doit obligatoirement être renseigné.
Managed By (Géré par)	Saisissez le groupe de l'entreprise ayant un accès administratif au profil.
Smart Groups (Groupes intelligents)	Ajoutez les Groupes intelligents auxquels vous souhaitez ajouter le profil. Ce champ comprend une option permettant la création d'un nouveau groupe intelligent pour lequel vous pouvez configurer les spécifications suivantes : exigences minimales en matière de système d'exploitation, modèles de périphérique, catégories de propriété, groupes de l'entreprise, parmi tant d'autres.
Exclusions	Indiquez si vous souhaitez inclure des exclusions. Si vous sélectionnez **Yes (Oui)**, le champ **Excluded Groups (Groupes exclus)** s'affiche, vous permettant de sélectionner les

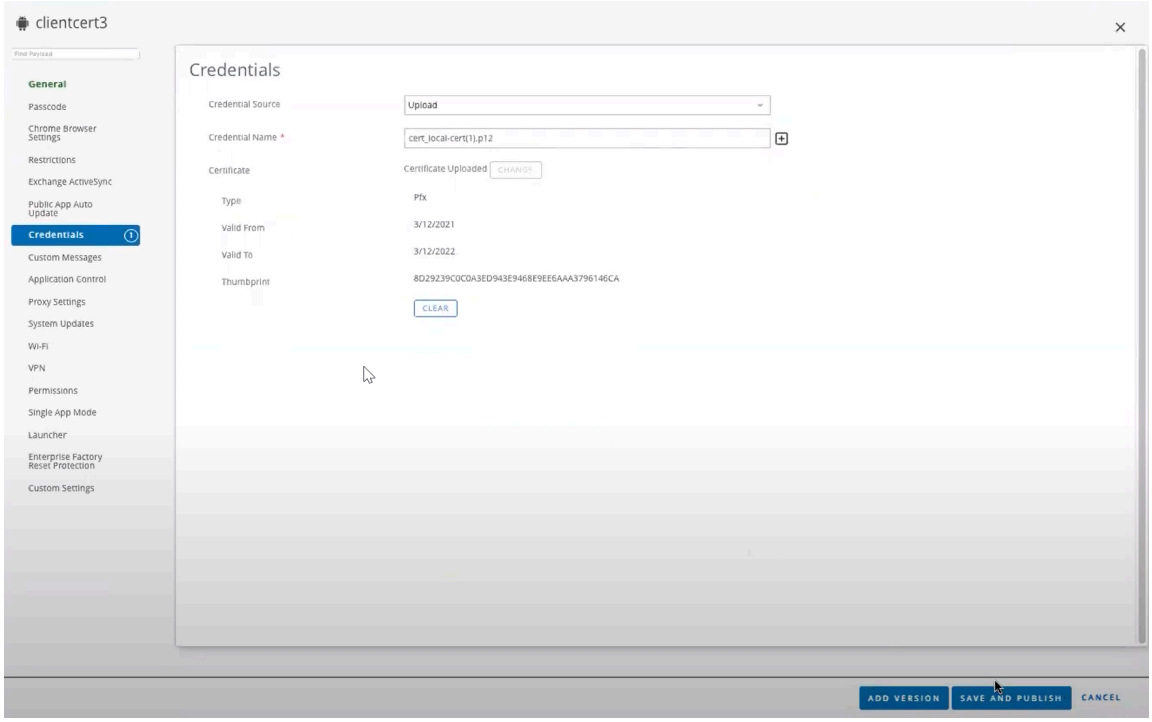
 ©2026 Palo Alto Networks, Inc.

Paramètre	Description
	groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.



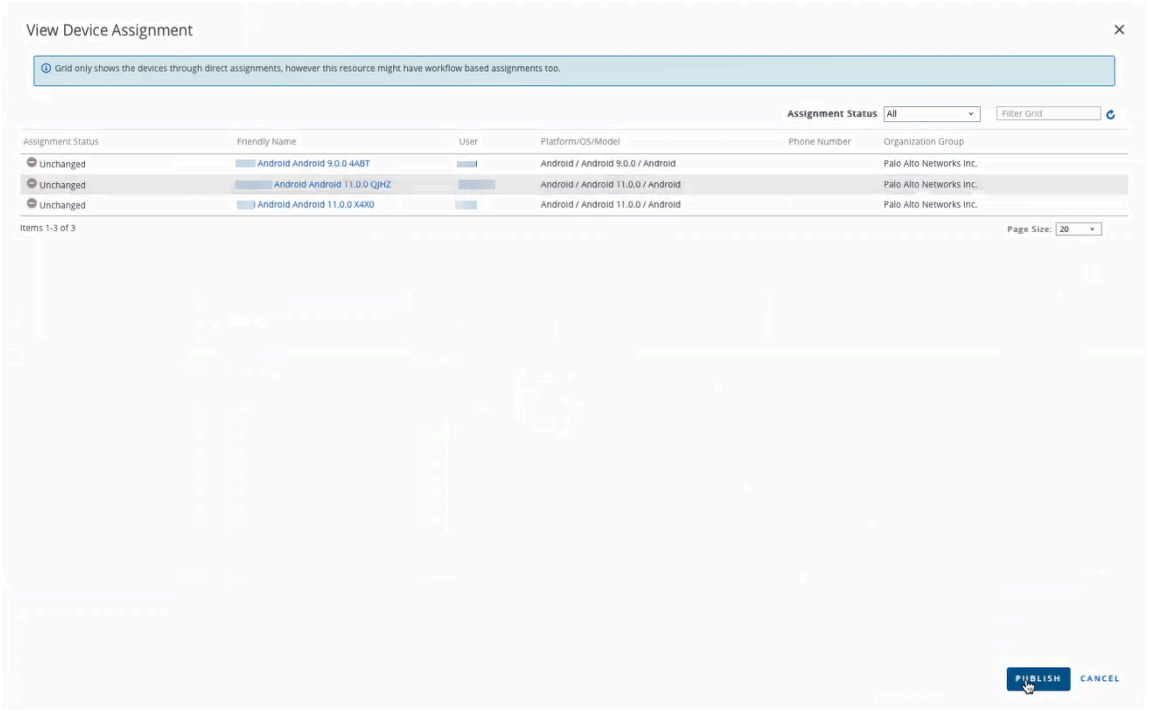
 ©2026 Palo Alto Networks, Inc.

4. Pour votre déploiement GlobalProtect, configurez les paramètres des **Credentials (informations d'identification)** pour télécharger un certificat client manuellement et pour créer un profil d'informations d'identification :
   1. Sélectionnez **Resources (Ressources)** > **Profiles & Baselines (Profils & références)** > **Profiles (Profils)** > **Add Profile (Ajouter profil)**.
   2. Sélectionnez la **Platform (plate-forme)** (**Android**).
   3. Sélectionnez **Credentials (Informations d'identification)**, puis **Configure (Configurer)**.
   4. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
   5. Saisissez un **Credential Name (Nom d'informations d'identification)**.
   6. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
   7. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.
   8. Cliquez sur **SAVE AND PUBLISH (Enregistrer et publier)** pour enregistrer vos modifications.



9. Cliquez sur **PUBLISH (PUBLIER)** pour pousser le point de terminaison vers les **Assigned Smart Groups (Groupes intelligents attribués)** qui auront accès à cette application.

 ©2026 Palo Alto Networks, Inc.



5. Vérifiez le profil d'informations d'identification et l'attribut d'identifiant unique universel (UUID).

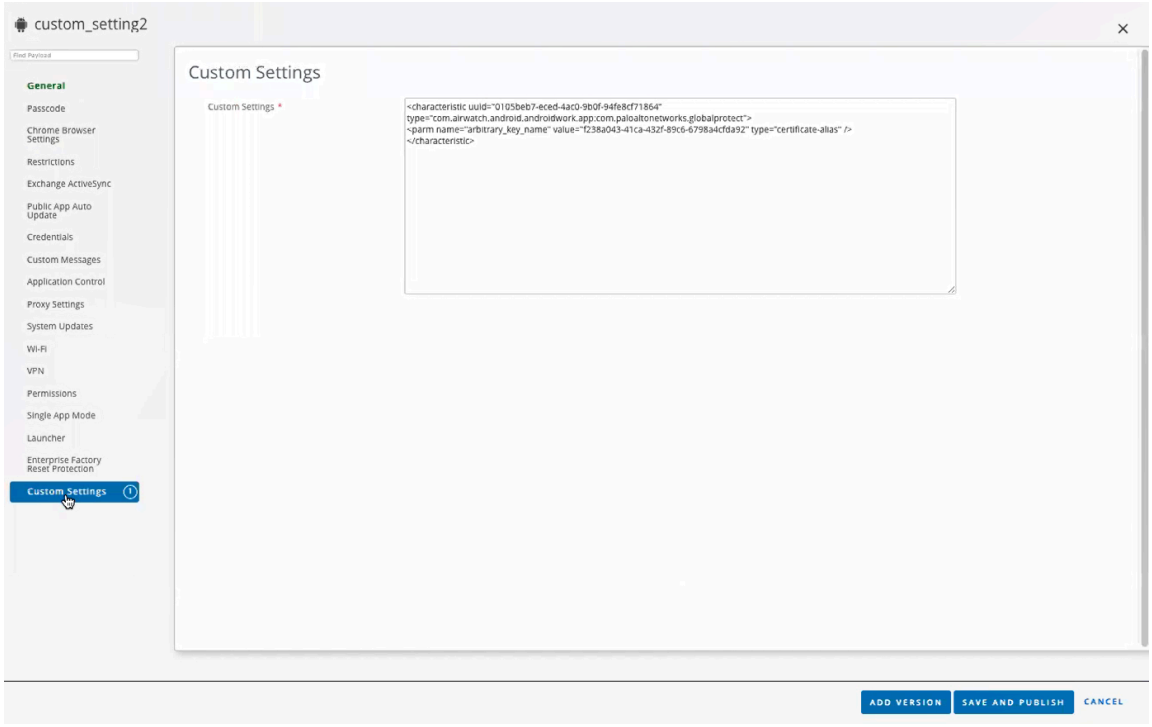
   1. Sélectionnez **Resources (Ressources)** > **Profiles & Baselines (Profils & références)** > **Profiles (Profils)**.
   2. Sélectionnez le bouton radio en regard du nouveau profil d'informations d'identification que vous avez ajouté à l'étape précédente, puis sélectionnez **</>XML** en haut du tableau.

      Vous pouvez modifier les éléments `arbitraire_key_name` et `UUID_from_profile` pour éviter les conflits de paramètres de paramètres et de noms de clé avec les paires clé-valeur (KVP) existantes que vous avez appliquées à un fichier de configuration géré de l'application GlobalProtect, comme illustré dans l'exemple de configuration suivant.

```
<characteristicuuid="0105beb7-eced-4ac0-9b0f-94fe8cf71864"
 type="com.airwatch.android.androidwork.app:your_package_id">
 <parm name="arbitrary_key_name" value="UUID_from_profile"
 type="certificate-alias" /> </characteristic>
```

 ©2026 Palo Alto Networks, Inc.

6. Créez un profil de paramètres personnalisés pour supprimer les notifications de sélection de certificat sur l'application GlobalProtect pour les points de terminaison Android.
   1. Sélectionnez **Resources (Ressources)** > **Profiles & Baselines (Profils & références)** > **Profiles (Profils)** > **Add Profile (Ajouter profil)**.
   2. Sélectionnez la **Platform (plate-forme)** (**Android**).
   3. Sélectionnez **Custom Settings (Paramètres personnalisés)** > **Configure (Configurer)**, puis copiez et collez la configuration modifiée.
   4. Cliquez sur **SAVE AND PUBLISH (Enregistrer et publier)** pour enregistrer vos modifications.

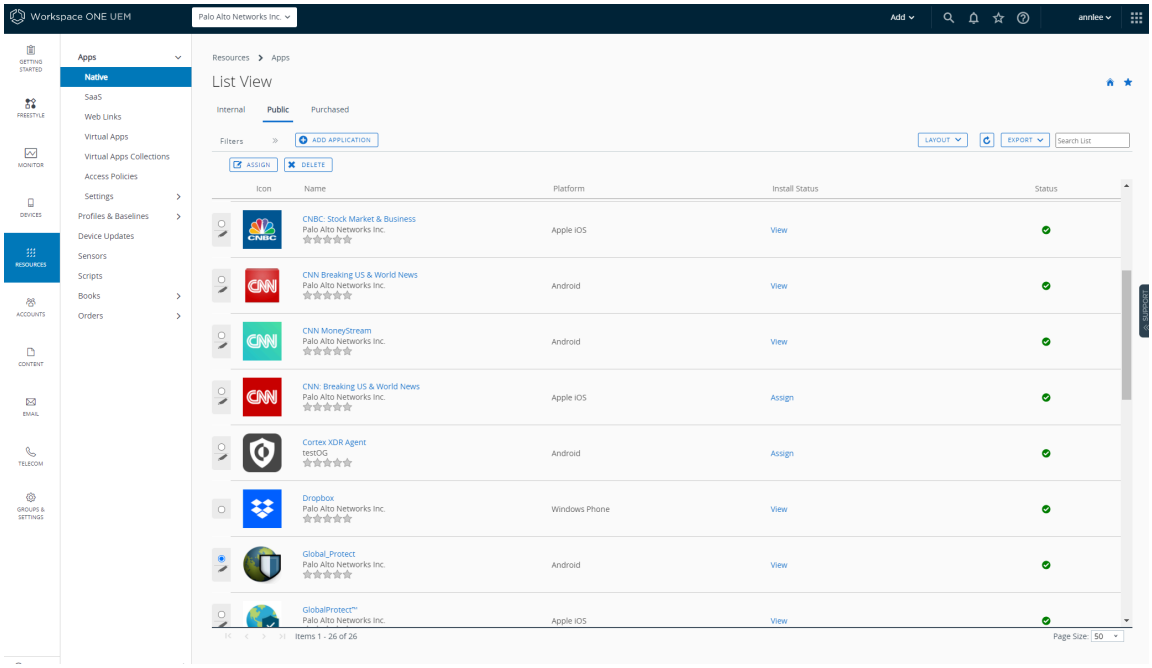


 ©2026 Palo Alto Networks, Inc.

7. Configurez les paramètres du profil VPN pour modifier les paramètres d'une application gérée existante.

Après avoir configuré les paramètres de l'application, vous pouvez publier l'application auprès d'un groupe d'utilisateurs et Workspace ONE peut intercepter la demande de sélection de certificat pour fournir le bon certificat à GlobalProtect.

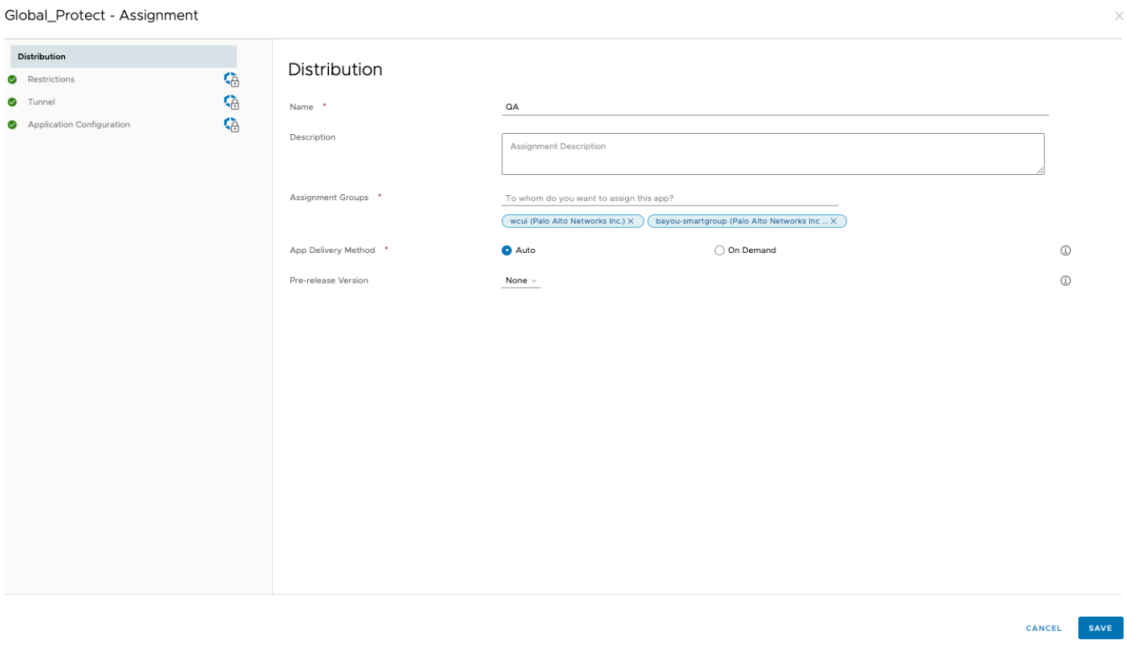
1. Sélectionnez > **Native** > **Public (publique)**.
2. Pour modifier les paramètres d'une application existante, recherchez l'application dans la liste des applications publiques (Vue liste), puis sélectionnez l'icône Modifier ( ) dans le menu d'action qui se trouve à côté de la rangée.



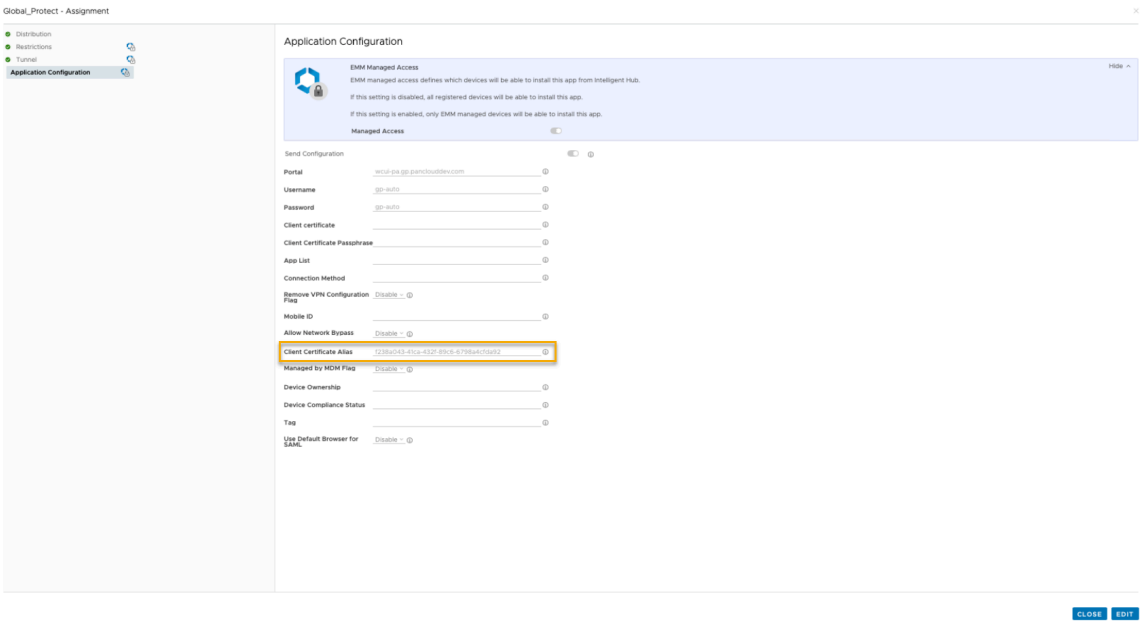
3. Sélectionnez l'application nouvellement ajoutée dans la liste des applications publiques (List View).
4. Sélectionnez **Assignment (Affectation)**, puis une affectation existante.

   La fenêtre **Distribution** affiche les **Assigned Smart Groups (Groupes intelligents attribués)** qui ont accès à l'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.



5. Sélectionnez **Application Configuration (Configuration des applications)**. Pour plus de détails sur les autres paramètres pertinents dans la configuration de l'application qui sont pertinents pour votre entreprise, voir Déployer l'application mobile GlobalProtect à l'aide de Workspace ONE.
6. Dans le champ **Client Certificate Alias (Alias du certificat client)**, spécifiez la même valeur UUID que vous avez utilisée pour le profil d'informations d'identification. Le **Client Certificate Alias (alias du certificat client)** est la valeur UUID unique utilisée pour identifier le certificat client lors de l'authentification du portail ou de la passerelle.
7. Cliquez sur **Edit (Modifier)** pour modifier les paramètres.



 ©2026 Palo Alto Networks, Inc.

Déployer l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

À partir de la version 5.0 de l'application GlobalProtect, vous pouvez déployer l'application GlobalProtect pour Android sur les Chromebooks gérés qui sont inscrits auprès de Workspace ONE. Après avoir déployé l'application, configurez et déployez un profil VPN pour configurer automatiquement l'application GlobalProtect pour les utilisateurs finaux.

L'application GlobalProtect pour Android n'est prise en charge que sur certains Chromebook. Les Chromebook qui ne prennent pas en charge les applications Android doivent continuer d'exécuter l'application GlobalProtect pour Chrome, qui n'est pas prise en charge à partir de la version 5.0 de l'application GlobalProtect.

Ne déployez pas l'application GlobalProtect pour Android et l'application GlobalProtect pour Chrome sur le même Chromebook.

Utilisez les étapes suivantes pour déployer l'application GlobalProtect pour Android sur les Chromebooks gérés à l'aide de Workspace ONE :

1. Configurez la console Google Admin.

   La console Google Admin vous permet de gérer les services Google des utilisateurs de votre organisation. Workspace ONE utilise la console d'administration Google pour l'intégration avec les Chromebooks.

   1. Connectez-vous à la console Google Admin en tant qu'administrateur.
   2. À partir de la console, sélectionnez **Security (Sécurité)** > **Advanced Settings (Paramètres avancés)** > **Manage API client access (Gérer l'accès client à l'API)**.
   3. Dans le champ **Client Name (Nom du client)**, saisissez l'ID de client qui vous a été fourni par Workspace ONE.
   4. Dans le champ **One or More API Scopes (une ou plusieurs étendues d'API)**, saisissez les étendues d'API Google suivantes pour lesquelles vous voulez contrôler l'accès applicatif :

      Chaque étendue d'API doit être séparée par une virgule.

      - https://www.googleapis.com/auth/chromedevicemanagementapi
      - https://www.googleapis.com/auth/admin.directory.user
      - https://www.googleapis.com/auth/admin.directory.device.chromeos
   5. Cliquez sur **Authorize (Autoriser)**.
   6. Activez **Chrome Management - Partner Access (Gestion de Chrome - Accès des partenaires)** pour les politiques des périphériques (**Device Management (Gestion des périphériques)** > **Device Settings (Paramètres des périphériques)** > **Chrome Management (Gestion de Chrome)** > **Device Settings (Paramètres des périphériques)**) et

 ©2026 Palo Alto Networks, Inc.

les politiques d'utilisateurs (**Device Management (Gestion des périphériques)** > **Device Settings (Paramètres des périphériques)** > **Chrome Management (Gestion de Chrome)** > **User Settings (Paramètres de l'utilisateur)**).

2. Enregistrez Workspace ONE en tant que fournisseur Enterprise Mobility Management (Gestion de la mobilité d'entreprise ; EMM) pour Google.

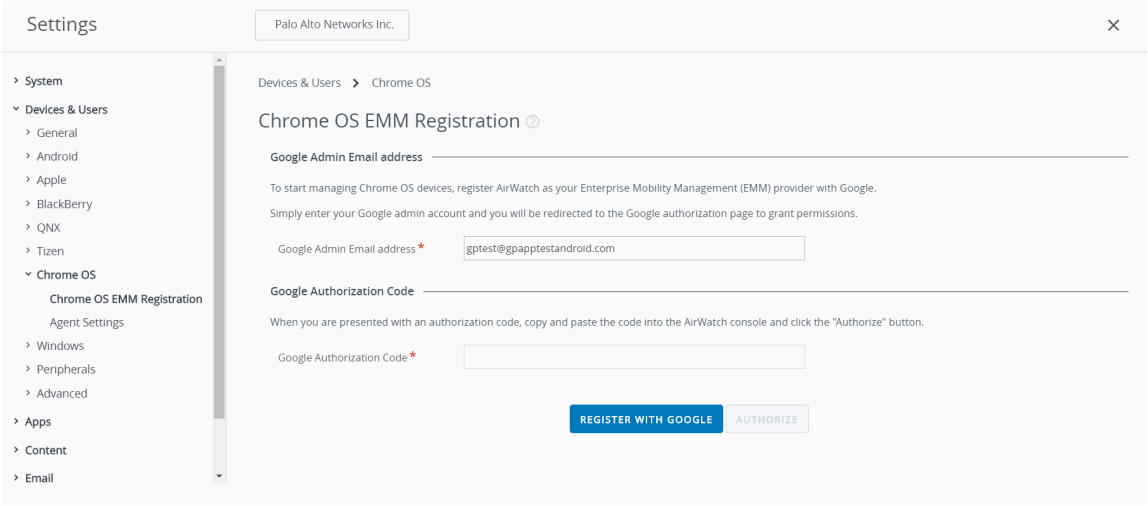
Pour gérer les Chromebooks à l'aide de Workspace ONE, vous devez enregistrer Workspace ONE sur la console d'administration Google.

1. Connectez-vous à votre console Workspace ONE.
2. Sélectionnez **Devices (Périphériques)** > **Devices Settings (Paramètres des périphériques)** > **Devices & Users (Périphériques et utilisateurs)** > **Chrome OS (Système d'exploitation**

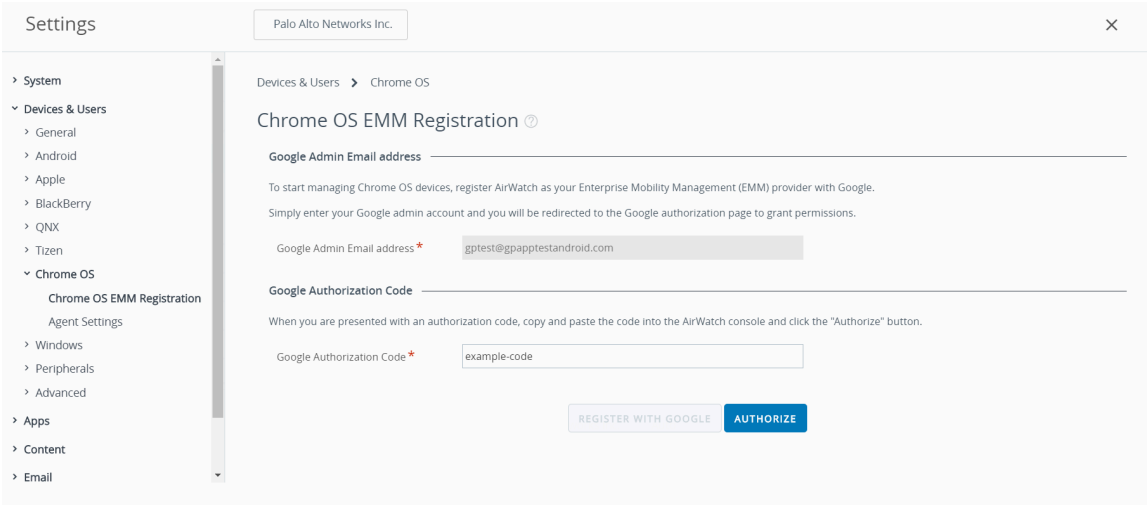
 ©2026 Palo Alto Networks, Inc.

Chrome) > Chrome OS EMM Registration (Enregistrement de l'EMM du système d'exploitation Chrome).

3. Saisissez la **Google Admin Email address (Adresse électronique de l'administrateur Google)** que vous avez utilisée pour accéder à la console Google Admin.
4. Cliquez sur **REGISTER WITH GOOGLE (Enregistrer auprès de Google)**. Vous serez redirigé vers la page d'autorisation de Google, où vous pouvez obtenir un code d'autorisation Google.



5. Saisissez le **Google Authorization Code (Code d'autorisation Google)** que vous avez obtenu sur la page d'autorisation de Google.
6. Cliquez sur **AUTHORIZE (Autoriser)** pour terminer l'enregistrement.



 ©2026 Palo Alto Networks, Inc.

3. Inscrivez vos Chromebooks sur Workspace ONE.

Avant de commencer à gérer vos Chromebooks à l'aide de Workspace ONE, vous devez inscrire vos Chromebooks à Workspace ONE et les synchroniser.

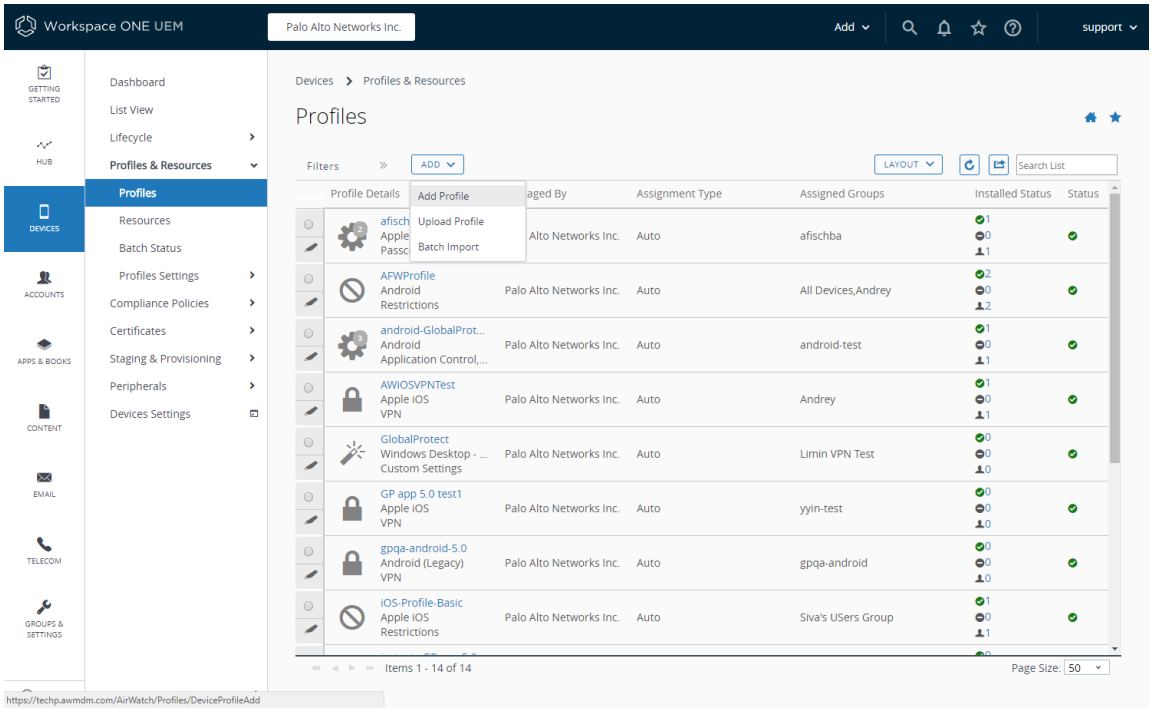
1. À partir de votre Chromebook, appuyez sur **CTRL+ALT+E** pour ouvrir l'écran d'inscription d'entreprise.
2. Saisissez le nom d'utilisateur et le mot de passe qui figuraient dans votre lettre de bienvenue à Google Admin ou saisissez vos informations d'identification d'utilisateur G Suite.
3. Cliquez sur **Enroll device (Inscrire le périphérique)**. Vous recevrez un message de confirmation lorsque le Chromebook aura été inscrit avec succès.
4. Connectez-vous à votre console Workspace ONE.
5. Sélectionnez **Devices (Périphériques)** > **Devices Settings & Users (Paramètres des périphériques et utilisateurs)** > **Chrome OS (Système d'exploitation Chrome)** > .
6. Cliquez sur **Device Sync (Synchronisation du périphérique)** pour synchroniser tous les Chromebook inscrits à Workspace ONE.

 ©2026 Palo Alto Networks, Inc.

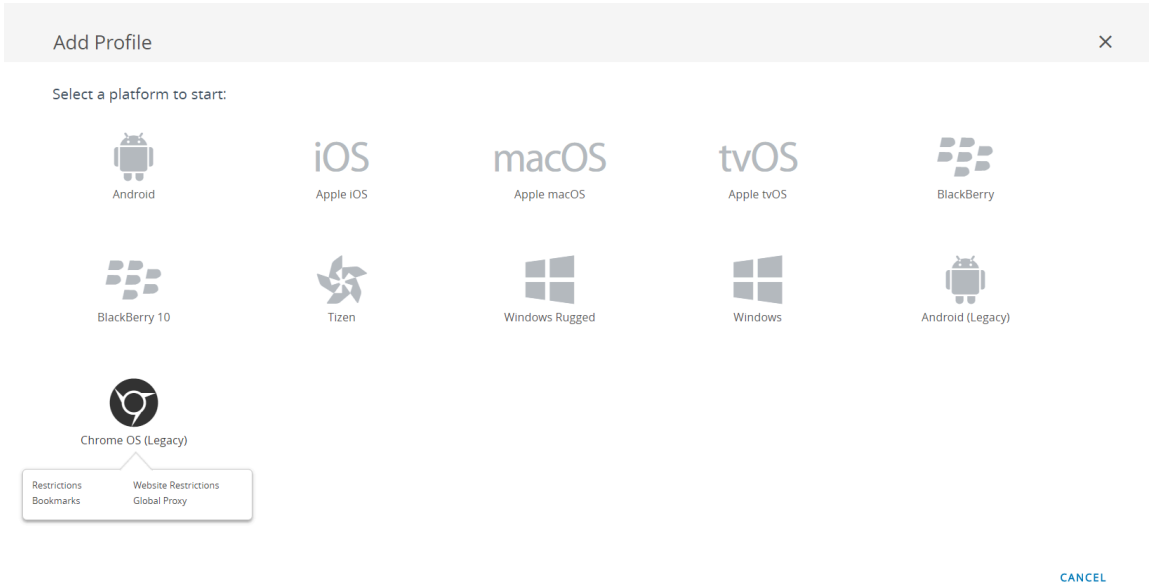
4. Ajoutez l'application GlobalProtect pour Android à un profil Chrome OS sur Workspace ONE.

Le profil de **Application Control (Contrôle des applications)** vous permet d'ajouter des applications à partir de Google Play et de la boutique Web de Chrome.

1. Connectez-vous à votre console Workspace ONE.
2. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)** pour**ADD (AJOUTER)** un nouveau profil Chrome OS.



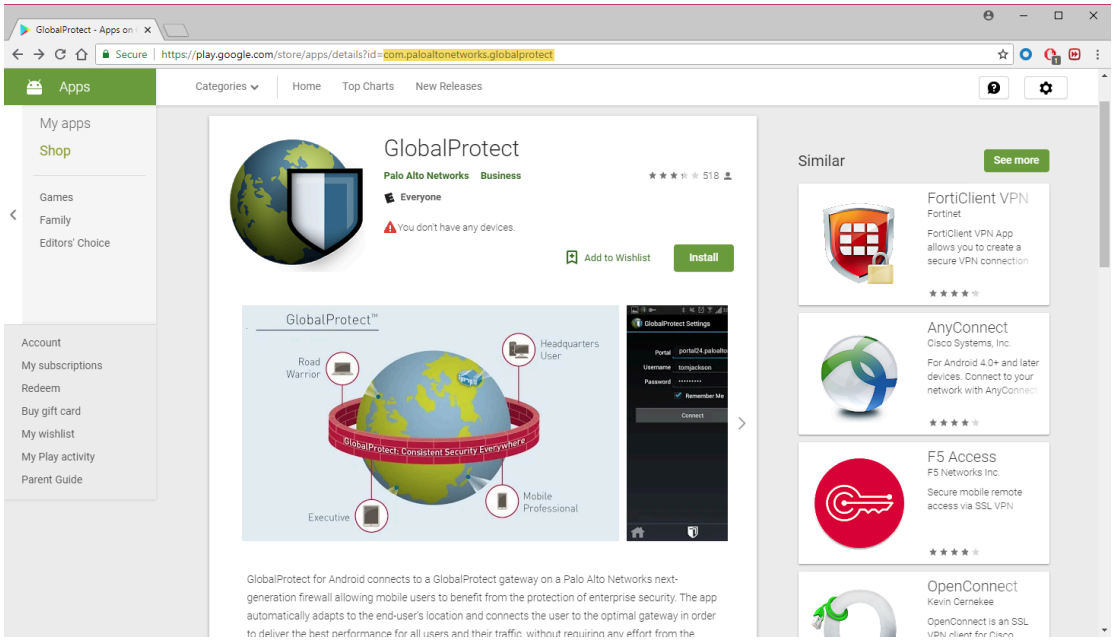
3. Sélectionnez **Chrome OS (Legacy) (Chrome OS (hérité)** de la liste de la plateforme.



4. Configurez les paramètres **General (généraux)**.
5. Configurez les paramètres de **Application Control (Contrôle des applications)**.

 ©2026 Palo Alto Networks, Inc.

1. Saisissez l'**App ID** de GlobalProtect qui s'affiche dans l'URL de Google Play (com.paloaltonetworks.globalprotect).



2. Saisissez le **Name (Nom)** de l'application.
3. Spécifiez si vous voulez **Pin App to Shelf (Épingler l'application à la tablette)**. Saisissez **Y (O)** pour épingler l'application à la tablette des applications Chromebook.
4. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

Configurer Workspace ONE pour les terminaux iOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

L'application GlobalProtect peut être déployée et configurée à l'aide de Workspace ONE pour fournir aux terminaux mobiles gérés un accès sécurisé aux ressources internes de l'entreprise.

Lorsqu'il est déployé avec Workspace ONE pour les terminaux iOS, GlobalProtect prend en charge les méthodes de connexion suivantes :

- Toujours actif

  Dans une configuration toujours active, GlobalProtect se connecte automatiquement dès que vous vous connectez.

 ©2026 Palo Alto Networks, Inc.

- À la demande (configuration VPN d'accès à distance initié par l'utilisateur)

  Dans une configuration à la demande, vous devez vous connecter manuellement à GlobalProtect via l'application. Le trafic est acheminé via l'application GlobalProtect uniquement après que vous ayez initié et établi la connexion.
- Par application

  Dans une configuration par application, vous pouvez définir quelles applications gérées sont autorisées à acheminer le trafic via GlobalProtect. Pour ce faire, vous pouvez attacher un profil VPN à une application, ajouter des URL pour l'application à laquelle vous souhaitez accéder, ou faire une combinaison des deux.

Configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans une configuration de VPN toujours active, la connexion GlobalProtect sécurisée est toujours active. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est toujours acheminé via le tunnel VPN.

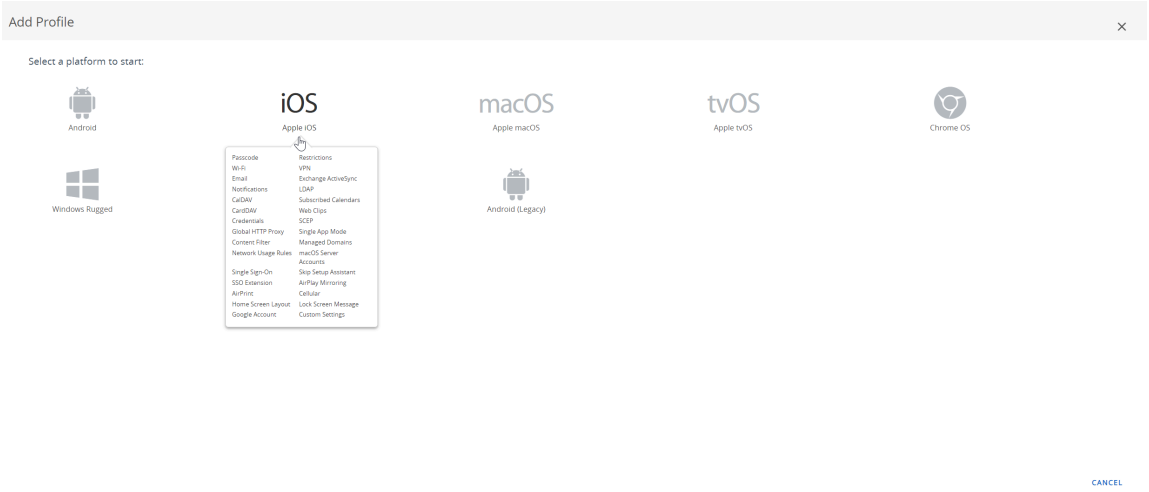
Utilisez les étapes suivantes pour configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide de Workspace ONE :

1. Téléchargement de l'application GlobalProtect pour Android
   - Déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   - Téléchargez l'app GlobalProtect directement à partir de l'App Store.

     L'app GlobalProtect pour iOS est disponible sur l'Apple App Store en Chine.

 ©2026 Palo Alto Networks, Inc.

2. Depuis la console AirWatch, modifiez un profil Apple iOS existant ou ajoutez-en un nouveau.
   1. Sélectionnez **Resources (Ressources)** > **Profiles & Baselines (Profils et références)** > **Profiles (Profils)** > **ADD (AJOUTER)**, puis **Add profile (Ajouter un profil)**.
   2. Sélectionnez **iOS** à partir de la liste de la plateforme.



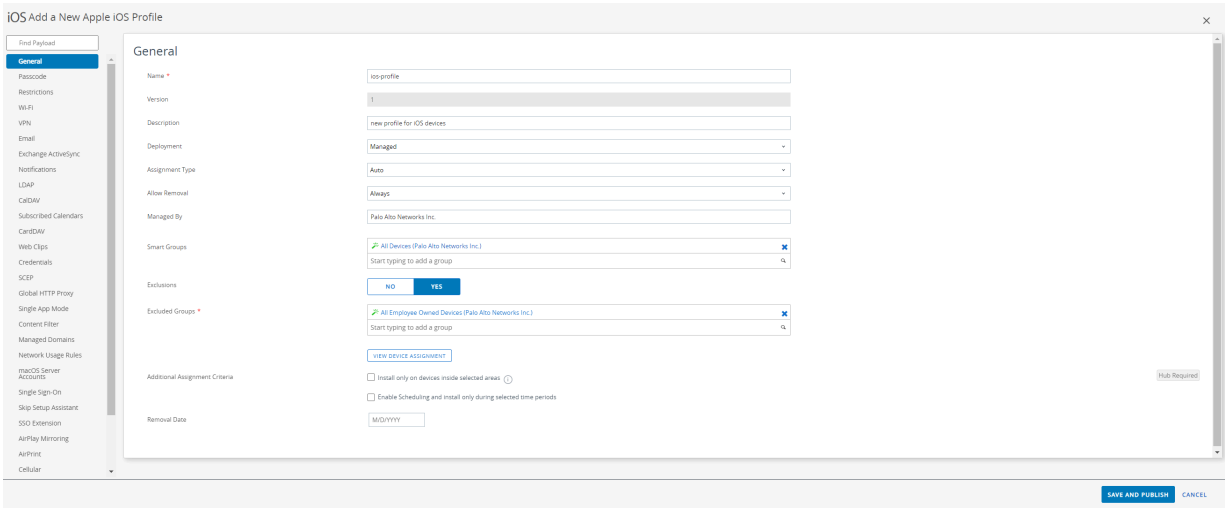
   3. Sélectionnez **Device Profile (Profil du périphérique)** dans la fenêtre **Select Context (sélectionner le contexte)**.

3. Configurez les paramètres **General (généraux)**.
   1. Saisissez un **Name (Nom)** pour le profil.
   2. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
   3. (Facultatif) Sélectionnez le mode de **Deployment (Déploiement)**, qui indique que le profil sera automatiquement supprimé au moment de la désinscription, soit **Managed (Géré)** (le profil est supprimé) ou **Manual (Manuel)** (le profil est installé jusqu'à ce qu'il soit supprimé par l'utilisateur final).
   4. (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les points de terminaison. Sélectionnez **Auto** pour déployer automatiquement le profil sur tous les points de terminaison, **Optional (Optionnel)** pour permettre à l'utilisateur final d'installer le profil à partir du portail SSP (portail libre-service) ou de déployer manuellement le profil sur des points de terminaison individuels, ou **Compliance (Conformité)** pour déployer le profil lorsqu'un utilisateur final enfreint une politique de conformité applicable au point de terminaison.
   5. (Facultatif) Sélectionnez si vous souhaitez **Allow Removal (Autoriser la suppression)** du profil par l'utilisateur final ou non. Sélectionner **Always (Toujours)** pour permettre à l'utilisateur final de supprimer manuellement le profil à tout moment, **Never (Jamais)** pour empêcher l'utilisateur final de supprimer le profil, ou **With Authorization (Avec autorisation)** pour permettre à l'utilisateur final de supprimer le profil avec l'autorisation de l'administrateur. Lorsque **With Authorization (Avec autorisation)** est sélectionné, un champ Password (Mot de passe) qui doit obligatoirement être renseigné s'ajoute.
   6. (Facultatif) Dans le champ **Managed By (Géré par)**, saisissez le groupe de l'entreprise ayant un accès administratif au profil.
   7. (Facultatif) Dans le champ **Assigned Groups (Groupes affectés)**, ajoutez les Groupes intelligents auxquels vous souhaitez ajouter le profil. Ce champ comprend une option

 ©2026 Palo Alto Networks, Inc.

permettant la création d'un nouveau groupe intelligent pour lequel vous pouvez configurer les spécifications suivantes : exigences minimales en matière de système d'exploitation, modèles de périphérique, catégories de propriété, groupes de l'entreprise, parmi tant d'autres.

8. (Facultatif) Indiquez si vous souhaitez ajouter des **Exclusions** à l'affectation de ce profil. Si vous sélectionnez **Yes (Oui)**, le champ **Excluded Groups (Groupes exclus)** s'affiche, vous permettant de sélectionner les groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.
9. (Facultatif) Si vous activez l'option visant à **Install only on devices inside selected areas (installer uniquement sur les périphériques dans des zones sélectionnées)**, le profil peut être installé seulement sur les points de terminaison dans des barrières géographiques ou des régions iBeacon spécifiques. Lorsque vous êtes invité à le faire, ajoutez les barrières géographoqies ou les régions iBeacon dans le champ **Assigned Geofence Areas (Zones de barrières géographiques affectées)**.
10. (Facultatif) Si vous **Enable Scheduling and install only during selected time periods (Activez la planification et installez uniquement lors des périodes de temps sélectionnées)**, vous pouvez appliquer un calendrier (**Devices (Périphériques)** > **Profiles & Resources (Profil et ressources)** > **Profiles Settings (Paramètres du profil)** > **Time Schedules (Calendriers)**) à l'installation du profil, ce qui limite les périodes de temps pendant lesquelles le profil peut être installé sur les points de terminaison. Lorsque vous êtes invité à le faire, saisissez le nom du calendrier dans le champ **Assigned Schedules (Calendriers affectés)**.
11. (Facultatif) Sélectionnez la **Removal Date (Date de suppression)** à laquelle vous voulez que le profil soit supprimé de tous les points de terminaison.



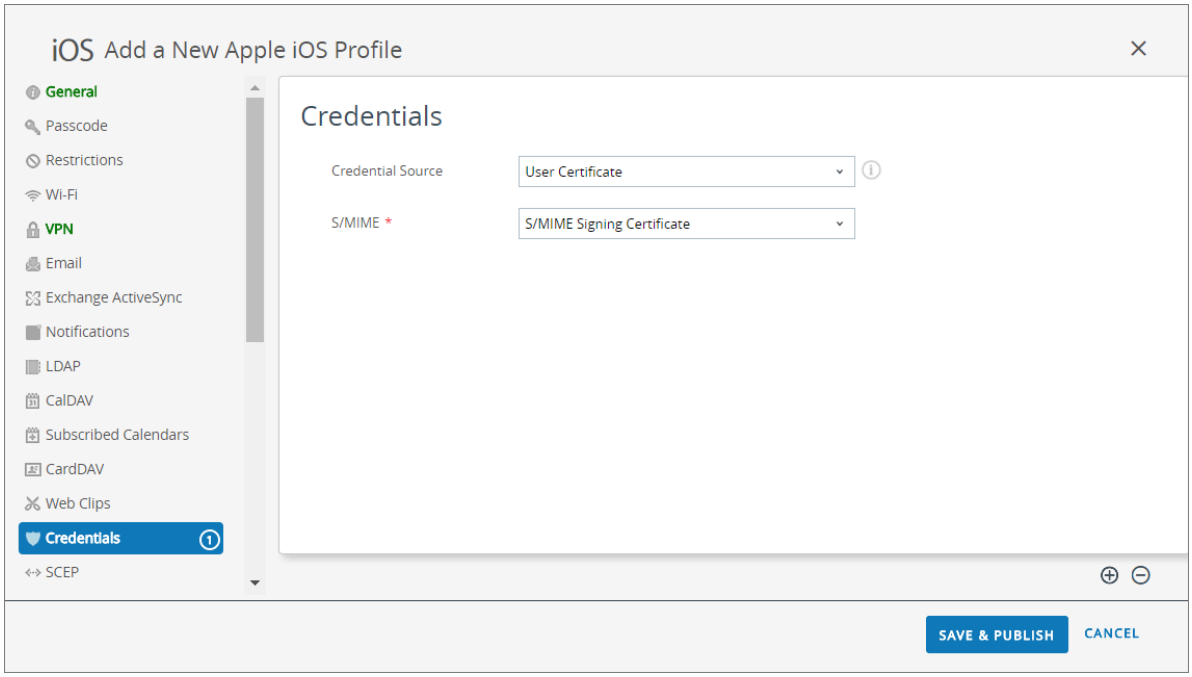
4. (Facultatif) Si votre déploiement GlobalProtect exige une authentification du certificat du client, configurez les paramètres des **Credentials (Informations d'identification)** :

   À partir de la version 12 d'iOS, si vous souhaitez utiliser les certificats de client pour procéder à l'authentification du client GlobalProtect, vous devez déployer les certificats de client dans le cadre du profil VPN qui est transmis du serveur MDM. Si vous déployez des certificats de

 ©2026 Palo Alto Networks, Inc.

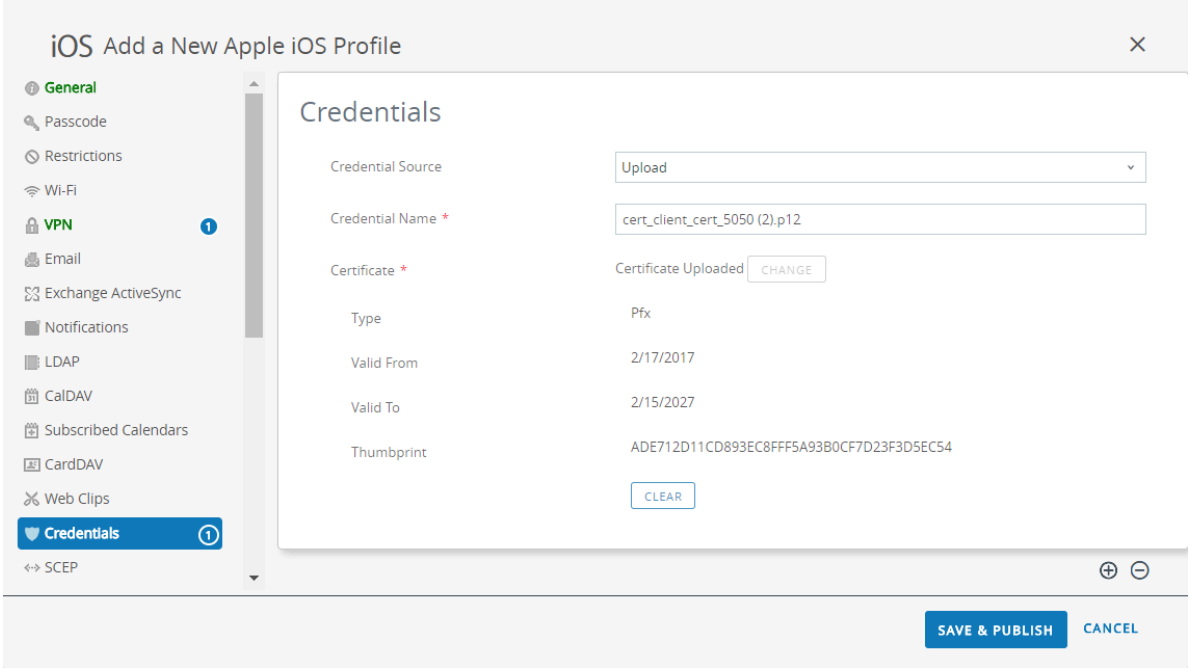
client à partir du serveur MDM au moyen d'une tout autre méthode, les certificats ne peuvent être utilisés par l'application GlobalProtect.

- Pour extraire les certificats de client des utilisateurs Workspace ONE :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).

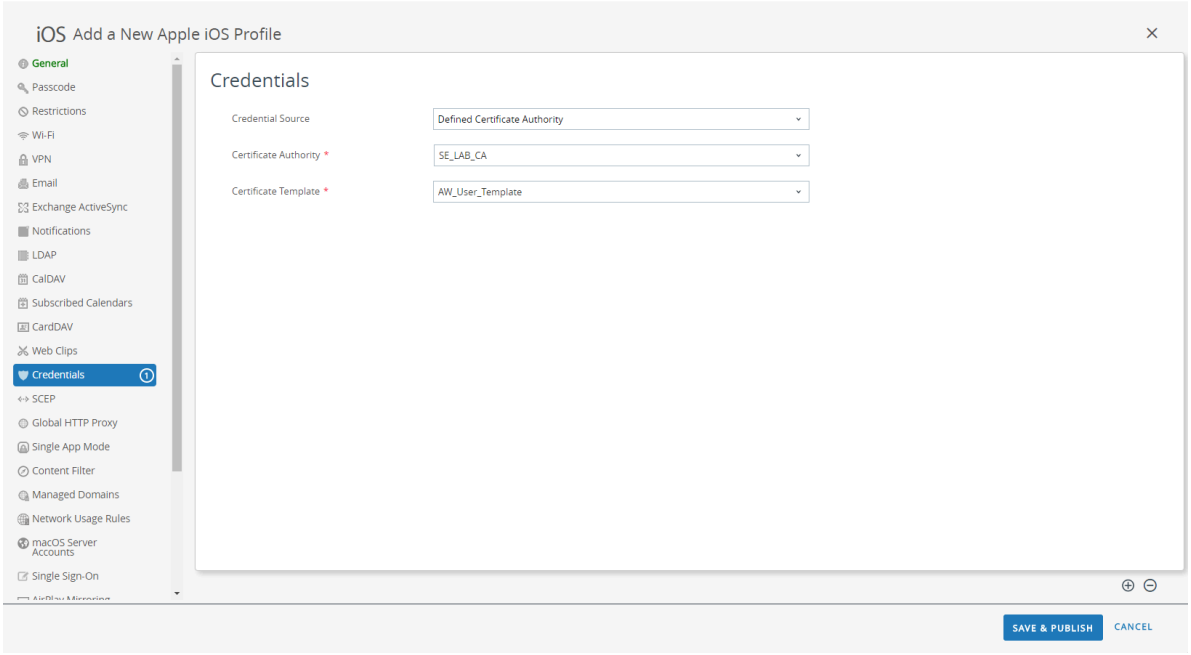


- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.

 ©2026 Palo Alto Networks, Inc.



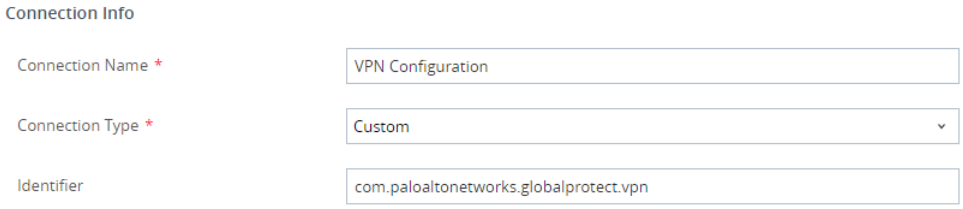
- Pour utiliser une autorité de certification et un modèle prédéfinis :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
  2. Sélectionnez la **Certificate Authority (Autorité de certification)** de laquelle vous souhaitez obtenir les certificats.
  3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.



 ©2026 Palo Alto Networks, Inc.

5. Configurez les paramètres **VPN** :
   1. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
   2. Sélectionnez le **Connection Type (Type de connexion)** du réseau :
      - Pour l'application 4.1.x de GlobalProtect et les versions antérieures, sélectionnez **Palo Alto Networks GlobalProtect**.
      - Pour l'application 5.0 de GlobalProtect et les versions ultérieures, sélectionnez **Custom (Personnalisé)**.
   3. (Facultatif) Si vous définissez le **Type de connexion** sur **Personnalisé**, saisissez l'ID de groupe suivante **com.paloaltonetworks.globalprotect.vpn** dans le champ **Identifier (Identifiant)** pour identifier l'application GlobalProtect.

      *Si vous avez téléchargé l'application GlobalProtect directement dans Apple App Store en Chine, saisissez l'ID de groupe**com.paloaltonetworks.globalprotect.vpn** dans le champ **Identifier (Identifiant)**.*

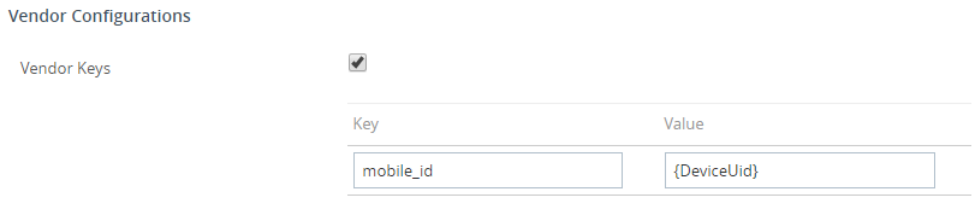
   4. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
   5. (Facultatif) Saisissez le nom d'utilisateur du **Account (Compte)** VPN ou cliquez sur le bouton d'ajout (**+**) pour afficher les valeurs de recherche prises en charge que vous pouvez insérer.
   6. (Facultatif) Dans le champ **Disconnect on idle (Déconnecter en cas d'Inactivité)**, spécifiez la durée de temps (en secondes) à l'issue de laquelle un point de terminaison se déconnecte de l'application GlobalProtect après que l'application cesse d'acheminer le trafic via le tunnel VPN.
   7. Dans la section Authentication (Authentification), sélectionnez une méthode de **Authentication (Authentification)** de l'utilisateur : **Password (Mot de passe)**, **Certificate (Certificat)**, **Password + Certificate (Mot de passe + Certificat)**.
   8. Lorsque vous êtes invité à le faire, saisissez un **Password (Mot de passe)** et/ou sélectionnez le **Identity Certificate (Certificat d'identité)** que GlobalProtect utilisera pour authentifier les utilisateurs. Le **Identity Certificate (Certificat d'identité)** est le même certificat que vous avez configuré dans les paramètres de **Credentials (Informations d'identification)**.
   9. **Activer le réseau privé virtuel à la demande** et **Utiliser des nouvelles clés à la demande**.
   10. Configurer une règle à la demande **Action : Connecter**.
   11. (Facultatif) Sélectionnez le type de **Proxy** et configurez les paramètres pertinents.

 ©2026 Palo Alto Networks, Inc.

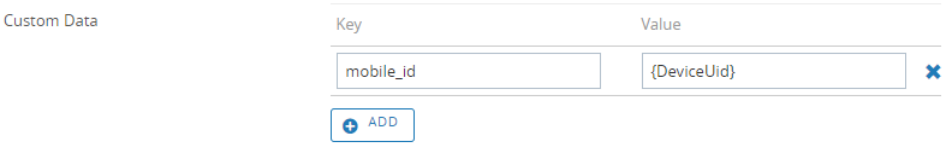
6. (Facultatif) (à compter de la version 5.0 de l'application GlobalProtect) Si votre déploiement GlobalProtect exige une intégration HIP avec MDM, précisez l'attribut de Unique device identifier (UDID ; Identificateur de périphérique unique).

   GlobalProtect prend en charge l'intégration avec MDM pour obtenir des attributs de périphériques mobiles du serveur MDM aux fins d'une application de la politique basée sur HIP. Pour que l'intégration MDM fonctionne, l'application GlobalProtect doit présenter l'UDID du point de terminaison vers la passerelle GlobalProtect. L'attribut UDID permet à l'application GlobalProtect de récupérer et d'utiliser les informations UDID dans les déploiements basés sur MDM. Si vous supprimez l'attribut UDID du profil, vous ne pouvez plus utiliser l'intégration MDM. L'application GlobalProtect génère un nouveau UDID, mais il ne peut être utilisé pour l'intégration.

   - Si vous utilisez **Palo Alto Networks GlobalProtect** comme **Connection Type (Type de connexion)** réseau, allez aux paramètres **VPN** et activez les **Vendor Keys (Clés de fournisseur)** dans la section Vendor Configurations (Configurations de fournisseur). Définissez la **Key (Clé)** sur **`mobile_id`** et la **Value (Valeur)** sur **`{DeviceUid}`**.

   - Si vous utilisez **Custom (Personnalisé)** comme **Connection Type (Type de connexion)** réseau, allez aux paramètres **VPN** et **ADD (AJOUTER)** les **Custom Data (données personnalisées)** dans la section Connection Info (Informations de connexion). Définissez la **Key (Clé)** sur **`mobile_id`** et la **Value (Valeur)** sur **`{DeviceUid}`**.

7. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les terminaux iOS à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans une configuration de VPN d'accès à distance (à la demande), les utilisateurs doivent lancer manuellement l'application pour établir la connexion GlobalProtect sécurisée. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle

 ©2026 Palo Alto Networks, Inc.

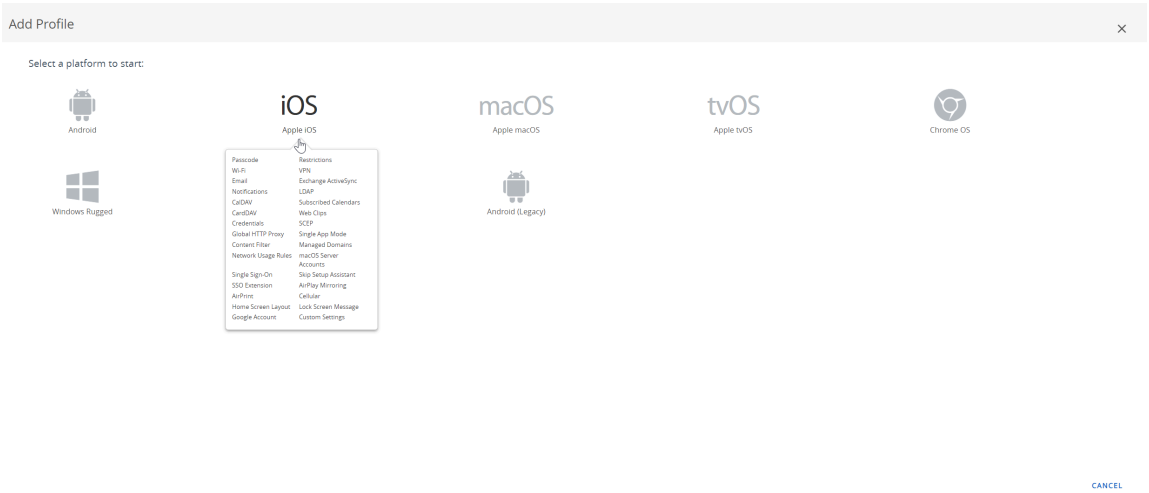
GlobalProtect est acheminé via le tunnel VPN seulement après que les utilisateurs ont initié et établi la connexion.

Utilisez les étapes suivantes pour configurer configuration de VPN d'accès à distance initié par l'utilisateur sur les terminaux iOS à l'aide de Workspace ONE :

1. Téléchargement de l'application GlobalProtect pour Android
   - Déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   - Téléchargez l'app GlobalProtect directement à partir de l'App Store.

     L'app GlobalProtect pour iOS est disponible sur l'Apple App Store en Chine.

2. Depuis la console AirWatch, modifiez un profil Apple iOS existant ou ajoutez-en un nouveau.
   1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajouter)** un nouveau profil.
   2. Sélectionnez **iOS** à partir de la liste de la plateforme.

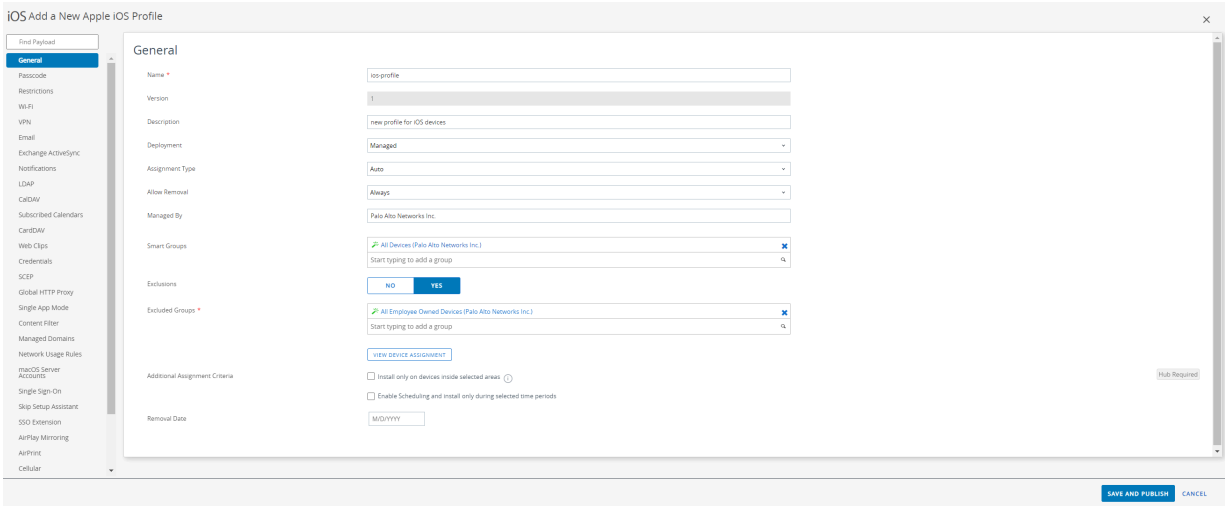


3. Configurez les paramètres **General (généraux)**.
   1. Saisissez un **Name (Nom)** pour le profil.
   2. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
   3. (Facultatif) Sélectionnez le mode de **Deployment (Déploiement)**, qui indique que le profil sera automatiquement supprimé au moment de la désinscription, soit **Managed (Géré)** (le profil est supprimé) ou **Manual (Manuel)** (le profil est installé jusqu'à ce qu'il soit supprimé par l'utilisateur final).
   4. (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les points de terminaison. Sélectionnez **Auto** pour déployer automatiquement le profil sur tous les points de terminaison, **Optional (Optionnel)** pour permettre à l'utilisateur final d'installer le profil à partir du portail SSP (portail libre-service) ou de déployer manuellement le profil sur des points de terminaison individuels, ou **Compliance (Conformité)** pour déployer le profil lorsqu'un utilisateur final enfreint une politique de conformité applicable au point de terminaison.
   5. (Facultatif) Sélectionnez si vous souhaitez **Allow Removal (Autoriser la suppression)** du profil par l'utilisateur final ou non. Sélectionner **Always (Toujours)** pour permettre à l'utilisateur final de supprimer manuellement le profil à tout moment, **Never (Jamais)**

 ©2026 Palo Alto Networks, Inc.

pour empêcher l'utilisateur final de supprimer le profil, ou **With Authorization (Avec autorisation)** pour permettre à l'utilisateur final de supprimer le profil avec l'autorisation de l'administrateur. Lorsque **With Authorization (Avec autorisation)** est sélectionné, un champ Password (Mot de passe) qui doit obligatoirement être renseigné s'ajoute.

6. (Facultatif) Dans le champ **Managed By (Géré par)**, saisissez le groupe de l'entreprise ayant un accès administratif au profil.
7. (Facultatif) Dans le champ **Assigned Groups (Groupes affectés)**, ajoutez les Groupes intelligents auxquels vous souhaitez ajouter le profil. Ce champ comprend une option permettant la création d'un nouveau groupe intelligent pour lequel vous pouvez configurer les spécifications suivantes : exigences minimales en matière de système d'exploitation, modèles de périphérique, catégories de propriété, groupes de l'entreprise, parmi tant d'autres.
8. (Facultatif) Indiquez si vous souhaitez ajouter des **Exclusions** à l'affectation de ce profil. Si vous sélectionnez **Yes (Oui)**, le champ **Excluded Groups (Groupes exclus)** s'affiche, vous permettant de sélectionner les groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.
9. (Facultatif) Si vous activez l'option visant à **Install only on devices inside selected areas (installer uniquement sur les périphériques dans des zones sélectionnées)**, le profil peut être installé seulement sur les points de terminaison dans des barrières géographiques ou des régions iBeacon spécifiques. Lorsque vous êtes invité à le faire, ajoutez les barrières géographoqies ou les régions iBeacon dans le champ **Assigned Geofence Areas (Zones de barrières géographiques affectées)**.
10. (Facultatif) Si vous **Enable Scheduling and install only during selected time periods (Activez la planification et installez uniquement lors des périodes de temps sélectionnées)**, vous pouvez appliquer un calendrier (**Devices (Périphériques)** > **Profiles & Resources (Profil et ressources)** > **Profiles Settings (Paramètres du profil)** > **Time Schedules (Calendriers)**) à l'installation du profil, ce qui limite les périodes de temps pendant lesquelles le profil peut être installé sur les points de terminaison. Lorsque vous êtes invité à le faire, saisissez le nom du calendrier dans le champ **Assigned Schedules (Calendriers affectés)**.
11. (Facultatif) Sélectionnez la **Removal Date (Date de suppression)** à laquelle vous voulez que le profil soit supprimé de tous les points de terminaison.



 ©2026 Palo Alto Networks, Inc.

4. Configurez les paramètres de **Credentials (Informations d'identification)** :

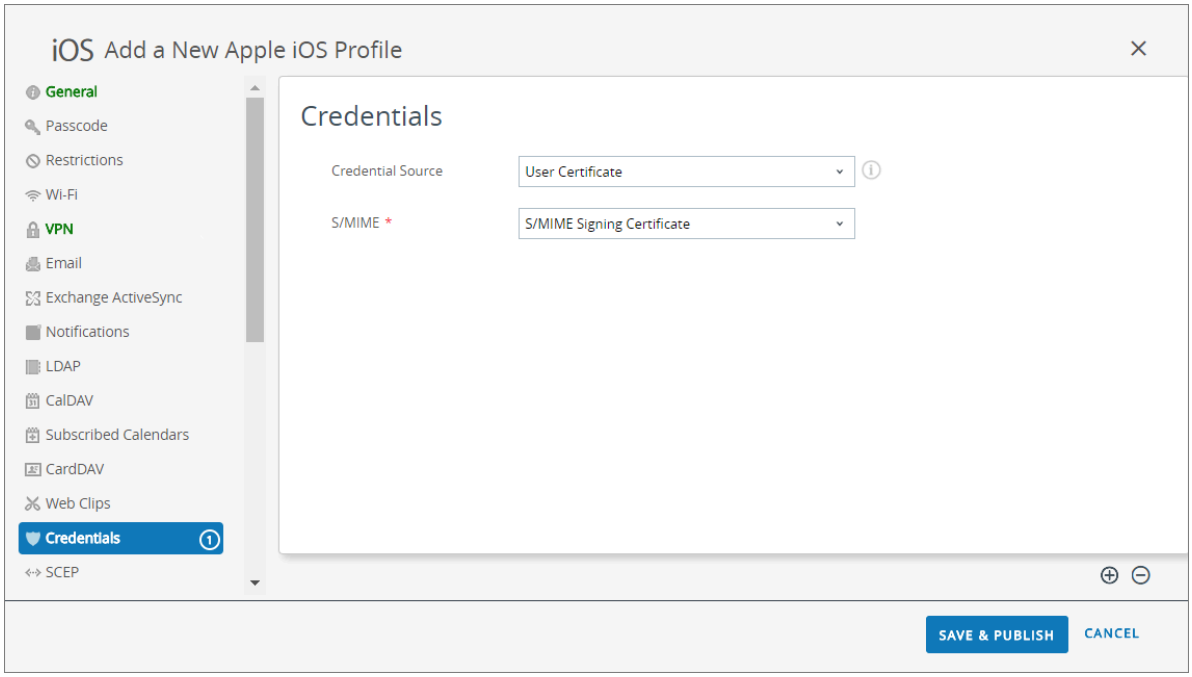
   Toutes les configurations de VPN d'accès à distance pour les terminaux iOS exigent une authentification basée sur le certificat.

   À partir de la version 12 d'iOS, si vous souhaitez utiliser les certificats de client pour procéder à l'authentification du client GlobalProtect, vous devez déployer les certificats de client dans le cadre du profil VPN qui est transmis du serveur MDM. Si vous déployez des certificats de

 ©2026 Palo Alto Networks, Inc.

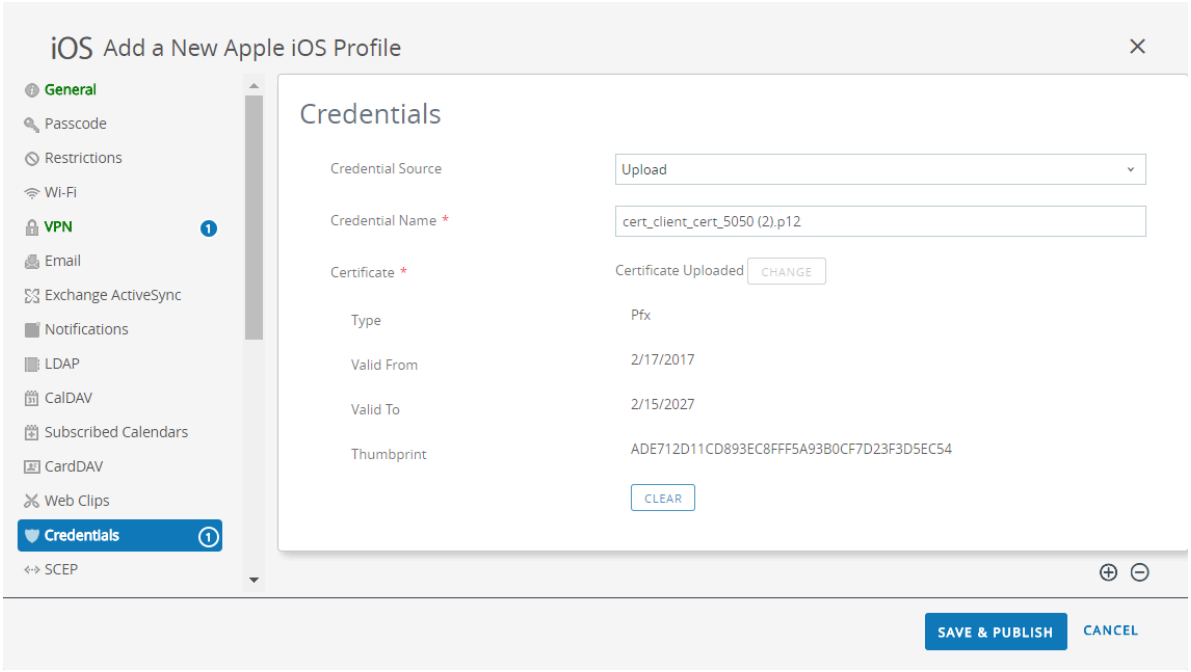
client à partir du serveur MDM au moyen d'une tout autre méthode, les certificats ne peuvent être utilisés par l'application GlobalProtect.

- Pour extraire les certificats de client des utilisateurs Workspace ONE :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).



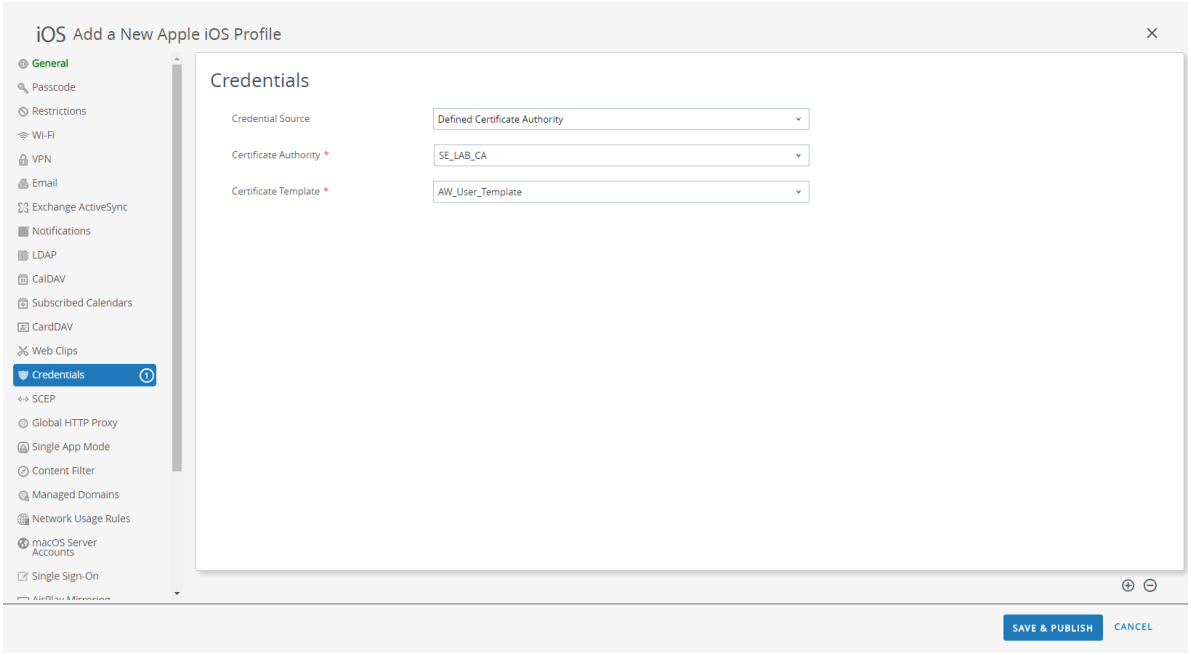
- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.

 ©2026 Palo Alto Networks, Inc.



- Pour utiliser une autorité de certification et un modèle prédéfinis :

  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
  2. Sélectionnez la **Certificate Authority (Autorité de certification)** de laquelle vous souhaitez obtenir les certificats.
  3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.

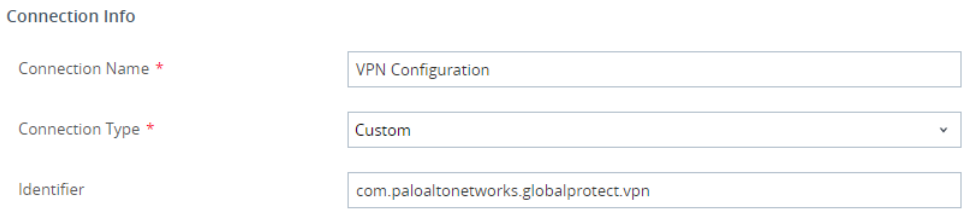


 ©2026 Palo Alto Networks, Inc.

5. Configurez les paramètres **VPN** :

1. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
2. Sélectionnez le **Connection Type (Type de connexion)** du réseau :
   - Pour l'application 4.1.x de GlobalProtect et les versions antérieures, sélectionnez **Palo Alto Networks GlobalProtect**.
   - Pour l'application 5.0 de GlobalProtect et les versions ultérieures, sélectionnez **Custom (Personnalisé)**.
3. (Facultatif) Si vous définissez le **Type de connexion** sur **Personnalisé**, saisissez l'ID de groupe suivante **com.paloaltonetworks.globalprotect.vpn** dans le champ **Identifier (Identifiant)** pour identifier l'application GlobalProtect.

   *Si vous avez téléchargé l'application GlobalProtect directement dans Apple App Store en Chine, saisissez l'ID de groupe**com.paloaltonetworks.globalprotect.vpn** dans le champ **Identifier (Identifiant)**.*



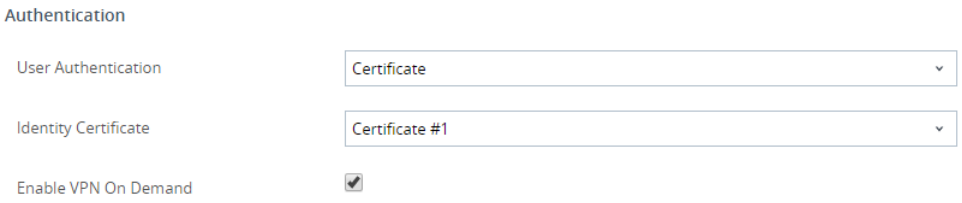
4. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
5. (Facultatif) Saisissez le nom d'utilisateur du **Account (Compte)** VPN ou cliquez sur le bouton d'ajout (**+**) pour afficher les valeurs de recherche prises en charge que vous pouvez insérer.
6. (Facultatif) Dans le champ **Disconnect on idle (Déconnecter en cas d'Inactivité)**, spécifiez la durée de temps (en secondes) à l'issue de laquelle un point de terminaison se déconnecte de l'application GlobalProtect après que l'application cesse d'acheminer le trafic via le tunnel VPN.
7. Dans la section Authentication (Authentification), définissez la méthode de **Authentication (Authentification)** sur **Certificate (Certificat)**.

   Toutes les configurations de VPN d'accès à distance pour les terminaux iOS exigent une authentification basée sur le certificat.
8. Lorsque vous êtes invité à le faire, sélectionnez le **Identity Certificate (Certificat d'identité)** que GlobalProtect utilisera pour authentifier les utilisateurs. Le **Identity Certificate**

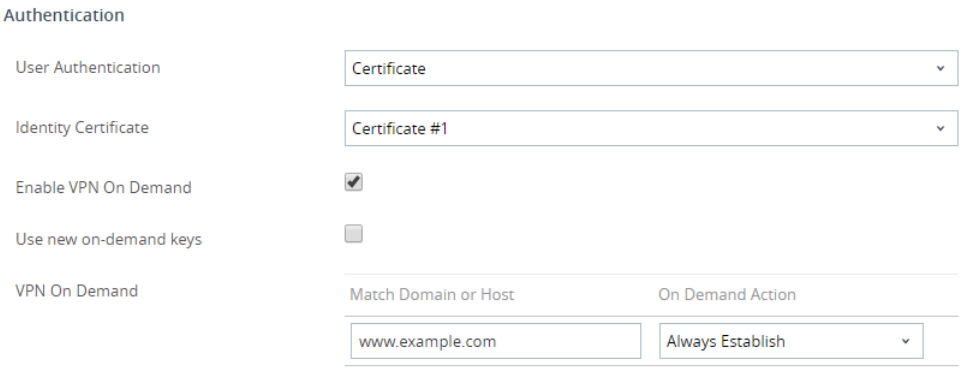
 ©2026 Palo Alto Networks, Inc.

(Certificat d'identité) est le même certificat que vous avez configuré dans les paramètres de **Credentials (Informations d'identification)**.

9. Assurez-vous que l'option **Enable VPN On Demand (Activer le réseau privé virtuel à la demande)** est cochée (paramètre par défaut).



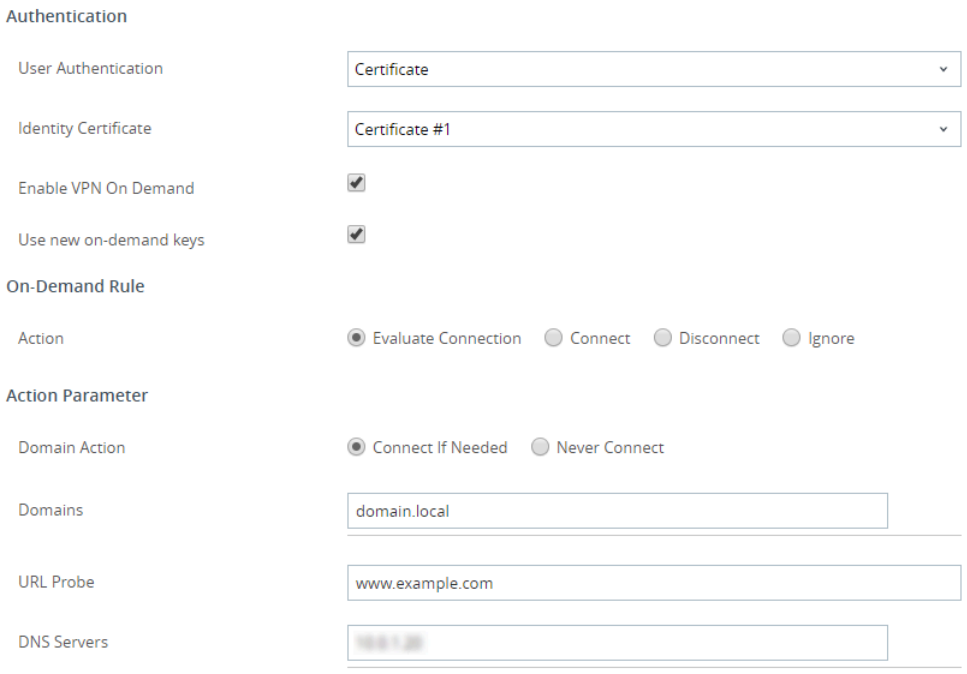
10. (Facultatif) Configurez les anciennes règles de connexion **VPN On-Demand (VPN à la demande)** :
    - **Match Domain or Host (Faire correspondre le domaine ou l'hôte)** : saisissez le domaine ou le nom d'hôte qui entraîne l'établissement de la connexion GlobalProtect lorsque les utilisateurs y accèdent.
    - **On Demand Action (Action à la demande)** : définissez la **On Demand Action (Action à la demande)** sur **Establish if Needed (Établir au besoin)** ou sur **Always Establish (Toujours établir)** pour établir la connexion GlobalProtect uniquement si les utilisateurs ne peuvent joindre directement le domaine ou le nom d'hôte indiqué. Définissez la **On Demand Action (Action à la demande)** sur **Never Establish (Ne jamais établir)** pour empêcher l'établissement de la connexion GlobalProtect lorsque les utilisateurs accèdent au domaine ou au nom d'hôte indiqué. Si la connexion est déjà établie, elle peut continuer à être utilisée.



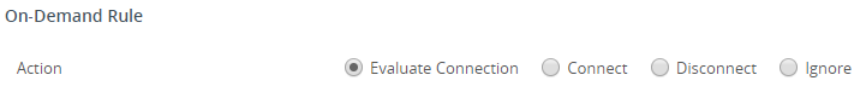
11. (Facultatif) Définissez des règles de connexion à la demande plus granulaires en activant l'application GlobalProtect à **Use new on-demand keys (Utiliser des nouvelles clés à la**

 ©2026 Palo Alto Networks, Inc.

demande). Vous pouvez ajouter plusieurs règles en cliquant sur **ADD RULE (Ajouter une règle)**.



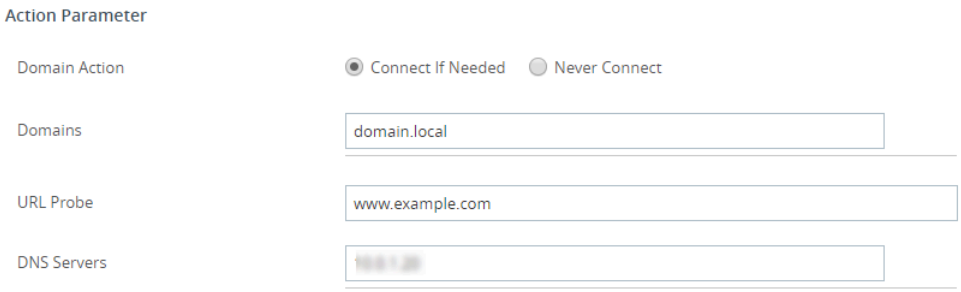
- Dans la section On-Demand Rule (Règle à la demande), sélectionnez une **Action** à appliquer à la connexion GlobalProtect selon les critères que vous définissez :
  - **Evaluate Connection (Évaluer la connexion)** : établit automatiquement la connexion GlobalProtect selon les paramètres de connexion et de réseau. Cette évaluation se produit chaque fois qu'un utilisateur tente de se connecter à un domaine.
  - **Connect (Se connecter)** : établit automatiquement la connexion GlobalProtect.
  - **Disconnect (Déconnecter)** : désactive automatiquement GlobalProtect et empêcher GlobalProtect de se reconnecter.
  - **Ignore (Ignorer)** : laisse la connexion GlobalProtect telle quelle et empêche GlobalProtect de se reconnecter en cas de déconnexion.



- (Facultatif) Si vous définissez l'**Action** de votre règle de connexion à la demande sur **Evaluate Connection (Évaluer la connexion)**, vous devez également configurer un paramètre d'action pour préciser si GlobalProtect peut tenter de se reconnecter, ou non, si la résolution du nom de domaine échoue lors de l'évaluation de la connexion (par exemple, si le serveur DNS n'arrive pas à répondre en raison d'une temporisation). Vous pouvez ajouter plusieurs paramètres en cliquant sur **ADD ACTION PARAMETERS (Ajouter des paramètres d'action)**.
  - Définissez la **Domain Action (Action du domaine)** sur **Connect if Needed (Se connecter au besoin)** pour permettre à GlobalProtect de se réconnecter ou sur **Never Connect (Ne jamais se connecter)** pour empêcher GlobalProtect de se reconnecter.

 ©2026 Palo Alto Networks, Inc.

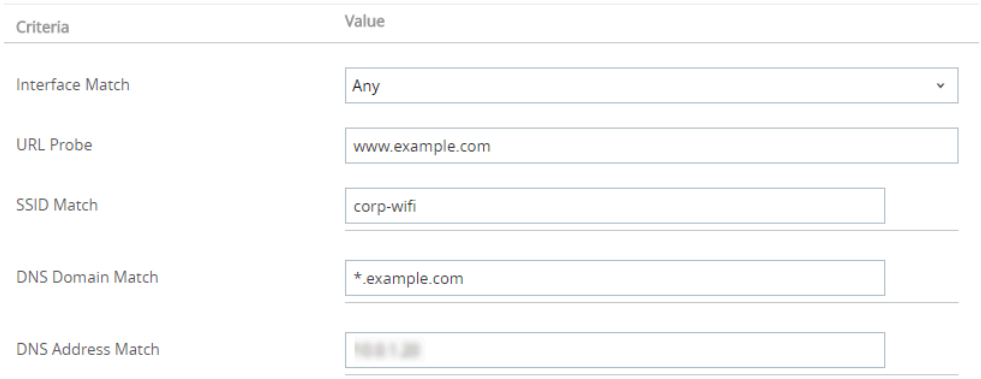
- Saisissez les **Domains (Domaines)** auxquels ce **Action Parameter (Paramètre d'action)** s'applique.
- (Facultatif) Si vous définissez la **Domain Action (Action du domaine)** sur **Connect if Needed (Se connecter au besoin)**, saisissez l'URL HTTP ou HTTPS URL que vous souhaitez sonder dans le champ **Sondage d'URL**. S'il est impossible de résoudre le nom d'hôte de l'URL, le serveur ne peut être joint ou si le serveur ne répond pas avec un code HTTP 200, la connexion GlobalProtect s'établit.
- (Facultatif) Si vous définissez la **Domain Action (Action du domaine)** sur **Connect if Needed (Se connecter au besoin)**, saisissez les adresses IP des **DNS Servers (Serveurs DNS)** (interne ou externe de confiance) utilisées pour résoudre les **Domains (Domaines)** spécifiés. Si les serveurs DNS ne peuvent être joints, la connexion GlobalProtect s'établit.



- Configurez les critères suivants à faire correspondre à votre règle de connexion à la demande. Si un point de terminaison correspond à tous les critères indiqués, la règle de connexion à la demande est appliquée à ce point de terminaison.
  - **Interface Match (Correspondance d'interface)** : précisez le type de connexion à faire correspondre à la carte réseau virtuel des points de terminaison : **Any (tout)**, **Ethernet**, **Wi-Fi**, **Cellular (cellulaire)**.
  - **URL Probe (Sondage URL)** : saisissez l'URL HTTP ou HTTPS URL à faire correspondre. Si la correspondance est réussie, un code d'état HTTP 200 est retourné.
  - **SSID Match (Correspondance SSID)** : saisissez le SSID de réseau à faire correspondre. Vous pouvez ajouter plusieurs SSID de réseau en cliquant sur le bouton d'ajout (**+**). Pour une correspondance réussie, le point de terminaison doit mettre en correspondance au moins un SSID de réseau précisé.
  - **DNS Domain Match (Correspondance de domaine DNS)** : saisissez le domaine de recherche DNS à faire correspondre. Vous pouvez également établir la correspondance avec un dossier comportant des caractères génériques (comme **`*.example.com`**) afin d'inclure tous les sous-domaines.
  - **DNS Address Match (Correspondance d'adresse DNS)** : saisissez l'adresse IP du serveur DNS à faire correspondre. Vous pouvez ajouter plusieurs adresses IP de serveur DNS en cliquant sur le bouton d'ajout (**+**). Vous pouvez également établir la correspondance avec un seul dossier comportant des caractères génériques (comme **`17.*`**) qui comprend tous les serveurs DNS sans adresses IP. Pour une

 ©2026 Palo Alto Networks, Inc.

correspondance réussie, toutes les adresses IP de serveur DNS énumérées sur le point de terminaison doivent correspondre aux adresses IP de serveur DNS indiquées.

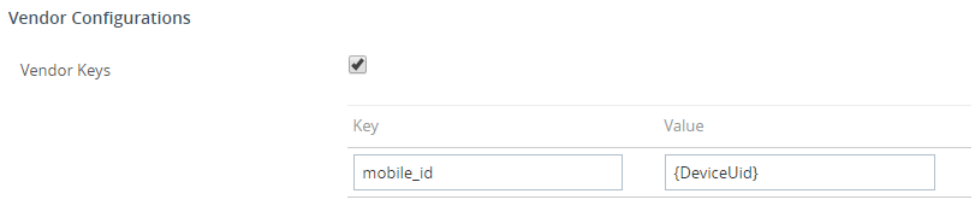


12. (Facultatif) Sélectionnez le type de **Proxy** et configurez les paramètres pertinents.

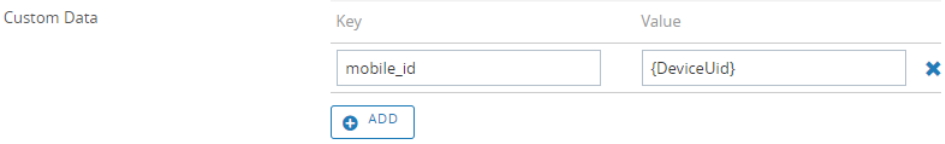
6. (Facultatif) (à compter de la version 5.0 de l'application GlobalProtect) Si votre déploiement GlobalProtect exige une intégration HIP avec MDM, précisez l'attribut de Unique device identifier (UDID ; Identificateur de périphérique unique).

GlobalProtect prend en charge l'intégration avec MDM pour obtenir des attributs de périphériques mobiles du serveur MDM aux fins d'une application de la politique basée sur HIP. Pour que l'intégration MDM fonctionne, l'application GlobalProtect doit présenter l'UDID du point de terminaison vers la passerelle GlobalProtect. L'attribut UDID permet à l'application GlobalProtect de récupérer et d'utiliser les informations UDID dans les déploiements basés sur MDM. Si vous supprimez l'attribut UDID du profil, vous ne pouvez plus utiliser l'intégration MDM. L'application GlobalProtect génère un nouveau UDID, mais il ne peut être utilisé pour l'intégration.

- Si vous utilisez **Palo Alto Networks GlobalProtect** comme **Connection Type (Type de connexion)** réseau, allez aux paramètres **VPN** et activez les **Vendor Keys (Clés de fournisseur)** dans la section Vendor Configuration (Configuration de fournisseur). Définissez la **Key (Clé)** sur **`mobile_id`** et la **Value (Valeur)** sur **`{DeviceUid}`**.



- Si vous utilisez **Custom (Personnalisé)** comme **Connection Type (Type de connexion)** réseau, allez aux paramètres **VPN** et **ADD (AJOUTER)** les **Custom Data (données personnalisées)** dans la section Connection Info (Informations de connexion). Définissez la **Key (Clé)** sur **`mobile_id`** et la **Value (Valeur)** sur **`{DeviceUid}`**.



 ©2026 Palo Alto Networks, Inc.

7. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

Configurer une configuration de VPN par application sur les terminaux iOS à l'aide de Workspace ONE

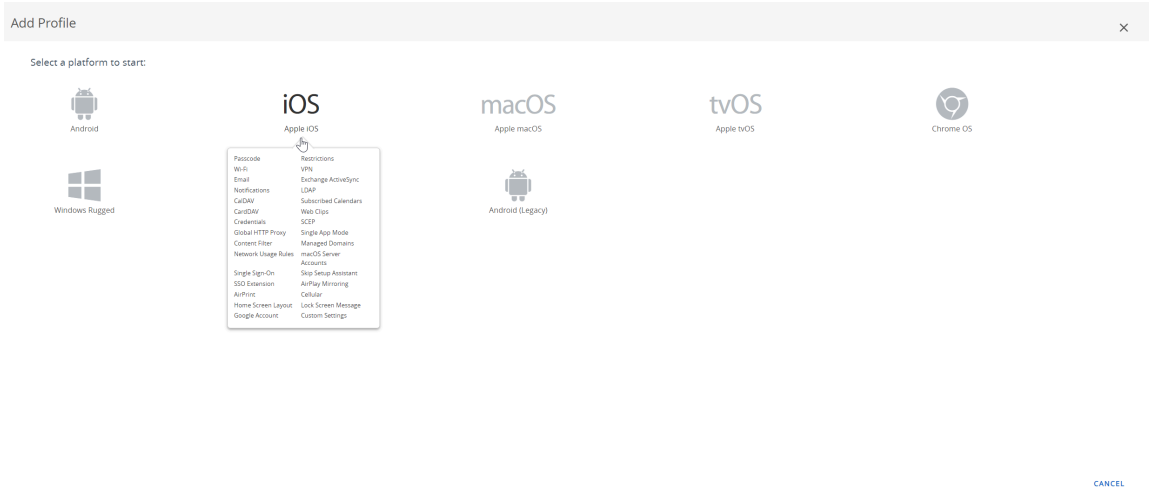
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez autoriser l'accès aux ressources internes à partir de vos périphériques mobiles gérés en configurant l'accès VPN GlobalProtect à l'aide de Workspace ONE. Dans une configuration VPN par application, vous pouvez indiquer les applications gérées qui peuvent acheminer le trafic via le tunnel VPN. Les applications non gérées continueront de se connecter directement par l'Internet plutôt que via le tunnel VPN.

Utilisez les étapes suivantes pour configurer une configuration par application sur les terminaux iOS à l'aide de MobileIron :

1. Téléchargement de l'application GlobalProtect pour iOS :
   - Déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   - Téléchargez l'app GlobalProtect directement à partir de l'App Store.

     L'app GlobalProtect pour iOS est disponible sur l'Apple App Store en Chine.
2. Depuis la console AirWatch, modifiez un profil Apple iOS existant ou ajoutez-en un nouveau.
   1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajouter)** un nouveau profil.
   2. Sélectionnez **iOS** à partir de la liste de la plateforme.

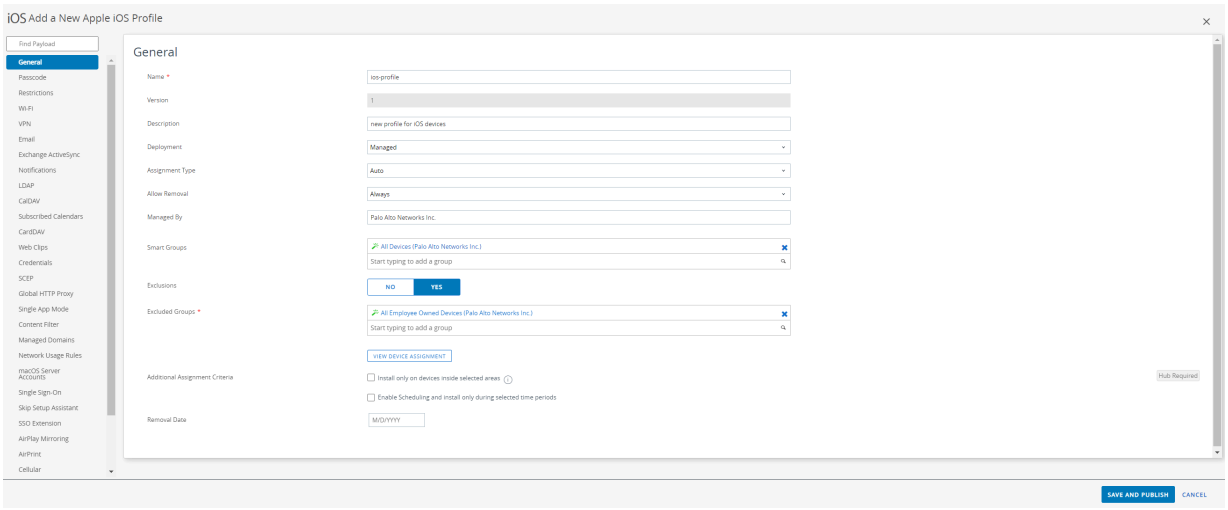


 ©2026 Palo Alto Networks, Inc.

3. Configurez les paramètres **General (généraux)**.
   1. Saisissez un **Name (Nom)** pour le profil.
   2. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
   3. (Facultatif) Sélectionnez le mode de **Deployment (Déploiement)**, qui indique que le profil sera automatiquement supprimé au moment de la désinscription, soit **Managed (Géré)** (le profil est supprimé) ou **Manual (Manuel)** (le profil est installé jusqu'à ce qu'il soit supprimé par l'utilisateur final).
   4. (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les points de terminaison. Sélectionnez **Auto** pour déployer automatiquement le profil sur tous les points de terminaison, **Optional (Optionnel)** pour permettre à l'utilisateur final d'installer le profil à partir du portail SSP (portail libre-service) ou de déployer manuellement le profil sur des points de terminaison individuels, ou **Compliance (Conformité)** pour déployer le profil lorsqu'un utilisateur final enfreint une politique de conformité applicable au point de terminaison.
   5. (Facultatif) Sélectionnez si vous souhaitez **Allow Removal (Autoriser la suppression)** du profil par l'utilisateur final ou non. Sélectionner **Always (Toujours)** pour permettre à l'utilisateur final de supprimer manuellement le profil à tout moment, **Never (Jamais)** pour empêcher l'utilisateur final de supprimer le profil, ou **With Authorization (Avec autorisation)** pour permettre à l'utilisateur final de supprimer le profil avec l'autorisation de l'administrateur. Lorsque **With Authorization (Avec autorisation)** est sélectionné, un champ Password (Mot de passe) qui doit obligatoirement être renseigné s'ajoute.
   6. (Facultatif) Dans le champ **Managed By (Géré par)**, saisissez le groupe de l'entreprise ayant un accès administratif au profil.
   7. (Facultatif) Dans le champ **Assigned Groups (Groupes affectés)**, ajoutez les Groupes intelligents auxquels vous souhaitez ajouter le profil. Ce champ comprend une option permettant la création d'un nouveau groupe intelligent pour lequel vous pouvez configurer les spécifications suivantes : exigences minimales en matière de système d'exploitation, modèles de périphérique, catégories de propriété, groupes de l'entreprise, parmi tant d'autres.
   8. (Facultatif) Indiquez si vous souhaitez ajouter des **Exclusions** à l'affectation de ce profil. Si vous sélectionnez **Yes (Oui)**, le champ **Excluded Groups (Groupes exclus)** s'affiche,

 ©2026 Palo Alto Networks, Inc.

vous permettant de sélectionner les groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.



4. Configurez les paramètres de **Credentials (Informations d'identification)** :

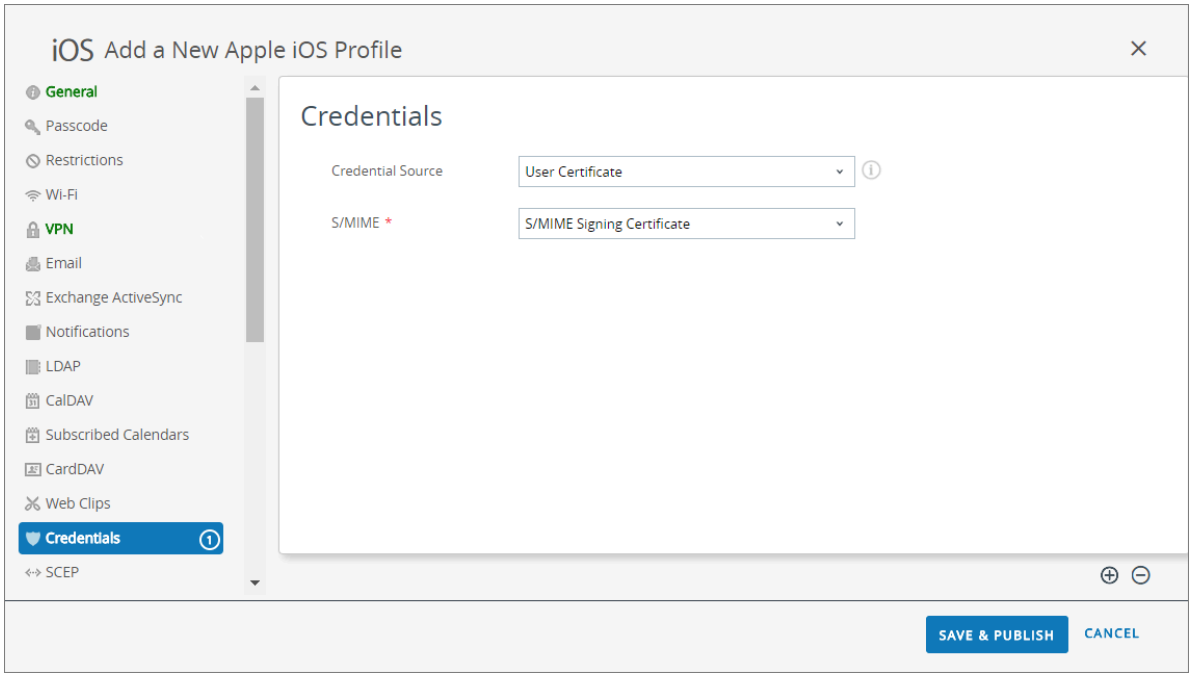
   Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

   À partir de la version 12 d'iOS, si vous souhaitez utiliser les certificats de client pour procéder à l'authentification du client GlobalProtect, vous devez déployer les certificats de client dans le cadre du profil VPN qui est transmis du serveur MDM. Si vous déployez des certificats de

 ©2026 Palo Alto Networks, Inc.

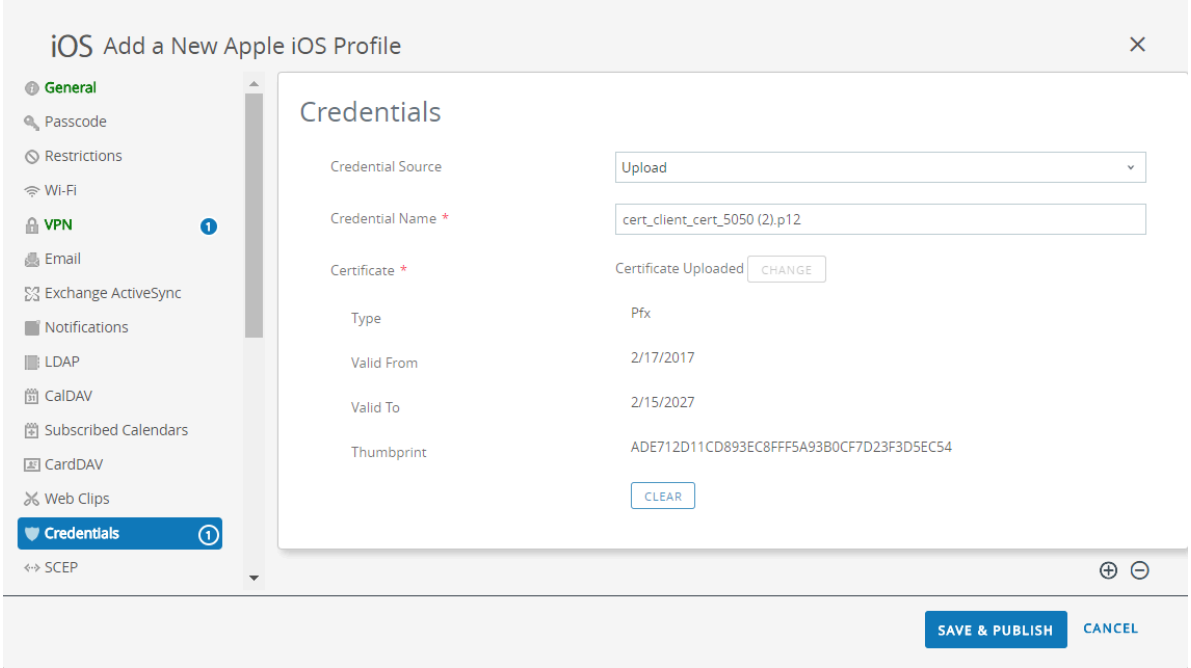
client à partir du serveur MDM au moyen d'une tout autre méthode, les certificats ne peuvent être utilisés par l'application GlobalProtect.

- Pour extraire les certificats de client des utilisateurs Workspace ONE :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).



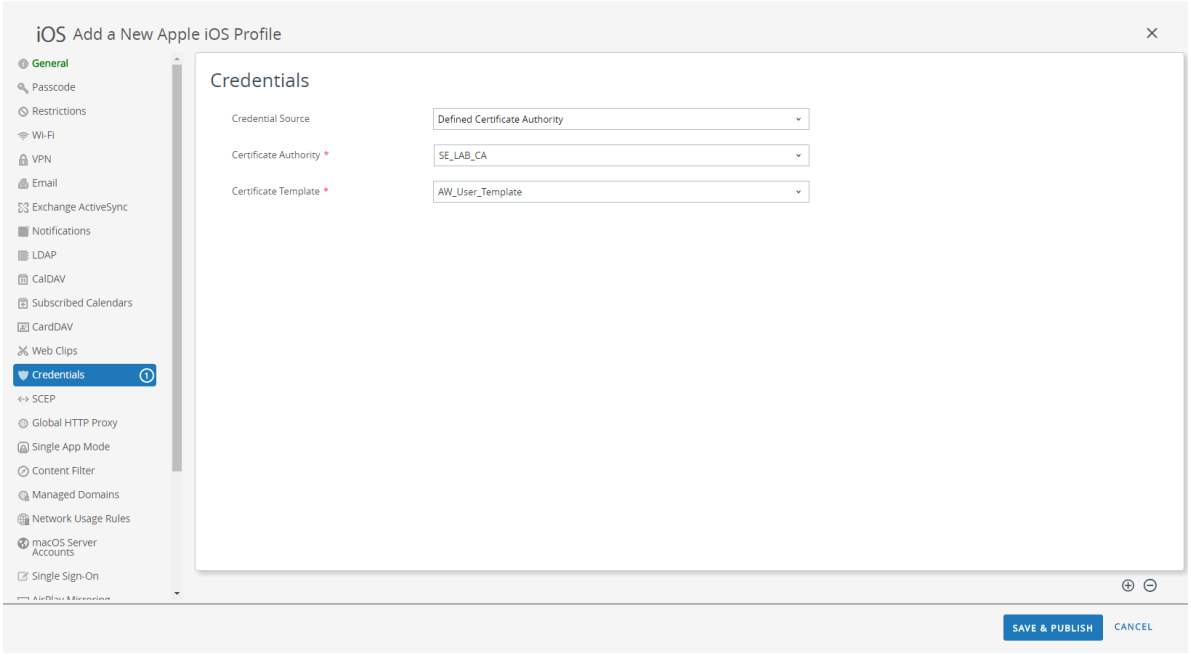
- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.

 ©2026 Palo Alto Networks, Inc.



- Pour utiliser une autorité de certification et un modèle prédéfinis :

  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
  2. Sélectionnez la **Certificate Authority (Autorité de certification)** de laquelle vous souhaitez obtenir les certificats.
  3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.

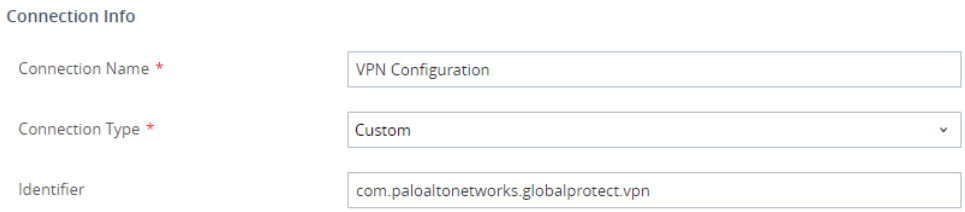


 ©2026 Palo Alto Networks, Inc.

5. Configurez les paramètres **VPN** :

   1. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
   2. Sélectionnez le **Connection Type (Type de connexion)** du réseau :
      - Pour l'application 4.1.x de GlobalProtect et les versions antérieures, sélectionnez **Palo Alto Networks GlobalProtect**.
      - Pour l'application 5.0 de GlobalProtect et les versions ultérieures, sélectionnez **Custom (Personnalisé)**.
   3. (Facultatif) Si vous définissez le **Type de connexion** sur **Personnalisé**, saisissez l'ID de groupe suivante **com.paloaltonetworks.globalprotect.vpn** dans le champ **Identifier (Identifiant)** pour identifier l'application GlobalProtect.

      *Si vous avez téléchargé l'application GlobalProtect directement dans Apple App Store en Chine, saisissez l'ID de groupe**com.paloaltonetworks.globalprotect.vpn** dans le champ **Identifier (Identifiant)**.*

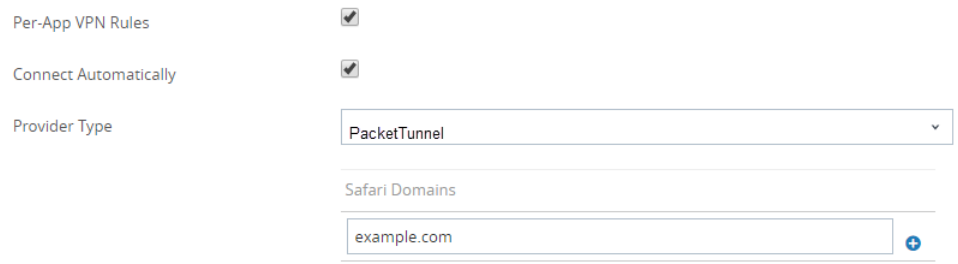
      

   4. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
   5. (Facultatif) Saisissez le nom d'utilisateur du **Account (Compte)** VPN ou cliquez sur le bouton d'ajout (**+**) pour afficher les valeurs de recherche prises en charge que vous pouvez insérer.
   6. (Facultatif) Dans le champ **Disconnect on idle (Déconnecter en cas d'Inactivité)**, spécifiez la durée de temps (en secondes) à l'issue de laquelle un point de terminaison se déconnecte de

 ©2026 Palo Alto Networks, Inc.

l'application GlobalProtect après que l'application cesse d'acheminer le trafic via le tunnel VPN.

7. Autorisez les **Per App VPN Rules (Règles VPN par application)** à acheminer tout le trafic des applications gérées via le tunnel VPN GlobalProtect.
   - Autorisez GlobalProtect à **Connect Automatically (se connecter automatiquement)** aux **Safari Domains (Domaines Safari)** précisés. Vous pouvez ajouter plusieurs **Safari Domains (Domaines Safari)** en cliquant sur le bouton d'ajout (**+**).
   - Sélectionnez le **Provider Type (Type de fournisseur)** pour indiquer la manière dont le trafic sera tunnelisé : soit au niveau de l'application ou de l'adresse IP. Utiliser PacketTunnel.



8. Dans la section Authentication (Authentification), définissez la méthode de **Authentication (Authentification)** sur **Certificate (Certificat)**.

   Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

9. Lorsque vous êtes invité à le faire, sélectionnez le **Identity Certificate (Certificat d'identité)** que GlobalProtect utilisera pour authentifier les utilisateurs. Le **Identity Certificate (Certificat d'identité)** est le même certificat que vous avez configuré dans les paramètres de **Credentials (Informations d'identification)**.

10. (Facultatif) Sélectionnez le type de **Proxy** et configurez les paramètres pertinents.

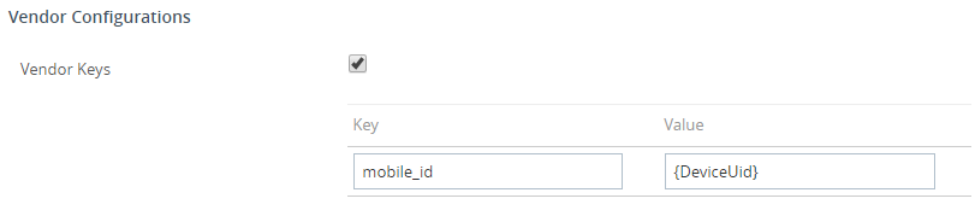
6. (Facultatif) (à compter de la version 5.0 de l'application GlobalProtect) Si votre déploiement GlobalProtect exige une intégration HIP avec MDM, précisez l'attribut de Unique device identifier (UDID ; Identificateur de périphérique unique).

GlobalProtect prend en charge l'intégration avec MDM pour obtenir des attributs de périphériques mobiles du serveur MDM aux fins d'une application de la politique basée sur HIP. Pour que l'intégration MDM fonctionne, l'application GlobalProtect doit présenter l'UDID du point de terminaison vers la passerelle GlobalProtect. L'attribut UDID permet à l'application GlobalProtect de récupérer et d'utiliser les informations UDID dans les déploiements basés sur MDM. Si vous supprimez l'attribut UDID du profil, vous ne pouvez plus utiliser l'intégration

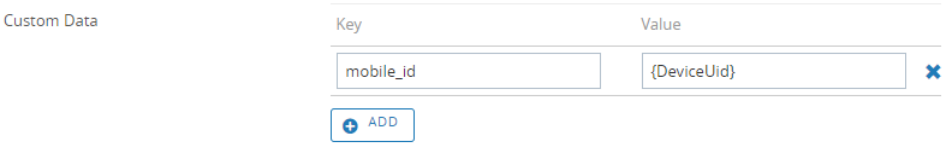
 ©2026 Palo Alto Networks, Inc.

MDM. L'application GlobalProtect génère un nouveau UDID, mais il ne peut être utilisé pour l'intégration.

- Si vous utilisez **Palo Alto Networks GlobalProtect** comme **Connection Type (Type de connexion)** réseau, allez aux paramètres **VPN** et activez les **Vendor Keys (Clés de fournisseur)** dans la section Vendor Configuration (Configuration de fournisseur). Définissez la **Key (Clé)** sur **`mobile_id`** et la **Value (Valeur)** sur **`{DeviceUid}`**.



- Si vous utilisez **Custom (Personnalisé)** comme **Connection Type (Type de connexion)** réseau, allez aux paramètres **VPN** et **ADD (AJOUTER)** les **Custom Data (données personnalisées)** dans la section Connection Info (Informations de connexion). Définissez la **Key (Clé)** sur **`mobile_id`** et la **Value (Valeur)** sur **`{DeviceUid}`**.



7. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

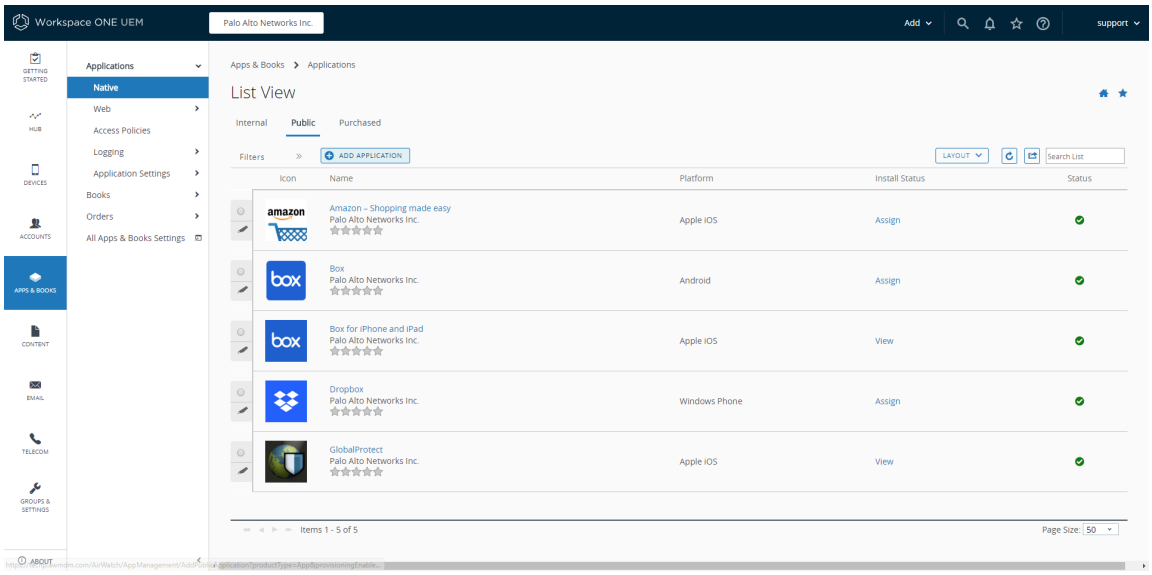
8. Configurez les paramètres VPN par application pour une nouvelle application gérée, ou modifiez les paramètres d'une application gérée existante.

Après avoir configuré les paramètres de l'application et activé le VPN par application, vous pouvez publier l'application à un groupe d'utilisateurs et autoriser l'application à acheminer le trafic via le tunnel VPN GlobalProtect.

1. Sélectionnez **APPS & BOOKS (Applications et livres)** > **Applications** > **Native (Natives)** > **Public (Public)**.
2. Pour ajouter une nouvelle application, sélectionnez **ADD APPLICATION (Ajouter une application)**. Pour modifier les paramètres d'une application existante, recherchez

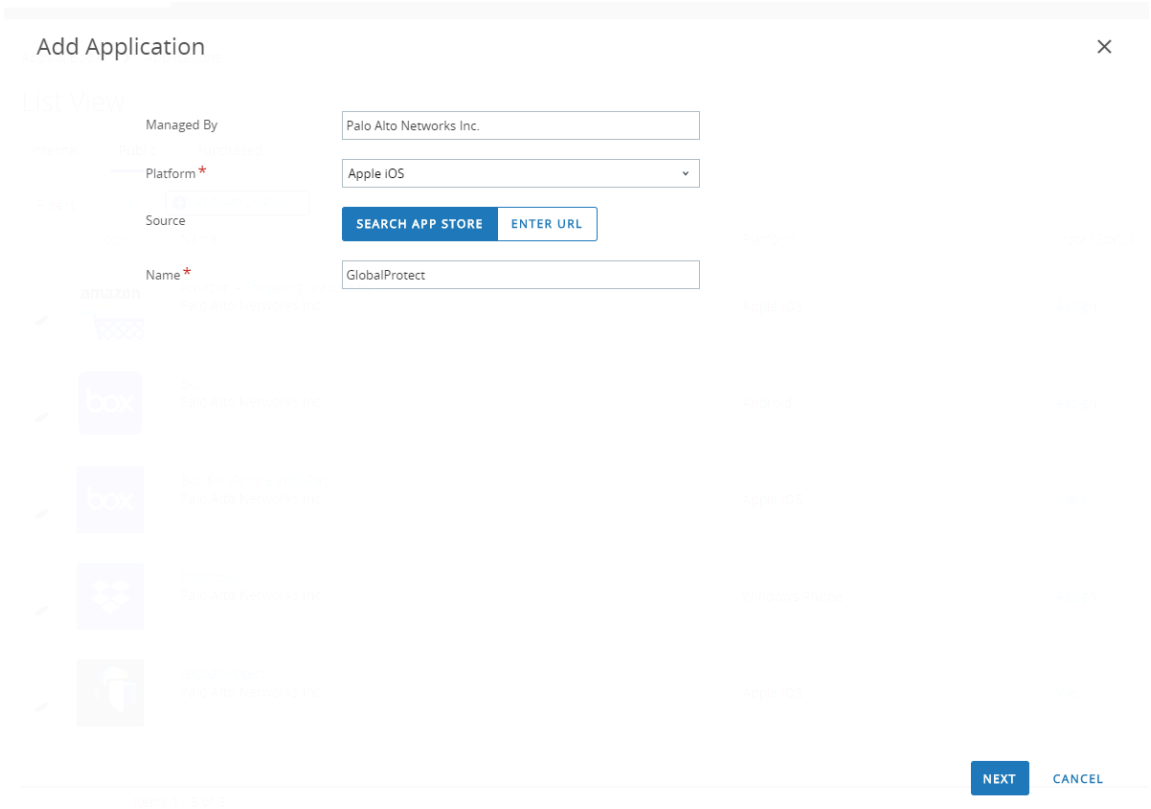
 ©2026 Palo Alto Networks, Inc.

l'application dans la liste des applications publiques (List View), puis sélectionnez l'icône Modifier (✎) dans le menu d'action qui se trouve à côté de la rangée.



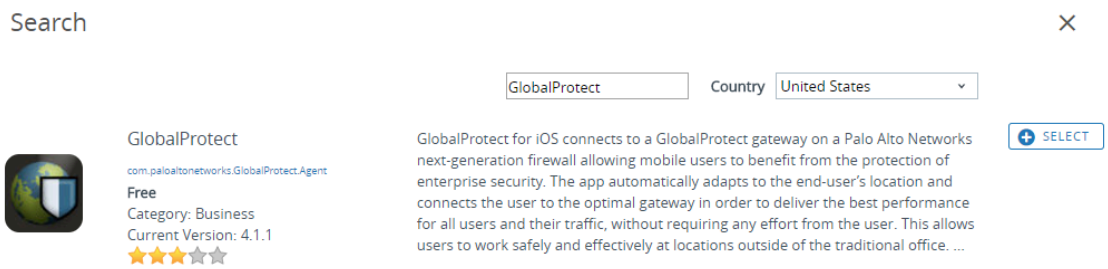
3. Dans le champ **Managed By (Géré par)**, sélectionnez le groupe de l'entreprise qui gérera cette application.
4. Définissez la **Platform (Plateforme)** sur **Apple iOS**.
5. Sélectionnez votre **Source** privilégiée pour trouver l'application :
   - **SEARCH APP STORE (Chercher dans l'App Store)** : saisissez le **Name (Nom)** de l'application.
   - **ENTER URL (SAISIR L'URL)** : saisissez l'URL de l'App Store de l'application (par exemple, pour ajouter l'application Box, saisissez https://itunes.apple.com/us/app/box-for-iphone-and-ipad/id290853822?mt=8&uo=4).

 ©2026 Palo Alto Networks, Inc.



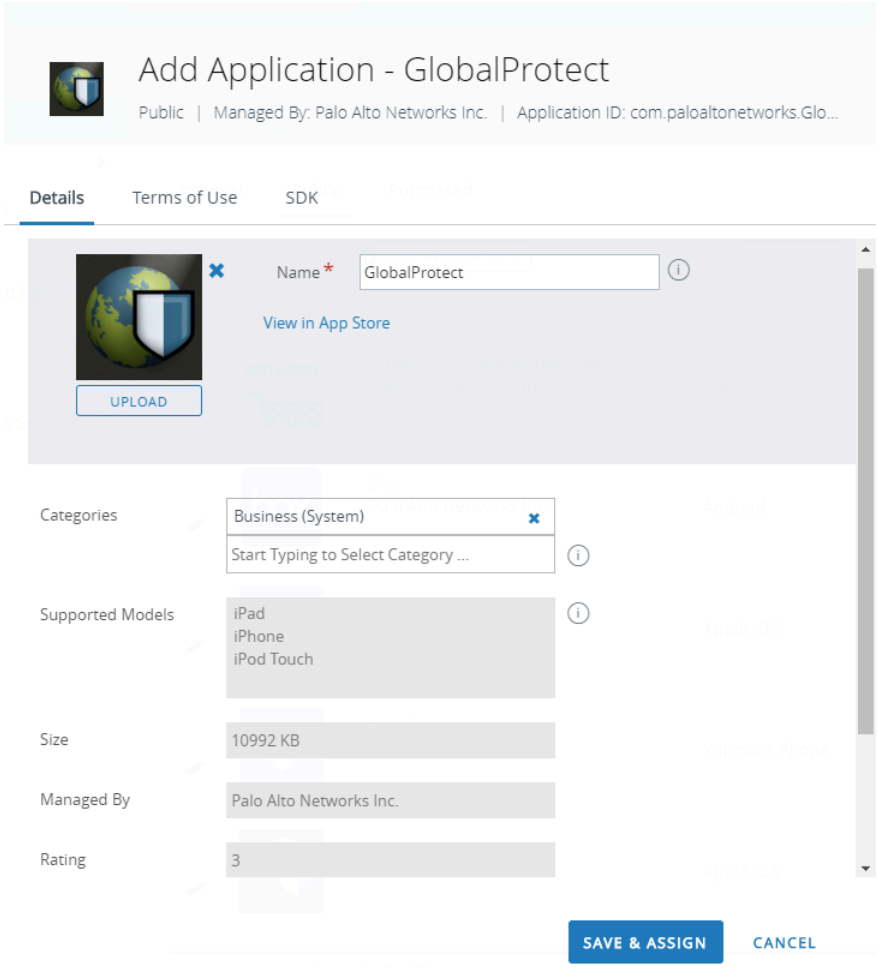
6. Cliquez sur **NEXT (Suivant)**.

   Si vous choisissez de rechercher l'application dans l'App Store, vous devez également **SELECT (Sélectionner)** l'application à partir d'une liste de résultats de recherche.



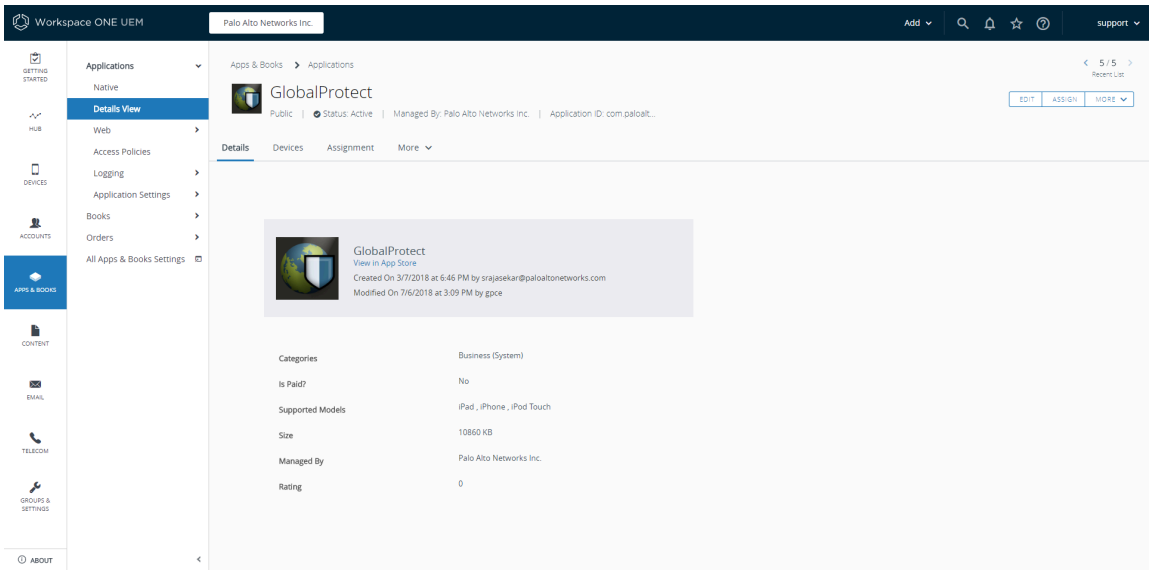
7. Sur le dialogue Add Application (Ajouter une application), assurez-vous que le **Name (Nom)** de l'application est bon. C'est le nom qui figurera dans le catalogue d'applications de Workspace ONE.
8. (Facultatif) Affectez l'application à des **Categories (Catégories)** prédéfinies ou personnalisées pour faciliter l'accès dans le catalogue d'applications de Workspace ONE.

 ©2026 Palo Alto Networks, Inc.



9. **SAVE & ASSIGN (Enregistrez et affectez)** la nouvelle application.
10. Sélectionnez l'application nouvellement ajoutée dans la liste des applications publiques (List View).
11. Dans **Applications (Applications)** > **Details View (Affichage des détails)**, cliquez sur **ASSIGN (AFFECTER)** dans le coin supérieur droit de l'écran.

 ©2026 Palo Alto Networks, Inc.

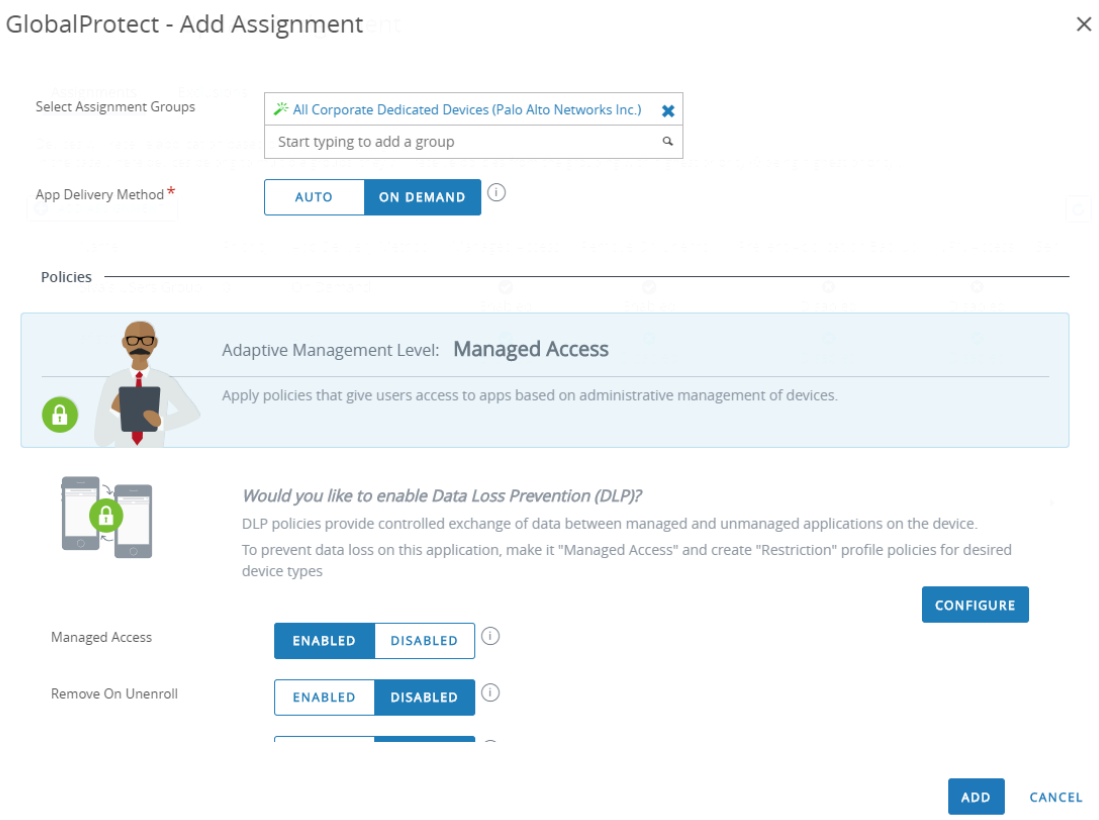


12. Sélectionnez **Assignments (Affectations)**, puis cliquez sur **ADD ASSIGNMENT (Ajouter l'affectation)** pour ajouter les groupes intelligents qui auront accès à cette application.
    1. Dans le champ **Select Assignment Groups (Sélectionner les groupes d'affectation)**, sélectionnez les groupes intelligents auxquels vous souhaitez accorder l'accès à cette application.
    2. Sélectionnez la **App Delivery Method (Méthode de livraison de l'application)**. Si vous sélectionnez **AUTO**, l'application est automatiquement déployée aux

 ©2026 Palo Alto Networks, Inc.

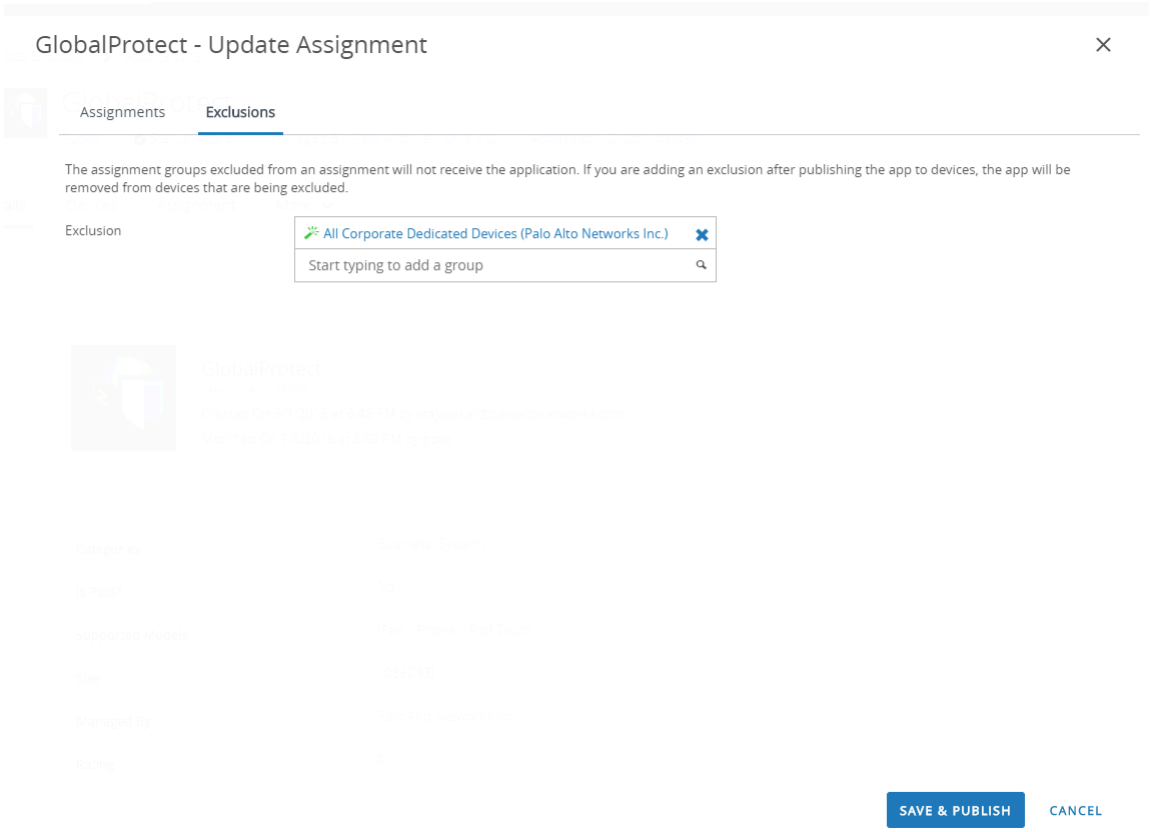
groupes intelligents indiqués. Si vous sélectionnez **ON DEMAND (À LA DEMANDE)**, l'application doit être déployée manuellement.

3. Définissez l'option **Managed Access (Accès géré)** sur **ENABLED (ACTIVÉ)**. Cette option donne aux utilisateurs un accès à l'application en fonction des politiques de gestion que vous appliquez.
4. Configurez les paramètres restants, au besoin.
5. **ADD (Ajoutez)** la nouvelle affectation.



13. (Facultatif) Pour empêcher certains groupes intelligents d'accéder à l'application, sélectionnez **Exclusions**, puis sélectionnez les groupes intelligents que vous souhaitez exclure dans le champ **Exclusion**.

©2026 Palo Alto Networks, Inc.



14. **SAVE & PUBLISH (Enregistrez et publiez)** la configuration dans les groupes intelligents affectés.

Configurer Workspace ONE pour les terminaux UWP Windows 10

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Lorsqu'il est déployé avec Workspace ONE pour les terminaux UWP Windows 10, GlobalProtect prend en charge les méthodes de connexion suivantes :

- Toujours actif

  Dans une configuration toujours active, GlobalProtect se connecte automatiquement dès que vous vous connectez.
- À la demande (configuration VPN d'accès à distance initié par l'utilisateur)

  Dans une configuration à la demande, vous devez vous connecter manuellement à GlobalProtect via l'application. Le trafic est acheminé via l'application GlobalProtect uniquement après que vous ayez initié et établi la connexion.

 ©2026 Palo Alto Networks, Inc.

- Par application

  Dans une configuration par application, vous pouvez définir quelles applications gérées sont autorisées à acheminer le trafic via GlobalProtect. Pour ce faire, vous pouvez attacher un profil VPN à une application, ajouter des URL pour l'application à laquelle vous souhaitez accéder, ou faire une combinaison des deux.

Configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans une configuration de VPN toujours active, la connexion GlobalProtect sécurisée est toujours active. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est toujours acheminé via le tunnel VPN. Pour des exigences de sécurité encore plus strictes, vous pouvez activer le verrouillage VP, qui force la connexion sécurisée à être toujours activée et connectée, en plus de désactiver l'accès au réseau lorsque l'application n'est pas connectée. Cette configuration est similaire à l'option **Enforce GlobalProtect for Network Access (appliquer GlobalProtect pour l'accès réseau)** que vous configurez généralement dans une configuration de portail GlobalProtect.

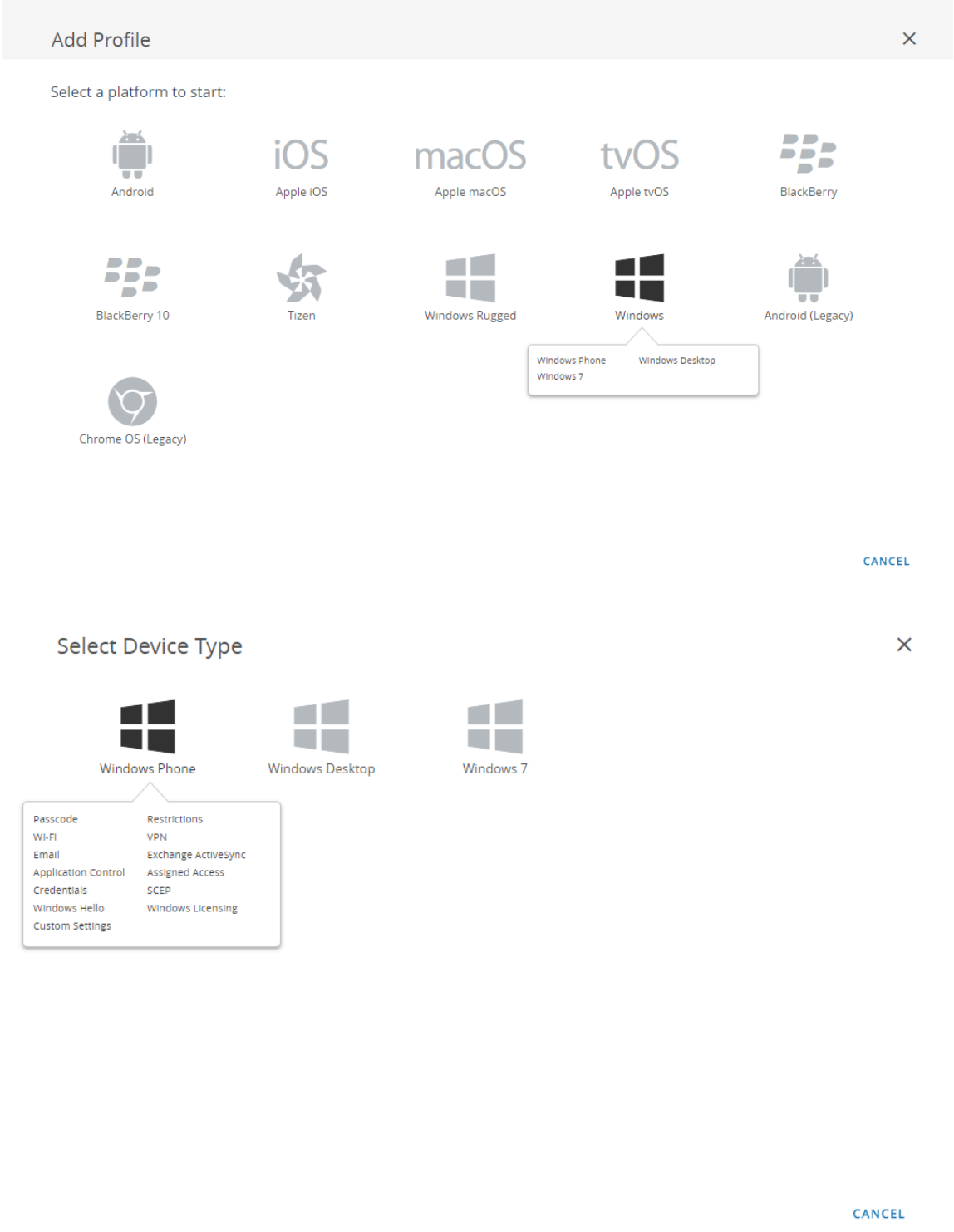
Parce que Workspace ONE ne répertorie pas encore GlobalProtect comme fournisseur de connexion officiel pour les terminaux Windows, vous devez sélectionner un autre fournisseur VPN, modifier les paramètres de l'application GlobalProtect et importer la configuration dans le profil VPN comme décrit dans le workflow suivant.

Utilisez les étapes suivantes pour configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide de Workspace ONE :

1. Téléchargez l'app GlobalProtect pour Windows 10 UWP :
   - Déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   - Téléchargez l'application GlobalProtect directement à partir du Microsoft Store.

 ©2026 Palo Alto Networks, Inc.

2. Depuis la console Workspace ONE, modifiez un profil UWP Windows 10 existant ou ajoutez-en un nouveau.
   1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajouter)** un nouveau profil.
   2. Sélectionnez **Windows** comme plateforme et **Windows Phone** comme type de configuration.

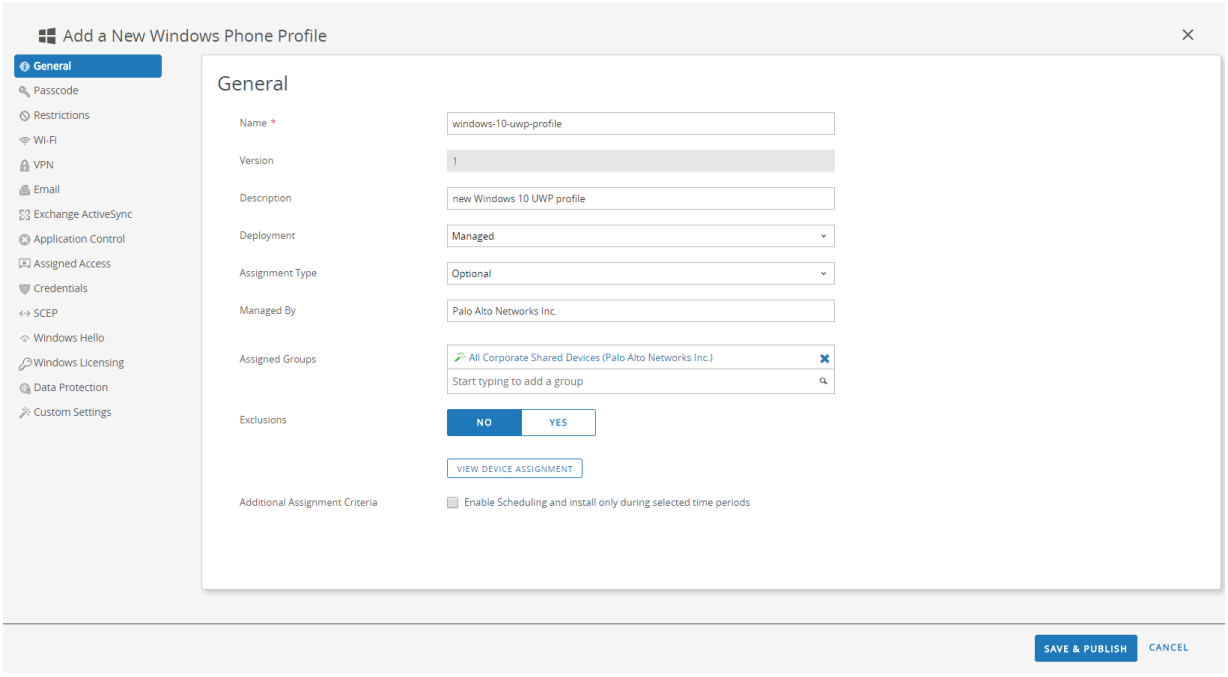


 ©2026 Palo Alto Networks, Inc.

3. Configurez les paramètres **General (généraux)**.
   1. Saisissez un **Name (Nom)** pour le profil.
   2. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
   3. (Facultatif) Définissez le mode de **Deployment (Déploiement)** sur **Managed (Géré)** pour permettre la suppression automatique du profil lors de la désinscription.
   4. (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les points de terminaison. Sélectionnez **Auto** pour déployer automatiquement le profil sur tous les points de terminaison, **Optional (Optionnel)** pour permettre à l'utilisateur final d'installer le profil à partir du portail SSP (portail libre-service) ou de déployer manuellement le profil sur des points de terminaison individuels, ou **Compliance (Conformité)** pour déployer le profil lorsqu'un utilisateur final enfreint une politique de conformité applicable au point de terminaison.
   5. (Facultatif) Dans le champ **Managed By (Géré par)**, saisissez le groupe de l'entreprise ayant un accès administratif au profil.
   6. (Facultatif) Dans le champ **Assigned Groups (Groupes affectés)**, ajoutez les Groupes intelligents auxquels vous souhaitez ajouter le profil. Ce champ comprend une option permettant la création d'un nouveau groupe intelligent pour lequel vous pouvez configurer les spécifications suivantes : exigences minimales en matière de système d'exploitation, modèles de périphérique, catégories de propriété, groupes de l'entreprise, parmi tant d'autres.
   7. (Facultatif) Indiquez si vous souhaitez ajouter des **Exclusions** à l'affectation de ce profil. Si vous sélectionnez **Yes (Oui)**, le champ **Excluded Groups (Groupes exclus)** s'affiche, vous permettant de sélectionner les groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.
   8. (Facultatif) Si vous **Enable Scheduling and install only during selected time periods (Activez la planification et installez uniquement lors des périodes de temps sélectionnées)**, vous pouvez appliquer un calendrier (**Devices (Périphériques)** > **Profiles & Resources (Profil et ressources)** > **Profiles Settings (Paramètres du profil)** > **Time Schedules (Calendriers)**) à l'installation du profil, ce qui limite les périodes de temps pendant lesquelles le profil peut

 ©2026 Palo Alto Networks, Inc.

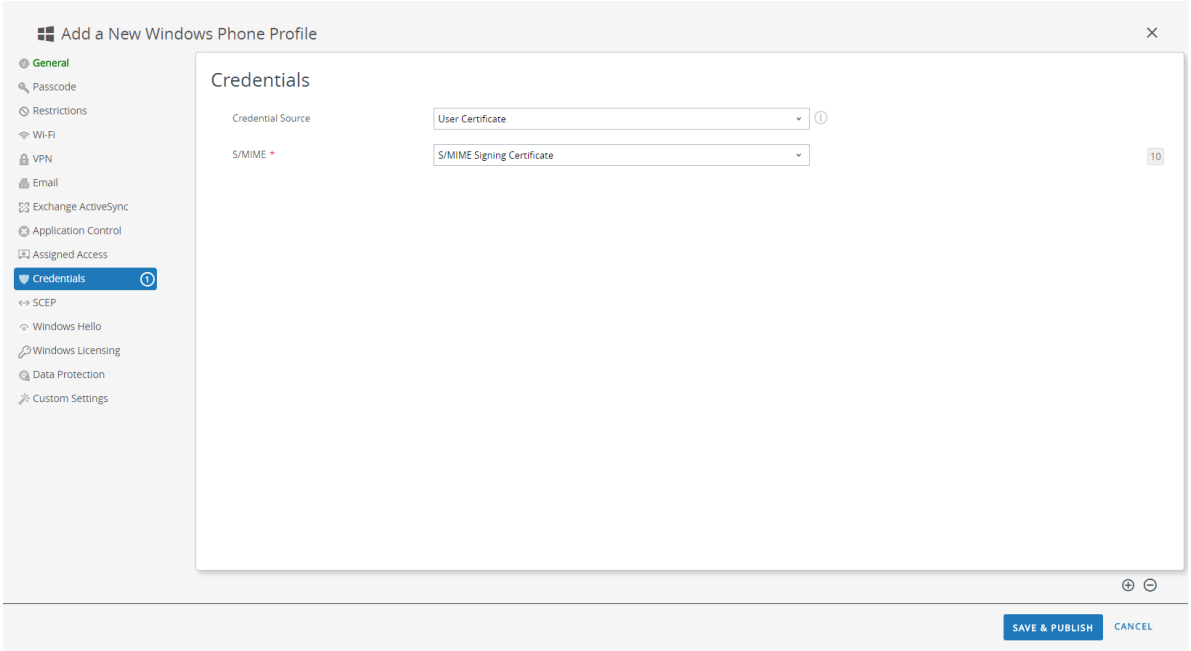
être installé sur les points de terminaison. Lorsque vous êtes invité à le faire, saisissez le nom du calendrier dans le champ **Assigned Schedules (Calendriers affectés)**.



 ©2026 Palo Alto Networks, Inc.

4. (Facultatif) Si votre déploiement GlobalProtect exige une authentification du certificat du client, configurez les paramètres des **Credentials (Informations d'identification)** :

- Pour extraire les certificats de client des utilisateurs Workspace ONE :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).



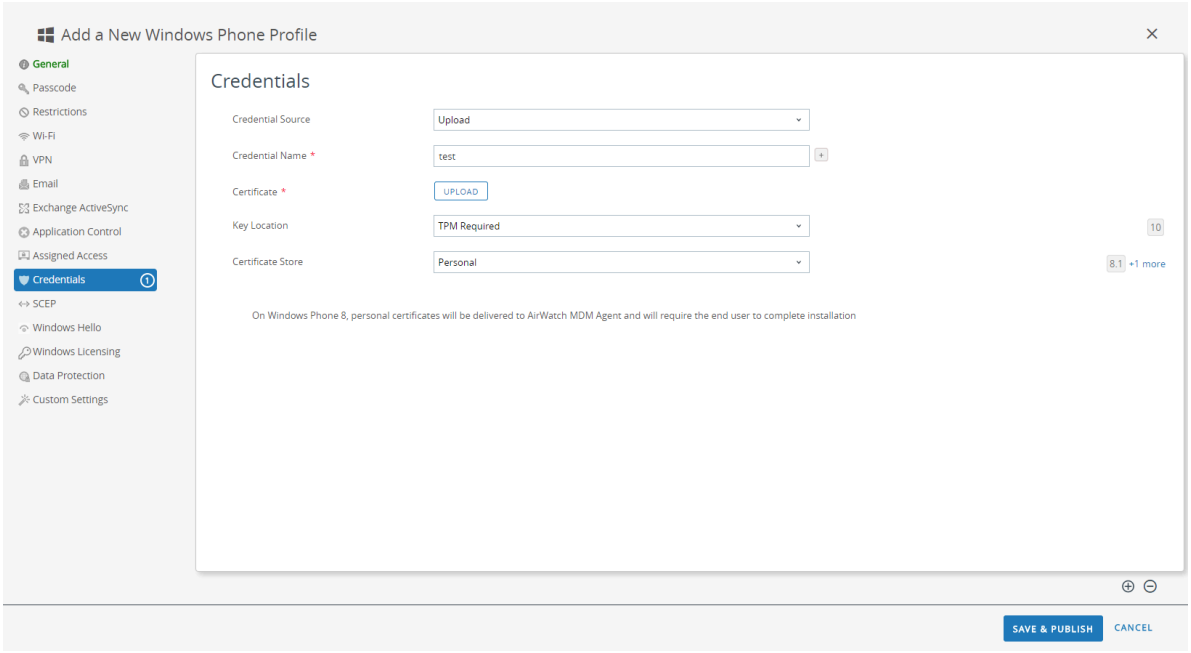
- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.
  5. Sélectionnez le **Key Location (Emplacement clé)** où vous voulez stocker la clé privée du certificat :
     - **TPM Required (TPM requis)** : stockez la clé privée sur un Module de plateforme de confiance. Si aucun module de plateforme de confiance n'est disponible sur le point de terminaison, la clé privée ne peut être installée.
     - **TPM si présent** : stockez la clé privée sur un module de plateforme de confiance s'il y en a un disponible sur le point de terminaison. Si aucun module de plateforme de

 ©2026 Palo Alto Networks, Inc.

confiance n'est disponible sur le point de terminaison, la clé privée est stockée dans le logiciel du point de terminaison.

- **Software (Logiciel)** : stocke la clé privée dans le logiciel du point de terminaison.
- **Passport (Passeport)** : enregistre la clé privée dans Microsoft Passport. Pour utiliser cette option, la protection de l'agent Workspace ONE doit être installé sur le terminal.

6. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.



- Pour utiliser une autorité de certification et un modèle prédéfinis :

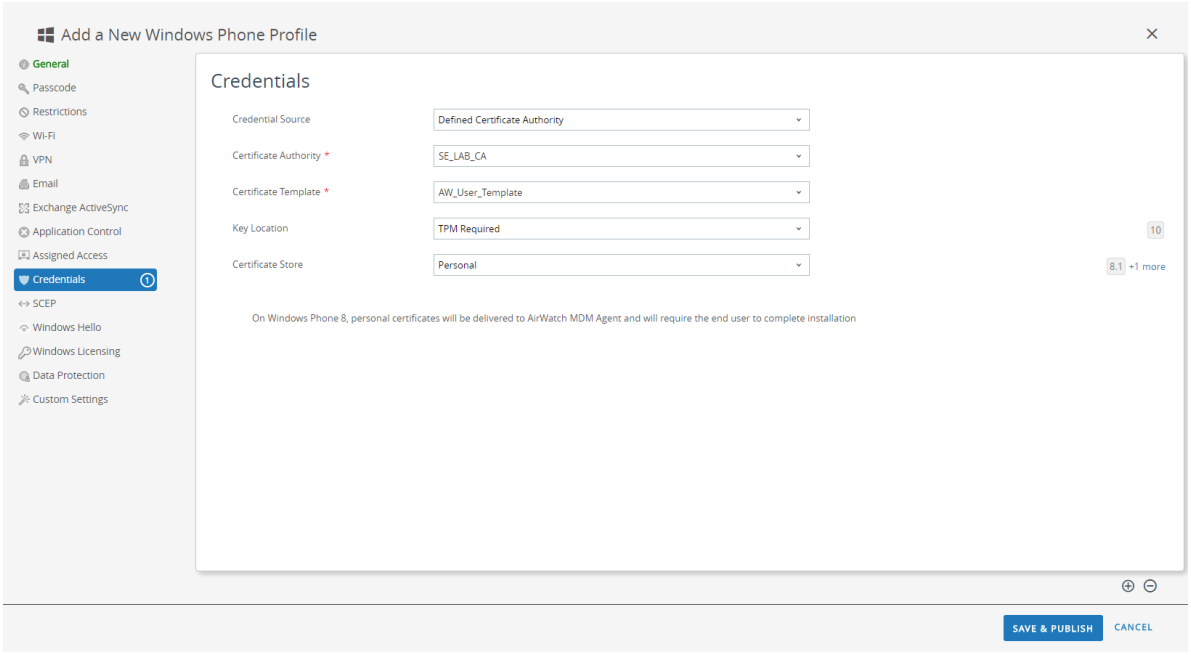
1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
2. Sélectionnez la **Certificate Authority (Autorité de certification)** de laquelle vous souhaitez obtenir les certificats.
3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.
4. Sélectionnez le **Key Location (Emplacement clé)** où vous voulez stocker la clé privée du certificat :
   - **TPM Required (TPM requis)** : stockez la clé privée sur un Module de plateforme de confiance. Si aucun module de plateforme de confiance n'est disponible sur le point de terminaison, la clé privée ne peut être installée.
   - **TPM si présent** : stockez la clé privée sur un module de plateforme de confiance s'il y en a un disponible sur le point de terminaison. Si aucun module de plateforme de

 ©2026 Palo Alto Networks, Inc.

confiance n'est disponible sur le point de terminaison, la clé privée est stockée dans le logiciel du point de terminaison.

- **Software (Logiciel)** : stocke la clé privée dans le logiciel du point de terminaison.
- **Passport (Passeport)** : enregistre la clé privée dans Microsoft Passport. Pour utiliser cette option, la protection de l'agent Workspace ONE doit être installé sur le terminal.

5. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.

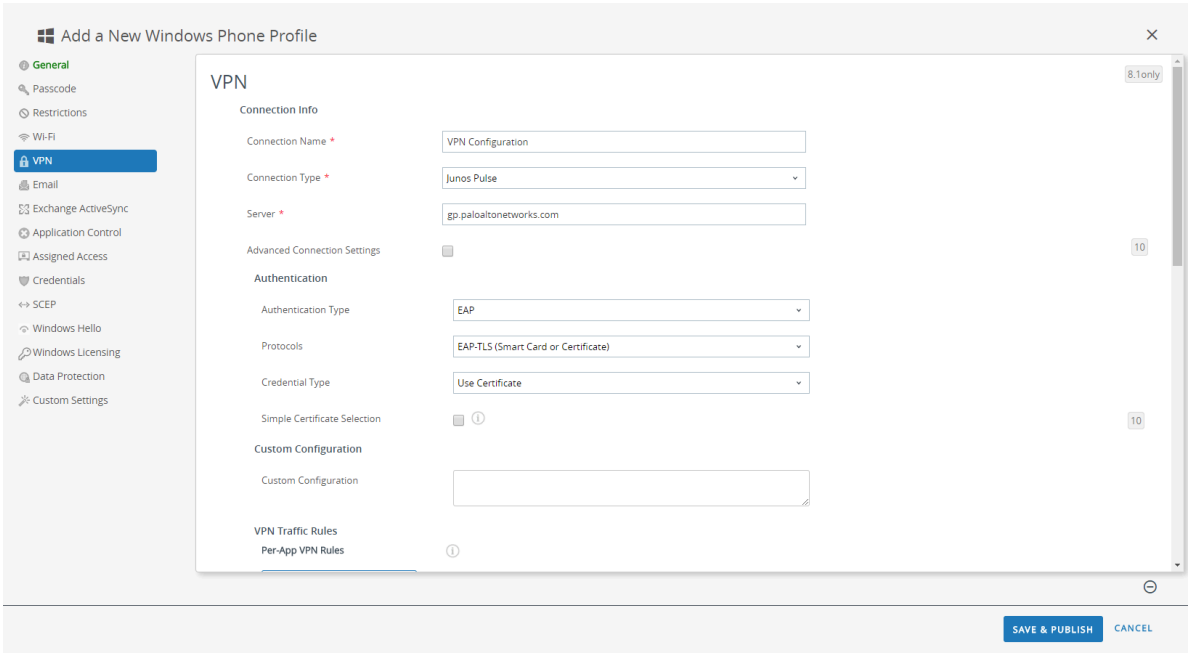


 ©2026 Palo Alto Networks, Inc.

5. Configurez les paramètres **VPN** :

1. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
2. Sélectionnez un autre fournisseur de **Connection Type (Type de connexion)** (ne sélectionnez pas **IKEv2**, **L2TP**, **PPTP** ou **Automatic (Automatique)**, car ceux-ci n'ont pas les paramètres de fournisseur associés requis pour le profil VPN GlobalProtect).

   Vous devez sélectionner un fournisseur de rechange, car Workspace ONE ne répertorie pas encore GlobalProtect en tant que fournisseur de connexions officiel pour les terminaux Windows.
3. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
4. Dans la section Authentication (Authentification), sélectionnez un **Authentication Type (Type d'authentication)** pour préciser la méthode d'authentification des utilisateurs finaux.

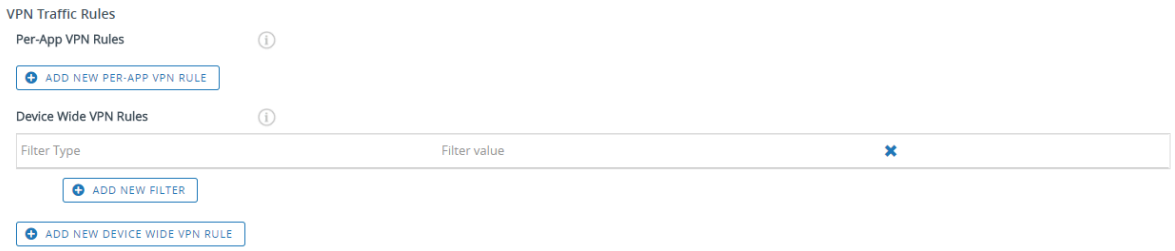


5. (Facultatif) Pour permettre à GlobalProtect d'enregistrer les informations d'identification de l'utilisateur, **ENABLE (ACTIVEZ)** l'option permettant de **Remember Credentials (Mémoriser les informations)** d'identification dans la zone de stratégies.
6. (Facultatif) Dans la section VPN Traffic Rules (Règles de trafic VPN), **ADD NEW DEVICE WIDE VPN RULE (AJOUTEZ UNE NOUVELLE RÈGLE VPN À L'ÉCHELLE DU PÉRIPHÉRIQUE)** pour acheminer le trafic correspondant via le tunnel VPN par un itinéraire spécifique. Ces règles ne sont pas liées par application, mais sont évaluées sur l'ensemble du

 ©2026 Palo Alto Networks, Inc.

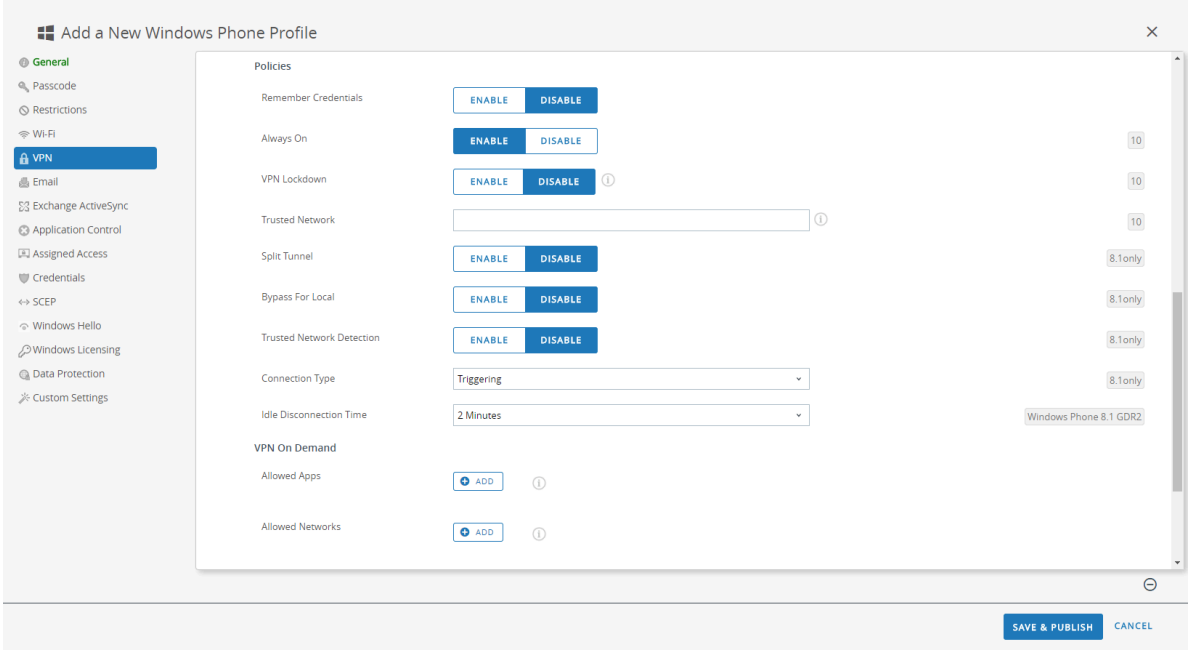
point de terminaison. Si le trafic correspond aux critères de correspondance précisés, il est acheminé par le biais du tunnel VPN.

Ajoutez un critère de correspondance en cliquant sur **ADD NEW FILTER (AJOUTER UN NOUVEAU FILTRE)**, puis saisissez un **Filter Type (Type de filtre)** et une **Filter Value (Valeur de filtrage)** correspondante.



7. Pour toujours maintenir la connexion GlobalProtect, configurez l'une des options suivantes dans la section Policies (Politiques) :

   - **ENABLE (ACTIVEZ)Always On (Toujours active)** pour forcer la connexion sécurisée à être toujours active.
   - **ENABLE (ACTIVEZ)** le **VPN Lockdown (Verrouillage VPN)** pour forcer la connexion sécurisée à être toujours ON et connectée et désactivez l'accès réseau lorsque l'application n'est pas connectée. L'option de **VPN Lockdown (Verrouillage VPN)** dans Workspace ONE est similaire à l'option **Enforce GlobalProtect for Network Access (appliquer GlobalProtect pour l'accès réseau)** que vous configurez dans une configuration de portail GlobalProtect.



8. (Facultatif) Spécifiez les adresses **Trusted Network (réseau de confiance)** si vous souhaitez que GlobalProtect se connecte uniquement lorsqu'il détecte une connexion réseau approuvée.

6. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

 ©2026 Palo Alto Networks, Inc.

7. Pour définir le fournisseur de type de connexion dans GlobalProtect, modifiez le profil VPN en XML.

   Pour minimiser les modifications supplémentaires dans le XML brut, examinez les paramètres de votre profil VPN avant d'exporter la configuration. Si vous avez besoin de modifier un paramètre après l'exportation du profil VPN, vous pouvez effectuer les modifications dans le XML brut ou, vous pouvez mettre à jour le paramètre dans le profil VPN et effectuer cette étape à nouveau.

   1. Dans **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue de la liste)**, sélectionnez le bouton d'option qui se trouve à côté du nouveau profil que vous avez ajouté aux étapes précédentes, puis sélectionnez **</>XML** en haut de la table. Workspace ONE ouvre l'affichage XML du profil.
   2. **Export (Exportez)**le profil, puis ouvrez-le dans un éditeur de texte de votre choix.
   3. Modifiez les paramètres suivants pour GlobalProtect :

   - Dans l'élément `LoclURI` qui spécifie le `PluginPackageFamilyName`, modifiez l'élément en :

     `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

   - Dans l'élément `Data` qui suit, changez la valeur en :

     `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

   1. Enregistrez vos modifications dans le profil exporté.
   2. Retournez à Workspace ONE et sélectionnez **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue liste)**.
   3. Créez et nommez un nouveau profil (sélectionnez **ADD (Ajouter)** > **Add Profile (Ajouter un profil)** > **Windows (Windows)** > **Windows Phone (Windows Phone)**).
   4. Sélectionnez **Custom Settings (Paramètres personnalisés)** > **Configure (Configurer)**, puis copiez et collez la configuration modifiée.
   5. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

8. Nettoyez le profil original en sélectionnant le sélectionnant à partir de **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue de la liste)**, puis sélectionnez **More Actions (Plus d'actions)** > **Deactivate (Désactiver)**. Workspace ONE déplace le profil sur la liste inactive.

9. Testez la configuration.

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les terminaux Windows 10 UWP à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

Dans une configuration de VPN d'accès à distance (à la demande), les utilisateurs doivent lancer manuellement l'application pour établir la connexion GlobalProtect sécurisée. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est acheminé via le tunnel VPN seulement après que les utilisateurs ont initié et établi la connexion.

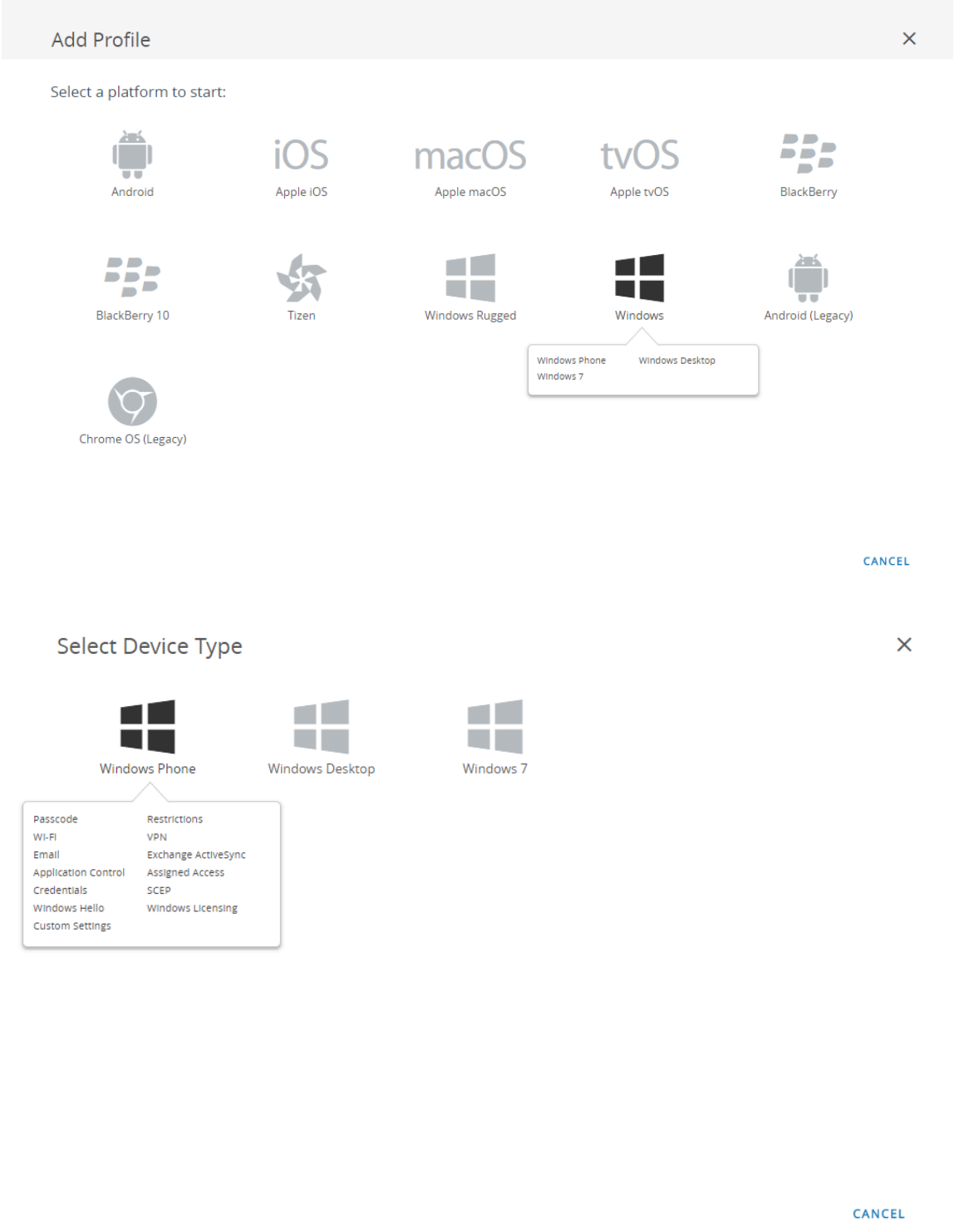
Parce que Workspace ONE ne répertorie pas encore GlobalProtect comme fournisseur de connexion officiel pour les terminaux Windows, vous devez sélectionner un autre fournisseur VPN, modifier les paramètres de l'application GlobalProtect et importer la configuration dans le profil VPN comme décrit dans le workflow suivant.

Utilisez les étapes suivantes pour configurer configuration de VPN d'accès à distance initié par l'utilisateur sur les terminaux Windows 10 UWP à l'aide de Workspace ONE :

1. Téléchargez l'app GlobalProtect pour Windows 10 UWP :
   - Déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   - Téléchargez l'application GlobalProtect directement à partir du Microsoft Store.

 ©2026 Palo Alto Networks, Inc.

2. Depuis la console Workspace ONE, modifiez un profil UWP Windows 10 existant ou ajoutez-en un nouveau.
   1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajouter)** un nouveau profil.
   2. Sélectionnez **Windows** comme plateforme et **Windows Phone** comme type de configuration.

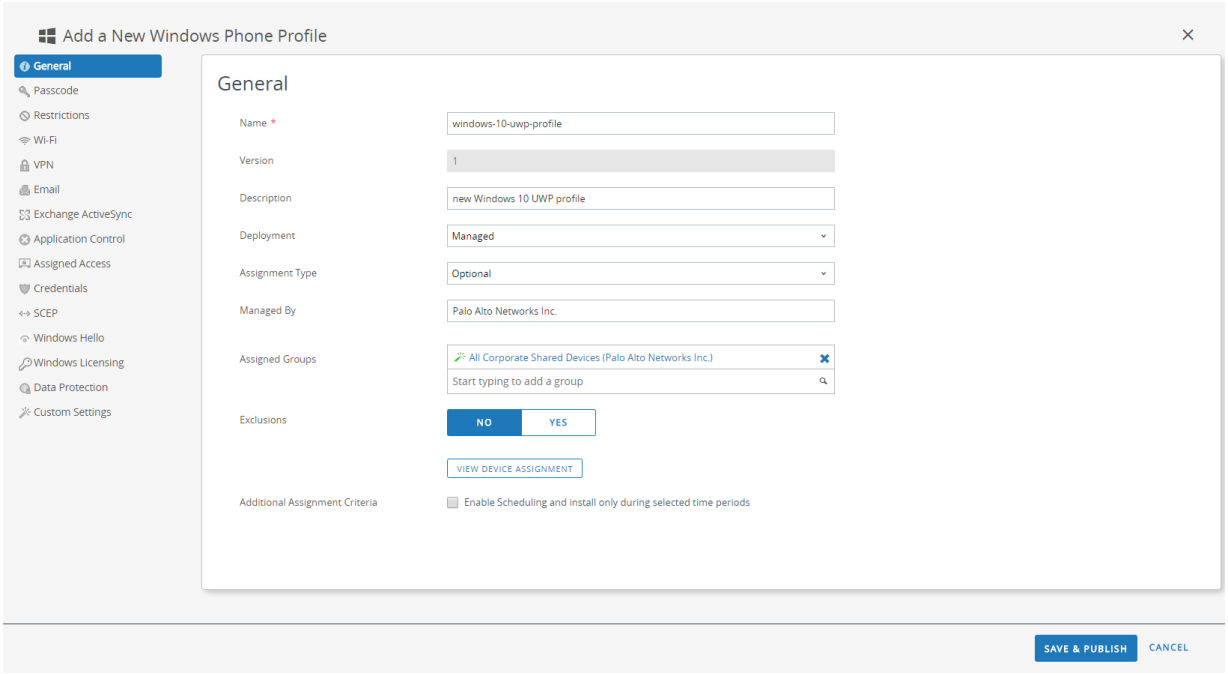


 ©2026 Palo Alto Networks, Inc.

3. Configurez les paramètres **General (généraux)**.
   1. Saisissez un **Name (Nom)** pour le profil.
   2. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
   3. (Facultatif) Définissez le mode de **Deployment (Déploiement)** sur **Managed (Géré)** pour permettre la suppression automatique du profil lors de la désinscription.
   4. (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les points de terminaison. Sélectionnez **Auto** pour déployer automatiquement le profil sur tous les points de terminaison, **Optional (Optionnel)** pour permettre à l'utilisateur final d'installer le profil à partir du portail SSP (portail libre-service) ou de déployer manuellement le profil sur des points de terminaison individuels, ou **Compliance (Conformité)** pour déployer le profil lorsqu'un utilisateur final enfreint une politique de conformité applicable au point de terminaison.
   5. (Facultatif) Dans le champ **Managed By (Géré par)**, saisissez le groupe de l'entreprise ayant un accès administratif au profil.
   6. (Facultatif) Dans le champ **Assigned Groups (Groupes affectés)**, ajoutez les Groupes intelligents auxquels vous souhaitez ajouter le profil. Ce champ comprend une option permettant la création d'un nouveau groupe intelligent pour lequel vous pouvez configurer les spécifications suivantes : exigences minimales en matière de système d'exploitation, modèles de périphérique, catégories de propriété, groupes de l'entreprise, parmi tant d'autres.
   7. (Facultatif) Indiquez si vous souhaitez ajouter des **Exclusions** à l'affectation de ce profil. Si vous sélectionnez **Yes (Oui)**, le champ **Excluded Groups (Groupes exclus)** s'affiche, vous permettant de sélectionner les groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.
   8. (Facultatif) Si vous **Enable Scheduling and install only during selected time periods (Activez la planification et installez uniquement lors des périodes de temps sélectionnées)**, vous pouvez appliquer un calendrier (**Devices (Périphériques)** > **Profiles & Resources (Profil et ressources)** > **Profiles Settings (Paramètres du profil)** > **Time Schedules (Calendriers)**) à l'installation du profil, ce qui limite les périodes de temps pendant lesquelles le profil peut

 ©2026 Palo Alto Networks, Inc.

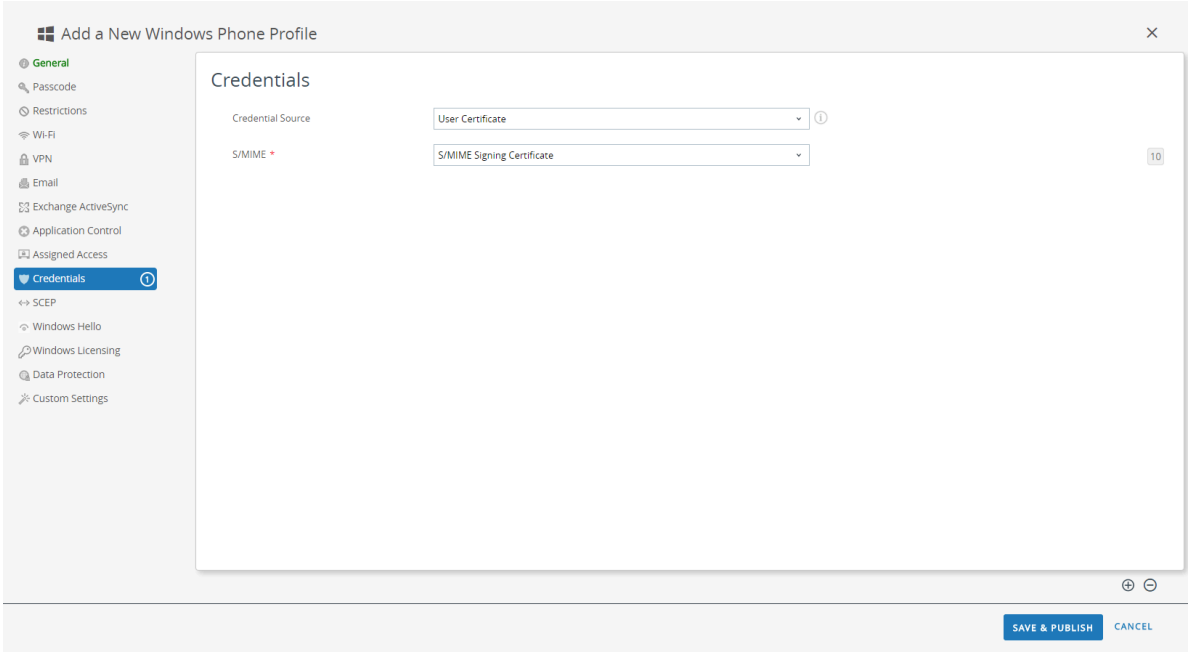
être installé sur les points de terminaison. Lorsque vous êtes invité à le faire, saisissez le nom du calendrier dans le champ **Assigned Schedules (Calendriers affectés)**.



 ©2026 Palo Alto Networks, Inc.

4. (Facultatif) Si votre déploiement GlobalProtect exige une authentification du certificat du client, configurez les paramètres des **Credentials (Informations d'identification)** :

- Pour extraire les certificats de client des utilisateurs Workspace ONE :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).



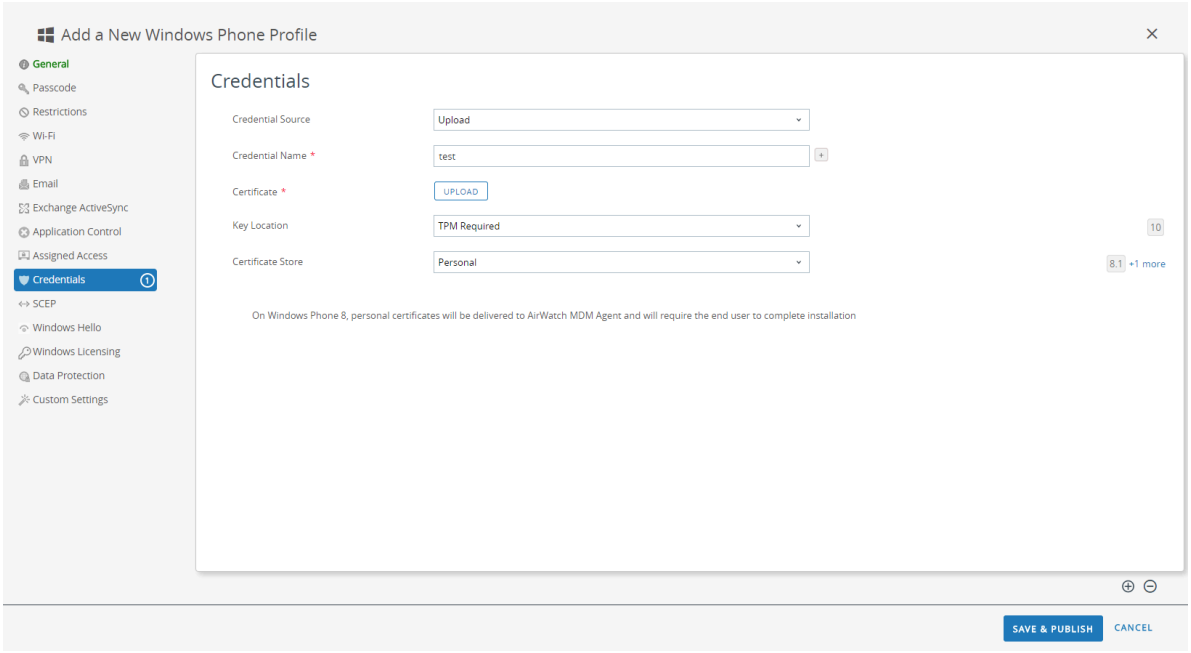
- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.
  5. Sélectionnez le **Key Location (Emplacement clé)** où vous voulez stocker la clé privée du certificat :
     - **TPM Required (TPM requis)** : stockez la clé privée sur un Module de plateforme de confiance. Si aucun module de plateforme de confiance n'est disponible sur le point de terminaison, la clé privée ne peut être installée.
     - **TPM si présent** : stockez la clé privée sur un module de plateforme de confiance s'il y en a un disponible sur le point de terminaison. Si aucun module de plateforme de

 ©2026 Palo Alto Networks, Inc.

confiance n'est disponible sur le point de terminaison, la clé privée est stockée dans le logiciel du point de terminaison.

- **Software (Logiciel)** : stocke la clé privée dans le logiciel du point de terminaison.
- **Passport (Passeport)** : enregistre la clé privée dans Microsoft Passport. Pour utiliser cette option, la protection de l'agent Workspace ONE doit être installé sur le terminal.

6. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.



- Pour utiliser une autorité de certification et un modèle prédéfinis :

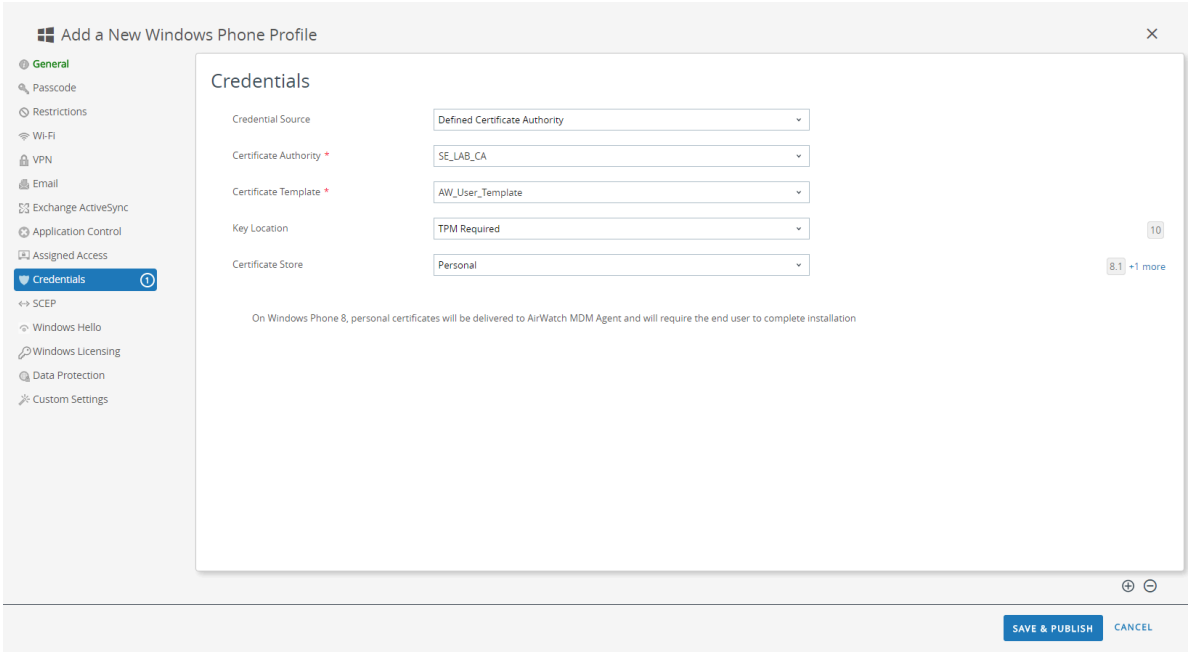
1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
2. Sélectionnez la **Certificate Authority (Autorité de certification)** de laquelle vous souhaitez obtenir les certificats.
3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.
4. Sélectionnez le **Key Location (Emplacement clé)** où vous voulez stocker la clé privée du certificat :
   - **TPM Required (TPM requis)** : stockez la clé privée sur un Module de plateforme de confiance. Si aucun module de plateforme de confiance n'est disponible sur le point de terminaison, la clé privée ne peut être installée.
   - **TPM si présent** : stockez la clé privée sur un module de plateforme de confiance s'il y en a un disponible sur le point de terminaison. Si aucun module de plateforme de

 ©2026 Palo Alto Networks, Inc.

confiance n'est disponible sur le point de terminaison, la clé privée est stockée dans le logiciel du point de terminaison.

- **Software (Logiciel)** : stocke la clé privée dans le logiciel du point de terminaison.
- **Passport (Passeport)** : enregistre la clé privée dans Microsoft Passport. Pour utiliser cette option, la protection de l'agent Workspace ONE doit être installé sur le terminal.

5. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.

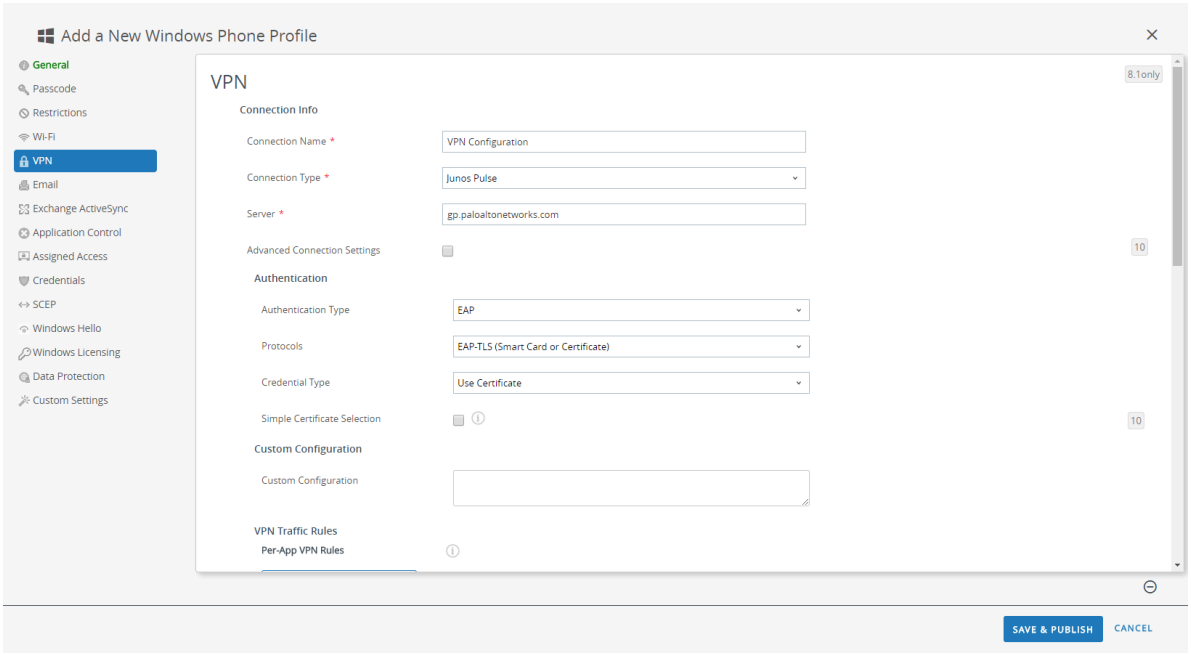


 ©2026 Palo Alto Networks, Inc.

5. Configurez les paramètres **VPN** :

   1. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
   2. Sélectionnez un autre fournisseur de **Connection Type (Type de connexion)** (ne sélectionnez pas **IKEv2**, **L2TP**, **PPTP** ou **Automatic (Automatique)**, car ceux-ci n'ont pas les paramètres de fournisseur associés requis pour le profil VPN GlobalProtect).

      Vous devez sélectionner un fournisseur de rechange, car Workspace ONE ne répertorie pas encore GlobalProtect en tant que fournisseur de connexions officiel pour les terminaux Windows.
   3. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
   4. Dans la section Authentication (Authentification), sélectionnez un **Authentication Type (Type d'authentication)** pour préciser la méthode d'authentification des utilisateurs finaux.

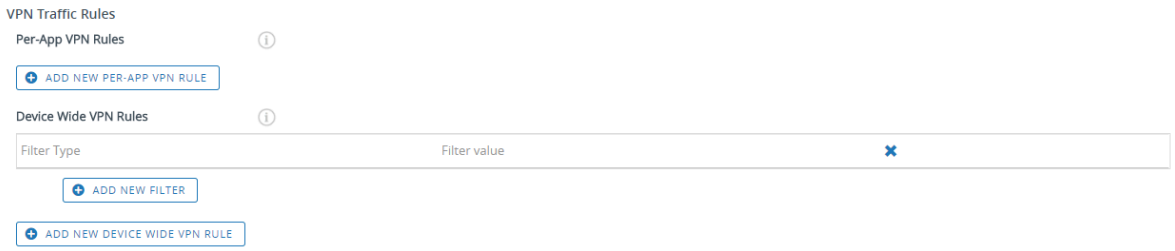


   5. (Facultatif) Pour permettre à GlobalProtect d'enregistrer les informations d'identification de l'utilisateur, **ENABLE (ACTIVEZ)** l'option permettant de **Remember Credentials (Mémoriser les informations)** d'identification dans la zone de stratégies.
   6. (Facultatif) Dans la section VPN Traffic Rules (Règles de trafic VPN), **ADD NEW DEVICE WIDE VPN RULE (AJOUTEZ UNE NOUVELLE RÈGLE VPN À L'ÉCHELLE DU PÉRIPHÉRIQUE)** pour acheminer le trafic correspondant via le tunnel VPN par un itinéraire spécifique. Ces règles ne sont pas liées par application, mais sont évaluées sur l'ensemble du

 ©2026 Palo Alto Networks, Inc.

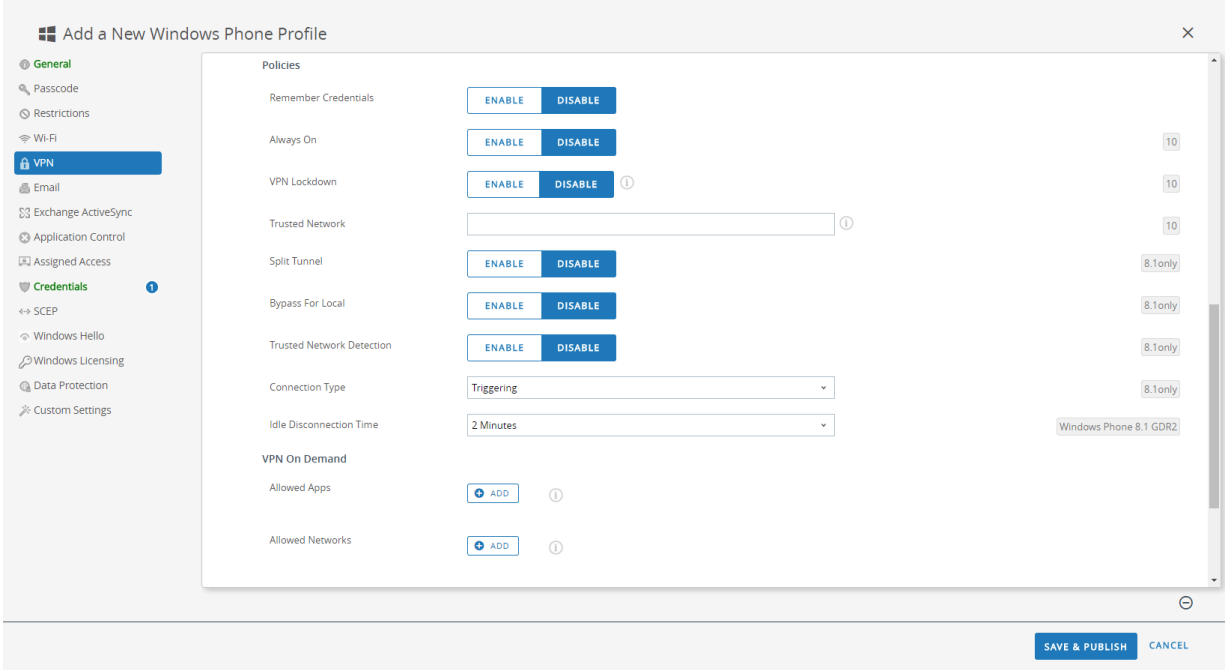
point de terminaison. Si le trafic correspond aux critères de correspondance précisés, il est acheminé par le biais du tunnel VPN.

Ajouter les critères de correspondance en cliquant sur **ADD NEW FILTER (Ajouter un nouveau filtre)**. Lorsque vous êtes invité à le faire, saisissez un **Filter Type (Type de filtre)** et la **Filter Value (Valeur de filtre)** correspondante.



7. Pour s'assurer que ce profil utilise la méthode de connexion à la demande, configurez les paramètres suivants dans la section Policies (Politiques) :

   - **DISABLE (DÉSACTIVEZ) Always On (Toujours active)**. Si ce champ est **ENABLED (Activé)**, la connexion sécurisée est toujours active.
   - **DISABLE (DÉSACTIVEZ) VPN Lockdown (Verouillage VPN)**. Si ce champ est **ENABLED (Activé)**, la connexion sécurisée est toujours active et l'accès au réseau est désactivé lorsque l'application n'est pas connectée. L'option de **VPN Lockdown (Verrouillage VPN)** dans Workspace ONE est similaire à l'option **Enforce GlobalProtect for Network Access (appliquer GlobalProtect pour l'accès réseau)** que vous configurez dans une configuration de portail GlobalProtect.



6. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

 ©2026 Palo Alto Networks, Inc.

7. Pour définir le fournisseur de type de connexion dans GlobalProtect, modifiez le profil VPN en XML.

   Pour minimiser les modifications supplémentaires dans le XML brut, examinez les paramètres de votre profil VPN avant d'exporter la configuration. Si vous avez besoin de modifier un paramètre après l'exportation du profil VPN, vous pouvez effectuer les modifications dans le XML brut ou, vous pouvez mettre à jour le paramètre dans le profil VPN et effectuer cette étape à nouveau.

   1. Dans **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue de la liste)**, sélectionnez le bouton d'option qui se trouve à côté du nouveau profil que vous avez ajouté aux étapes précédentes, puis sélectionnez **</>XML** en haut de la table. Workspace ONE ouvre l'affichage XML du profil.
   2. **Export (Exportez)**le profil, puis ouvrez-le dans un éditeur de texte de votre choix.
   3. Modifiez les paramètres suivants pour GlobalProtect :

   - Dans l'élément `LoclURI` qui spécifie le `PluginPackageFamilyName`, modifiez l'élément en :

     `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

   - Dans l'élément `Data` qui suit, changez la valeur en :

     `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

   1. Enregistrez vos modifications dans le profil exporté.
   2. Retournez à Workspace ONE et sélectionnez **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue liste)**.
   3. Créez (sélectionnez **Add (Ajouter)** > **Add Profile (Ajouter un profil)** > **Windows (Windows)** > **Windows Phone (Windows Phone)**) et nommez un nouveau profil.
   4. Sélectionnez **Custom Settings (Paramètres personnalisés)** > **Configure (Configurer)**, puis copiez et collez la configuration modifiée.
   5. **Save & Publish (Enregistrez et publiez)** vos modifications.

8. Nettoyez le profil original en sélectionnant le sélectionnant à partir de **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue de la liste)**, puis sélectionnez **More Actions (Plus d'actions)** > **Deactivate (Désactiver)**. Workspace ONE déplace le profil sur la liste inactive.

9. Testez la configuration.

Configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

Vous pouvez autoriser l'accès aux ressources internes à partir de vos périphériques mobiles gérés en configurant l'accès VPN GlobalProtect à l'aide de Workspace ONE. Dans une configuration VPN par application, vous pouvez indiquer les applications gérées qui peuvent acheminer le trafic via le tunnel VPN GlobalProtect. Les applications non gérées continueront de se connecter directement par l'Internet plutôt que via le tunnel VPN GlobalProtect.

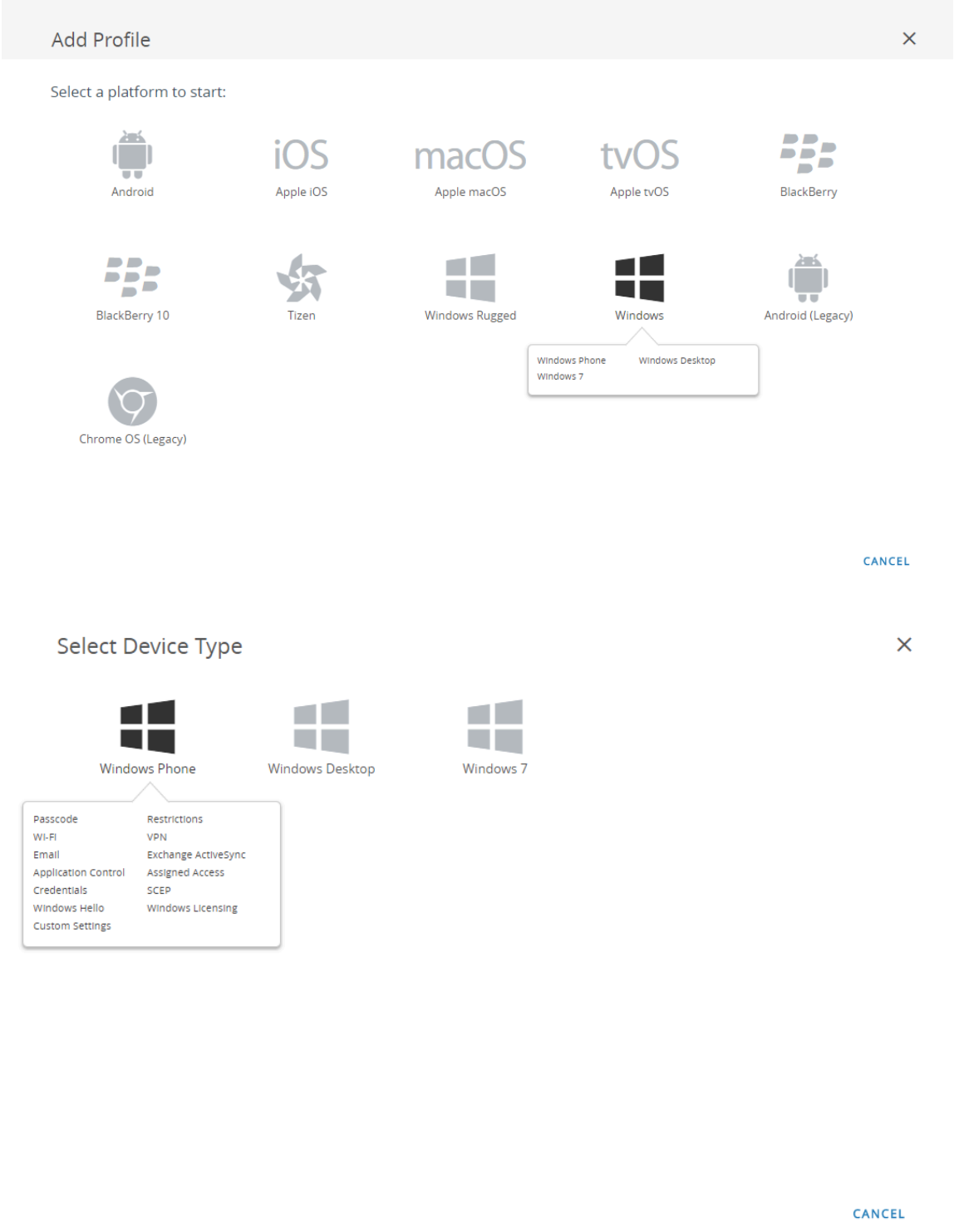
Parce que Workspace ONE ne répertorie pas encore GlobalProtect comme fournisseur de connexion officiel pour les terminaux Windows, vous devez sélectionner un autre fournisseur VPN, modifier les paramètres de l'application GlobalProtect et importer la configuration dans le profil VPN comme décrit dans le workflow suivant.

Utilisez les étapes suivantes pour configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide de Workspace ONE :

1. Téléchargez l'app GlobalProtect pour Windows 10 UWP :
   - Déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   - Téléchargez l'application GlobalProtect directement à partir du Microsoft Store.

 ©2026 Palo Alto Networks, Inc.

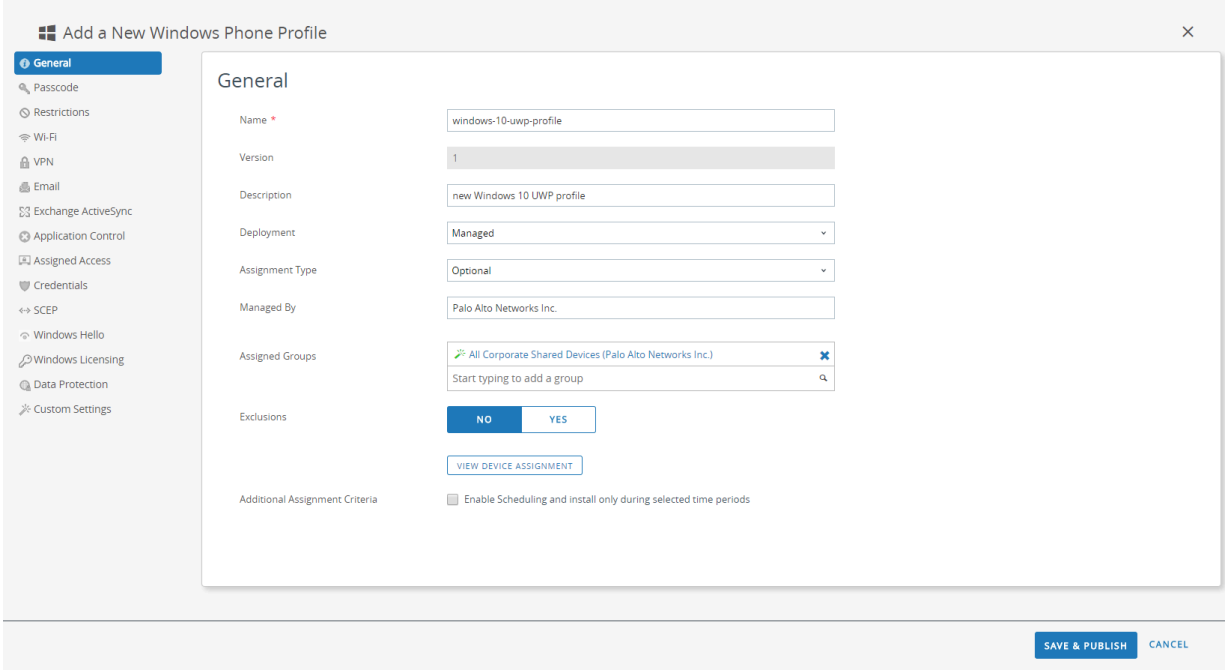
2. Depuis la console Workspace ONE, modifiez un profil UWP Windows 10 existant ou ajoutez-en un nouveau.
   1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajouter)** un nouveau profil.
   2. Sélectionnez **Windows** comme plateforme et **Windows Phone** comme type de configuration.



 ©2026 Palo Alto Networks, Inc.

3. Configurez les paramètres **General (généraux)**.

- Saisissez un **Name (Nom)** pour le profil.
- (Facultatif) Saisissez une brève **description** du profil qui indique son but.
- (Facultatif) Définissez le mode de **Deployment (Déploiement)** sur **Managed (Géré)** pour permettre la suppression automatique du profil lors de la désinscription.
- (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les points de terminaison. Sélectionnez **Auto** pour déployer automatiquement le profil sur tous les points de terminaison, **Optional (Optionnel)** pour permettre à l'utilisateur final d'installer le profil à partir du portail SSP (portail libre-service) ou de déployer manuellement le profil sur des points de terminaison individuels, ou **Compliance (Conformité)** pour déployer le profil lorsqu'un utilisateur final enfreint une politique de conformité applicable au point de terminaison.
- (Facultatif) Dans le champ **Managed By (Géré par)**, saisissez le groupe de l'entreprise ayant un accès administratif au profil.
- (Facultatif) Dans le champ **Assigned Groups (Groupes affectés)**, ajoutez les Groupes intelligents auxquels vous souhaitez ajouter le profil. Ce champ comprend une option permettant la création d'un nouveau groupe intelligent pour lequel vous pouvez configurer les spécifications suivantes : exigences minimales en matière de système d'exploitation, modèles de périphérique, catégories de propriété, groupes de l'entreprise, parmi tant d'autres.
- (Facultatif) Indiquez si vous souhaitez ajouter des **Exclusions** à l'affectation de ce profil. Si vous sélectionnez **Yes (Oui)**, le champ **Excluded Groups (Groupes exclus)** s'affiche, vous permettant de sélectionner les groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.

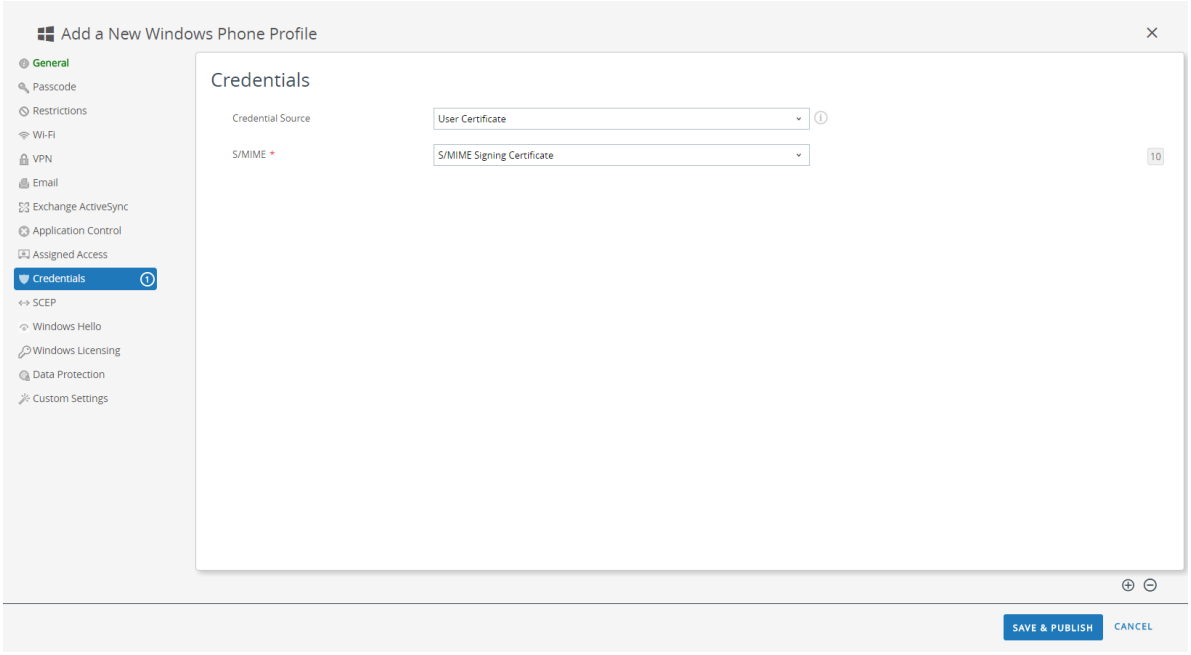


 ©2026 Palo Alto Networks, Inc.

4. Configurez les paramètres de **Credentials (Informations d'identification)** :

   Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

- Pour extraire les certificats de client des utilisateurs Workspace ONE :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).



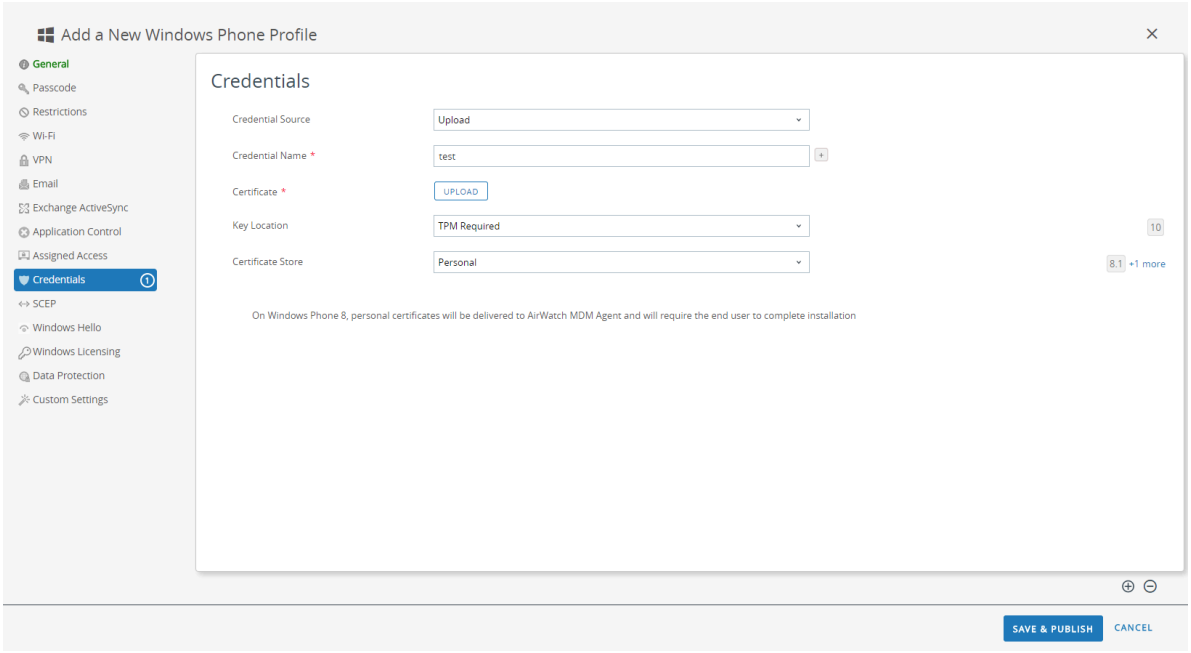
- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.
  5. Sélectionnez le **Key Location (Emplacement clé)** où vous voulez stocker la clé privée du certificat :
     - **TPM Required (TPM requis)** : stockez la clé privée sur un Module de plateforme de confiance. Si aucun module de plateforme de confiance n'est disponible sur le point de terminaison, la clé privée ne peut être installée.
     - **TPM si présent** : stockez la clé privée sur un module de plateforme de confiance s'il y en a un disponible sur le point de terminaison. Si aucun module de plateforme de

 ©2026 Palo Alto Networks, Inc.

confiance n'est disponible sur le point de terminaison, la clé privée est stockée dans le logiciel du point de terminaison.

- **Software (Logiciel)** : stocke la clé privée dans le logiciel du point de terminaison.
- **Passport (Passeport)** : enregistre la clé privée dans Microsoft Passport. Pour utiliser cette option, la protection de l'agent Workspace ONE doit être installé sur le terminal.

6. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.



- Pour utiliser une autorité de certification et un modèle prédéfinis :

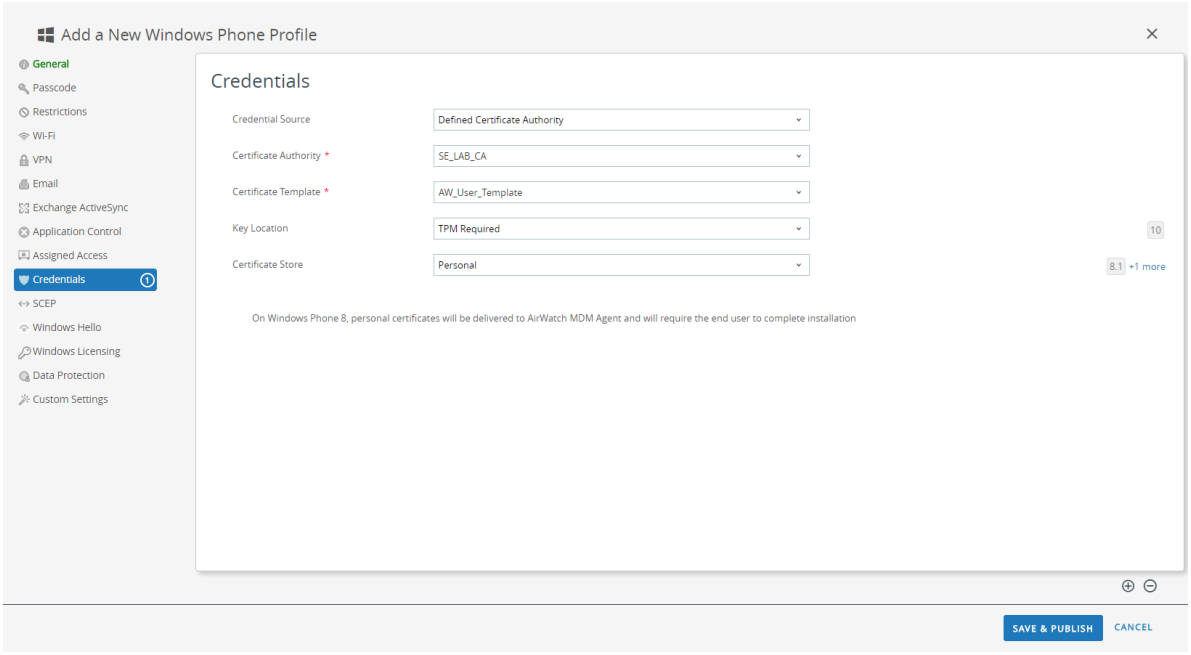
1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
2. Sélectionnez la **Certificate Authority (Autorité de certification)** de laquelle vous souhaitez obtenir les certificats.
3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.
4. Sélectionnez le **Key Location (Emplacement clé)** où vous voulez stocker la clé privée du certificat :
   - **TPM Required (TPM requis)** : stockez la clé privée sur un Module de plateforme de confiance. Si aucun module de plateforme de confiance n'est disponible sur le point de terminaison, la clé privée ne peut être installée.
   - **TPM si présent** : stockez la clé privée sur un module de plateforme de confiance s'il y en a un disponible sur le point de terminaison. Si aucun module de plateforme de

 ©2026 Palo Alto Networks, Inc.

confiance n'est disponible sur le point de terminaison, la clé privée est stockée dans le logiciel du point de terminaison.

- **Software (Logiciel)** : stocke la clé privée dans le logiciel du point de terminaison.
- **Passport (Passeport)** : enregistre la clé privée dans Microsoft Passport. Pour utiliser cette option, la protection de l'agent Workspace ONE doit être installé sur le terminal.

5. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.



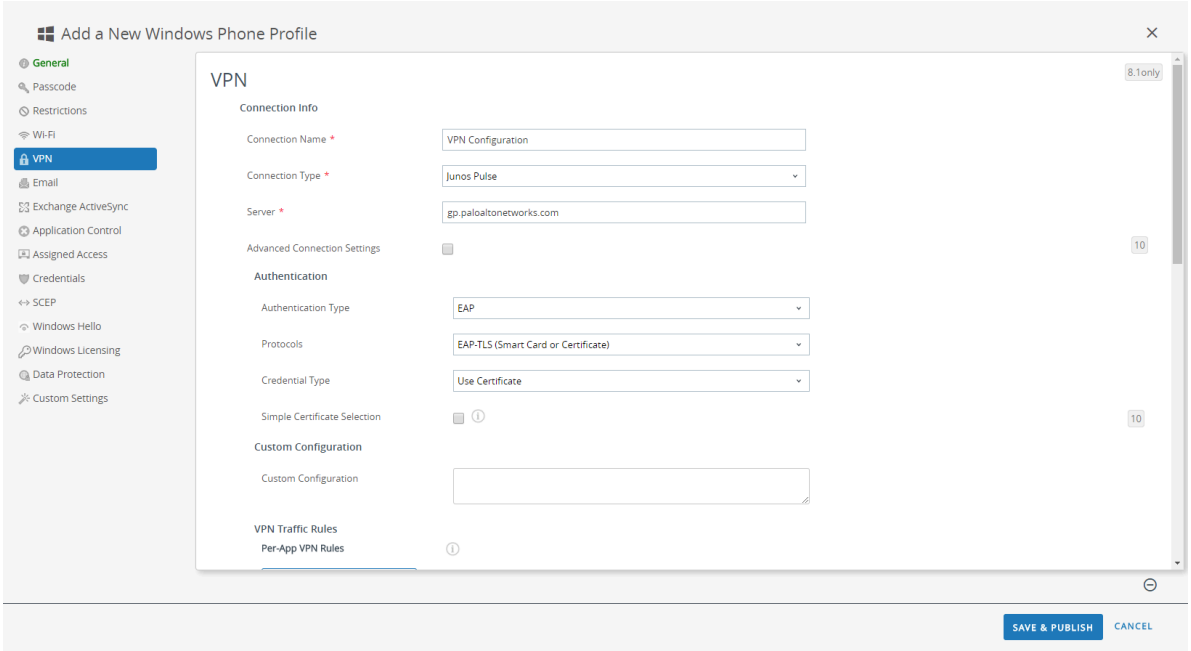
 ©2026 Palo Alto Networks, Inc.

5. Configurez les paramètres **VPN** :

   1. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
   2. Sélectionnez un autre fournisseur de **Connection Type (Type de connexion)** (ne sélectionnez pas **IKEv2**, **L2TP**, **PPTP** ou **Automatic (Automatique)**, car ceux-ci n'ont pas les paramètres de fournisseur associés requis pour le profil VPN GlobalProtect).

      Vous devez sélectionner un fournisseur de rechange, car Workspace ONE ne répertorie pas encore GlobalProtect en tant que fournisseur de connexions officiel pour les terminaux Windows.
   3. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
   4. Dans la section Authentication (Authentification), sélectionnez un **Authentication Type (Type d'authentication)** basé sur le certificat pour préciser la méthode d'authentification des utilisateurs finaux.

      Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

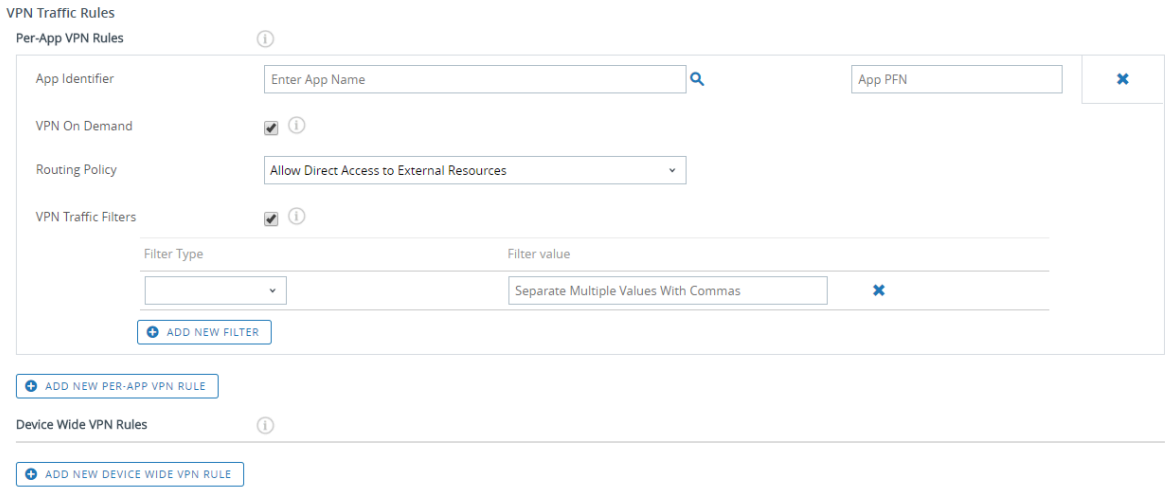
   5. (Facultatif) Pour permettre à GlobalProtect d'enregistrer les informations d'identification de l'utilisateur, **ENABLE (ACTIVEZ)** l'option permettant de **Remember Credentials (Mémoriser les informations)** d'identification dans la zone de stratégies.
   6. Dans la section VPN Traffic Rules (Règles de trafic VPN), **ADD NEW PER-APP VPN RULE (Ajouter une nouvelle règle VPN par App)** pour spécifier les règles applicables aux applications héritées précisées (généralement les fichiers .exe) ou aux applications modernes (généralement téléchargées à partir du Microsoft Store)

      1. (Facultatif) Activez **VPN On Demand (VPN à la demande)** pour permettre à la connexion GlobalProtect de s'établir automatiquement au lancement de l'application.
      2. Sélectionnez une **Routing Policy (Politique d'acheminement)** pour préciser si le trafic de l'application doit être acheminé via le tunnel VPN.

 ©2026 Palo Alto Networks, Inc.

3. (Facultatif) Configurez des **VPN Traffic Filters (Filtres de trafic VPN)** spécifiques pour acheminer le trafic d'application via le VPN uniquement s'il correspond aux critères de correspondance précis que vous définissez, tels que l'adresse IP et le port.

   Ajouter les critères de correspondance en cliquant sur **ADD NEW FILTER (Ajouter un nouveau filtre)**. Lorsque vous êtes invité à le faire, saisissez un **Filter Name (Nom de filtre)** et la **Filter Value (Valeur de filtre)** correspondante.



6. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

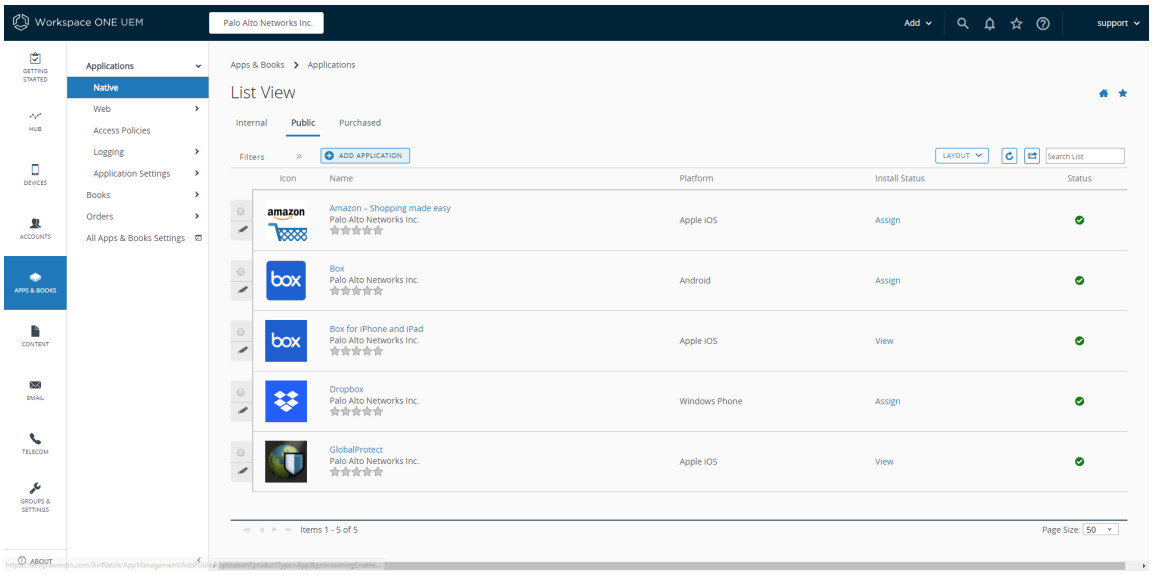
7. Configurez les paramètres VPN par application pour une nouvelle application gérée, ou modifiez les paramètres d'une application gérée existante.

Après avoir configuré les paramètres de l'application et activé le VPN par application, vous pouvez publier l'application à un groupe d'utilisateurs et autoriser l'application à acheminer le trafic via le tunnel VPN GlobalProtect.

1. Sélectionnez **APPS & BOOKS (Applications et livres)** > **Applications** > **Native (Natives)** > **Public (Public)**.
2. Pour ajouter une nouvelle application, sélectionnez **ADD APPLICATION (Ajouter une application)**. Pour modifier les paramètres d'une application existante, recherchez

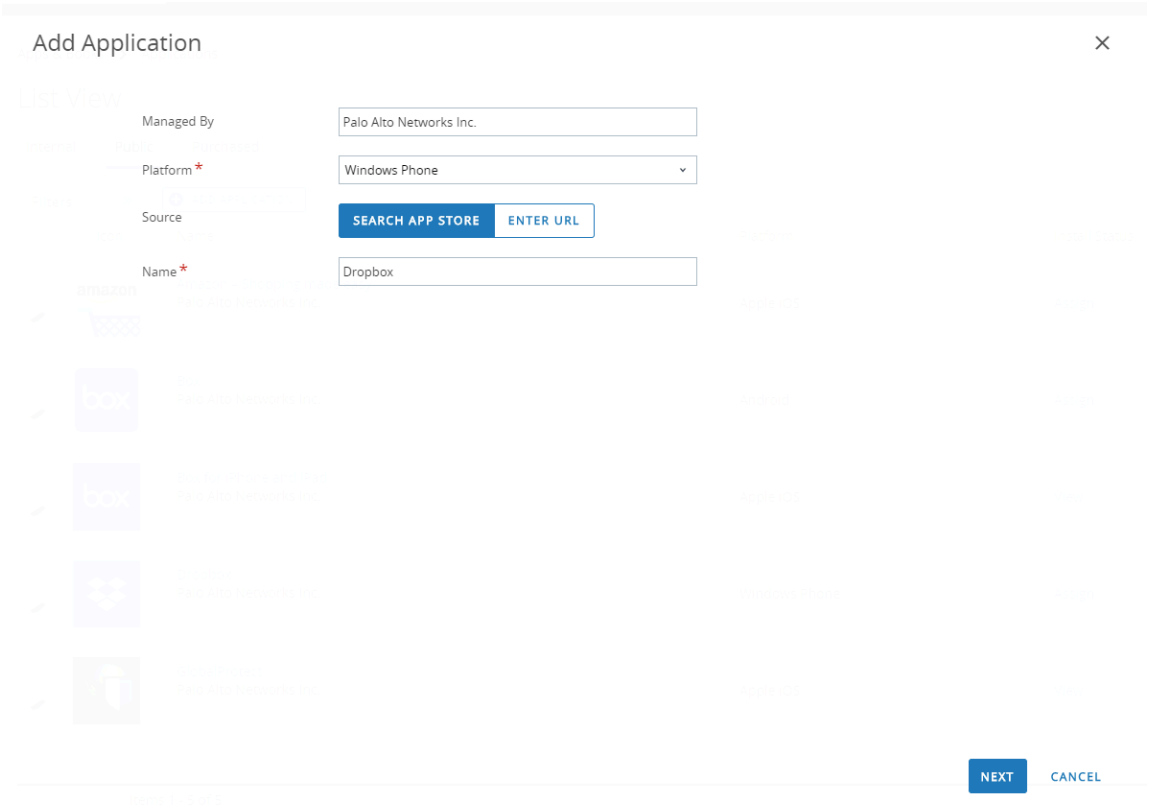
 ©2026 Palo Alto Networks, Inc.

l'application dans la liste des applications publiques, puis sélectionnez l'icône Modifier (✎) dans le menu d'action qui se trouve à côté de la rangée.



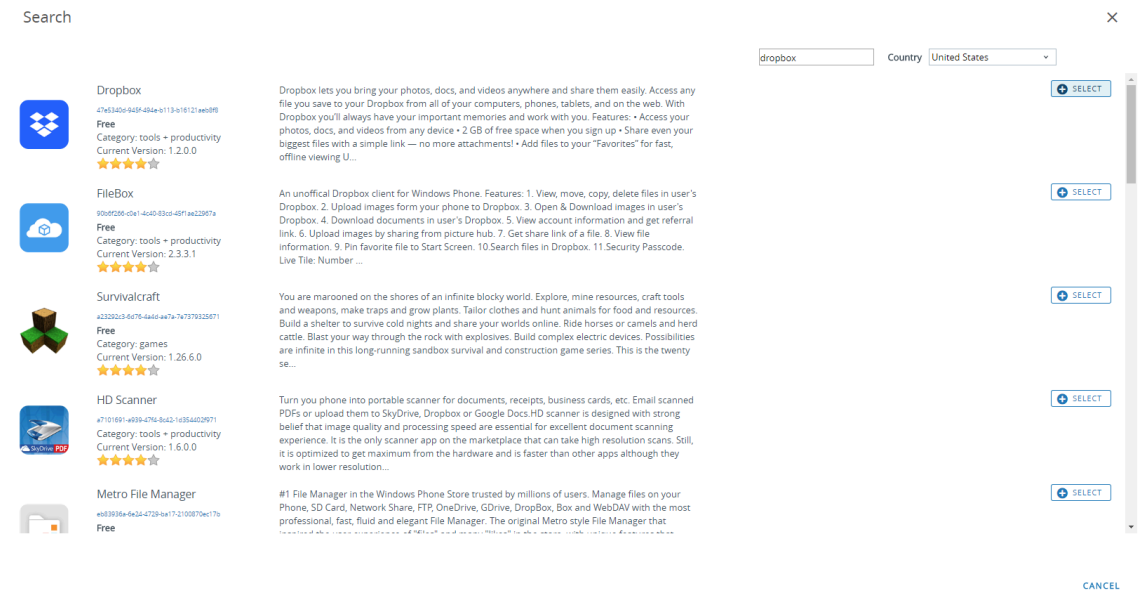
3. Dans le champ **Managed By (Géré par)**, sélectionnez le groupe de l'entreprise qui gérera cette application.
4. Définissez la **Platform (Plateforme)** sur **Windows Phone**.
5. Sélectionnez votre **Source** privilégiée pour trouver l'application :
   - **SEARCH APP STORE (Chercher dans l'App Store)** : saisissez le **Name (Nom)** de l'application.
   - **ENTER URL (SAISIR L'URL)** : saisissez l'URL Microsoft Store de l'application (par exemple, pour chercher l'application Dropbox mobile par URL, saisissez https://www.microsoft.com/en-us/p/dropbox-mobile/9wzdncrfj0pk)

 ©2026 Palo Alto Networks, Inc.



6. Cliquez sur **NEXT (Suivant)**.

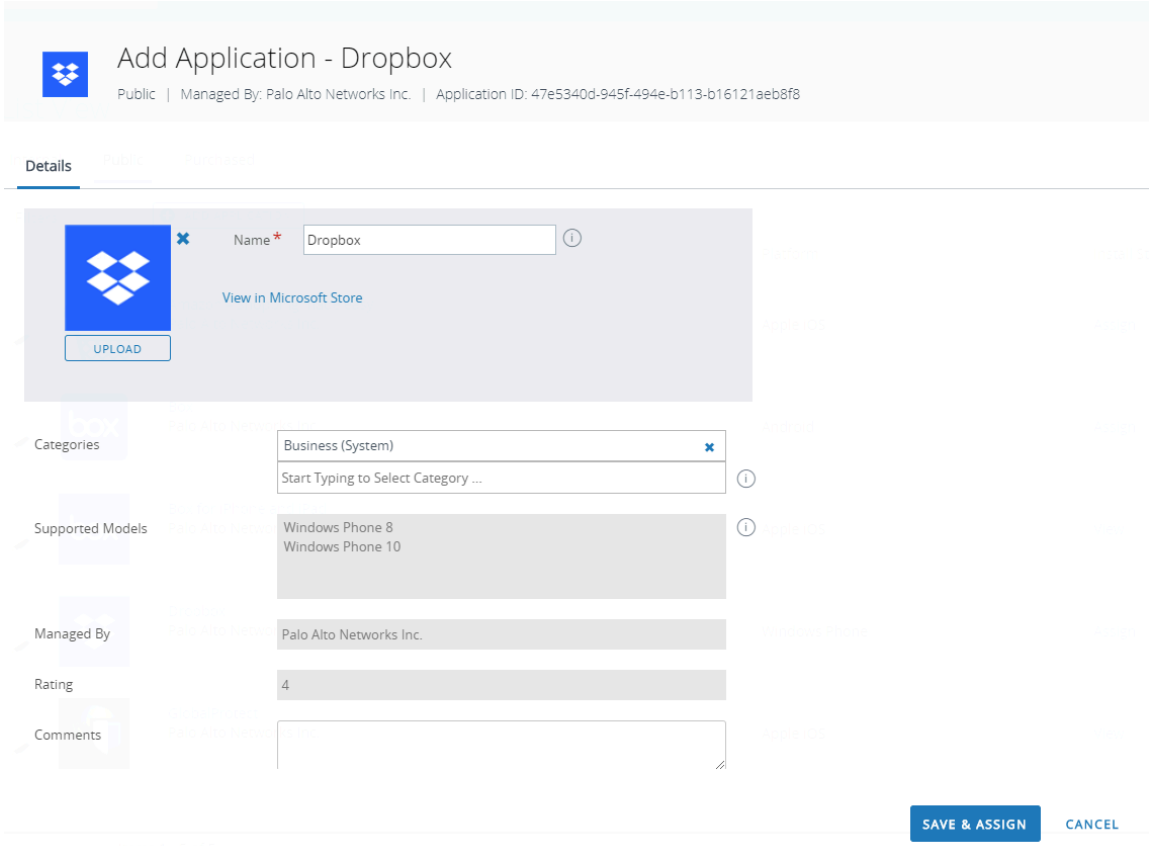
   Si vous choisissez de rechercher l'application dans le Microsoft Store, **SELECT (Sélectionnez)** l'application à partir d'une liste de résultats de recherche.



7. Sur le dialogue Add Application (Ajouter une application), assurez-vous que le **Name (Nom)** de l'application est bon. C'est le nom qui figurera dans le catalogue d'applications de Workspace ONE.

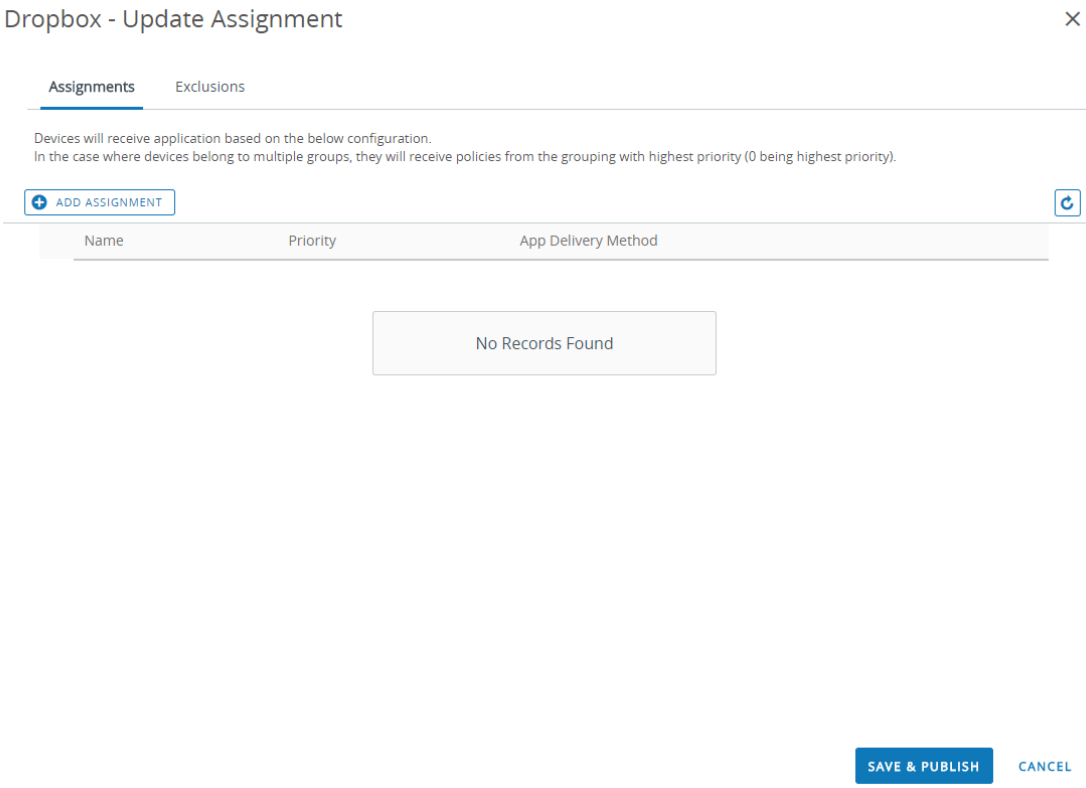
 ©2026 Palo Alto Networks, Inc.

8. (Facultatif) Affectez l'application à des **Categories (Catégories)** prédéfinies ou personnalisées pour faciliter l'accès dans le catalogue d'applications de Workspace ONE.



9. **SAVE & ASSIGN (Enregistrez et affectez)** la nouvelle application.
10. Dans la boîte de dialogue Update Assignment (Mise à jour de l'affectation), sélectionnez **Assignments (Affectations)**, puis cliquez sur **ADD ASSIGNMENT (Ajouter l'affectation)** pour ajouter les groupes intelligents qui auront accès à cette application.

©2026 Palo Alto Networks, Inc.

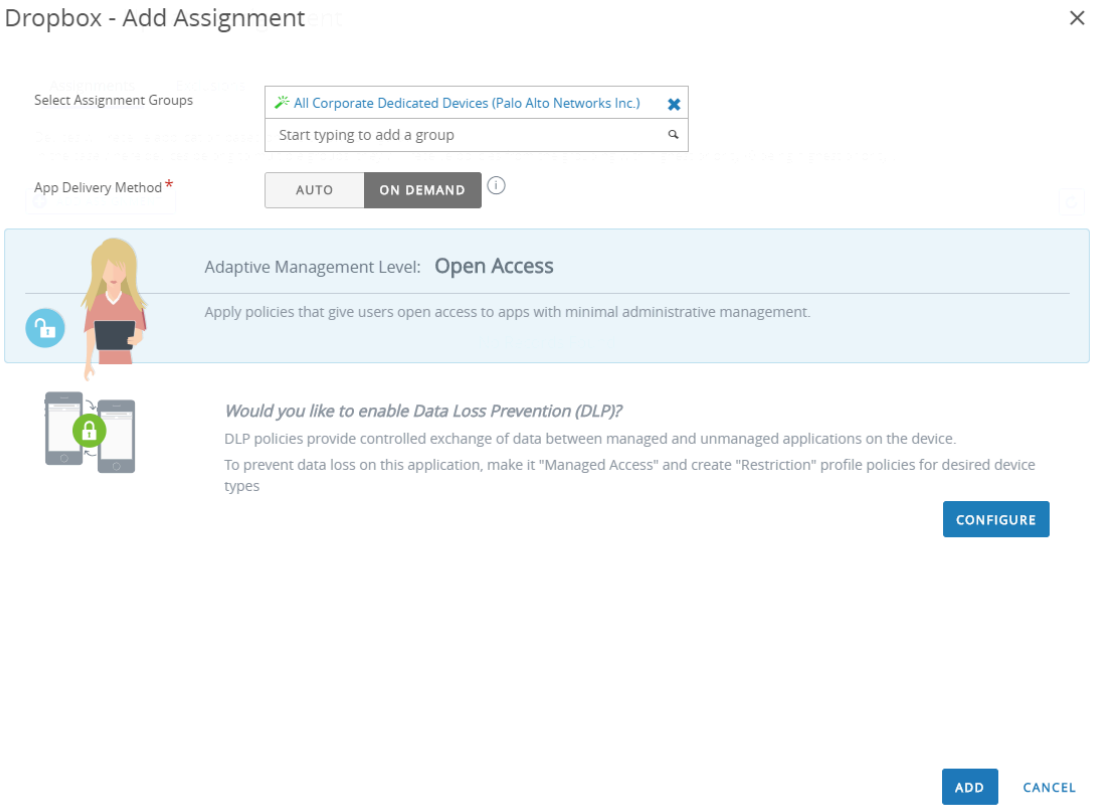


1. Dans le champ **Select Assignment Groups (Sélectionner les groupes d'affectation)**, sélectionnez les groupes intelligents auxquels vous souhaitez accorder l'accès à cette application.
2. Sélectionnez la **App Delivery Method (Méthode de livraison de l'application)**. Si vous sélectionnez **AUTO**, l'application est automatiquement déployée aux

 ©2026 Palo Alto Networks, Inc.

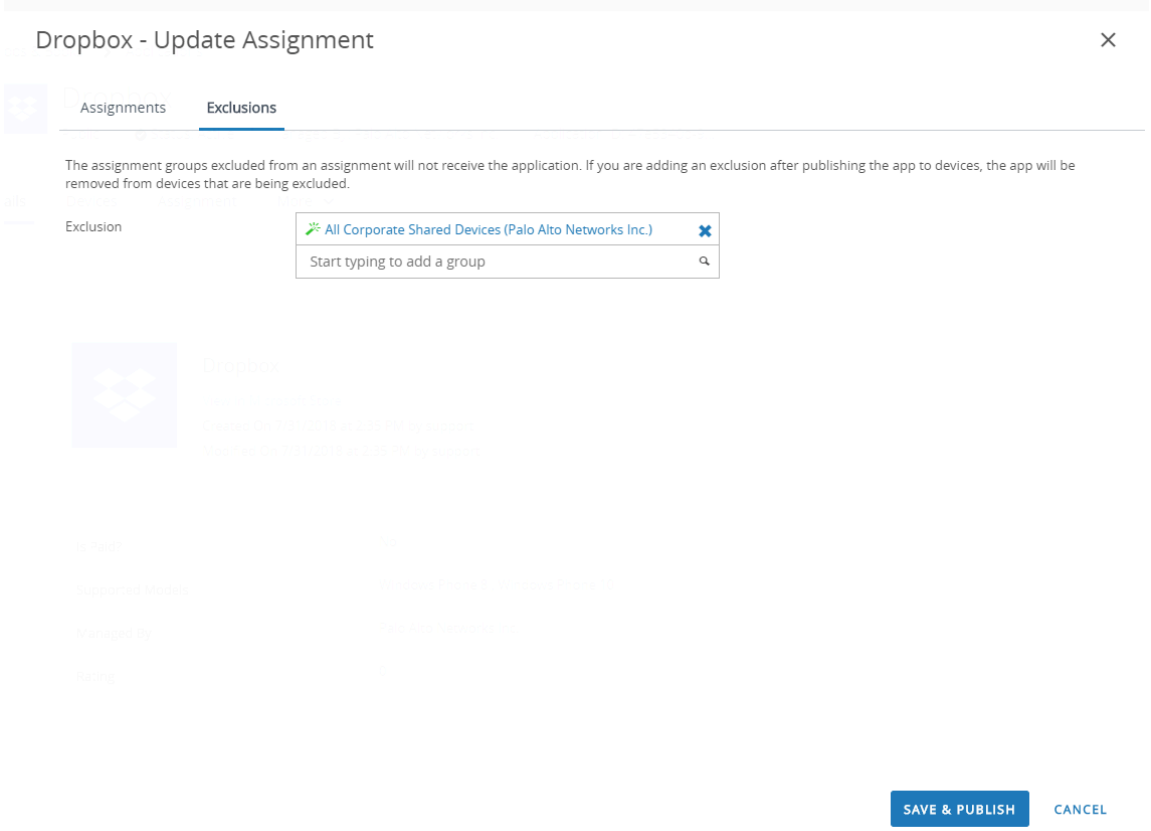
groupes intelligents indiqués. Si vous sélectionnez **ON DEMAND (À LA DEMANDE)**, l'application doit être déployée manuellement.

3. **ADD (Ajoutez)** la nouvelle affectation.



11. (Facultatif) Pour empêcher certains groupes intelligents d'accéder à l'application, sélectionnez **Exclusions**, puis sélectionnez les groupes intelligents que vous souhaitez exclure dans le champ **Exclusion**.

 ©2026 Palo Alto Networks, Inc.



12. **SAVE & PUBLISH (Enregistrez et publiez)** la configuration dans les groupes intelligents affectés.

8. Pour définir le fournisseur de type de connexion dans GlobalProtect, modifiez le profil VPN en XML.

   Pour minimiser les modifications supplémentaires dans le XML brut, examinez les paramètres de votre profil VPN avant d'exporter la configuration. Si vous avez besoin de modifier un paramètre après l'exportation du profil VPN, vous pouvez effectuer les modifications dans le XML brut ou, vous pouvez mettre à jour le paramètre dans le profil VPN et effectuer cette étape à nouveau.

   1. Dans **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue de la liste)**, sélectionnez le bouton d'option qui se trouve à côté du nouveau profil que vous avez ajouté aux étapes précédentes, puis sélectionnez **</>XML** en haut de la table. Workspace ONE ouvre l'affichage XML du profil.
   2. **Export (Exportez)**le profil, puis ouvrez-le dans un éditeur de texte de votre choix.
   3. Modifiez les paramètres suivants pour GlobalProtect :

- Dans l'élément `LoclURI` qui spécifie le `PluginPackageFamilyName`, modifiez l'élément en :

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

 ©2026 Palo Alto Networks, Inc.

- Dans l'élément `Data` qui suit, changez la valeur en :

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

  1. Enregistrez vos modifications dans le profil exporté.
  2. Retournez à Workspace ONE et sélectionnez **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue liste)**.
  3. Créez (sélectionnez **Add (Ajouter)** > **Add Profile (Ajouter un profil)** > **Windows (Windows)** > **Windows Phone (Windows Phone)**) et nommez un nouveau profil.
  4. Sélectionnez **Custom Settings (Paramètres personnalisés)** > **Configure (Configurer)**, puis copiez et collez la configuration modifiée.
  5. **Save & Publish (Enregistrez et publiez)** vos modifications.

9. Nettoyez le profil original en sélectionnant le sélectionnant à partir de **Devices (Périphériques)** > **Profiles (Profils)** > **List View (Vue de la liste)**, puis sélectionnez **More Actions (Plus d'actions)** > **Deactivate (Désactiver)**. Workspace ONE déplace le profil sur la liste inactive.

10. Testez la configuration.

Configurer Workspace ONE pour les terminaux Android

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

L'application GlobalProtect peut être déployée et configurée à l'aide de Workspace ONE pour fournir aux terminaux mobiles gérés un accès sécurisé aux ressources internes de l'entreprise. Cette intégration prend en charge la configuration de politiques VPN par application, qui contrôlent de manière granulaire le comportement de tunneling. Lorsqu'une politique par application est active, seul le trafic des applications gérées explicitement définies est envoyé à travers le tunnel VPN GlobalProtect. Tout autre trafic provenant d'applications non gérées se connecte directement à Internet, contournant le tunnel sécurisé.

Reportez-vous aux sections suivantes pour des informations sur la façon de configurer des paramètres VPN pour les terminaux Android en utilisant Workspace ONE :

- Configurer une configuration de VPN par application sur les terminaux Android à l'aide de Workspace ONE

 ©2026 Palo Alto Networks, Inc.

Configurer une configuration de VPN par application sur les terminaux Android à l'aide de Workspace ONE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez autoriser l'accès aux ressources internes à partir de vos périphériques mobiles gérés en configurant l'accès VPN GlobalProtect à l'aide de Workspace ONE. Dans une configuration VPN par application, vous pouvez indiquer les applications gérées qui peuvent acheminer le trafic via le tunnel VPN GlobalProtect. Les applications non gérées continueront de se connecter directement par l'Internet plutôt que via le tunnel VPN GlobalProtect.

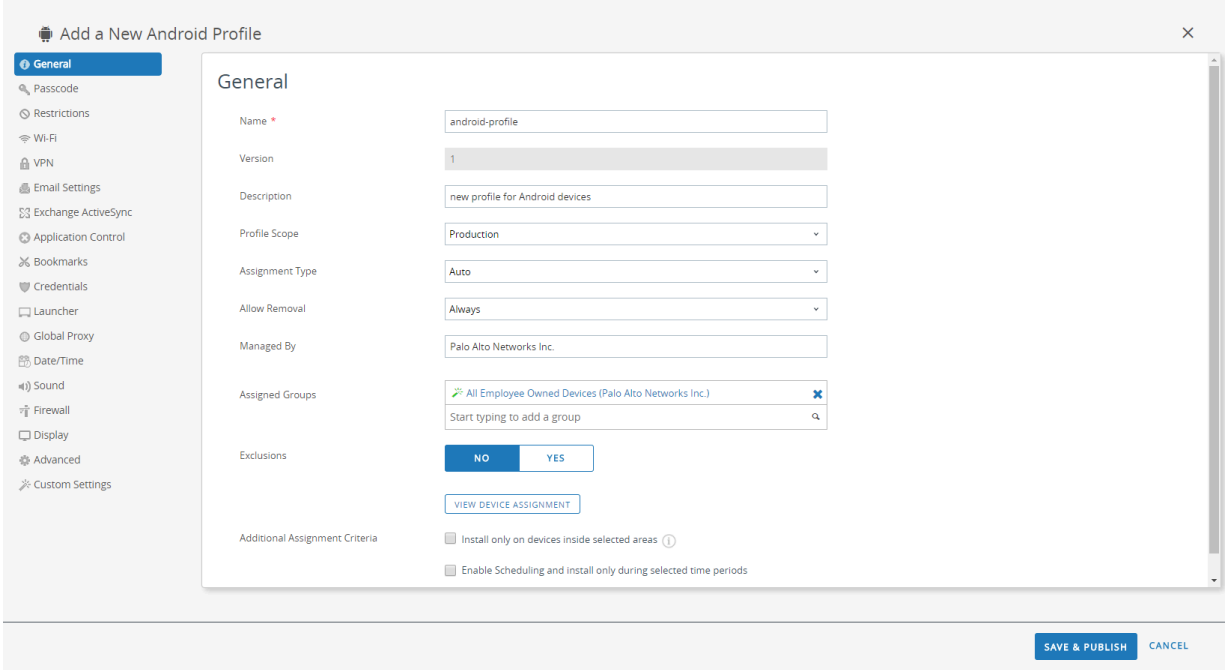
Utilisez les étapes suivantes pour configurer une configuration par application sur les terminaux Android à l'aide de Workspace ONE :

1. Téléchargement de l'application GlobalProtect pour Android :
   - Déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   - Téléchargez l'app GlobalProtect directement à partir de Google Play.
2. Depuis la console Workspace ONE, modifiez un profil Android existant ou ajoutez-en un nouveau.
   1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajouter)** un nouveau profil.
   2. Sélectionnez **Android (Legacy) (Android (hérité)** de la liste de la plateforme.
3. Configurez les paramètres **General (généraux)**.
   1. Saisissez un **Name (Nom)** pour le profil.
   2. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
   3. (Facultatif) Sélectionnez la **Profile Scope (Portée du profil)**, soit **Production, Staging (Pré-production)** ou **Both (les deux)**.
   4. (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les points de terminaison. Sélectionnez **Auto** pour déployer automatiquement le profil sur tous les points de terminaison, **Optional (Optionnel)** pour permettre à l'utilisateur final d'installer le profil à partir du portail SSP (portail libre-service) ou de déployer manuellement le profil sur des points de terminaison individuels, ou **Compliance (Conformité)** pour déployer le profil lorsqu'un utilisateur final enfreint une politique de conformité applicable au point de terminaison.
   5. (Facultatif) Sélectionnez si vous souhaitez **Allow Removal (Autoriser la suppression)** du profil par l'utilisateur final ou non. Sélectionner **Always (Toujours)** pour permettre à l'utilisateur final de supprimer manuellement le profil à tout moment, **Never (Jamais)** pour empêcher l'utilisateur final de supprimer le profil, ou **With Authorization (Avec autorisation)** pour permettre à l'utilisateur final de supprimer le profil avec l'autorisation de

 ©2026 Palo Alto Networks, Inc.

l'administrateur. Lorsque **With Authorization (Avec autorisation)** est sélectionné, un champ Password (Mot de passe) qui doit obligatoirement être renseigné s'ajoute.

6. (Facultatif) Dans le champ **Managed By (Géré par)**, saisissez le groupe de l'entreprise ayant un accès administratif au profil.
7. (Facultatif) Dans le champ **Assigned Groups (Groupes affectés)**, ajoutez les Groupes intelligents auxquels vous souhaitez ajouter le profil. Ce champ comprend une option permettant la création d'un nouveau groupe intelligent pour lequel vous pouvez configurer les spécifications suivantes : exigences minimales en matière de système d'exploitation, modèles de périphérique, catégories de propriété, groupes de l'entreprise, parmi tant d'autres.
8. (Facultatif) Indiquez si vous souhaitez ajouter des **Exclusions** à l'affectation de ce profil. Si vous sélectionnez **Yes (Oui)**, le champ **Excluded Groups (Groupes exclus)** s'affiche, vous permettant de sélectionner les groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.

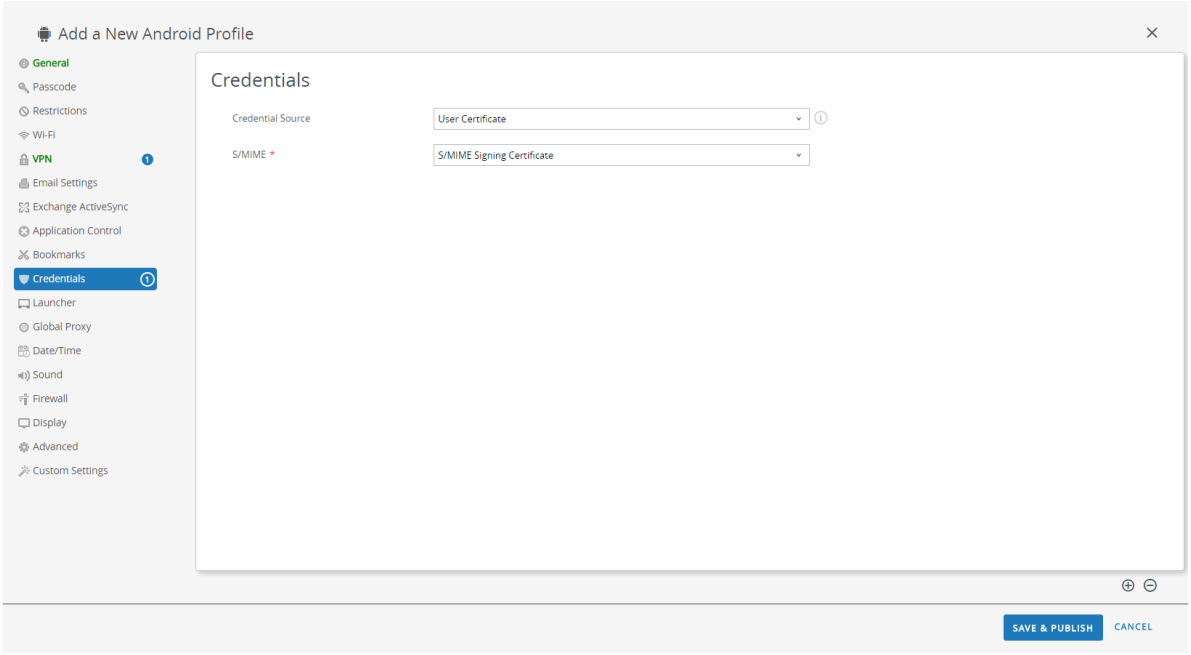


 ©2026 Palo Alto Networks, Inc.

4. Configurez les paramètres de **Credentials (Informations d'identification)** :

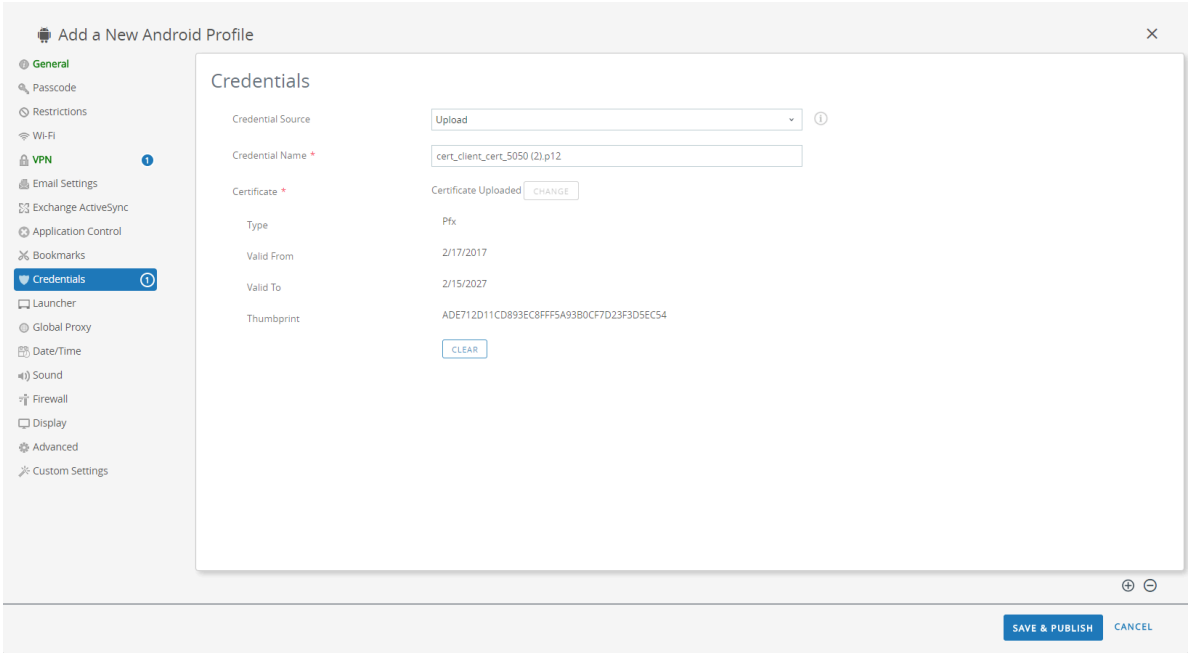
   Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

- Pour extraire les certificats de client des utilisateurs Workspace ONE :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).

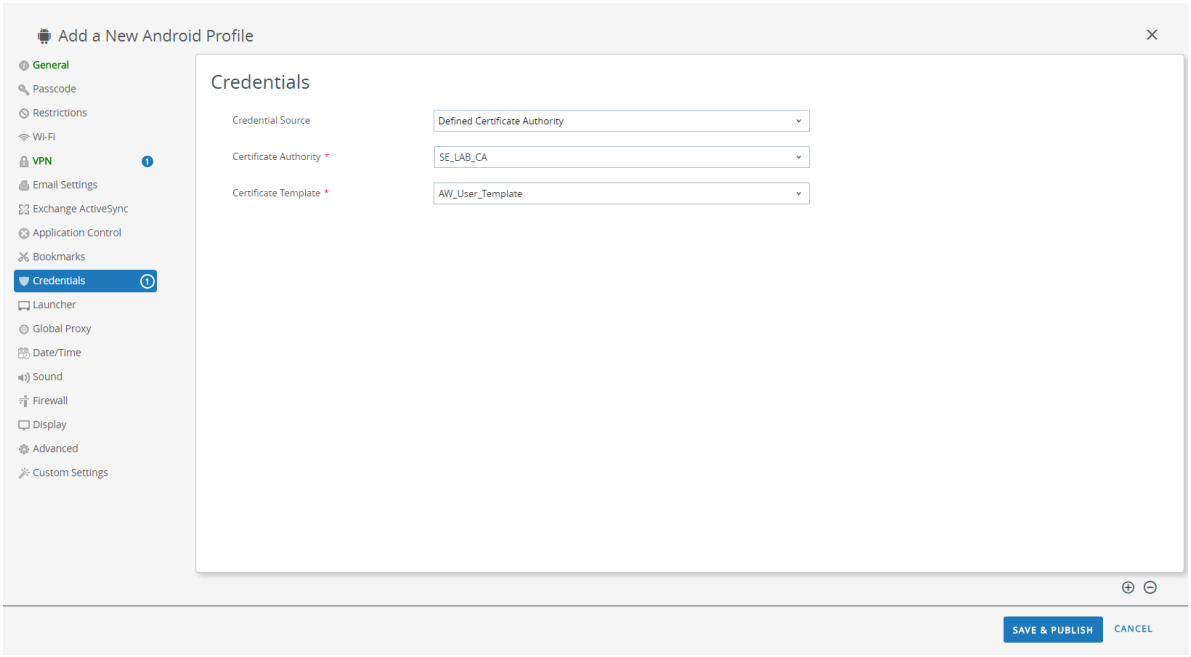


- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.

 ©2026 Palo Alto Networks, Inc.



- Pour utiliser une autorité de certification et un modèle prédéfinis :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
  2. Sélectionnez la **Certificate Authority (Autorité de certification)** de laquelle vous souhaitez obtenir les certificats.
  3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.

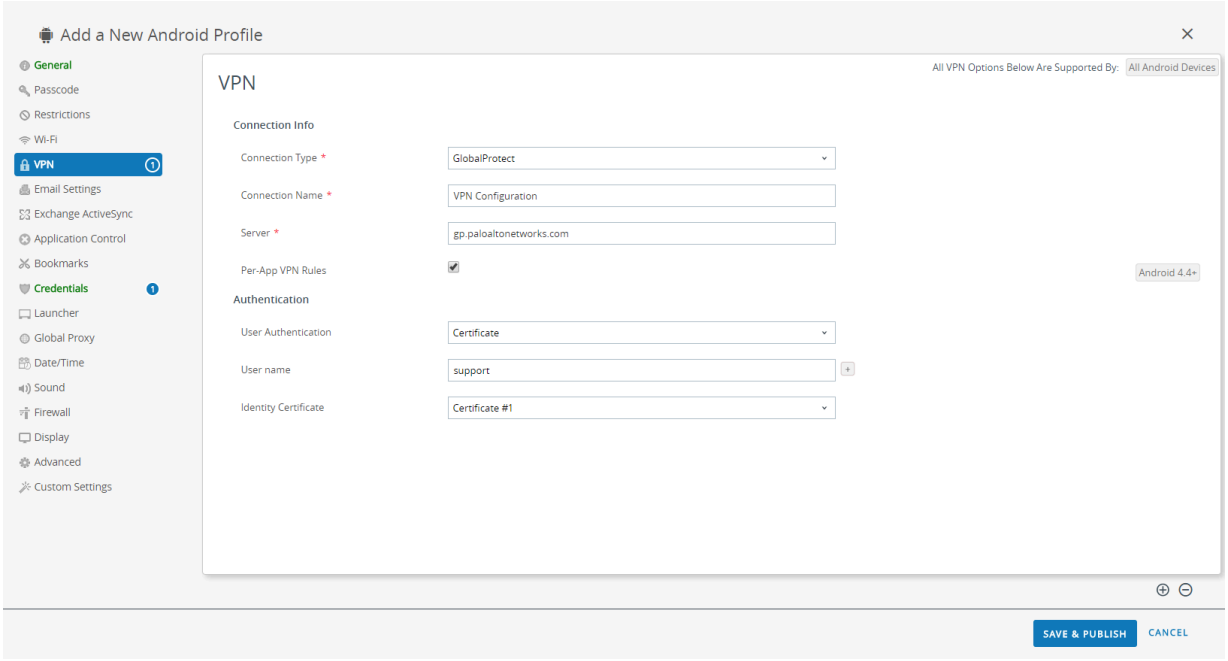


 ©2026 Palo Alto Networks, Inc.

5. Configurez les paramètres **VPN** :

1. Définissez le **Connection type (Type de connexion)** du réseau sur **GlobalProtect**.
2. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
3. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
4. Autorisez les **Per App VPN Rules (Règles VPN par application)** à acheminer tout le trafic des applications gérées via le tunnel VPN GlobalProtect.
5. Dans la section Authentication (Authentification), définissez la méthode de **User Authentication (Authentification de l'utilisateur)** sur **Certificate (Certificat)**.

   Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.
6. Saisisissez le **User name** (Nom d'utilisateur) du compte VPN ou cliquez sur le bouton d'ajout (+) pour afficher les valeurs de recherche prises en charge que vous pouvez insérer.
7. Lorsque vous êtes invité à le faire, sélectionnez le **Identity Certificate (Certificat d'identité)** que GlobalProtect utilisera pour authentifier les utilisateurs. Le **Identity Certificate (Certificat d'identité)** est le même certificat que vous avez configuré dans les paramètres de **Credentials (Informations d'identification)**.



6. **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

©2026 Palo Alto Networks, Inc.

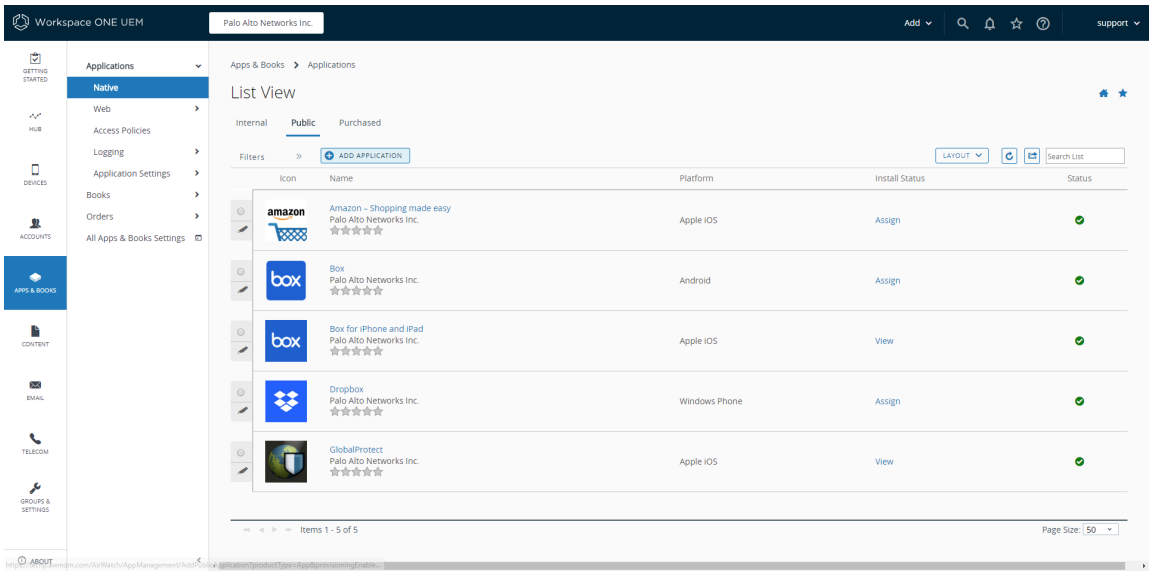
7. Configurez les paramètres VPN par application pour une nouvelle application gérée, ou modifiez les paramètres d'une application gérée existante.

   Après avoir configuré les paramètres de l'application et activé le VPN par application, vous pouvez publier l'application à un groupe d'utilisateurs et autoriser l'application à acheminer le trafic via le tunnel VPN GlobalProtect.

   1. Sélectionnez **APPS & BOOKS (Applications et livres)** > **Applications** > **Native (Natives)** > **Public (Public)**.
   2. Pour ajouter une nouvelle application, sélectionnez **ADD APPLICATION (Ajouter une application)**. Pour modifier les paramètres d'une application existante, recherchez

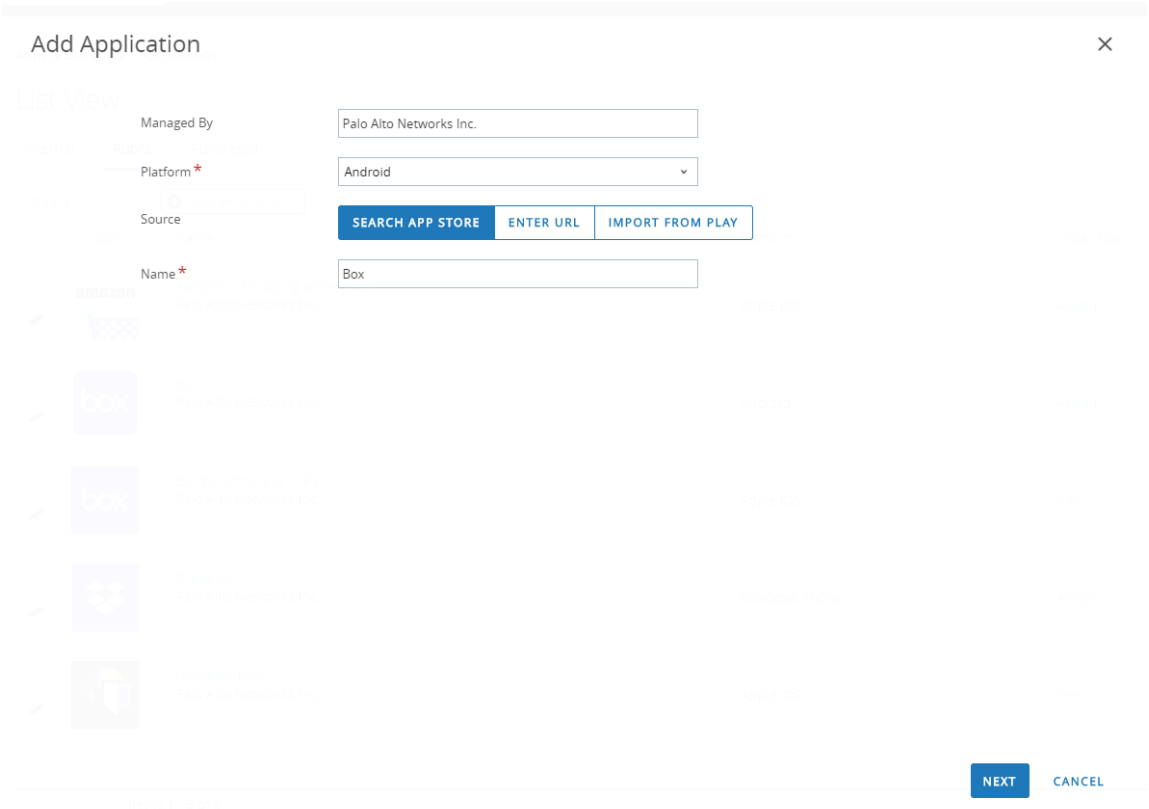
 ©2026 Palo Alto Networks, Inc.

l'application dans la liste des applications publiques (List View), puis sélectionnez l'icône Modifier (✎) dans le menu d'action qui se trouve à côté de la rangée.



3. Dans le champ **Managed By (Géré par)**, sélectionnez le groupe de l'entreprise qui gérera cette application.
4. Définissez la **Platform (Plateforme)** sur **Android**.
5. Sélectionnez votre **Source** privilégiée pour trouver l'application :
   - **SEARCH APP STORE (Chercher dans l'App Store)** : saisissez le **Name (Nom)** de l'application.
   - **ENTER URL (SAISIR L'URL)** : saisissez l'URL Google Play de l'application (par exemple, pour chercher l'application Box par URL, saisissez https://play.google.com/store/apps/details?id=com.box.android).
   - **IMPORT FROM PLAY (Importer de Play)** : Importez une application de la liste des applications approuvées de l'entreprise à partir de Google Play.

 ©2026 Palo Alto Networks, Inc.

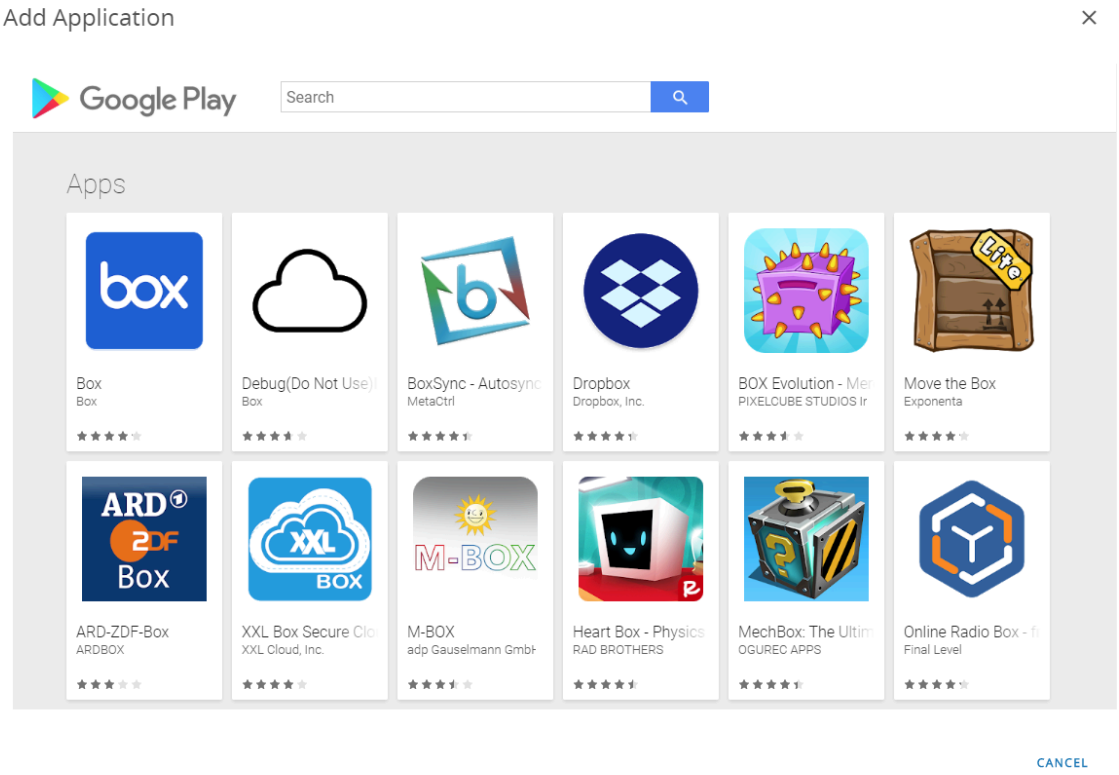


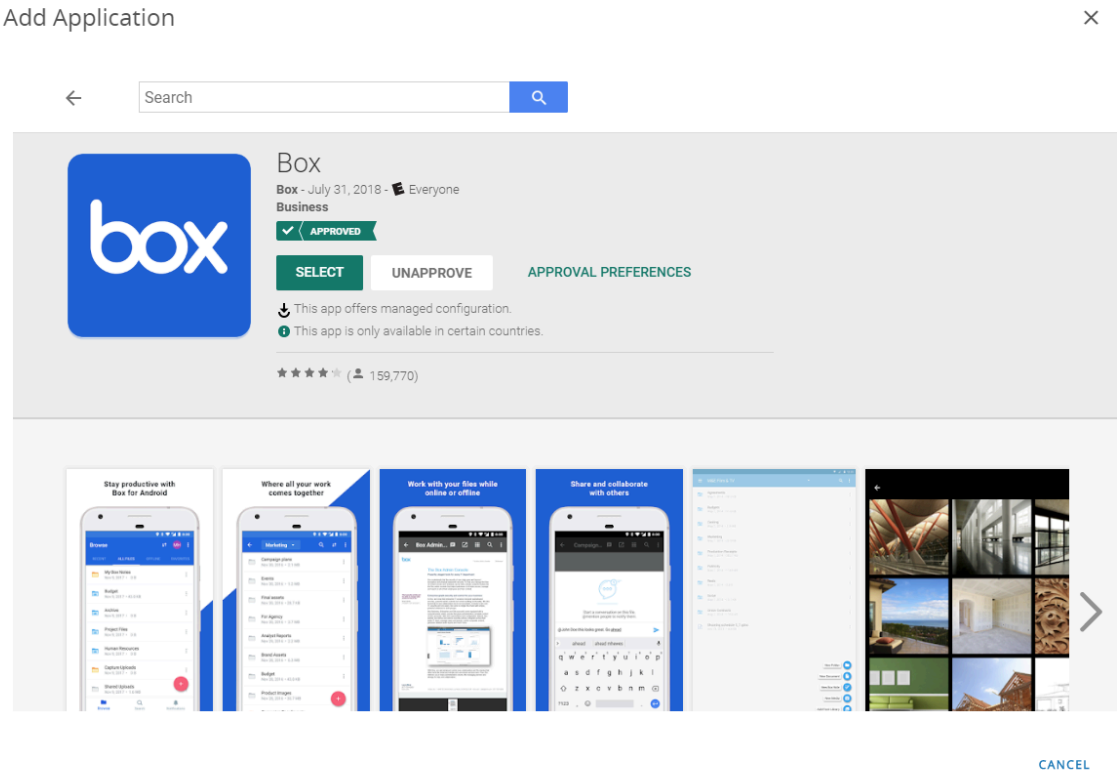
6. Cliquez sur **NEXT (Suivant)**.

   Si vous décidez d'effectuer une recherche dans Google Play, cliquez sur l'icône de l'application dans la liste des résultats de la recherche. Si l'application n'a pas encore été

 ©2026 Palo Alto Networks, Inc.

approuvée pour votre entreprise, vous devez **APPROVE (Approuver)** l'application. Une fois l'application approuvée, **SELECT (Sélectionnez)**-la.



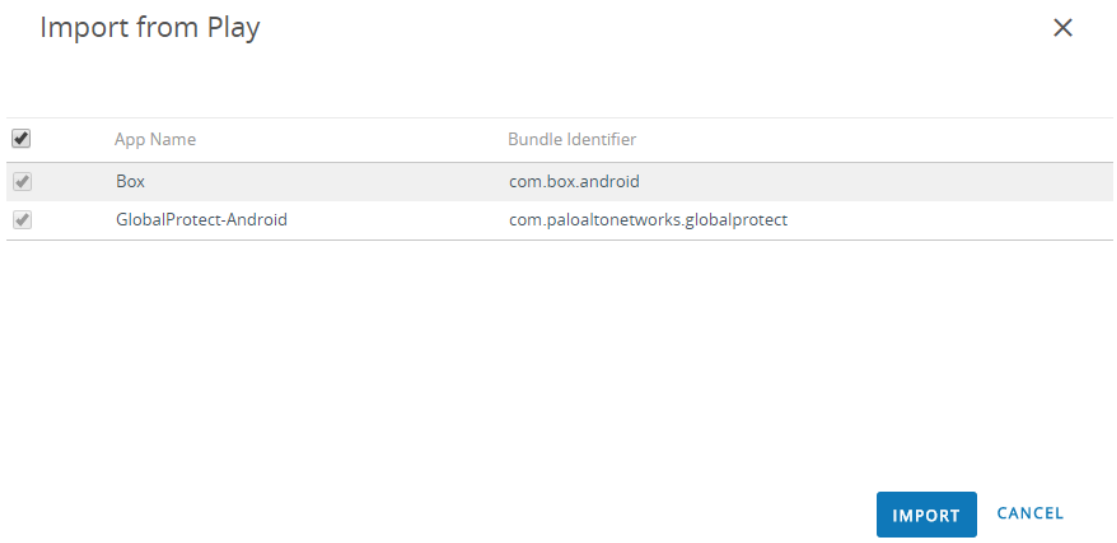


 ©2026 Palo Alto Networks, Inc.

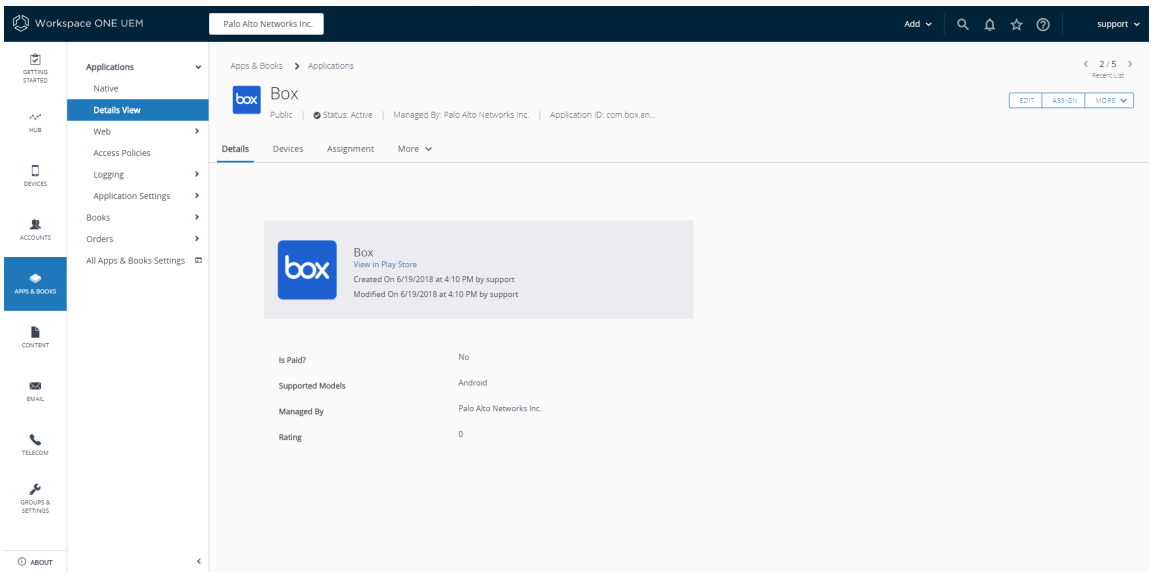
Si vous décidez d’importer l’application à partir de Google Play, sélectionnez l'application dans la liste des applications approuvées de l'entreprise, puis cliquez sur **IMPORT**

 ©2026 Palo Alto Networks, Inc.

(Importer). Si vous ne voyez pas l'application dans la liste, communiquez avec votre administrateur Android for Work pour qu'il approuve l'application.



7. Sélectionnez l'application nouvellement ajoutée dans la liste des applications publiques (List View).
8. Dans **Applications (Applications)** > **Details View (Affichage des détails)**, cliquez sur **ASSIGN (AFFECTER)** dans le coin supérieur droit de l'écran.

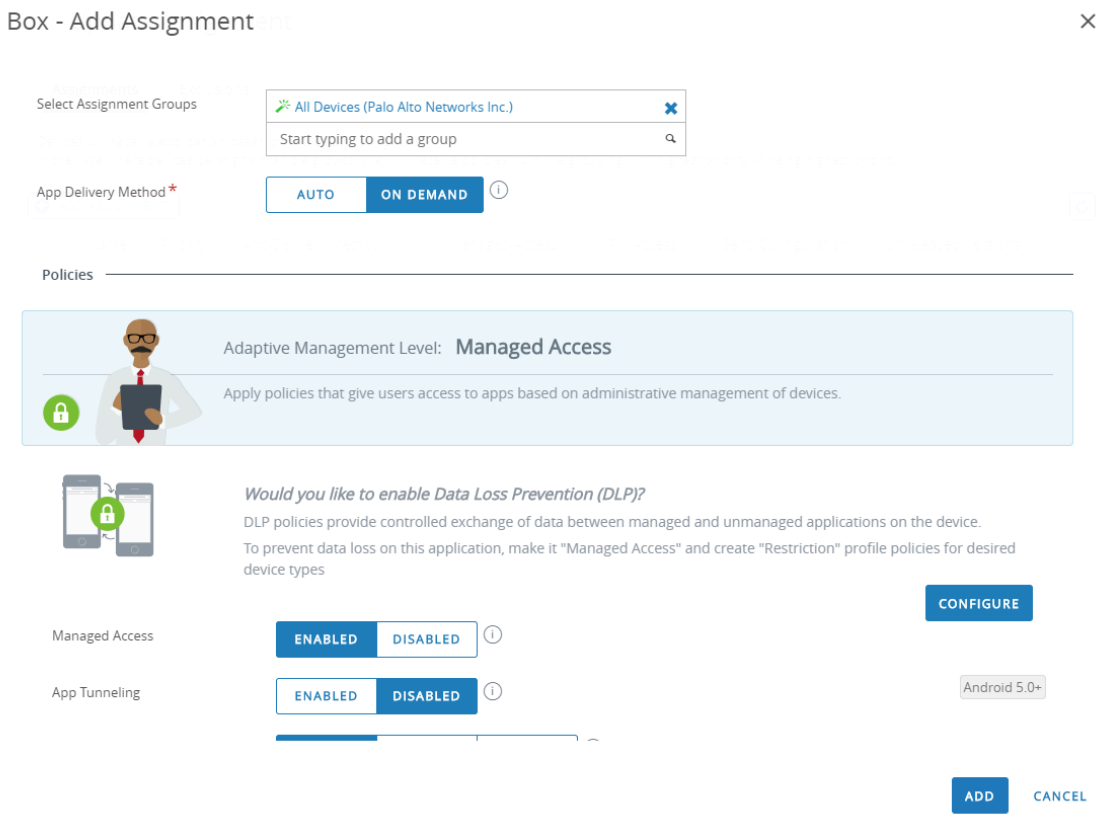


9. Sélectionnez **Assignments (Affectations)**, puis cliquez sur **ADD ASSIGNMENT (Ajouter l'affectation)** pour ajouter les groupes intelligents qui auront accès à cette application.
   1. Dans le champ **Select Assignment Groups (Sélectionner les groupes d'affectation)**, sélectionnez les groupes intelligents auxquels vous souhaitez accorder l'accès à cette application.
   2. Sélectionnez la **App Delivery Method (Méthode de livraison de l'application)**. Si vous sélectionnez **AUTO**, l'application est automatiquement déployée aux

 ©2026 Palo Alto Networks, Inc.

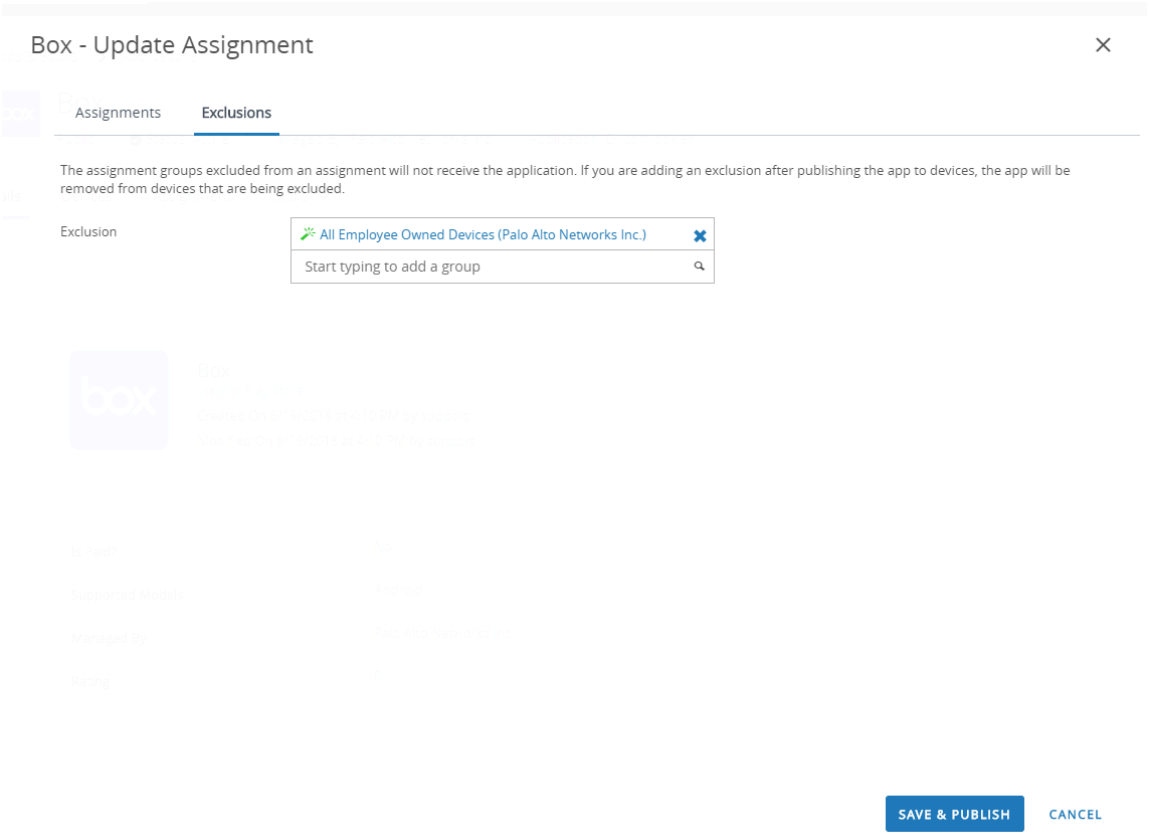
groupes intelligents indiqués. Si vous sélectionnez **ON DEMAND (À LA DEMANDE)**, l'application doit être déployée manuellement.

3. Définissez l'option **Managed Access (Accès géré)** sur **ENABLED (ACTIVÉ)**. Cette option donne aux utilisateurs un accès à l'application en fonction des politiques de gestion que vous appliquez.
4. Configurez les paramètres restants, au besoin.
5. **ADD (Ajoutez)** la nouvelle affectation.



10. (Facultatif) Pour empêcher certains groupes intelligents d'accéder à l'application, sélectionnez **Exclusions**, puis sélectionnez les groupes intelligents que vous souhaitez exclure dans le champ **Exclusion**.

 ©2026 Palo Alto Networks, Inc.



11. **SAVE & PUBLISH (Enregistrez et publiez)** la configuration dans les groupes intelligents affectés.

Activer l'intégration de l'analyse d'application avec WildFire

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

En activant App Scan dans Workspace ONE, vous pouvez tirer parti de l'intelligence de menaces WildFire® sur les applications pour détecter les logiciels malveillants sur les terminaux Android. Lorsqu'il est activé, l'agent Workspace ONE envoie la liste des applications qui sont installées sur le terminal Android vers Workspace ONE. Cela se produit lors de l'inscription et par la suite sur tout enregistrement de point de terminaison. Workspace ONE interroge périodiquement WildFire pour les verdicts et peut prendre des mesures de conformité sur le terminal en fonction du verdict.

1. Avant de commencer, procurez-vous une clé API Wildfire. Si vous n'avez pas déjà une clé API, contactez le support.

 ©2026 Palo Alto Networks, Inc.

2. Dans Workspace ONE, sélectionnez **Groups & Settings (Groupes et paramètres)** > **All Settings (Tous les paramètres)** > **Apps (Applications)** > **App Scan (Application d'analyse)** > **Third Party Integration (Intégration tierce)**.

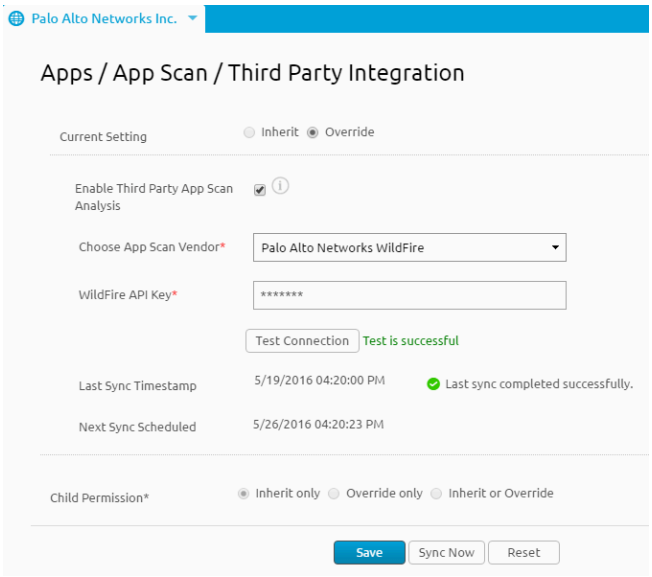
3. Sélectionnez le **Current Setting (réglage actuel)** : Override (Substituer).

4. Sélectionnez **Enable Third Party App Scan Analysis (Activer l'analyse de scan d'une application tierce)** pour permettre la communication entre Workspace ONE et WildFire.

5. Choisissez **Palo Alto Networks WildFire** à partir du menu déroulant **Choose App Scan Vendor (Choisir la recherche d'analyse d'application)**.

6. Saisissez votre clé API Wildfire.

7. Cliquez sur **Test Connection (Tester la connexion)** pour vous assurer que Workspace ONE peut communiquer avec WildFire. Si le test n'est pas réussi, vérifiez la connectivité à Internet, saisissez de nouveau la clé API, puis réessayez.



8. Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications. Workspace ONE planifie une tâche de synchronisation pour communiquer avec WildFire pour obtenir les derniers verdicts pour les hachages d'application et exécute la tâche à intervalles réguliers. Cliquez sur **Sync Now** (Synchroniser maintenant) pour initier une synchronisation manuelle avec WildFire.

Gérer l'application GlobalProtect à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

Microsoft Intune est une plateforme de gestion de mobilité d'entreprise basée sur le nuage qui vous permet de gérer des points d'extrémité mobiles, à partir d'un emplacement central. L'application GlobalProtect fournit une connexion sécurisée pour ces terminaux. L'utilisation de GlobalProtect en tant que connexion sécurisée assure l'homogénéité de l'inspection du trafic et de l'application des règles de sécurité du réseau pour la prévention des menaces.

Si vous n'utilisez pas de système MDM de tiers qualifié, vous pouvez Gérer l'application GlobalProtect à l'aide d'autres MDM tiers.

Configurer l'application GlobalProtect sur les terminaux Android à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect déployé avec Microsoft Intune prend en charge les configurations suivantes :

- Toujours actif

  Dans une configuration toujours active, GlobalProtect se connecte automatiquement dès que vous vous connectez. Pour les appareils configurés avec cette méthode de connexion, vous pouvez activer le mode verrouillage, qui impose à GlobalProtect d'être connecté pour accéder au réseau
- À la demande

  Dans une configuration à la demande, vous devez vous connecter manuellement à GlobalProtect via l'application. Le trafic est acheminé via l'application GlobalProtect uniquement après que vous ayez initié et établi la connexion.
- Par application

  Dans une configuration par application, vous pouvez spécifier les applications gérées qui peuvent acheminer le trafic via GlobalProtect lorsqu'elles sont connectées. Si vous utilisez une liste d'autorisation, seules les applications spécifiées seront acheminées via GlobalProtect. Si vous utilisez une liste de blocage, tout le trafic sera acheminé via GlobalProtect, sauf pour les applications spécifiées.

  Sur les périphériques Android, GlobalProtect ne se connecte pas automatiquement lorsque vous ouvrez des applications configurées avec une liste d'autorisation ou une liste de blocage. Par conséquent, nous recommandons de définir la méthode de connexion toujours active pour les configurations par application.

GlobalProtect fonctionne à la fois avec des périphériques Android avec un profil professionnel et des périphériques Android entièrement gérés.

 ©2026 Palo Alto Networks, Inc.

Configurer l'environnement Microsoft Intune pour les terminaux Android

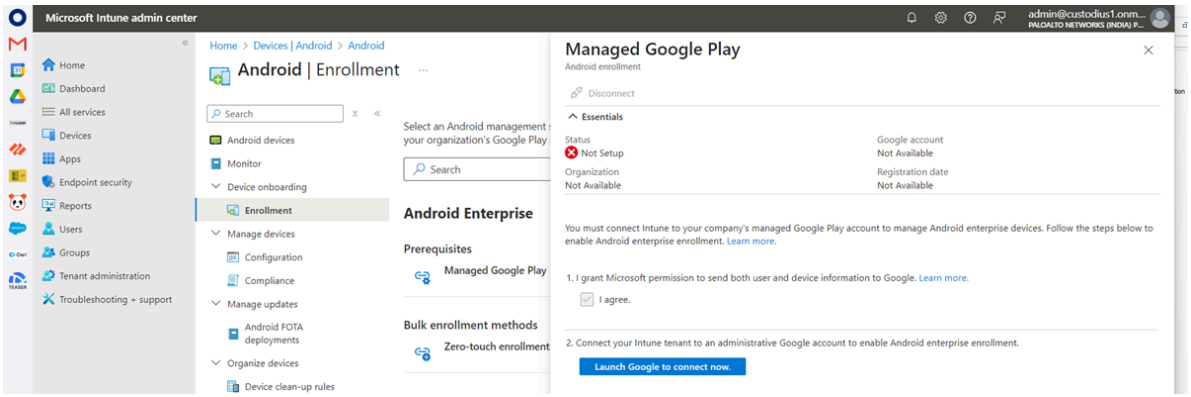
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Au cours de cette étape, vous liez votre compte Google Play géré à Intune, puis créez un profil d'inscription. Si votre périphérique est déjà géré par Intune, passez à Déployer l'application GlobalProtect sur des terminaux Android en utilisant Microsoft Intune.

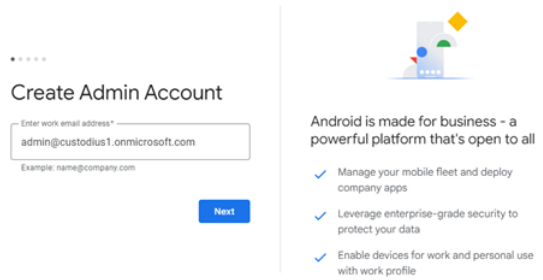
1. Complétez les étapes suivantes pour lier votre compte Google Play géré à Intune.

   Pour une démonstration sur comment lier votre compte Google Play géré à Intune, regardez cette vidéo.

   1. Accédez au Centre d'administration Microsoft Intune à l'adresse **https://intune.microsoft.com** et connectez-vous avec les informations d'identification de l'administrateur pour Intune.
   2. Cliquez sur **Devices (Périphériques)** > **Android** > **Enrollment (Inscription)** > **Prerequisites (Conditions préalables)** > **Managed Google Play (Google Play géré)**, puis cliquez sur **Launch Google to Connect Now (Lancer Google pour se connecter dès maintenant)**.



   3. Inscrivez-vous avec votre adresse e-mail professionnelle.

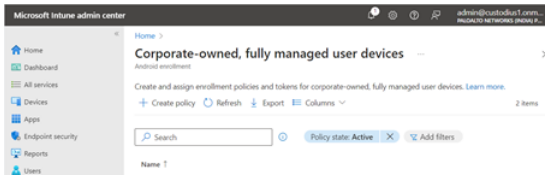


 ©2026 Palo Alto Networks, Inc.

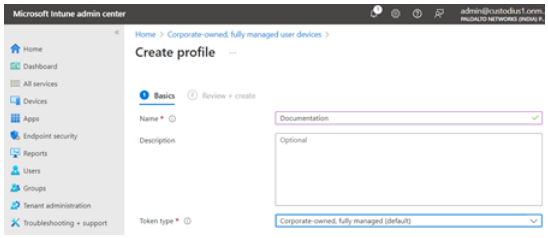
2. Créez un profil d'inscription pour votre périphérique. Suivez les étapes ci-dessous pour un périphérique entièrement géré appartenant à l'entreprise ou un profil de travail pour les périphériques appartenant aux employés (BYOD).

   Pour une démonstration sur la façon de créer un profil d'inscription pour votre périphérique, regardez cette vidéo.

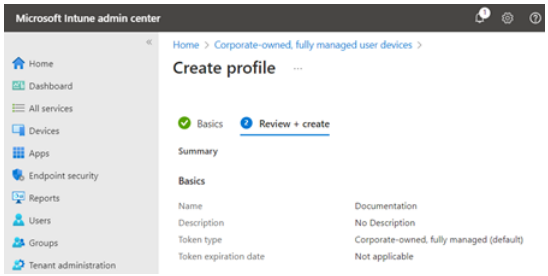
   1. Sur la page d'inscription Android, sélectionnez le type d'appareil.

   2. Cliquez sur **Create policy (Créer une politique)**.

   3. Saisissez un nom, une description et définissez le **Token type (Type de jeton)** sur **Corporate Owned fully managed (default) (Entièrement géré appartenant à l'entreprise [par défaut])**.
   4. Cliquez sur **Next (Suivant)**, examinez les détails du profil et cliquez sur **Create (Créer)**.

3. Inscrivez votre périphérique dans Microsoft Intune. Pour plus d'informations, consultez le Guide d'inscription Microsoft.

Déployer l'application GlobalProtect sur des terminaux Android en utilisant Microsoft Intune

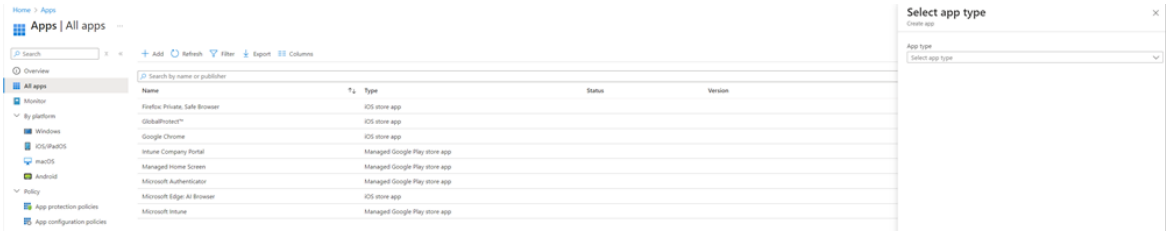
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans cette section, vous déployez l'application GlobalProtect sur vos terminaux Android en utilisant Microsoft Intune.

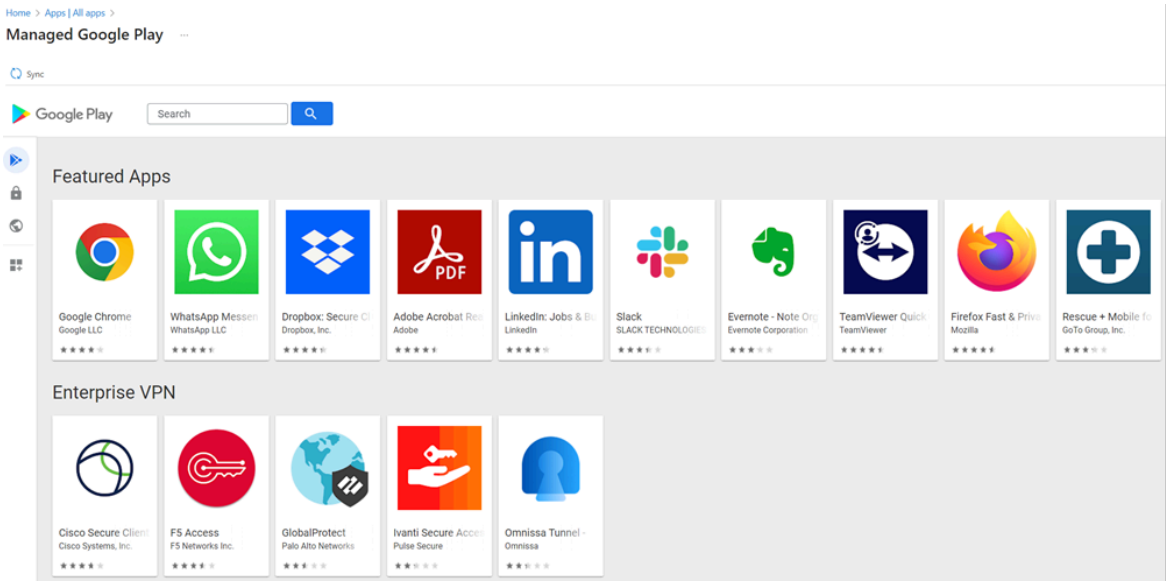
 ©2026 Palo Alto Networks, Inc.

Pour une démonstration sur la façon de compléter les prérequis pour inscrire votre appareil Android sur Intune, regardez cette vidéo.

1. Cliquez sur **Apps (Applications)** > **All Apps (Toutes les applications)**, puis sur **Add (Ajouter)**.

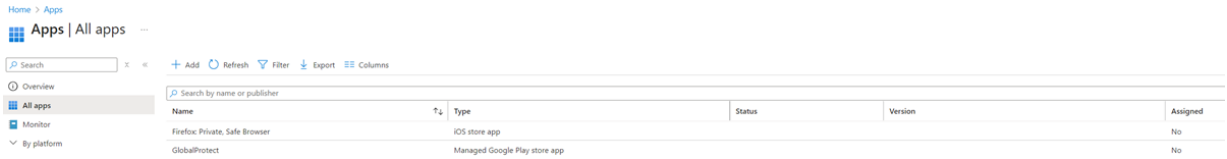


2. Définissez l'**App (Application)** sur **Managed Google Play App (Application Google Play gérée)** et cliquez sur **Select (Sélectionner)**.



3. Sélectionnez **GlobalProtect**, puis cliquez sur **Sync (Synchroniser)** en haut à gauche de la page.

4. Cliquez sur **Refresh (Actualiser)** pour afficher l'application nouvellement ajoutée.



5. Pour utiliser des certificats pour l'authentification, reportez-vous à la section Certificates (Certificats) dans la documentation de Microsoft Intune.

Pour la méthode de connexion toujours activée, les certificats sont le mode d'authentification préféré.

 ©2026 Palo Alto Networks, Inc.

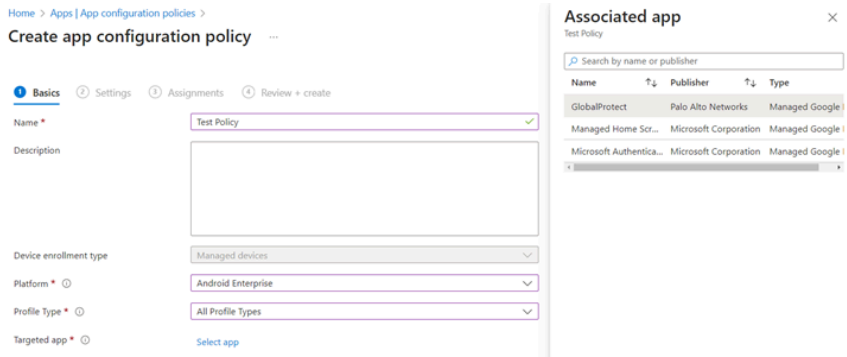
Créer une configuration d'application sur des terminaux Android à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez créer une configuration d'application dans Microsoft Intune pour permettre aux administrateurs de personnaliser et de gérer les paramètres d'application GlobalProtect pour les appareils Android sans obliger les utilisateurs à configurer manuellement l'application GlobalProtect eux-mêmes. Cette politique permet aux administrateurs du département informatique de spécifier les paramètres de configuration qui peuvent contrôler le comportement des applications, activer des fonctionnalités spécifiques et renforcer la sécurité sur les périphériques gérés.

Pour une démonstration de la façon de créer une politique de configuration pour votre appareil Android sur Intune, regardez cette vidéo.

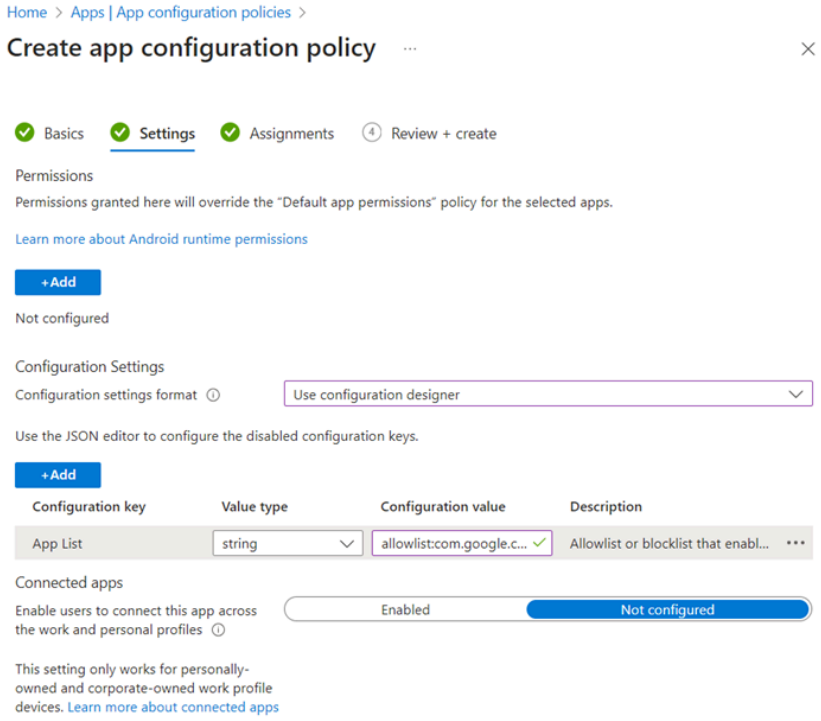
1. Sur la page Applications, cliquez sur **Policy (Politique)** > **App configuration policies (Politiques de configuration des applications)**, puis cliquez sur **Create (Créer)** > **Managed Devices (Périphériques gérés)**.
2. Saisissez un nom et une description pour la politique, puis sélectionnez la plateforme (Android Enterprise) et le type de profil.
3. Cliquez sur **Select app (Sélectionner l'application)** à côté de Targeted app (Application ciblée), sélectionnez GlobalProtect, puis cliquez sur OK.



4. Cliquez sur **Next (Suivant)**.

 ©2026 Palo Alto Networks, Inc.

5. Dans le format des paramètres de configuration, , sélectionnez **Use configuration designer (Utiliser le concepteur de configuration)** et ajoutez les clés requises.



Clé	Type de valeur	Description	Exemple
portal *Attribut requis pour toutes les configurations*	Chaîne	Adresse IP ou nom de domaine complet (FQDN) du portail.	**`10.1.8.190`**
app_list *Attribut requis pour les configurations par application*	Chaîne	Configuration du VPN par application. Commencez la chaîne par le mot clé de la **allowlist (liste d'autorisation)** ou de la **(liste de blocage)** suivie de deux-points, et faites-la suivre par un tableau de noms d'applications séparés par des points-virgules. Ajoutez aussi un point-virgule à la fin de la liste. La liste d'autorisation indique les applications qui utiliseront l'application GlobalProtect	**`whiltelist | blacklist: com.google.calendar; com.android.email; com.android.chrome`** Valeur par défaut : aucune.

 ©2026 Palo Alto Networks, Inc.

Clé	Type de valeur	Description	Exemple
		pour la communication réseau. Le trafic réseau de toute application qui ne figure pas sur la liste d'autorisation ou qui n'est pas expressément nommée dans la liste de blocage ne passera pas par le tunnel VPN.	
connect_method	Chaîne	• Choisissez `user-logon` pour la méthode de connexion toujours active. Cela connecte automatiquement GlobalProtect avec vos informations d'identification. Sur les appareils Android, GlobalProtect ne se connecte pas automatiquement lorsque vous ouvrez des applications configurées avec une liste d'autorisation ou une liste de blocage. Par conséquent, nous recommandons de définir la méthode de connexion toujours activée pour les configurations par application. • Choisissez `à la demande` pour vous assurer que les utilisateurs connectent manuellement GlobalProtect via l'application.	**`user-logon | on-demand`** Valeur par défaut : vierge, auquel cas la méthode de connexion spécifiée sur la configuration du portail est utilisée.
nom d'utilisateur	Chaîne	Nom d'utilsateur associé à l'utilisateur.	**`john`**
password	Chaîne	Mot de passe associé à l'utilisateur.	**`Password!1234`**
managed	Booléenne	Indique si le périphérique est géré par un MDM.	**`vraie| fausse`** Valeur par défaut : faux

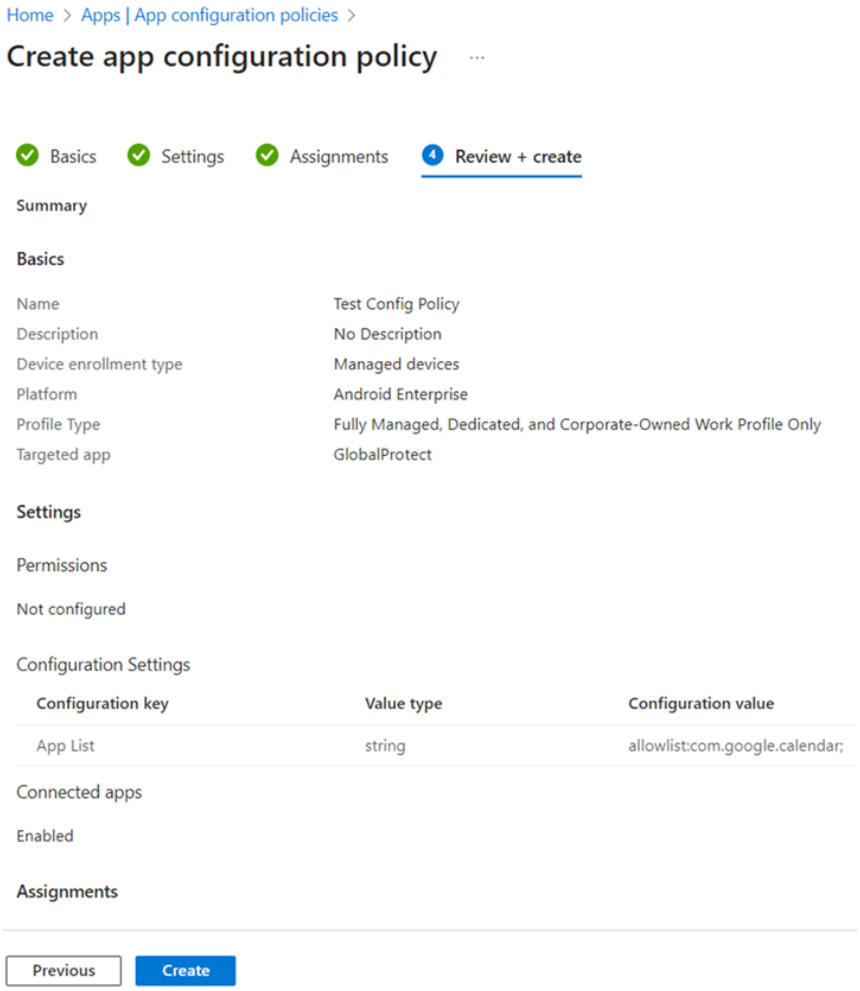
©2026 Palo Alto Networks, Inc.

Clé	Type de valeur	Description	Exemple
mobile_id	Chaîne	L'ID mobile est utilisé comme ID d'hôte.	**5188a8193be43f42d332dde5cb2c941e**
use_default_browser_for_saml	Booléen	• Choisissez `vrai` pour utiliser le navigateur par défaut pour l'authentification SAML • Choisissez `faux` pour utiliser le navigateur intégré pour l'authentification SAML.	**vraie| fausse** Valeur par défaut : faux
compliance	Chaîne	Indique si le périphérique est conforme aux politiques de conformité. Ce paramètre est inclus dans le rapport HIP et peut être utilisé pour créer des politiques de sécurité.	**yes | no (oui | non)**
Etiquette	Chaîne	Mettre une étiquette pour identifier un appareil. Ce paramètre est inclus dans le rapport HIP et peut être utilisé pour créer des politiques de sécurité. Vous pouvez spécifier n'importe quelle valeur pour ce paramètre.	**HR_Department**
proxy-url	Chaîne	Indique l'URL de votre fichier d'auto-configuration (PAC) proxy. Vous pouvez spécifier les paramètres du proxy lorsque vous configurez le profil VPN sur vos terminaux Android. Cette clé est disponible uniquement à partir de l'application GlobalProtect pour Android version 6.1.7 et ultérieure.	http://example.com/proxy.pac https://example.com/proxy.pac
ownership	Chaîne	Indique si le périphérique appartient à l'entreprise ou s'il est personnel. Ce paramètre est inclus dans le rapport HIP et peut être utilisé pour créer des politiques de sécurité. Vous pouvez spécifier	**corp-owned**

 ©2026 Palo Alto Networks, Inc.

Clé	Type de valeur	Description	Exemple
		n'importe quelle valeur pour ce paramètre.	

6. Cliquez sur **Next (Suivant)**.
7. Attribuez la politique aux utilisateurs ou groupes appropriés. Pour déployer la politique à grande échelle sur tous les périphériques applicables, sélectionnez **Add all users (Ajouter tous les utilisateurs)** ou **Add all devices (Ajouter tous les périphériques)**.
8. Cliquez sur **Next (Suivant)**.
9. Examinez vos paramètres et cliquez sur **Create (Créer)**.



Déploiement de configuration automatique proxy (PAC) depuis GlobalProtect sur les terminaux Android

À partir de la version 6.1.7 de l'application Android GlobalProtect, vous pouvez configurer et déployer des URL de fichiers d'auto-configuration proxy (PAC) sur des terminaux Android, en utilisant les plateformes de gestion des périphériques mobiles (MDM). En poussant ces

 ©2026 Palo Alto Networks, Inc.

configurations par le biais de la gestion des appareils mobiles (MDM), les paramètres proxy sont appliqués uniformément sur tous les terminaux android, garantissant un déploiement transparent et des mesures de sécurité cohérentes.

Vous pouvez ajouter l'URL du fichier PAC à l'aide des valeurs suivantes tout en créant une règle de politique de configuration d'application sur les terminaux Android à l'aide de plateformes MDM.

Clé : `proxy-url`

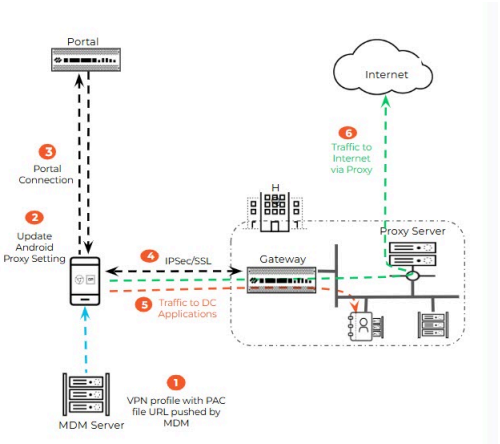
Type de valeur : `<String>`, par exemple,

`http://pac./proxy.pac`,

`https://pac./proxy.pac`

Cette fonctionnalité étend la capacité de bureau existante de GlobalProtect pour configurer des proxys tiers via des URL de fichiers d'auto-configuration de proxy (PAC) vers la plateforme mobile Android également et elle élimine le besoin d'autres outils tiers pour le déploiement d'URL de fichiers PAC.

La méthode d'URL de fichier PAC prise en charge inclut la norme d'auto-configuration du proxy (PAC) et la fonctionnalité est prise en charge sur Android version 11 et suivantes.



Configurer le mode de verrouillage pour la méthode de connexion toujours activée sur les terminaux Android à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

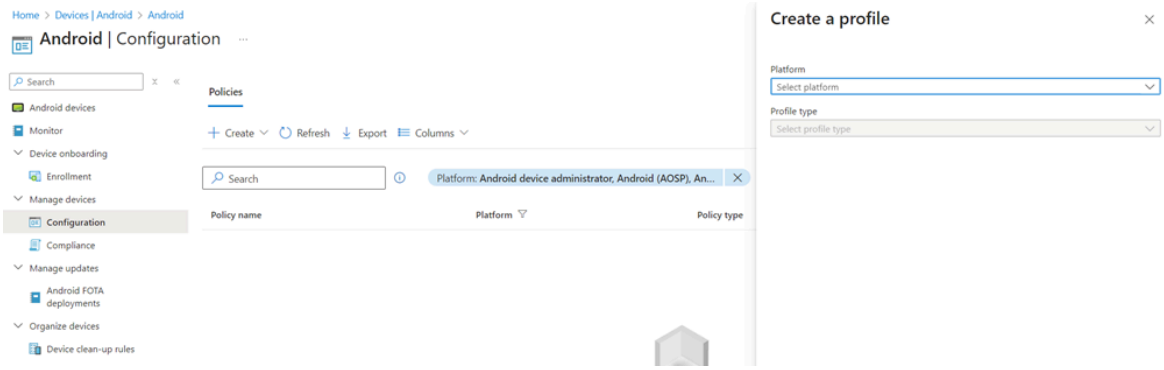
Pour les périphériques configurés avec la méthode de connexion toujours activée, vous devez activer le verrouillage, qui force la connexion sécurisée à être toujours active et connectée en plus de désactiver l'accès au réseau lorsque l'application n'est pas connectée.

Pour une démonstration de la configuration du mode verrouillage, regardez cette vidéo.

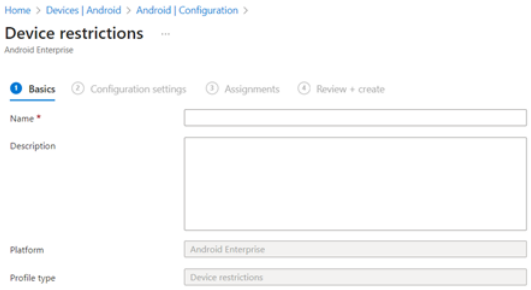
 ©2026 Palo Alto Networks, Inc.

1. Sur le centre d'administration Microsoft Intune, accédez à **Devices (Périphériques)** > **Android** > **Configuration**.

2. Cliquez sur **Create (Créer)** > **New Policy (Nouvelle politique)**.



3. Définissez **Platform (Plateforme)** sur **Android Enterprise** et **Profile Type (Type de profil)** sur **Device restrictions (Restrictions de périphérique)**, puis cliquez sur **Create (Créer)**.

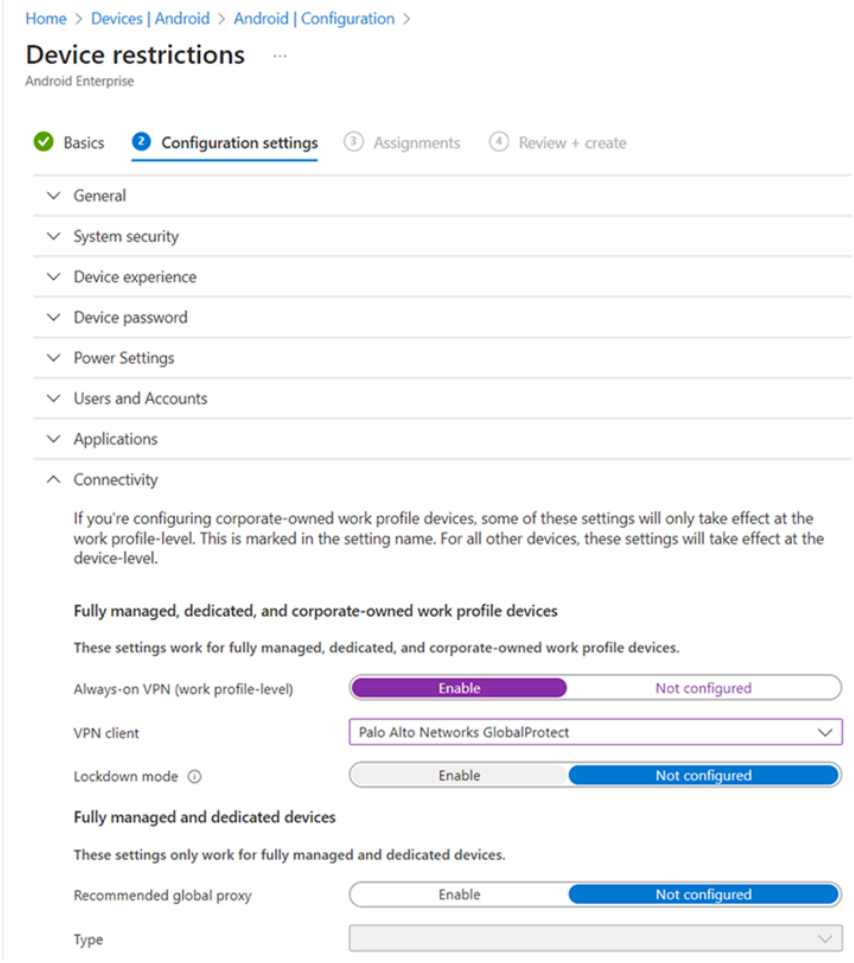


4. Saisissez un nom et une description et cliquez sur **Next (Suivant)**.

5. Développez **Connectivity (Connectivité)** et activez **Always-on VPN (work profile-level) (VPN Toujours actif [au niveau du profil professionnel])**.

 ©2026 Palo Alto Networks, Inc.

6. Définissez le **VPN client (Client VPN)** sur **Palo Alto Networks GlobalProtect**.



7. Activez le **Lockdown mode (Mode verrouillage)** si nécessaire.

   Le mode Verrouillage est similaire à la fonctionnalité Application de GlobalProtect pour l'accès au réseau et garantit que tout le trafic réseau des terminaux Android passe par l'application GlobalProtect, appliquant ainsi les politiques de sécurité et empêchant tout accès non autorisé. Lorsqu'il est activé, il bloque tout le trafic réseau sur le terminal jusqu'à ce qu'une connexion à la passerelle GlobalProtect soit établie.

8. Cliquez sur **Next (Suivant)**.

9. Affectez la politique aux groupes d'utilisateurs inclus et cliquez sur **Next (Suivant)**.

10. Examinez les paramètres et cliquez sur **Create (Créer)**.

Configurer Micrsoft Intune pour les terminaux macOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (géré par Panorama ou Strata Cloud Manager)	

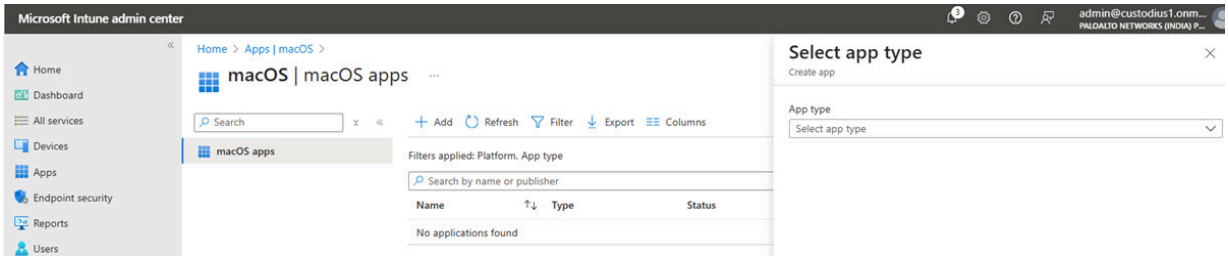
La configuration de Microsoft Intune pour les terminaux macOS implique un ensemble complet d'étapes pour assurer une gestion sécurisée et efficace des périphériques Apple au sein de l'infrastructure d'une organisation. Vous commencez par déployer l'application GlobalProtect avec Microsfot Intune, puis configurez les paramètres GlobalProtect sur les terminaux macOS à l'aide d'Intune, appliquez les connexions pour l'accès au réseau et accordez un accès complet au disque à l'application GlobalProtect pour une sécurité et une efficacité renforcées.

Déployer l'application GlobalProtect sur les terminaux macOS à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Téléchargez le package GlobalProtect que vous avez reçu de votre représentant du support technique, spécifiez le portail et la méthode de connexion, puis indiquez le système d'exploitation de l'application.

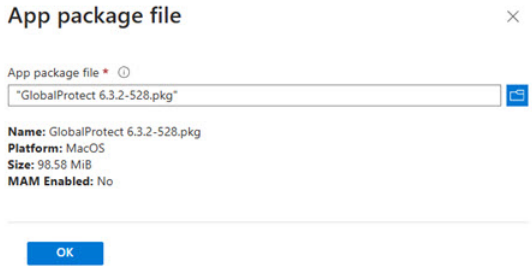
1. Accédez au Centre d'administration Microsoft Intune à l'adresse **https://intune.microsoft.com** et connectez-vous avec les informations d'identification de l'administrateur pour Intune.
2. Sélectionnez **Apps (Applications)** > **macOS**, puis cliquez sur **Ajouter (Add)**.



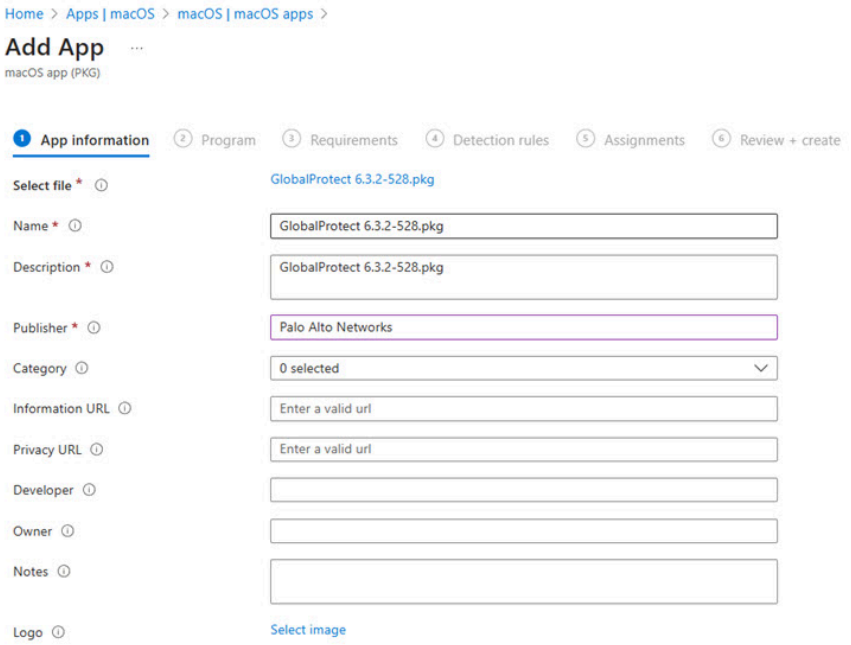
3. Dans le volet Sélectionner le type d'application, s'ouvrant à droite, sélectionnez **macOS app (PKG) (Application macOS [PKG])** et cliquez sur **Select (Sélectionner)**.

 ©2026 Palo Alto Networks, Inc.

4. Cliquez sur **Select app package file (Sélectionner un fichier)** de package d'applications, téléchargez le fichier de package GlobalProtect à partir de votre ordinateur et cliquez sur **OK**.



5. Dans l'onglet Informations sur l'application, précisez le **Publisher (Éditeur)** comme Palo Alto Networks, saisissez des informations supplémentaires si nécessaire et cliquez sur **Next (Suivant)**.



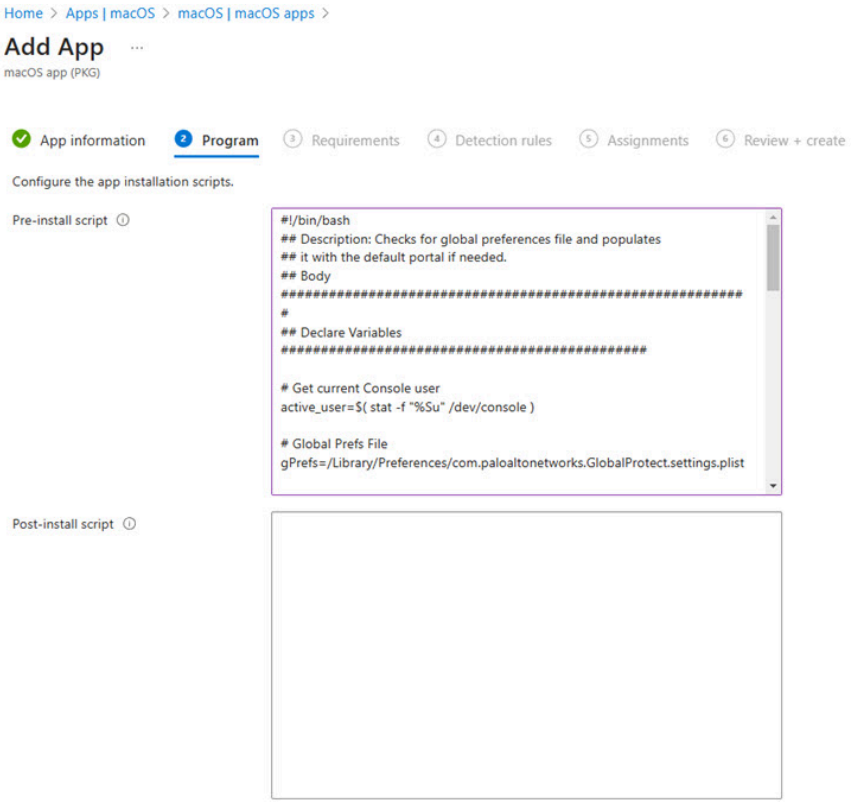
6. Dans l'onglet Programme, saisissez le script de pré-installation à exécuter avant l'installation de l'application GlobalProtect. Avec ce script, vous pouvez spécifier le portail, la méthode de connexion et si le navigateur par défaut doit être utilisé pour l'authentification.

Copiez collez le script suivant dans le script Pré-installation après avoir mis à jour les valeurs `Portal`, `connect-method` et `default-browser`.

```
#!/bin/bash ## Description : Checks for global preferences file
 and populates ## it with the default portal if needed. ## Body
 ######################################################## ##
 Declare Variables ##############################################
 # Get current Console user active_user=$( stat -f "%Su" /
dev/console ) # Global Prefs File gPrefs=/Library/Preferences/
com.paloaltonetworks.GlobalProtect.settings.plist ## Logic
 ######################################################## # Check
 to see if the global preference file already exists... if [[ -
e $gPrefs ]]; then echo "Default global portal already exists.
 Skipping." else echo "Setting default GP portal to: {Portal FQDN
```

 ©2026 Palo Alto Networks, Inc.

```
 here}" # If it does not already exist, create it and populate the
 default portal using the echo command echo '<?xml version="1.0"
 encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
 <plist version="1.0"> <dict> <key>Palo Alto Networks</key>
 <dict> <key>GlobalProtect</key> <dict> <key>PanSetup</key>
 <dict> <key>Portal</key> <string>{Portal FQDN here}</string>
 </dict> <key>Settings</key> <dict> <key>connect-method</key>
 <string>on-demand | always-on</string> <key>default-browser</key>
 <string>{Value}</string> [yes | no] </dict> </dict> </dict> </
dict> </plist> ' > $gPrefs echo $? # Kill the Preference caching
 daemon to prevent it from overwriting any changes killall cfprefsd
 echo $? fi # Check exit code. exit $?
```



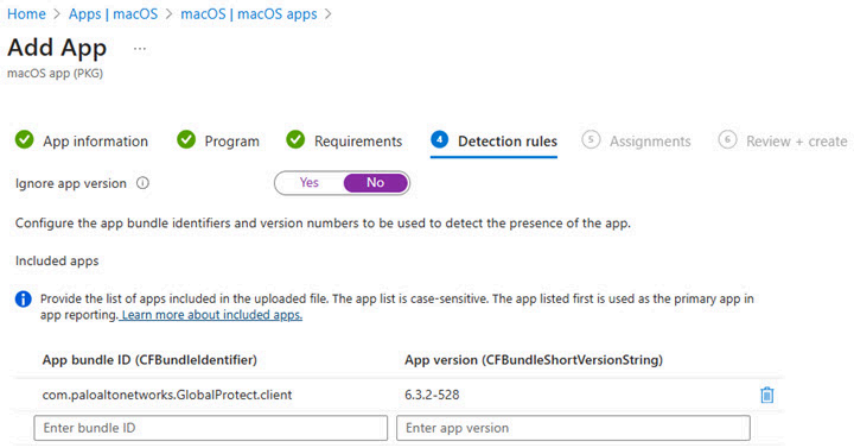
7. Cliquez sur **Next (Suivant)**.

8. Dans l'onglet Configuration requise, sélectionnez le système d'exploitation minimum requis pour installer l'application GlobalProtect et cliquez sur **Next (Suivant)**.

 ©2026 Palo Alto Networks, Inc.

9. Dans l'onglet Règles de détection, définissez **Ignore app version (Ignorer la version de l'application)** sur Non.

Ce paramètre garantit que Microsoft Intune vérifie le bundleID et le numéro de version de l'application GlobalProtect avant l'installation.

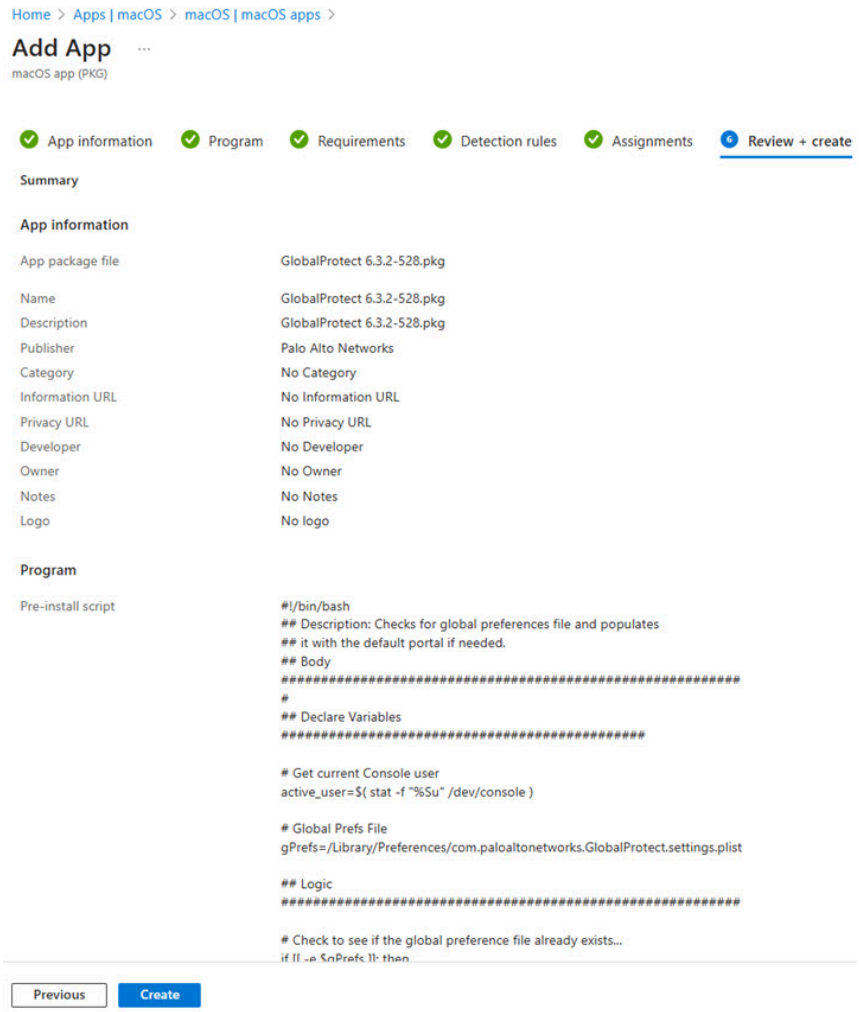


10. Laissez inchangées les valeurs de l'identifiant de bundle de l'application et de la version de l'application et cliquez sur **Next (Suivant)**.

11. Sélectionnez les affectations d'utilisateurs appropriées et cliquez sur **Next (Suivant)**.

 ©2026 Palo Alto Networks, Inc.

12. Examinez le résumé de l'application et cliquez sur **Create (Créer)**.



Configurer les paramètres de GlobalProtect sur macOS via Microsoft Intune

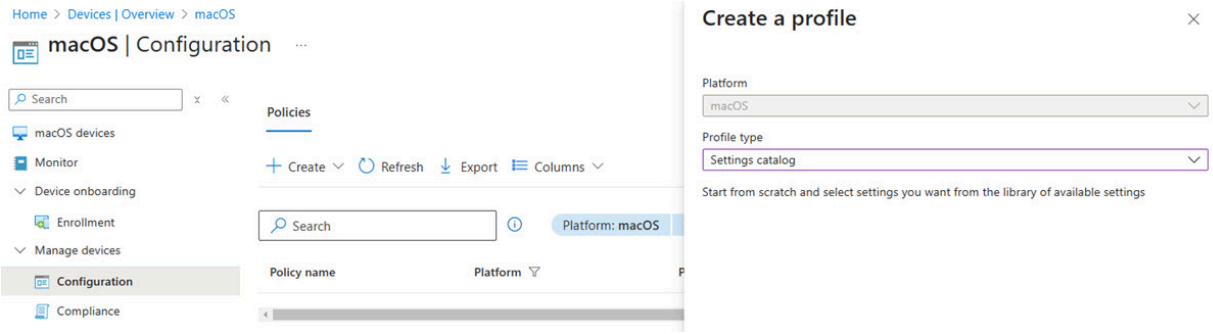
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous déployez des extensions système, appliquez des connexions pour l'accès réseau et accordez un accès complet au disque à l'application GlobalProtect pour une sécurité et une efficacité accrues. Le déploiement des extensions système permet à GlobalProtect d'accéder au système et de fonctionner correctement sur macOS. Les extensions système permettent à GlobalProtect de s'intégrer au système d'exploitation pour améliorer la sécurité et les capacités de gestion du réseau.

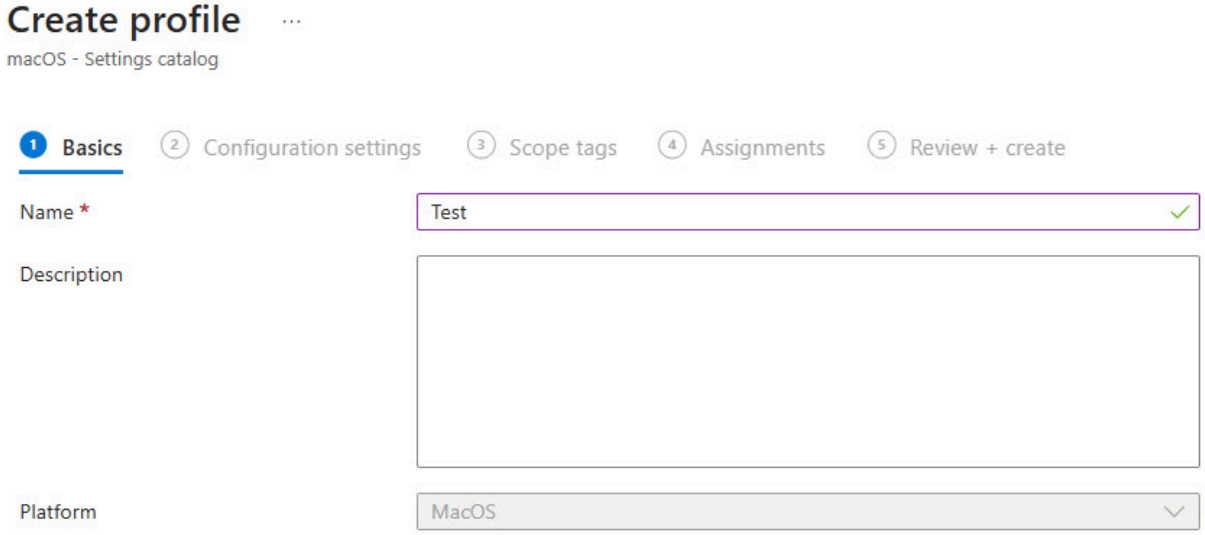
1. Dans le centre d'administration Microsoft Intune, accédez à **Devices (Périphériques)** > **macOS** > **Configuration**.

 ©2026 Palo Alto Networks, Inc.

2. Cliquez sur **Create (Créer)** > **New Policy (Nouvelle politique)**.
3. Définissez le type de profil sur le Catalogue de paramètres et cliquez sur **Create (Créer)**.



4. Saisissez un nom et une description et cliquez sur **Next (Suivant)**.

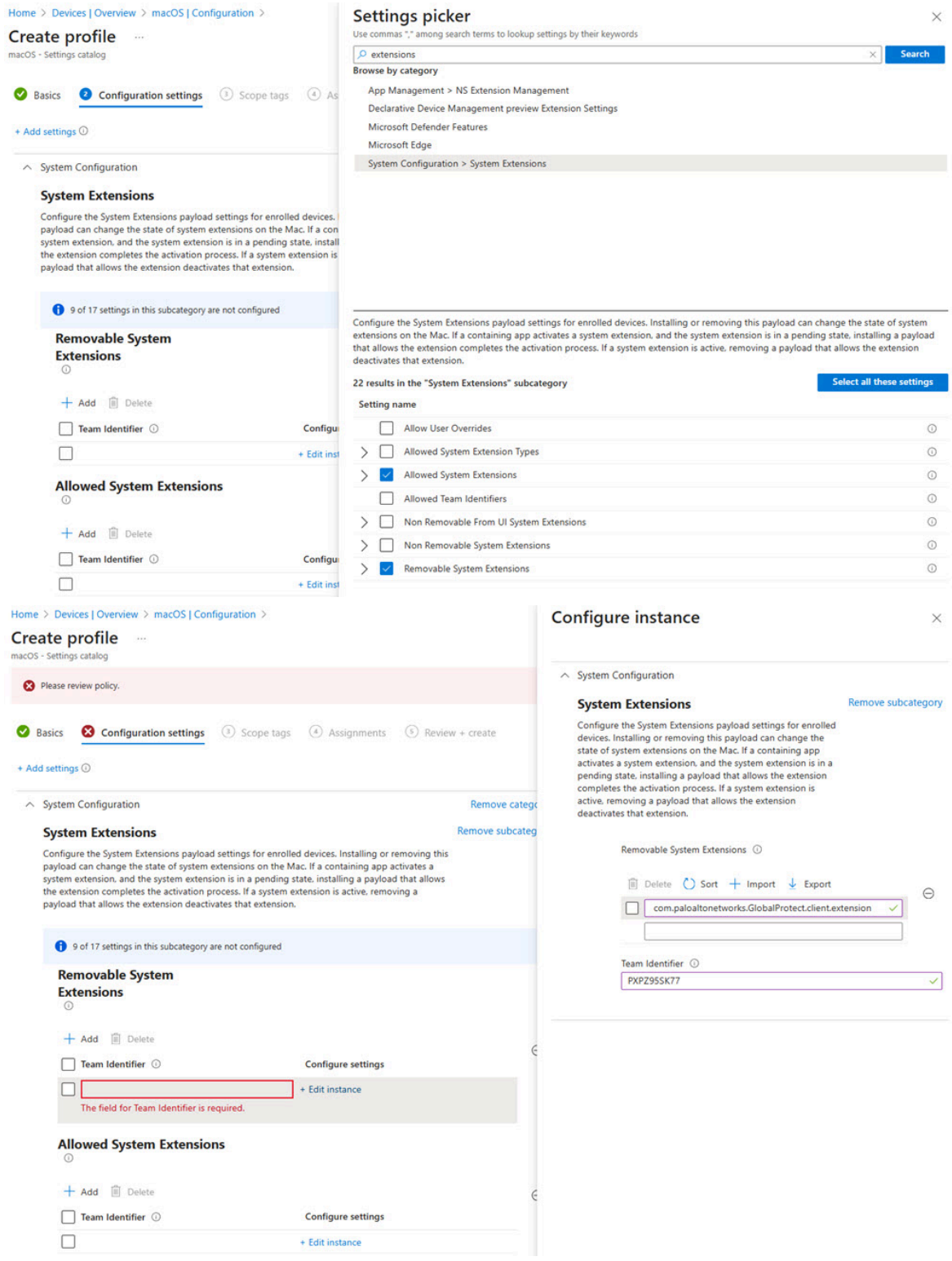


5. Dans l'onglet Paramètres de configuration, cliquez sur **Add settings (Ajouter des paramètres)**.
6. Recherchez et ajoutez des paramètres selon le tableau suivant.

Tâche et valeur de recherche	Sélectionnez	Ajoutez des champs et spécifier des valeurs dans le panneau d'extension système
Pour déployer des extensions système, recherchez des extensions.	**System Configuration (Configuration système)> System Extensions (Extensions système)**	1. Sélectionnez les cases à cocher Extensions système autorisées et Extensions système amovibles. 2. Fermez le panneau des paramètres. 3. Dans le panneau des extensions système, cliquez sur Modifier l'instance dans les Extensions système amovibles et entrez les valeurs suivantes : • Identifiant du bundle : com.paloaltonetworks.GlobalProtect.client.extension • Identifiant de l'équipe : PXPZ95SK77

 ©2026 Palo Alto Networks, Inc.

Tâche et valeur de recherche	Sélectionnez	Ajoutez des champs et spécifier des valeurs dans le panneau d'extension système
		4. Répétez l'étape ci-dessus dans les Extensions système amovibles



 ©2026 Palo Alto Networks, Inc.

Tâche et valeur de recherche	Sélectionnez	Ajoutez des champs et spécifier des valeurs dans le panneau d'extension système
(Facultatif) Pour appliquer GlobalProtect pour l'accès réseau, recherchez le filtre de contenu	**Web > Web Content Filter (> Filtre de contenu web)**	1. Sélectionnez les cases à cocher suivantes : • Identifiant de bundle du fournisseur de données de filtre • Exigence désignée du fournisseur de données de filtre • Grade de filtre • Identifiant de bundle du fournisseur de paquets de filtre • Exigence désignée du fournisseur de paquets de filtre • Filtrer les paquets • Filtrer les sockets • Type de filtre • ID de bundle du plugin 2. Fermez le panneau des paramètres. 3. Indiquez les options suivantes. • Identifiant de bundle du fournisseur de données de filtre : com.paloaltonetworks.GlobalProtect.client.extension • Exigence désignée du fournisseur de données de filtre : com.paloaltonetworks.GlobalProtect.client.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] / * exists **/ or certificate 1[field.1.2.840.113635.100.6.2.6] /** exists **/ and certificate leaf[field.1.2.840.113635.100.6.1.13] /** exists */ and certificate leaf[subject.OU] = PXPZ95SK77) • Grade de filtre : pare-feu • Identifiant de bundle du fournisseur de paquets de filtre : com.paloaltonetworks.GlobalProtect.client.extension • Exigence désignée du fournisseur de paquets de filtre : ancre apple générique et identifiant "com.paloaltonetworks.GlobalProtect.client.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /

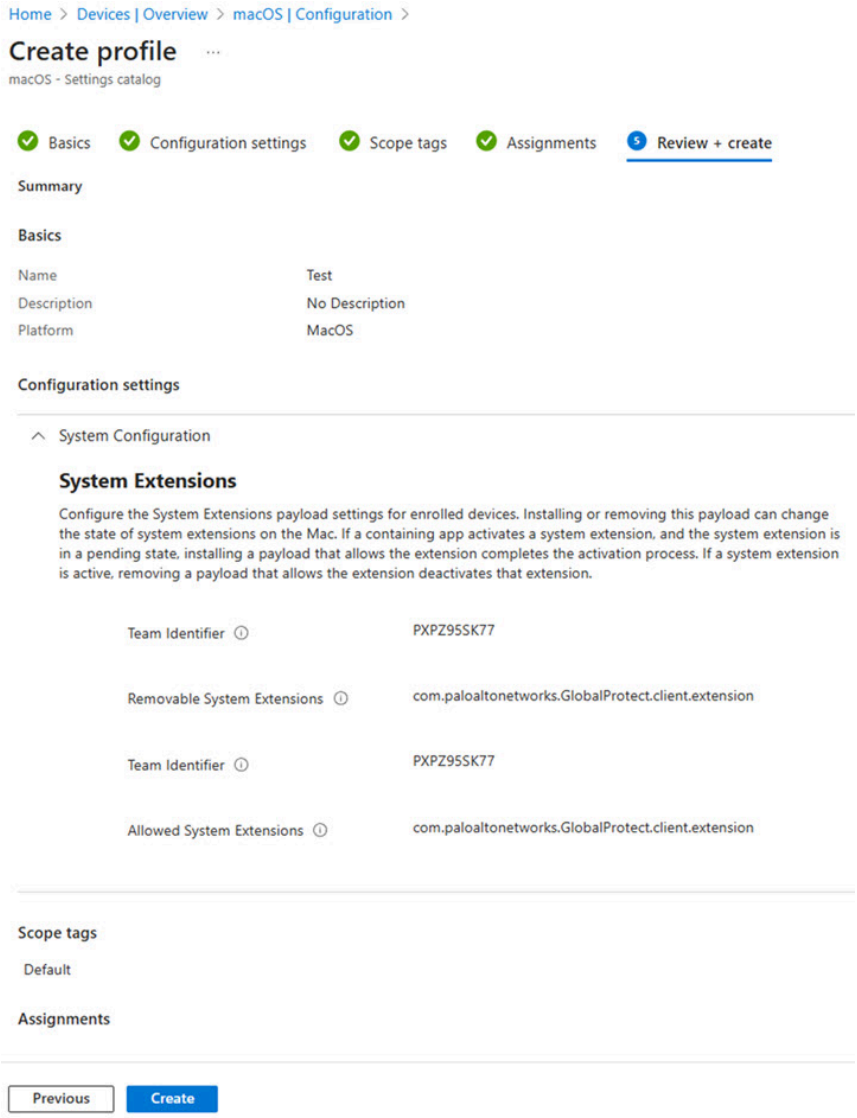
©2026 Palo Alto Networks, Inc.

Tâche et valeur de recherche	Sélectionnez	Ajoutez des champs et spécifier des valeurs dans le panneau d'extension système
		* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] / * exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = PXPZ95SK77) • Filtrer les paquets : Vrai • Filtres de sockets : Vrai • Type de filtre : Plug-in • Identifiant du bundle du plugin : com.paloaltonetworks.GlobalProtect.client
Pour accorder un accès complet au disque à l'application GlobalProtect, recherchez la confidentialité.	**Privacy (Confidentialité) > Privacy Preferences Policy Control (Contrôle des préférences de confidentialité)**	1. Développez les services et sélectionnez la case à cocher Système de politique Tous les fichiers. 2. Fermez le panneau des paramètres. 3. Cliquez sur Modifier l'instance et saisissez les valeurs suivantes dans le panneau de Contrôle de la politique de préférences de confidentialité : • Autorisé : Vrai • Autorisation : non requise, vous pouvez donc supprimer ce champ • Exigence de code : ancre apple générique et identifiant "com.paloaltonetworks.GlobalProtect.client.extension" et (certificat feuille[field.1.2.840.113635.100.6.1.9] / * existe / ou certificat 1[field.1.2.840.113635.100.6.2.6] / existe / et certificat feuille[field.1.2.840.113635.100.6.1.13] / existe */ et certificat feuille[subject.OU] = PXPZ95SK77) • Identifiant : PXPZ95SK77 • Type d'identifiant : identifiant de bundle • Code statique : Faux

7. Cliquez sur **Next (Suivant)**.
8. Ne faites aucun changement dans l'onglet des étiquettes de portée et cliquez sur **Next (Suivant)**.
9. Sélectionnez les affectations d'utilisateurs appropriées et cliquez sur **Next (Suivant)**.

 ©2026 Palo Alto Networks, Inc.

10. Assignez cette politique aux groupes appropriés et cliquez sur **Next (Suivant)**.
11. Examinez le résumé de la politique et cliquez sur **Create (Créer)**.



Mettre à niveau l'application GlobalProtect sur macOS via Microsft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

1. Désaffectez les utilisateurs et les groupes auxquels l'application GlobalProtect est actuellement affectée.

 ©2026 Palo Alto Networks, Inc.

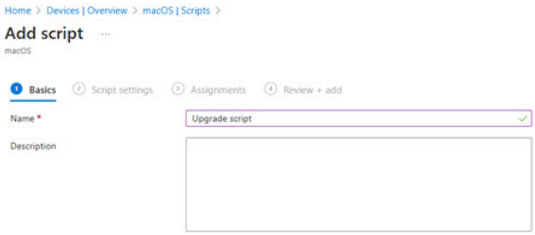
2. Ajoutez le texte suivant à un éditeur de texte et enregistrez-le sur votre ordinateur en tant que fichier .sh :

```
#!/bin/bash sh "/Applications/GlobalProtect.app/Contents/Resources/
uninstall_gp.sh" exit $?
```

3. Dans le centre d'administration Microsoft Intuit, accédez à **Devices (Périphériques)** > **macOS** > **Scripts**.

4. Cliquez sur **Add (Ajouter)**.

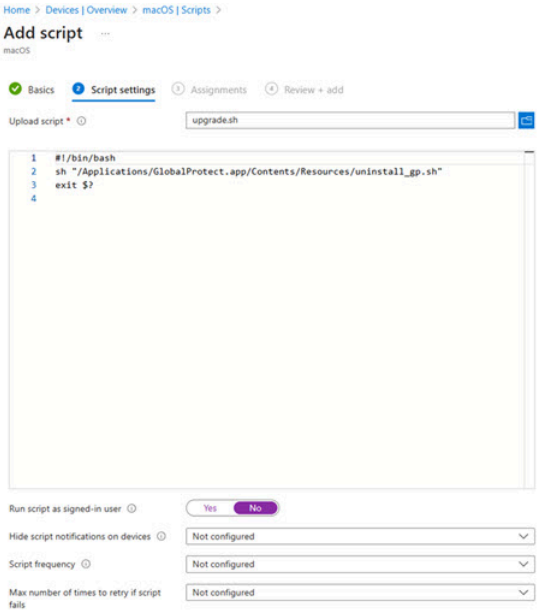
5. Tapez un nom et une description pour le script et cliquez sur **Next (Suivant)**.



6. Ajoutez une description et cliquez sur **Next (Suivant)**.

7. Téléchargez le script de mise à niveau que vous avez créé à l'étape 2.

8. Définissez Exécuter le script en tant qu'utilisateur connecté sur **No (Non)**.
Cela permet au système d'exécuter le script en tant qu'utilisateur racine.

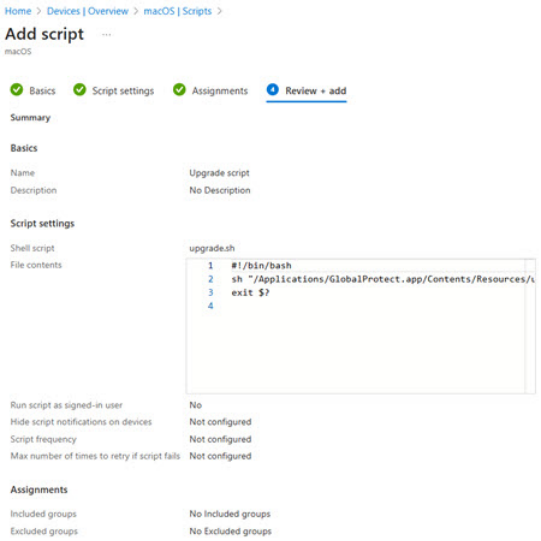


9. Spécifiez des informations supplémentaires si nécessaire et cliquez sur **Next (Suivant)**.

10. Effectuez des affectations d'utilisateurs pour la nouvelle version de l'application GlobalProtect et cliquez sur **Next (Suivant)**.

 ©2026 Palo Alto Networks, Inc.

11. Passez en revue le résumé du script et cliquez sur **Add (Ajouter)**.



Le script de désinstallation s'exécute lorsque Microsoft Intune le transmet aux périphériques.

12. Déployez la version requise de l'application GlobalProtect.

Télécharger des certificats pour les terminaux macOS via Microsoft Intune

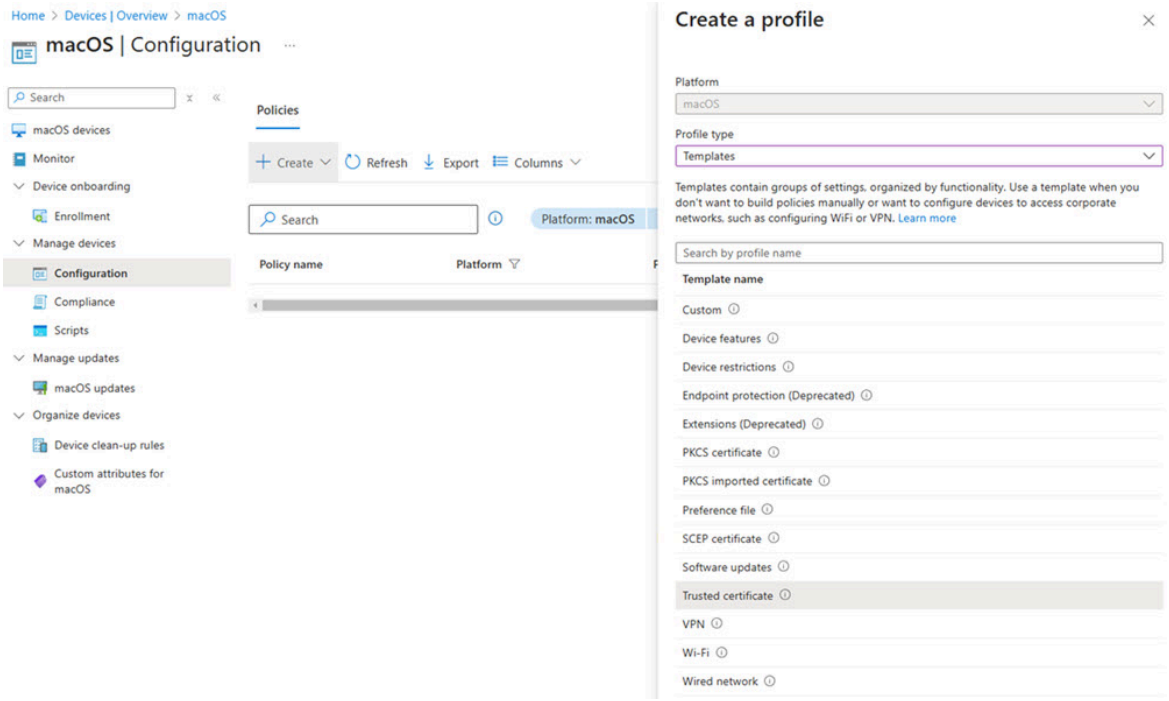
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez télécharger un certificat utilisateur ou de périphérique sur le terminal macOS.

1. Dans le centre d'administration Microsoft Intuit, accédez à **Devices (Périphériques)** > **macOS** > **Configuration**.
2. Cliquez sur **Create (Créer)** > **New Policy (Nouvelle politique)**.
3. Définissez le type de profil sur Modèles.

 ©2026 Palo Alto Networks, Inc.

4. Effectuez l'une des sélections suivantes :
   - Pour le CA racine, sélectionnez Certificat de confiance.
   - Pour le certificat SCEP, sélectionnez Certificat SCEP.



5. Cliquez sur **Create (Créer)**.

6. Spécifiez les champs suivants en fonction du certificat sélectionné.

Type de certificat	Informations à spécifier
CA racine	1. Saisissez un nom et une description et cliquez sur **Next (Suivant)**. 2. Spécifiez le canal de déploiement. 3. Sélectionnez le fichier de certificat. 4. Effectuez l'affectation aux utilisateurs et groupes appropriés et cliquez sur **Next (Suivant)**. 5. Examinez le récapitulatif et cliquez sur **Create (Créer)**.
Certificat SCEP	1. Entrez un nom, une description et d'autres informations obligatoires telles que l'utilisation de clé étendue et le canal de déploiement. 2. Téléchargez le certificat racine associé qui peut être imprimé en tant qu'émetteur de ce certificat SCEP.

©2026 Palo Alto Networks, Inc.

Type de certificat	Informations à spécifier
	3. Spécifiez le format du nom du sujet, la période de validité, l'utilisation de la clé, la taille de la clé et l'URL du serveur SCEP. 4. Cliquez sur **Next (Suivant)**. 5. Effectuez l'affectation aux utilisateurs et groupes appropriés et cliquez sur **Next (Suivant)**. 6. Examinez le récapitulatif et cliquez sur **Create (Créer)**.

Configurer Microsoft Intune pour les terminaux iOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Lorsqu'il est déployé avec Microsoft Intune, GlobalProtect prend en charge les méthodes de connexion suivantes :

- Toujours actif

  Dans une configuration toujours active, GlobalProtect se connecte automatiquement dès que vous vous connectez.

- À la demande

  Dans une configuration à la demande, vous devez vous connecter manuellement à GlobalProtect via l'application. Le trafic est acheminé via l'application GlobalProtect uniquement après que vous ayez initié et établi la connexion.

- Par application

  Dans une configuration par application, vous pouvez définir quelles applications gérées sont autorisées à acheminer le trafic via GlobalProtect. Pour ce faire, vous pouvez attacher un profil VPN à une application, ajouter des URL pour l'application à laquelle vous souhaitez accéder, ou faire une combinaison des deux.

GlobalProtect avec Microsoft Intune prend en charge l'authentification basée sur des certificats (SCEP uniquement) et SAML. Avant de déployer l'application, déterminez les méthodes de connexion et d'authentification appropriées pour votre environnement.

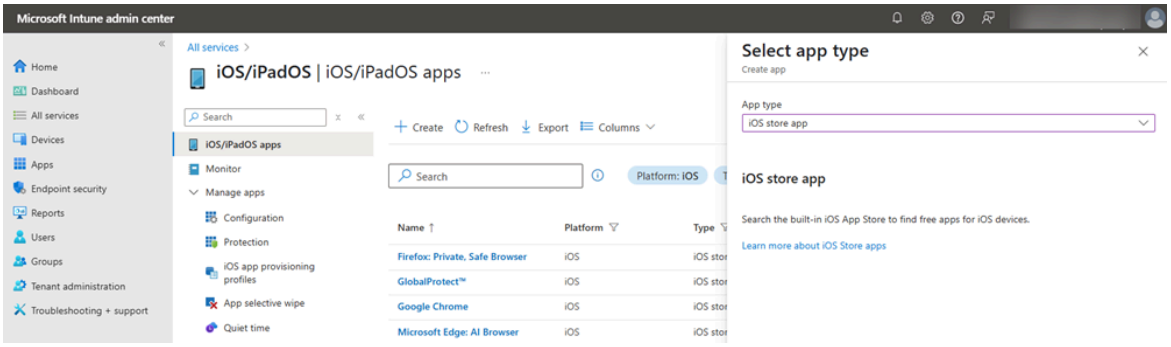
Sur les appareils iOS, l'application GlobalProtect est mise à jour automatiquement par l'App Store d'Apple.

 ©2026 Palo Alto Networks, Inc.

Déployer l'application GlobalProtect sur les terminaux iOS en utilisant Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

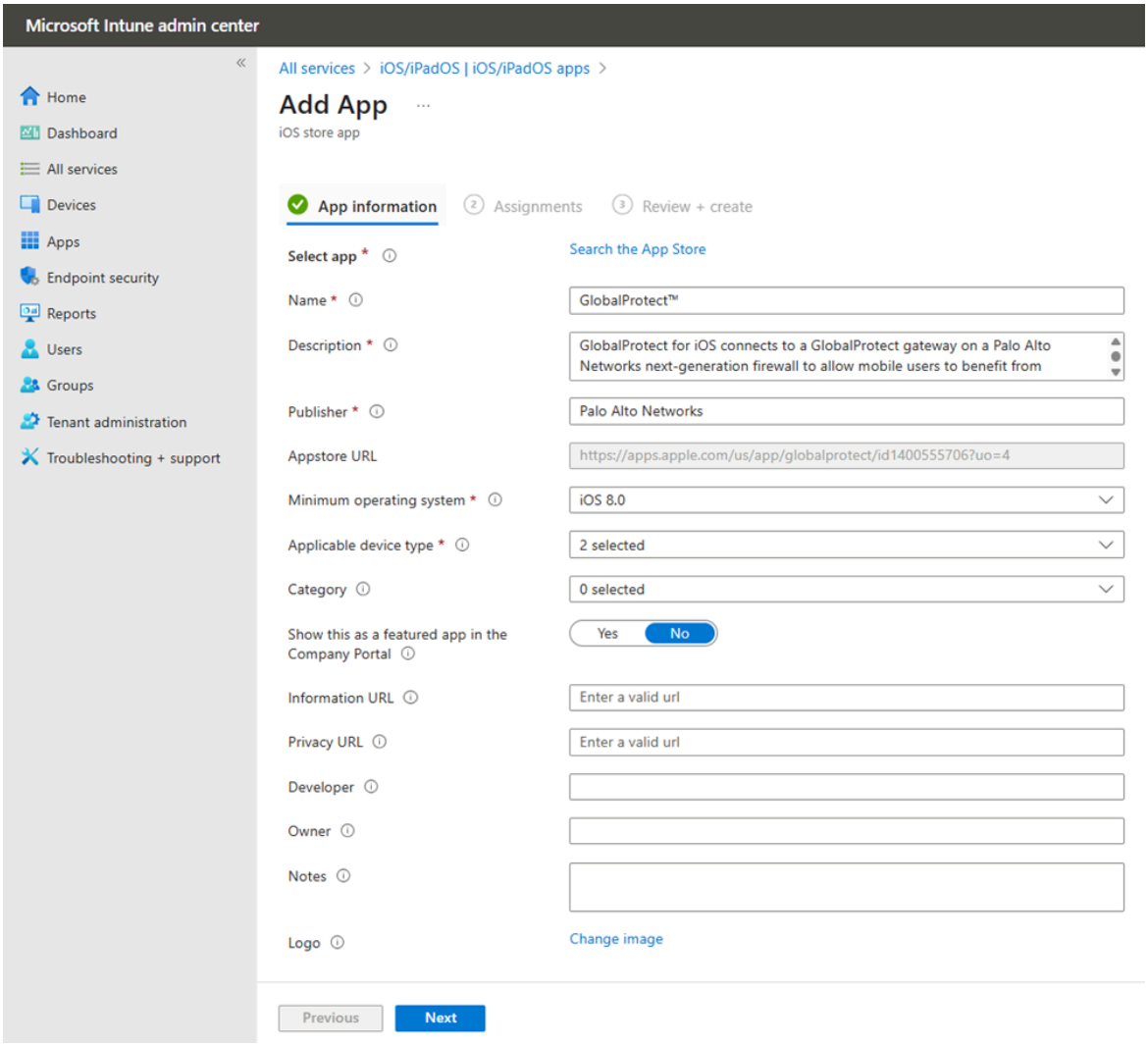
1. Inscrivez votre périphérique iOS dans Microsoft Intune. Pour plus d'informations, consultez le Guide d'inscription Microsoft.
2. Accédez au Centre d'administration Microsoft Intune à l'adresse **https://intune.microsoft.com** et connectez-vous avec les informations d'identification de l'administrateur pour Intune.
3. Sélectionnez **Applications** > **iOS/iPadOS** puis cliquez sur **Create (Créer)**.
4. Sélectionnez l'application de la boutique iOS et cliquez sur **Select (Sélectionner)**.



5. Dans la fenêtre Ajouter une application, cliquez sur Rechercher dans l'App Store et tapez GlobalProtect.
6. Cliquez sur GlobalProtect puis cliquez sur **Select (Sélectionner)**.

 ©2026 Palo Alto Networks, Inc.

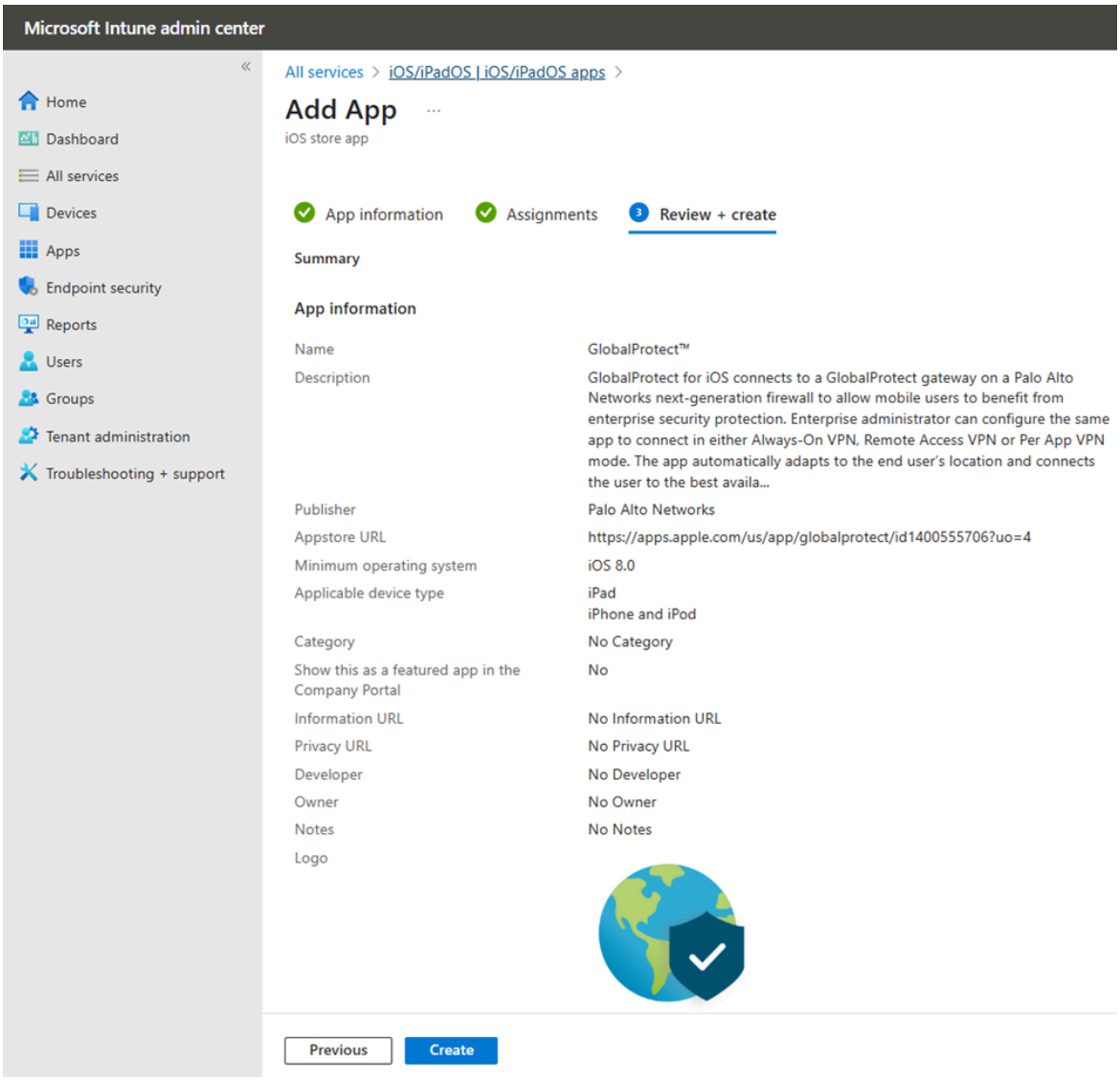
7. Dans l'onglet Informations sur l'application, modifiez ou entrez des informations supplémentaires si nécessaire, puis cliquez sur **Next (Suivant)**.



8. Dans l'onglet Affectations, ajoutez des affectations d'utilisateurs si nécessaire et cliquez sur **Next (Suivant)**.

 ©2026 Palo Alto Networks, Inc.

9. Examinez le résumé de l'application et cliquez sur **Create (Créer)**.



Authentification utilisateur pour iOS sur Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect™ avec Microsoft Intune prend en charge l'authentification basée sur des certificats (SCEP uniquement) et l'authentification SAML. Si vous utilisez l'authentification SAML, vous pouvez passer à l'étape suivante, Configurer les paramètres de GlobalProtect sur les appareils iOS via Microsoft Intune.

L'authentification SAML n'est pas prise en charge pour la méthode de connexion toujours active.

 ©2026 Palo Alto Networks, Inc.

Si vous souhaitez utiliser l'authentification basée sur des certificats, créez un profil de certificat SCEP en suivant les étapes ci-dessous.

1. Dans le centre d'administration Microsoft Intune, accédez à **Devices (Périphériques)** > **iOS/iPadOS devices (périphériques iOS/iPadOS)** > **Configuration**.
2. Cliquez sur **Create (Créer)** > **New Policy (Nouvelle politique)**.
3. Définissez le Type de profil sur **Templates (Modèles)** et sélectionnez **SCEP Certificate (Certificat SCEP)** comme nom de modèle.
4. Cliquez sur **Create (Créer)**.
5. Saisissez un nom et une description et cliquez sur **Next (Suivant)**.
6. Dans l'onglet Paramètres de configuration, sélectionnez un type en fonction de la manière dont vous prévoyez d'utiliser le profil de certificat :
   - **User (Utilisateur)** : Les certificats d'utilisateur peuvent contenir à la fois des attributs d'utilisateur et de périphérique dans le sujet et le SAN du certificat.
   - **Device (Périphérique)** : Les certificats de périphérique ne peuvent contenir que des attributs de périphérique dans le sujet et le SAN du certificat.
7. Entrez les attributs et valeurs de **Subject alternative name (Autre nom de l'objet)** pour le profil. Vous pouvez entrer plus d'un autre nom de l'objet. La valeur textuelle peut contenir des variables et du texte statique pour les attributs.
8. Entrez la **Certificate validity period (Période de validité du certificat)**. Intune prend en charge une période de validité allant jusqu'à 24 mois.
9. Sélectionnez les options d'utilisation des clés pour le certificat :
   - **Digital signature (Signature numérique)** : Autorisez l'échange de clés uniquement lorsqu'une signature numérique aide à protéger la clé.
   - **Key encipherment (Clé de chiffrement)** : Autorisez l'échange de clés uniquement lorsque la clé est chiffrée.
10. Sélectionnez le nombre de bits contenus dans la clé.
11. Sélectionnez le profil de **Root Certificate (Certificat racine)** de confiance que vous avez précédemment configuré et attribué aux utilisateurs et périphériques concernés pour ce profil de certificat SCEP. Le profil de certificat de confiance est utilisé pour fournir aux utilisateurs et aux périphériques le certificat CA racine de confiance.
12. Ajoutez des valeurs pour **Extended key usage (Utilisation de clé étendue)** pour l'objectif prévu du certificat.
13. Cliquez sur **Next (Suivant)**.
14. Ajoutez des affectations d'utilisateur et cliquez sur **Next (Suivant)**.
15. Examinez les détails du certificat et cliquez sur **Create (Créer)**.

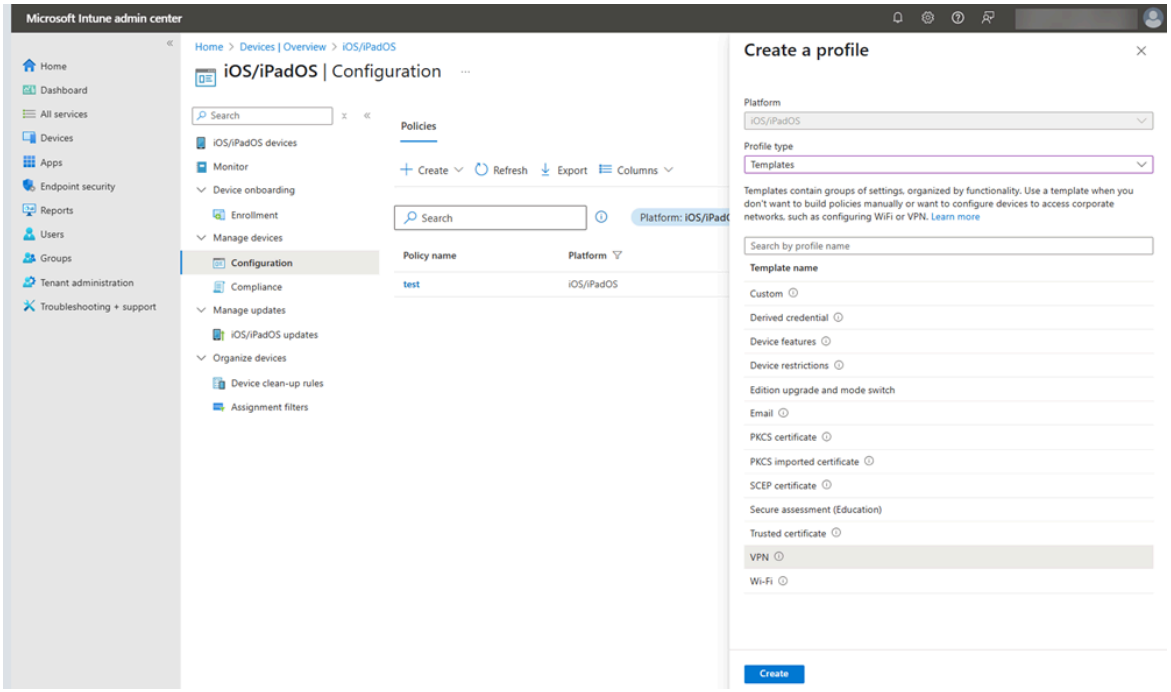
 ©2026 Palo Alto Networks, Inc.

Configurer les paramètres de GlobalProtect sur les appareils iOS via Microsoft Intune

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

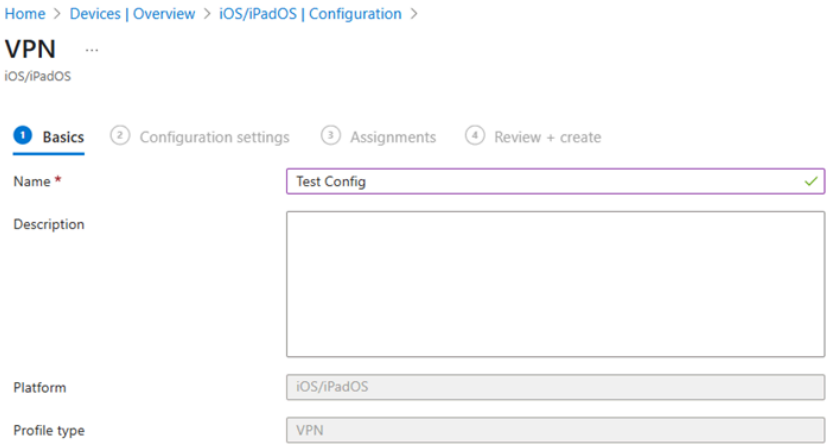
Vous créez un profil VPN personnalisé avec la méthode d'authentification et la méthode de connexion souhaitées. Si vous souhaitez utiliser un certificat pour l'authentification, assurez-vous d'avoir créé un certificat client. Reportez-vous à la section Authentification utilisateur pour iOS sur Microsoft Intune.

1. Dans le centre d'administration Microsoft Intune, accédez à **Devices (Périphériques)** > **iOS/iPadOS devices (périphériques iOS/iPadOS)** > **Configuration**.
2. Cliquez sur **Create (Créer)** > **New Policy (Nouvelle politique)**.
3. Définissez le type de profil sur modèles et sélectionnez **VPN** comme nom de modèle.
4. Cliquez sur **Create (Créer)**.



 ©2026 Palo Alto Networks, Inc.

5. Saisissez un nom et une description et cliquez sur **Next (Suivant)**.



6. Dans l'onglet Paramètres de configuration, spécifiez le type de connexion comme **Custom VPN (VPN personnalisé)**.

7. Développez la section VPN de base et entrez le **Connection name (Nom de connexion)** qui sera affiché aux utilisateurs finaux sur leurs terminaux.

8. Dans **VPN server address (adresse du serveur VPN)**, saisissez le nom du portail GlobalProtect.

9. Sélectionnez la méthode d'authentification :

Méthode d'authentification	Étapes
Authentification SAML	Définissez la **Authentication method (Méthode d'authentification)** sur nom d'utilisateur et mot de passe. L'authentification locale est également prise en charge. *L'authentification SAML n'est pas prise en charge pour la méthode de connexion toujours active.*
Certificats	1. Définissez **Authentication method (Méthode d'authentification)** sur Certificats. 2. Sélectionnez le certificat SCEP pour authentifier la connexion. Pour des informations sur la création du certificat, consultez Authentification utilisateur pour iOS sur Microsoft Intune.

10. **Split Tunneling (Segmentation de tunnel)** n'est pas pris en charge, vous pouvez donc laisser la valeur par défaut telle quelle.

11. Indiquez **VPN identifier (Identifiant VPN)** comme **`com.paloaltonetworks.globalprotect.vpn`**.

 ©2026 Palo Alto Networks, Inc.

12. Entrez des paires clé-valeur pour les attributs VPN personnalisés de votre organisation. Les paires suivantes sont prises en charge sur Microsoft Intune pour les appareils iOS.

Clé	Type de valeur	Description	Exemple
Etiquette	Chaîne	Les étiquettes vous permettent de faire correspondre le périphérique à d'autres attributs.	GuestAccount, HRdeparment
compliance	Chaîne	Indique si le périphérique est conforme.	yes
ownership	Chaîne	Indique la catégorie de propriété du périphérique, comme employé.	propriété de la société
mobile_id	Chaîne	Si cela est spécifié, cela est défini comme l'ID de l'hôte.	device_id

13. Développez la section VPN automatique et effectuez l'une des actions suivantes en fonction de la méthode de connexion.

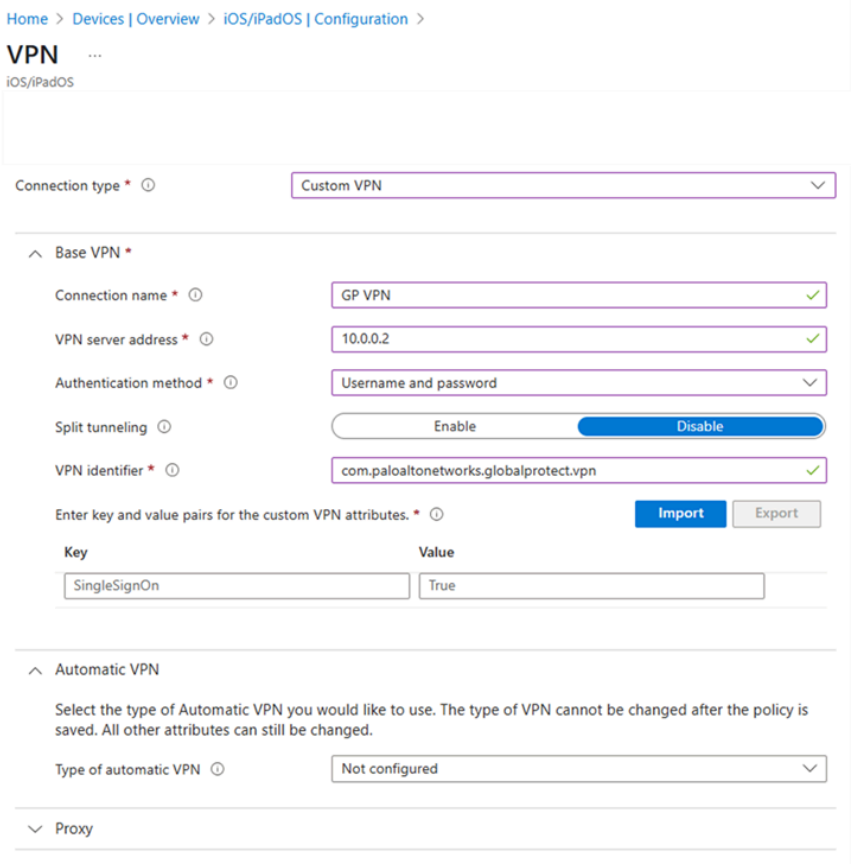
Méthode de connexion	Étapes à suivre
À la demande **Assure que les utilisateurs se connectent manuellement à GlobalProtect via l'application.**	Définissez **Type of Automatic VPN (Type de VPN automatique)** sur non configuré.
Toujours actif **Connecte automatiquement GlobalProtect avec vos identifiants.**	1. Définissez **Type of Automatic VPN (Type de VPN automatique)** sur VPN à la demande. 2. Ajoutez une règle à la demande en cliquant sur **Add (Ajouter)**. 3. Définissez **I want to do the following (Je veux faire ce qui suit)** sur VPN personnalisé. 4. Définissez **I want to restrict (Je veux restreindre)** sur Tous les domaines.

©2026 Palo Alto Networks, Inc.

Méthode de connexion	Étapes à suivre
	5. Cliquez sur **Save (Enregistrer)**. S'il y a une correspondance avec votre règle, alors le périphérique effectue l'action que vous sélectionnez.
Par application **Associe des applications spécifiques à la connexion GlobalProtect. Lorsque l'application s'exécute, le trafic est automatiquement acheminé via GlobalProtect.**	Vous pouvez attacher un profil VPN à une application, ajouter des URL pour l'application à laquelle vous souhaitez accéder, ou faire une combinaison des deux. Pour attacher un profil, consultez Associer votre profil VPN iOS à une application. Pour ajouter des URL d'application : 1. **Type of Automatic VPN (Type de VPN automatique)** sur **Per-app VPN (VPN par application)**. 2. Ajoutez une ou plusieurs URL de site web. Lorsque ces URL sont visitées à l'aide du navigateur Safari sur l'appareil, la connexion VPN est automatiquement établie. 3. Entrez **Associated Domains (Domaines associés)** à utiliser avec GlobalProtect. 4. Dans **Excluded Domains (Domaines exclus)**, saisissez les domaines Safari qui peuvent contourner GlobalProtect pour la méthode de connexion par application. Le trafic vers les domaines exclus utilise Internet public même si GlobalProtect est connecté. 5. Vous pouvez **Block users from disabling automatic VPN (Empêcher**

 ©2026 Palo Alto Networks, Inc.

Méthode de connexion	Étapes à suivre
	les utilisateurs de désactiver le VPN automatique).



14. Cliquez sur **Next (Suivant)**.

15. Sélectionnez les affectations d'utilisateurs appropriées et cliquez sur **Next (Suivant)**.

16. Examinez le résumé de la politique et cliquez sur **Create (Créer)**.

Le profil de configuration du périphérique pour les appareils iOS est créé. Après avoir commencé à gérer vos terminaux iOS avec Microsoft Intune, vous pouvez générer des journaux pour le dépannage. Pour plus d'informations, consultez Report an Issue From the GlobalProtect App for iOS (Signaler un problème depuis l'application GlobalProtect pour iOS).

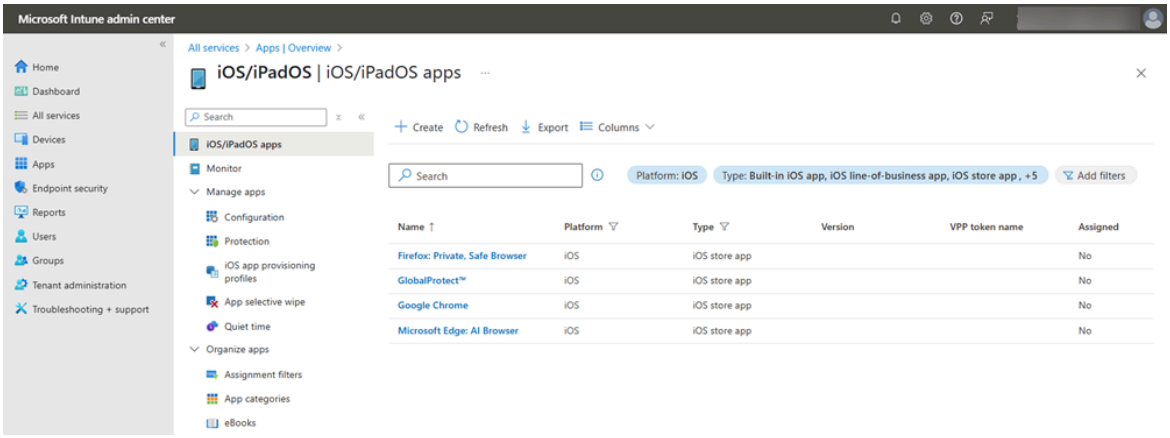
Associer votre profil VPN iOS à une application

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Licence Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence GlobalProtect Gateway ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

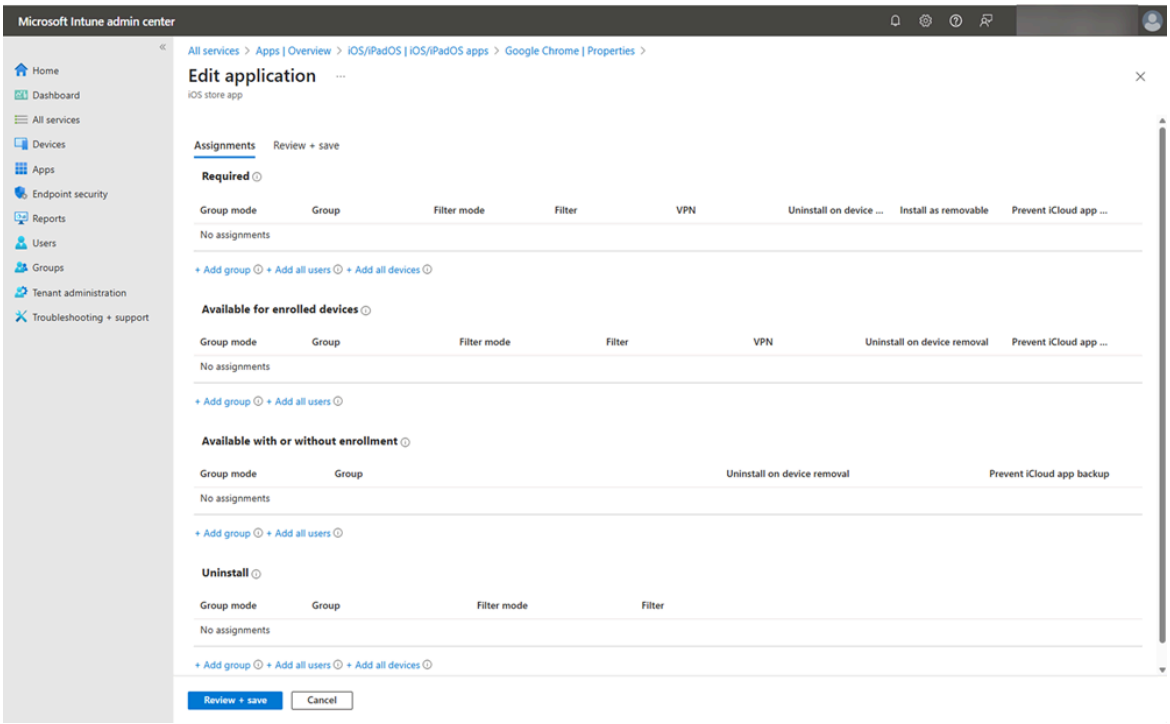
Pour la méthode de connexion par application, vous devez associer votre profil VPN par application aux applications auxquelles vous souhaitez accéder via GlobalProtect.

1. Dans le centre d'administration de Microsoft Intune, accédez à **Apps (Applications** > **iOS/iPadOS**, puis cliquez sur l'application à laquelle vous souhaitez accéder via GlobalProtect.



2. Cliquez sur **Manage (Gérer)** > **Properties (Propriétés)**.

3. Cliquez sur **Assignments (Affectations)** > **Edit (Modifier)** pour le groupe d'utilisateurs que vous souhaitez associer au profil par application.



4. Cliquez sur **VPN** et sélectionnez le profil.

5. Cliquez sur **OK**, puis cliquez sur **Save (Enregistrer)**.

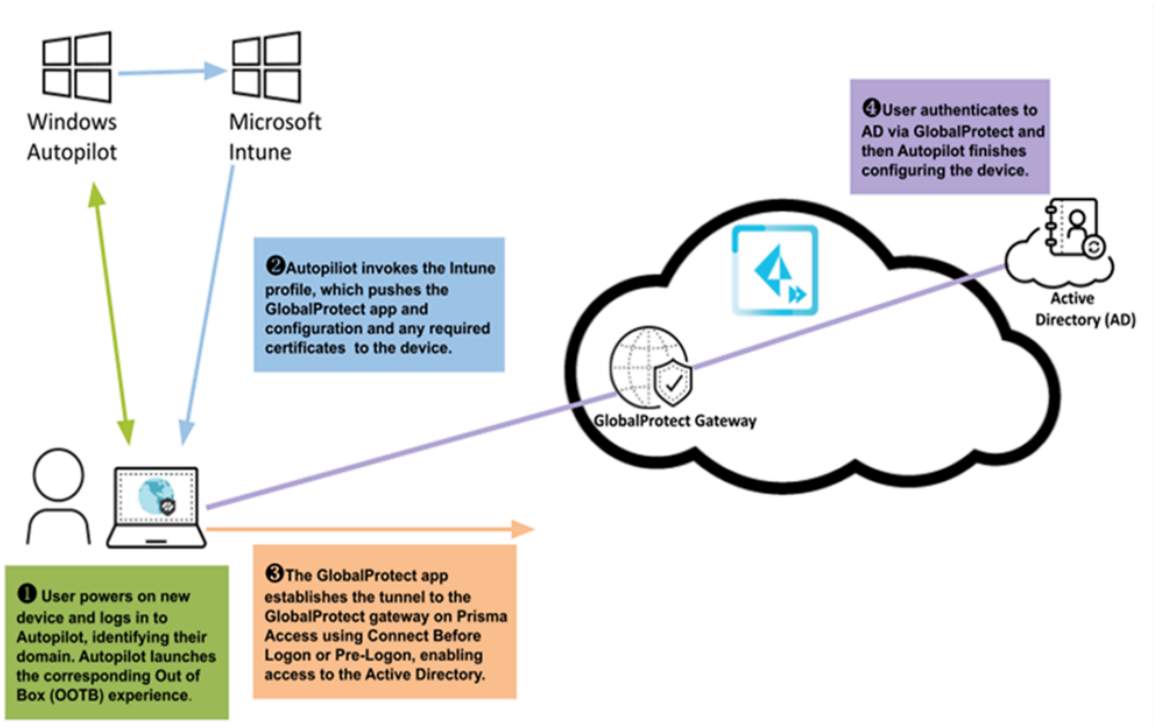
6. Cliquez sur **Review + Save (Réviser + Enregistrer)**.

 ©2026 Palo Alto Networks, Inc.

Déployer un nouveau périphérique à l'aide de Windows Autopilot et Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Compatible avec l'application GlobalProtect pour Windows (la version 5.2 ou ultérieure est requise pour le déploiement se connection avant identification) Les terminaux doivent exécuter Windows 10 (64 bits) ou Windows 11

Vous pouvez envoyer un nouveau périphérique Windows à un utilisateur final et déployer automatiquement l'application GlobalProtect ainsi que tous les paramètres PKI ou d'authentification requis en utilisant Microsoft Intune et Windows Autopilot. Ceci est utile dans les environnements où vous souhaitez envoyer un périphérique directement d'un fournisseur ou d'un entrepôt sans avoir à effectuer de configuration, comme le déploiement PKI et de certificats, le déploiement de l'application GlobalProtect avant la livraison à l'utilisateur final.



Il existe deux façons de provisionner un nouveau périphérique Windows à l'aide de Windows Autopilot et Microsoft Intune :

- Se connecter avant identification : ce déploiement ne nécessite aucune infrastructure PKI et est la méthode de déploiement la plus simple.

 ©2026 Palo Alto Networks, Inc.

- Préouverture de session : ce déploiement nécessite une infrastructure PKI ainsi qu'un déploiement CA Microsoft configuré pour déployer les certificats d'ordinateur pour la méthode de connexion de préouverture de session.

Utiliser Autopilot pour déployer GlobalProtect en mode Se connecter avant identification

En mode Se connecter avant identification, l'application GlobalProtect agit en tant que fournisseur d'accès pour pré-ouverture de session (PLAP) pour fournir un accès à votre réseau d'entreprise avant que l'utilisateur ne se connecte au périphérique Windows, permettant aux utilisateurs sur un terminal qui n'est pas encore configuré avec un profil local, des certificats ou des comptes utilisateurs d'accéder au contrôleur de domaine et de rejoindre le domaine. Ce déploiement ne nécessite pas d'environnement PKI et utilise plutôt une séquence de connexion basée sur l'utilisateur (LDAP, RADIUS, SAML, authentification basée sur nom d'utilisateur/mot de passe, cartes intelligentes ou authentification OTP sont prises en charge). Dans ce déploiement, le périphérique de l'utilisateur final est provisionné comme suit :

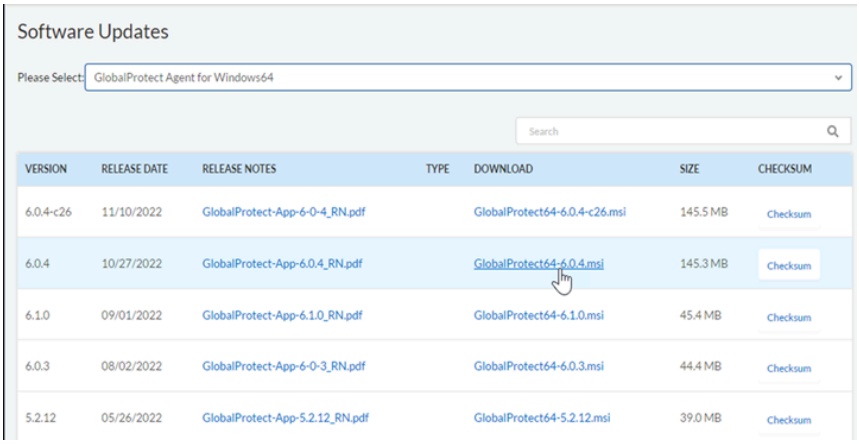
1. L'utilisateur final se connecte à Autopilot, en identifiant son domaine.
2. Autopilot se connecte ensuite à Intune, qui a été configuré pour déployer l'application GlobalProtect avec l'adresse du portail par défaut, les paramètres Se connecter avant identification et la configuration pour rejoindre le domaine.
3. L'utilisateur final clique sur le bouton fournisseur d'accès pour pré-ouverture de session (PLAP) pour se connecter à GlobalProtect et établir le tunnel vers la passerelle GlobalProtect (sur site ou Prisma Access), permettant l'accès au contrôleur de domaine.
4. GlobalProtect invite l'utilisateur à se connecter au fournisseur d'identification, après quoi Windows Autopilot peut terminer la configuration du périphérique.

Pour utiliser ce déploiement, vous devrez créer un package pour Microsoft Intune à déployer sur Windows Autopilot. Ce package contiendra le fichier MSI de GlobalProtect ainsi que deux scripts wrapper que vous créerez pour installer le MSI et définir les paramètres de configuration nécessaires pour déployer l'application en mode Se connecter avant identification, et un deuxième script pour lancer l'installateur en mode 64 bits (Intune se lance en mode 32 bits par défaut). Vous téléchargerez ensuite le package sur Intune pour créer l'application et l'ajouter au groupe ciblé pour Autopilot.

 ©2026 Palo Alto Networks, Inc.

1. Téléchargez le fichier MSI de l'application GlobalProtect depuis le Portail assistance clientèle de Palo Alto Networks.

   Pour que ce déploiement fonctionne, vous devez utiliser la version 5.2.x ou ultérieure de l'application GlobalProtect (c'est à ce moment-là que Se connecter avant identification a été introduit).



2. Créez un script wrapper PowerShell pour indiquer à Microsoft Intune comment installer GlobalProtect.

   Le script doit inclure les instructions suivantes :

   - Définir l'adresse du portail de sorte que l'utilisateur n'ait pas à la saisir (**PORTAL="portal_name"**)
   - Définir l'application pour utiliser le navigateur par défaut après la connexion initiale (**DEFAULTBROWSER="yes"**)
   - Définir la méthode de connexion sur Se connecter avant identification (**CONNECTMETHOD="user-logon"**)
   - Enregistrer GlobalProtect avec le fournisseur d'identifiants Windows pour permettre Se connecter avant identification à l'écran de connexion

   Vous pouvez également utiliser des paramètres supplémentaires pour personnaliser le déploiement de l'application GlobalProtect. Voici un exemple de script wrapper que vous pouvez copier et modifier avec vos propres valeurs pour l'adresse du portail et le nom du fichier MSI :

```
$PortalAddress = 'myportal.gpcloudservice.com' $MSIFileName =
 'GlobalProtect64-6.0.4.msi' $MSISwitches = '/quiet /norestart'
 $ScriptPath = Split-Path -Path $MyInvocation.MyCommand.Path
 $InstallProcess = Start-Process -FilePath "msiexec" -ArgumentList
 ("/i " + [char]34 + $ScriptPath + "\" + $MSIFileName + [char]34
 PORTAL=”myportal.gpcloudservice.com”” DEFAULTBROWSER=””yes””
 CONNECTMETHOD=””user-logon”” #Register PLAP provider Start-Process
 -FilePath "$env:ProgramFiles\Palo Alto Networks\GlobalProtect
\PanGPS.exe" -ArgumentList "-registerplap" -Wait Write-Host
 ("Installation completed, exiting with last return code (" +
 $InstallProcess.ExitCode + ")") Exit $InstallProcess.ExitCode
```

 ©2026 Palo Alto Networks, Inc.

3. (Hybrid Azure AD uniquement) Installez le connecteur Intune pour Active Directory et le connecteur AzureAD.

4. Enregistrez les périphériques des utilisateurs finaux avec Autopilot et créez le groupe pour l'expérience Out of Box (OOBE) que vous créez pour déployer l'application GlobalProtect.

   Reportez-vous à la documentation de Microsoft Windows Autopilot pour les instructions.

 ©2026 Palo Alto Networks, Inc.

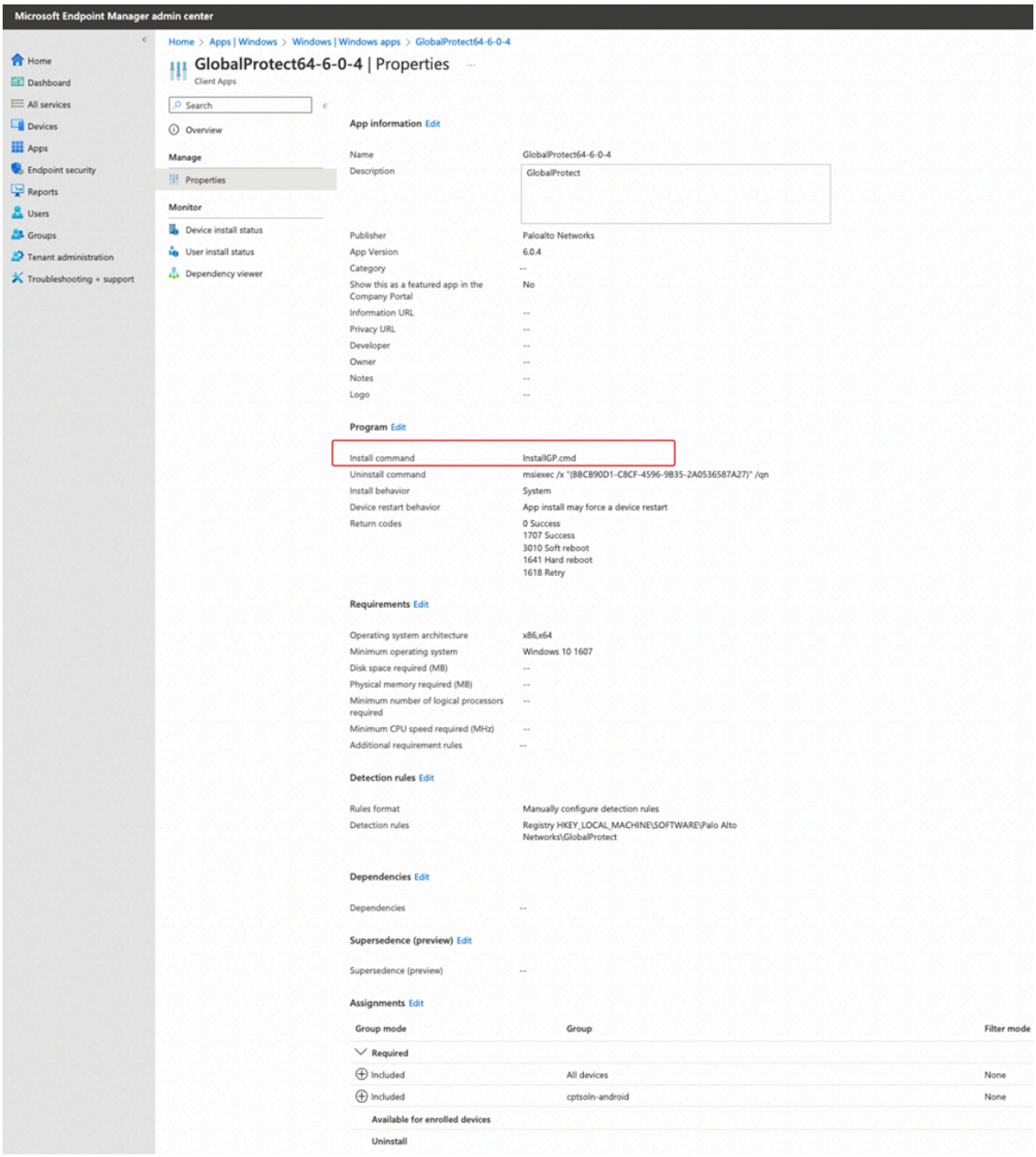
5. Créez le package d'installation de l'application GlobalProtect (le fichier MSI et les scripts) et téléchargez-le sur Microsoft Intune.
   1. Utilisez l'outil de préparation de contenu Microsoft Win32 pour créer le package de l'application.

      Par défaut, l'installateur se lance en mode 32 bits. Utilisez le script pour le convertir en mode 64 bits comme dans l'exemple suivant :

      ```
      IntuneWinAppUtil.exe -c C:\Temp\GlobalProtectPackage\Install -s
      GlobalProtect64-6.0.4.msi -o C:\Temp\GlobalProtectPackage\Output
      ```
   2. Téléchargez le package d'application sur Microsoft Intune.

      Assurez-vous que **Install command (Commande d'installation)** pointe vers le fichier batch que vous avez créé pour lancer le MSI en mode 64 bits.

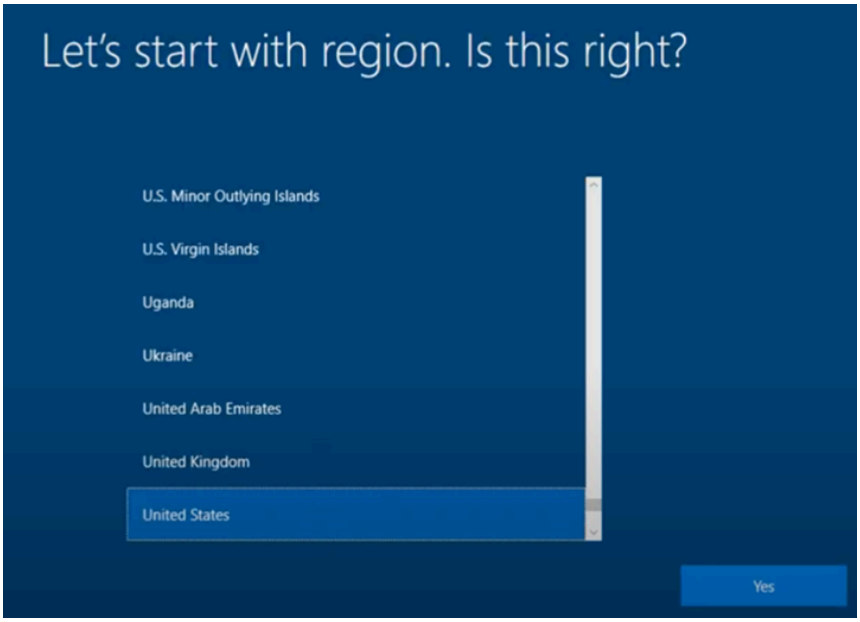
 ©2026 Palo Alto Networks, Inc.



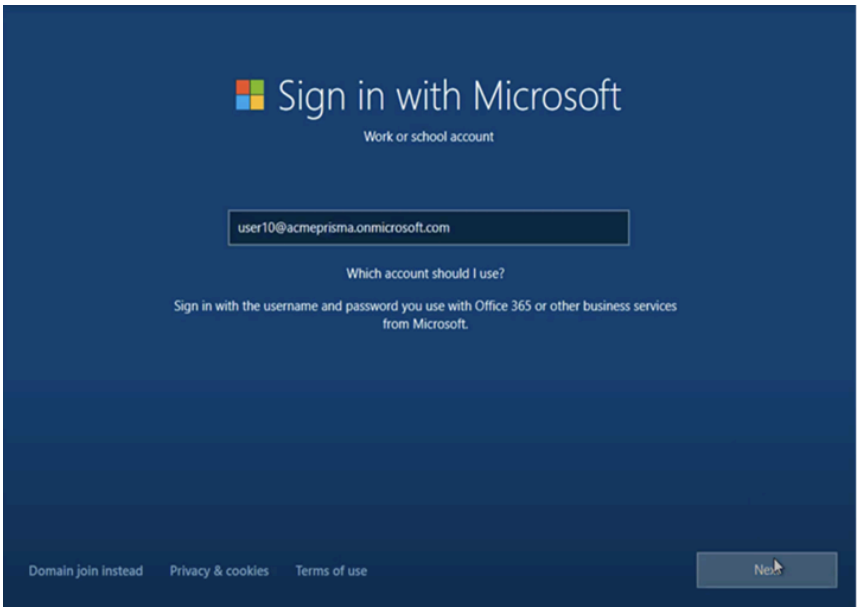
3. Assignez l'application au groupe que vous avez créé pour Autopilot.

 ©2026 Palo Alto Networks, Inc.

6. Vérifiez le processus de déploiement.
   1. Allumez le périphérique, qui se connectera automatiquement à Autopilot puis lancera l'expérience OOBE que vous avez personnalisée.



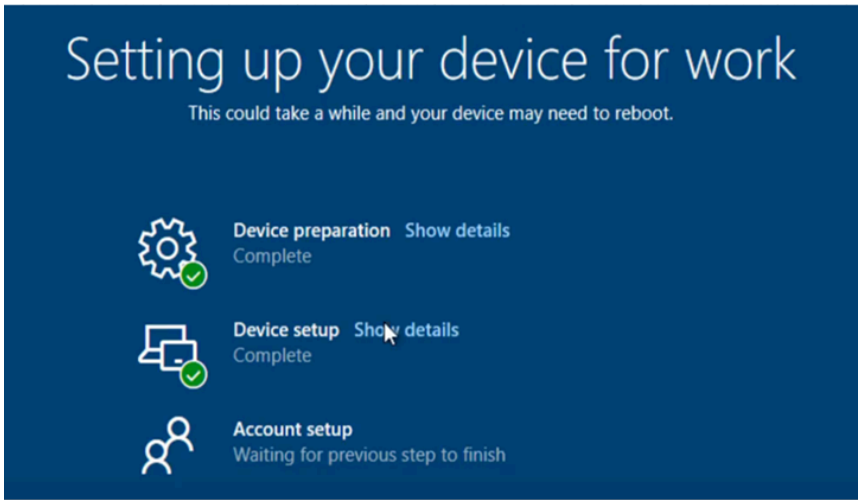
   2. Lorsque vous y êtes invité, ajoutez votre nom d'utilisateur pour identifier l'organisation à laquelle vous appartenez afin de pouvoir compléter l'enregistrement sur Autopilot.



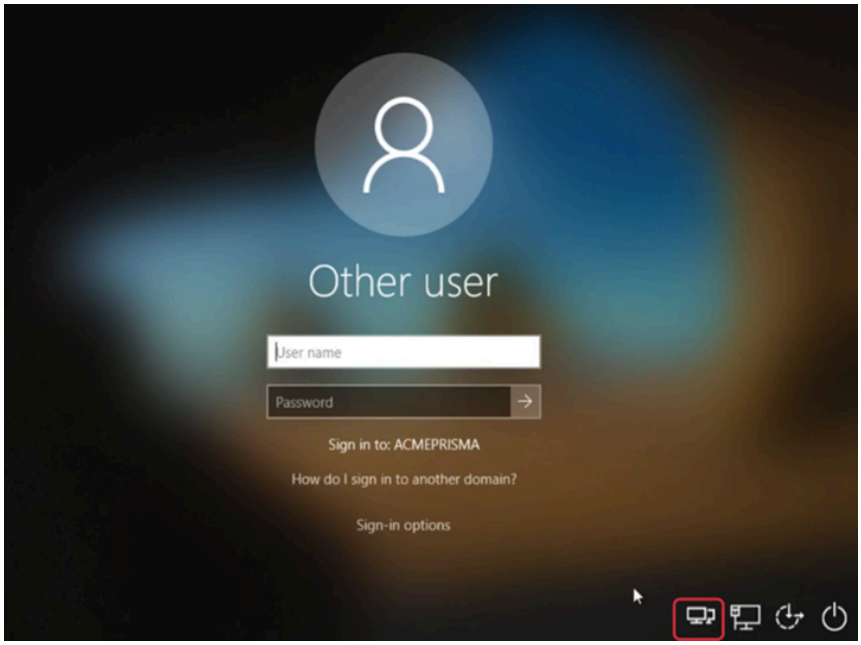
      Cela initie l'enregistrement sur Autopilot. Autopilot redémarre ensuite le système et invoque le profil Intune que vous avez créé et assigné au périphérique, ce qui commence le processus de déploiement de l'application GlobalProtect et des paramètres que vous avez définis pour spécifier le portail, définir le mode Se connecter avant identification, et les drapeaux de commande pour enregistrer GlobalProtect avec le

 ©2026 Palo Alto Networks, Inc.

fournisseur d'identifiants sur le périphérique, ainsi que toutes les autres applications et configurations que vous avez définies dans le profil Intune.

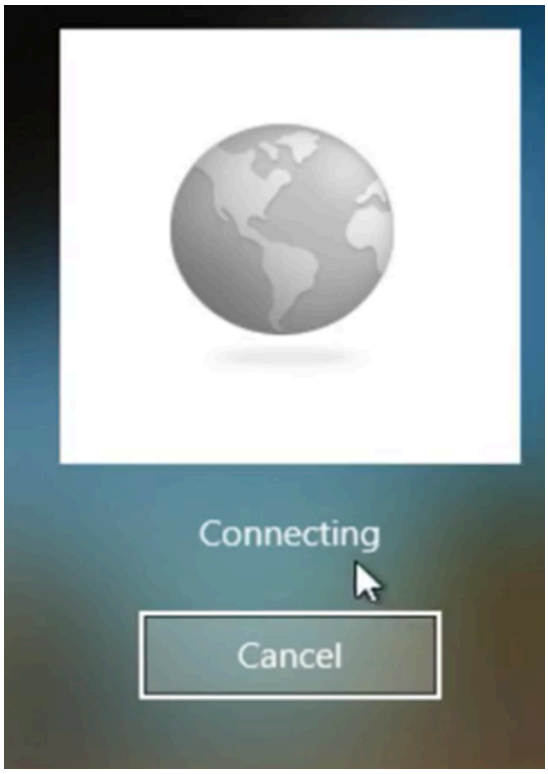


3. Après que les configurations et les applications ont été déployées sur le terminal, cliquez sur le bouton fournisseur d'accès pour pré-ouverture de session (PLAP) pour vous connecter à GlobalProtect et établir le tunnel.



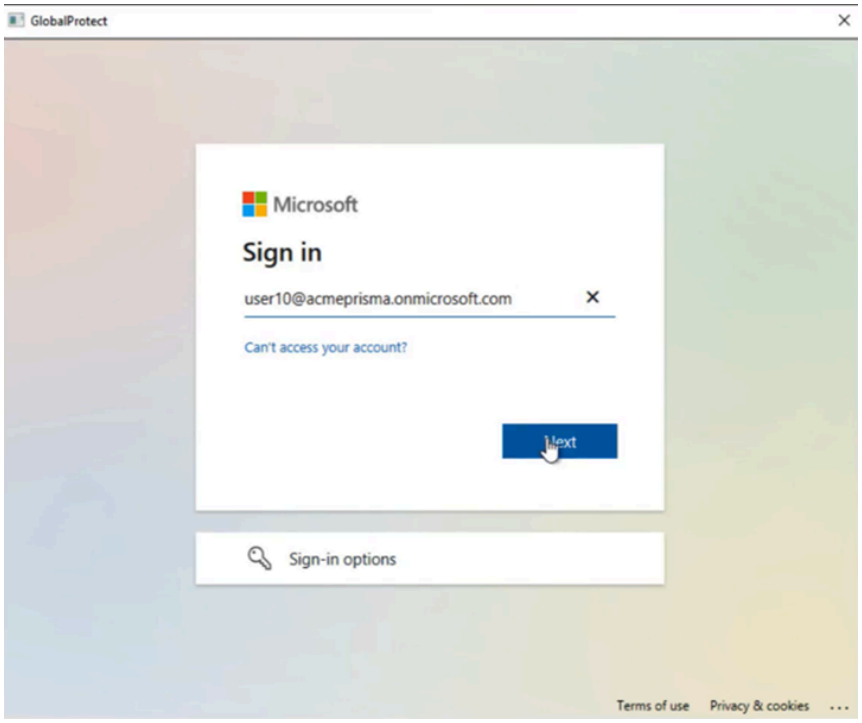
GlobalProtect commence à se connecter en utilisant le nom du portail que vous avez fourni dans votre script wrapper.

 ©2026 Palo Alto Networks, Inc.



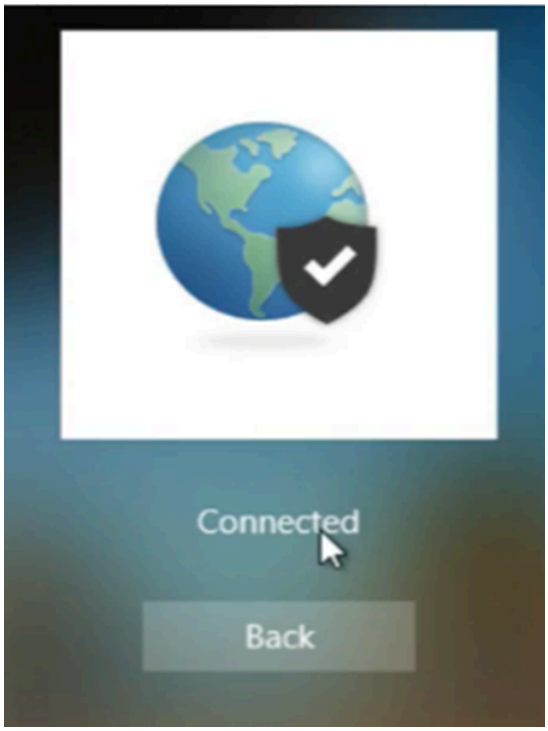
4. Après avoir établi avec succès le tunnel, GlobalProtect vous invite à vous connecter au fournisseur d'identifiants. Saisissez vos identifiants de domaine.

   Si vous utilisez SAML, GlobalProtect présente le navigateur intégré même si vous avez poussé des paramètres pour utiliser le navigateur par défaut. C'est parce que l'utilisateur n'est pas encore connecté.

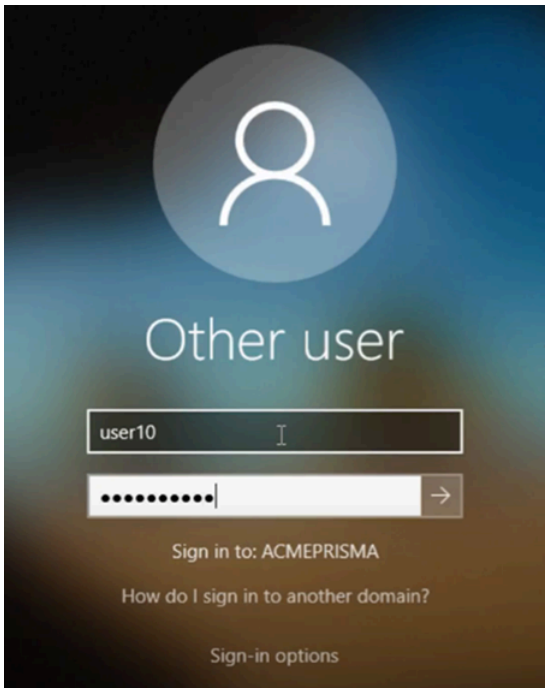


 ©2026 Palo Alto Networks, Inc.

5. Après une authentification réussie, l'écran GlobalProtect Connected s'affiche. Le périphérique dispose désormais de la connectivité requise pour atteindre le contrôleur de domaine et rejoindre le domaine. Cliquez sur **Back (Retour)**.

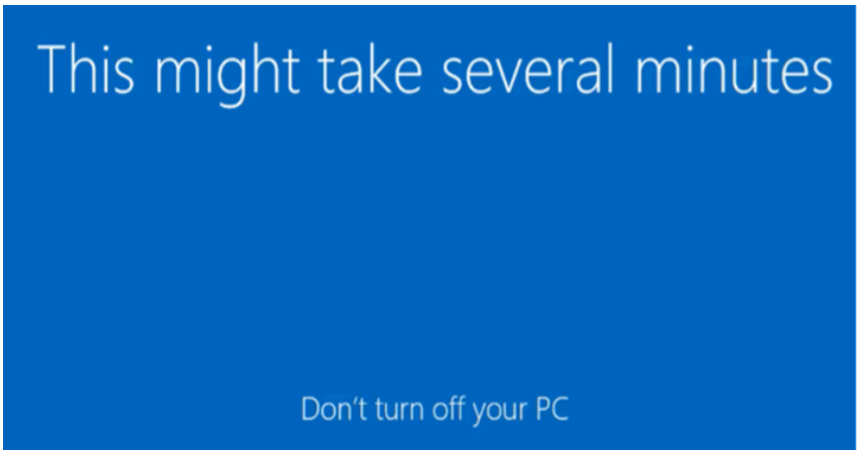


6. Entrez vos identifiants de connexion au domaine Windows pour vous connecter au périphérique et rejoindre le domaine.



7. Une fois l'authentification réussie à l'aide des informations d'identification du domaine, Autopilot termine la configuration du profil utilisateur.

 ©2026 Palo Alto Networks, Inc.



8. Vérifiez que GlobalProtect a bien été installé et que la politique est appliquée comme prévu.

   Examinez les journaux du trafic pour vous assurer que le périphérique respecte la politique de sécurité que vous avez configurée pour vos utilisateurs de GlobalProtect. Par exemple, dans les journaux ci-dessous, nous pouvons voir que user10@acmeprismaaccess.com respecte la règle qui permet aux utilisateurs mobiles qui passent le contrôle HIP d'accéder au réseau interne.

GENERATE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
07/25 19:09:22	end	trust	inter-fw	172.16.3.6	user10@acmepris...	10.4.11.9	389	ldap	allow	Allow Remote Networks Internal
07/25 18:55:37	end	trust	inter-fw	172.16.3.6	user10@acmepris...	10.4.11.9	389	ldap	allow	Allow Remote Networks Internal
07/25 18:43:52	end	trust	inter-fw	172.16.3.6	user10@acmepris...	10.4.11.9	389	ldap	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:41:02	end	trust	inter-fw	172.16.3.6	user10@acmepris...	10.4.11.9	123	ntp-base	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:40:42	end	trust	trust	172.16.3.6	user10@acmepris...	172.16.3.1	53	dns-base	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:40:42	end	trust	trust	172.16.3.6	user10@acmepris...	172.16.3.1	53	dns-base	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:40:02	end	trust	trust	172.16.3.6	user10@acmepris...	172.16.3.1	53	dns-base	allow	Allow Compliant HIP Mobile Users Internal
07/25 18:39:52	end	trust	trust	172.16.3.6	user10@acmepris...	172.16.3.1	53	dns-base	allow	Allow Compliant HIP Mobile Users Internal

Utiliser Autopilot pour déployer GlobalProtect en mode préouverture de session

En mode préouverture de session, l'application GlobalProtect établit le tunnel avant que l'utilisateur ne se connecte pour permettre l'accès à des ressources telles que vos contrôleurs de domaine. Avec ce déploiement, l'application GlobalProtect et le certificat requis pour la préouverture de session sont poussés vers le périphérique, permettant à GlobalProtect d'établir le tunnel nécessaire pour accéder au service d'authentification. Un élément clé de ce déploiement est que vous devez configurer l'infrastructure pour prendre en charge SCEP avec Intune afin de pousser un certificat d'ordinateur vers le nouveau périphérique Windows de l'utilisateur final pour une utilisation de GlobalProtect avec une préouverture de session. En plus du certificat d'ordinateur que le périphérique demandera à l'infrastructure SCEP de Microsoft, vous devrez également configurer Intune pour pousser l'application GlobalProtect et les paramètres de configuration pour la préouverture de session, la configuration pour rejoindre le domaine et les certificats de confiance pour le déchiffrement et l'authentification par certificat. Dans ce déploiement, le périphérique de l'utilisateur final est provisionné comme suit :

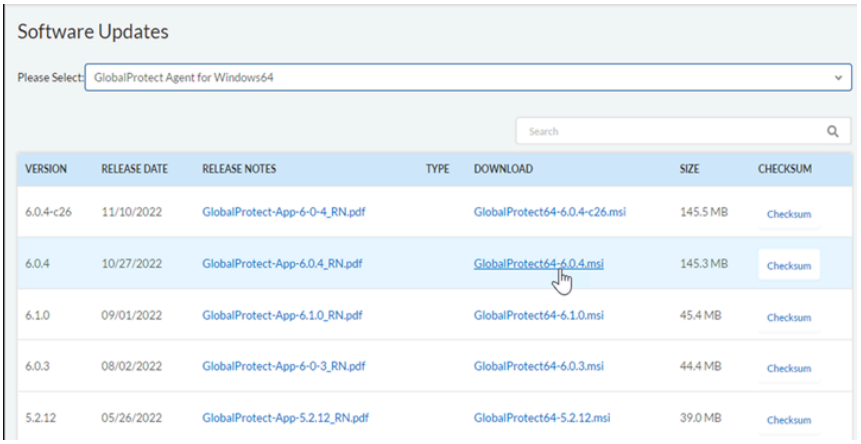
 ©2026 Palo Alto Networks, Inc.

1. Si vous ne l'avez pas déjà paramétré, configurez l'infrastructure pour prendre en charge SCEP avec Intune.

   Pour que ce déploiement fonctionne, vous devez configurer Microsoft Intune pour déployer un Simple Certificate Enrollment Protocol (protocole simple d'enregistrement de certificat - SCEP) sur le périphérique afin de permettre la connexion en préouverture de session à GlobalProtect. Vous devez utiliser la CA Microsoft pour déployer les certificats SCEP. Pour configurer cela, vous devez :

   - Installer la CA Microsoft sur le serveur Active Directory.
   - Sur un autre Windows Server,
     - Installer le connecteur de certificat pour Microsoft Intune
     - Configurez Windows Server où vous avez installé le connecteur de certificat avec le Service d'inscription des périphériques réseau (NDES).
     - Publiez le service NDES via le proxy d'application Azure AD.

2. Téléchargez le fichier MSI de l'application GlobalProtect depuis le Portail assistance clientèle de Palo Alto Networks.



3. Créez un script wrapper pour indiquer à Microsoft Intune comment installer GlobalProtect.

   Le script doit inclure les instructions suivantes :

   - Définir l'adresse du portail de sorte que l'utilisateur n'ait pas à la saisir (**PORTAL="*portal_name*"**)
   - Définir l'application pour utiliser le navigateur par défaut après la connexion initiale (**DEFAULTBROWSER="yes"**)
   - Définir la méthode de connexion sur Se connecter avant identification (**CONNECTMETHOD="pre-logon"**)
   - Clés de registre pour obtenir l'état de préouverture de session sur l'écran de connexion pour la première connexion

   Vous pouvez également utiliser des paramètres supplémentaires pour personnaliser le déploiement de l'application GlobalProtect. Voici un exemple de script wrapper que vous

 ©2026 Palo Alto Networks, Inc.

pouvez copier et modifier avec vos propres valeurs pour le nom du portail et le nom du fichier MSI :

```
$PortalAddress = 'myportal.gpcloudservice.com' $MSIFileName =
 'GlobalProtect64-6.0.4.msi' $MSISwitches = '/quiet /norestart'
 $ScriptPath = Split-Path -Path $MyInvocation.MyCommand.Path
 $InstallProcess = Start-Process -FilePath "msiexec" -ArgumentList
 ("/i " + [char]34 + $ScriptPath + "\" + $MSIFileName + [char]34
 PORTAL="myportal.gpcloudservice.com"" DEFAULTBROWSER=""yes""
 CONNECTMETHOD=""pre-logon"" New-Item -Path 'HKLM:\SOFTWARE\Palo
 Alto Networks\GlobalProtect\PanSetup' -Name 'PreLogonState' -
Force | Out-Null New-ItemProperty -Path 'HKLM\SOFTWARE\Palo Alto
 Networks\GlobalProtect\PanSetup\PreLogonState' -Name 'LogonFlag'
 -Value 0 -PropertyType Dword -Force | Out-Null New-ItemProperty
 -Path 'HKLM\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup
\PreLogonState' -Name 'LogonState' -Value 0 -PropertyType Dword
 -Force | Out-Null Write-Host ("Installation completed, exiting
 with last return code (" + $InstallProcess.ExitCode + ")") Exit
 $InstallProcess.ExitCode
```

4. Enregistrez les périphériques des utilisateurs finaux avec Autopilot et créez le groupe pour l'expérience Out of Box (OOBE) que vous créez pour déployer l'application GlobalProtect.

Reportez-vous à la documentation de Microsoft Windows Autopilot pour les instructions.

 ©2026 Palo Alto Networks, Inc.

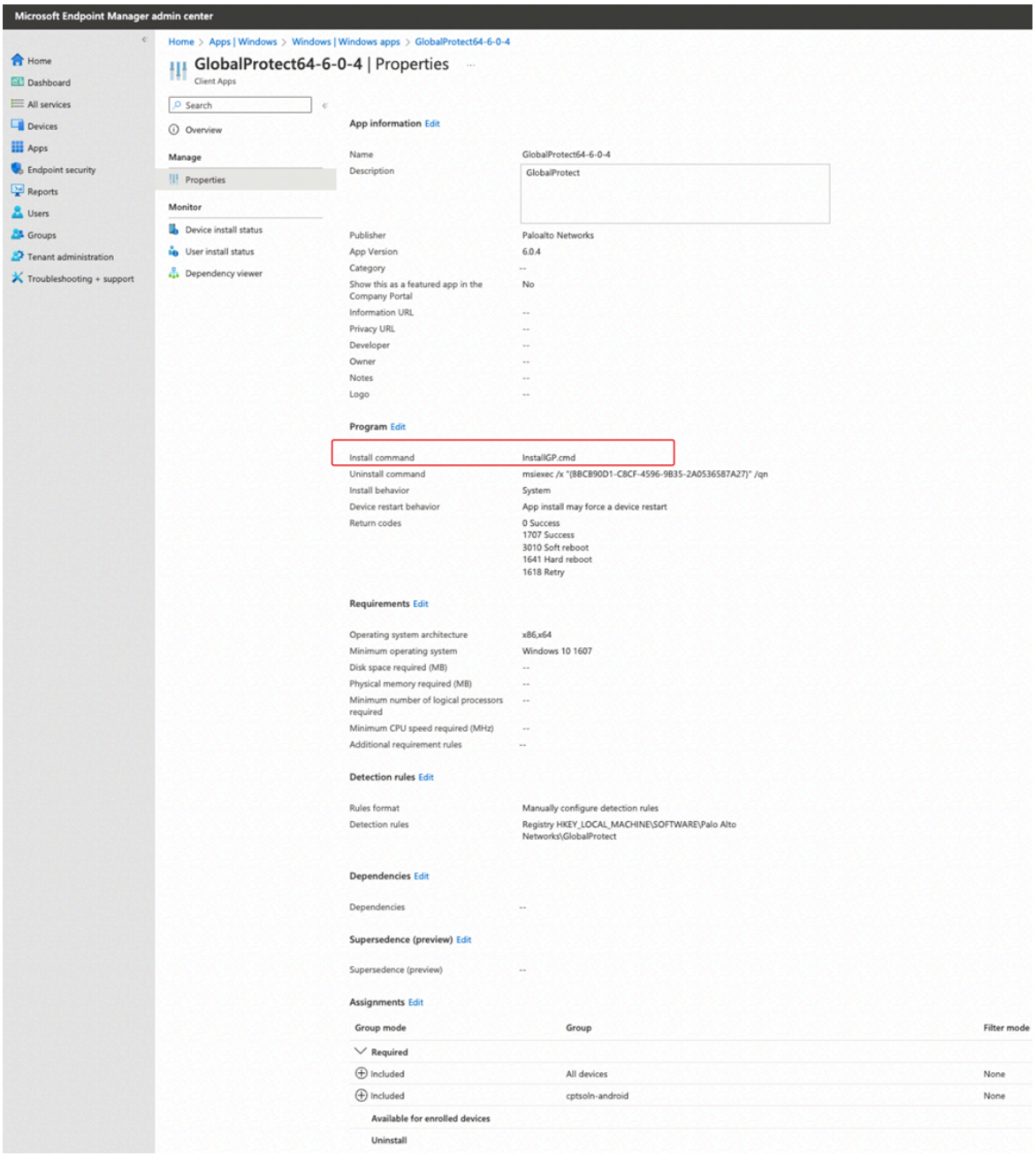
5. Créez le package d'installation de l'application GlobalProtect (le fichier MSI et les scripts) et téléchargez-le sur Microsoft Intune.
   1. Utilisez l'outil de préparation de contenu Microsoft Win32 pour créer le package de l'application.

      Par défaut, l'installateur se lance en mode 32 bits. Utilisez le script pour le convertir en mode 64 bits comme dans l'exemple suivant :

      ```
      IntuneWinAppUtil.exe -c C:\Temp\GlobalProtectPackage\Install -s
      GlobalProtect64-6.0.4.msi -o C:\Temp\GlobalProtectPackage\Output
      ```
   2. Téléchargez le package d'application sur Microsoft Intune.

      Assurez-vous que **Install command (Commande d'installation)** pointe vers le fichier batch que vous avez créé pour lancer le MSI en mode 64 bits.

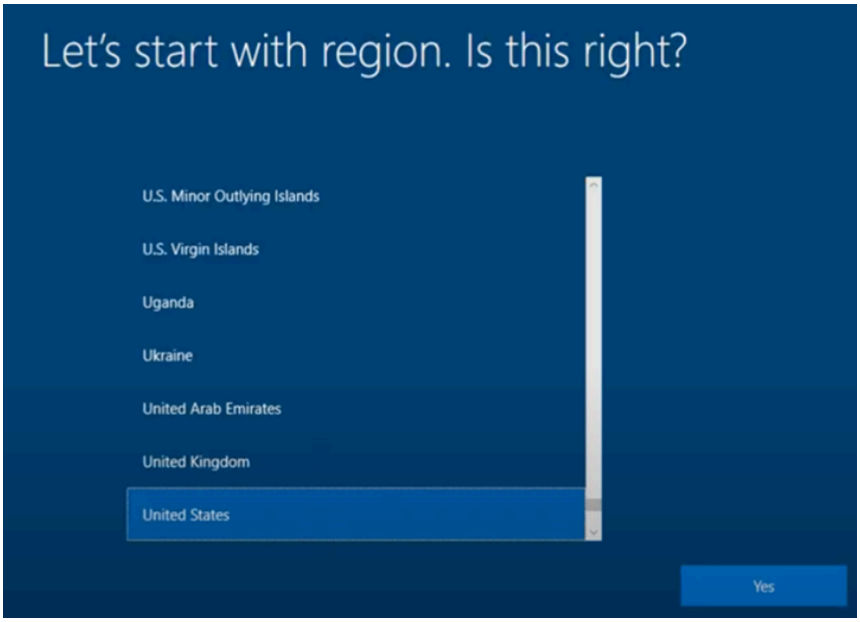
 ©2026 Palo Alto Networks, Inc.



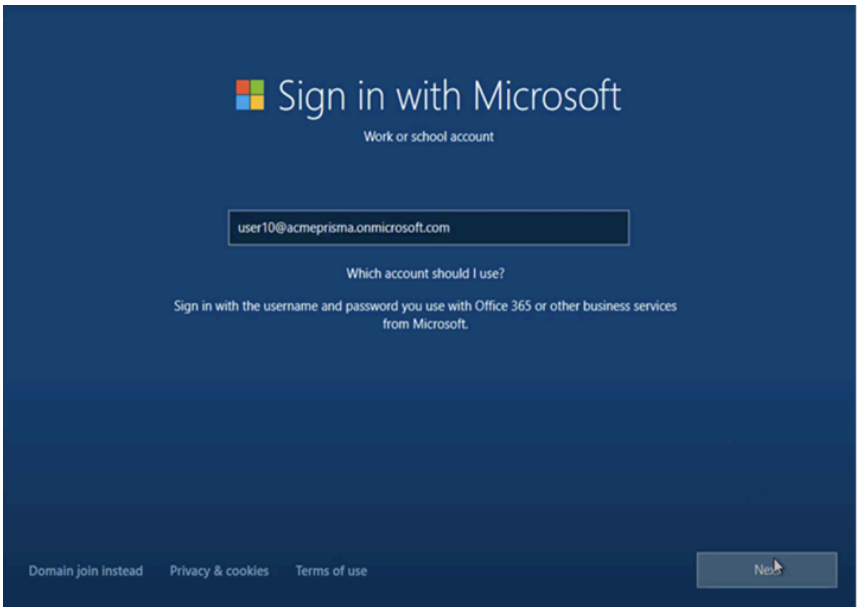
3. Assignez l'application au groupe que vous avez créé pour Autopilot.

 ©2026 Palo Alto Networks, Inc.

6. Vérifiez le processus de déploiement.
   1. Allumez le périphérique, qui se connectera automatiquement à Autopilot puis lancera l'expérience OOBE que vous avez personnalisée.



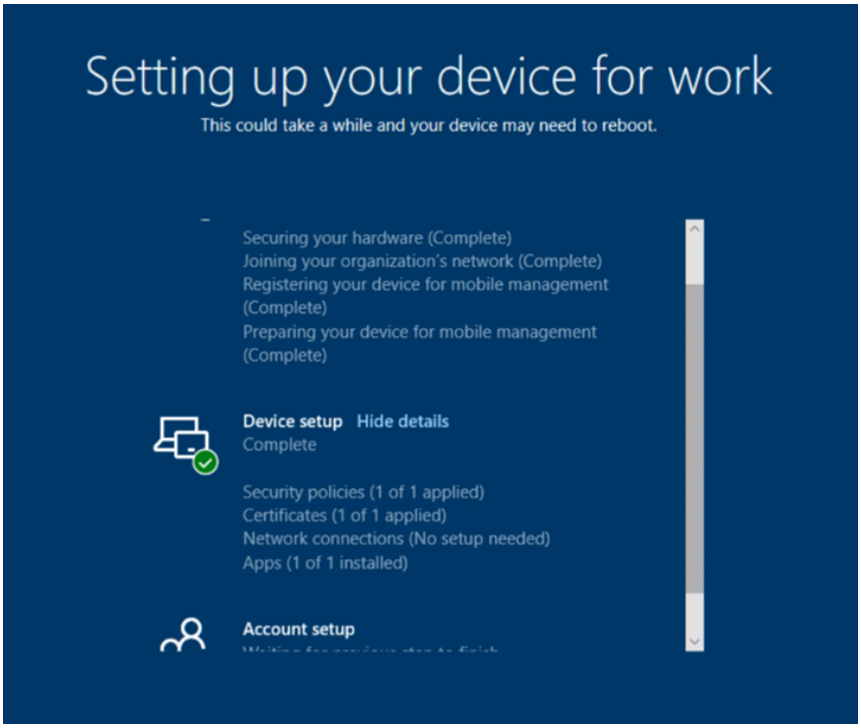
   2. Lorsque vous y êtes invité, ajoutez votre nom d'utilisateur pour identifier l'organisation à laquelle vous appartenez afin de pouvoir compléter l'enregistrement sur AutoPilot.



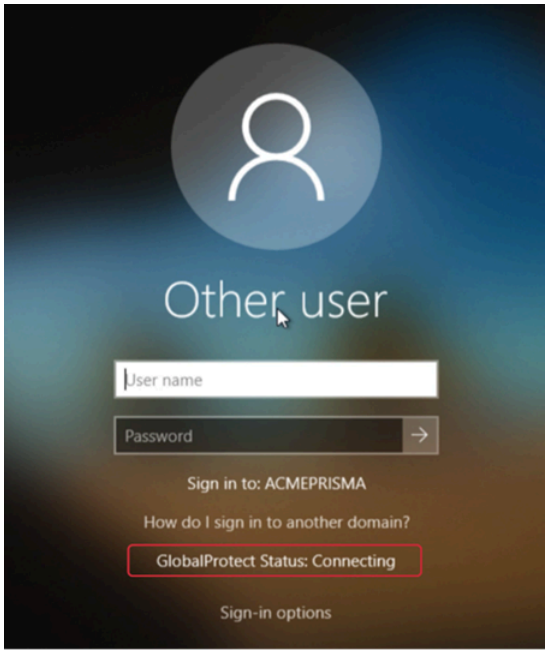
      Cela initie l'enregistrement sur Autopilot. Autopilot redémarre ensuite le système et invoque le profil Intune que vous avez créé et attribué au périphérique, ce qui commence le processus de déploiement de l'application GlobalProtect et des paramètres que vous avez définis pour spécifier le portail, définir le mode de préouverture de session, la configuration pour rejoindre le domaine et les certificats de confiance pour le

 ©2026 Palo Alto Networks, Inc.

déchiffrement et l'authentification par certificat, ainsi que toutes les autres applications et configurations que vous avez définies dans le profil Intune.

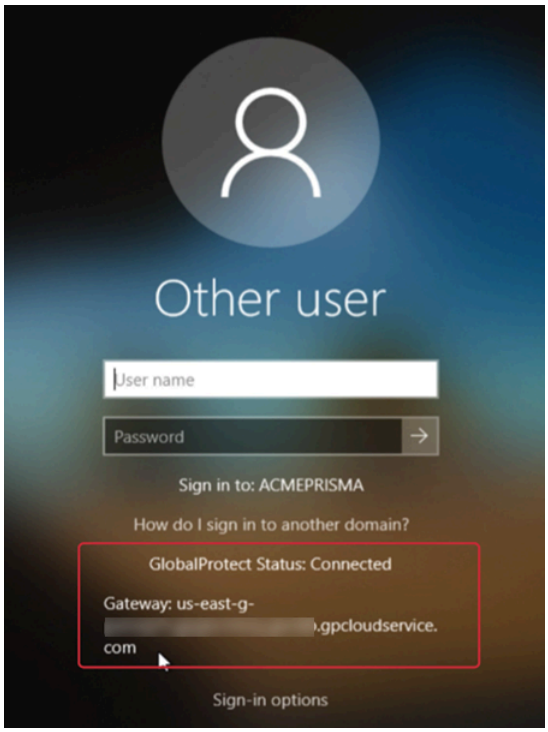


3. Après que les configurations et les applications ont été déployées sur le terminal, l'application GlobalProtect commence à se connecter automatiquement au portail que vous avez défini dans le script wrapper en utilisant la préouverture de session.

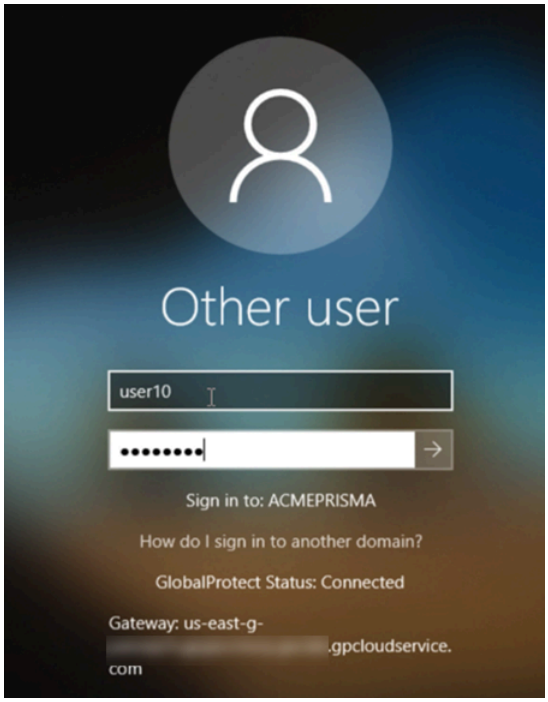


Une fois le tunnel établi, l'application affiche des informations sur la passerelle à laquelle vous êtes connecté.

 ©2026 Palo Alto Networks, Inc.

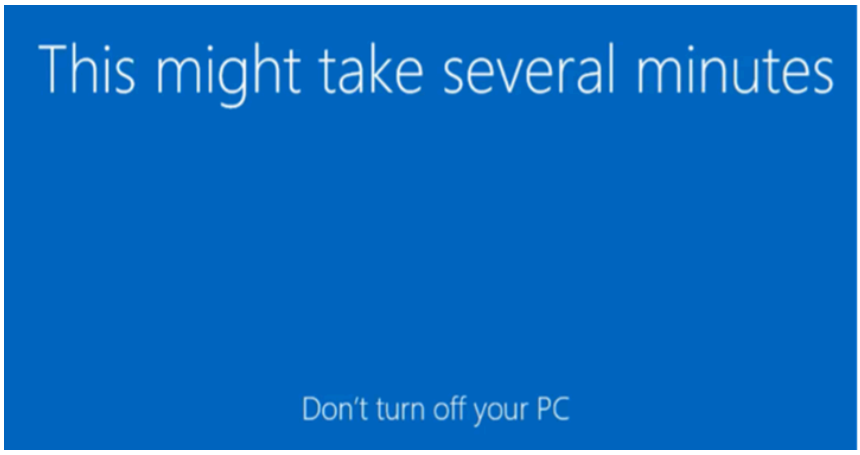


4. Une fois le tunnel établi, GlobalProtect vous invite à vous connecter à la machine. Saisissez vos informations d'identification de connexion.



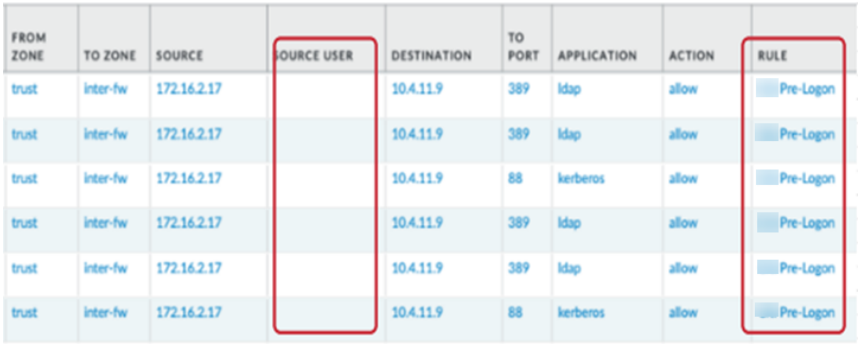
5. Une fois connecté, Autopilot termine la configuration du profil utilisateur.

 ©2026 Palo Alto Networks, Inc.



6. Vérifiez que GlobalProtect a bien été installé et que la politique est appliquée comme prévu.

   Examinez les journaux du trafic pour vous assurer que le périphérique respecte la politique de sécurité de préouverture de session que vous avez configurée pour vos utilisateurs GlobalProtect. Par exemple, dans les journaux ci-dessous, nous pouvons voir que le périphérique respecte la règle de préouverture de session qui permet l'accès aux ressources internes nécessaires à l'authentification.



FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
trust	inter-fw	172.16.2.17		10.4.11.9	389	ldap	allow	Pre-Logon
trust	inter-fw	172.16.2.17		10.4.11.9	389	ldap	allow	Pre-Logon
trust	inter-fw	172.16.2.17		10.4.11.9	88	kerberos	allow	Pre-Logon
trust	inter-fw	172.16.2.17		10.4.11.9	389	ldap	allow	Pre-Logon
trust	inter-fw	172.16.2.17		10.4.11.9	389	ldap	allow	Pre-Logon
trust	inter-fw	172.16.2.17		10.4.11.9	88	kerberos	allow	Pre-Logon

Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez déployer l'application GlobalProtect sur les points de terminaison gérés qui sont inscrits auprès de Microsoft Intune ou aux utilisateurs dont les points de terminaison ne sont pas inscrits auprès de Microsoft Intune (iOS uniquement). Après avoir déployé l'application, configurez et déployez un profil VPN sur les points de terminaison gérés pour configurer automatiquement l'application GlobalProtect pour les utilisateurs finaux.

 ©2026 Palo Alto Networks, Inc.

1. Inscrivez les terminaux auprès de Microsoft Intune.

   Pour déployer l'application GlobalProtect sur vos points de terminaison, assurez-vous que les points de terminaison sont inscrits auprès de Microsoft Intune.

2. Ajoutez l'application GlobalProtect à Microsoft Intune.

   Avant de pouvoir affecter l'application GlobalProtect à des utilisateurs ou à des points de terminaison, vous devez ajouter l'application à Microsoft Intune.

3. Définissez le type d'affectation pour l'application GlobalProtect.

   Vous pouvez déterminer qui a accès à l'application GlobalProtect en affectant l'application aux utilisateurs ou aux points de terminaison. Avant de pouvoir affecter l'application, vous devez définir le type d'affectation pour l'application. Le type d'affectation rend l'application disponible ou obligatoire ou désinstalle l'application.

4. Affectez l'application GlobalProtect à des utilisateurs ou à des terminaux spécifiques.

   Après avoir défini le type d'affectation pour l'application GlobalProtect, vous pouvez affecter l'application à des utilisateurs ou à des points de terminaison spécifiques.

   (iOS uniquement) Vous pouvez affecter l'application GlobalProtect aux utilisateurs dont les points de terminaison ne sont pas inscrits auprès de Microsoft Intune.

Configurer Microsoft Intune pour les terminaux UWP Windows 10

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect prend en charge des configurations VPN distinctes pour sécuriser le trafic des terminaux, dont un mode Toujours Actif et un Par Application. La configuration Toujours Actif maintient une connexion constante, forçant tout le trafic qui correspond aux filtres de passerelle prédéfinis (tels que des ports et adresses IP spécifiques) à passer par le tunnel sécurisé. A contrario, la configuration VPN Par Application, généralement activée pour les terminaux mobiles gérés utilisant une solution comme Microsoft Intune, fournit un contrôle granulaire en permettant uniquement aux applications gérées spécifiées d'acheminer le trafic via le tunnel VPN pour accéder aux ressources internes, tandis que tout le trafic des applications non gérées contourne le tunnel et se connecte directement à Internet.

Lorsqu'il est déployé avec Microsoft Intune pour les terminaux UWP Windows 10, GlobalProtect prend en charge les méthodes de connexion suivantes :

- Toujours actif

  Dans une configuration toujours active, GlobalProtect se connecte automatiquement dès que vous vous connectez.

 ©2026 Palo Alto Networks, Inc.

- Par application

  Dans une configuration par application, vous pouvez définir quelles applications gérées sont autorisées à acheminer le trafic via GlobalProtect. Pour ce faire, vous pouvez attacher un profil VPN à une application, ajouter des URL pour l'application à laquelle vous souhaitez accéder, ou faire une combinaison des deux.

Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez déployer l'application GlobalProtect sur les points de terminaison gérés qui sont inscrits auprès de Microsoft Intune ou aux utilisateurs dont les points de terminaison ne sont pas inscrits auprès de Microsoft Intune (iOS uniquement). Après avoir déployé l'application, configurez et déployez un profil VPN sur les points de terminaison gérés pour configurer automatiquement l'application GlobalProtect pour les utilisateurs finaux.

1. Inscrivez les terminaux auprès de Microsoft Intune.

   Pour déployer l'application GlobalProtect sur vos points de terminaison, assurez-vous que les points de terminaison sont inscrits auprès de Microsoft Intune.

2. Ajoutez l'application GlobalProtect à Microsoft Intune.

   Avant de pouvoir affecter l'application GlobalProtect à des utilisateurs ou à des points de terminaison, vous devez ajouter l'application à Microsoft Intune.

3. Définissez le type d'affectation pour l'application GlobalProtect.

   Vous pouvez déterminer qui a accès à l'application GlobalProtect en affectant l'application aux utilisateurs ou aux points de terminaison. Avant de pouvoir affecter l'application, vous devez définir le type d'affectation pour l'application. Le type d'affectation rend l'application disponible ou obligatoire ou désinstalle l'application.

4. Affectez l'application GlobalProtect à des utilisateurs ou à des terminaux spécifiques.

   Après avoir défini le type d'affectation pour l'application GlobalProtect, vous pouvez affecter l'application à des utilisateurs ou à des points de terminaison spécifiques.

   (iOS uniquement) Vous pouvez affecter l'application GlobalProtect aux utilisateurs dont les points de terminaison ne sont pas inscrits auprès de Microsoft Intune.

 ©2026 Palo Alto Networks, Inc.

Configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans une configuration de VPN toujours active, la connexion GlobalProtect sécurisée est toujours active. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est toujours acheminé via le tunnel VPN.

Utilisez les étapes suivantes pour configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide de Microsoft Intune :

1. Téléchargez l'app GlobalProtect pour Windows 10 UWP :
   - Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune.
   - Téléchargez l'application GlobalProtect directement à partir du Microsoft Store.
2. (Facultatif) Si votre déploiement exige une authentification basée sur les certificats, configurez un profil de certificat.
3. Créez un nouveau profil VPN Windows 10 UWP.
   - Définissez la **Platform (Plateforme)** sur **Windows 10 and later (Windows 10 et versions ultérieures)**.
4. Configurez les paramètres de la configuration VPN toujours active pour les terminaux Windows 10 UWP.
   - Définissez le **Connection type (Type de connexion)** sur **Palo Alto Networks GlobalProtect**.
   - Activez le VPN **Always On (Toujours actif)**.

Configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide de Microsoft Intune

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez autoriser l'accès aux ressources internes à partir de vos périphériques mobiles gérés en configurant l'accès VPN GlobalProtect à l'aide de Microsoft Intune. Dans une configuration VPN par application, vous pouvez indiquer les applications gérées qui peuvent acheminer le trafic

 ©2026 Palo Alto Networks, Inc.

via le tunnel VPN. Les applications non gérées continueront de se connecter directement par l'Internet plutôt que via le tunnel VPN.

Utilisez les étapes suivantes pour configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide de Microsoft Intune :

1. Téléchargez l'app GlobalProtect pour Windows 10 UWP :
   - Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune.
   - Téléchargez l'application GlobalProtect directement à partir du Microsoft Store.
2. Configurez un profil de certificat.

   Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.
3. Créez un nouveau profil VPN Windows 10 UWP.
   - Définissez la **Platform (Plateforme)** sur **Windows 10 and later (Windows 10 et versions ultérieures)**.
4. Configurez les paramètres de la configuration VPN par application pour les terminaux Windows 10 UWP.
   - Définissez le **Connection type (Type de connexion)** sur **Palo Alto Networks GlobalProtect**.
   - Dans la section Apps and Traffic rules (Règles d'applications et de trafic), définissez l'option **Associate WIP or apps with this VPN (Associer WIP ou des applications à ce VPN)** sur **Associate apps with this connection (Associer les applications à cette connexion)**. **Enable (Activez)** l'option afin de **Restrict VPN connection to these apps (Restreindre la connexion VPN à ces applications)**, puis **Add (Ajoutez)** les applications associées qui doivent utiliser la connexion VPN.

Gérer l'application GlobalProtect à l'aide de MobileIron

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

MobileIron est une plateforme de gestion de mobilité d'entreprise qui vous permet de gérer des points d'extrémité mobiles, à partir d'une console centrale. L'application GlobalProtect offre une connexion sécurisée entre le pare-feu et les points de terminaison mobiles gérés par MobileIron au niveau du périphérique ou de l'application. L'utilisation de GlobalProtect en tant que connexion sécurisée assure l'homogénéité de l'inspection du trafic et de l'application des règles de sécurité du réseau pour la prévention des menaces sur les points de terminaison mobiles.

Si vous n'utilisez pas de système MDM de tiers qualifié, vous pouvez Gérer l'application GlobalProtect à l'aide d'autres MDM tiers.

 ©2026 Palo Alto Networks, Inc.

Déployez l'application mobile GlobalProtect à l'aide de MobileIron

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez déployer l'app GlobalProtect vers des points de terminaison gérés qui sont inscrits à MobileIron. Après avoir déployé l'application, configurez et déployez un profil VPN pour configurer automatiquement l'application GlobalProtect pour l'utilisateur final.

1. Ajouter des utilisateurs à MobileIron.

   Avant que des utilisateurs puissent enregistrer leurs points de terminaison auprès de MobileIron, vous devez créer une entrée utilisateur pour chaque utilisateur.

2. (Facultatif) Affecter des utilisateurs à des groupes d'utilisateurs.

   Pour déployer l'application GlobalProtect selon une appartenance de groupes plutôt que selon des utilisateurs individuels, vous pouvez affecter des utilisateurs à des groupes d'utilisateurs distincts.

3. Inviter des utilisateurs à inscrire leurs points de terminaison auprès de MobileIron.

   Après que vous avez ajouté des utilisateurs à MobileIron, vous pouvez les inviter à inscrire leurs points de terminaison.

4. Ajouter l'application GlobalProtect au catalogue d'applications MobileIron.

   Le catalogue d'applications énumère les applications mobiles qui sont offertes à vos utilisateurs. Vous pouvez chercher l'application GlobalProtect dans un magasin public (comme l'App Store d'Apple) et l'ajouter ou charger l'application directement dans MobileIron en tant qu'application interne. Vous devez ensuite configurer les paramètres de distribution de l'application pour indiquer la manière dont l'application GlobalProtect sera installée et configurée sur les points de terminaison inscrits.

Configurer MobileIron pour les terminaux iOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

L'application GlobalProtect peut être déployée et configurée à l'aide de MobileIron pour les terminaux iOS pour fournir aux terminaux mobiles gérés un accès sécurisé aux ressources internes de l'entreprise.

 ©2026 Palo Alto Networks, Inc.

Lorsqu'il est déployé avec MobileIron pour les terminaux iOS, GlobalProtect prend en charge les méthodes de connexion suivantes :

- Toujours actif

  Dans une configuration toujours active, GlobalProtect se connecte automatiquement dès que vous vous connectez.
- À la demande (configuration VPN d'accès à distance initié par l'utilisateur)

  Dans une configuration à la demande, vous devez vous connecter manuellement à GlobalProtect via l'application. Le trafic est acheminé via l'application GlobalProtect uniquement après que vous ayez initié et établi la connexion.
- Par application

  Dans une configuration par application, vous pouvez définir quelles applications gérées sont autorisées à acheminer le trafic via GlobalProtect. Pour ce faire, vous pouvez attacher un profil VPN à une application, ajouter des URL pour l'application à laquelle vous souhaitez accéder, ou faire une combinaison des deux.

Configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide de MobileIron

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans une configuration de VPN toujours active, la connexion GlobalProtect sécurisée est toujours active. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est toujours acheminé via le tunnel VPN.

Utilisez les étapes suivantes pour configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide de MobileIron :

1. Téléchargement de l'application GlobalProtect pour Android
   - Déployez l'application mobile GlobalProtect à l'aide de MobileIron.
   - Téléchargez l'app GlobalProtect directement à partir de l'App Store.
2. (Facultatif) Si votre déploiement nécessite une authentification basée sur les certificats, ajoutez une configuration de certificat, puis configurez les paramètres du certificat.
3. Ajoutez une configuration de VPN toujours active.
   - Définissez le type de configuration sur **Always On VPN (Configuration VPN toujours active)**.
4. Configurez les paramètres de la configuration VPN toujours active pour iOS.

 ©2026 Palo Alto Networks, Inc.

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison iOS à l'aide de MobileIron

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans une configuration de VPN d'accès à distance (à la demande), les utilisateurs doivent lancer manuellement l'application pour établir la connexion GlobalProtect sécurisée. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est acheminé via le tunnel VPN seulement après que les utilisateurs ont initié et établi la connexion.

Utilisez les étapes suivantes pour configurer configuration de VPN d'accès à distance initié par l'utilisateur sur les terminaux iOS à l'aide de MobileIron :

1. Téléchargement de l'application GlobalProtect pour Android
   - Déployez l'application mobile GlobalProtect à l'aide de MobileIron.
   - Téléchargez l'app GlobalProtect directement à partir de l'App Store.
2. Ajoutez une configuration de certificat, puis configurez les paramètres du certificat.

   Toutes les configurations VPN à la demande doivent reposer sur l'authentification basée sur les certificats.
3. Ajoutez une configuration VPN à la demande (accès à distance.
   - Définissez le type de configuration sur **VPN On-Demand (VPN à la demande)**.
4. Configurez les paramètres de la configuration VPN à la demande pour iOS.
   - Définissez le **Connection Type (Type de connexion)** sur **Palo Alto Networks GlobalProtect**, puis configurez les paramètres connexes.

Configurer une configuration de VPN par application sur les points de terminaison iOS à l'aide de MobileIron

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez autoriser l'accès aux ressources internes à partir de vos périphériques mobiles gérés en configurant l'accès VPN GlobalProtect à l'aide de MobileIron. Dans une configuration VPN par application, vous pouvez indiquer les applications gérées qui peuvent acheminer le trafic via le

 ©2026 Palo Alto Networks, Inc.

tunnel VPN. Les applications non gérées continueront de se connecter directement par l'Internet plutôt que via le tunnel VPN.

Utilisez les étapes suivantes pour configurer une configuration par application sur les terminaux iOS à l'aide de MobileIron :

1. Téléchargement de l'application GlobalProtect pour Android
   - Déployez l'application mobile GlobalProtect à l'aide de MobileIron.
   - Téléchargez l'app GlobalProtect directement à partir de l'App Store.
2. Ajoutez une configuration de certificat, puis configurez les paramètres du certificat.

   Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.
3. Ajoutez une configuration de VPN par application.
   - Définissez le type de configuration sur **Per-app VPN (Configuration VPN par application)**.
4. Configurez les paramètres de la configuration VPN par application pour iOS.
   - Définissez le **Connection Type (Type de connexion)** sur **Palo Alto Networks GlobalProtect**, puis configurez les paramètres connexes.

Configurer MobileIron pour les terminaux Android

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez configurer GlobalProtect en mode Toujours Actif pour les terminaux Android en utilisant MobileIron. La configuration VPN Toujours Actif établit une connexion GlobalProtect persistante, acheminant en continu tout le trafic qui correspond aux filtres définis par la passerelle (comme le port et l'adresse IP) à via le tunnel sécurisé.

- Configurer une configuration de VPN toujours active sur les terminaux Android à l'aide de MobileIron

Configurer une configuration de VPN toujours active sur les terminaux Android à l'aide de MobileIron

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

Dans une configuration de VPN toujours active, la connexion GlobalProtect sécurisée est toujours active. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est toujours acheminé via le tunnel VPN.

Utilisez les étapes suivantes pour configurer une configuration de VPN toujours active sur les terminaux Android à l'aide de MobileIron :

1. Téléchargement de l'application GlobalProtect pour Android
   - Déployez l'application mobile GlobalProtect à l'aide de MobileIron.
   - Téléchargez l'app GlobalProtect directement à partir de Google Play.
2. (Facultatif) Si votre déploiement nécessite une authentification basée sur les certificats, ajoutez une configuration de certificat, puis configurez les paramètres du certificat.
3. Ajoutez une configuration de VPN toujours active.
   - Définissez le type de configuration sur **Always On VPN (Configuration VPN toujours active)**.
4. Configurez les paramètres de la configuration VPN toujours active pour Android.

Gérer l'application GlobalProtect à l'aide de la console Google Admin

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

La console Google Admin est une plateforme de gestion de mobilité d'entreprise basée sur le nuage qui vous permet de gérer Chromebooks à partir d'une console centrale. L'application GlobalProtect offre une connexion sécurisée entre le pare-feu et les Chrombooks gérés par la console Google Admin au niveau du périphérique ou de l'application. L'utilisation de GlobalProtect en tant que connexion sécurisée assure l'homogénéité de l'inspection du trafic et de l'application des règles de sécurité du réseau pour la prévention des menaces sur les points de terminaison mobiles.

Si vous n'utilisez pas de système MDM de tiers qualifié, vous pouvez Gérer l'application GlobalProtect à l'aide d'autres MDM tiers.

 ©2026 Palo Alto Networks, Inc.

Déployer l'application GlobalProtect pour Android sur les Chromebooks gérés à l'aide de la console Google Admin

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

La console Google Admin vous permet de gérer les paramètres et les applications Chromebook à partir d'un emplacement central et basé sur le Web. Vous pouvez déployer l'application GlobalProtect pour Android sur les Chromebook gérés et configurer les paramètres VPN associés à partir de la console.

Pour configurer automatiquement l'application pour l'utilisateur, vous pouvez éventuellement utiliser la console Google Chromebook Management pour configurer et déployer les paramètres aux appareils Chrome gérés. Vous pouvez utiliser la console Google Admin pour gérer les paramètres et les applications Chromebook.

Suivez ces recommandations pour déployer l'application GlobalProtect pour Android sur les Chromebook gérés :

- *Vous ne pouvez transmettre aux appareils qui utilisent la console Google Admin un certificat unique à des fins d'authentification.*
- *À partir de votre Chromebook, appuyez sur **CTRL+ALT+T** pour ouvrir la ligne de commande du terminal. Utilisez la commande `route` pour afficher les itinéraires qui sont installés sur le périphérique. Vous pouvez décider d'inclure les itinéraires d'accès pour la séparation du tunnel.*
- *Bien souvent les applications utilisent des formats de fichiers différents, c'est pourquoi vous pouvez utiliser OpenSSL pour convertir les certificats du format PKCS #12 au format Base64. Utilisez la commande `openssl base64 -A -in` <certificate-in-p12-format> `-out` <cert.txt>.*

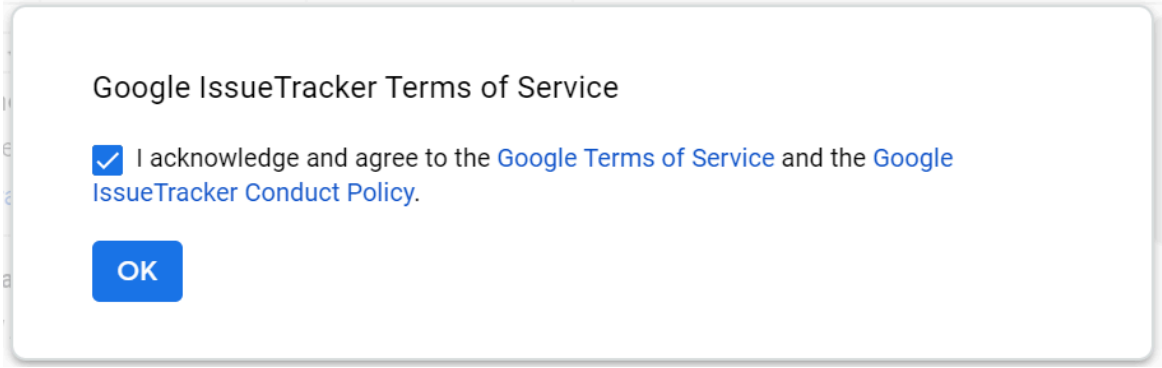
Utilisez les étapes suivantes pour déployer l'application GlobalProtect pour Android sur les Chromebook gérés à l'aide de la console Google Admin :

1. Avant de commencer :
   - Configurez les passerelles GlobalProtect pour qu'elles prennent en charge l'application GlobalProtect pour Android sur des Chromebook gérés. Reportez-vous à la section Configurer une passerelle GlobalProtect.
   - Configurez le portail et personnalisez l'application GlobalProtect pour Android sur des Chromebook gérés. Vous devez configurer au moins une passerelle à laquelle l'application GlobalProtect peut se connecter. Reportez-vous à la section Paramétrer l'accès au portail GlobalProtect. Reportez-vous à la grille de compatibilité Palo Alto Networks pour obtenir une liste des fonctionnalités prises en charge pour Android sur Chrome.
   - (Recommandé) Pour faciliter l'authentification, activez le SSO SAML pour l'application GlobalProtect pour Android sur les Chromebook. Nous vous recommandons d'établir le SSO SAML pour permettre aux utilisateurs de se connecter automatiquement après s'être

 ©2026 Palo Alto Networks, Inc.

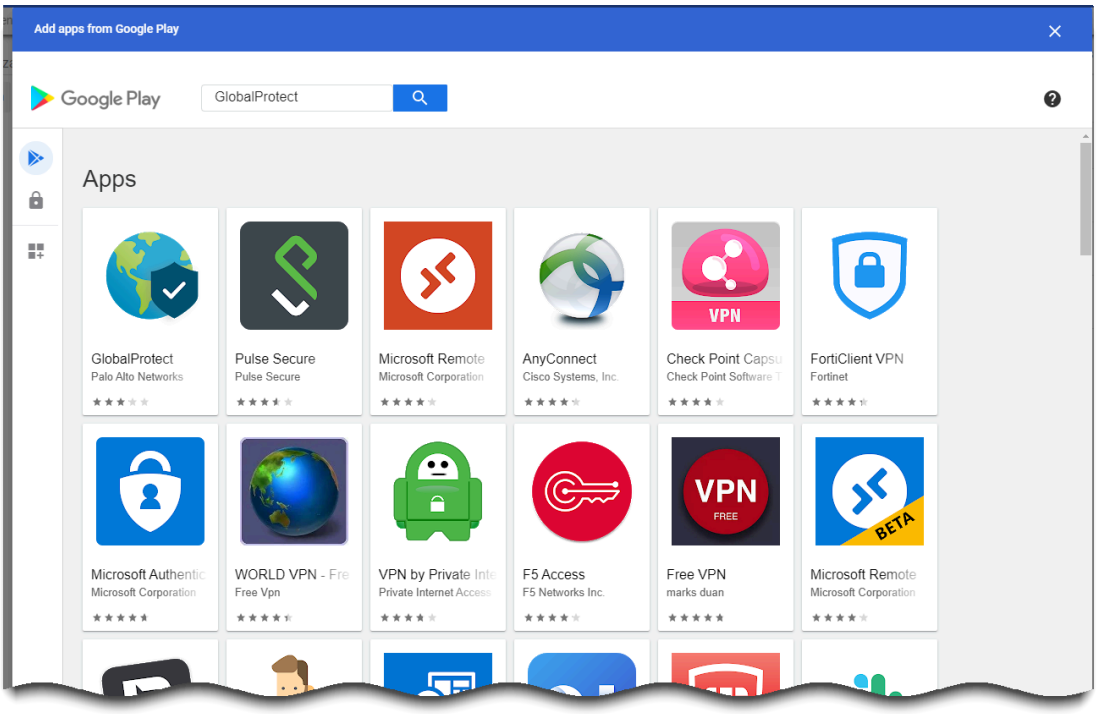
connectés au Chromebook sans avoir à saisir de nouveau les informations d'identification dans l'application GlobalProtect. Les utilisateurs ont ainsi accès à la sécurité toujours activée. Reportez-vous à la section Configurer l'authentification SAML.

- Lorsque les utilisateurs se connectent pour la première fois à GlobalProtect sur Android au moyen d'un Chromebook géré, il faut confirmer le message de notification de suppression VPN suivant avant que le tunnel soit établi :



 ©2026 Palo Alto Networks, Inc.

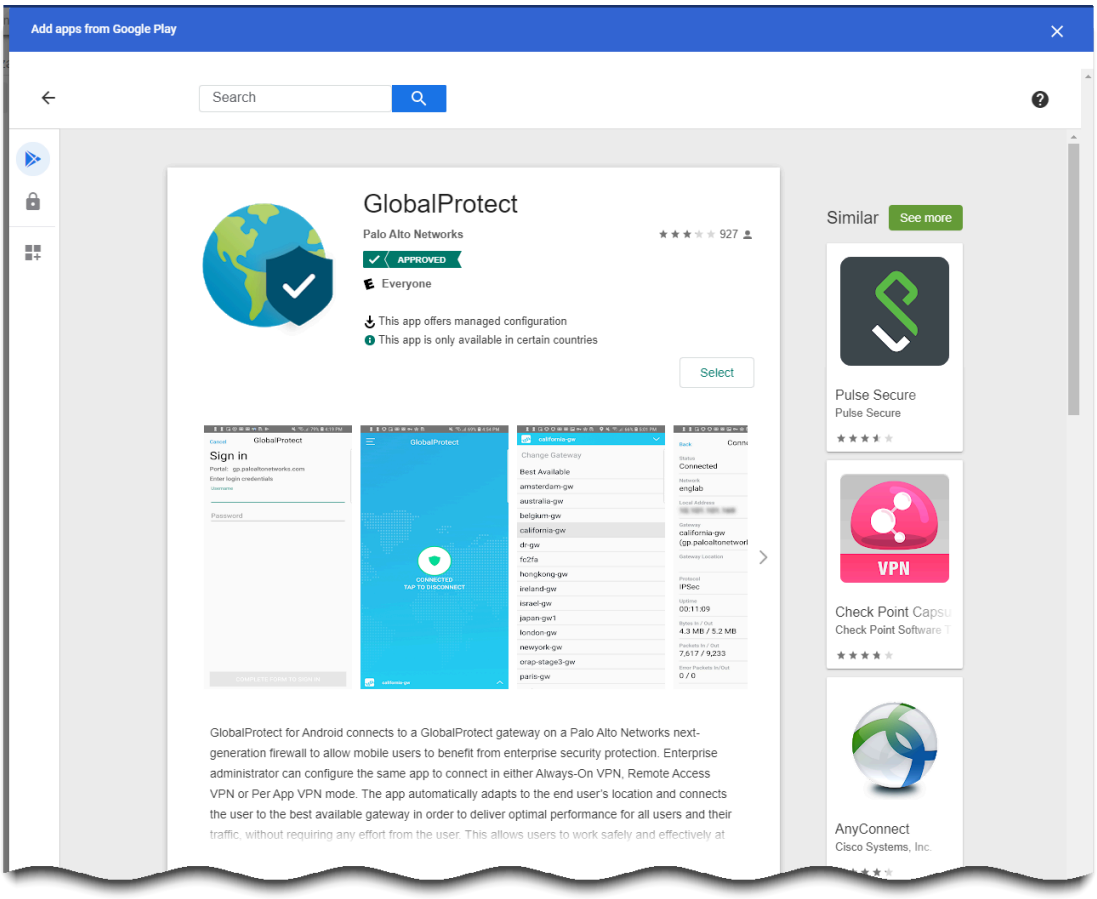
2. Approuvez l'application GlobalProtect pour les utilisateurs Chromebook.
   1. Connectez-vous à la console Google Admin en tant qu'administrateur.
   2. À partir de la console, sélectionnez **Gestion des appareils** > **Gestion de Chrome** pour afficher et modifier les paramètres de gestion de Chrome.
   3. Sélectionnez **Applications et extensions**.
   4. Dans la section Applications et extensions, cliquez sur le lien **page consacrée aux paramètres de l'application**.
   5. Cliquez sur le bouton d'ajout ( ) pour ajouter GlobalProtect à la liste des applications pour Android approuvées du Google Playstore.
   6. Lors du lancement du magasin Google Play, cherchez **`GlobalProtect`**, puis cliquez sur l'icône de l'application GlobalProtect.



   7. Cliquez sur **Sélectionner** pour ajouter l'application GlobalProtect.

      Un message s'affiche si l'application GlobalProtect est ajoutée avec succès.

 ©2026 Palo Alto Networks, Inc.



3. Déterminez la façon dont l'application GlobalProtect est installée sur les Chromebook.

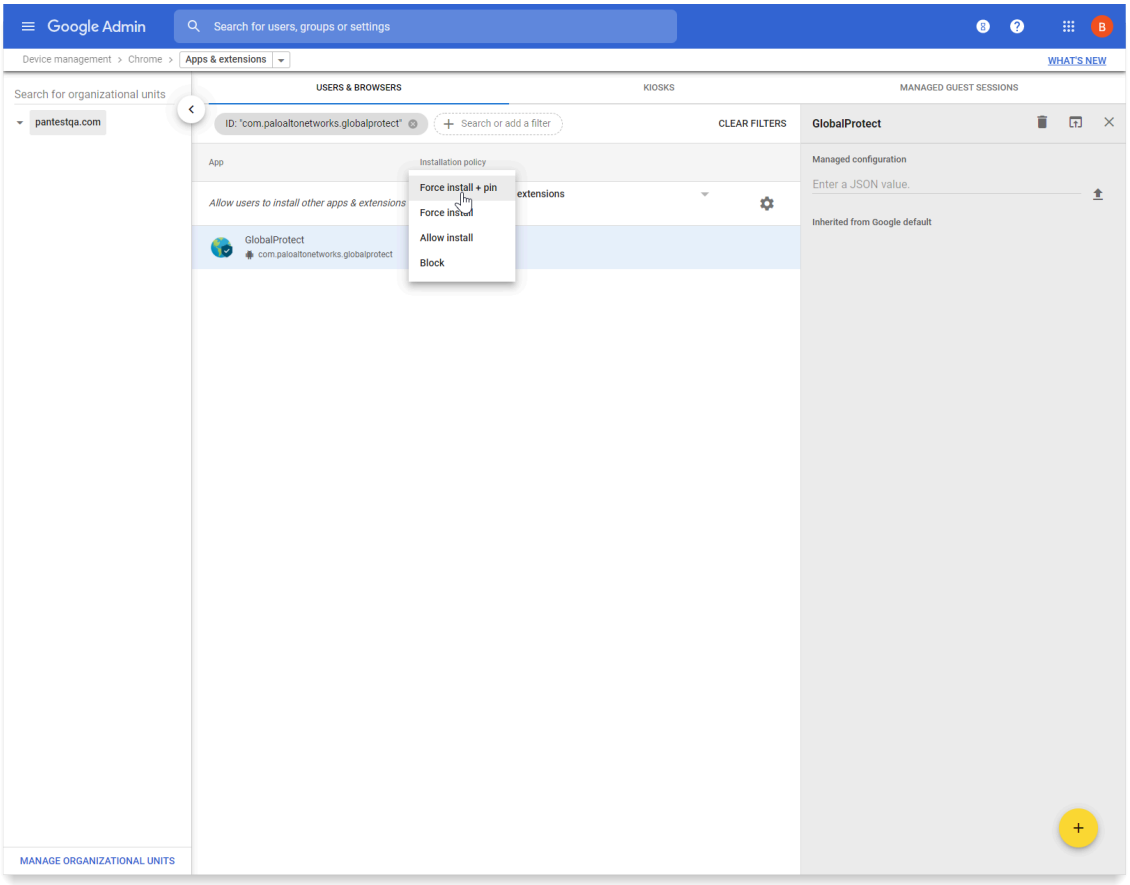
Après avoir approuvé l'application GlobalProtect, vous devez spécifier la manière dont l'application est installée sur les Chromebook. Pour empêcher les utilisateurs de contourner GlobalProtect en désinstallant l'application, forcez tous les Chromebook à installer l'application GlobalProtect automatiquement lorsque les utilisateurs se connectent à leur Chromebook.

1. À partir des paramètres de gestion des extensions de applications (**Gestion des appareils** > **Chrome** > **Applications et extensions**), sélectionnez **GlobalProtect** dans la liste des applications.
2. Sélectionnez votre unité organisationnelle dans la liste qui se trouve sur le côté gauche de la page.
3. Sélectionnez l'une des options suivantes :
   - Recommandé**Installation forcée + épingler** : active l'application GlobalProtect dont l'installation a été forcée et l'épingle à la barre des tâches. Si vous avez sélectionné cette option, les utilisateurs n'auront pas l'option de se déconnecter de l'application.
   - **Installation forcée** utilisez cette option si vous voulez vous assurer que l'application GlobalProtect est automatiquement installée sur chaque Chromebook lorsque les utilisateurs se connectent à leurs Chromebook. Pour empêcher les utilisateurs de désinstaller l'application GlobalProtect et de contourner les exigences en matière de sécurité et de conformité, vous appliquez l'option **Installation forcée**. Si vous avez

 ©2026 Palo Alto Networks, Inc.

sélectionné cette option, les utilisateurs n'auront pas l'option de se déconnecter de l'application.

- **Autoriser l'installation** : installez cette application manuellement à partir du Google Playstore. Cette option permet aux utilisateurs de désinstaller l'application GlobalProtect de leurs Chromebook.
- **Bloquer** : empêchez les utilisateurs d'installer cette application.



4. **SAVE (Sauvegardez)** vos modifications.

4. Appliquez une configuration gérée à l'application GlobalProtect.

Si vous avez activez l'installation forcée de l'application GlobalProtect, vous pouvez appliquer un fichier de configuration géré à l'application. Le fichier de configuration géré contient des valeurs pour les paramètres d'applications configurables.

1. À partir des paramètres de gestion des applications (**Gestion des appareils** > **Gestion de Chrome** > **Applications et extensions**), sélectionnez **GlobalProtect** dans la liste des applications.
2. Sélectionnez votre unité organisationnelle dans la liste qui se trouve sur le côté gauche de la page.
3. Cliquez sur l'icône **Charger à partir du fichier** qui se trouve du côté droit de la page pour sélectionner et charger votre fichier de configuration géré. Vous pouvez également saisir

 ©2026 Palo Alto Networks, Inc.

le nom de la valeur de la clé au format JSON, comme le montre la configuration type suivante.

```
{ "portal": "acme.portal.com", "username": "user123" }
```

Le tableau suivant présente un exemple des paramètres contenus dans le fichier de configuration géré. Pour connaître les paramètres qui sont pertinents pour votre entreprise, veuillez contacter votre administrateur informatique.

Paramètre	Description	Type de valeur	Exemple
portal	Adresse IP ou nom de domaine complet (FQDN) du portail.	Chaîne	**acme.portal.com**
nom d'utilisateur	Nom d'utilisateur pour l'authentification de portail.	Chaîne	**user123**
password	Mot de passe pour l'authentification de portail.	Chaîne	**password123**
client_certificate	Certificat client pour l'authentification de portail.	Chaîne (en Base 64)	**DAFDSaweEWQ23wDSAFD…**
client_certificate _passphrase	Phrase secrète du certificat client pour l'authentification de portail.	Chaîne	**PA$$W0RD$123**
app_list	Commencez la chaîne par le mot clé de la **allowlist (liste d'autorisation)** ou de la **(liste de blocage)** suivie de deux-points, et faites-la suivre par un tableau de noms d'applications séparés par des points-virgules. Liste de blocage ou liste d'autorisation qui vous permet de contrôler le trafic d'application qui peut traverser le tunnel VPN dans une	Chaîne	**allowlist | blacklist: com.google.calendar; com.android.email; com.android.chrome**

 ©2026 Palo Alto Networks, Inc.

Paramètre	Description	Type de valeur	Exemple
	configuration de VPN par application.		
connect_method	Méthode de connexion VPN	Chaîne	**user-logon | on-demand**
mobile_id	Identifiant unique utilisé pour identifier les points de terminaison mobiles, selon la configuration d'un système MDM tiers.	Chaîne	**5188a8193be43f42d332dde5cb2c941e**
remove_vpn_config_via_restriction	Indicateur pour la suppression de la configuration VPN.	Booléenne	**vraie| fausse**
allow_vpn_bypass	Indicateur autorisant le trafic de l'application à contourner le tunnel VPN.	Booléenne	**vraie| fausse**
cert_alias	Nom unique utilisé pour identifier le certificat client lors de l'authentification au portail ou à la passerelle.	Chaîne	**Client utilisateur de l'entreprise**
managed	Indicateur indiquant si le périphérique est inscrit auprès d'un serveur MDM.	Booléenne	**vraie| fausse**
ownership	Catégorie d'appartenance de l'appareil (par exemple, **appartient à l'employé**).	Chaîne	**byod**
compliance	État de conformité qui indique si l'appareil est conforme aux politiques de conformité que vous avez définies.	Chaîne	**yes**

©2026 Palo Alto Networks, Inc.

Paramètre	Description	Type de valeur	Exemple
Etiquette	les tags vous permettent d'identifier les appareils. Chaque tag doit être séparée par une virgule.	Chaîne	**`Compte invité, bureau satellite`**

4. **SAVE (Sauvegardez)** vos modifications.

5. Appliquez les politiques sur l'application GlobalProtect pour Android sur les Chromebook gérés.
   - Créez des objets HIP à l'aide des **infos sur l'hôte** qui sont propres à Android sur les Chromebook gérés. Puis, utilisez-les comme conditions de correspondance dans les HIP (profils d'informations sur l'hôte).
   - Appliquez la politique de sécurité correspondante à l'aide d'un profil HIP comme condition de correspondance dans une règle de politique. L'application collecte par défaut des données sur les catégories d'informations pour permettre d'identifier l'état de sécurité de l'hôte.

Configurer la console d'administration Google pour les terminaux Android

Les Chromebook prennent en charge la configuration VPN toujours active via le soutien étendu de l'application GlobalProtect pour Android. Dans une configuration de VPN toujours active, la connexion GlobalProtect sécurisée est toujours active. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est toujours acheminé via le tunnel VPN. En permettant à vos utilisateurs finaux d'exécuter l'application GlobalProtect pour Android sur leurs Chromebook, vous pouvez vous assurer qu'ils sont toujours connectés à GlobalProtect et qu'ils ont accès à une sécurité toujours active.

- *L'application GlobalProtect pour Android n'est prise en charge que sur certains Chromebook.*
- *Les Chromebook qui ne prennent pas en charge les applications Android doivent continuer d'utiliser l'application GlobalProtect pour Chrome. Cependant, ces Chromebook ne prendront pas en charge le VPN toujours actif.*
- *Si l'application GlobalProtect pour Android est installée sur un Chomebook pour utiliser la capicité VPN toujours actif, l'application GlobalProtect pour Chrome ne doit pas être installée sur le même Chromebook.*

Utilisez les étapes suivantes pour configurer une configuration de VPN toujours active sur les Chromebook à l'aide de la console Google Admin.

Suivez les étapes suivantes pour déployer l'application GlobalProtect pour Android sur les Chromebook gérés à l'aide de la console Google Admin. À l'heure actuelle, Workspace ONE ne prend pas en charge les configurations VPN toujours actif pour l'application GlobalProtect pour Android sur des Chromebook gérés.

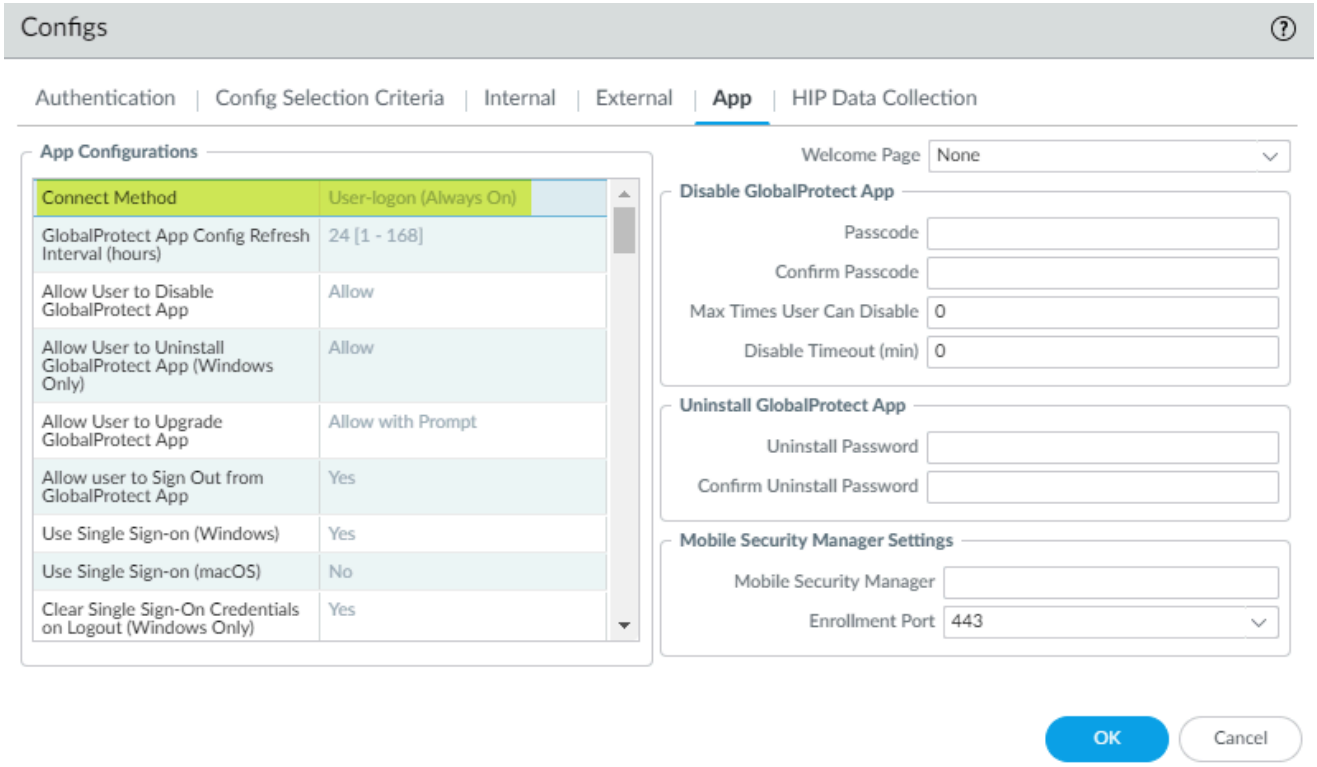
1. À partir de votre pare-feu Palo Alto Networks, Paramétrer l'accès au portail GlobalProtect.

2. Définir les configurations de l'agent GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

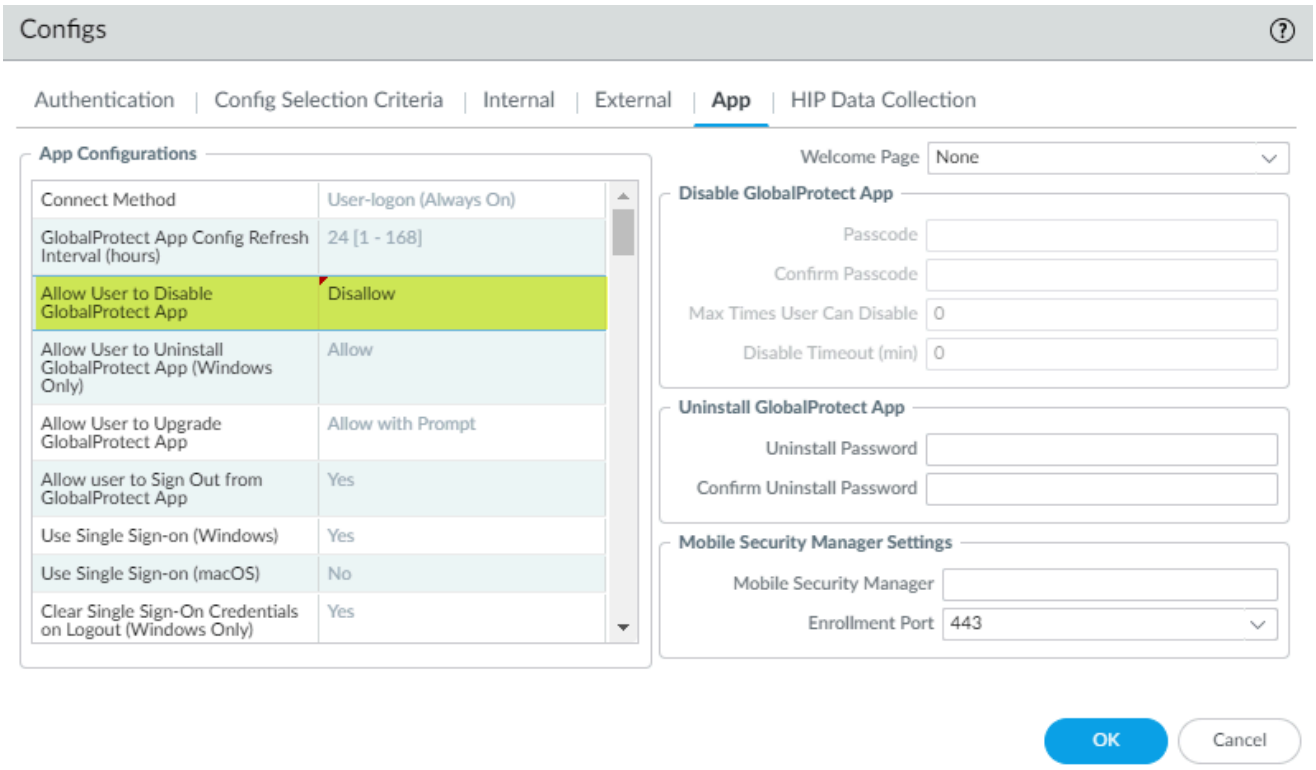
3. Personnaliser l'application GlobalProtect.

- Pour configurer la connexion à GlobalProtect pour qu'elle soit toujours active, définissez la **Connect Method (Méthode de connexion)** sur **User-logon (Always On) (Ouverture de session utilisateur [Toujours active])**.



- Pour empêcher les utilisateurs de désactiver l'application GlobalProtect, définissez l'option **Allow User to Disable GlobalProtect App (Autoriser l'utilisateur à désactiver l'application GlobalProtect)** sur **Disallow (Interdire)**.

 ©2026 Palo Alto Networks, Inc.

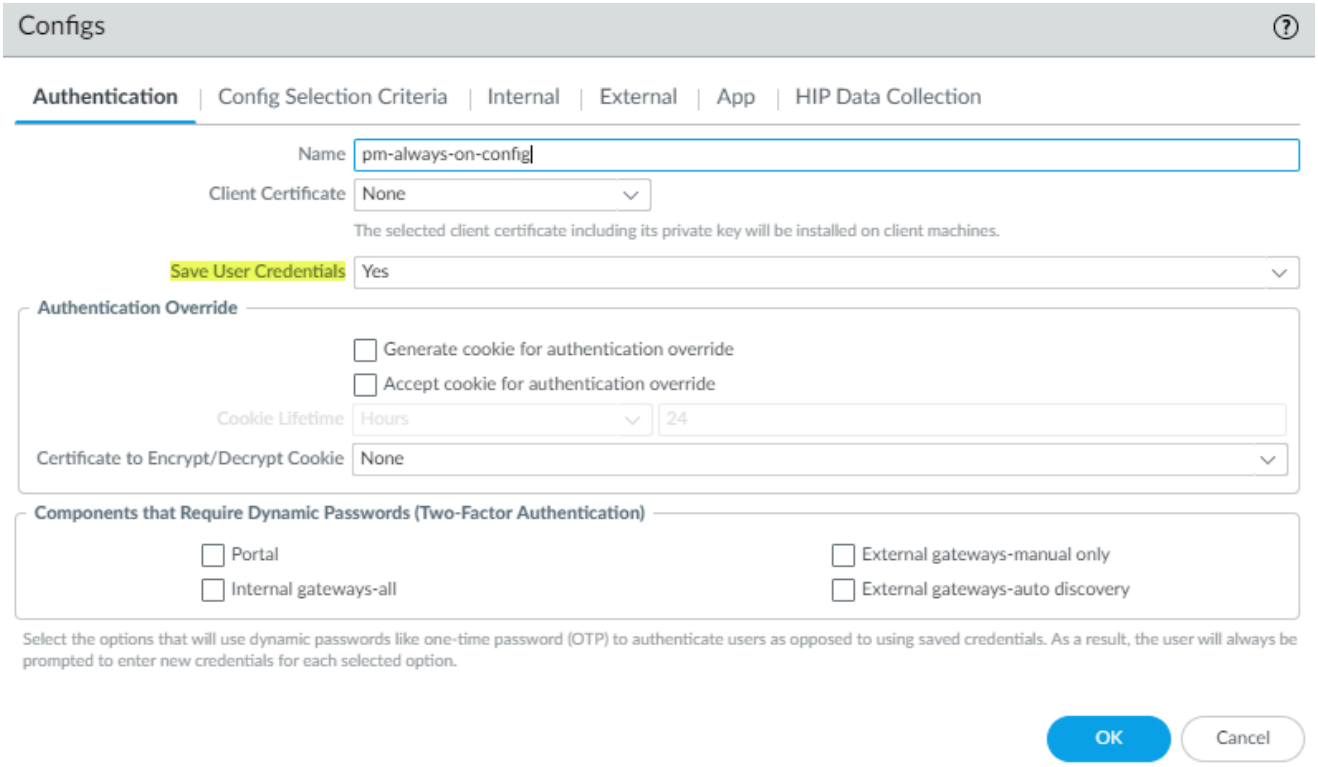


 ©2026 Palo Alto Networks, Inc.

4. Activez l'authentification transparente pour GlobalProtect.

Pour empêcher les utilisateurs de sauter les invites d'authentification GlobalProtect et, par le fait même, de contourner la connexion à GlobalProtect lors de la déconnexion de GlobalProtect, configurez l'une des options d'authentification transparente suivante :

- Activez l'authentification transparente des utilisateurs à GlobalProtect en utilisant l'authentification du certificat du client.
- Activez l'enregistrement du nom d'utilisateur et du mot de passe sur l'application GlobalProtect pour assurer la transparence de l'ouverture de session.
  1. À partir de la configuration de l'agent du portail (**Network [Réseau]** > **GlobalProtect** > **Portals [Portails]** > ***<portal-config>*** > **Agent** > ***<agent-config>***), sélectionnez **Authentication (Authentification)**.
  2. Définissez l'option **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)** sur **Yes (Oui)**.

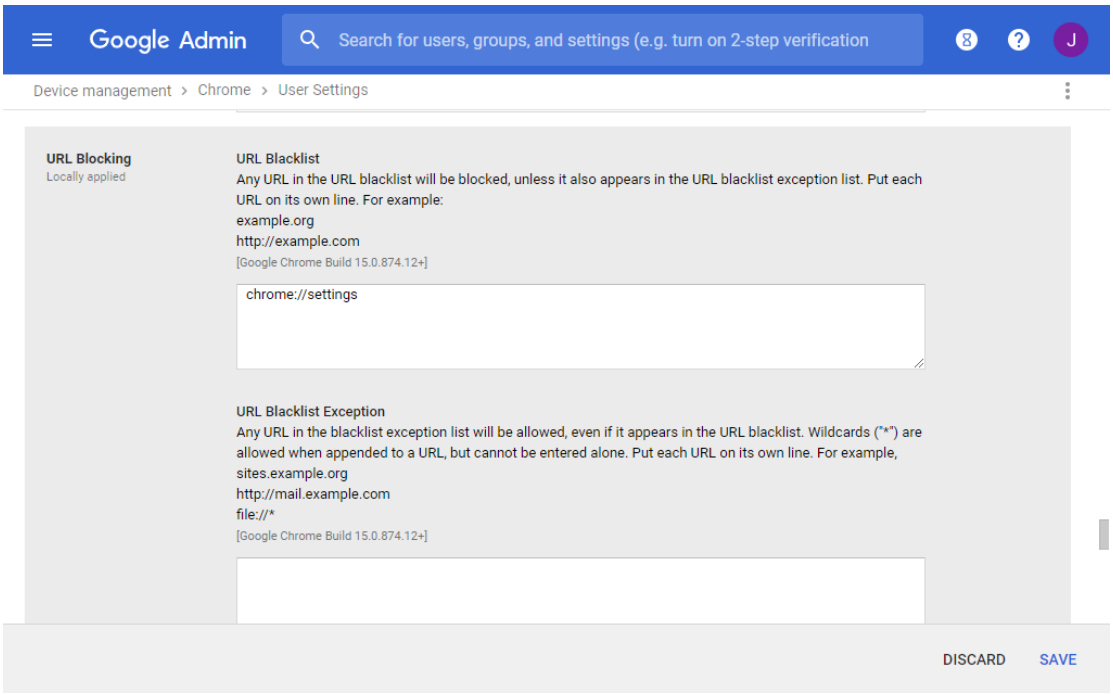


  3. Cliquez deux fois sur **OK** pour enregistrer la configuration de l'agent du portail.

5. Cliquez sur **Commit (Valider)** pour valider les modifications que vous avez apportées au pare-feu.

 ©2026 Palo Alto Networks, Inc.

6. Empêchez les utilisateurs de Chrome de contourner GlobalProtect en utilisant les paramètres VPN du système d'exploitation de Chrome.
   1. Connectez-vous à la console Google Admin en tant qu'administrateur.
   2. Déployer l'application GlobalProtect pour Android sur les Chromebooks gérés à l'aide de la console Google Admin sur tous les Chromebook gérés.
   3. Mettez les paramètres de Chrome sur la liste blocage (**`chrome://settings`**) pour empêcher les utilisateurs de modifier les paramètres VPN :
      1. Sélectionnez **Device Management (Gestion des périphériques)** > **Chrome management (Gestion de Chrome)** > **User Settings (Paramètres de l'utilisateur)**.
      2. Dans la zone Content (Contenu) > URL Blocking (Blocage des URL), saisissez **`chrome://settings`** dans la zone de saisie **URL Blocklist (Liste de blocage des URL)**.



   4. **SAVE (Sauvegardez)** vos modifications.

Gérer l'application GlobalProtect à l'aide de Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect pour macOS 6.0.4 et versions ultérieures et 6.1 et versions ultérieures Application GlobalProtect pour iOS 6.1 et versions ultérieures

©2026 Palo Alto Networks, Inc.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	Terminaux exécutant les versions macOS et iOS prises en charge Terminaux exécutant macOS 11 (Big Sur), macOS 12 (Monterey) ou macOS 13 (Ventura)

Jamf Pro est une plateforme de gestion de mobilité d'entreprise qui vous permet de gérer des terminaux macOS et iOS , à partir d'une console centrale. L'application GlobalProtect offre une connexion sécurisée entre le pare-feu et les terminaux mobiles gérés par Jamf Pro au niveau du périphérique ou de l'application. L'utilisation de GlobalProtect en tant que connexion sécurisée assure l'homogénéité de l'inspection du trafic et de l'application des règles de sécurité du réseau pour la prévention des menaces sur les points de terminaison mobiles.

Si vous n'utilisez pas de système MDM de tiers qualifié, vous pouvez Gérer l'application GlobalProtect à l'aide d'autres MDM tiers.

Gérer l'application GlobalProtect pour iOS à l'aide de Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect pour iOS 6.1 et versions ultérieures Terminaux exécutant des versions iOS prises en charge

Vous pouvez utiliser Jamf Pro pour gérer les terminaux iOS depuis une console centrale. L'application GlobalProtect fournit une connexion sécurisée entre le pare-feu et les terminaux iOS que Jamf Pro gère au niveau du périphérique ou de l'application. L'utilisation de GlobalProtect en tant que connexion sécurisée assure l'homogénéité de l'inspection du trafic et de l'application des règles de sécurité du réseau pour la prévention des menaces sur les points de terminaison mobiles.

Reportez-vous aux sections suivantes pour obtenir des informations sur la configuration des terminaux iOS et le déploiement de l'application GlobalProtect à l'aide de Jamf Pro :

- Configurer les terminaux iOS à l'aide des profils de configuration Jamf
- Déployer l'application mobile GlobalProtect pour iOS en utilisant Jamf Pro
- Vérifier le déploiement de l'application GlobalProtect pour iOS à l'aide de Jamf Pro

 ©2026 Palo Alto Networks, Inc.

Configurer les terminaux iOS à l'aide des profils de configuration Jamf

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect pour iOS 6.1 et versions ultérieures Terminaux exécutant des versions iOS prises en charge

Avant de déployer l'application GlobalProtect, vous pouvez définir des configurations VPN pour les terminaux iOS en utilisant des profils de configuration Jamf qui spécifient comment le trafic est acheminé dans le tunnel. Vous pouvez spécifier une configuration VPN pour vous assurer que la connexion GlobalProtect sécurisée est toujours activée, initiée par l'utilisateur (à la demande), ou spécifier les applications gérées qui peuvent acheminer le trafic via le tunnel.

Configurer une configuration de VPN toujours active sur les terminaux iOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect pour iOS 6.1 et versions ultérieures Terminaux exécutant des versions iOS prises en charge

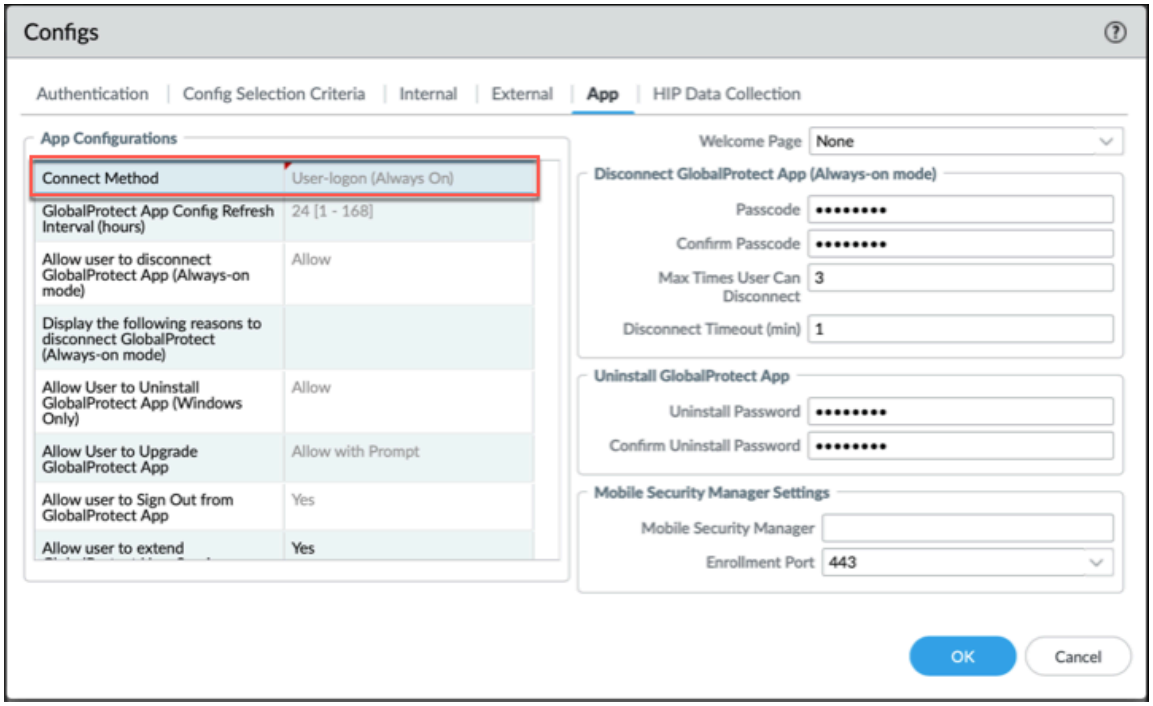
Dans une configuration de VPN toujours active, la connexion GlobalProtect sécurisée est toujours active. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la passerelle GlobalProtect est toujours acheminé via le tunnel.

Pour les terminaux iOS, vous pouvez configurer une configuration VPN toujours active sur le pare-feu ou Prisma Access.

©2026 Palo Alto Networks, Inc.

Pour configurer une configuration VPN toujours active à l'aide de l'interface utilisateur web (sur le pare-feu ou Prisma Access géré par Panorama) :

1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez une configuration de portail et sélectionnez l'onglet **Agent**.
3. Sélectionnez une configuration d'agent puis l'onglet **App (Application)**.
4. Pour la **Connect Method (Méthode de connexion)**, sélectionnez **User-logon (Always On) (Ouverture de session utilisateur [Toujours activé])**.

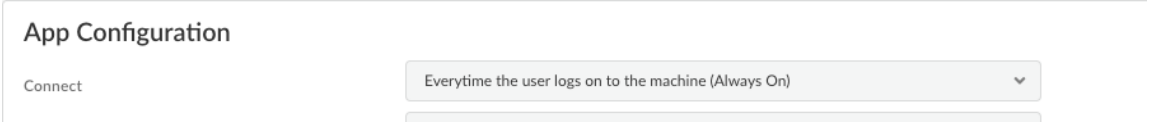


5. Cliquez sur **OK**.
6. Validez et appliquez vos modifications apportées aux utilisateurs mobiles.

 ©2026 Palo Alto Networks, Inc.

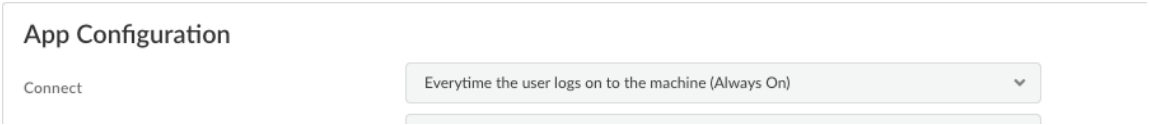
Pour configurer une configuration VPN toujours active depuis Strata Cloud Manager pour Prisma Access :

1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect**.
2. Sélectionnez l'onglet **GlobalProtect App (Application GlobalProtect)**.
3. Pour le paramètre **Connect (Connexion)** dans la section Configuration de l'application, sélectionnez **Every time the user logs on to the machine (Always On) (Chaque fois que l'utilisateur se connecte à la machine [Toujours activé])**.



4. Cliquez sur **Save (Enregistrer)** pour enregistrer les paramètres puis sur **Push Config (Transmettre la configuration)**.

1. Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration Prisma Access)** > **GlobalProtect**.
2. Sélectionnez l'onglet **GlobalProtect App (Application GlobalProtect)**.
3. Sélectionnez un paramètre d'application.
4. Pour le paramètre **Connect (Connexion)** dans la section Configuration de l'application, sélectionnez **Every time the user logs on to the machine (Always On) (Chaque fois que l'utilisateur se connecte à la machine [Toujours activé])**.



5. Cliquez sur **Save (Enregistrer)** pour enregistrer les paramètres puis sur **Push Config (Transmettre la configuration)**.

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les terminaux iOS à l'aide de Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect pour iOS 6.1 et versions ultérieures Terminaux exécutant des versions iOS prises en charge

Dans une configuration de VPN d'accès à distance (à la demande), les utilisateurs doivent lancer manuellement l'application GlobalProtect pour établir la connexion GlobalProtect sécurisée. Le trafic qui correspond à des filtres spécifiques (tels que le port et l'adresse IP) configurés sur la

 ©2026 Palo Alto Networks, Inc.

passerelle GlobalProtect est acheminé via le tunnel seulement après que les utilisateurs ont initié et établi la connexion.

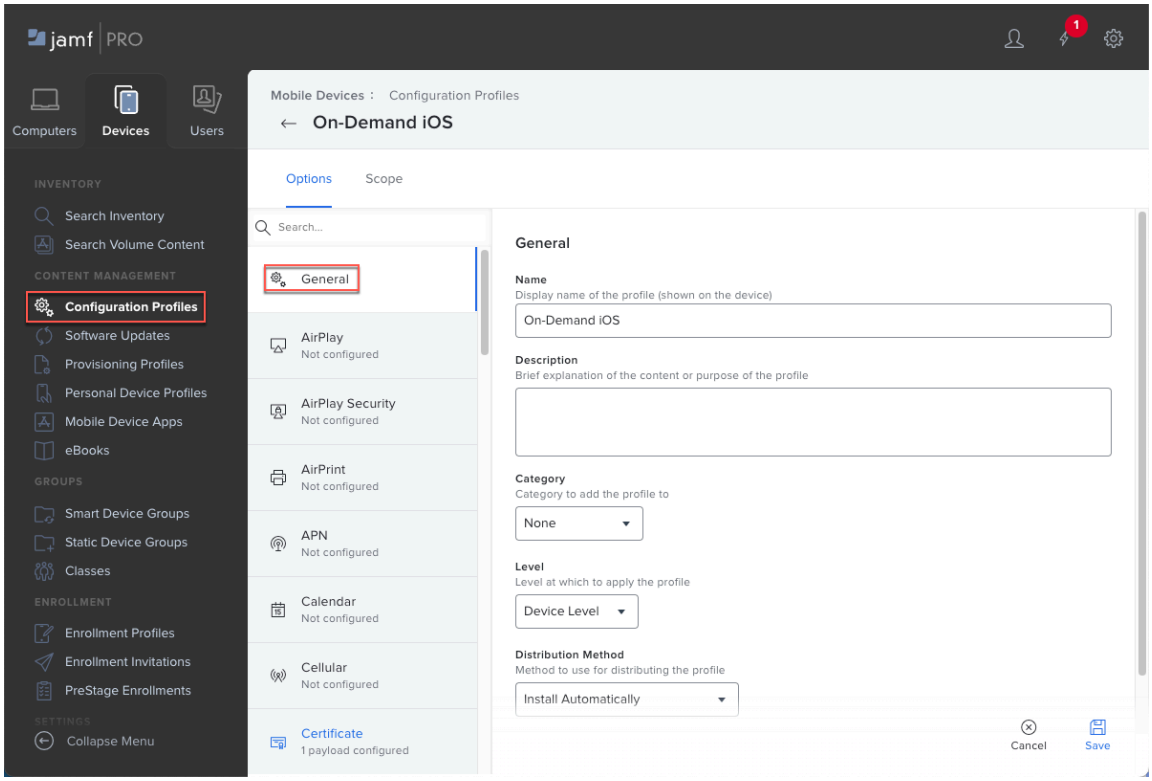
Pour configurer une configuration VPN à la demande, utilisez Jamf Pro pour créer un profil de configuration que vous pouvez déployer sur des périphériques iOS gérés.

1. (Facultatif) Configurez des groupes d'appareils intelligents ou statiques pour regrouper les périphériques iOS gérés qui recevront le profil de configuration.

2. Créez un profil de configuration pour la configuration VPN et spécifiez les paramètres **General (Généraux)**.
    1. Dans Jamf Pro, sélectionnez **Devices (Périphériques)** > **Configuration Profiles (Profils de configuration)** > **New (Nouveau)**.
    2. Entrez un **Display Name (Nom d'affichage)** significatif pour le profil. Ce nom de profil apparaîtra sur le périphérique iOS.
    3. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
    4. (Facultatif) Sélectionnez une **Category (Catégorie)** à laquelle vous souhaitez ajouter le profil.
    5. Pour le **Level (Niveau)** auquel appliquer le profil de configuration, sélectionnez **Device Level (Niveau du périphérique)**, qui permet de distribuer le profil à un périphérique, soit automatiquement, soit installé par l'utilisateur depuis l'application Jamf Self Service.
    6. Sélectionnez l'option **Distribution Method (Méthode de distribution)**, soit **Make available in Self Service (Rendre disponible dans Self Service)**, ce qui permet à l'utilisateur final de télécharger l'application depuis l'application Jamf Self Service, soit

 ©2026 Palo Alto Networks, Inc.

Install Automatically (Installer automatiquement), ce qui pousse l'application sur le périphérique de l'utilisateur final automatiquement.



7. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

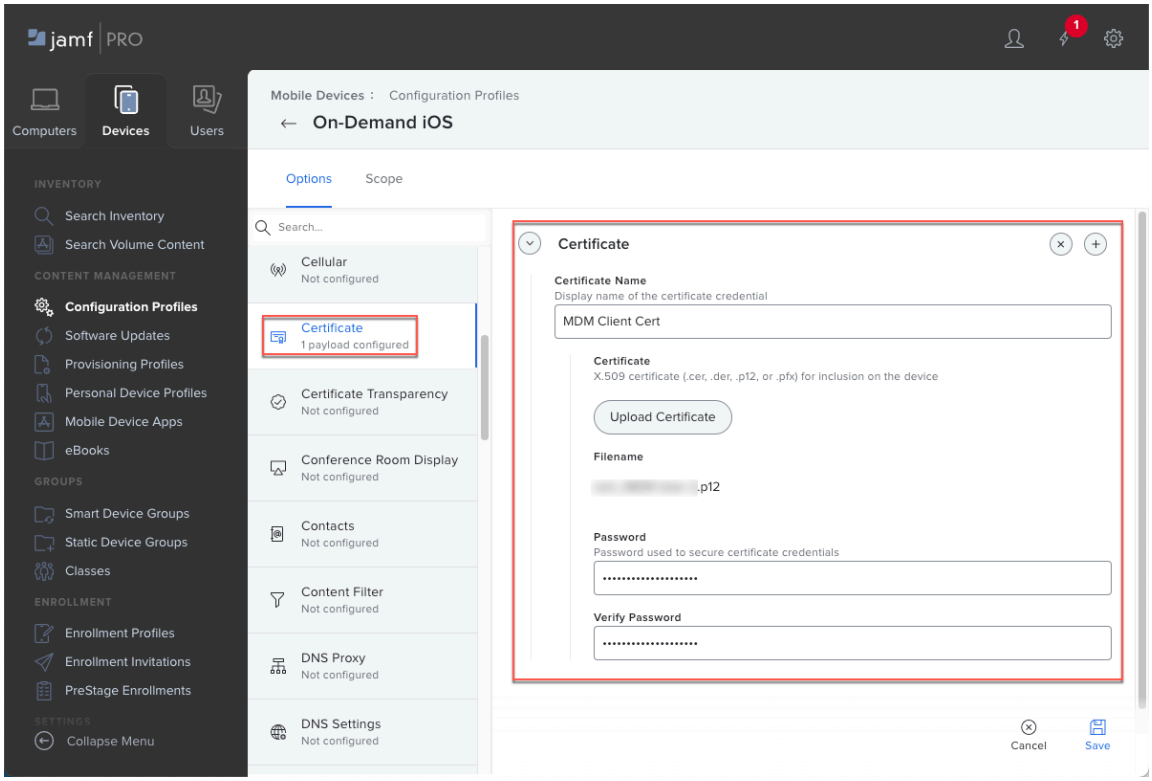
3. (Facultatif) Si votre déploiement GlobalProtect exige une authentification du certificat du client, configurez la charge utile du **Certificate (Certificat)**.

   À partir de la version 12 d'iOS, si vous souhaitez utiliser les certificats de client pour procéder à l'authentification du client GlobalProtect, vous devez déployer les certificats de client dans le cadre du profil VPN qui est transmis de Jamf Pro. Si vous déployez des certificats de client à partir de Jamf Pro au moyen d'une tout autre méthode, les certificats ne peuvent être utilisés par l'application GlobalProtect.

   1. Si vous avez enregistré votre profil à l'étape précédente, vous pouvez le **Edit (Modifier)**.
   2. Sélectionnez **Certificate (Certificat)** > **Configure (Configurer)**.
   3. Saisissez le **Certificate Name (nom du certificat)**.
   4. Sélectionnez l'option de certificat **Upload (Charger)**.

©2026 Palo Alto Networks, Inc.

5. Cliquez sur **Upload Certificate (Charger le certificat)** pour localiser et sélectionner le certificat que vous voulez charger. Si nécessaire, entrez le **Password (Mot de passe)** pour le certificat et **Verify Password (Vérifier le mot de passe)**.



6. (Facultatif) Cliquez sur **+** pour ajouter d'autres certificats.
7. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

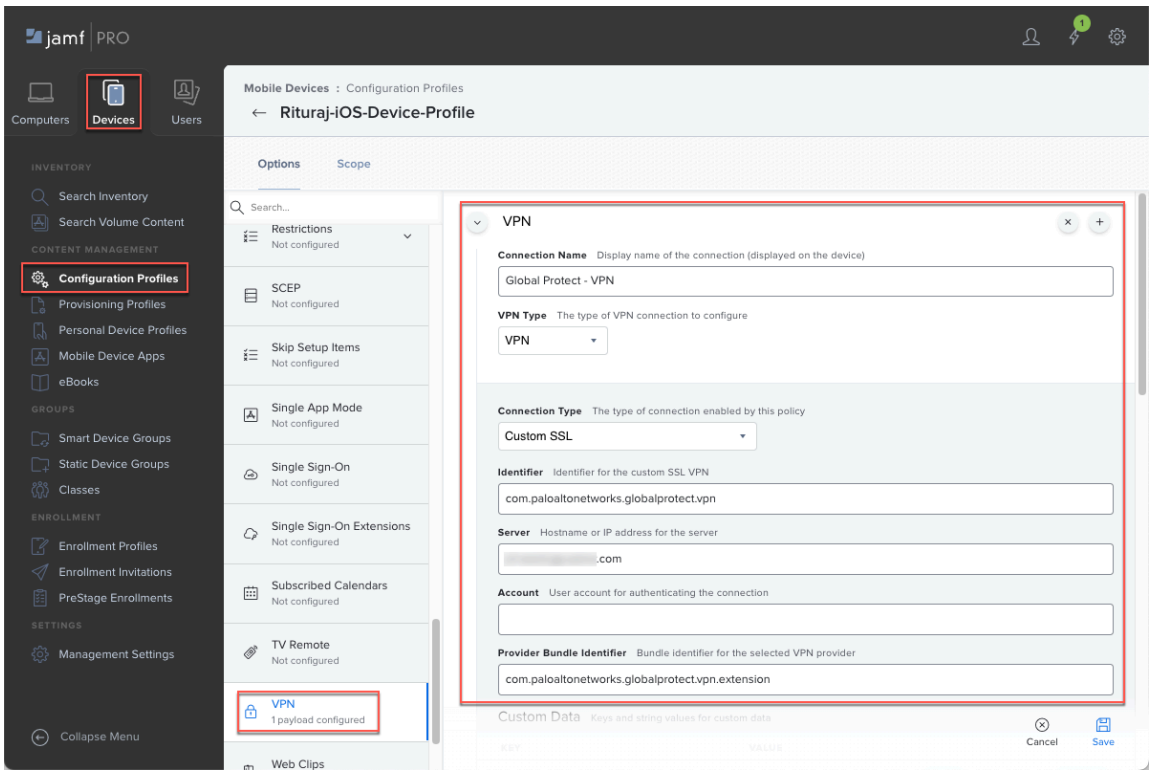
4. Configurez les paramètres **VPN**.
   1. Si vous avez enregistré votre profil à l'étape précédente, vous pouvez le **Edit (Modifier)**.
   2. Sélectionnez **VPN** > **Configure (Configurer)**.
   3. Saisissez un **Display Name (Nom d'affichage)** significatif pour la connexion, tel que **`GlobalProtect VPN (VPN GlobalProtect)`**.
   4. Pour le **VPN Type (Type VPN)**, sélectionnez **VPN** pour acheminer tout le trafic à travers le tunnel GlobalProtect.
   5. Pour le **Connection Type (Type de connexion)**, sélectionnez **Custom SSL (SSL personnalisé)**.
   6. Pour l'**Identifier (Identifiant)**, saisissez **`com.paloaltonetworks.globalprotect.vpn`**.

      Si vous avez téléchargé l'application GlobalProtect directement dans Apple App Store en Chine, saisissez l'ID de

 ©2026 Palo Alto Networks, Inc.

groupe ***com.paloaltonetworks.globalprotect.vpn*** *dans le champ* ***Identifier (Identifiant)***.

7. Pour le **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs se connecteront, tel que **gp.paloaltonetworks.com**.
8. Pour **Provider Bundle Identifier (Identifiant de groupe du fournisseur)**, saisissez **com.paloaltonetworks.globalprotect.vpn.extension**.



9. (Facultatif) Pour les **Custom Data (Données personnalisées)**, **Add (Ajouter)** et **Save (Enregistrer)** des clés et des valeurs personnalisées pour définir des configurations d'application GlobalProtect supplémentaires.

   Le tableau suivant montre certaines des clés et valeurs que vous pouvez utiliser :

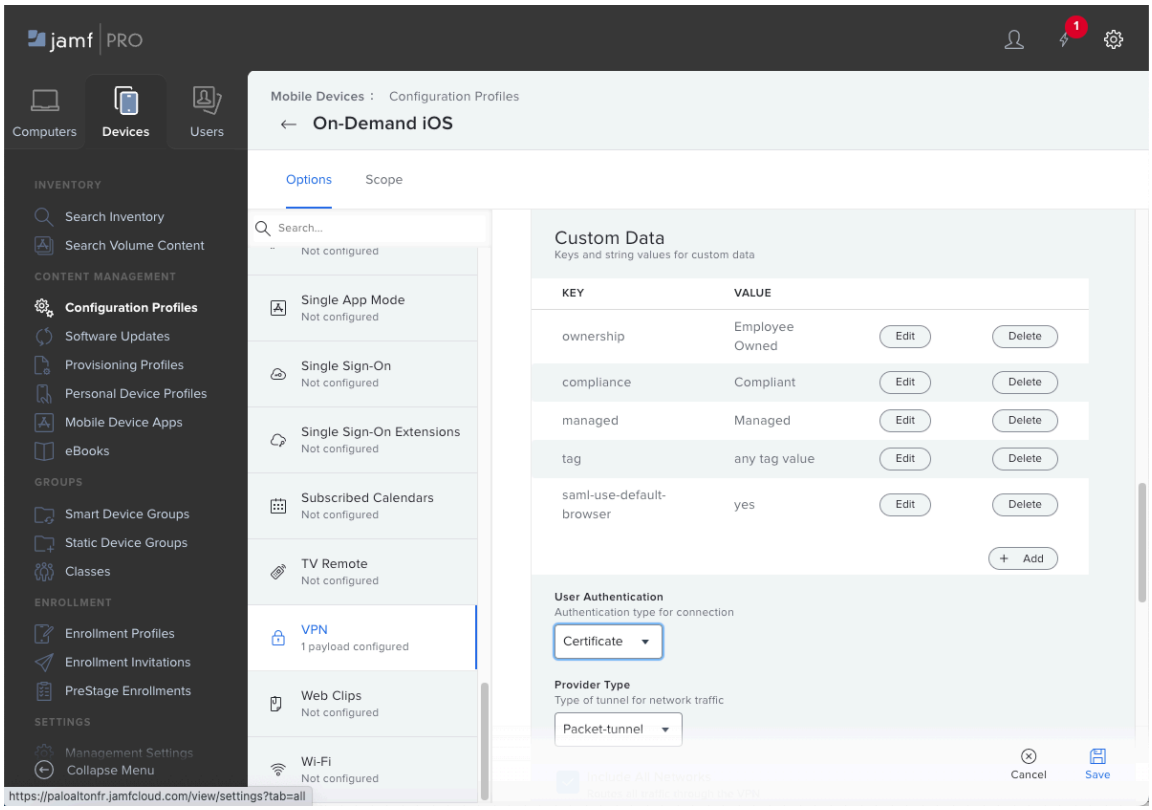
Clé	Valeur	Description
compliance	**Compliant (Conforme)**	État de conformité qui indique si le terminal est conforme aux politiques de conformité Mobile Device Management (gestion des appareils mobiles - MDM) que vous avez définies (par exemple, **Compliant [Conforme]**). Cette valeur est annexée à l'attribut **Tag (Étiquette)** indiqué dans le rapport HIP.

 ©2026 Palo Alto Networks, Inc.

Clé	Valeur	Description
enable-fips-cc-mode	**no | yes**	Option qui active le FIPS-CC mode (mode FIPS-CC) pour incorporer les exigences des Critères communs (CC) et de la Federal Information Processing Standard (norme fédérale de traitement de l'information) (FIPS 140-2).
managed	**yes | no**	Valeur qui indique si le point de terminaison est géré.
ownership	**Employee Owned (Appartient à l'employé)**	Catégorie d'appartenance du point de terminaison (par exemple, **Employee Owned (appartient à l'employé)**). Cette valeur est annexée à l'attribut **Tag (Étiquette)** indiqué dans le rapport HIP.
saml-use-default-browser	**vraie| fausse**	Option qui permet à un terminal d'utiliser le navigateur système par défaut pour l'authentification SAML. Si vous avez configuré le portail GlobalProtect pour authentifier les utilisateurs via l'authentification SAML, les utilisateurs finaux peuvent se connecter à l'application ou à d'autres applications compatibles SAML sans avoir à ressaisir leurs identifiants, offrant une expérience de Single Sign-On (ouverture de session unique - SSO).
Etiquette	**fonctionne**	Étiquettes pour vous permettre de faire correspondre aux autres attributs fondés sur MDM. Cette valeur est annexée

 ©2026 Palo Alto Networks, Inc.

Clé	Valeur	Description
		à l'attribut Tag (Étiquette) indiqué dans le rapport HIP.

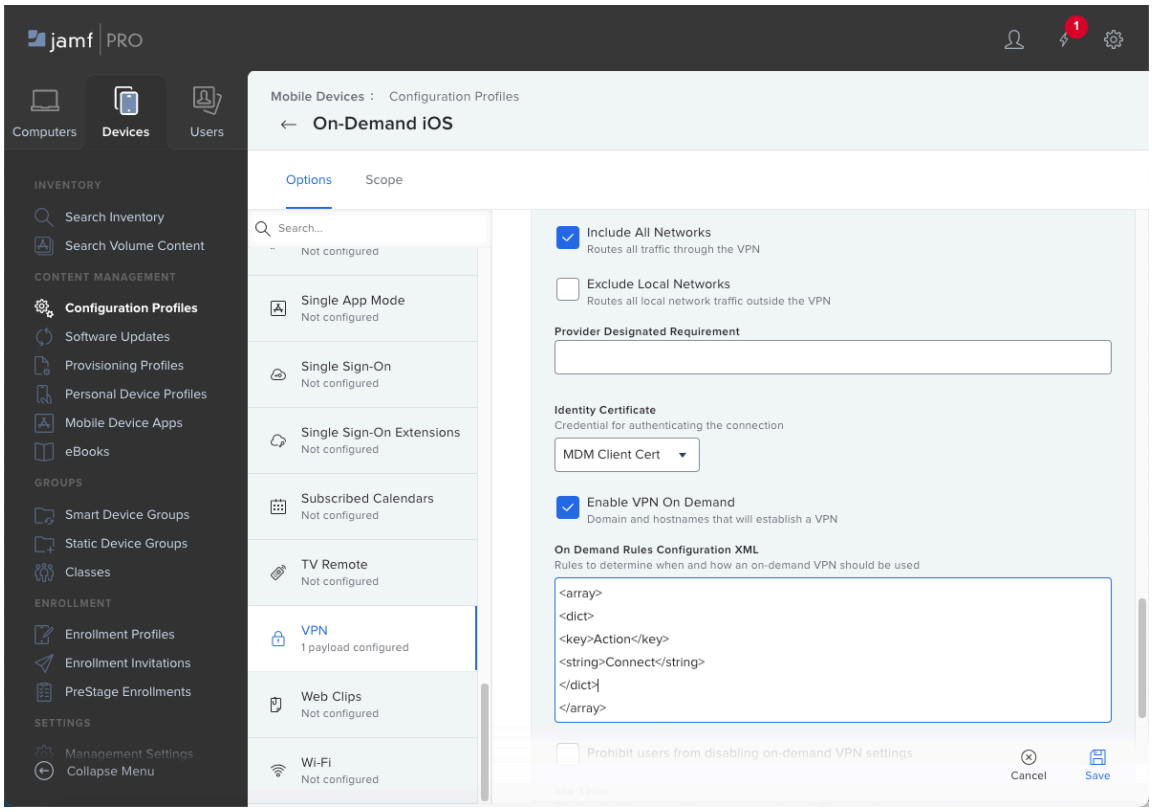


10. Pour l'**User Authentication (Authentification de l'utilisateur)**, sélectionnez **Certificate (Certificat)** si GlobalProtect utilise des certificats pour authentifier les utilisateurs, ou sélectionnez **Password (Mot de passe)** pour entrer un mot de passe pour authentifier les utilisateurs.
11. (Authentification par mot de passe uniquement) Entrez le **Password (Mot de passe)** et **Verify Password (Vérifier le mot de passe)**.
12. Sélectionnez le **Provider Type (Type de fournisseur)** pour indiquer la manière dont le trafic sera tunnelisé : soit au niveau de l'application ou de l'adresse IP. Sélectionnez **Packet-tunnel (Tunnel-paquets)**.
13. Sélectionnez **Include All Networks (Inclure tous les réseaux)** pour acheminer tout le trafic via le VPN.
14. (Authentification du certificat uniquement) Pour **Identity Certificate (Certificat d'identité)**, sélectionnez le certificat que vous avez configuré dans la charge utile **Certificate (Certificat)**. GlobalProtect utilisera ce certificat pour authentifier les utilisateurs.

 ©2026 Palo Alto Networks, Inc.

15. Sélectionnez **Enable VPN On Demand (Activer VPN à la demande)** et saisissez le **On Demand Rules Configuration XML (XML de configuration des règles à la demande)** suivant :

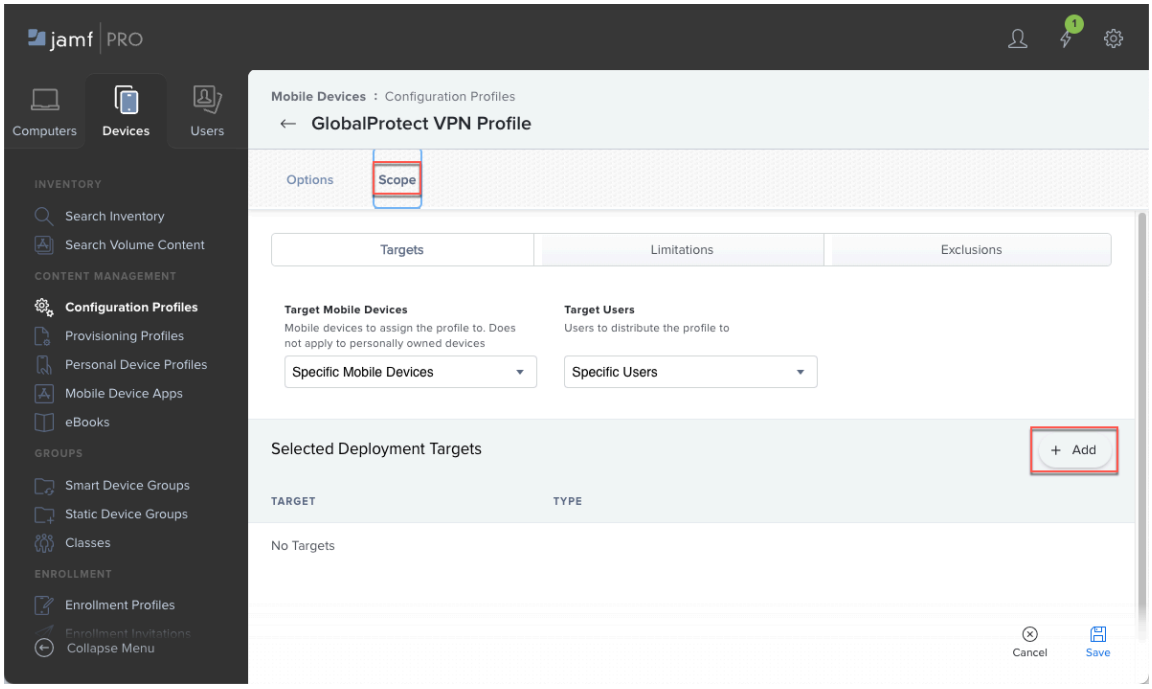
```
<array> <dict> <key>Action</key> <string>Connect</string> </
dict> </array>
```



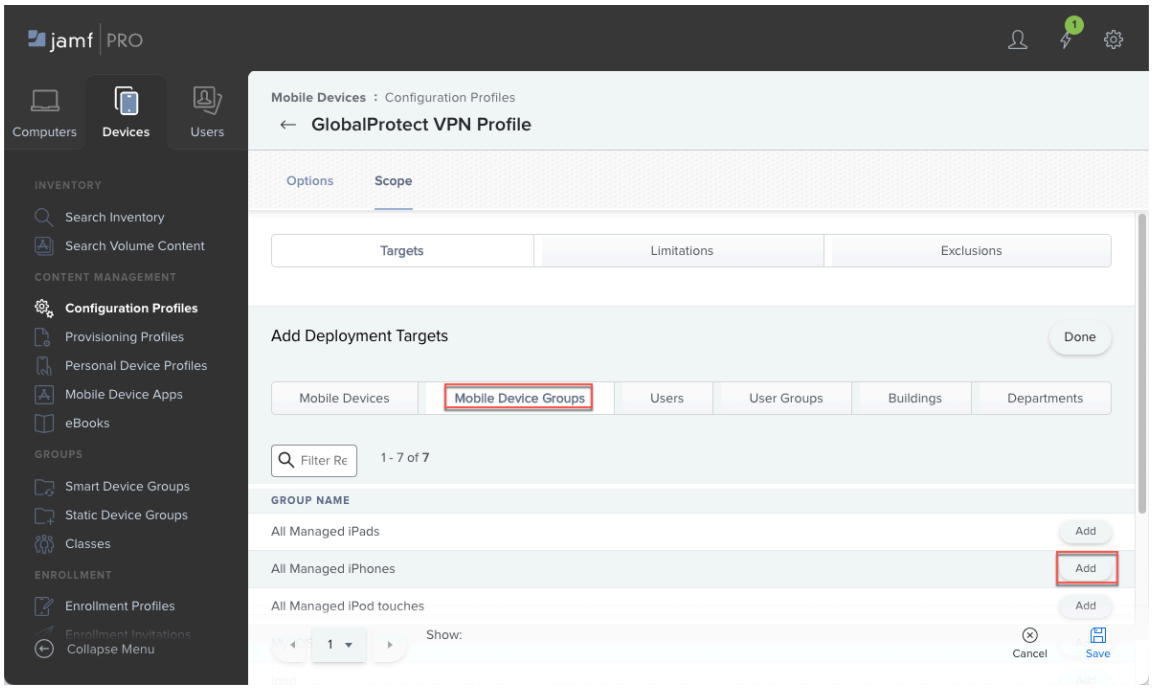
16. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

5. Définissez la portée pour définir les périphériques qui recevront le profil de configuration.
   1. Cliquez sur **Edit (Modifier)** si vous avez enregistré vos paramètres à l'étape précédente.
   2. Cliquez sur **Scope (Portée)** et **Add (Ajouter)** une cible de déploiement.



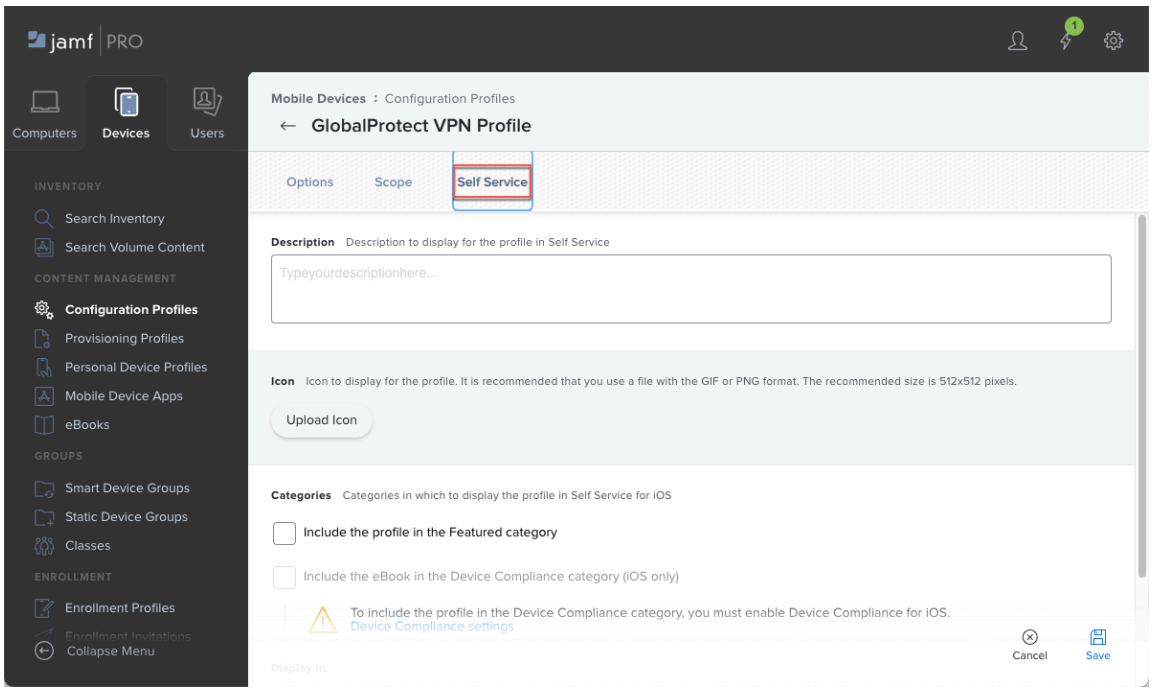
   3. **Add (Modifier)** des périphériques individuels à partir du tableau des **Mobile Devices (Périphériques mobiles)**, ou sélectionnez **Mobile Device Groups (Groupes d'appareils mobiles)** et **Add (Ajouter)** les groupes de périphériques intelligents ou statiques que vous avez configurés précédemment.



   4. (Facultatif) Si vous avez choisi de rendre le profil de configuration disponible dans l'application Self Service, sélectionnez **Self Service** et indiquez comment vous souhaitez

 ©2026 Palo Alto Networks, Inc.

que le profil de configuration apparaisse dans l'application Self Service, par exemple en téléchargeant une icône pour le profil ou en incluant le profil dans la catégorie **Featured (En Vedette)** dans Jamf.



5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

6. Pour vérifier si Jamf Pro a installé le profil de configuration sur un terminal :
   1. Depuis Jamf Pro, sélectionnez **Devices (Périphériques)**.
   2. **Search (Rechercher)** un périphérique mobile.
   3. Sélectionnez un périphérique mobile dans la liste.
   4. Sélectionnez **History (Historique)** et consultez les **Completed Commands (Commandes terminées)**, **Pending Commands (Commandes en attente)** ou **Failed Commands (Commandes échouées)**. Dans les **Completed Commands (Commandes terminées)**, recherchez la commande `Installer le profil de configuration <your_profile>`.

      Si vous ne voyez pas la commande `Installer le profil de configuration <your_profile>` dans la liste, ou si la commande apparaît dans la liste **Fail Commands (Commandes échouées)**, sélectionnez **Management (Gestion)** > **Management Commands (Commandes de gestion)** > **Update Inventory (Mettre à jour l'inventaire)** pour pousser le profil de configuration vers le périphérique.

Configurer une configuration de VPN par application sur les terminaux iOS à l'aide de Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

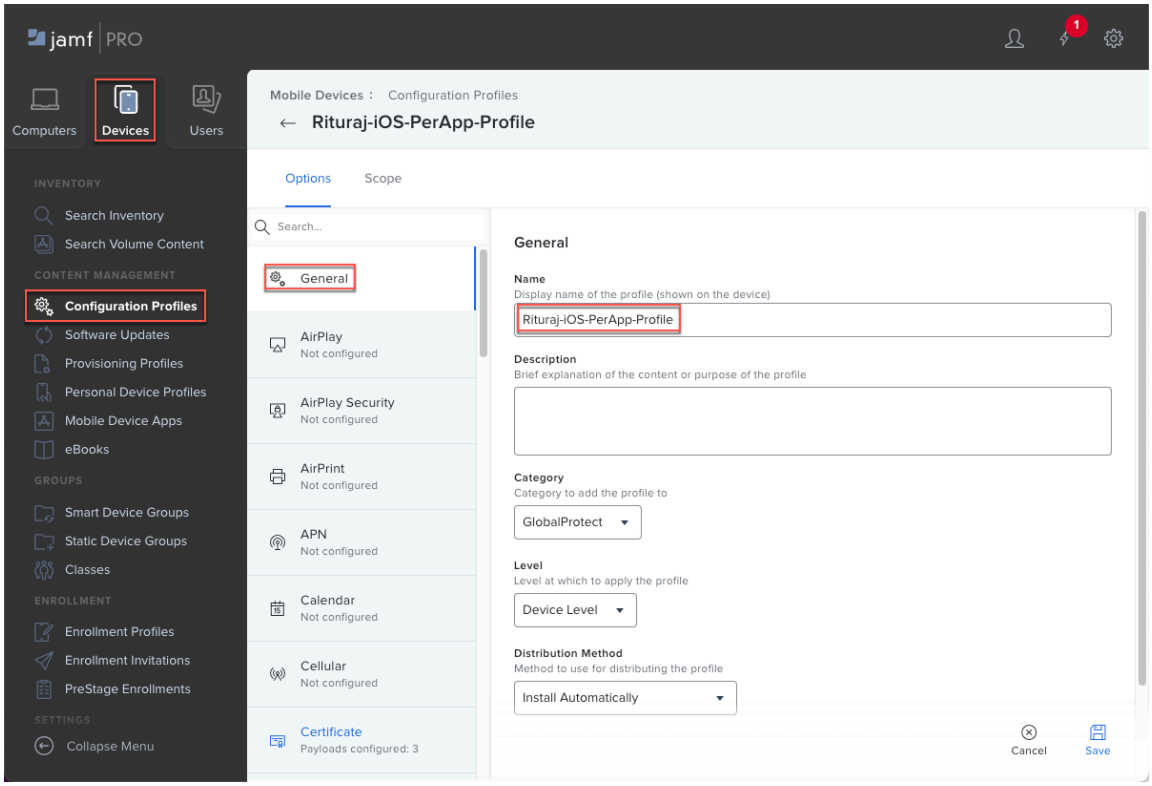
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (géré par Panorama ou Strata Cloud Manager)	Application GlobalProtect pour iOS 6.1 et versions ultérieures Terminaux exécutant des versions iOS prises en charge

Vous pouvez autoriser l'accès aux ressources internes à partir de vos terminaux iOS gérés en configurant l'accès VPN GlobalProtect à l'aide de Jamf Pro. Dans une configuration VPN par application, vous pouvez indiquer les applications gérées qui peuvent acheminer le trafic via le tunnel. Les applications non gérées continueront de se connecter directement par l'Internet plutôt que via le tunnel.

1. (Facultatif) Configurez des groupes d'appareils intelligents ou statiques pour regrouper les périphériques iOS gérés qui recevront le profil de configuration.
2. Créez un profil de configuration pour la configuration VPN par application et indiquez les paramètres **General (Généraux)**.
   1. Dans Jamf Pro, sélectionnez **Devices (Périphériques)** > **Configuration Profiles (Profils de configuration)** > **New (Nouveau)**.
   2. Entrez un **Display Name (Nom d'affichage)** significatif pour le profil. Ce nom de profil apparaîtra sur le périphérique iOS.
   3. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
   4. (Facultatif) Sélectionnez une **Category (Catégorie)** à laquelle vous souhaitez ajouter le profil.
   5. Pour le **Level (Niveau)** auquel appliquer le profil de configuration, sélectionnez **Device Level (Niveau du périphérique)**, qui distribuera le profil à un périphérique, soit automatiquement, soit installé par l'utilisateur depuis l'application Jamf Self Service.
   6. Sélectionnez l'option **Distribution Method (Méthode de distribution)**, soit **Make available in Self Service (Rendre disponible dans Self Service)**, ce qui permet à l'utilisateur final de télécharger l'application depuis l'application Jamf Self Service, soit

 ©2026 Palo Alto Networks, Inc.

Install Automatically (Installer automatiquement), ce qui pousse l'application sur le périphérique de l'utilisateur final automatiquement.



7. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

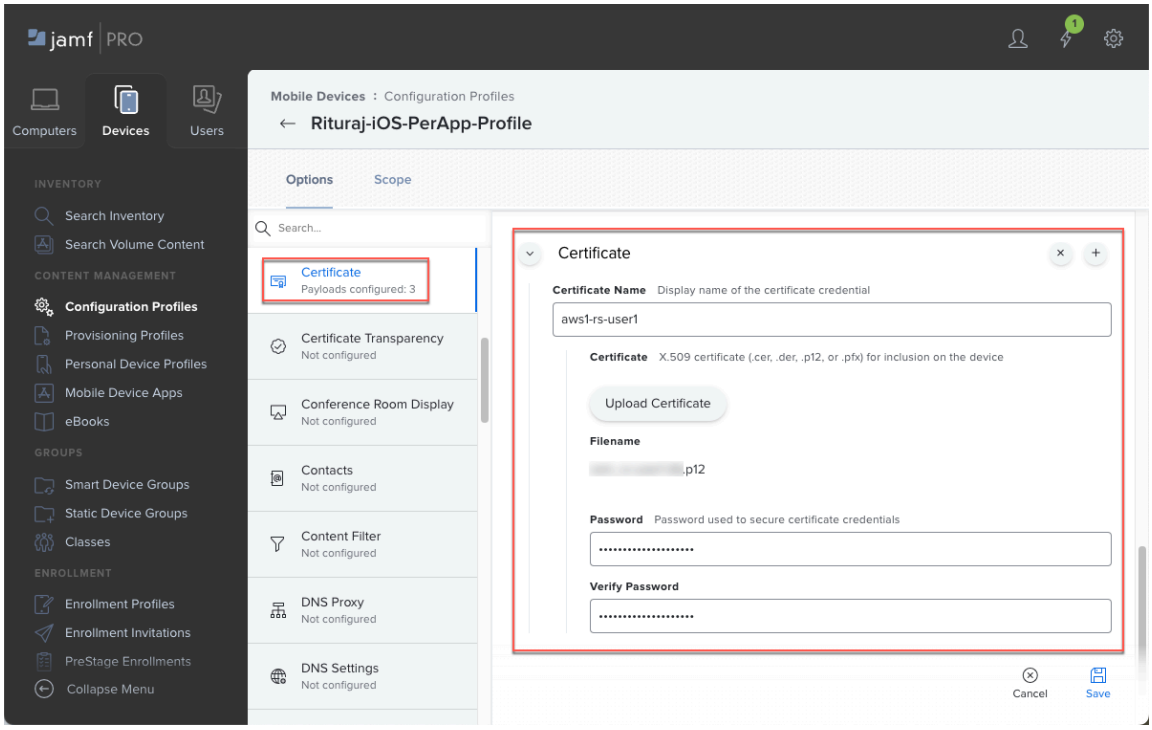
3. Configurez la charge utile du **Certificate (Certificat)**. Toutes les configurations VPN par application pour GlobalProtect nécessitent une authentification par certificat.

   À partir de la version 12 d'iOS, si vous souhaitez utiliser les certificats de client pour procéder à l'authentification du client GlobalProtect, vous devez déployer les certificats de client dans le cadre du profil VPN qui est transmis de Jamf Pro. Si vous déployez des certificats de client à partir de Jamf Pro au moyen d'une tout autre méthode, les certificats ne peuvent être utilisés par l'application GlobalProtect.

   1. Si vous avez enregistré votre profil à l'étape précédente, vous pouvez le **Edit (Modifier)**.
   2. Sélectionnez **Certificate (Certificat)** > **Configure (Configurer)**.
   3. Saisissez le **Certificate Name (nom du certificat)**.
   4. Sélectionnez l'option de certificat **Upload (Charger)**.

 ©2026 Palo Alto Networks, Inc.

5. Cliquez sur **Upload Certificate (Charger le certificat)** pour localiser et sélectionner le certificat que vous voulez charger. Si nécessaire, entrez le **Password (Mot de passe)** pour le certificat et **Verify Password (Vérifier le mot de passe)**.

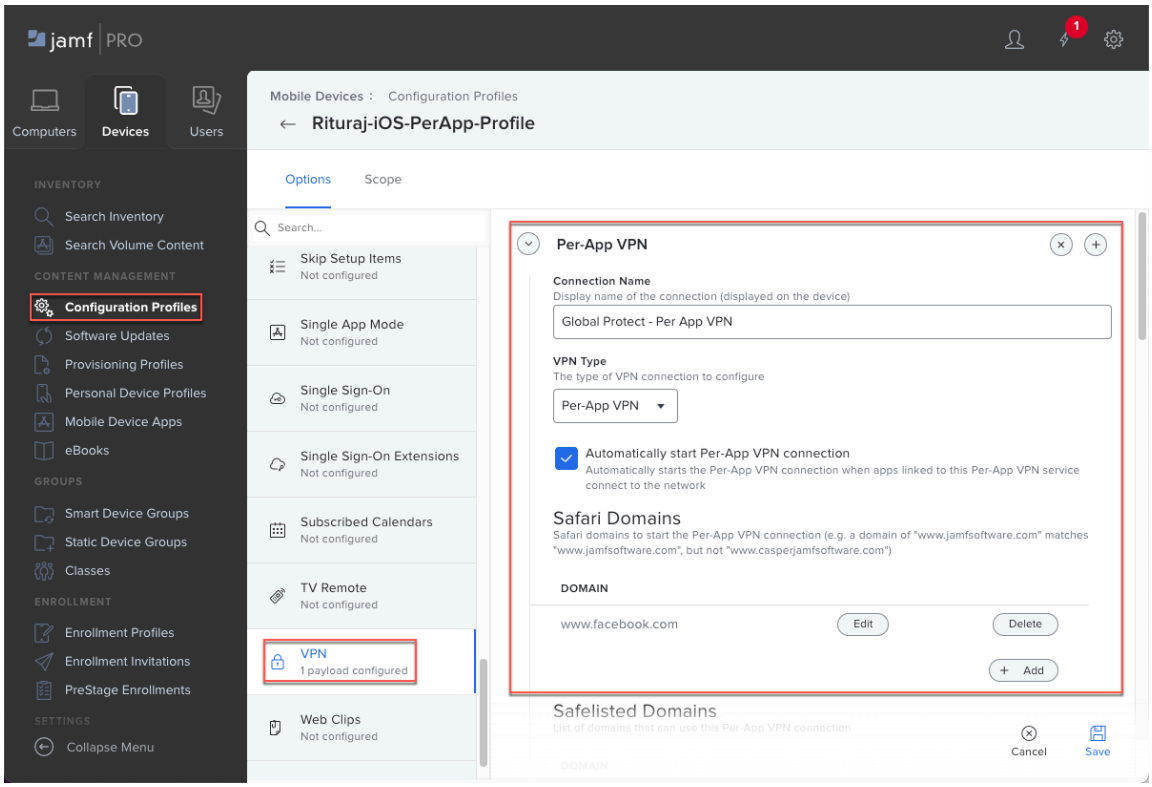


6. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.
7. (Facultatif) Cliquez sur **+** pour ajouter d'autres certificats.

4. Configurez la charge utile **VPN**.
   1. Si vous avez enregistré votre profil à l'étape précédente, vous pouvez le **Edit (Modifier)**.
   2. Sélectionnez **VPN** > **Configure (Configurer)**.
   3. Entrez un **Connection Name (Nom de connexion)** approprié, tel que **`GlobalProtect - VPN par application`**.
   4. Pour **VPN Type (Type de VPN)**, sélectionnez les **Per App VPN Rules (Règles VPN par application)** pour acheminer tout le trafic des applications gérées via le tunnel VPN GlobalProtect.
   5. Activez l'option **Automatically start Per-App VPN connection (Démarrer automatiquement la connexion VPN par application)** pour démarrer la connexion lorsque les applications spécifiées pour cette connexion rejoignent le réseau.
   6. Indiquez les **Safari Domains (Domaines Safari)** qui démarreront la connexion VPN par application dans le navigateur Safari. Lorsque les utilisateurs utilisent les applications liées au domaine, une connexion VPN par application est utilisée. Vous pouvez **Add**

 ©2026 Palo Alto Networks, Inc.

(Ajouter) plusieurs domaines. N'incluez pas le protocole **`http://`** ou **`https://`** dans le domaine.



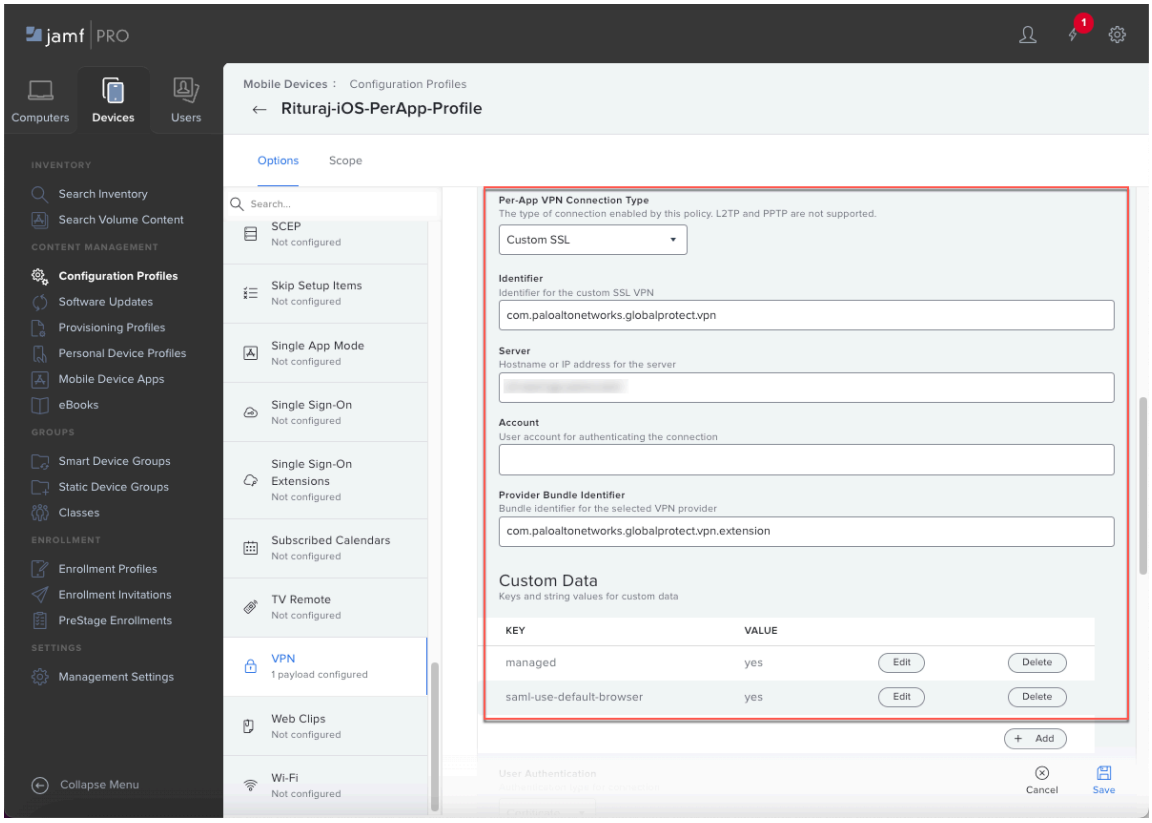
7. Pour le **Per-App VPN Connection Type (Type de connexion VPN par application)**, sélectionnez **Custom SSL (SSL personnalisé)**.
8. Pour l'**Identifier (Identifiant)**, saisissez **`com.paloaltonetworks.globalprotect.vpn`**.

   Si vous avez téléchargé l'application GlobalProtect directement dans Apple App Store en Chine, saisissez l'ID de

 ©2026 Palo Alto Networks, Inc.

*groupe**`com.paloaltonetworks.globalprotect.vpn`** dans le champ **Identifier (Identifiant)**.*

9. Pour le **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs se connecteront, tel que **`gp.paloaltonetworks.com`**.
10. Pour **Provider Bundle Identifier (Identifiant de groupe du fournisseur)**, saisissez **`com.paloaltonetworks.globalprotect.vpn.extension`**.



11. (Facultatif) Pour **Custom Data (Données personnalisées)**, **Add (Ajouter)** et **Save (Enregistrer)** des clés et des valeurs personnalisées pour définir des configurations d'application GlobalProtect supplémentaires.

    Le tableau suivant montre certaines des clés et valeurs que vous pouvez utiliser :

Clé	Valeur	Description
`compliance`	**`Compliant (Conforme)`**	État de conformité qui indique si le terminal est conforme aux politiques de conformité Mobile Device Management (gestion des appareils mobiles - MDM) que vous avez définies (par exemple, **Compliant [Conforme]**). Cette valeur est annexée à l'attribut **Tag**

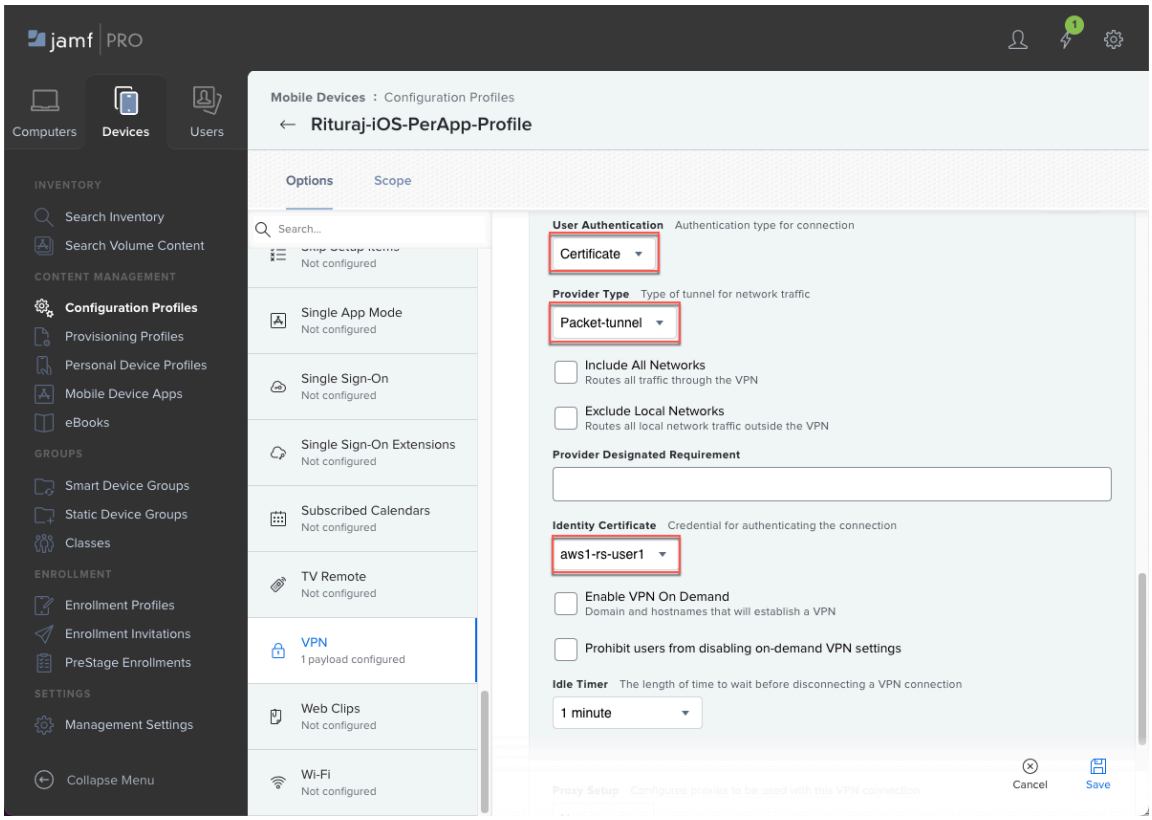
 ©2026 Palo Alto Networks, Inc.

Clé	Valeur	Description
		(Étiquette) indiqué dans le rapport HIP.
enable-fips-cc-mode	**no | yes**	Option qui active le FIPS-CC mode (mode FIPS-CC) pour incorporer les exigences des Critères communs (CC) et de la Federal Information Processing Standard (norme fédérale de traitement de l'information) (FIPS 140-2).
managed	**yes | no (oui | non)**	Valeur qui indique si le point de terminaison est géré.
ownership	**Employee Owned (Appartient à l'employé)**	Catégorie d'appartenance du point de terminaison (par exemple, **Employee Owned (appartient à l'employé)**). Cette valeur est annexée à l'attribut **Tag (Étiquette)** indiqué dans le rapport HIP.
saml-use-default-browser	**vraie| fausse**	Option qui permet à un terminal d'utiliser le navigateur système par défaut pour l'authentification SAML. Si vous avez configuré le portail GlobalProtect pour authentifier les utilisateurs via l'authentification SAML, les utilisateurs finaux peuvent se connecter à l'application ou à d'autres applications compatibles SAML sans avoir à ressaisir leurs identifiants, offrant une expérience de Single Sign-On (ouverture de session unique - SSO).
Etiquette	**fonctionne**	Étiquettes pour vous permettre de faire correspondre aux autres attributs fondés sur MDM. Cette valeur est annexée

 ©2026 Palo Alto Networks, Inc.

Clé	Valeur	Description
		à l'attribut Tag (Étiquette) indiqué dans le rapport HIP.

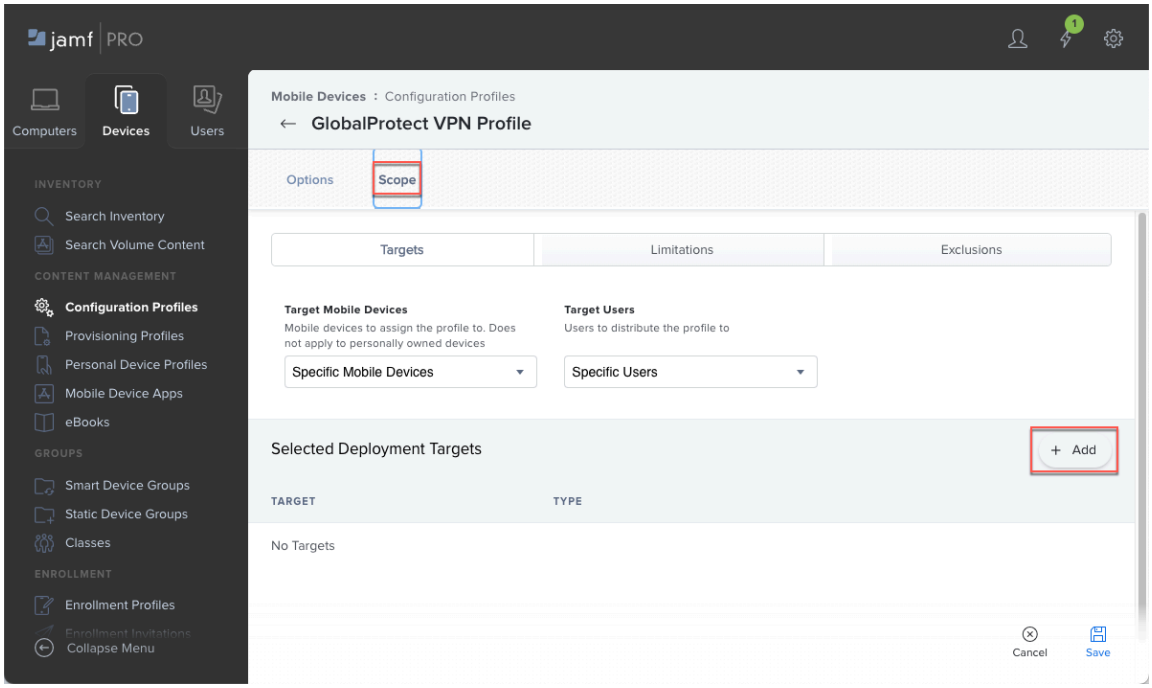
12. Pour **User Authentication (Authentification de l'utilisateur)**, sélectionnez **Certificate (Certificat)**. Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.
13. Sélectionnez le **Provider Type (Type de fournisseur)** pour indiquer la manière dont le trafic sera tunnelisé : soit au niveau de l'application ou de l'adresse IP. Sélectionnez **Packet-tunnel (Tunnel-paquets)**.
14. Pour le **Identity Certificate (Certificat d'identité)**, sélectionnez le certificat que vous avez configuré dans la charge utile **Certificate (Certificat)**. GlobalProtect utilisera ce certificat pour authentifier les utilisateurs.



15. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres. Vous pouvez maintenant sélectionner ce profil de configuration dans le menu déroulant **Per-App VPN (VPN par application)** lorsque vous ajoutez l'application GlobalProtect dans Jamf Pro.

 ©2026 Palo Alto Networks, Inc.

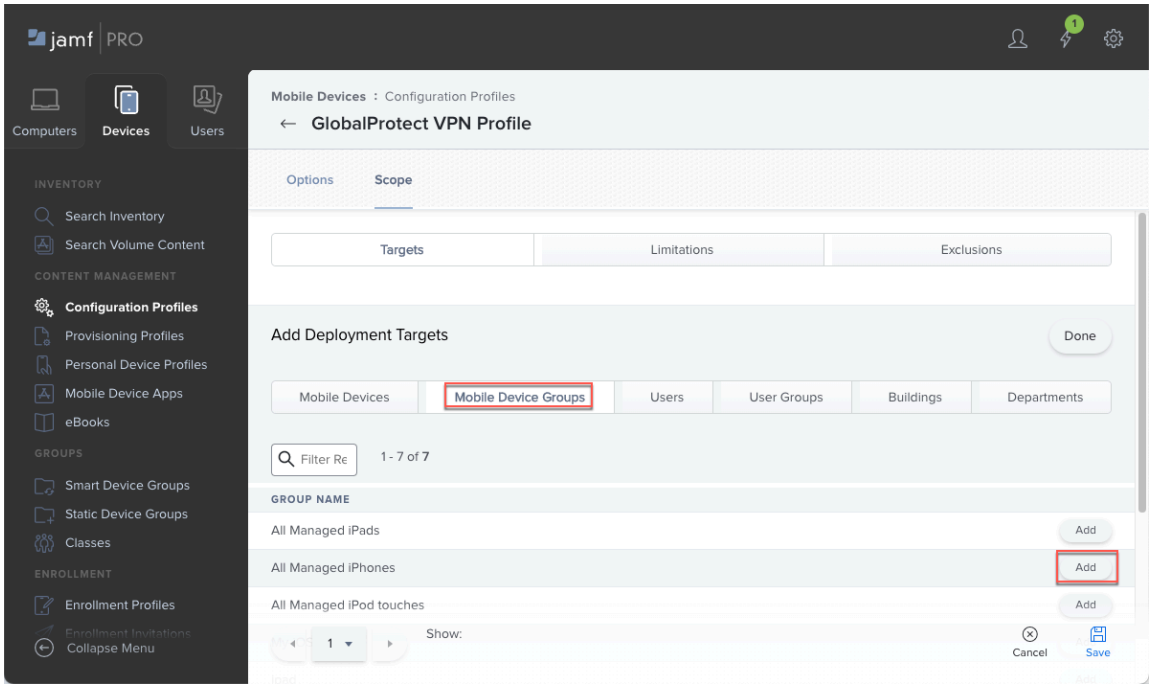
5. Si vous utilisez des groupes d'appareils intelligents ou statiques, définissez la portée pour définir les périphériques qui recevront le profil de configuration.
   1. Cliquez sur **Edit (Modifier)** si vous avez enregistré vos paramètres à l'étape précédente.
   2. Cliquez sur **Scope (Portée)** et **Add (Ajouter)** une cible de déploiement.



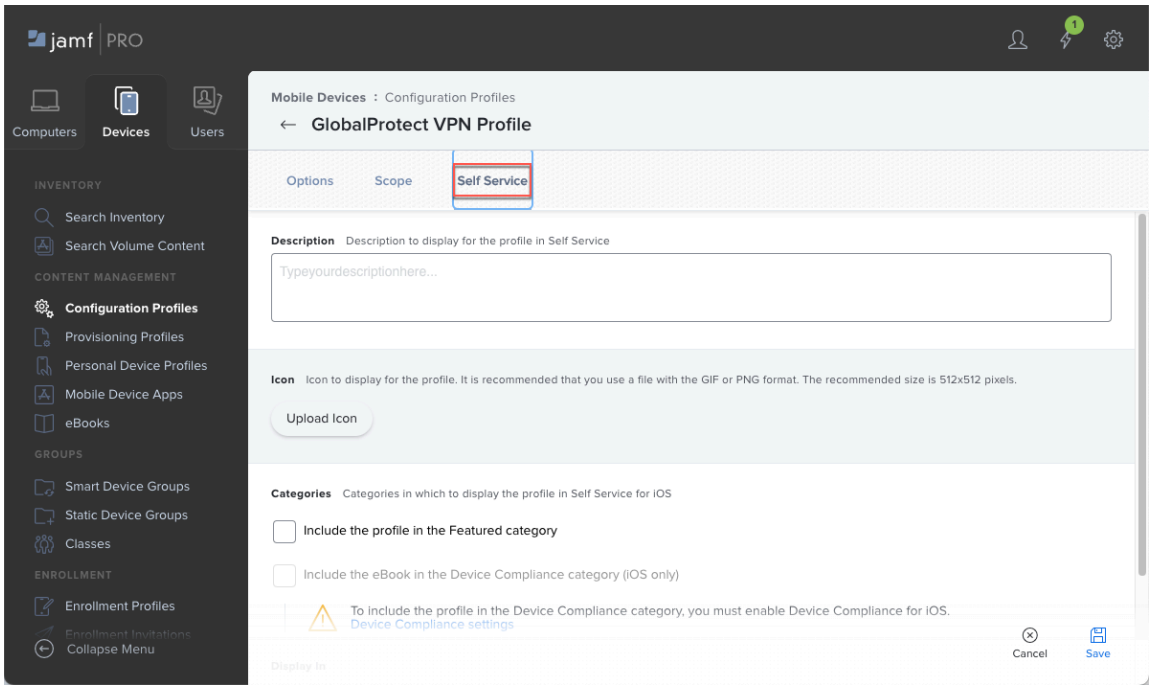
   3. **Add (Modifier)** des périphériques individuels à partir du tableau des **Mobile Devices (Périphériques mobiles)**, ou sélectionnez **Mobile Device Groups (Groupes d'appareils**

 ©2026 Palo Alto Networks, Inc.

mobiles) et **Add (Ajouter)** les groupes de périphériques intelligents ou statiques que vous avez configurés précédemment.



4. (Facultatif) Si vous avez choisi de rendre le profil de configuration disponible dans l'application Self Service, sélectionnez **Self Service** et indiquez comment vous souhaitez que le profil de configuration apparaisse dans l'application Self Service, par exemple en téléchargeant une icône pour le profil ou en incluant le profil dans la catégorie **Featured (En Vedette)** dans Jamf.



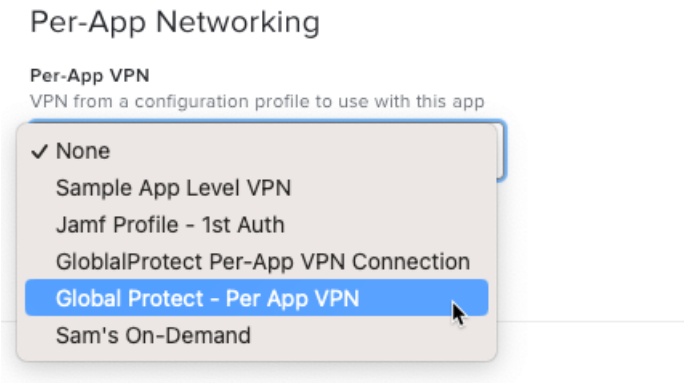
5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

6. Pour vérifier si Jamf Pro a installé le profil de configuration sur un terminal :
   1. Depuis Jamf Pro, sélectionnez **Devices (Périphériques)**.
   2. **Search (Rechercher)** un périphérique mobile.
   3. Sélectionnez un périphérique mobile dans la liste.
   4. Sélectionnez **History (Historique)** et consultez les **Completed Commands (Commandes terminées)**, **Pending Commands (Commandes en attente)** ou **Failed Commands (Commandes échouées)**. Dans les **Completed Commands (Commandes terminées)**, recherchez la commande `Installer le profil de configuration <your_profile>`.

      Si vous ne voyez pas la commande `Installer le profil de configuration <your_profile>` dans la liste, ou si la commande apparaît dans la liste **Fail Commands (Commandes échouées)**, sélectionnez **Management (Gestion)** > **Management Commands (Commandes de gestion)** > **Update Inventory (Mettre à jour l'inventaire)** pour pousser le profil de configuration vers le périphérique.

7. Indiquez lesquelles de vos applications gérées (comme Google Chrome) peut acheminer le trafic à travers le tunnel :
   1. Depuis Jamf Pro, allez à **Devices (Périphériques)** > **Mobile Devices App (Application périphériques mobiles)**.
   2. Sélectionnez l'application gérée dont vous souhaitez envoyer le trafic à travers le tunnel et **Edit (Modifier)**.
   3. Pour **Per-App VPN (VPN par application)**, sélectionnez la connexion VPN par application que vous avez configurée à l'étape 4.



   4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.
   5. Répétez pour chaque application gérée dont vous souhaitez envoyer le trafic à travers le tunnel.

Déployer l'application mobile GlobalProtect pour iOS en utilisant Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

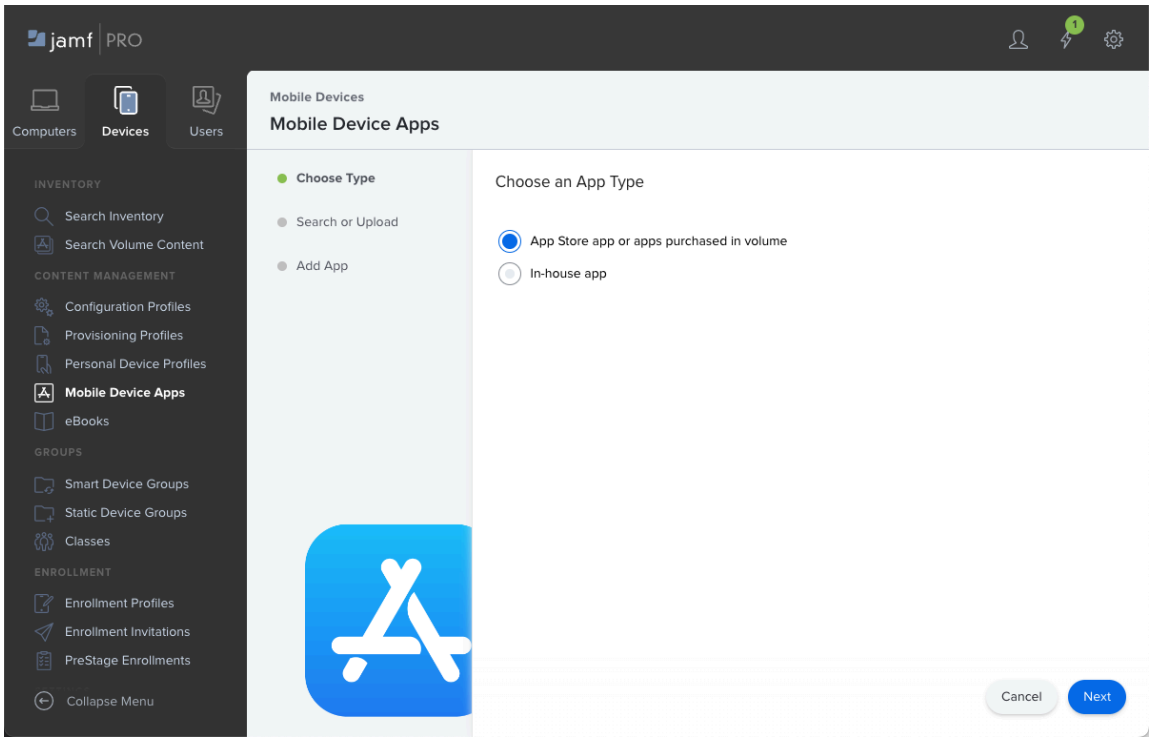
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (géré par Panorama ou Strata Cloud Manager)	Application GlobalProtect pour iOS 6.1 et versions ultérieures Terminaux exécutant des versions iOS prises en charge

Vous pouvez déployer l'application GlobalProtect pour iOS sur les terminaux gérés qui sont enregistrés auprès de Jamf Pro. Après avoir créé un profil de configuration qui configure l'application GlobalProtect pour les utilisateurs finaux, vous pouvez ajouter l'application GlobalProtect à la liste des applications de périphériques mobiles dans Jamf Pro et définir une méthode de distribution pour l'application.

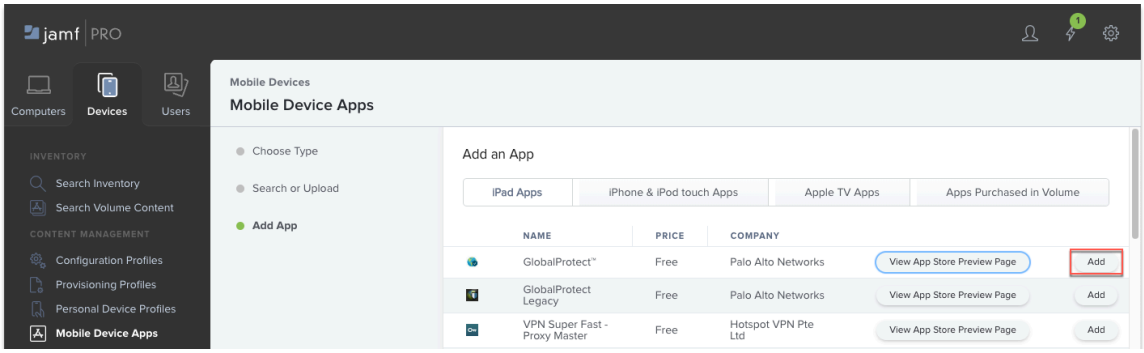
1. Avant de commencer, assurez-vous que les terminaux auxquels vous souhaitez déployer l'application GlobalProtect sont inscrits à Jamf Pro.
2. (Facultatif) Configurez des groupes de périphériques intelligents ou statiques pour regrouper les périphériques iOS gérés qui recevront l'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

3. Ajoutez l'application GlobalProtect à Jamf Pro.
   1. Dans Jamf Pro, sélectionnez **Devices (Périphériques)** > **Mobil Device Apps (Applications de périphériques mobiles)** > **New (Nouveau)**.
   2. Sélectionnez **Applications de l'App Store ou applications achetées en volume** et cliquez sur **Next (Suivant)**.



   3. **Search (Rechercher)** `GlobalProtect` et cliquez sur **Next (Suivant)**.
   4. **Add (Ajouter)** l'application GlobalProtect.



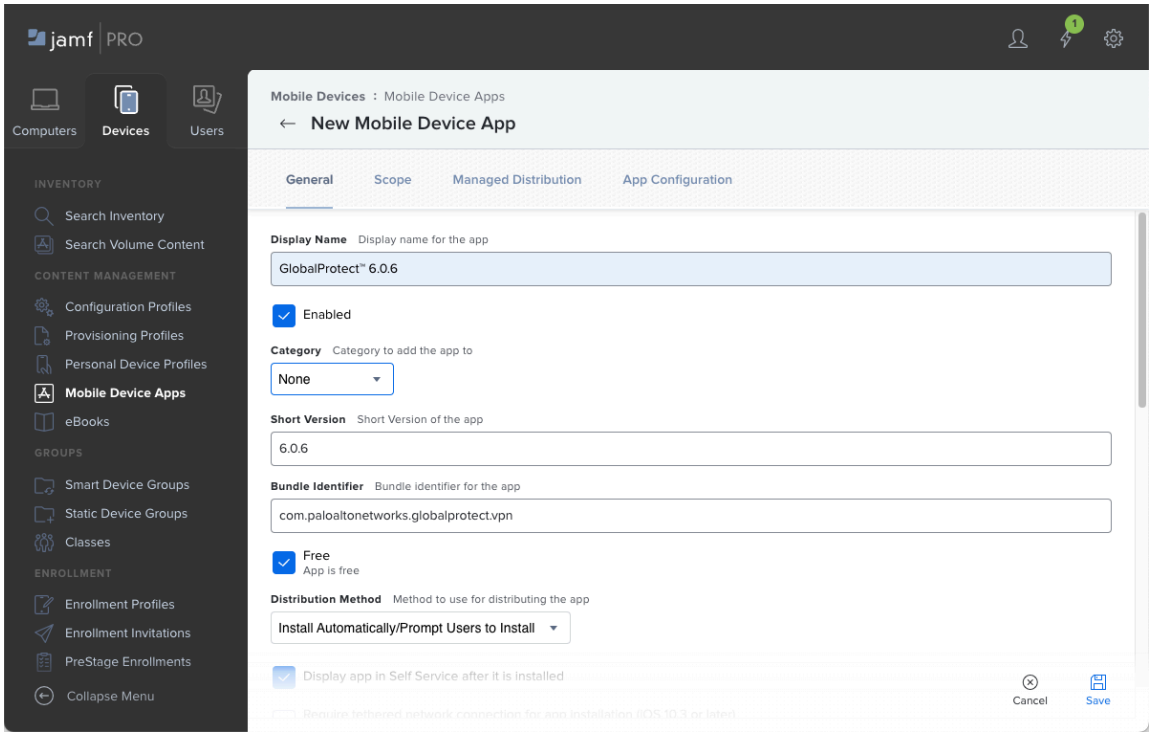
4. Configurez les paramètres **General (généraux)**.
   1. Saisissez un **Display Name (Nom d'affichage)** pour l'application de périphérique mobile.
   2. Assurez-vous que l'application est **Enabled (Activée)** pour le déploiement, sinon elle ne sera pas déployée sur les terminaux.
   3. (Facultatif) Sélectionnez une **Category (Catégorie)** à laquelle vous souhaitez ajouter l'application.
   4. Sélectionnez une **Distribution Method (Méthode de distribution)**, soit **Make available in Self Service (Rendre disponible dans Self Service)**, ce qui permet à l'utilisateur final de

 ©2026 Palo Alto Networks, Inc.

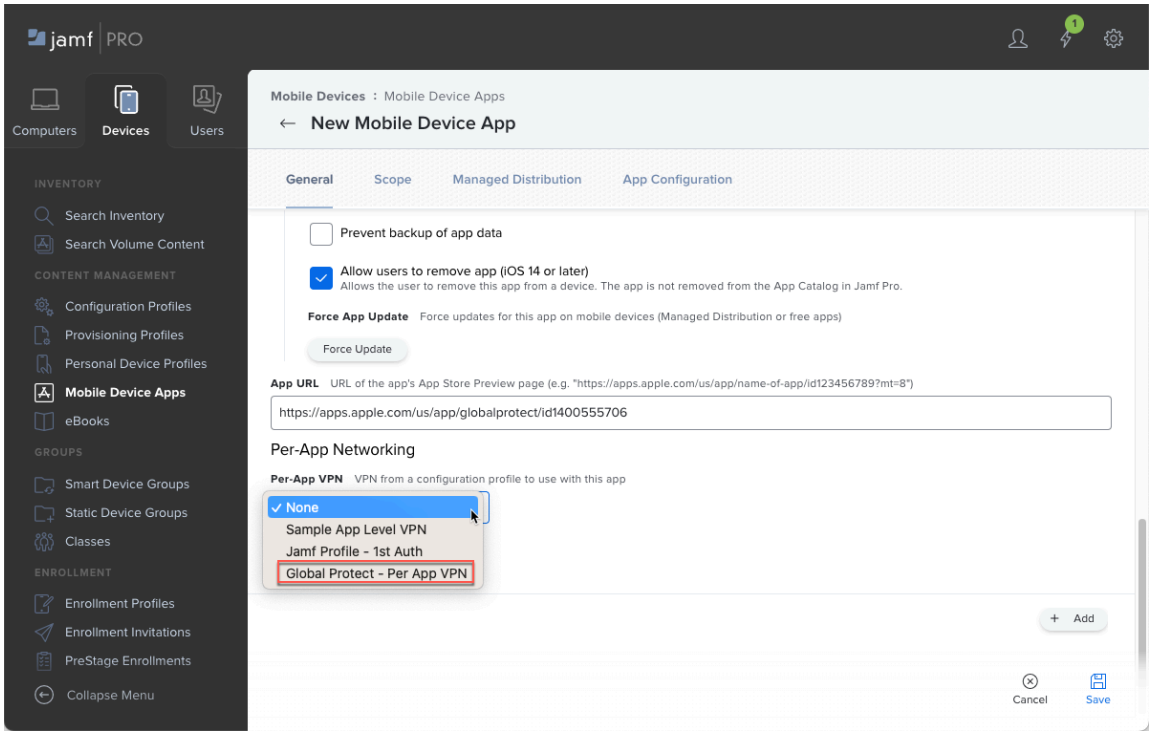
télécharger l'application depuis l'application Jamf Self Service, ou **Install Automatically/ Prompt Users to Install (Installer automatiquement/Inviter les utilisateurs à installer)**,

 ©2026 Palo Alto Networks, Inc.

ce qui pousse l'application sur le périphérique de l'utilisateur final automatiquement ou invite l'utilisateur à l'installer.



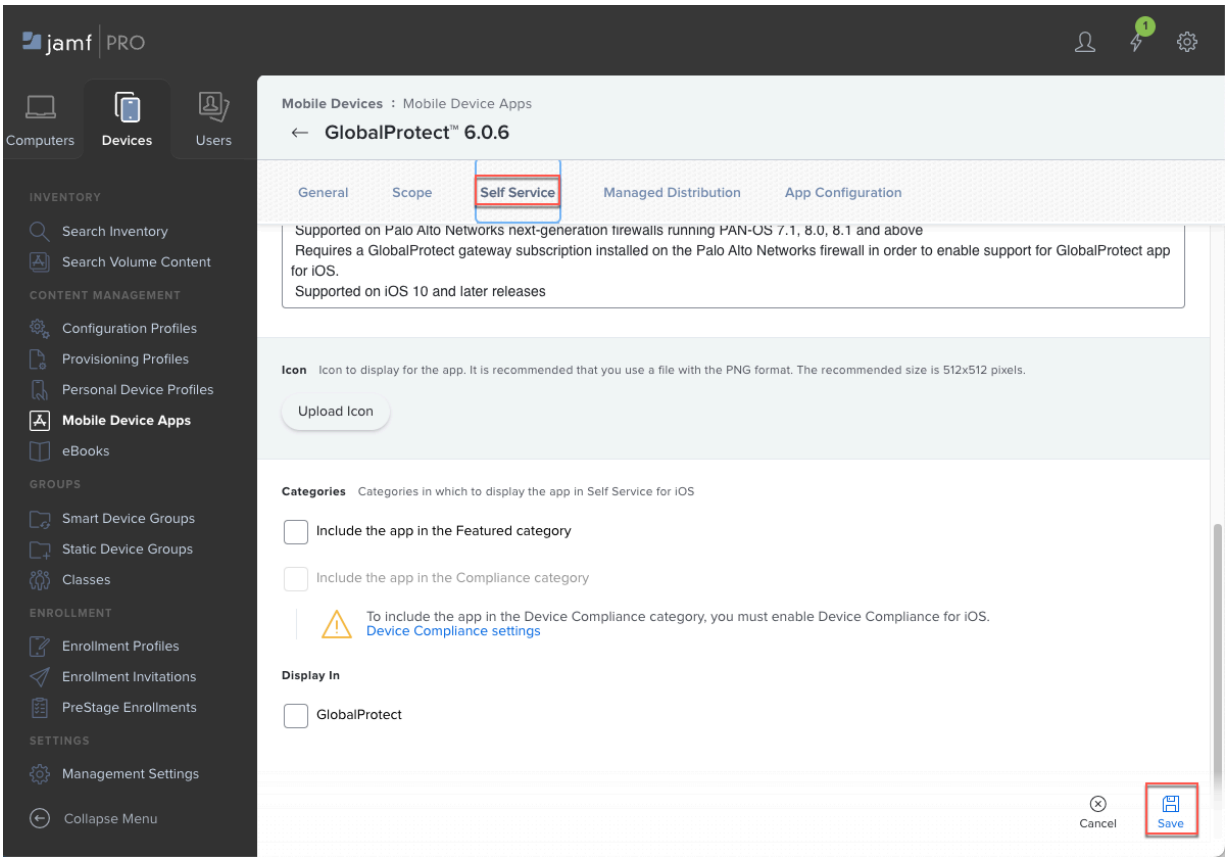
5. (Facultatif) Sélectionnez un profil de configuration **Per-App VPN (VPN par application)** si vous en avez déjà configuré un.



6. Spécifiez d'autres Jamf settings (Paramètres Jamf) si nécessaire et **Save (Enregistrez)** vos paramètres.

 ©2026 Palo Alto Networks, Inc.

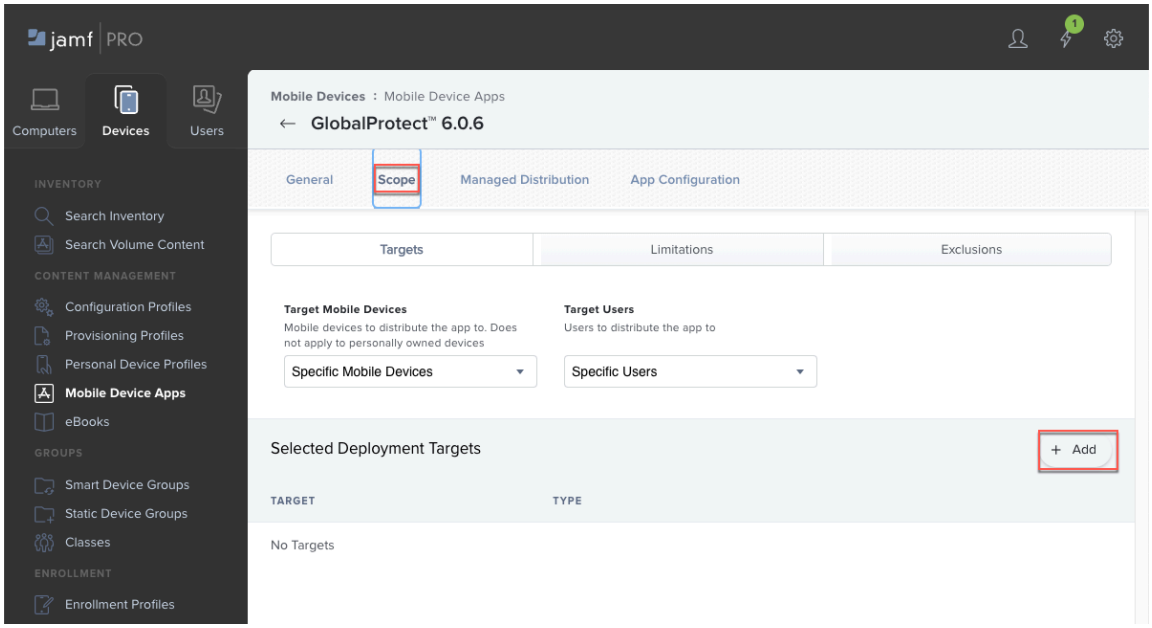
5. (Facultatif) Si vous avez choisi de rendre l'application GlobalProtect disponible dans l'application Self Service, sélectionnez **Self Service** et spécifiez comment vous souhaitez que l'application GlobalProtect apparaisse dans l'application Self Service, comme télécharger une icône pour l'application ou inclure l'application dans la catégorie **Featured (En vedette)** dans Jamf.



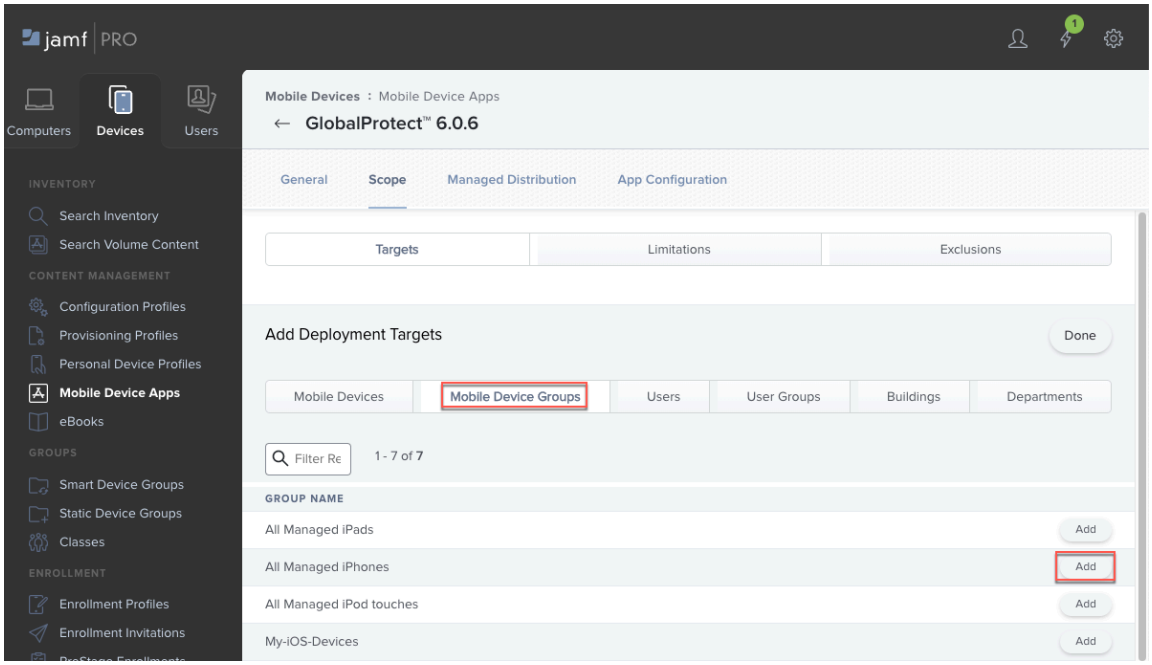
Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

6. Définissez la portée pour définir les périphériques qui recevront l'application.
   1. Cliquez sur **Edit (Modifier)** si vous avez enregistré vos paramètres à l'étape précédente.
   2. Sélectionnez **Scope (Portée)** et **Add (Ajouter)** une cible de déploiement.



   3. **Add (Modifier)** des périphériques individuels à partir du tableau des **Mobile Devices (Périphériques mobiles)**, ou sélectionnez **Mobile Device Groups (Groupes d'appareils mobiles)** et **Add (Ajouter)** les groupes de périphériques intelligents ou statiques que vous avez configurés précédemment.



   4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

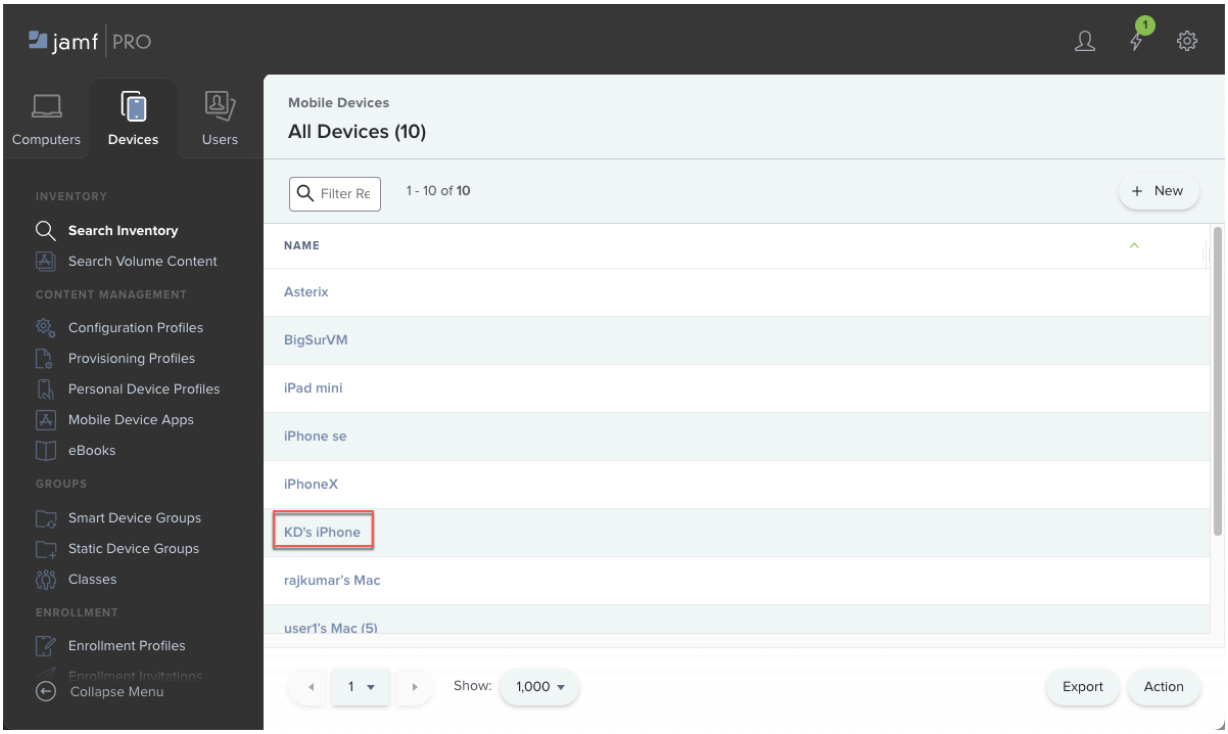
 ©2026 Palo Alto Networks, Inc.

Vérifier le déploiement de l'application GlobalProtect pour iOS à l'aide de Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect pour iOS 6.1 et versions ultérieures Terminaux exécutant des versions iOS prises en charge

Après que vous Déployer l'application mobile GlobalProtect pour iOS en utilisant Jamf Pro, vous pouvez vérifier si Jamf Pro a installé l'application GlobalProtect sur un terminal iOS.

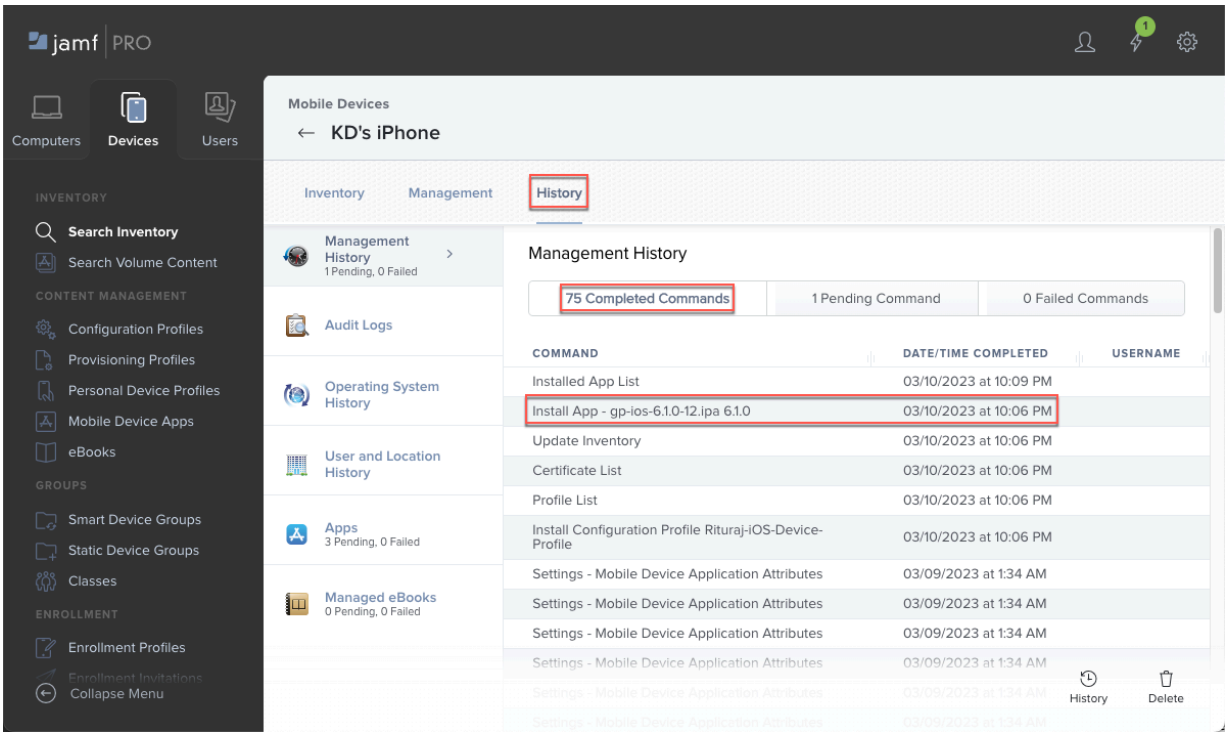
1. Depuis Jamf Pro, sélectionnez **Devices (Périphériques)**.
2. **Search (Rechercher)** un périphérique mobile.
3. Sélectionnez un périphérique mobile dans la liste.



4. Sélectionnez **History (Historique)** et consultez les **Completed Commands (Commandes terminées)**, **Pending Commands (Commandes en attente)** ou **Failed Commands (Commandes**

 ©2026 Palo Alto Networks, Inc.

échouées). Dans les **Completed Commands (Commandes terminées)**, recherchez la commande `Installer l'application – <app_filename>` pour GlobalProtect.



Si vous ne voyez pas la commande `Installer l'application – <app_filename>` dans la liste, ou si la commande apparaît dans la liste **Fail Commands (Commandes échouées)**, sélectionnez **Management (Gestion)** > **Management Commands (Commandes de gestion)** > **Update Inventory (Mettre à jour l'inventaire)** pour pousser l'application GlobalProtect vers le périphérique.

5. Répétez les étapes 1 – 4 pour vérifier le déploiement de l'application GlobalProtect.

Gérez l'application GlobalProtect pour macOS en utilisant Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect pour macOS 6.0.4 et versions ultérieures et 6.1 et versions ultérieures Terminaux exécutant macOS 11 (Big Sur), macOS 12 (Monterey) ou macOS 13 (Ventura)

Vous pouvez utiliser Jamf Pro pour déployer l'application GlobalProtect pour macOS avec un script personnalisé contenant des paramètres plist GlobalProtect, qui peut être exécuté avant ou après l'installation du client GlobalProtect. Vous pouvez également utiliser des profils de

 ©2026 Palo Alto Networks, Inc.

configuration Jamf Pro pour empêcher les notifications des utilisateurs finaux en chargeant automatiquement les extensions système et réseau liées à des fonctionnalités telles que la segmentation de tunnel, le DNS segmenté et l'application de la politique.

> *La méthode de profil de configuration Jamf Pro pour déployer les paramètres VPN n'est pas prise en charge. Vous pouvez configurer les paramètres VPN via le portail GlobalProtect ou en utilisant les paramètres plist GlobalProtect avant de pouvoir déployer l'application à l'aide de Jamf Pro.*

Créer un groupe d'ordinateurs intelligents pour le déploiement de l'application GlobalProtect

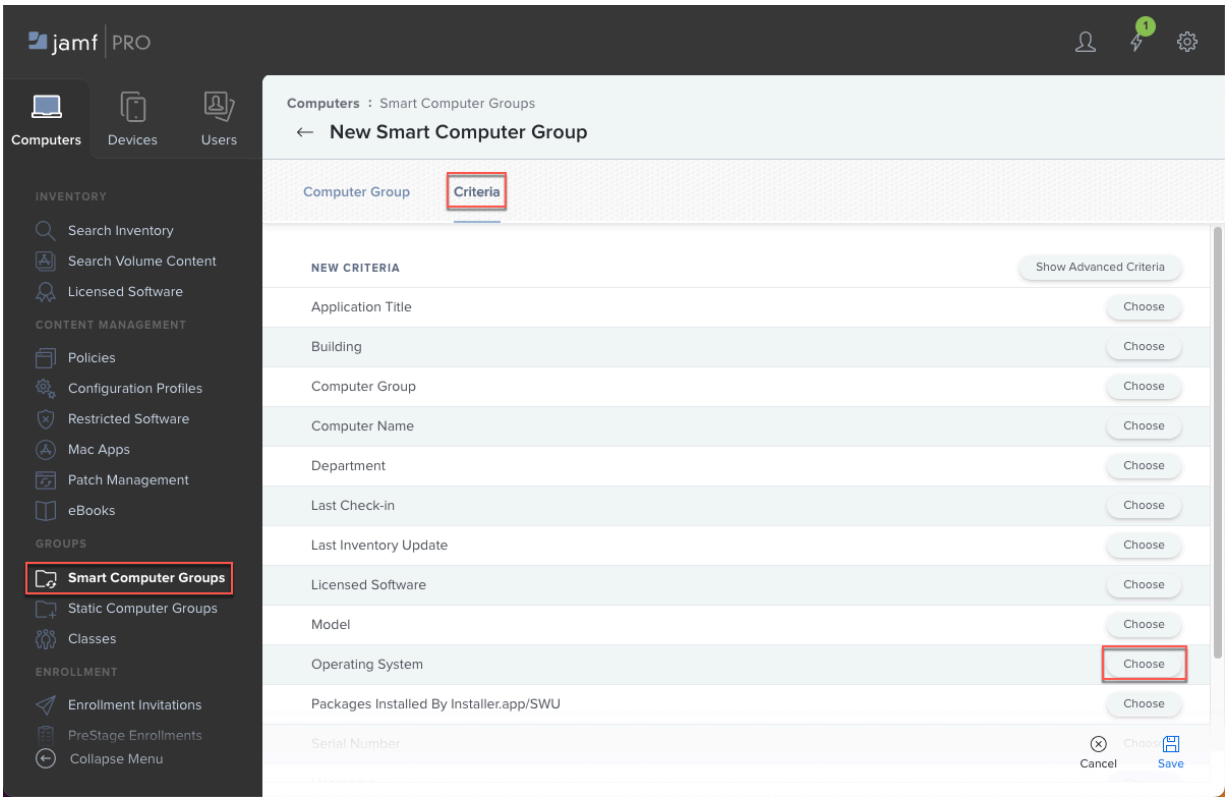
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez créer un groupe d'ordinateurs intelligents dans Jamf Pro pour cibler les périphériques macOS gérés pour l'installation de l'application GlobalProtect. Lorsque vous configurez des profils de configuration ou des politiques Jamf pour le déploiement de l'application GlobalProtect, vous pouvez définir la portée sur le groupe d'ordinateurs intelligents que vous avez créé.

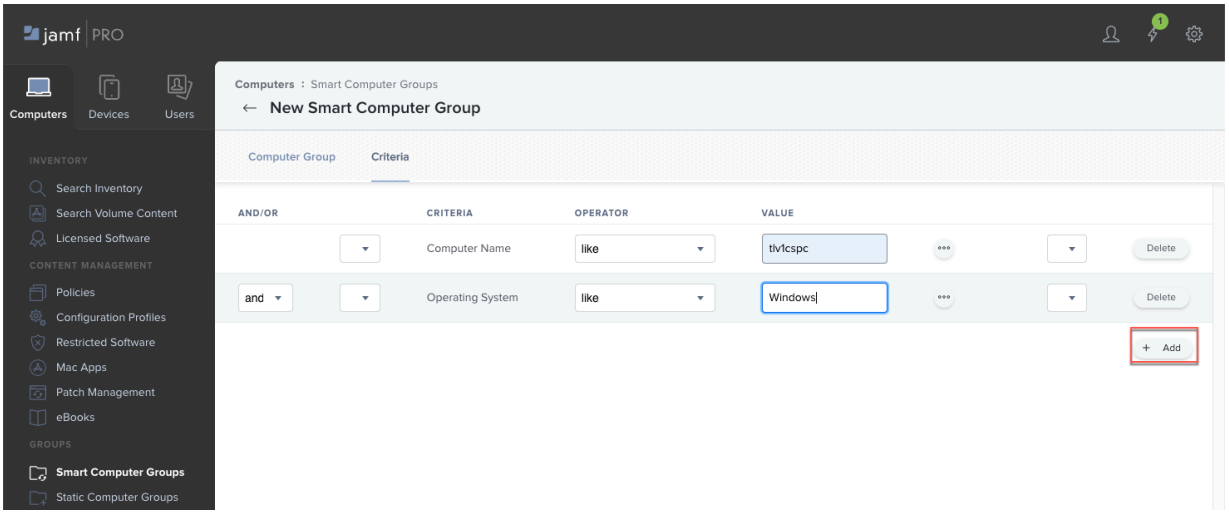
1. Dans Jamf Pro, sélectionnez **Computers (Ordinateurs)** > **Smart Computer Groups (Groupes d'ordinateurs intelligents)** > **New (Nouveau)**.
2. Saisissez un **Display Name (Nom d'affichage)** pour le groupe.
3. Sélectionnez **Criteria (Critères)** et **Add (Ajouter)** un critère pour le groupe.

 ©2026 Palo Alto Networks, Inc.

4. **Choose (Choisir)** un critère dans la liste.



5. Sélectionnez **Operator (Opérateur)** et la **Value (Valeur)** pour les critères. Si nécessaire, vous pouvez **Add (Ajouter)** d'autres critères.



6. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

Créer un profil de configuration unique pour l'application GlobalProtect pour macOS

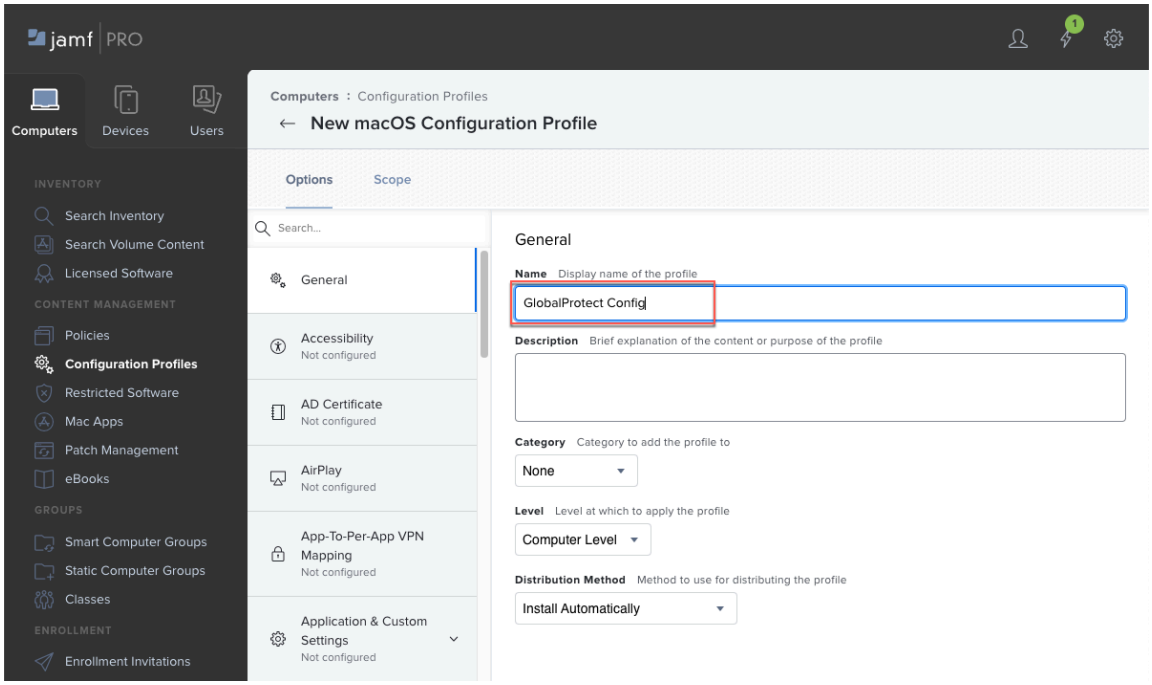
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Avant de Déployer l'application mobile GlobalProtect pour macOS en utilisant Jamf Pro, vous pouvez créer et déployer un profil de configuration unique qui définit la configuration de l'application GlobalProtect 6.0.4 et versions ultérieures et 6.1 ainsi que les versions ultérieures sur les périphériques macOS gérés. Par exemple, vous pouvez configurer le profil de configuration pour charger des extensions système afin de fournir une expérience fluide lorsque les utilisateurs exécutent l'application GlobalProtect pour accéder à Internet, aux applications SaaS, aux applications privées et aux ressources de votre organisation.

> *Si vous souhaitez utiliser plusieurs profils de configuration au lieu d'un profil de configuration unique, passez cette procédure et* Activer les extensions système et réseau sur les terminaux macOS à l'aide de plusieurs profils de configuration.

Avant de commencer, Créer un groupe d'ordinateurs intelligents pour le déploiement de l'application GlobalProtect afin que vous puissiez déployer ce profil de configuration sur les ordinateurs du groupe d'ordinateurs intelligents.

1. Créez un profil de configuration pour l'application GlobalProtect et spécifiez les paramètres généraux.
   1. Dans Jamf Pro, sélectionnez **Computers (Ordinateurs)** > **Configuration Profiles (Profils de configuration)** > **New (Nouveau)**.
   2. Entrez un **Display Name (Nom d'affichage)** pour le profil de configuration.

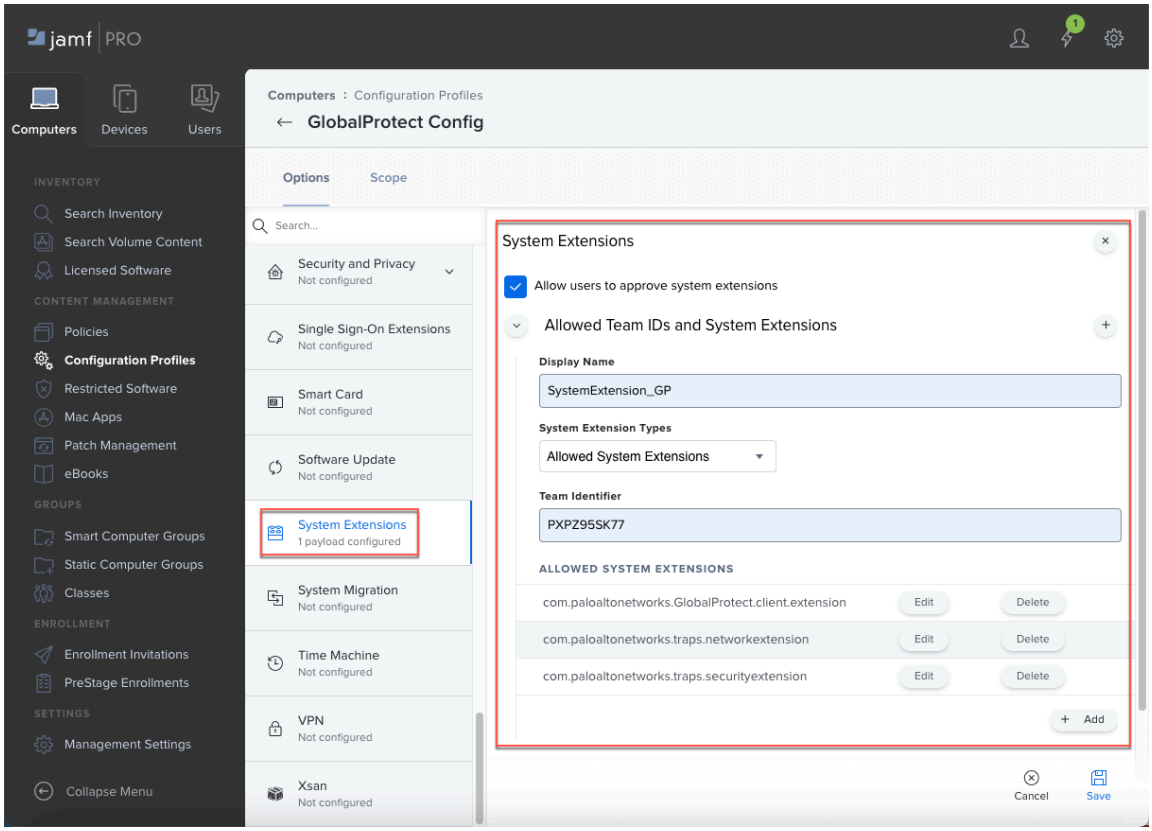


 ©2026 Palo Alto Networks, Inc.

2. Créez une charge utile pour charger automatiquement les extensions système GlobalProtect. Cette configuration supprime les fenêtres contextuelles de notification et permet à l'application GlobalProtect de fonctionner sans demander aux utilisateurs d'accepter les extensions.
   1. Si vous avez enregistré vos paramètres à l'étape précédente, cliquez sur **Edit (Modifier)**.
   2. Sélectionnez **System Extensions (Extensions du système)** > **Configure (Configurer)**.

 ©2026 Palo Alto Networks, Inc.

3. Définissez les paramètres suivants :
   - **Display Name (Nom d'affichage)** : entrez un nom pour la charge utile des extensions système, tel que **`SystemExtension_GP`**
   - **System Extension Types (Types d'extensions de système)** : sélectionnez **Allowed System Extensions (Extensions de système autorisées)**
   - **Team Identifier (Identifiant d'équipe)** : saisissez **PXPZ95SK77**
   - **ALLOWED SYSTEM EXTENSIONS (EXTENSIONS SYSTÈME AUTORISÉES)** : **Add (Ajouter)** et **Save (Enregistrer)** les extensions système suivantes :
     - **`com.paloaltonetworks.GlobalProtect.client.extension`** : active les extensions système, qui sont utilisées pour la segmentation de tunnel et applique les connexions GlobalProtect pour les fonctionnalités d'accès réseau
     - **`com.paloaltonetworks.traps.networkextension`** : active les extensions réseau pour Cortex XDR (nécessaire uniquement si vous utilisez Cortex XDR)
     - **`com.paloaltonetworks.traps.securityextension`** : active les extensions de sécurité pour Cortex XDR (nécessaire uniquement si vous utilisez Cortex XDR)



4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

3. Si vous avez configuré l'application GlobalProtect avec la fonctionnalité appliquer les connexions GlobalProtect pour l'accès réseau (exécutant) sur les terminaux macOS, créez une charge utile pour filtrer le contenu réseau.
   1. Si vous avez enregistré vos paramètres à l'étape précédente, cliquez sur **Edit (Modifier)**.
   2. Sélectionnez **Content Filter (Filtre de contenu)**.
   3. Définissez les paramètres suivants :
      - **Filter Name (Nom du filtre)** : entrez le nom du filtre, comme **`GlobalProtectEn`**
      - **Identifier (Identifiant)** : entrez **`com.paloaltonetworks.GlobalProtect.client`**
      - **Socket Filter Bundle Identifier (Identifiant de groupe du filtre de socket)** : entrez **`com.paloaltonetworks.GlobalProtect.client.extension`**
      - **Socket Filter Designated Requirement (Exigence désignée du filtre de socket)** : entrez la condition suivante :

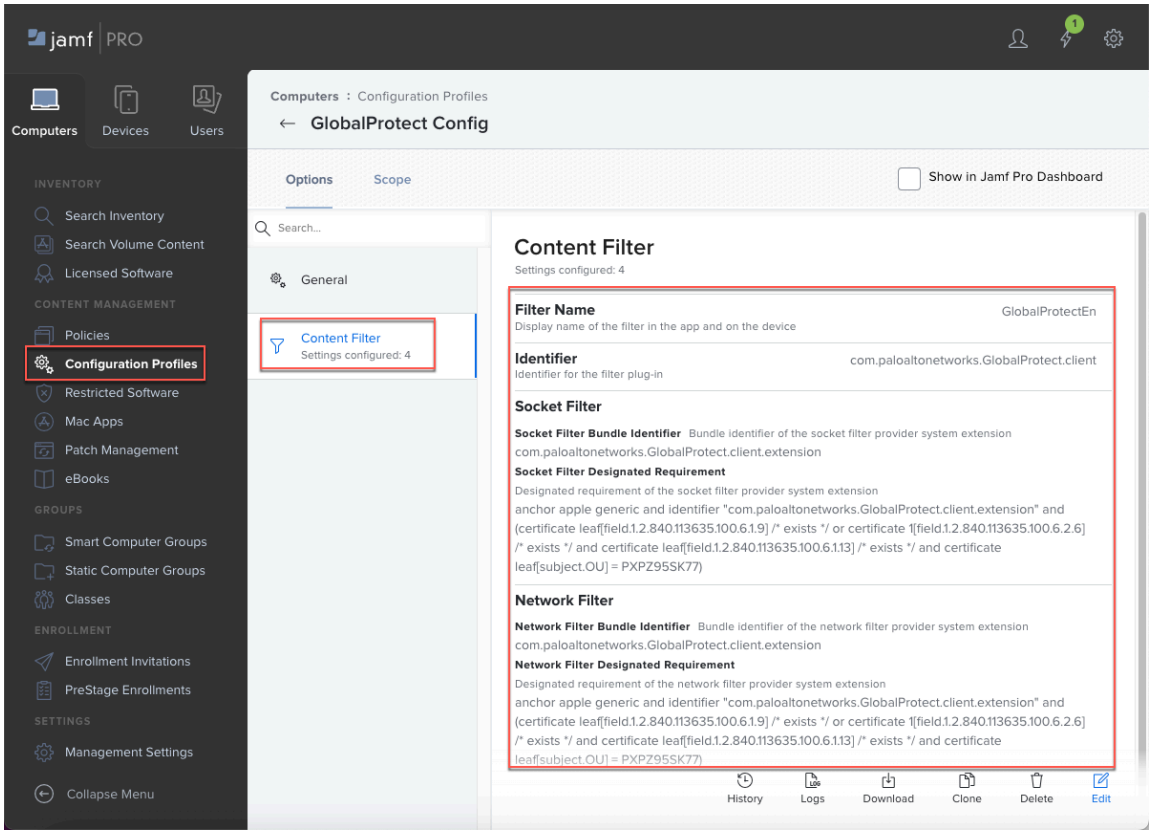
        ```
        ancre apple générique et identifiant
        "com.paloaltonetworks.GlobalProtect.client.extension" and
        (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists
        */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists
        */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*
        exists */ and certificate leaf[subject.OU] = PXPZ95SK77)
        ```

      - **Network Filter Bundle Identifier (Identifiant de groupe du filtre de réseau)** : entrez **`com.paloaltonetworks.GlobalProtect.client.extension`**
      - **Network Socket Filter Designated Requirement (Exigence désignée du filtre réseau)** : entrez la condition suivante :

        ```
        anchor apple generic and identifier
        "com.paloaltonetworks.GlobalProtect.client.extension" and
        (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists
        */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists
        ```

 ©2026 Palo Alto Networks, Inc.

```
*/ and certificate leaf[field.1.2.840.113635.100.6.1.13] /*
exists */ and certificate leaf[subject.OU] = PXPZ95SK77)
```

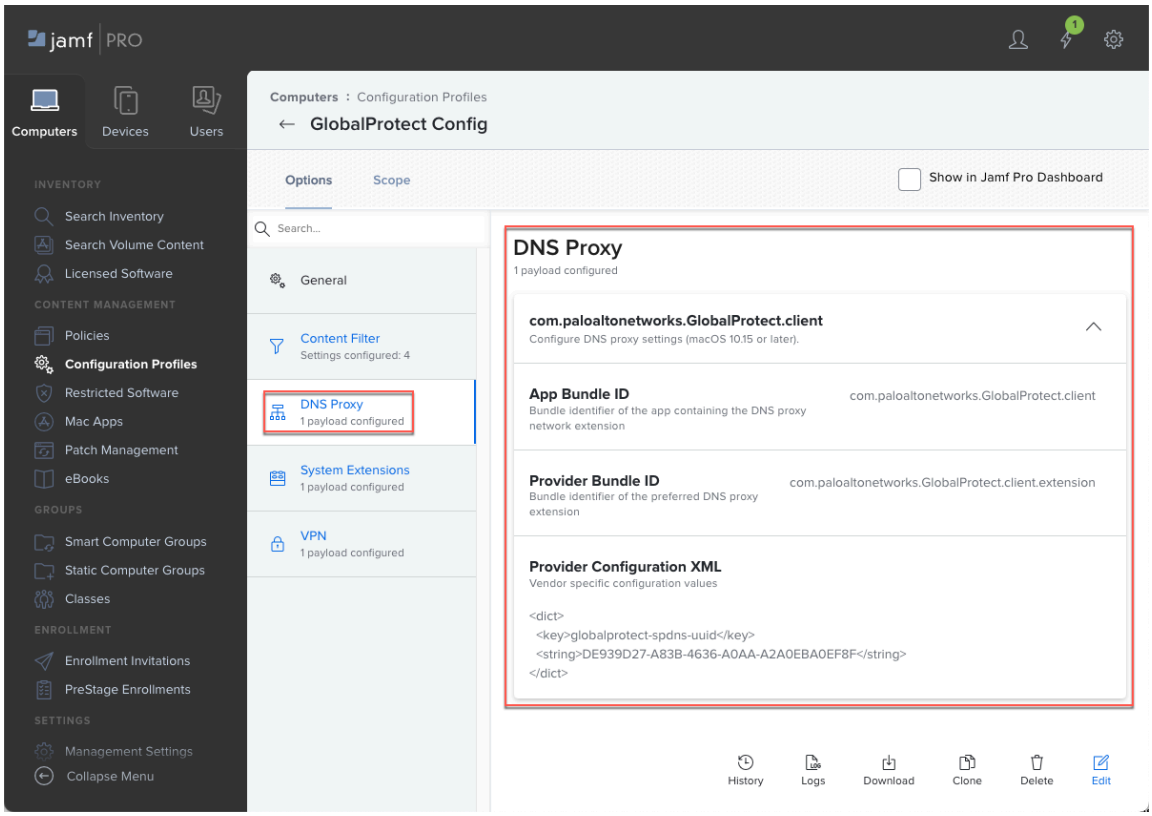


4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

4. Facultatif : Créez une charge utile de proxy DNS si vous avez configuré la fonctionnalité Split DNS (Segmentation du DNS).
   1. Si vous avez enregistré vos paramètres à l'étape précédente, cliquez sur **Edit (Modifier)**.
   2. Sélectionnez **DNS Proxy (Proxy DNS)** > **Add (Ajouter)**.
   3. Définissez les paramètres suivants :
      - **App Bundle ID (Identifiant du groupe d'applications)** : entrez **`com.paloaltonetworks.GlobalProtect.client`**
      - **Provider Bundle ID (Identifiant du groupe de fournisseurs)** : entrez **`com.paloaltonetworks.GlobalProtect.client.extension`**
      - **Provider Configuration XML (XML de configuration du fournisseur)** : entrez le texte suivant :

```
<dict> <key>globalprotect-spdns-uuid</key> <string>DE939D27-A83B-4636-A0AA-A2A0EBA0EF8F</string> </dict>
```



 ©2026 Palo Alto Networks, Inc.

5. Facultatif : Si vous avez configuré une segmentation de tunnel pour inclure ou exclure le trafic en fonction des applications, créez une charge utile VPN.

   Il ne peut y avoir qu'une seule charge utile VPN par profil de configuration. Si vous avez besoin de plus d'une charge utile VPN, vous devez créer un profil de configuration séparé avec la charge utile supplémentaire.

   1. Si vous avez enregistré vos paramètres à l'étape précédente, cliquez sur **Edit (Modifier)**.
   2. Sélectionnez **VPN** > **Configure (Configurer)**.
   3. Définissez les paramètres suivants :
      - **Connection Name (Nom de la connexion)** : entrez un nom pour la connexion, tel que **`GP_split_tunnel_app`**
      - **VPN Type (Type de VPN)** : sélectionnez **Per-App VPN (VPN par application)**
      - **Per-App VPN Connection Type (Type de connexion VPN par application)** : sélectionnez **Custom SSL (SSL personnalisé)**
      - **Identifier (Identifiant)** : entrez **`com.paloaltonetworks.GlobalProtect.client`**
      - **Server (Serveur)** : entrez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs vont se connecter
      - **Custom Data (Données personnalisées)** : **Add (Ajouter)** et **Save (Enregistrer)** la clé et la valeur suivantes :
        - **KEY (CLÉ)** : entrez **`globalprotect-spapp-uuid`**
        - **VALUE (VALEUR)** : entrez **`B078FC83-11E5-4559-AA53-E24D2A63B0F9`**
      - **Provider Type (Type de fournisseur)** : sélectionnez **App-proxy (Proxy d'application)**
   4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

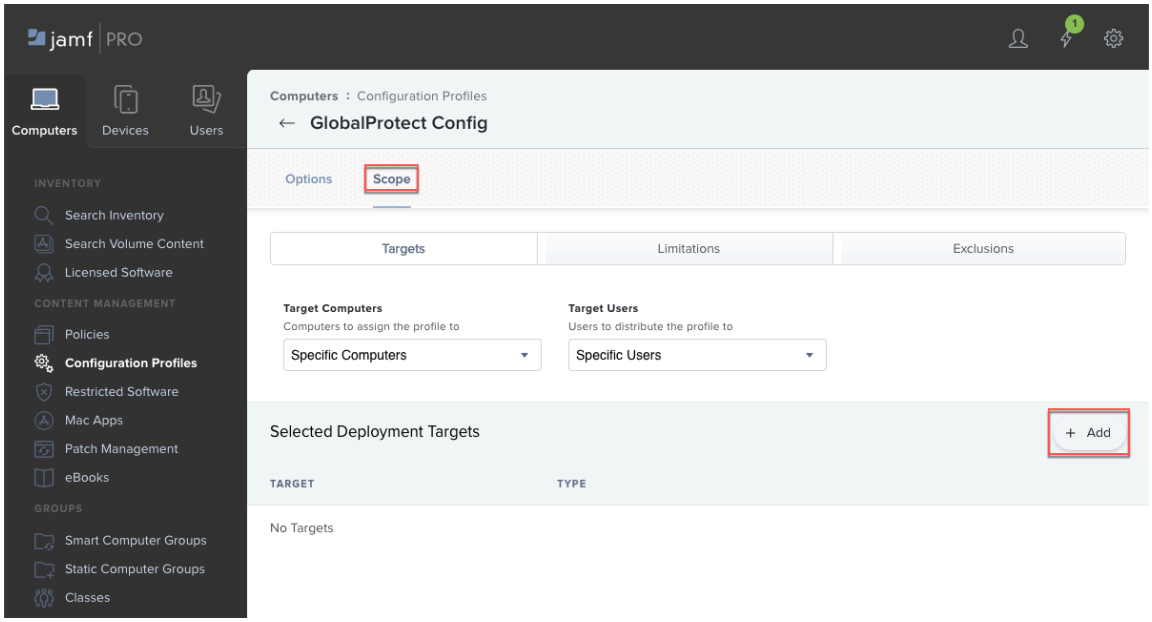
6. Facultatif : Si vous avez configuré une segmentation de tunnel pour inclure ou exclure le trafic en fonction du domaine, créez une charge utile VPN.

   Il ne peut y avoir qu'une seule charge utile VPN par profil de configuration. Si vous avez besoin de plus d'une charge utile VPN, vous devez créer un profil de configuration séparé avec la charge utile supplémentaire.

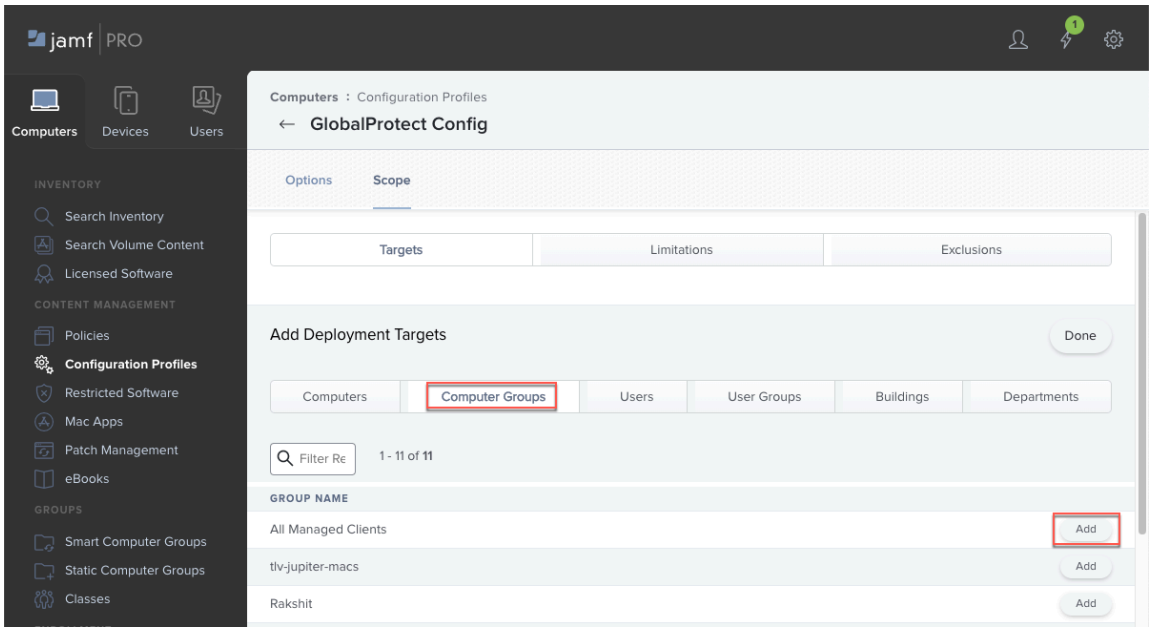
   1. Si vous avez enregistré vos paramètres à l'étape précédente, cliquez sur **Edit (Modifier)**.
   2. Sélectionnez **VPN** > **Configure (Configurer)**.
   3. Définissez les paramètres suivants :
      - **Connection Name (Nom de la connexion)** : entrez un nom pour la connexion, tel que **`GP_split_tunnel_domain`**
      - **VPN Type (Type de VPN)** : sélectionnez **Per-App VPN (VPN par application)**
      - **Per-App VPN Connection Type (Type de connexion VPN par application)** : sélectionnez **Custom SSL (SSL personnalisé)**
      - **Identifier (Identifiant)** : entrez **`com.paloaltonetworks.GlobalProtect.client`**
      - **Server (Serveur)** : entrez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs vont se connecter
      - **Custom Data (Données personnalisées)** : **Add (Ajouter)** et **Save (Enregistrer)** la clé et la valeur suivantes :
        - **KEY (CLÉ)** : entrez **`globalprotect-spdomain-uuid`**
        - **VALUE (VALEUR)** : entrez **`0894A92D-70D2-475A-B5B6-FB07F2DEAA77`**
      - **Provider Type (Type de fournisseur)** : sélectionnez **App-proxy (Proxy d'application)**
   4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

7. Définissez la portée pour le profil de configuration.
   1. **Edit(Modifier)** le profil de configuration.
   2. Sélectionnez **Scope (Portée)** et **Add (Ajouter)** une cible de déploiement.

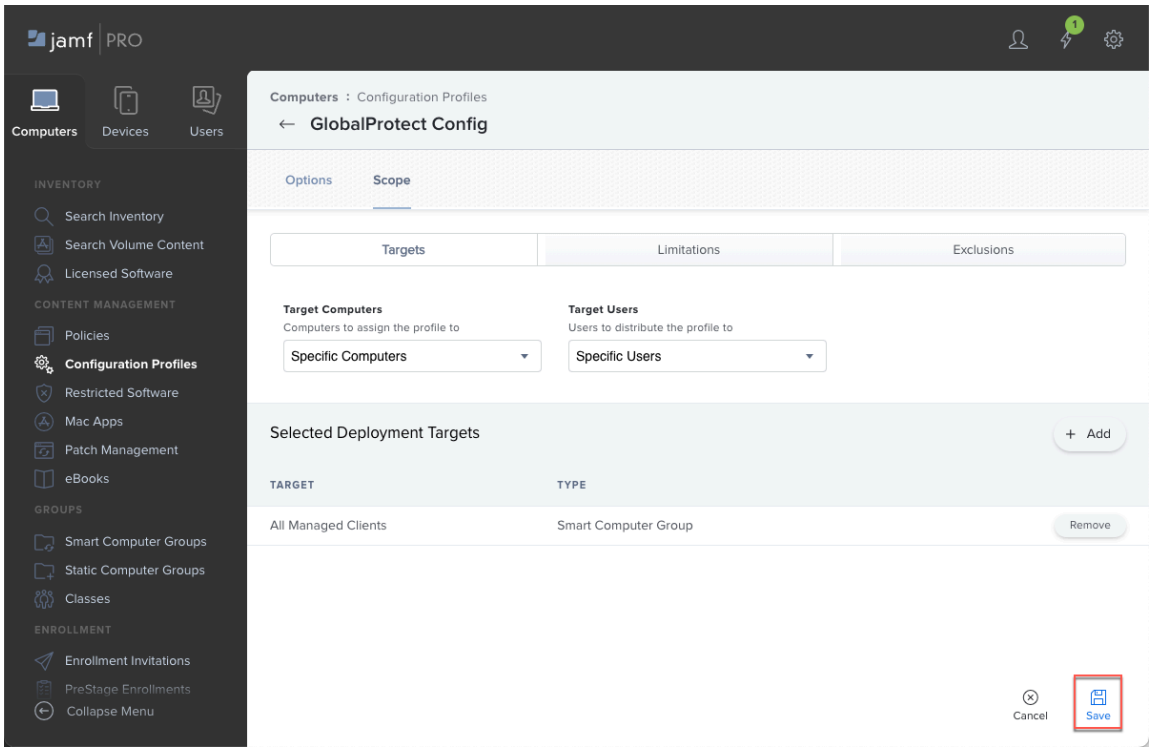


   3. Cliquez sur **Computer Groups (Groupes d'ordinateurs)** et **Add (Ajouter)** le groupe d'ordinateurs intelligents que vous avez créé. Cliquez ensuite sur **Done (Terminé)**.



   4. **Save (Enregistrer)** la portée du profil. Jamf distribuera le profil aux appareils du groupe d'ordinateurs sélectionné la prochaine fois qu'ils contacteront Jamf Pro.

 ©2026 Palo Alto Networks, Inc.



Déployer l'application mobile GlobalProtect pour macOS en utilisant Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

À partir de l'application GlobalProtect 6.0.4 et des versions ultérieures et 6.1, vous pouvez déployer l'application GlobalProtect sur des terminaux macOS gérés qui se sont inscrits avec Jamf Pro en utilisant un script qui préremplit les paramètres de l'application GlobalProtect tels que l'adresse du portail par défaut et la méthode de connexion. En tant que meilleure pratique, vous pouvez également cibler l'installation ou la mise à niveau de l'application sur un groupe plus restreint de terminaux avant de déployer l'installation au reste de votre organisation.

Si vous avez configuré des portails GlobalProtect doubles, vous pouvez configurer le script pour prendre en charge plusieurs portails. Cette méthode ne fonctionne que lors des déploiements initiaux, lorsque vous déployez l'application GlobalProtect pour la première fois sur vos terminaux sans aucune configuration préexistante. Dans ce cas, vous devez configurer la politique Jamf pour exécuter le script avant d'installer le package GlobalProtect.

> *Pour une démonstration sur la façon de déployer l'application GlobalProtect en utilisant Jamf Pro, regardez cette vidéo.*

Pour des instructions étape par étape, reportez-vous à la procédure suivante :

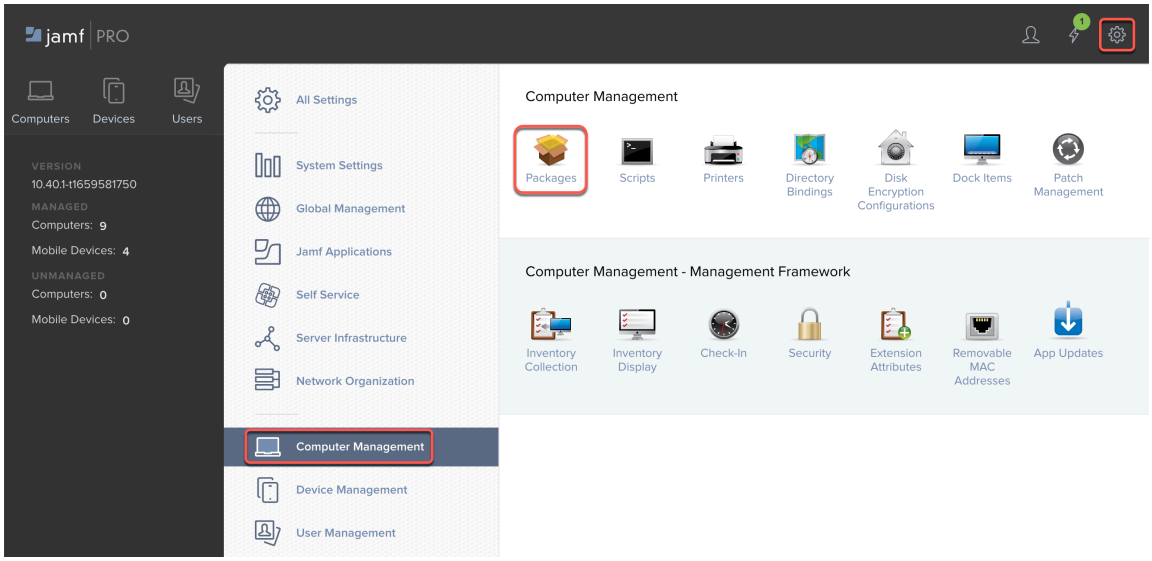
 ©2026 Palo Alto Networks, Inc.

1. Téléchargez le package de l'application GlobalProtect pour macOS depuis le portail de support client.
   1. Connectez-vous au portail de support client de Palo Alto Networks (https://support.paloaltonetworks.com/).

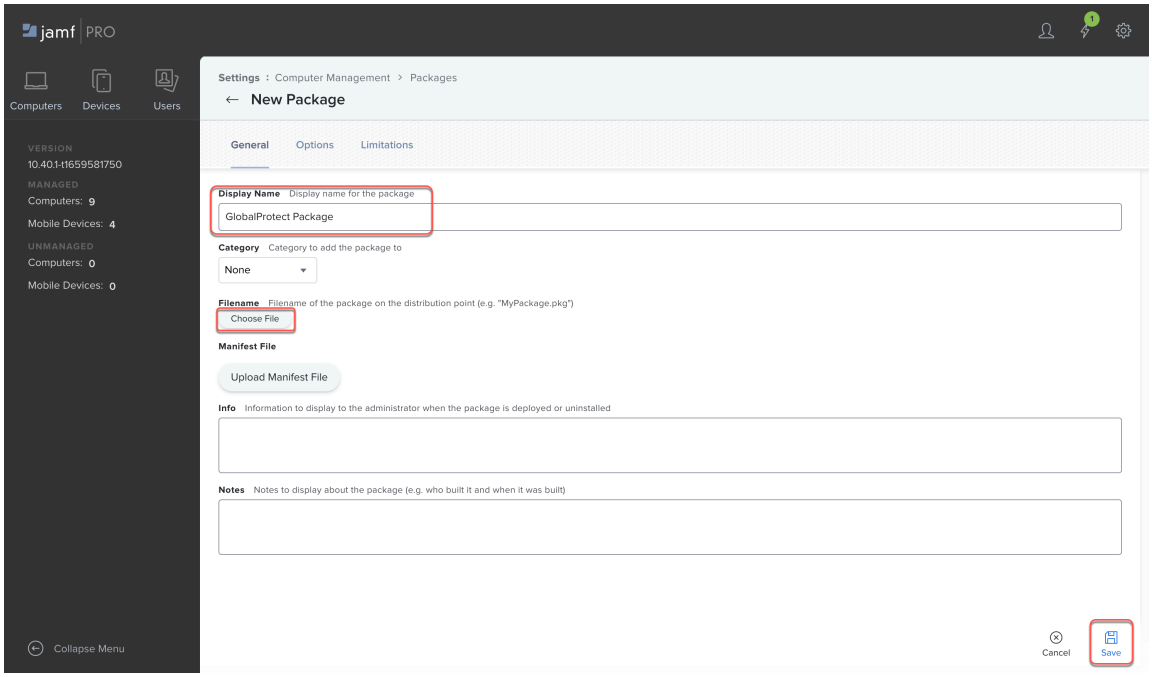
      Vous devez disposer d'un compte valide sur le portail du support client de Palo Alto Networks pour vous connecter et télécharger des logiciels à partir de la page Mises à jour logicielles.
   2. Sélectionnez **Mises à jour** > **Mises à jour logicielles**.
   3. Sélectionne la version active de l'application GlobalProtect pour macOS
   4. Passez en revue les Notes de version de la version de l'application, puis sélectionnez le lien de téléchargement.

 ©2026 Palo Alto Networks, Inc.

2. Téléchargez le fichier PKG de l'application GlobalProtect sur Jamf Pro :
   1. Sélectionnez **Settings (Paramètres)** > **Computer Management (Gestion des ordinateurs)** > **Packages**.



   2. Cliquez sur **New (Nouveau)**.
   3. Configurez les paramètres généraux pour le package, y compris le nom d'affichage et la catégorie (facultatif).
   4. Cliquez sur **Choose File (Choisir un fichier)** et sélectionnez le package de l'application GlobalProtect à télécharger.
   5. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.



 ©2026 Palo Alto Networks, Inc.

3. Créez un script que vous ajouterez à Jamf Pro qui préremplit les paramètres par défaut, tels que le portail GlobalProtect par défaut et la méthode de connexion. Vous pouvez également configurer le script pour prendre en charge plusieurs portails GlobalProtect.

Les exemples suivants sont fournis à titre de référence. Personnalisez le script et les paramètres de l'application selon vos besoins pour votre environnement.

Script de portail unique :

```
#!/bin/bash ## Description : Checks for global preferences file
 and populates ## it with the default portal if needed. ## Body
 ########################################################## ##
 Declare Variables ##############################################
 # Get current Console user active_user=$( stat -f "%Su" /
dev/console ) # Global Prefs File gPrefs=/Library/Preferences/
com.paloaltonetworks.GlobalProtect.settings.plist ## Logic
 ########################################################## #
 Check to see if the global preference file already exists...
 if [[ -e $gPrefs ]]; then echo "Default global portal already
 exists. Skipping." else echo "Setting default global portal to:
 your.portal.here.com" # If it does not already exist, create
 it and populate the default portal using the echo command
 echo '<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist
 PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd"> <plist version="1.0"> <dict>
 <key>Palo Alto Networks</key> <dict> <key>GlobalProtect</
key> <dict> <key>PanSetup</key> <dict> <key>Portal</key>
 <string>your.portal.here.com</string> <key>Prelogon</key>
 <string>0</string> </dict> <key>Settings</key> <dict>
 <key>connect-method</key> <string>on-demand</string> </dict>
 </dict> </dict> </dict> </plist> ' > $gPrefs echo $? # Kill the
 Preference caching daemon to prevent it from overwriting any
 changes killall cfprefsd echo $? fi # Check exit code. exit $?
```

Script pour plusieurs portails :

```
#!/bin/bash ## Description : Checks for global and user
 preferences and populates with a test portal if needed. ## Body
 ############################################################## ##
 Declare Variables
 ################################################ # Get
 current Console user active_user=$( stat -f "%Su" /dev/
console ) # Global Prefs File gPrefs=/Library/Preferences/
com.paloaltonetworks.GlobalProtect.settings.plist # User
 Prefs File uPrefs=/Users/${active_user}/Library/Preferences/
com.paloaltonetworks.GlobalProtect.client.plist ## Logic
 ############################################################
 echo "Setting default global portal to: your.portal.here.com
 in GPS" # If it does not already exist, create it and populate
 the default portal using PlistBuddy /usr/libexec/PlistBuddy
 -c "Add Palo\ Alto\ Networks:GlobalProtect:PanSetup:Portal
 string your.portal.here.com" \ -c "Add Palo\ Alto\
 Networks:GlobalProtect:PanSetup:Prelogon string 0" $gPrefs
 echo $? # Kill the Preference caching daemon to prevent
 it from overwriting any changes killall cfprefsd echo $?
```

 ©2026 Palo Alto Networks, Inc.

```
 #convert plist files from binary to xml format plutil -
convert xml1 $uPrefs echo "Setting default user portal to:
 your.portal.here.com in GPA" # If it does not already exist,
 create it and populate the default portal using the echo command
 echo '<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist
 PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd"> <plist version="1.0"> <dict>
 <key>PanPortalList</key> <array> <string>your.portal.here.com</
string> <string>your.second.portal.here.com</string> </array> </
dict> </plist> ' > $uPrefs echo $? # Kill the Preference caching
 daemon to prevent it from overwriting any changes killall cfprefsd
 echo $? # Assign ownership of the user preference file to the
 signed in user chown $active_user $uPrefs echo $? #restart
 GlobalProtect pkill GlobalProtect # Check exit code. exit $?
```

4. (Facultatif) Si vous avez configuré le portail GlobalProtect pour authentifier les utilisateurs via l'authentification SAML, les utilisateurs finaux peuvent se connecter à des applications activées par SAML sans avoir besoin de saisir à nouveau leurs informations d'identification offrant une expérience Single Sign-On (ouverture de session unique - SSO) sans problème. Pour permettre à un terminal d'utiliser le navigateur système par défaut pour l'authentification SAML, ajoutez les déclarations suivantes au dictionnaire **Settings (Paramètres)** dans le script de paramètres par défaut :

```
   <key>default-browser (navigateur par défaut)</key> <string>yes
 (oui)</string>
```

Par exemple, l'échantillon de script suivant pousse l'adresse du portail GlobalProtect par défaut, la méthode de connexion et le paramètre pour utiliser le navigateur système par défaut pour l'authentification SAML :

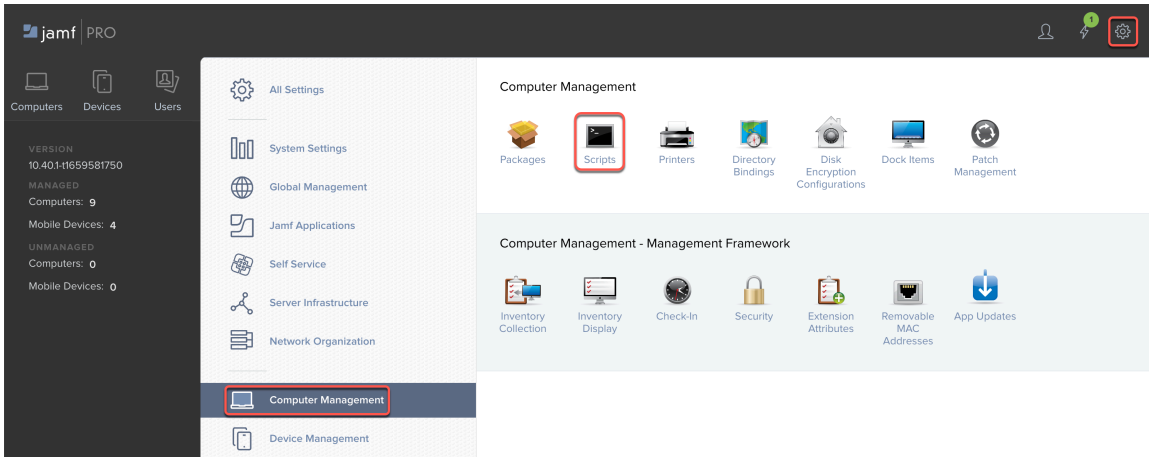
```
#!/bin/bash ## Description : Checks for global preferences file
 and populates ## it with the default portal if needed. ## Body
 ############################################################ ##
 Declare Variables ################################################
 # Get current Console user active_user=$( stat -f "%Su" /
dev/console ) # Global Prefs File gPrefs=/Library/Preferences/
com.paloaltonetworks.GlobalProtect.settings.plist ## Logic
 ############################################################ #
 Check to see if the global preference file already exists...
 if [[ -e $gPrefs ]]; then echo "Default global portal already
 exists. Skipping." else echo "Setting default global portal
 to: your.portal.here.com" echo "Setting fips mode" # If it
 does not already exist, create it and populate the default
 portal using the echo command echo '<?xml version="1.0"
 encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
 <plist version="1.0"> <dict> <key>Palo Alto Networks</key>
 <dict> <key>GlobalProtect</key> <dict> <key>PanSetup</key>
 <dict> <key>Portal</key> <string>your.portal.here.com</string>
 <key>Prelogon</key> <string>0</string> </dict> <key>Settings</
key> <dict> <key>connect-method</key> <string>on-demand</string>
 <key>default-browser</key> <string>yes</string> </dict> </dict>
 </dict> </dict> </plist> ' > $gPrefs echo $? # Kill the Preference
```

 ©2026 Palo Alto Networks, Inc.

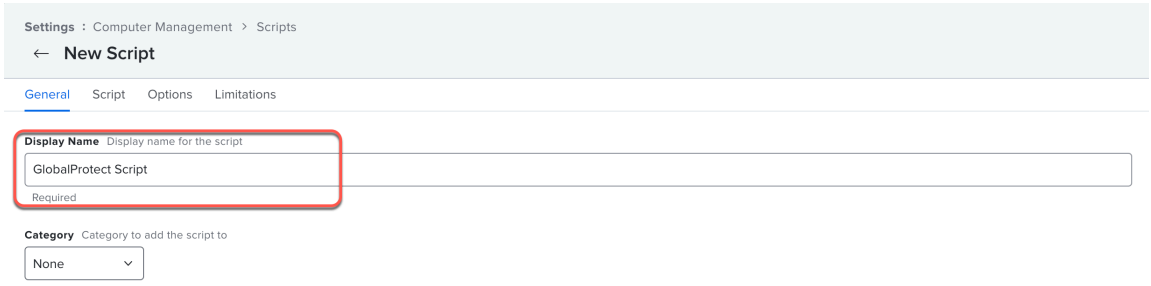
```
caching daemon to prevent it from overwriting any changes killall
cfprefsd echo $? fi # Check exit code. exit $?
```

 ©2026 Palo Alto Networks, Inc.

5. Ajoutez le script à Jamf Pro.
   1. Sélectionnez **Settings (Paramètres)** > **Computer Management (Gestion des ordinateurs)** > **Scripts**.

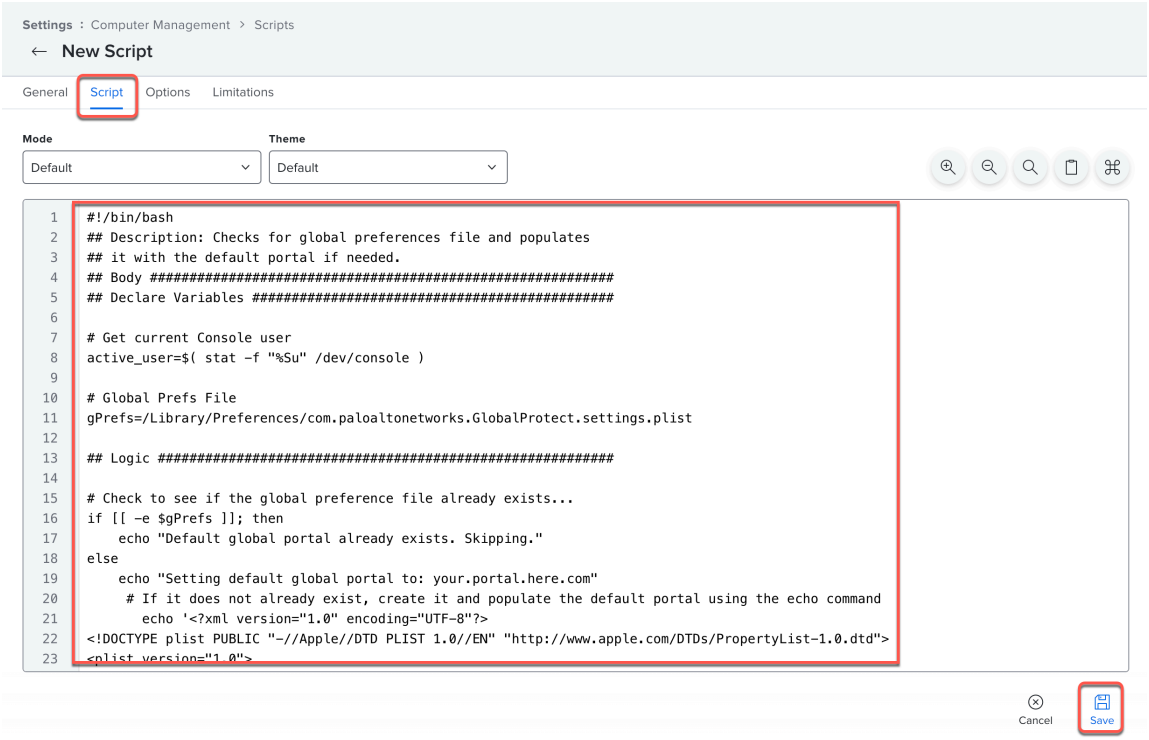


   2. Cliquez sur **New (Nouveau)**.
   3. Saisissez un **Display Name (Nom d'affichage)** pour le script.



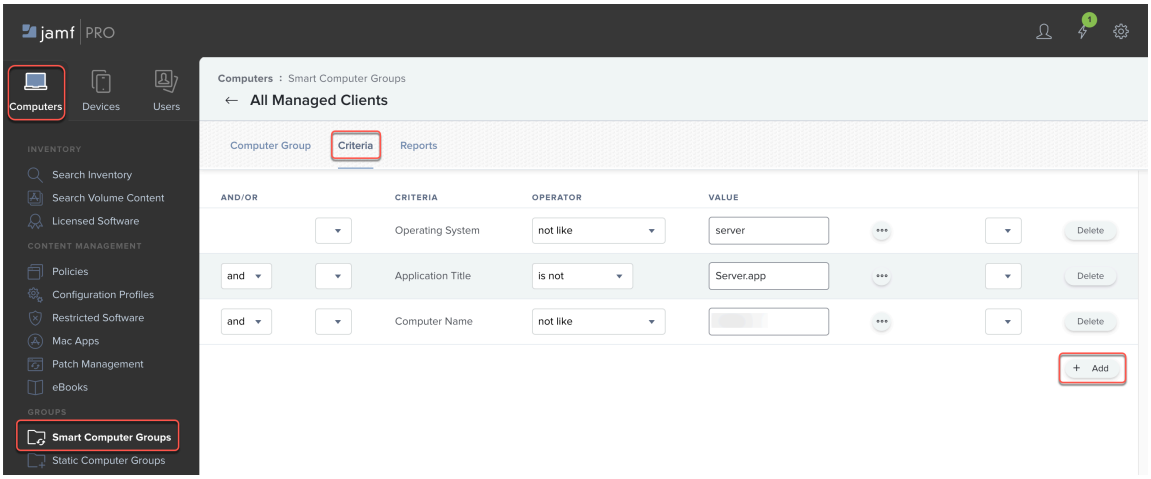
   4. Sélectionnez **Script** puis copiez-collez votre script dans l'éditeur.

 ©2026 Palo Alto Networks, Inc.



5. **Save (Enregistrer)** le script.

6. Si vous ne l'avez pas déjà fait, créez un groupe d'ordinateurs intelligents Jamf pour cibler des périphériques macOS spécifiques pour l'installation de l'application GlobalProtect.
   1. Sélectionnez **Computers (Ordinateurs)** > **Smart Computer Groups (Groupes d'ordinateurs intelligents)** > **New (Nouveau)**.
   2. Saisissez un **Display Name (Nom d'affichage)** pour le groupe.
   3. Sélectionnez **Criteria (Critère)** et **Add (Ajouter)** les critères pour le groupe.

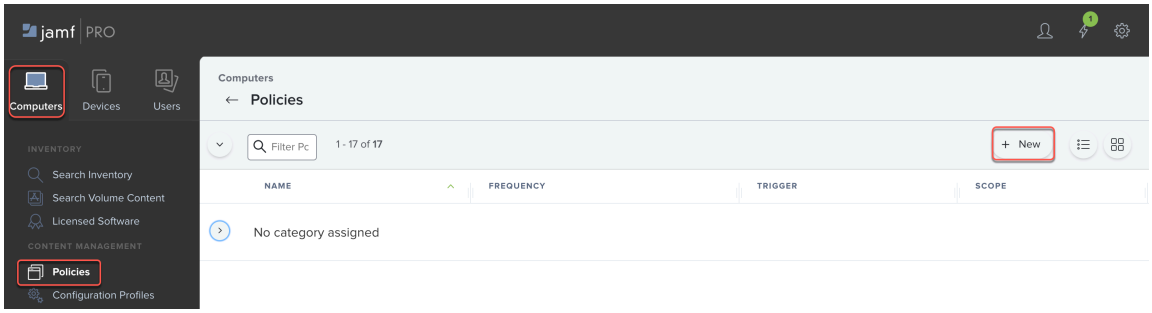


4. Cliquez sur **Save (Enregistrer)** pour enregistrer vos paramètres.

 ©2026 Palo Alto Networks, Inc.

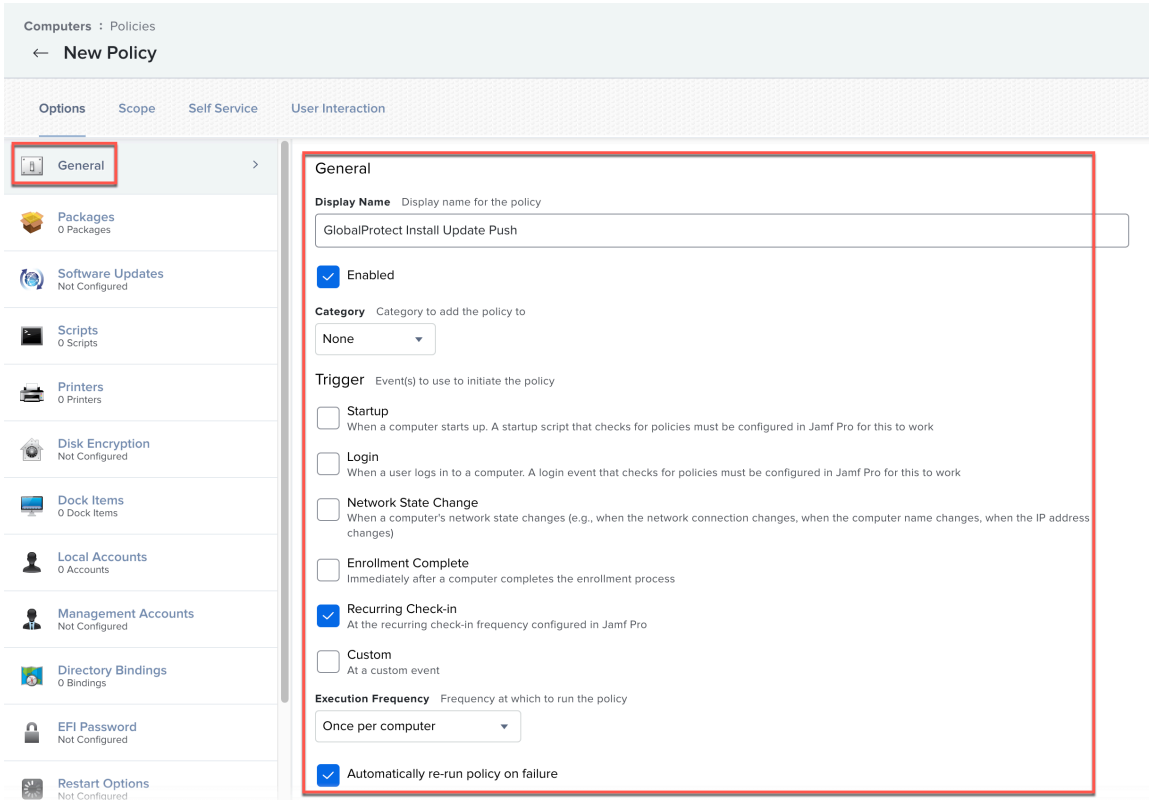
7. Créez une politique Jamf en ajoutant le package GlobalProtect et le script à la politique, et en définissant la portée sur le groupe d'ordinateurs intelligents que vous avez créé pour vos périphériques macOS à l'étape 6.

   1. Dans Jamf Pro, sélectionnez **Computers (Ordinateurs)** > **Policies (Politiques)** > **New (Nouveau)**.



   2. Dans la charge utile **General (Générale)**, configurez les paramètres de base pour la politique :

      - Entrez un **Display Name (Nom d'affichage)** pour la politique et **Enable (Activer)** la politique.
      - (Facultatif) Sélectionnez une **Category (Catégorie)**.
      - Spécifiez un **Trigger (Déclencheur)** qui initiera une politique, tel que **Recurring Check-in (Vérification récurrente)**.
      - Sélectionnez une **Execution Frequency (Fréquence d'exécution)**, telle que **Once per computer (Une fois par ordinateur)** et **Automatically re-run the policy on failure (Réexécuter automatiquement la politique en cas d'échec)**.



 ©2026 Palo Alto Networks, Inc.

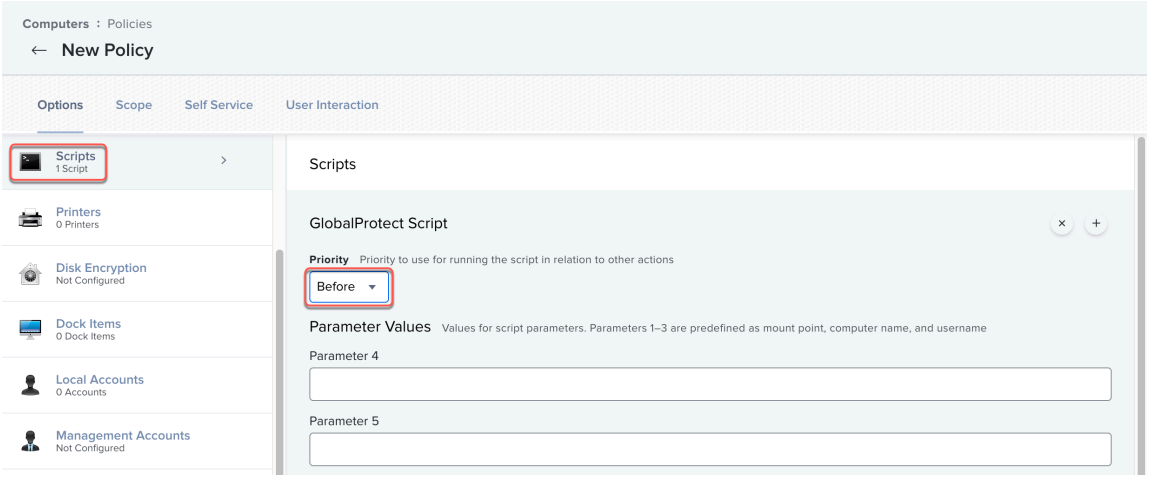
3. Configurez la charge utile des scripts en sélectionnant **Scripts** > **Configure (Configurer)**.

   Add (Ajouter) le script que vous avez créé à l'étape 5 et sélectionnez la **Priority (Priorité)** pour l'exécution du script. Pour le support de plusieurs portails, assurez-vous de définir

 ©2026 Palo Alto Networks, Inc.

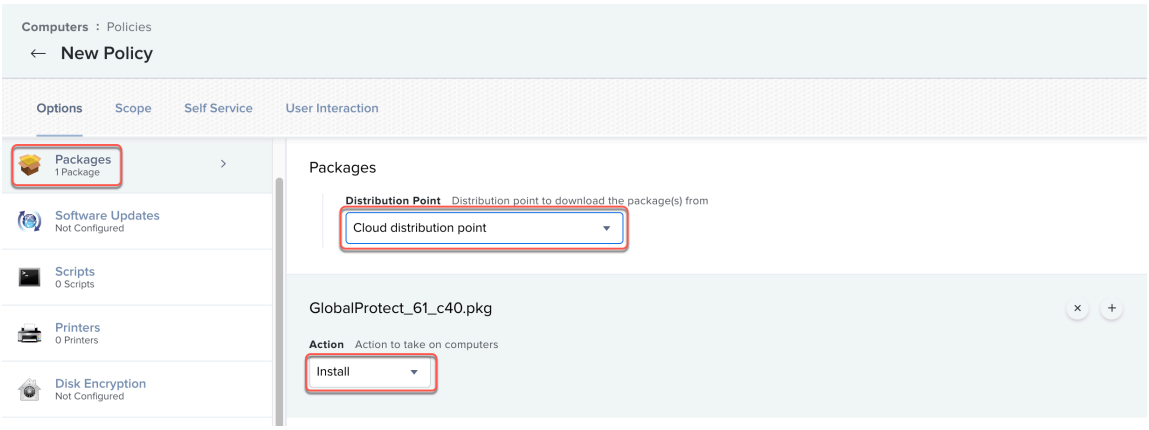
la **Priority (Priorité)** sur **Before (Avant)** afin que le script s'exécute avant l'installation du package GlobalProtect.

*Si vous définissez la priorité sur **After (Après)**, assurez-vous de redémarrer l'application GlobalProtect après la fin du déploiement afin que la configuration puisse prendre effet.*



4. Configurez la charge utile des packages en sélectionnant **Packages** > **Configure (Configurer)**.

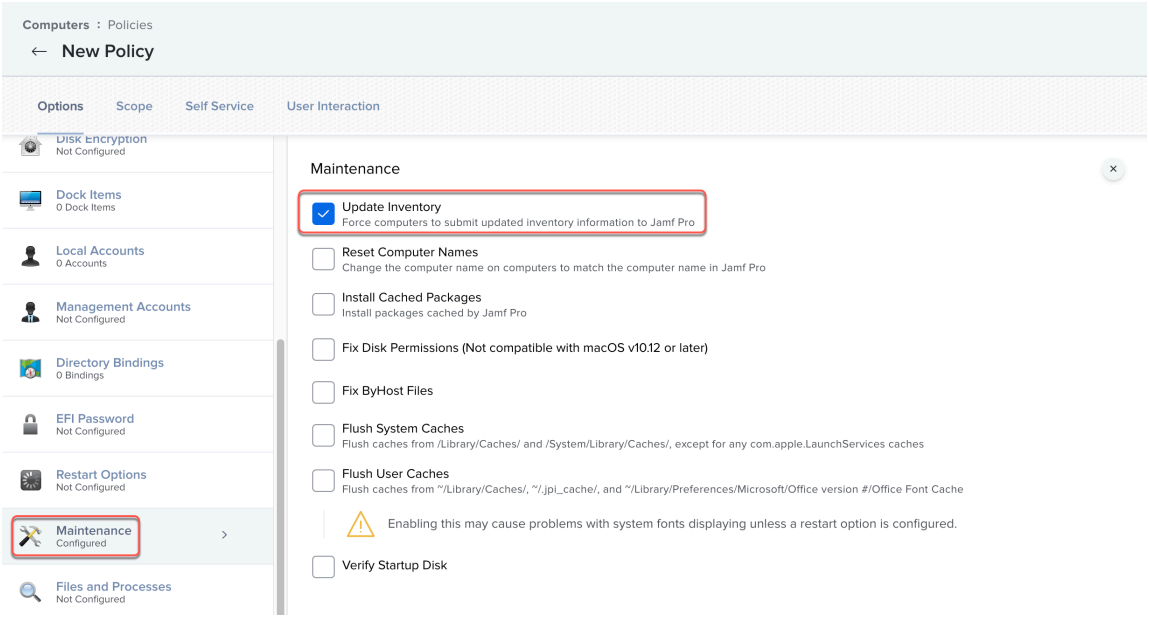
   1. **Add (Ajouter)** le package de l'application GlobalProtect que vous avez téléchargé à l'étape 2.
   2. Sélectionnez un **Distribution Point (Point de distribution)**.
   3. Sélectionnez **Install (Installer)** dans le menu **Action**.



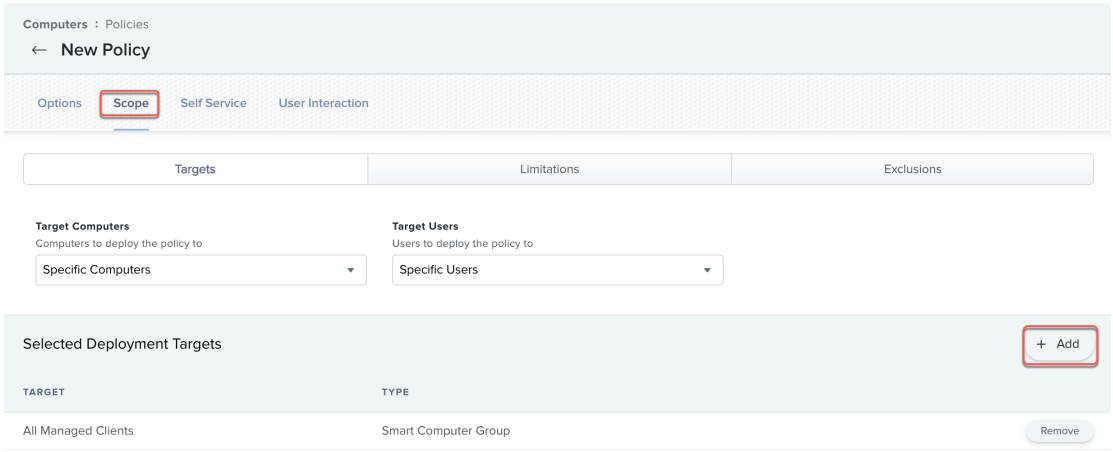
5. Configurez la charge utile de maintenance en sélectionnant **Maintenance** > **Configure (Configurer)**.

   Sélectionnez **Update Inventory (Mettre à jour l'inventaire)**.

 ©2026 Palo Alto Networks, Inc.



6. Configurez la portée de la politique.
   1. Sélectionnez **Scope (Portée)** et **Add (Ajouter)** une cible de déploiement.



   2. Cliquez sur **Computer Groups (Groupes d'ordinateurs)** et **Add (Ajouter)** le groupe d'ordinateurs intelligents que vous avez créé dans l'étape 6.
   3. Cliquez sur **Terminé**. Les ordinateurs du groupe d'ordinateurs sélectionné seront ciblés pour le déploiement de l'application GlobalProtect.
7. **Enregistrez** la politique.

   La prochaine fois que les terminaux macOS dans le groupe d'ordinateurs intelligents qui est lié à la politique se connectent à Jamf Pro et répondent au déclencheur dans la charge utile générale, la politique s'exécutera et déploiera l'application GlobalProtect sur les terminaux.

 ©2026 Palo Alto Networks, Inc.

Activer les extensions système et réseau sur les terminaux macOS à l'aide de plusieurs profils de configuration

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect 6.0.4 et versions ultérieures et 6.1 fonctionnant sur macOS Big Sur 11, macOS Monterey ou macOS Ventura

Les utilisateurs finaux doivent activer les extensions système et réseau sur les terminaux macOS si l'application GlobalProtect est configurée avec l'une des fonctionnalités suivantes :

- Segmentation du tunnel basée sur le nom de domaine de destination et le nom du processus d'application
- Application des connexions GlobalProtect pour l'accès réseau (consultez Personnaliser l'application GlobalProtect) sans nécessiter d'extensions du noyau
- DNS segmenté

Après l'installation ou la mise à niveau de l'application GlobalProtect sur un périphérique macOS, des messages de notification apparaissent pour inviter les utilisateurs à charger l'extension système GlobalProtect et les extensions réseau qui ont été bloquées lors du chargement.

Pour permettre à l'application GlobalProtect de fonctionner sans interruption sur les terminaux macOS, vous pouvez créer des profils de configuration signés GlobalProtect et les déployer à l'aide de Jamf Pro pour charger les extensions système et réseau,et supprimer automatiquement les fenêtres de notification.

Les procédures suivantes supposent que les terminaux macOS n'ont pas d'extensions réseau activées manuellement. Si les utilisateurs ont déjà activé les extensions réseau lorsqu'ils ont été notifiés par des fenêtres contextuelles GlobalProtect, le déploiement de profils de configuration à l'aide de Jamf Pro pour activer les extensions réseau créera des entrées d'extensions réseau en double sur les terminaux macOS.

Reportez-vous aux sections suivantes pour obtenir des informations sur la manière d'activer les extensions système et réseau sur l'application GlobalProtect pour les terminaux macOS :

- Activer les extensions système GlobalProtect sur les terminaux macOS à l'aide de Jamf Pro
- Activer les extensions de réseau GlobalProtect sur les terminaux macOS Big Sur à l'aide de Jamf Pro
- Ajouter un profil de configuration pour l'exécutant GlobalProtect en utilisant Jamf Pro 10.26.0

 ©2026 Palo Alto Networks, Inc.

- Vérifier les profils de configuration déployés par Jamf Pro
- Supprimer les extensions système sur les terminaux macOS Monterey à l'aide de Jamf Pro

  Si vous souhaitez utiliser un seul profil de configuration pour configurer vos périphériques macOS gérés, vous pouvez Créer un profil de configuration unique pour l'application GlobalProtect pour macOS.

Pour les utilisateurs de l'application GlobalProtect 6.0.3 et versions antérieurs, vous pouvez Supprimer les notifications sur l'application GlobalProtect pour les terminaux macOS en utilisant un Mobile Device Management (gestion des appareils mobiles - MDM) tiers pris en charge tel que Workspace ONE.

Activer les extensions système GlobalProtect sur les terminaux macOS à l'aide de Jamf Pro

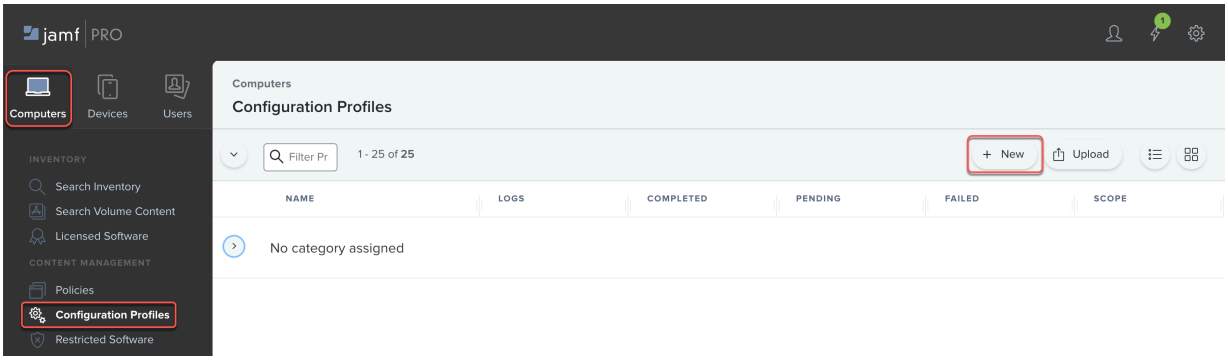
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect 6.0.4 et versions ultérieures et 6.1 fonctionnant sur macOS Big Sur 11, macOS Monterey ou macOS Ventura

Sur l'application GlobalProtect 6.0.4 et versions ultérieures et 6.1 fonctionnant sur macOS Big Sur 11, vous pouvez utiliser Jamf Pro pour configurer un profil de configuration signé GlobalProtect afin de charger automatiquement les extensions système requises pour la segmentation du tunnel, d'imposer les connexions GlobalProtect pour l'accès réseau et les fonctionnalités de DNS segmenté.

Pour les utilisateurs de l'application GlobalProtect 6.0.3 et versions antérieurs, vous pouvez Supprimer les notifications sur l'application GlobalProtect pour les terminaux macOS *en utilisant un* Mobile Device Management (gestion des appareils mobiles - MDM) tiers pris en charge *tel que Workspace ONE.*

Pour activer l'extension système GlobalProtect sur les terminaux macOS à l'aide de Jamf Pro :

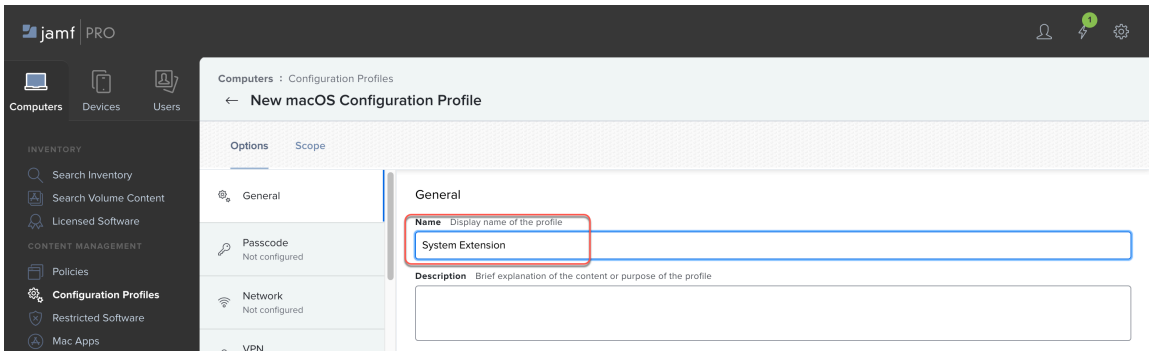
1. Dans Jamf Pro, sélectionnez **Computers (Ordinateurs)** > **Configuration Profiles (Profils de configuration)** > **New (Nouveau)**.



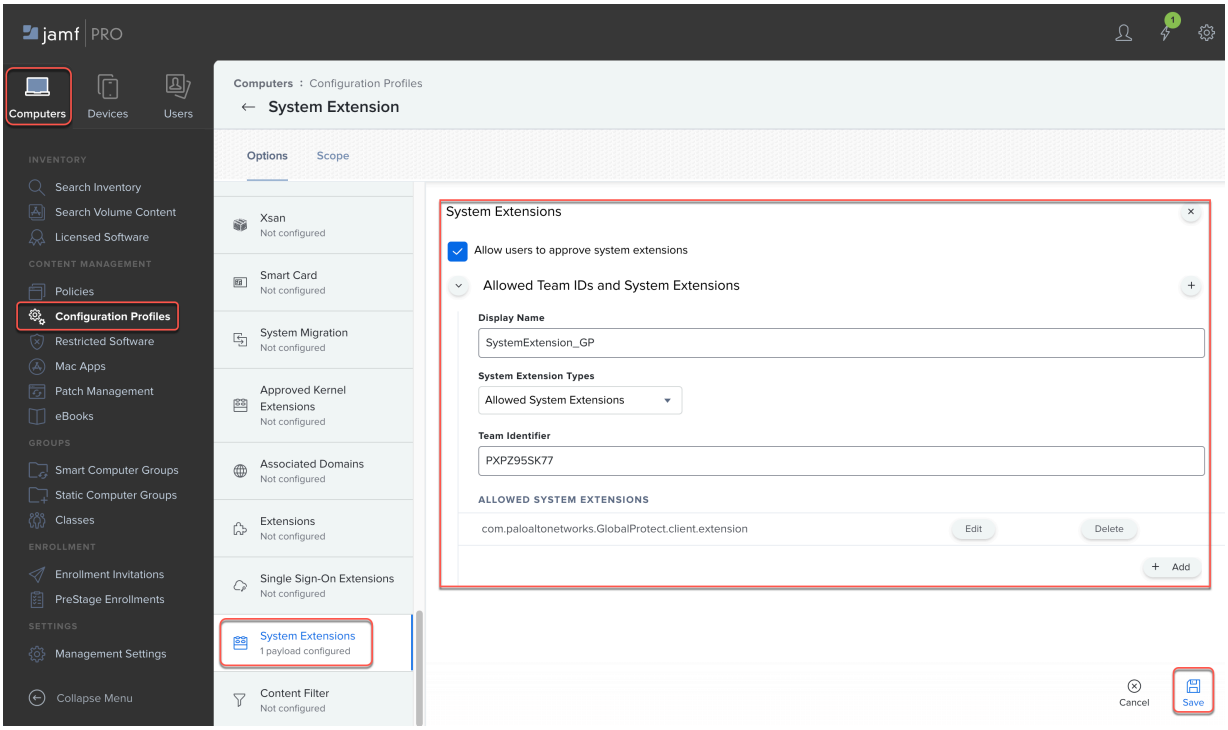
 ©2026 Palo Alto Networks, Inc.

2. Créez un profil de configuration pour activer les extensions système GlobalProtect.

1. Entrez un **Display Name (Nom d'affichage)** pour le profil de configuration.



2. Sélectionnez **System Extensions (Extensions du système)** > **Configure (Configurer)**.
3. (Facultatif) Entrez un **Display Name (Nom d'affichage)**.
4. Dans **System Extension Types (Types d'extensions de système)**, sélectionnez **Allowed System Extensions (Extensions de système autorisées)**
5. Saisissez le **Team Identifier (Identifiant d'équipe)** pour l'application GlobalProtect (**PXPZ95SK77**).
6. Dans la section **ALLOWED SYSTEM EXTENSIONS (EXTENSIONS SYSTÈME AUTORISÉES)**, **Add (Ajouter)** l'identifiant de bundle pour les extensions système GlobalProtect (**`com.paloaltonetworks.GlobalProtect.client.extension`**) et **Save (Enregistrer)** l'extension système autorisée.
7. **Enregistrez** le profil de configuration.



 ©2026 Palo Alto Networks, Inc.

3. Déployez le package de l'application GlobalProtect et activez les extensions système immédiatement après l'installation de l'application GlobalProtect.
   1. Créez un fichier de paramètres appelé `install_system_extensions.xml` avec le contenu suivant :

```
<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist
 PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
DTDs/PropertyList-1.0.dtd"> <plist version="1.0">
 <array> <dict> <key>attributeSetting</key> <integer>1</
integer> <key>choiceAttribute</key> <string>selected</
string> <key>choiceIdentifier</key> <string>third</
string> </dict> <dict> <key>attributeSetting</key>
 <integer>1</integer> <key>choiceAttribute</key>
 <string>selected</string> <key>choiceIdentifier</key>
 <string>com.paloaltonetworks.globalprotect.systemext.pkg</
string> </dict> </array> </plist>
```

   2. Déployez le package de l'application GlobalProtect en exécutant la commande suivante :

      `sudo installer -pkg GlobalProtect.pkg -applyChoiceChangesXML install_system_extensions.xml -target /`

Activer les extensions de réseau GlobalProtect sur les terminaux macOS Big Sur à l'aide de Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect 6.0.4 et versions ultérieures et 6.1 fonctionnant sur macOS 11 (Big Sur), macOS 12 (Monterey) ou macOS 13 (Ventura)

Sur l'application GlobalProtect 6.0.4 et versions ultérieures ou 6.1 fonctionnant sur macOS Big Sur 11, vous pouvez utiliser Jamf Pro pour configurer un profil de configuration signé GlobalProtect afin de permettre automatiquement les extensions de réseau requises pour la segmentation du tunnel, le DNS segmenté et d'appliquer les connexions GlobalProtect pour les fonctionnalités d'accès réseau.

Après l'installation ou la mise à niveau de l'application GlobalProtect sur les terminaux macOS, une fenêtre contextuelle apparaît pour inviter l'utilisateur à autoriser le filtrage de contenu réseau pour GlobalProtect.

Pour autoriser cette extension de réseau automatiquement et supprimer la fenêtre contextuelle, utilisez la même procédure que Ajouter un profil de configuration pour l'exécutant GlobalProtect en utilisant Jamf Pro 10.26.0.

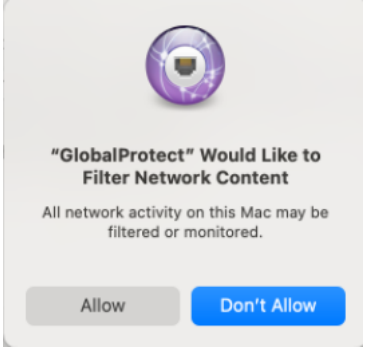
 ©2026 Palo Alto Networks, Inc.

Ajouter un profil de configuration pour l'exécutant GlobalProtect en utilisant Jamf Pro 10.26.0

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Si vous utilisez Jamf Pro 10.26.0 et que vous avez configuré l'application GlobalProtect 6.0.4 et version ultérieure ou les versions 6.1 avec la fonctionnalité d'application des connexions GlobalProtect pour l'accès réseau (exécutant), vous devez ajouter un profil de configuration pour filtrer le contenu réseau et le déployer sur vos terminaux macOS.

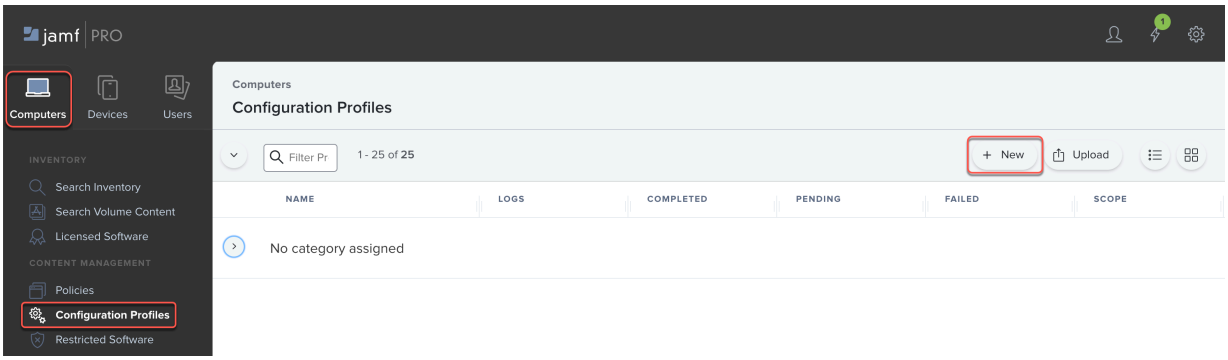
Lors de l'installation ou de la mise à niveau de l'application GlobalProtect, le message de notification suivant apparaît :



Pour autoriser cette extension réseau et supprimer automatiquement la fenêtre contextuelle, vous devez ajouter un profil de configuration pour filtrer le contenu réseau en utilisant Jamf Pro 10.26.0.

Pour déployer des applications GlobalProtect sur des terminaux macOS Big Sur 11, vous pouvez aussi utiliser les instructions suivantes sur toutes les versions de Jamf Pro pour autoriser les extensions réseau et supprimer automatiquement les messages de notification.

1. Dans Jamf Pro, sélectionnez **Computers (Ordinateurs)** > **Configuration Profiles (Profils de configuration)** > **New (Nouveau)**.



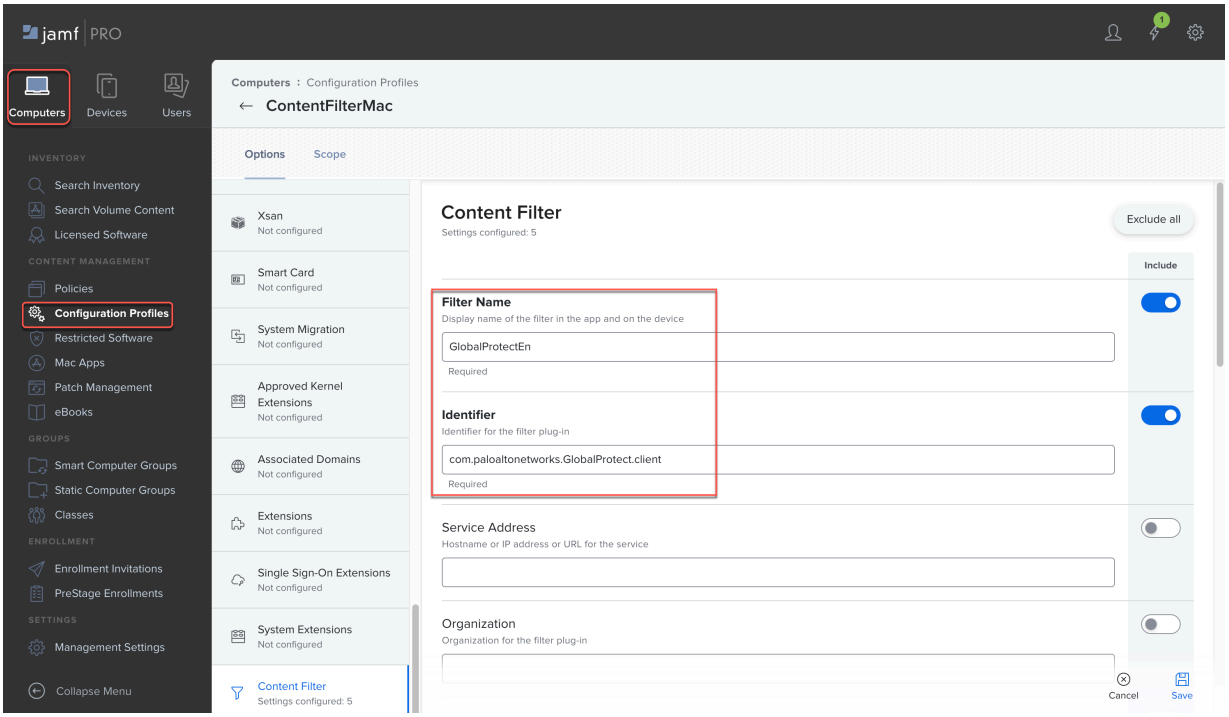
 ©2026 Palo Alto Networks, Inc.

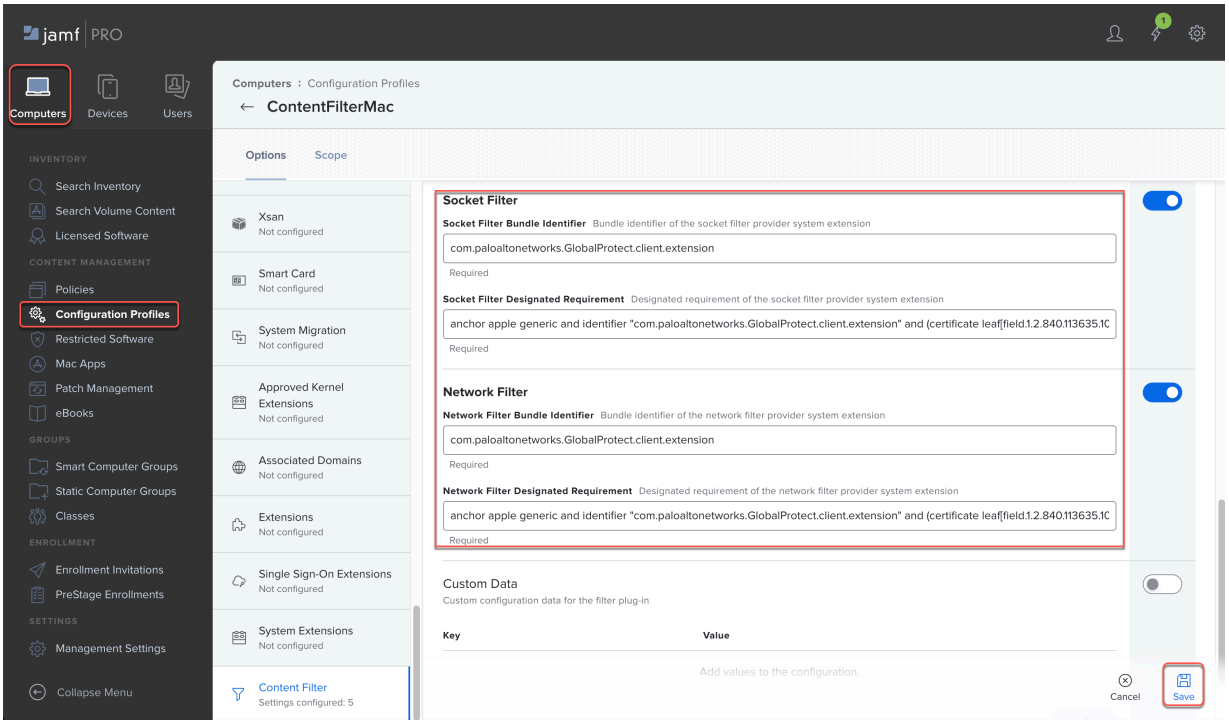
2. Sélectionnez **Content Filter (Filtre de contenu)** dans l'onglet **Options** et configurez les valeurs suivantes sur la page :

   - **FilterName (Nom du filtre)** = **`GlobalProtectEn`**
   - **Identifier (Identifiant)** = **`com.paloaltonetworks.GlobalProtect.client`**
   - **Socket Filter Bundle Identifier (Identifiant de groupe du filtre de socket)** = **`com.paloaltonetworks.GlobalProtect.client.extension`**
   - **Socket Filter Designated Requirement (Exigence désignée du filtre de socket)** = **`anchor apple generic and identifier "com.paloaltonetworks.GlobalProtect.client.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = PXPZ95SK77)`**
   - **Network Filter Bundle Identifier (Identifiant de groupe du filtre réseau)** = **`com.paloaltonetworks.GlobalProtect.client.extension`**
   - **Network Filter Designated Requirement (Exigence désignée du filtre réseau)** = **`anchor apple generic and identifier "com.paloaltonetworks.GlobalProtect.client.extension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and`**

 ©2026 Palo Alto Networks, Inc.

```
certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and
certificate leaf[subject.OU] = PXPZ95SK77)
```





3. **Enregistrez** le profil de configuration.

 ©2026 Palo Alto Networks, Inc.

Vérifier les profils de configuration déployés par Jamf Pro

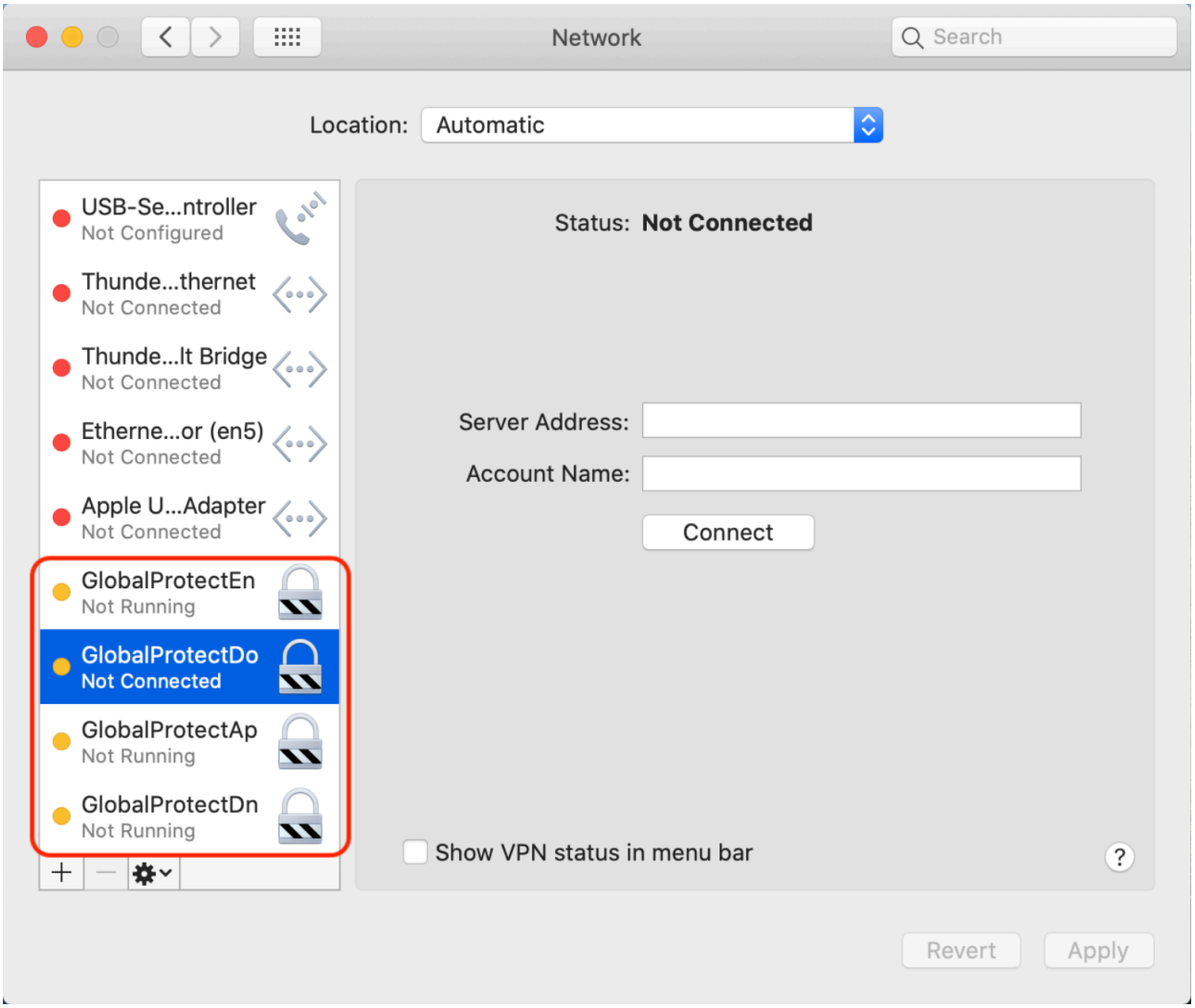
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Après avoir déployé les profils de configuration à l'aide de Jamf Pro, les interfaces réseau suivantes sont créées sur les périphériques macOS :

- `GloblaProtectDo` - Interface réseau pour GlobalProtect Domain
- `GloblaProtectAp` - Interface réseau pour GlobalProtect Application
- `GloblaProtectFr` - Interface réseau pour GlobalProtect Enforcer
- `GloblaProtectDn` - Interface réseau pour GlobalProtect DNS

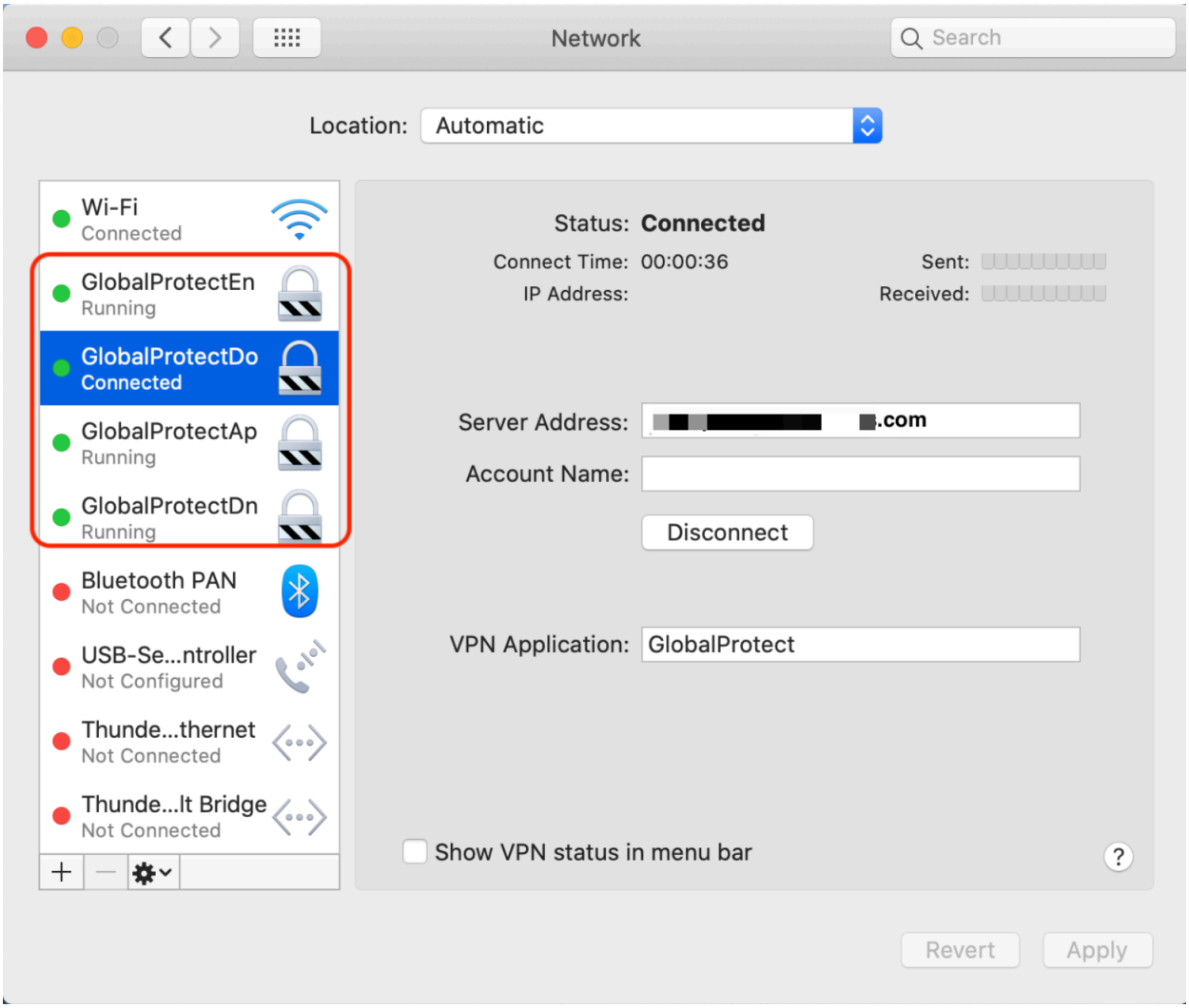
 ©2026 Palo Alto Networks, Inc.

1. Vérifiez que les interfaces réseau GlobalProtect ont été déployées sur macOS en sélectionnant **System Preferences (Préférences système)** > **Network (Réseau)**.



 ©2026 Palo Alto Networks, Inc.

2. Une fois le tunnel VPN GlobalProtect établi, les interfaces réseau deviennent actives, connectées ou en cours d'exécution comme indiqué ci-dessous :



Supprimer les extensions système sur les terminaux macOS Monterey à l'aide de Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile GlobalProtect 6.0.4 et versions ultérieures ou 6.1 Terminaux exécutant macOS Monterey 12.2.1

Dans macOS Monterey 12, Apple a introduit une fonctionnalité dans laquelle les extensions système peuvent être supprimées à l'aide d'un profil de configuration poussé à partir de Jamf Pro.

 ©2026 Palo Alto Networks, Inc.

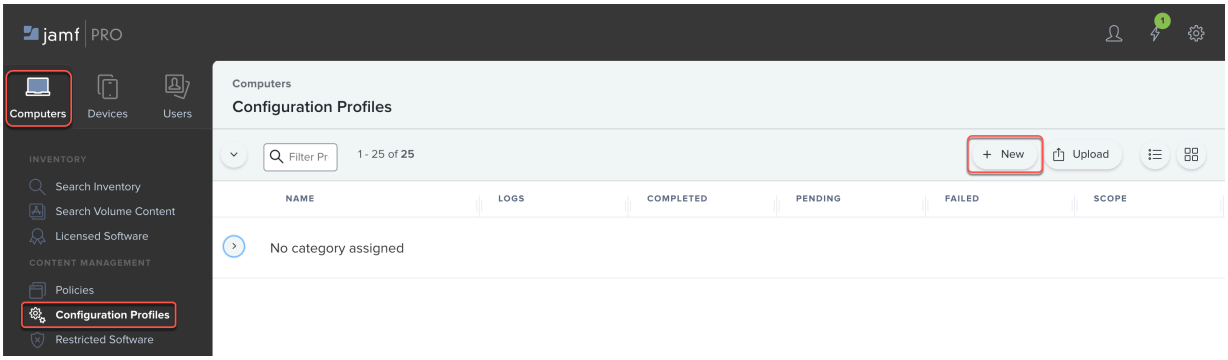
Si vous désinstallez l'application GlobalProtect 6.0.4 et versions ultérieures ou 6.1 des terminaux macOS Monterey 12.2.1 en exécutant la commande **`/Applications/GlobalProtect.app/Contents/Resources/uninstall_gp.sh`** dans un script shell, les utilisateurs finaux ne sont pas invités à saisir le nom d'utilisateur et le mot de passe de l'administrateur pour supprimer les extensions système lors de la désinstallation de l'application GlobalProtect.

Si vous désinstallez l'application GlobalProtect des terminaux macOS Monterey à l'aide du fichier PKG de l'application GlobalProtect, les utilisateurs finaux sont toujours invités par une fenêtre contextuelle à saisir le nom d'utilisateur et le mot de passe de l'administrateur pour supprimer l'extension système.

Sur les terminaux macOS antérieurs à macOS Monterey, que l'application GlobalProtect soit désinstallée à l'aide d'une commande ou d'un fichier PKG, les utilisateurs finaux sont toujours invités par une fenêtre contextuelle à saisir le nom d'utilisateur et le mot de passe de l'administrateur pour supprimer l'extension système.

Pour supprimer l'extension système de l'application GlobalProtect en envoyant un profil de configuration à partir de Jamf Pro :

1. Sélectionnez **Computers (Ordinateurs)** > **Configuration Profiles (Profils de configuration)** > **New (Nouveau)**.

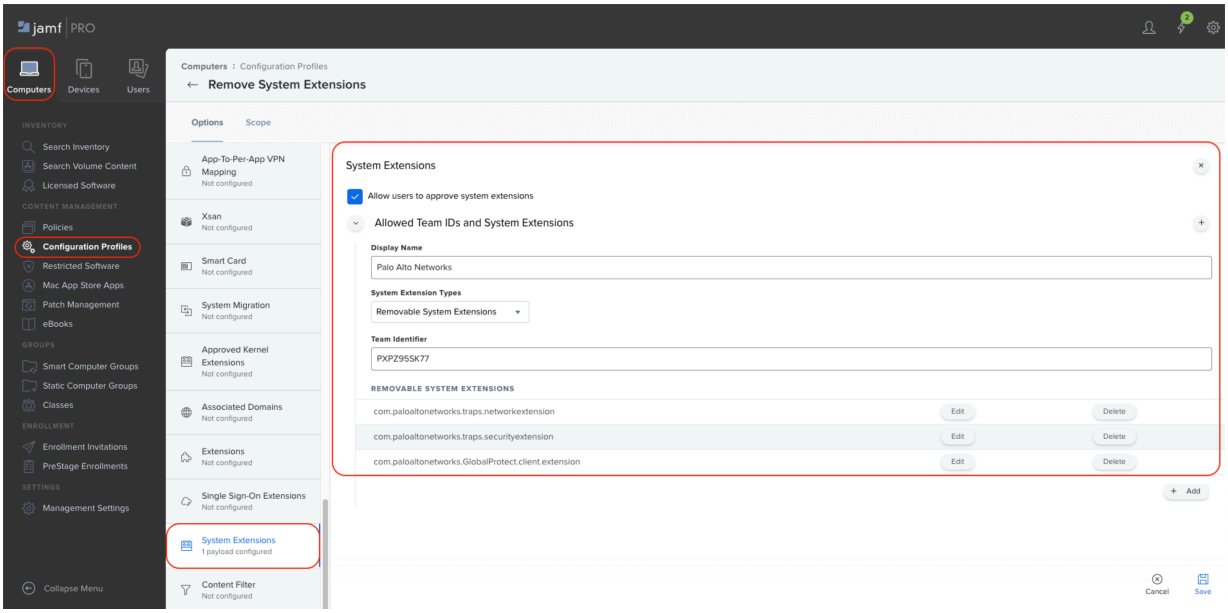


2. Créez un profil de configuration pour supprimer les extensions système GlobalProtect.
   1. Entrez un **Display Name (Nom d'affichage)** pour le profil de configuration.
   2. Sélectionnez **System Extensions (Extensions du système)** > **Configure (Configurer)**.
   3. (Facultatif) Entrez un **Display Name (Nom d'affichage)**.
   4. Dans **System Extension Types (Types d'extensions système)**, sélectionnez **Removable System Extensions (Extensions système amovibles)**.
   5. Saisissez le **Team Identifier (Identifiant d'équipe)** pour l'application GlobalProtect (**PXPZ95SK77**).
   6. Dans la section **REMOVABLE SYSTEM EXTENSIONS (EXTENSIONS DE SYSTÈME AMOVIBLES)**, **Add (Ajouter)** l'identifiant de forfait pour les extensions de système

 ©2026 Palo Alto Networks, Inc.

GlobalProtect (**`com.paloaltonetworks.GlobalProtect.client.extension`**) et **Save (Enregistrer)** l'extension de système amovible que vous avez configurée.

7. **Enregistrez** le profil de configuration.



Extensions système non amovibles sur les terminaux macOS Sequoia utilisant Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile GlobalProtect 6.2.6 et versions ultérieures. Terminaux exécutant macOS 15 (Sequoia)

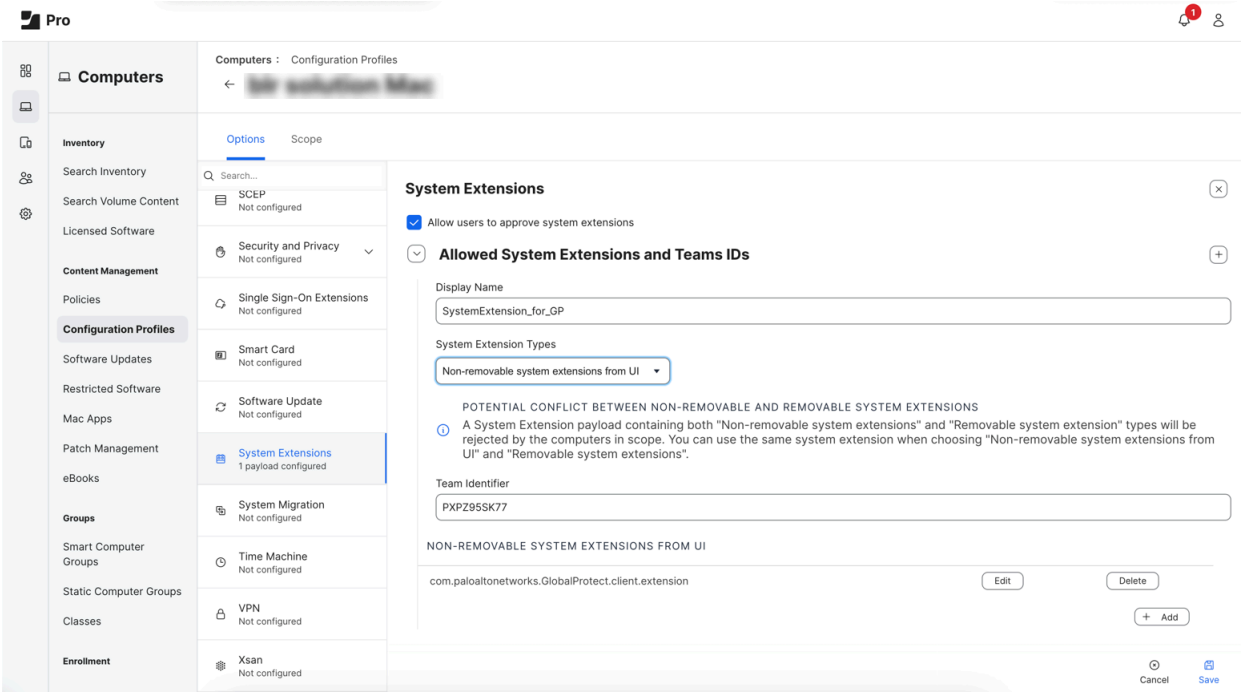
Vous pouvez maintenant utiliser le nouveau type d'extension système **Non-removable system extensions from UI (Extensions système non amovibles de l'UI)** introduit par Jamf Pro pour les périphériques fonctionnant sur macOS 15 Sequoia ou des versions ultérieures afin d'empêcher les utilisateurs finaux de désactiver les extensions système GlobalProtect sur les terminaux, réduisant ainsi les risques associés aux extensions système désactivées. La version de l'application GlobalProtect 6.2.6 et ultérieure prend en charge macOS 15 Sequoia. Cette fonctionnalité est disponible uniquement pour les périphériques fonctionnant sur macOS 15 Sequoia ou des versions ultérieures.

Avec cette nouvelle fonctionnalité, le type d'extension système **Non-removable system extensions from UI (Extensions système non amovibles de l'UI)** dans Jamf Pro empêche les utilisateurs de désactiver l'extension système GlobalProtect via les paramètres MDM (**General [Général]** > **Settings [Paramètres]** > **Network Extensions [Extensions réseau]**).

1. Mettez à niveau l'application GlobalProtect vers la version 6.2.6 ou ultérieure.
2. Mettez à niveau macOS vers la version 15 Sequoia ou ultérieure.

 ©2026 Palo Alto Networks, Inc.

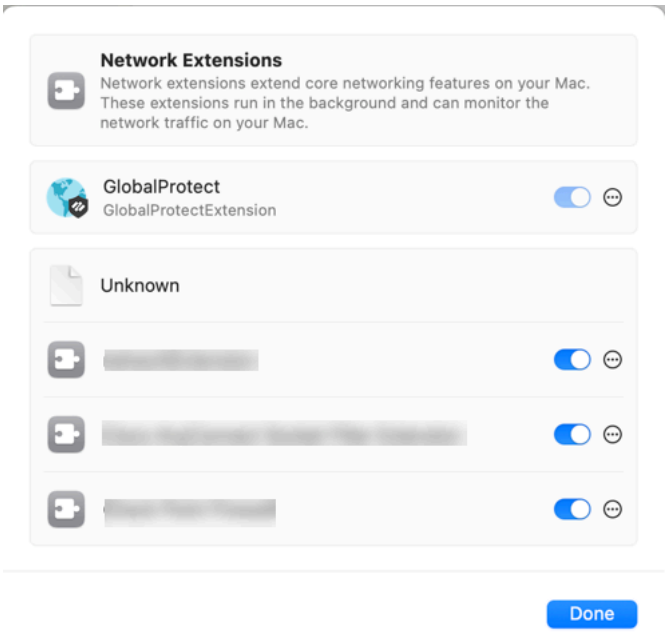
3. Dans Mobile Device Management (gestion des appareils mobiles - MDM, Jamf Pro, créez un profil de configuration pour empêcher les utilisateurs finaux de supprimer les extensions système GlobalProtect.
   1. Entrez un **Display Name (Nom d'affichage)**.
   2. Définissez le **System Extension Type (Type d'extension système)** comme **Non-removable system extensions from UI (Extensions système non amovibles de l'UI)** lors de la configuration de **Configuration Profile (Profil de configuration).**



   3. Saisissez le **Team Identifier (Identifiant d'équipe)** pour l'application GlobalProtect (**PXPZ95SK77**).
   4. **Enregistrez** le profil de configuration.

Après avoir activé l'option **Non-removable system extensions from UI (Extensions système non amovibles de l'UI)**, les utilisateurs finaux ne peuvent pas désactiver l'extension système GlobalProtect.

©2026 Palo Alto Networks, Inc.



Si les extensions système GlobalProtect sont désactivées par l'utilisateur final, les fonctionnalités GlobalProtect suivantes ne fonctionnent pas :

- Split-tunnel by Domain (Segmentation du tunnel par domaine)
- Split-tunnel by App (Segmentation du tunnel par application)
- Enforcer (Exécuteur)
- Split-DNS (DNS segmenté)
- Traffic Enforcement (Application du trafic)

Désinstaller l'application mobile GlobalProtect à l'aide de Jamf Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Application GlobalProtect 6.0.4 et versions ultérieures et 6.1

À partir de l'application GlobalProtect 6.0.4 et versions ultérieures et 6.1, vous pouvez désinstaller l'application à partir des terminaux macOS en configurant une politique contenant un script avec la commande de désinstallation de l'application GlobalProtect. Lorsque la politique est déclenchée, l'application GlobaProtect est désinstallée sur les terminaux macOS.

Pour les terminaux macOS Monterey 12.2.1, avant de commencer, supprimez les extensions système à l'aide de Jamf Pro*. Pendant la désinstallation, les utilisateurs finaux sur les terminaux macOS Monterey 12.2.1 ne sont pas invités à supprimer l'extension système GlobalProtect.*

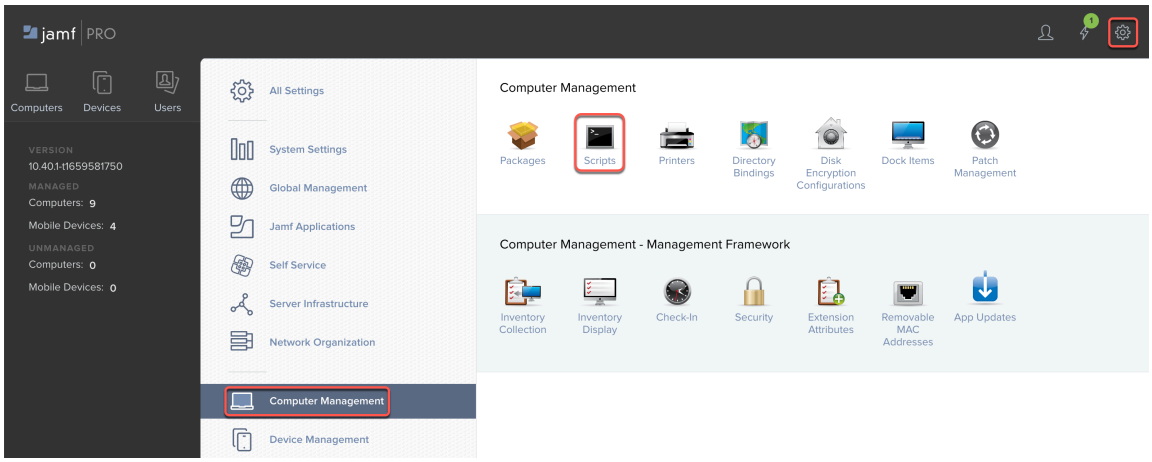
 ©2026 Palo Alto Networks, Inc.

Si vous désinstallez l'application GlobalProtect des terminaux macOS Monterey à l'aide du fichier PKG de l'application GlobalProtect, les utilisateurs finaux sont invités par une fenêtre contextuelle à saisir le nom d'utilisateur et le mot de passe de l'administrateur pour supprimer l'extension système.

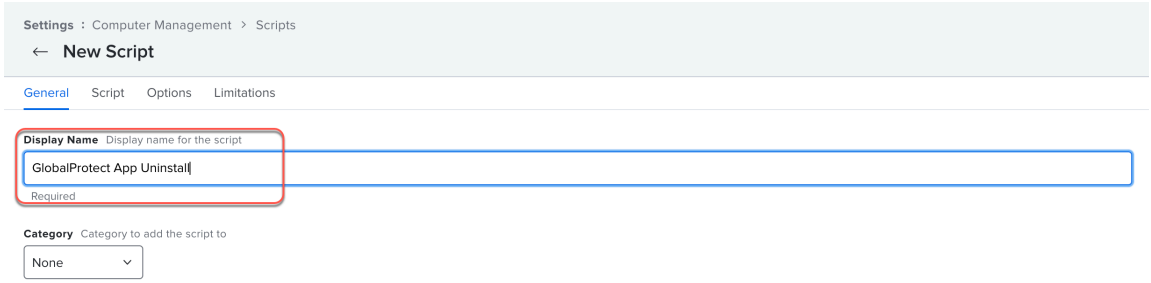
Pour les terminaux macOS antérieurs à macOS Monterey, que l'application GlobalProtect soit désinstallée à l'aide d'une commande ou d'un fichier PKG, les utilisateurs finaux sont toujours invités par une fenêtre contextuelle à saisir le nom d'utilisateur et le mot de passe de l'administrateur pour supprimer l'extension système.

 ©2026 Palo Alto Networks, Inc.

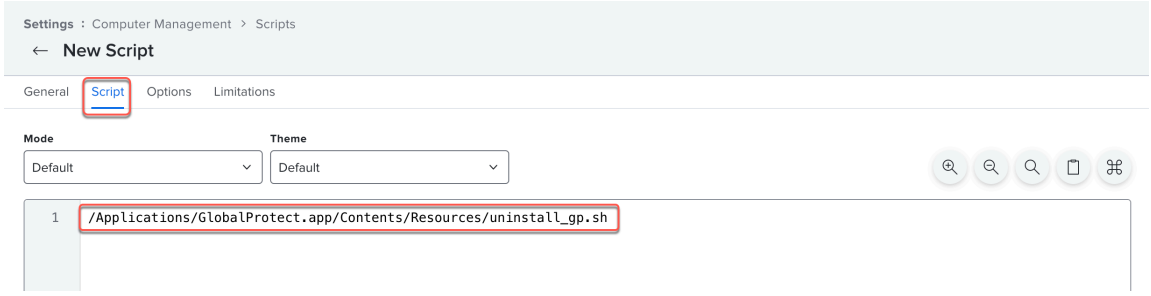
1. Dans Jamf Pro, créez un script pour désinstaller l'application GlobalProtect des terminaux macOS.
   1. Sélectionnez **Settings (Paramètres)** > **Computer Management (Gestion des ordinateurs)** > **Scripts**.



   2. Cliquez sur **New (Nouveau)**.
   3. Saisissez un **Display Name (Nom d'affichage)** pour le script.



   4. Sélectionnez **Script** et entrez la commande suivante dans l'éditeur :
      `/Applications/GlobalProtect.app/Contents/Resources/uninstall_gp.sh`

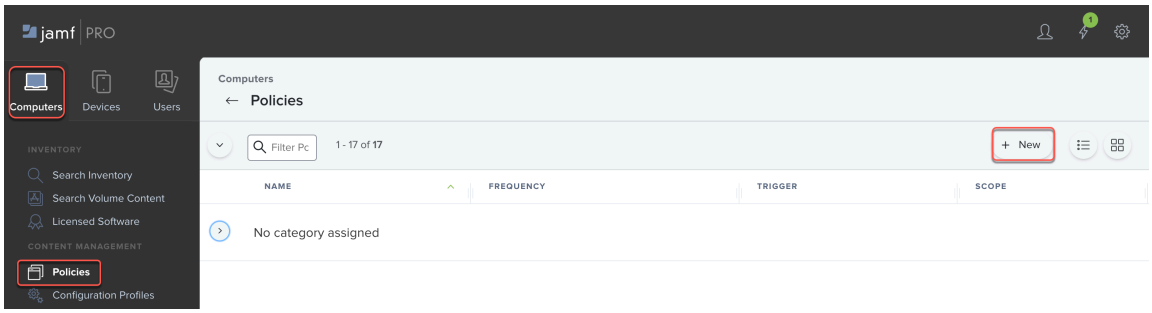


      Le script sera exécuté avec l'autorité du super utilisateur.
   5. **Save (Enregistrer)** le script.

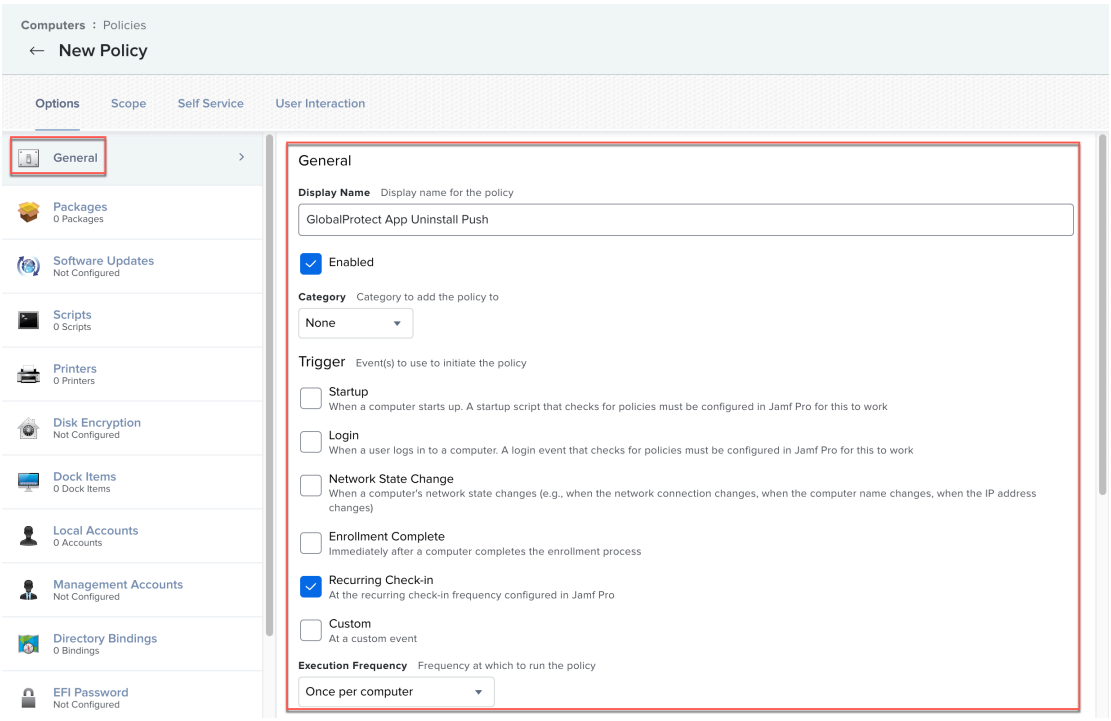
 ©2026 Palo Alto Networks, Inc.

2. Créez une politique Jamf pour exécuter le script de désinstallation.

1. Sélectionnez **Computers (Ordinateurs)** > **Policies (Politiques)** > **New (Nouveau)**.



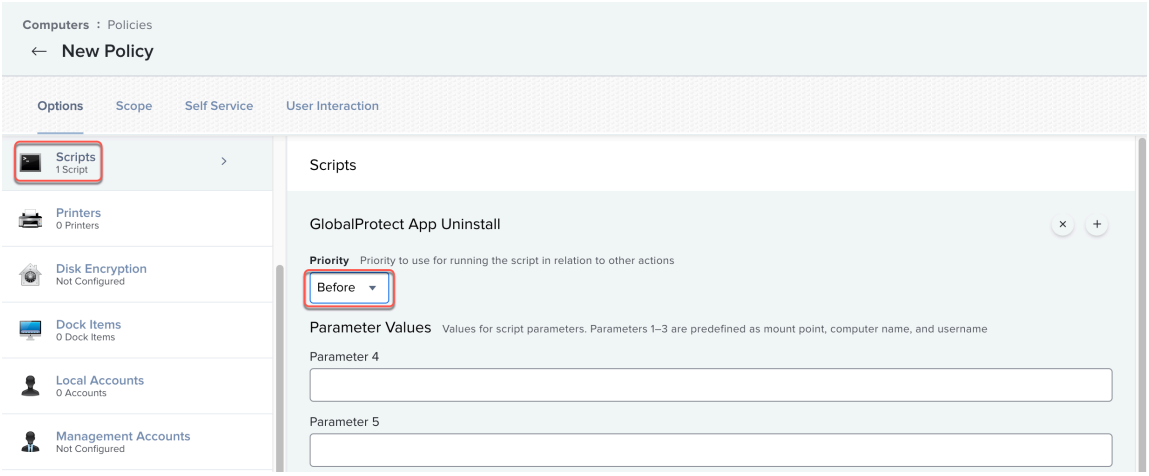
2. Dans la charge utile **General (Générale)**, configurez les paramètres de base pour la politique :
   - Entrez un **Display Name (Nom d'affichage)** pour la politique et **Enable (Activer)** la politique.
   - (Facultatif) Sélectionnez une **Category (Catégorie)**.
   - Spécifiez un **Trigger (Déclencheur)** qui exécutera la politique.
   - Sélectionnez une **Execution Frequency (Fréquence d'exécution)**, telle que **Once per computer (Une fois par ordinateur)** et **Automatically re-run the policy on failure (Réexécuter automatiquement la politique en cas d'échec)**.



3. Configurez la charge utile des scripts en sélectionnant **Scripts** > **Configure (Configurer)**.

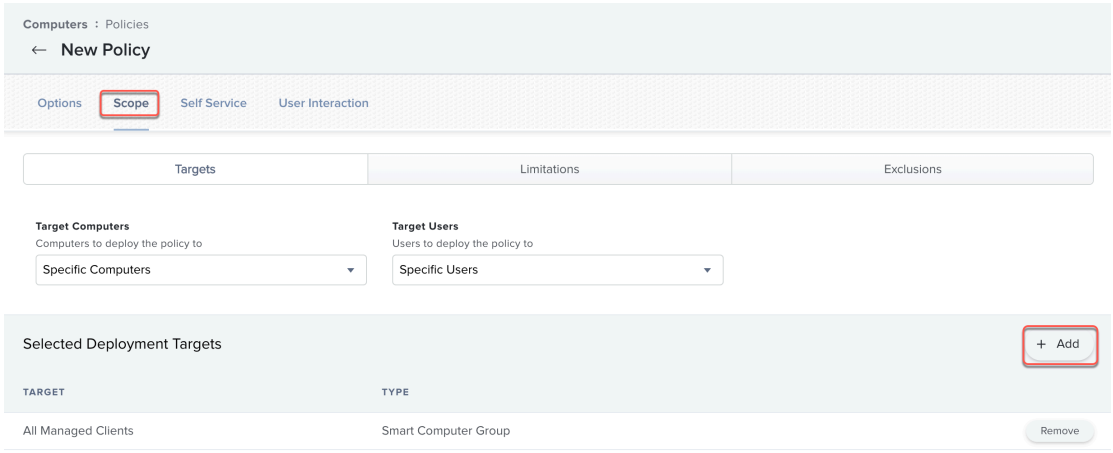
   Add (Ajouter) le script que vous avez créé à l'étape 1 et sélectionnez la **Priority (Priorité)** pour l'exécution du script.

 ©2026 Palo Alto Networks, Inc.



4. (Facultatif) Si vous avez créé un groupe intelligent pour vos utilisateurs, configurez l'étendue de la politique pour cibler ce groupe.

   1. Sélectionnez **Scope (Portée)** et **Add (Ajouter)** une cible de déploiement.



   2. Cliquez sur **Computer Groups (Groupes d'ordinateurs)** et **Add (Ajouter)** le groupe d'ordinateurs intelligents pour vos utilisateurs.
   3. Cliquez sur **Terminé**. Les ordinateurs du groupe d'ordinateurs sélectionné seront ciblés pour la désinstallation de l'application GlobalProtect.

5. **Enregistrez** la politique.

   La prochaine fois que les terminaux macOS s'enregistrent avec Jamf Pro et rencontrent le déclencheur dans la charge utile générale, la politique s'exécutera et désinstallera l'application GlobalProtect des terminaux.

 ©2026 Palo Alto Networks, Inc.

Supprimer les notifications sur l'application GlobalProtect pour les terminaux macOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

L'application GlobalProtect sur macOS prend en charge deux types d'extension : noyau (le périphérique macOS doté de la version macOS Catalina 10.15.3 ou d'une version antérieure) et système (périphérique macOS doté de la version macOS Catalina 10.15.4 ou d'une version ultérieure et de l'application GlobalProtect 5.1.4 ou d'une version ultérieure). Si vous avez configuré un tunnel partagé sur la passerelle GlobalProtect ou que vous appliquez des connexions GlobalProtect pour l'accès au réseau (voir Personnalisation de l'application GlobalProtect), un message de notification s'affiche sur l'application GlobalProtect. Le message invite les utilisateurs à activer, dans macOS, l'extension de noyau ou l'extension système dont le chargement était bloqué lorsqu'ils accèdent à l'application GlobalProtect pour laquelle ces fonctionnalités sont activées.

Pour permettre aux utilisateurs de l'application GlobalProtect 6.0.4 et versions ultérieures ou 6.1 de charger automatiquement l'extension du noyau ou l'extension système sans recevoir de notification, vous pouvez utiliser Jamf Pro pour créer une politique pour cette extension.

Pour permettre aux utilisateurs de l'application GlobalProtect 6.0.3 ou d'une version antérieure de charger automatiquement l'extension du noyau ou l'extension système sans recevoir de notification, vous pouvez utiliser un système de Mobile Device Management (gestion des appareils mobiles - MDM) tiers pris en charge tel que Workspace ONE pour créer une politique pour cette extension.

Activer les extensions de noyau dans l'application GlobalProtect pour les terminaux macOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

À compter de macOS 10.13, Apple a introduit un changement logiciel selon lequel les utilisateurs doivent approuver les extensions de noyau avant de pouvoir les utiliser.

Bien que les utilisateurs puissent activer manuellement l'extension de noyau sur macOS **Préférences système** > **Sécurité et confidentialité** et sélection de**Autoriser** l'extension de noyau, vous pouvez utiliser n'importe quel fournisseur MDM qualifié pour créer une politique et approuver l'extension de noyau. La note technique d'Apple TN2450 décrit le processus.

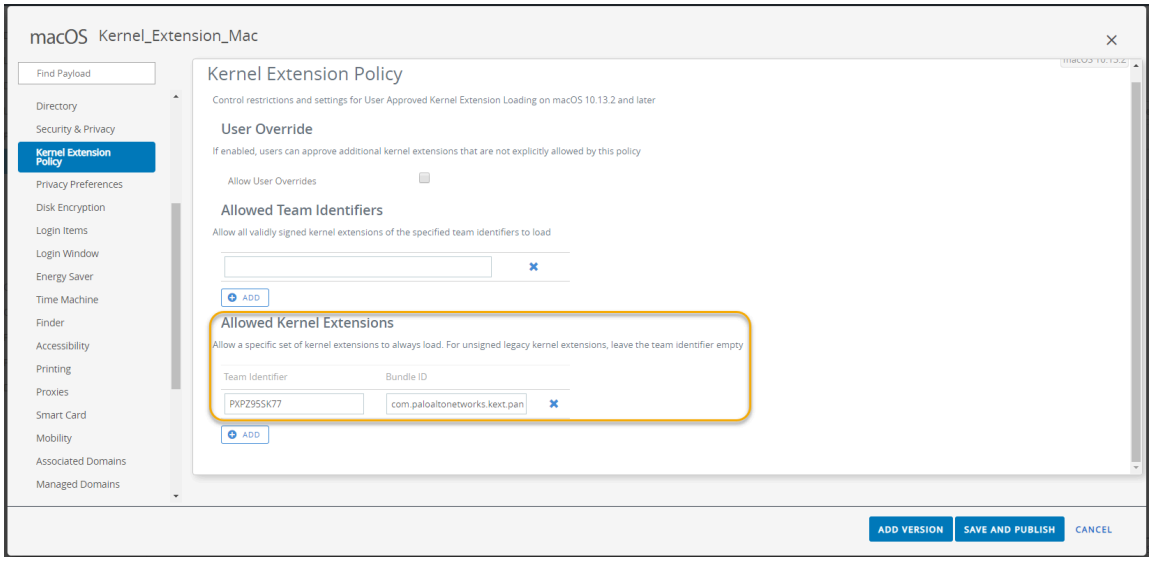
 ©2026 Palo Alto Networks, Inc.

Le flux de production suivant a été testé à l'aide de Workspace ONE.

1. Créer une politique d'extension de noyau.
   1. Connectez-vous à Workspace ONE UEM en tant qu'administrateur.
   2. Sélectionner **Devices** > **Profils et ressources** > **Profils**, puis sélectionnez **Ajouter** > **Ajouter le profil** à partir de la liste déroulante.
   3. Dans la zone **Ajouter le profil**, cliquez sur **Apple macOS**, puis cliquez sur l'icône **Profil de l'appareil**.
   4. Spécifiez le nom du profil dans la zone **Général**.

      Vous pouvez également sélectionner un profil d'extension de noyau existant **Appareils** > **Profils et ressources** > **Profils** dans la liste.

2. Ajoutez une extension de noyau et distribuez la politique pertinente aux appareils macOS.
   1. Créez une **politique d'extension de noyau**.
   2. Saisissez le **Identifiant d'équipe** utilisé par l'application GlobalProtect **PXPZ95SK77**.
   3. Entrez l'**identifiant de groupe** (**com.paloaltonetworks.kext.pangpd**).

   4. Cliquez sur **Enregistrer et publier** pour enregistrer vos modifications.

Activer les extensions de système dans l'application GlobalProtect pour les terminaux macOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

 ©2026 Palo Alto Networks, Inc.

À partir de la version 10.15.4 de macOS, Apple a limité la prise en charge des extensions kernel. L'application GlobalProtect utilisera les extensions système plutôt que les extensions kernel. Les utilisateurs doivent approuver les extensions système avant de pouvoir les utiliser.

En plus d'activer les extensions du système, vous pouvez activer les extensions du réseau dans l'application GlobalProtect, pour supprimer les invitations pop-up de ***Network Extensions Configuration (Configuration des extensions réseau)****qui sont utilisées pour le Tunnel séparé et appliquer les connexions GlobalProtect Connections pour les fonctionnalités d'accès au réseau. Vous pouvez utiliser le système de Mobile Device Management (gestion des appareils mobiles - MDM) comme Jamf Pro pour charger les extensions de réseau automatiquement sans recevoir les invitations pop-up.*

- *Pour l'application GlobalProtect 6.0.4 et ultérieure ou les versions 6.1, vous pouvez* Activer les extensions système et réseau sur les terminaux macOS à l'aide de plusieurs profils de configuration.
- *Pour l'application GlobalProtect 6.0.3 ou version antérieurs, reportez-vous à l'article de la base de données de connaissances à l'adresse* https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8 *pour des informations sur la façon de activer le système et les extensions de réseau en utilisant Jamf Pro.*

Si vous n'utilisez pas Jamf Pro, suivez les étapes suivantes pour configurer un profil afin d'approuver automatiquement l'extension système en utilisant Workspace ONE. Cette configuration a été testée avec Workspace ONE. Vous pouvez toutefois utiliser n'importe quel fournisseur MDM qualifié pour créer et mettre en œuvre ce profil.

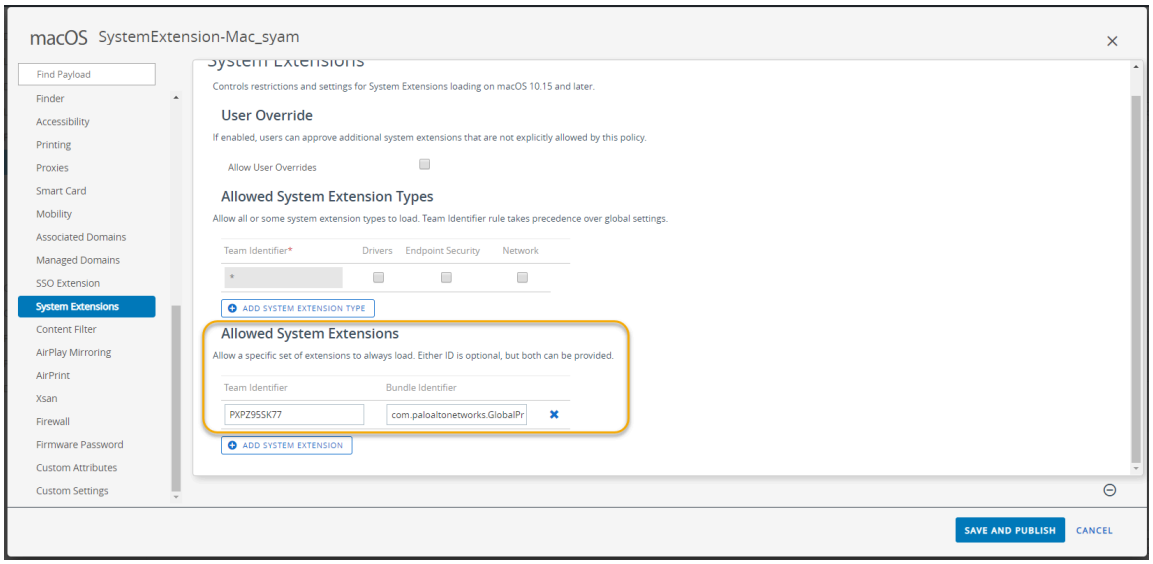
Lorsque vous utilisez des extensions système et que vous devez passer aux extensions du noyau, *consultez* Déployer les paramètres d'application dans la Plist MacOS *pour plus de détails.*

1. Créez un profil d'extension système.
   1. Connectez-vous à Workspace ONE UEM en tant qu'administrateur.
   2. Sélectionner **Devices** > **Profils et ressources** > **Profils**, puis sélectionnez **Ajouter** > **Ajouter le profil** à partir de la liste déroulante.
   3. Dans la zone **Ajouter le profil**, cliquez sur **Apple macOS**, puis cliquez sur l'icône **Profil de l'appareil**.
   4. Spécifiez le nom du profil dans la zone **Général**.

      Vous pouvez également sélectionner un profil d'extension système existant (**Périphériques** > **Profils et ressources** > **Profils**) dans la liste.

 ©2026 Palo Alto Networks, Inc.

2. Ajoutez une extension système.
   1. Sélectionnez **extensions du système**.
   2. Saisissez le **Identifiant d'équipe** utilisé par l'application GlobalProtect **PXPZ95SK77**.
   3. Saisissez le **Identifiant de kit** (**com.paloaltonetworks.GlobalProtect.client.extension**)



   4. Cliquez sur **Enregistrer et publier** pour enregistrer vos modifications.

Gérer l'application GlobalProtect à l'aide d'autres MDM tiers

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Si vous n'utilisez pas de fournisseur MDM de tiers qualifié, vous pouvez utiliser d'autres systèmes MDM de tiers pour déployer et gérer l'application GlobalProtect :

- Configuration de l'application GlobalProtect pour iOS
  - Exemple : Configuration de VPN au niveau périphérique de l'application iOS GlobalProtect
  - Exemple : Configuration de VPN au niveau application de l'application iOS GlobalProtect
- Configuration de l'application GlobalProtect pour Android
  - Exemple : Paramétrer la configuration VPN
  - Exemple : Supprimer la configuration VPN

 ©2026 Palo Alto Networks, Inc.

Configuration de l'application GlobalProtect pour iOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Tandis qu'un MDM indépendant vous permet de forcer les paramètres de configuration qui autorisent l'accès à vos ressources d'entreprise et fournit un mécanisme pour mettre en œuvre les restrictions de point de terminaison, il n'assure pas la sécurité de la connexion entre le périphérique mobile et les services auxquels il se connecte. Pour activer l'application et établir des connexions sécurisées, vous devez activer le support VPN sur le point de terminaison.

Le tableau suivant décrit les paramètres types que vous pouvez configurer à l'aide de votre système MDM indépendant. Notez que la valeur dans la colonne Paramètre peut changer en fonction du système MDM avec lequel vous travaillez.

Paramètre	Description	Valeur
Connection Type	Type de connexion activée par la stratégie.	**`Custom SSL`**
Identifiant	Identifiant du VPN SSL personnalisé au format DNS inversé.	**`com.paloaltonetworks.globalprotect.v`**
Serveur	Nom d'hôte ou adresse IP du portail GlobalProtect.	**`<hostname or IP address>`** Par exemple : **`gp.paloaltonetworks.com`**
Compte	Compte utilisateur pour authentifier la connexion.	**`<username>`**
Authentification de l'utilisateur	Type d'authentification pour la connexion.	**`Certificat | Mot de passe`**
Informations d'identification	(Certificat pour l'authentification utilisateur uniquement) Informations d'authentification pour authentifier la connexion.	**`<credential>`** Par exemple : **`clientcredial.p12`**
Activer le réseau privé virtuel à la demande	(Facultatif) Le domaine et le nom d'hôte qui établissent la connexion et l'action à la demande :	**`<domain and hostname and the on-demand action>`** Par exemple :

 ©2026 Palo Alto Networks, Inc.

Paramètre	Description	Valeur
	• Toujours établir une connexion • Ne jamais établir de connexion • Établir une connexion au besoin	`gp.acme.com; Never establish`

Exemple : Configuration de VPN au niveau périphérique de l'application iOS GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

L'exemple suivant illustre la configuration XML contenant une charge utile VPN que vous pouvez utiliser pour vérifier la configuration VPN au niveau périphérique de l'application GlobalProtect pour iOS. Notez que les valeurs clés dans votre fichier de configuration peuvent être différentes de l'exemple en fonction du système MDM tiers avec lequel vous travaillez.

```
<?xml version="1.0"
encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd"> <plist
 version="1.0"> <dict> <key>PayloadContent</key> <array> <dict>
 <key>PayloadDescription</key> <string>Configure les paramètres VPN,
 y compris l'authentification.</string> <key>PayloadDisplayName</key>
 <string>VPN (VPN au niveau de l'application échantillon)</string>
 <key>PayloadIdentifier</key> <string>Sample Device Level VPN.vpn</
string> <key>PayloadOrganization</key> <string>Palo Alto Networks</
string> <key>PayloadType</key> <string>com.apple.vpn.managed</
string> <key>PayloadVersion</key> <integer>1</integer>
 <key>PayloadUUID</key> <string>5436fc94-205f-7c59-0000-011d</
string> <key>UserDefinedName</key> <string>Sample
 Device Level VPN</string> <key>Proxies</key> <dict/>
 <key>VPNType</key> <string>VPN</string> <key>VPNSubType</key>
 <string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
 <key>IPv4</key> <dict> <key>OverridePrimary</key> <integer>0</
integer> </dict> <key>VPN</key> <dict> <key>RemoteAddress</key>
 <string>cademogp.paloaltonetworks.com</string> <key>AuthName</key>
 <string></string> <key>DisconnectOnIdle</key> <integer>0</integer>
 <key>OnDemandEnabled</key> <integer>1</integer> <key>OnDemandRules</
key> <array> <dict> <key>Action</key> <string>Connect</
string> </dict> </array> <key>AuthenticationMethod</key>
 <string>Password</string> </dict> <key>VendorConfig</key>
 <dict> <key>AllowPortalProfile</key> <integer>0</integer>
 <key>FromAspen</key> <integer>1</integer> </dict> </dict> </array>
 <key>PayloadDisplayName</key> <string>Sample Device Level VPN</
```

 ©2026 Palo Alto Networks, Inc.

```
string> <key>PayloadOrganization</key> <string>Palo Alto Networks</
string> <key>PayloadDescription</key> <string>Profile Description</
string> <key>PayloadIdentifier</key> <string>Sample Device Level
 VPN</string> <key>PayloadType</key> <string>Configuration</
string> <key>PayloadVersion</key> <integer>1</integer>
 <key>PayloadUUID</key> <string>5436fc94-205f-7c59-0000-011c</string>
 <key>PayloadRemovalDisallowed</key> <false/> </dict> </plist>
```

Exemple : Configuration de VPN au niveau application de l'application iOS GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

L'exemple suivant illustre la configuration XML contenant une charge utile VPN que vous pouvez utiliser pour vérifier la configuration VPN au niveau de l'application de l'application GlobalProtect pour iOS. Notez que les valeurs clés dans votre fichier de configuration peuvent être différentes de l'exemple en fonction du système MDM tiers avec lequel vous travaillez.

```
<?xml version="1.0"
encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST
 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
 <plist version="1.0"> <dict> <key>PayloadContent</key>
 <array> <dict> <key>PayloadDescription</key> <string>Configure
 les paramètres VPN, y compris l'authentification.</string>
 <key>PayloadDisplayName</key> <string>VPN (VPN au niveau de
 l'application échantillon)</string> <key>PayloadIdentifier</key>
 <string>Sample App Level VPN.vpn</string> <key>PayloadOrganization</
key> <string>Palo Alto Networks</string> <key>PayloadType</
key> <string>com.apple.vpn.managed.applayer</string>
 <key>PayloadVersion</key> <integer>1</integer> <key>VPNUUID</key>
 <string>cGFuU2FtcGxlIEFwcCBMZXZlbCBWUE52cG5TYW1wbGUgQXBwIExldmVsIFZQTg==</
string> <key>SafariDomains</key> <array>
 <string>*.paloaltonetworks.com</string> </array>
 <key>PayloadUUID</key> <string>54370008-205f-7c59-0000-01a1</
string> <key>UserDefinedName</key> <string>Sample
 App Level VPN</string> <key>Proxies</key> <dict/>
 <key>VPNType</key> <string>VPN</string> <key>VPNSubType</key>
 <string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
 <key>IPv4</key> <dict> <key>OverridePrimary</key> <integer>0</
integer> </dict> <key>VPN</key> <dict> <key>RemoteAddress</key>
 <string>cademogp.paloaltonetworks.com</string> <key>AuthName</
key> <string></string> <key>OnDemandMatchAppEnabled</key>
 <integer>1</integer> <key>OnDemandEnabled</key> <integer>1</
integer> <key>DisconnectOnIdle</key> <integer>0</integer>
 <key>AuthenticationMethod</key> <string>Password</string> </
dict> <key>VendorConfig</key> <dict> <key>OnlyAppLevel</key>
 <integer>1</integer> <key>AllowPortalProfile</key> <integer>0</
integer> <key>FromAspen</key> <integer>1</integer> </dict> </dict>
```

 ©2026 Palo Alto Networks, Inc.

```
 </array> <key>PayloadDisplayName</key> <string>Sample App Level
 VPN</string> <key>PayloadOrganization</key> <string>Palo Alto
 Networks</string> <key>PayloadDescription</key> <string>Profile
 Description</string> <key>PayloadIdentifier</key> <string>Sample App
 Level VPN</string> <key>PayloadType</key> <string>Configuration</
string> <key>PayloadVersion</key> <integer>1</integer>
 <key>PayloadUUID</key> <string>5436fc94-205f-7c59-0000-011c</string>
 <key>PayloadRemovalDisallowed</key> <false/> </dict> </plist>
```

Configuration de l'application GlobalProtect pour Android

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez déployer et configurer l'application GlobalProtect sur des points de terminaison Android For Work à partir de toute gestion de périphériques mobiles (MDM) indépendante qui prend en charge les restrictions relatives aux données des applications Android For Work.

Sur les points de terminaison Android, le trafic est acheminé via le tunnel VPN en fonction des itinéraires d'accès qui sont configurés sur la passerelle GlobalProtect. Depuis votre MDM indépendant qui gère les points de terminaison Android for Work, vous pouvez affiner davantage le trafic qui est acheminé via le tunnel VPN.

Dans un environnement où le point de terminaison appartient à une entreprise, son propriétaire gère le point de terminaison dans son entièreté, y compris l'ensemble des applications qui y sont installées. Par défaut, toutes les applications installées peuvent acheminer le trafic via le tunnel VPN selon les itinéraires d'accès définis sur la passerelle.

Dans un environnement Apportez Votre Propre Appareil (Bring-Your-Own-Device ; BYOD), le point de terminaison n'appartient pas à une entreprise ; il utilise un profil de travail pour séparer les applications personnelles des applications professionnelles. Par défaut, seules les applications installées sur le profil de travail peuvent acheminer le trafic via le tunnel VPN selon les itinéraires d'accès qui sont définis sur la passerelle. Les applications installées du côté personnel du point de terminaison ne peuvent acheminer le trafic via le tunnel VPN établi par l'application gérée GlobalProtect, qui est installée dans le profil de travail.

Pour acheminer le trafic à partir d'un plus petit ensemble d'applications, vous pouvez activer le VPN par application afin que GlobalProtect n'achemine que le trafic provenant de certaines applications gérées. Pour le VPN par application, vous pouvez mettre les applications gérées sur votre liste d'autorisation ou sur votre liste de blocage pour acheminer le trafic via le tunnel VPN.

> *Les points de terminaison exécutant Android ne lanceront pas automatiquement l'application GlobalProtect lorsque l'utilisateur lance une application dans la liste d'autorisation. Cependant, les points de terminaison exécutant iOS lancent automatiquement l'application GlobalProtect et établissent le tunnel VPN lorsque l'utilisateur lance une application à partir de la liste d'autorisation.*

 ©2026 Palo Alto Networks, Inc.

Dans le cadre de la configuration VPN, vous pouvez également indiquer la méthode que l'utilisateur utilise pour se connecter au VPN. Lorsque vous configurez la méthode de connexion en tant que **user-logon (connexion utilisateur)**, l'application GlobalProtect établit une connexion automatiquement. Lorsque vous configurez la méthode de connexion en tant que **on-demand (sur demande)**, les utilisateurs doivent initier une connexion manuellement.

La méthode de connexion VPN définie dans le MDM est prioritaire sur la méthode de connexion définie dans la configuration du portail GlobalProtect.

La suppression de la configuration VPN rétablit automatiquement les paramètres de configuration initiaux de l'application GlobalProtect.

Pour configurer l'application GlobalProtect pour Android, configurez les restrictions de l'application pour Android suivantes :

Clé	Type de valeur	Description	Exemple
portal	Chaîne	Adresse IP ou nom de domaine complet (FQDN) du portail.	**10.1.8.190**
nom d'utilisateur	Chaîne	Nom d'utilsateur associé à l'utilisateur.	**john**
password	Chaîne	Mot de passe associé à l'utilisateur.	**Passwd!234**
mobile_id	Chaîne	ID Mobile configuré dans un service MDM indépendant afin d'identifier un appareil mobile de manière unique. GlobalProtect utilise cet ID mobile pour récupérer les informations sur le périphérique.	**5188a8193be43f42d332dde5cb2c941e**
certificate	Chaîne (en Base 64)	Certificat client (cert) utilisé pour authentifier l'agent et le portail.	**DAFDSaweEWQ23wDSAFD….**
client_certificate_passphrase	Chaîne	Clé associée au certificat client.	**PA$$W0RD$123**
app_list	Chaîne	Configuration du VPN par application. Commencez la chaîne par le mot clé de la **allowlist (liste d'autorisation)** ou de la **(liste de blocage)** suivie de deux-points, et	**whiltelist | blacklist: com.google.calendar; com.android.email; com.android.chrome**

 ©2026 Palo Alto Networks, Inc.

Clé	Type de valeur	Description	Exemple
		faites-la suivre par un tableau de noms d'applications séparés par des points-virgules. La liste d'autorisation indique les applications qui utiliseront le tunnel VPN pour la communication réseau. Le trafic réseau de toute application qui ne figure pas sur la liste d'autorisation ou qui n'est pas expressément nommée dans la liste de blocage ne passera pas par le tunnel VPN.	*Les mots clés* ***allowlist (liste d'autorisation)*** *et* ***blocklist (liste de blocage)*** *sont devenus* ***allowlist (liste d'autorisation)*** *et* ***blocklist (liste de blocage)*** *dans PAN-OS 10.1. Vous devrez modifier les paramètres de votre MDM lors de la mise à niveau vers la version 10.1.*
connect_method	Chaîne	Soit user-logon (connexion utilisateur) pour que l'utilisateur soit automatiquement connecté au portail GlobalProtect au moyen de leurs informations d'identification de Windows ou on-demand (à la demande) pour que l'utilisateur soit manuellement connecté à la passerelle.	**user-logon | on-demand**
remove_vpn_config_via_restriction	Booléenne	Supprime de manière permanente toutes les informations sur la configuration VPN de GlobalProtect.	**vraie| fausse**

 ©2026 Palo Alto Networks, Inc.

Exemple : Paramétrer la configuration VPN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

```
private static String RESTRICTION_PORTAL = "portal"; private
 static String RESTRICTION_USERNAME = "username"; private static
 String RESTRICTION_PASSWORD = "password"; private static String
 RESTRICTION_CONNECT_METHOD = "connect_method"; private static
 String RESTRICTION_CLIENT_CERTIFICATE = "client_certificate";
 private static String RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE
 = "client_certificate_passphrase"; private static String
 RESTRICTION_APP_LIST = "app_list"; private static String
 RESTRICTION_REMOVE_CONFIG = "remove_vpn_config_via_restriction";
 Bundle config = new Bundle(); config.putString(RESTRICTION_PORTAL,
 "192.168.1.1"); config.putString(RESTRICTION_USERNAME,
 "john"); config.putString(RESTRICTION_PASSWORD, "Passwd!
234"); config.putString(RESTRICTION_CONNECT_METHOD, "user-
logon"); config.putString(RESTRICTION_CLIENT_CERTIFICATE,
 "DAFDSaweEWQ23wDSAFD….");
 config.putString(RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE,
 "PA$$W0RD$123"); config.putString(RESTRICTION_APP_LIST,
 "allow list:com.android.chrome;com.android.calendar");
 DevicePolicyManager dpm = (DevicePolicyManager)
 getSystemService(Context.DEVICE_POLICY_SERVICE);
 dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.getComponentName(th
 "com.paloaltonetworks.globalprotect", config);
```

Exemple : Supprimer la configuration VPN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

```
Bundle config = new Bundle();
 config.putBoolean(RESTRICTION_REMOVE_CONFIG, true );
 DevicePolicyManager dpm = (DevicePolicyManager)
 getSystemService(Context.DEVICE_POLICY_SERVICE);
 dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.
 getComponentName(this),"com.paloaltonetworks.globalprotect",
 config);
```


©2026 Palo Alto Networks, Inc.

Déployer les paramètres d'application de façon transparente

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Au lieu de déployer les paramètres d'application à partir de la configuration du portail, vous pouvez les définir directement à partir des points de terminaison suivants :

- Windows—Registre ou Windows Installer (Msiexec)
- macOS : liste globale macOS
- Linux—fichier de configuration de pré-déploiement (`pangps.xml`)

L'avantage de cette alternative est que vous pouvez activer le déploiement des paramètres de l'application GlobalProtect sur les points de terminaison avant leur première connexion au portail GlobalProtect.

> *Certains paramètres n'ont pas de paramètres de configuration de portail correspondants sur l'interface Web, et doivent être configurés à l'aide du Registre Windows, MsiExec ou de la plist macOS. Ces paramètres sont répertoriés dans les* Paramètres d'application *personnalisables comme « Pas sur le portail ».*

Les paramètres définis dans la configuration du portail remplacent toujours les paramètres définis dans le registre Windows, macOS plist ou le fichier de configuration de pré-déploiement (`pangps.xml`) pour Linux. Si vous définissez les paramètres dans le registre, la plist ou `pangps.xml`, mais que la configuration du portail indique des paramètres différents, les paramètres que l'application reçoit du portail annulent les paramètres définis sur le point de terminaison. Cette annulation s'applique également aux paramètres d'ouverture de session tels que : faut-il se connecter à la demande, faut-il utiliser l'ouverture de session unique, et l'application peut-elle se connecter si le certificat de portail n'est pas valide. Vous devriez donc éviter de définir des paramètres contradictoires. En outre, la configuration du portail est mise en cache sur le point de terminaison et cette configuration mise en cache est utilisée chaque fois que l'application GlobalProtect redémarre ou que le point de terminaison est réamorcé.

Les sections suivantes décrivent les paramètres disponibles d'application personnalisables disponibles et comment déployer ces paramètres en toute transparence sur des points de terminaison Windows, MacOS et Linux :

- Paramètres d'application personnalisables
- Déployer les paramètres d'application sur des points de terminaison Windows
- Déployer les paramètres d'application sur des points de terminaison MacOS
- Déployer les paramètres de l'application sur les points de terminaison Linux

> *En plus d'utiliser le registre Windows, la plist MacOS ou la configuration de prédéploiement de Linux pour déployer les paramètres de l'application GlobalProtect, vous pouvez autoriser l'application GlobalProtect à collecter des informations spécifiques sur le Registre Windows ou la plist MacOS des points de terminaison, y compris les données sur les applications installées*

 ©2026 Palo Alto Networks, Inc.

sur les points de terminaison, les processus exécutés sur les points de terminaison et les attributs ou les propriétés de ces applications et processus. Vous pouvez ensuite surveiller les données et les ajouter à une règle de sécurité pour les utiliser en tant que critères de correspondance. Le trafic du point de terminaison correspondant aux paramètres de registre que vous définissez peut être mis en œuvre conformément à la règle de sécurité. En outre, vous pouvez configurer des vérifications personnalisées pour recueillir des données d'application et de traitement des points de terminaison.

Paramètres d'application personnalisables

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

En plus du pré-déploiement de l'adresse du portail, vous pouvez également définir les paramètres de l'application. Pour Deploy App Settings to Windows Endpoints (Déployer les paramètres d'application sur des terminaux Windows), vous devez définir des clés dans le Registre Windows (chemin `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect` sauf indication contraire). Pour Déployer les paramètres d'application sur des points de terminaison MacOS, vous devez définir des entrées dans le dictionnaire des `Settings (paramètres)` de la plist macOS (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`). Pour Déployer les paramètres de l'application sur les points de terminaison Linux, vous devez définir des entrées sous `<Settings>` du fichier de configuration de déploiement préalable `/opt/paloaltonetworks/globalprotect/pangps.xml`. Sur les points de terminaison Windows uniquement, vous pouvez également utiliser Windows Installer pour déployer des paramètres d'application de MsiExec.

Les rubriques suivantes décrivent chaque paramètre d'application personnalisable. Les paramètres définis dans la configuration de client du portail GlobalProtect ont priorité sur les paramètres définis dans le registre Windows ou la Plist MacOS.

Certains paramètres n'ont pas de paramètres de configuration de portail correspondants sur l'interface Web, et doivent être configurés à l'aide du Registre Windows ou MsiExec. Ceux-ci incluent, sans toutefois s'y limiter, des paramètres tels que : `can-prompt-user-credential`, `wrap-cp-guid` et `filter-non-gpcp`. Ils sont répertoriés dans les options suivantes comme « Pas dans le portail ».

- Affichage de l'application
- Comportement de l'utilisateur
- Comportement de l'application
- Déploiement de script

Options d'affichage de l'application

Le tableau suivant répertorie les options que vous pouvez configurer dans le Registre Windows ou MacOS plist pour personnaliser l'affichage de l'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Tableau 6 : Tableau : Paramètres d'application personnalisables

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
Activer la visualisation avancée	`enable-advanced-view yes | no`	`ENABLEADVANCEDVIEW="yes | no"`	yes
Afficher l'icône GlobalProtect	`show-agent-icon yes | no`	`SHOWAGENTICON="yes | no"`	yes
Activer l'option de Redécouverte du réseau	`rediscover-network yes | no`	`REDISCOVERNETWORK="yes | no"`	yes
Activer l'option de Renvoi du profil d'hôte	`resubmit-host-info yes | no`	S. O.	yes
Afficher les notifications dans la barre des tâches	`show-system-tray-notifications yes | no`	`SHOWSYSTEMTRAYNOTIFICATIONS="yes | no"`	yes

Options de comportement utilisateur

Le tableau suivant répertorie les options que vous pouvez configurer dans le Registre Windows et plist MacOS pour personnaliser le comportement de l'application GlobalProtect.

> *Certains paramètres n'ont pas de paramètres de configuration de portail correspondants sur l'interface Web, et doivent être configurés à l'aide du Registre Windows, MsiExec ou de la plist macOS. Ces paramètres sont listés dans le tableau comme « Pas sur le portail ». Ils incluent, sans toutefois s'y limiter, des paramètres tels que les suivants : `ShowPrelogonButton` et `can-save-password`.*

Tableau 7 : Tableau : Options de comportement utilisateur personnalisables

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
Permettre à l'Utilisateur de modifier l'Adresse du portail	`Peut-il changer le portail oui | non`	`CANCHANGEPORTAL="yes | no"`	yes
Permettre à l'utilisateur de désactiver la page de bienvenue	`Ouvrir-cacher-la page de bienvenue oui | non`	`ENABLEHIDEWELCOMEPAGE= "yes | no"`	yes

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
Permettre à l'utilisateur de continuer avec un certificat de serveur de portail invalide	**`can-continue-if-portal-cert-invalid yes | no`**	**`CANCONTINUEIFPORTALCERTINVALID= ”yes | no”`**	**`no`**
Autoriser l'utilisateur à désactiver GlobalProtect App	**`Autorisé à désactiver oui | non`**	**`DISABLEALLOWED="yes | no"`**	**`no`**
Autoriser l'utilisateur à désinstaller l'application GlobalProtect 1. Le chemin du registre est **`..\Settings\<portal>`**. 2. Ajoutez un 0 pour permettre manuellement aux utilisateurs de désinstaller l'application GlobalProtect avec un mot de passe. Ajoutez un 1 pour empêcher les utilisateurs de désinstaller l'application GlobalProtect. 3. Redémarrez les services de l'agent PAN GP ou redémarrez la machine pour lire la nouvelle valeur.	**`Uninstall 0 | 1`**	S. O.	S. O.
Enregistrer les informations	**`Sauvegarder les informations`**	S. O.	S. O.

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
d'identification de l'utilisateur Spécifiez un 0 pour empêcher GlobalProtect d'enregistrer des informations d'identification, 1 pour enregistrer le nom d'utilisateur et le mot de passe, ou sur 2 pour enregistrer uniquement le nom d'utilisateur.	**d'identification 0 | 1 | 2**		
Pas sur le portail Le paramètre **Allow user to save password (autoriser l'utilisateur à enregistrer le mot de passe)** est obsolète dans l'interface Web dans Pan-OS 7.1 et versions ultérieures, mais est configurable à partir du Registre Windows et de la plist MacOS. Toute valeur spécifiée dans le champ **Save User Credentials (enregistrer les informations d'identification de l'utilisateur)** remplace une valeur spécifiée ici.	**Peut-il sauvegarder un mot de passe oui | non**	**CANSAVEPASSWORD=”yes | no”**	**yes**
Windows uniquement/pas sur le portail	**ShowPrelogonButton yes | no**	S. O.	**no**

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
Ce paramètre permet au fournisseur d'informations d'identification de GlobalProtect d'afficher le bouton **Start GlobalProtect Connection (Lancer la connexion à GlobalProtect)**, qui permet aux utilisateurs d'initier manuellement la connexion de pré-ouverture de session à GlobalProtect.			
Windows 10 only/Not in portal (Windows uniquement/pas sur le portail) Ce paramètre est utilisé conjointement avec l'authentification unique GlobalProtect et permet au fournisseur d'informations d'identification GlobalProtect d'être défini comme option de connexion par défaut lors de la prochaine connexion Windows et pour les connexions suivantes. Pour plus d'informations, reportez-vous à la sectionDéployer les paramètres du fournisseur	`MakeGPCPDefault yes | no (MakeGPCPDefault oui | Non)`	`MAKEGPCPDEFAULT="yes | no" «MAKEGPCPDEFAULT="oui | non"`	S. O.

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
d'informations d'identification GlobalProtect dans le Registre Windows.			
Windows only/Not in portal (Windows uniquement/Pas dans le portail) Ce paramètre est utilisé conjointement avec l'authentification unique GlobalProtect et définit le nombre de secondes pendant les secondes pendant les utilisateurs pour se connecter à Windows avant d'établir une connexion de tunnel. Pour plus d'informations, reportez-vous à la section Déployer les paramètres du fournisseur d'informations d'identification GlobalProtect dans le Registre Windows.	**`LogonWaitTime <5-30 seconds>`**	S. O.	S. O.
Windows uniquement/Pas dans le portail Ce paramètre est utilisé conjointement avec l'authentification unique GlobalProtect et définit le nombre de secondes pour retarder la	**`LogonPostWaitTime <3-10 seconds>`**	S. O.	S. O.

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
connexion des utilisateurs à Windows après l'établissement d'une connexion tunnel. Pour plus d'informations, reportez-vous à la section Déployer les paramètres du fournisseur d'informations d'identification GlobalProtect dans le Registre Windows.			

Options de comportement de l'application

Le tableau suivant répertorie les options que vous pouvez configurer dans le Registre Windows et MacOS plist pour personnaliser le comportement de l'application GlobalProtect.

> *Certains paramètres n'ont pas de paramètres de configuration de portail correspondants sur l'interface Web, et doivent être configurés à l'aide du Registre Windows, MsiExec ou de la plist macOS. Ces paramètres sont listés dans le tableau comme « Pas sur le portail ». Ils incluent, mais ne se limitent pas à, des paramètres tels que les suivants : `portal (portail) <IPaddress>`, `prelogon 1 (préconnexion 1)`, et `can-prompt-user-credential (peut-inviter-utilisateur-infoconnexion)`.*

Tableau 8 : Tableau : Options de comportement de l'application personnalisables

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
Autoriser les utilisateurs à désactiver Se connecter avant identification (CBL)	**`allow-disable-cbl yes | no`**	**`ALLOWDISABLECBL="yes | no"`**	**no**
Méthode de connexion	**`connect-method on-demand | pre-logon | user-logon`**	**`CONNECTMETHOD="on-demand | pre-logon | user-logon"`**	**`user-logon`**
Méthode de connexion	**`conditional-connect yes | no`**	S. O.	**no**

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
conditionnelle basée sur le type de réseau			
Non pris en charge sur le portail	**intelligent-portal yes | no**	**INTELLIGENTPORTAL=”yes | no”**	**no**
Adresse IP du portail pour les États-Unis et la Chine	**portal-country-map "<IP address>(US);<IP address>(CN)"**	**PORTALCOUNTRYMAP = "<Portal IP address>(US);<Portal IP address>(CN)"**	S. O.
Emplacement de l'utilisateur	**intelligent-portal-service "URL"**	**INTELLIGENTPORTALSERVICE = "<IP location URL>"**	S. O.
Non pris en charge sur le portail	**SAMLAUTHPROXY="--proxy-server=<proxy server>"** Par exemple, `--proxy-pac-url="https://example.com/proxy.pac"` Pris en charge uniquement pour les terminaux Windows.	**SAMLAUTHPROXY="--proxy-server=<proxy server>"**	S. O.
Utiliser le navigateur par défaut pour le portail captif	**CPUSINGDEFBROWSER = yes | no** Pris en charge uniquement pour les terminaux Windows.	**CPUSINGDEFBROWSER = yes | no**	oui Le navigateur par défaut est utilisé pour le portail captif.
Intervalle de rafraîchissement de configuration de l'application GlobalProtect (en heures)	**refresh-config-interval <hours>**	**REFRESHCONFIGINTERVAL= ”<hours>”**	**24**

©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
Envoyer immédiatement un rapport HIP si l'état du centre de sécurité de Windows (WSC) change (Windows uniquement)	**`wsc-autodetect yes | no (wsc-autodetect oui | non)`**	S. O.	**`no`**
Détecter le proxy pour chaque connexion (Windows uniquement)	**`proxy-multiple-autodetect yes | no (proxy-multiple-autodetect oui | non)`**	S. O.	**`no`**
Effacer les identifiants d'ouverture de session unique à la fermeture de session (Windows uniquement)	**`logout-remove-sso yes | no (déconnexion-supprimer-sso oui | non)`**	**`LOGOUTREMOVESSO="yes | no" (DeconnexionSuppressionSSO Oui | Non)`**	**`yes`**
Désactiver le Single Sign-On (ouverture de session unique - SSO) sur les machines locales Ce paramètre vous permet de désactiver la fonctionnalité SSO même si elle est configurée sur le portail. Il écrase la configuration du portail lorsque vous ajoutez manuellement la clé au Registre Windows ou à la plist macOS et définissez la valeur comme **Yes (Oui)**.	Pour les terminaux Windows, vous devez ajouter manuellement ce paramètre au Registre Windows : **Chemin Windows :** **`HKEY_LOCAL_MACHINE \SOFTWARE\Palo Alto Networks \GlobalProtect \Settings`** **Nom/valeur de la clé :** **`force-sso-disable yes | no`** Pour les terminaux macOS, vous devez ajouter manuellement ce paramètre à la plist macOS : **Chemin macOS :**	Ce paramètre n'est pas pris en charge dans msiexec.	S. O.

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
	/Library/Preferences/ com.paloaltonetworks. GlobalProtect.settings.plist Ajoutez le paramètre sous **Palo Alto Networks > GlobalProtect > Settings (Palo Alto Networks > GlobalProtect > Paramètres)** Nom/valeur de la clé : **force-sso-disable yes | no**		
Utiliser l'authentification par défaut en cas d'échec d'authentification Kerberos (Windows uniquement)	**Solution de repli si échec d'authentification Kerberos oui | non**	**KRBAUTHFAILFALLBACK= "yes | no"**	**no**
Utiliser le navigateur par défaut pour l'authentification SAML	(macOS plist) **default-browser yes | no**	**DEFAULTBROWSER= "yes | no"**	**no**
Message personnalisé d'expiration de mot de passe (authentification LDAP uniquement)	(Deprecated) **PasswordExpiryMessage <message>**	S. O.	**Le mot de passe expire dans <number> jours**
Délai d'expiration de connexion au portail (sec.)	**portal-timeout (portail-expirationdélai) <portaltimeout>**	S. O.	**5**
Délai d'expiration de connexion TCP (sec.)	**connect-timeout (connexion_expiratiodélai) <connect-timeout>**	S. O.	**5**

©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
Délai d'expiration de réception TCP (sec)	**receive-timeout (recevoir-expirationdélai) <receive-timeout>**	S. O.	**30**
Recherche dans le magasin de certificats du client	**certificate-store-lookup user | machine | user and machine | invalid**	**CERTIFICATESTORELOOKUP="user | machine | user and machine | invalid"**	**utilisateur et machine**
Période de renouvellement de certificat SCEP (jours)	**scep-certificate-renewal-period <renewalPeriod>**	S. O.	**7**
Nombre maximum de tentatives de connexion à la passerelle interne	**max-internal-gateway-connection-attempts <maxValue>**	**MIGCA="<maxValue>"**	**0**
Sélection du Certificat Client selon un OID inclus dans une clé étendue	**ext-key-usage-oid-for-client-cert <oidValue>**	**EXTCERTOID="<oidValue>"**	S. O.
Activer la vérification stricte des certificats	**enable-strict-certificate-check yes | no | Use Pre-deployed Setting**		**Utiliser le paramètre pré-déployé**
Délai d'expiration pour renommer le tunnel de bascule d'utilisateur (sec)	**user-switch-tunnel-rename-timeout <renameTimeout>**	S. O.	**0**
Utiliser l'ouverture de session unique (Windows uniquement)	**use-sso yes | no**	**USESSO="yes | no"**	**yes**

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
Use Single Sign-On for Smart Card (Windows Only) (Utiliser l'authentification unique pour la carte à puce (Windows uniquement))	**use-sso-pin yes | no (utiliser-sso-pin oui | non)**	**USESSOPIN="yes | no" (UTILISERCODESSO="oui | non")**	**no**
Message d'authentification entrant	**authentication-message (Message d'authentification)**	S. O.	S. O.
Autoriser le remplacement du nom d'utilisateur d'un certificat du client	**override-cc-username yes | no (effacer-cc-nomutilisateur oui | non**	S. O.	**no**
Pas sur le portail Ce paramètre indique l'adresse IP du portail par défaut (ou le nom d'hôte).	**portal** <IPaddress>	**PORTAL="**<IPaddress>**"**	S. O.
Pas sur le portail Ce paramètre autorise GlobalProtect à initier une connexion VPN avant qu'un utilisateur ne se connecte au périphérique et au portail GlobalProtect.	**pré-connexion 1**	**PRELOGON="1"**	**1**
Pas sur le portail Ce paramètre est utilisé en association avec	(Windows) **can-prompt-user-credential yes | no (peut-inviter-utilisateur-**	**CANPROMPTUSERCREDENTIAL="yes | no"**	**yes**

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
l'ouverture de session unique et indique s'il faut inviter l'utilisateur à fournir des informations d'identification en cas d'échec de l'ouverture de session unique.	**infoconnexion oui | non)**		
Windows uniquement/pas sur le portail Ce paramètre filtre la fenêtre d'informations d'identification indépendantes du fournisseur dans la page de connexion Windows de sorte que seule la fenêtre Windows native s'affiche.*	**wrap-cp-guid {guide du fournisseur d'informations d'identification indépendantes}**	**WRAPCPGUID="{guid_value}" FILTERNONGPCP="yes | no"**	**no**
Windows uniquement/pas sur le portail Ce paramètre est une option supplémentaire pour le paramètre wrap-cp-guid, et autorise l'affichage de la fenêtre du fournisseur d'informations d'identification indépendantes sur la page de connexion Windows, en plus de la fenêtre	**filter-non-gpcp no**	S. O.	S. O.

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
de connexion Windows native.*			
Windows uniquement/pas sur le portail Ce paramètre vous permet d'affecter des adresses IP statiques à des points de terminaison Windows.	**reserved-ipv4** <**reserved-ipv4**> **reserved-ipv6** <**reserved-ipv6**>	**RESERVEDIPV4="**<**reserved-ipv4**>**"** **RESERVEDIPV6="**<**reserved-ipv6**>**"**	S. O.
(Windows uniquement) Ce paramètre vous permet de définir une passerelle par défaut valide sur l'adaptateur virtuel GlobalProtect lorsque vous configurez l'application GlobalProtect en mode tunnel complet.	**fake-default-gateway yes | no**	**FIXDEFAULTGATEWAY yes | no**	S. O.
Pas sur le portail Ce paramètre vous permet de pré-déployer l'indicateur de vérification complète de la chaîne de certificats.	Pour les terminaux macOS, vous devez ajouter manuellement ce paramètre à la plist macOS : **Chemin macOS :** **/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist** Ajoutez le paramètre sous **Palo Alto Networks > GlobalProtect > Settings (Palo Alto Networks > GlobalProtect > Paramètres)**	S. O.	S. O.

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
	Nom/valeur de la clé : **`full-chain-cert-verify yes | no`**		
(Windows uniquement) Ce paramètre vous permet de collecter des données HIP sur les terminaux Windows.	**`collect-hip-data yes | no`**	**`COLLECTHIPDATA= ”yes | no”`**	S. O.
(Windows uniquement) Ce paramètre vous permet d'enregistrer les mots de passe de la passerelle sur les terminaux Windows.	**`save-gateway-password yes | no`**	**`SAVEGATEWAYPASSWORD= ”yes | no”`**	S. O.
Windows uniquement/pas sur le portail Ce paramètre vous permet d'appuyer sur la touche **Entrée** pour vous connecter à GlobalProtect depuis le navigateur intégré sur les terminaux Windows lors de l'authentification SAML. Dans certains cas, l'activation de ce paramètre empêchera la touche **Entrée** d'être reconnue lors de la	**Chemin du Registre Windows :** **`HKEY_CURRENT_USER\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`** **Nom/valeur de la clé :** **`translate-enter-key yes | no`**	**`TRANSLATEENTERKEY= "yes | no"`**	**`yes`**

©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Par défaut
connexion. Si cela se produit, changez le paramètre en **no (non)**.			

Pour des étapes détaillées pour activer ces paramètres en utilisant le Registre Windows ou l'installateur Windows (Msiexec), rendez-vous sur Englobement de l'ouverture de session unique pour les fournisseurs d'informations d'identification indépendantes sur les clients Windows.

Options de déploiement de scripts

Les paramètres suivants permettent à GlobalProtect d'initier des scripts avant et après l'établissement d'une connexion et avant la déconnexion. Étant donné que ces options ne sont pas disponibles dans le portail, vous devez définir les valeurs de la clé correspondante, soit pre-vpn-connect, post-vpn-connect,ou pre-vpn-disconnect, partir du Registre Windows ou la plist MacOS. Pour obtenir des étapes détaillées pour déployer des scripts, voir déployer des scripts à l'aide du Registre Windows, déployer des scripts à l'aide de msiexec ou déployer des scripts à l'aide de la plist MacOS.

Si vous autorisez les utilisateurs finaux à établir la connexion VPN au réseau d'entreprise avant de vous connecter au point de terminaison Windows à l'aide de Se connecter avant ouverture de session, vous devez exécuter des scripts de connexion VPN avec la valeur ***context admin (administrateur de contexte)*** *spécifiée dans le Registre Windows. Vous ne pouvez pas spécifier la valeur* ***context user (utilisateur de contexte)*** *par défaut car il n'y a pas d'utilisateur avant l'ouverture de session Windows.*

Tableau : Options de déploiement de scripts personnalisables

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
Exécutez le script indiqué dans le paramètre de la commande (y compris les paramètres transmis au script). *Les variables d'environnement sont prises en charge.* *Indiquez le chemin d'accès*	**command <parameter1> <parameter2> [...]** Exemple Windows : **command %userprofile% \vpn_script.bat c: test_user** Exemple macOS : **command $HOME/ vpn_script.sh /**	**PREVPNCONNECTCOMMAND= "<parameter1> <parameter2> [...]"** **POSTVPNCONNECTCOMMAND= "<parameter1> <parameter2> [...]"** **PREVPNDISCONNECTCOMMAND= "<parameter1> <parameter2> [...]"**	**S. O.**

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
complet dans les commandes.	**Users/test_user test_user**		
(Facultatif) Spécifiez les privilèges sous lesquels les commandes peuvent être exécutées (l'utilisateur par défaut est user : si vous ne spécifiez pas le contexte, la commande s'exécute en tant qu'utilisateur actif actuel).	**context admin | user**	**PREVPNCONNECTCONTEXT= "admin | user"** **POSTVPNCONNECTCONTEXT= "admin | user"** **PREVPNDISCONNECTCONTEXT= "admin | user"**	**user**
(Facultatif) Spécifiez le nombre de secondes pendant lesquelles l'application GlobalProtect attend la commande à exécuter (la plage est de 0 à 120). Si la commande n'aboutit pas avant l'expiration du délai d'attente, l'application passe alors à l'établissement d'une connexion ou d'une déconnexion. Une valeur de 0 (définie par défaut) signifie que l'application n'attend pas avant d'exécuter la commande. *Non pris en charge pour la valeur post-vpn-connect.*	**timeout <valeur>** Exemple : **timeout 60**	**PREVPNCONNECTTIMEOUT= "<valeur>"** **PREVPNDISCONNECTTIMEOUT= "<valeur>"**	**0**
(Facultatif) Précisez le chemin d'accès complet d'un fichier utilisé dans une commande. L'application GlobalProtect vérifie	**file <chemin_fichier>**	**PREVPNCONNECTFILE= "<chemin_fichier>"** **POSTVPNCONNECTFILE= "<chemin_fichier>"**	**S. O.**

©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
l'integrité du fichier en le contrôlant avec la valeur indiquée dans la clé checksum. *Les variables d'environnement sont prises en charge.*		**PREVPNDISCONNECTFILE= ”<chemin_fichier>”**	
(Facultatif) Indiquez la somme de contrôle sha256 du fichier qui est référencée dans la clé de fichier. Si la somme de contrôle est spécifiée, l’application GlobalProtect exécute la ou les commandes uniquement si la somme de contrôle générée par l’application GlobalProtect correspond à la valeur de checksum spécifiée ici.	**checksum** <**valeur**>	**PREVPNCONNECTCHECKSUM= ”<valeur>”** **POSTVPNCONNECTCHECKSUM= ”<valeur>”** **PREVPNDISCONNECTCHECKSUM =”<valeur>”**	**S. O.**
(Facultatif) Spécifiez un message d’erreur pour informer l’utilisateur que la ou les commandes ne peuvent pas exécuter ou que la ou les commandes sont sorties avec un code de retour non nul. *Le message doit contenir un maximum de 1 024 caractères ANSI.*	**error-msg** <**message**> Exemple : **error-msg Échec de l'exécution de l'action pre-vpn-connect!**	**PREVPNCONNECTERRORMSG= ”<message>”** **POSTVPNCONNECTERRORMSG= ”<message>”** **PREVPNDISCONNECTERRORMSG =”<message>”**	**S. O.**

©2026 Palo Alto Networks, Inc.

Configurer la méthode de connexion conditionnelle en fonction du type de réseau

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Version de l'application GlobalProtect 6.2 ou ultérieure pour Windows et macOS

Configurez la Connexion conditionnelle pour permettre à l'application GlobalProtect de modifier la méthode de connexion dynamiquement en fonction de la détection interne de l'hôte qui détermine que l'utilisateur est sur le réseau interne ou travaille à partir d'un emplacement distant. Vous déployez le paramètre conditional-connect de manière transparente depuis la liste macOS ou le Registre Windows. Avant d'activer la Connexion conditionnelle, assurez-vous d'avoir :

Activé la détection d'hôte interne

Configuré les terminaux pour utiliser la méthode de connexion à la demande

Déployez la Connexion conditionnelle aux terminaux Windows.

1. Dans le Registre Windows, rendez-vous sur **\HKEY_LOCAL_MACHINE > SOFTWARE> Palo Alto Networks > GlobalProtect > Settings**.
2. Définissez la clé comme **conditional-connect (connexion-conditionnelle)** et la valeur sur **Yes (Oui)**.

Déployez la Connexion conditionnelle aux terminaux macOS.

1. Dans le fichier plist (/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist), allez dans **/Palo Alto Networks/GlobalProtect/Settings**.
2. Définissez **conditional-connect (conditionnelle-connect)** sur **Yes (Oui)**.

Déployer les paramètres d'application sur des points de terminaison Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Utilisez le registre Windows ou le programme d'installation Windows (Msiexec) pour déployer l'application GlobalProtect et ses paramètres de manière transparente sur des points de terminaison Windows.

- Déployer les paramètres d'agent dans le registre Windows

 ©2026 Palo Alto Networks, Inc.

- Déployer les paramètres de l'agent via Msiexec
- Déployer des scripts à l'aide du registre Windows
- Déployer des scripts à l'aide de Msiexec
- Déployer les paramètres de Connexion avant identification dans le registre de Windows
- Déployer les paramètres du fournisseur d'informations d'identification GlobalProtect dans le Registre Windows
- Englobement de l'ouverture de session unique pour les fournisseurs d'informations d'identification indépendantes sur les clients Windows
- Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le registre Windows
- Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le programme d'installation Windows

Déployer les paramètres d'application dans le registre Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Vous pouvez activer le déploiement des paramètres de l'application GlobalProtect sur les points de terminaison Windows avant leur première connexion au portail GlobalProtect à l'aide du registre Windows. Utilisez les options décrites dans le tableau suivant pour personnaliser des paramètres d'application pour points de terminaison Windows à l'aide du registre Windows.

Outre l'utilisation du registre Windows pour déployer les paramètres d'application GlobalProtect, vous pouvez autoriser l'application GlobalProtect à collecter des informations de registre Windows spécifiques sur les points de terminaison Windows. Vous pouvez ensuite surveiller les données et les ajouter à une règle de sécurité pour les utiliser en tant que critères de correspondance. Le trafic du point de terminaison correspondant aux paramètres de registre que vous définissez peut être mis en œuvre conformément à la règle de sécurité. En outre, vous pouvez configurer des vérifications personnalisées pour recueillir des données d'application et de traitement des points de terminaison.

1. Recherchez les paramètres de personnalisation d'application GlobalProtect dans le registre Windows.

   Ouvrez le registre Windows (saisissez **`regedit`** dans l'invite de commande) et accédez à :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
   \
   ```

 ©2026 Palo Alto Networks, Inc.

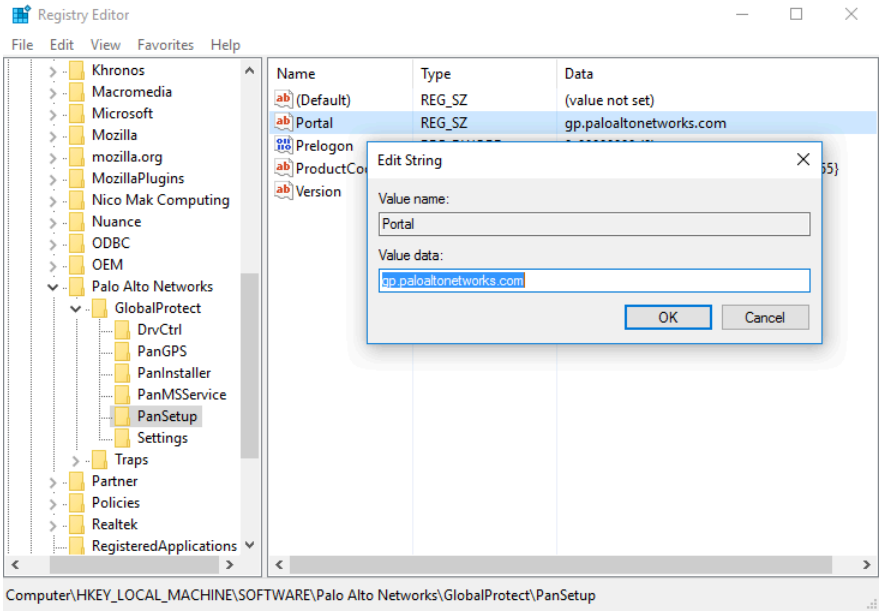
2. Définissez le nom du portail.

Si vous ne souhaitez pas que l'utilisateur final puisse saisir manuellement l'adresse du portail même pour la première connexion, vous pouvez pré-déployer l'adresse du portail via le registre Windows.

Si vous souhaitez définir tous les autres paramètres de l'application, vous pouvez définir des clés dans le registre Windows (`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`

1. Dans le registre Windows, accédez à :

   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`
2. Cliquez avec le bouton droit sur **Portal (Portail)** et sélectionnez **Modify (Modifier)**.
3. Saisissez le nom du portail dans le champ **Value data (Données de valeur)**, puis cliquez sur **OK**.



3. Déployez divers paramètres au point de terminaison Windows, y compris la méthode de connexion utilisée pour l'application GlobalProtect et l'ouverture de session unique.

Consultez Paramètres d'application personnalisables pour obtenir une liste complète des commandes et des valeurs que vous pouvez configurer à l'aide du Registre Windows.

Vous avez le choix de deploy connect before logon settings (déployer la connexion anat les paramètres de connexion) sur les terminaux Windows avant d'autoriser les utilisateurs finaux à se connecter au VPN avant la connexion au terminal.

Vous avez la possibilité de deploy GlobalProtect credential provider settings (déployer les paramètres du fournisseur d'informations d'identification GlobalProtect) sur les points de terminaison Windows pour retarder la demande de connexion Windows du fournisseur d'informations d'identification GlobalProtect ou appliquer le fournisseur d'informations d'identification GlobalProtect comme option de connexion par défaut.

 ©2026 Palo Alto Networks, Inc.

4. Permettez à l'application GlobalProtect d'englober des informations d'identification indépendantes sur le point de terminaison Windows, autorisant ainsi l'ouverture de session unique lorsqu'un fournisseur d'informations d'identification indépendantes est utilisé.

   Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le registre Windows

Déployer les paramètres d'application via Msiexec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Sur les clients Windows, vous avez l'option de déployer automatiquement l'application GlobalProtect et les paramètres de l'application depuis le programme d'installation Windows (Msiexec) en utilisant la syntaxe suivante :

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec est un programme exécutable qui installe ou configure un produit depuis la ligne de commande. Sur les points de terminaison dotés de Microsoft Windows XP ou d'une version ultérieure, la longueur maximale de la chaîne que vous pouvez utiliser dans l'invite de commande est de 8 191 caractères.

Example Msiexec	Description
`msiexec.exe /i GlobalProtect.msi /quiet PORTAL="portal.acme.com"`	Installez GlobalProtect en mode silencieux (aucune interaction utilisateur) et configurez l'adresse du portail.
`msiexec.exe /i GlobalProtect.msi CANCONTINUEIFPORTALCERTINVALID="no"`	Installez GlobalProtect avec l'option d'empêcher les utilisateurs de se connecter au portail si le certificat n'est pas valide.

Pour une liste complète des paramètres et des valeurs correspondantes par défaut, reportez-vous à la section Paramètres d'application personnalisables.

Vous pouvez également Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le programme d'installation Windows.

Déployer des scripts à l'aide du registre Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

 ©2026 Palo Alto Networks, Inc.

Vous pouvez activer le déploiement de scripts personnalisés sur les systèmes clients Windows à l'aide du registre Windows.

Vous pouvez configurer l'application GlobalProtect pour qu'il initie et exécute un script lorsque l'un ou l'autre des événements suivants survient : avant et après l'établissement du tunnel et après la déconnexion du tunnel. Pour exécuter le script lorsqu'un événement donné se produit, référencez le script de commande depuis une entrée de commande au registre applicable à cet événement.

Selon les paramètres de configuration, l'application GlobalProtect peut exécuter un script avant et après qu'elle établit une connexion avec la passerelle et avant de se déconnecter. Utilisez le flux de travail suivant pour personnaliser des paramètres d'application pour points de terminaison Windows à l'aide du registre Windows.

Les paramètres du registre qui vous permettent de déployer des scripts sont pris en charge sur les points de terminaison fonctionnant avec l'application GlobalProtect 2.3 ou une version ultérieure.

1. Ouvrez le registre Windows et recherchez les paramètres de personnalisation de l'application GlobalProtect.

   Ouvrez le registre Windows (saisissez **`regedit`** dans l'invite de commande) et accédez à l'un des emplacements de clé suivant, selon le moment où vous voulez exécuter les scripts (avant / après la connexion ou avant la déconnexion) :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
   \pre-vpn-connect
   ```

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
   \post-vpn-connect
   ```

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
   \pre-vpn-disconnect
   ```

   *Si la clé n'existe pas dans la touche **Settings (Paramètres)**, créez-la en cliquant avec le bouton droit de la souris sur **Settings (Paramètres)** et en sélectionnant **New (Nouvelle)** > **Key (Clé)**).*

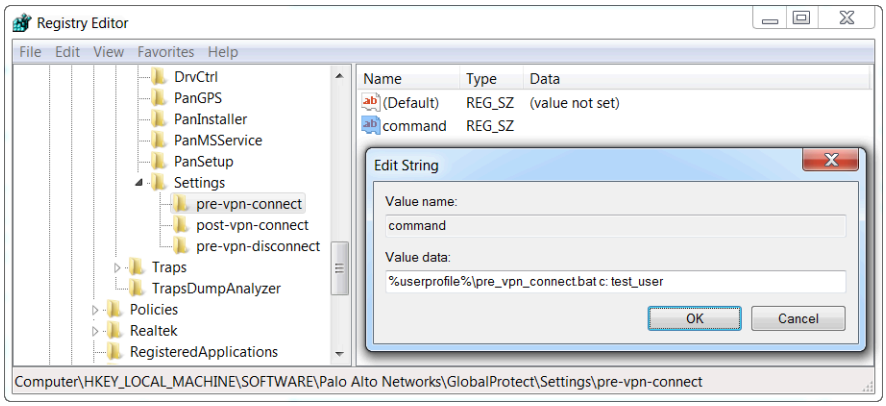
 ©2026 Palo Alto Networks, Inc.

2. Permettez à l'application GlobalProtect d'exécuter des scripts en créant une nouvelle valeur de chaîne nommée `command`.

   Le fichier batch indiqué ici devrait contenir le script spécifique (y compris les paramètres transmis au script) que vous souhaitez exécuter sur le périphérique.

   1. Si la chaîne `command` n'existe pas encore, créez-la en faisant un clic droit sur la clé `pre-vpn-connect`, `post-vpn-connect` ou `pre-vpn-disconnect`, en sélectionnant **New (Nouvelle)** > **String Value (Valeur de chaîne)** et en la nommant **`command`**).
   2. Cliquez avec le bouton droit sur `command`, puis sélectionnez **Modify (Modifier)**.
   3. Saisissez les commandes ou le script que l'application GlobalProtect doit exécuter. Par exemple :

      ```
      %userprofile%\pre_vpn_connect.bat c:test_user
      ```

3. (Facultatif) Au besoin, ajoutez d'autres entrées de registre pour chaque commande.

   Créez ou modifiez les chaînes du registre et leurs valeurs correspondantes, notamment `context`, `timeout`, `file`, `checksum` ou `error-msg`. Pour plus d'informations, consultez Paramètres d'application personnalisables.

Déployer des scripts à l'aide de Msiexec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Sur les terminaux Windows, vous pouvez utiliser le programme d'installation de Windows (Msiexec) pour déployer l'application GlobalProtect, les paramètres de l'application et les scripts que l'application exécutera automatiquement (consultez Paramètres d'application personnalisables). Pour ce faire, utilisez la syntaxe suivante :

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec est un programme exécutable qui installe ou configure un produit depuis une ligne de commande. Sur les points de terminaison qui utilisent Microsoft Windows XP ou toute version

 ©2026 Palo Alto Networks, Inc.

ultérieure de Windows, la longueur maximale de la chaîne que vous pouvez utiliser dans l'invite de commande est de 8 191 caractères.

Cette restriction s'applique à la ligne de commande, aux variables d'environnement individuelles (comme la variable USERPROFILE) qui sont héritées par d'autres processus et à l'ensemble des expansions de variables. Si vous exécutez des fichiers batch à partir de la ligne de commande, cette restriction s'applique également au traitement des fichiers batch.

Par exemple, pour déployer des scripts qui s'exécutent lors d'événements de connexion ou de déconnexion donnés, vous pouvez utiliser une syntaxe semblable aux exemples suivants :

Exemple : Utiliser Msiexec pour déployer des scripts qui s'exécutent avant un événement de connexion

Pour un script que vous pouvez copier et coller, allez ici.

```
msiexec.exe /i GlobalProtect.msi PREVPNCONNECTCOMMAND="%userprofile
%\pre_vpn_connect.bat c: test_user" PREVPNCONNECTCONTEXT="user"
 PREVPNCONNECTTIMEOUT="60" PREVPNCONNECTFILE="C:\Users\test_user
\pre_vpn_connect.bat"
 PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
 8647ccf599" PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect
 action."
```

Pour une liste complète des paramètres et des valeurs correspondantes par défaut, consultez Paramètres d'application personnalisables.

Exemple : Utiliser Msiexec pour déployer des scripts qui s'exécutent lors d'événements de pré-connexion, de post-connexion et de pré-déconnexion

Pour un script que vous pouvez copier et coller, allez ici.

```
msiexec.exe /i GlobalProtect.msi PREVPNCONNECTCOMMAND="%userprofile
%\pre_vpn_connect.bat c: test_user" PREVPNCONNECTCONTEXT="user"
 PREVPNCONNECTTIMEOUT="60" PREVPNCONNECTFILE="C:\Users\test_user
\pre_vpn_connect.bat"
 PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
 8647ccf599" PREVPNCONNECTERRORMSG="Failed executing pre-vpn-
connect action." POSTVPNCONNECTCOMMAND="c:\users\test_user
\post_vpn_connect.bat c: test_user" POSTVPNCONNECTCONTEXT="admin"
 POSTVPNCONNECTFILE="%userprofile%\post_vpn_connect.bat"
 POSTVPNCONNECTCHECKSUM="b48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
 8647ccf598" POSTVPNCONNECTERRORMSG="Failed executing post-
vpn-connect action." PREVPNDISCONNECTCOMMAND="%userprofile%
\pre_vpn_disconnect.bat c: test_user" PREVPNDISCONNECTCONTEXT="admin"
 PREVPNDISCONNECTTIMEOUT="0" PREVPNDISCONNECTFILE="C:
\Users\test_user\pre_vpn_disconnect.bat"
 PREVPNDISCONNECTCHECKSUM="c48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0
 118647ccf597" PREVPNDISCONNECTERRORMSG="Failed executing pre-vpn-
disconnect action."
```

Pour une liste complète des paramètres et des valeurs correspondantes par défaut, consultez Paramètres d'application personnalisables.

 ©2026 Palo Alto Networks, Inc.

Déployer les paramètres de Connexion avant identification dans le registre de Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Vous pouvez déployer la connexion avant les paramètres d'identification sur les terminaux Windows 10 avant d'autoriser les utilisateurs finaux à se connecter au VPN avant la connexion au terminal en utilisant le Registre Windows. GlobalProtect récupère les clés de registre une seule fois : lors de l'initialisation de l'application GlobalProtect.

Suivez ces instructions lors du déploiement des paramètres de connexion avant l'ouverture de session :

- *Les méthodes de préouverture de session et préouverture de session puis connexion à la demande ne sont pas possibles de façon simultanée avec Se connecter avant identification.*
- *Si vous utilisez l'authentification par carte à puce ou l'authentification par nom d'utilisateur/mot de passe pour la connexion utilisateur à l'aide d'un service d'authentification tel que LDAP, RADIUS ou OTP, vous devez configurer des exclusions pour des noms de domaine complets spécifiques pour le portail et la passerelle en les saisissant sur* ***Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established (Autoriser le trafic vers le nom de domaine complet spécifié lorsque Appliquer la connexion GlobalProtect pour l'accès au réseau est activé et que la connexion GlobalProtect n'est pas établie)*** *en tant que* app setting (paramètre d'application) *dans la zone* ***App Configurations (configurations d'application)*** *du portail GlobalProtect. Si vous utilisez l'authentification SAML pour la connexion des utilisateurs et les fournisseurs d'identité SAML (IdP) configurés tels qu'Okta, vous devez également configurer des exclusions pour *okta.com et *oktacdn.com. Pour les autres IdP, vous devez configurer des exclusions pour les URL qui contiennent des adresses IP ou des noms de domaine complets uniquement si l'état Appliquer est activé.*

1. Configurer les clés de registre sur les terminaux Windows de l'utilisateur final.

   Vous devez modifier le registre de Windows sur les terminaux Windows de l'utilisateur final avant de pouvoir activer Se connecter avant identification. Vous pouvez ajouter automatiquement ou manuellement les clés de registre.

   - Pour ajouter les clés de registre automatiquement `PanPlapProvider` et `PanPlapProvider.dll` dans**PanGPS.exe** (`C:\Program Files\Palo Alto Networks\GlobalProtect`), utilisez la commande `-registerplap` pour lancer en tant qu'administrateur en utilisant la syntaxe suivante :

     ```
     PanGPS.exe -registerplap
     ```

   - Pour supprimer des clés de registre automatiquement `PanPlapProvider` et `PanPlapProvider.dll` dans**PanGPS.exe** (`C:\Program Files\Palo Alto`

 ©2026 Palo Alto Networks, Inc.

Networks\GlobalProtect), utilisez la commande `-unregisterplap` pour lancer en tant qu'administrateur en utilisant la syntaxe suivante :

```
PanGPS.exe -unregisterplap
```

Pour ajouter manuellement des clés de registre, ourez l'éditeur de clés de registre Windows et saisissez **regedit** dans l'invite de commande.

Vous devez créer le dossier `CLSID`.

1. Dans le registre Windows, allez à `HKEY_CLASSES_ROOT\CLSID\{20A29589-E76A-488B-A520-63582302A285}`.

   Ajoutez la valeur `PanPlapProvider` au format **`@=PanPlapProvider`**.
2. Dans le registre Windows, allez à `HKEY_CLASSES_ROOT\CLSID\{20A29589-E76A-488B-A520-63582302A285}\InprocServer32@="PanPlapProvider.dll"`.

   Vérifiez que la valeur du **ThreadingModel (modèle multitâche)** est réglée sur **Apartment (appartement)**. Il s'agit de la valeur par défaut.
3. Dans le registre Windows, allez à `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{20A29589-E76A-488B-A520-63582302A285}@="PanPlapProvider"`.

   Ajoutez la valeur `PanPlapProvider` au format **`@=PanPlapProvider`**.

2. (En option) Configurez des adresses de portail supplémentaires ou des noms à afficher.

   Si elle est configurée, l'option Se connecter avant identification utilisera l'adresse ou le nom du portail par défaut dans le registre Windows (`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` avec le portail `de la clé`).

Vous pouvez configurer d'autres adresses ou noms de portail que vous voulez afficher dans la liste déroulante des portails en modifiant les clés de registre sur les terminaux Windows de l'utilisateur final. Vous pouvez ajouter jusqu'à cinq adresses ou noms de portail. Vous devez

 ©2026 Palo Alto Networks, Inc.

modifier le registre de Windows sur les terminaux Windows de l'utilisateur final avant de pouvoir définir les adresses ou noms de portail.

Ouvrez l'éditeur de registre Windows et saisissez **regedit** dans l'invite de commande.

1. Dans le registre Windows, créez le dossierCBL sous `HKEY_LOCAL_MACHINE \SOFTWARE\Palo Alto Networks\GlobalProtect`.
2. Dans le registre Windows, allez à`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
3. Sélectionnez **Edit (Modifier)** > **New (Nouveau)** > **String Value (Valeur de la chaîne)** pour créer une entrée de registre pour chaque portail que vous souhaitez ajouter.

   Vous devez indiquer chaque entrée comme *Portal1 Portail1)*, *Portal2 (Portail2)*, *Portal3 (Portail3)*, *Portal4 (Portail4)*, et *Portal5 (Portail5)*. Chaque entré ne doit pas contenir d'espace.
4. Faites un clic droit sur la valeur de registre du*portal (portail)* puis sélectionnez **Modify (Modifier)**.
5. Saisissez l'adresse IP ou le nom du portail GlobalProtect dans le champ **Value Data (Données de la valeur)** puis cliquez sur **OK**.
6. Répétez les étapes 3 et 4 pour chaque portail que vous souhaitez ajouter;

3. (En option) Affichez les adresses ou noms de portail prédéfinis.

Vous pouvez modifier le registre Windows sur les terminaux Windows de l'utilisateur final avant de pouvoir afficher les adresses ou les noms de portail.

Ouvrez l'éditeur de registre Windows et saisissez **regedit** dans l'invite de commande.

1. Dans le registre Windows, créez le dossierCBL sous `HKEY_LOCAL_MACHINE \SOFTWARE\Palo Alto Networks\GlobalProtect`.
2. Dans le registre Windows, allez à`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
3. Sélectionnez **Edit (Modifier)** > **New (Nouveau)** > **String Value (Valeur de la chaîne)** pour créer une entrée de registre pour *AlwaysShowPortal (toujours afficher le portail).*.
4. Saisissez la valeur*yes (oui)* dans le champ **Value data (Données de valeur)**, puis cliquez sur **OK**.

   Par défaut, Se connecter avant identification n'affiche pas l'adresse ou le nom du portail si un seul portail est défini.

 ©2026 Palo Alto Networks, Inc.

4. (En option) Activez les utilisateurs finaux afin qu'ils s'authentifient avec une Smart card.

   Vous devez modifier le registre de Windows sur les terminaux Windows de l'utilisateur final avant de pouvoir activer l'authentification par smart card.

   Ouvrez l'éditeur de registre Windows et saisissez **regedit** dans l'invite de commande.

   1. Dans le registre Windows, créez le dossierCBL sous `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`.
   2. Dans le registre Windows, allez à`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\CBL`.
   3. Sélectionnez **Edit (Modifier)** > **New (Nouveau)** > **String Value (Valeur de la chaîne)** pour créer une entrée de registre pour *UseSmartCard (utiliser une smart card)*..
   4. Saisissez la valeur*yes (oui)* dans le champ **Value data (Données de valeur)**, puis cliquez sur **OK**.

5. Redémarrer le terminal.

   Vous devez redémarrer le terminal afin que les clés de registre PLAP et Se connecter avent identification prennent effet.

6. Vérifiez la configuration.

   Une fois que vous avez configurer les paramètres dans le registre Windows et pour utiliser Se connecter avant identification à partir de la version 5.2 de l'application GlobalProtect, choisissez la méthode d'authentification :

   - Connect Before Logon Using Smart Card Authentication (Se connecter avant identification en utilisant l'authentification Smart card)
   - Connect Before Logon Using SAML Authentication (Se connecter avant identification en utilisant l'authentification SAML)
   - Connect Before Logon Using Username/Password-Based Authentication (Se connecter avant identification en utilisant l'authentification basée sur un nom d'utilisateur/mot de passe)

Déployer les paramètres du fournisseur d'informations d'identification GlobalProtect dans le Registre Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Vous pouvez déployer les paramètres du fournisseur d'informations d'identification GlobalProtect pour retarder la demande de connexion Windows du fournisseur d'informations d'identification GlobalProtect ou pour appliquer le fournisseur d'informations d'identification GlobalProtect comme option de connexion par défaut pour Windows 10 en utilisant le registre Windows.

 ©2026 Palo Alto Networks, Inc.

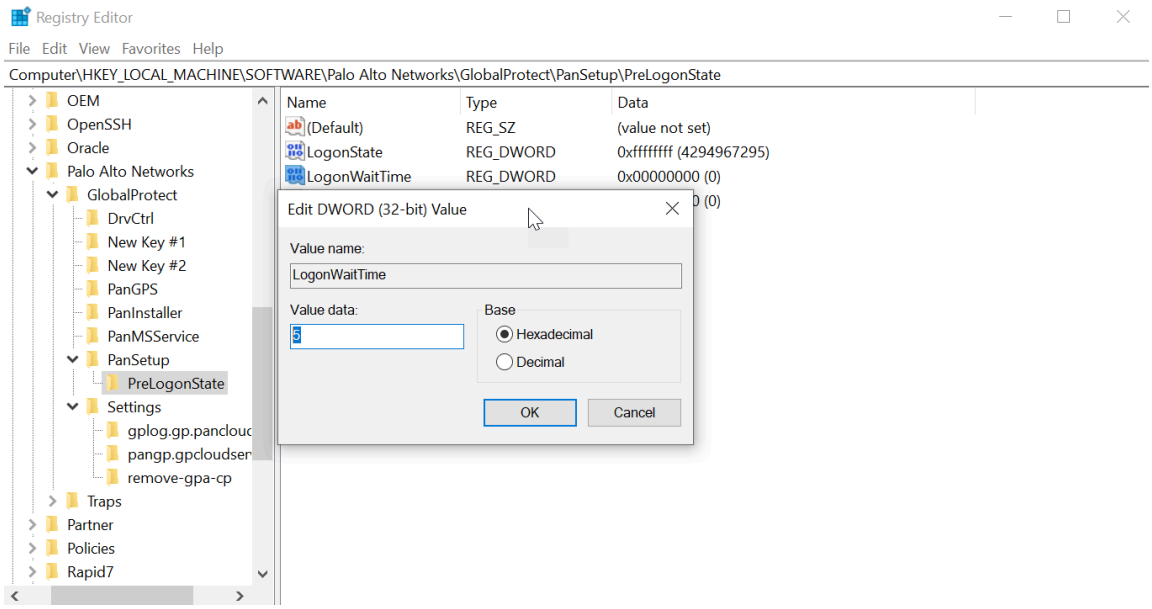
1. Retardez la demande de connexion Windows du fournisseur d'informations d'identification GlobalProtect.

L'établissement du tunnel GlobalProtect avant la connexion Windows peut être utile dans certaines situations. Par exemple, vous souhaiterez peut-être forcer l'appareil Windows à synchroniser les données avec Active Directory ou retarder la demande de connexion Windows du fournisseur d'informations d'identification GlobalProtect.

Vous pouvez configurer la durée (en secondes) pendant laquelle le fournisseur d'informations d'identification GlobalProtect attend que le tunnel soit établi avant de soumettre une demande de connexion Windows lorsque l'authentification unique (SSO) est activée. Par défaut, la prise en charge du fournisseur d'informations d'identification GlobalProtect pour retarder la connexion Windows avant d'établir la connexion tunnel est désactivée et le fournisseur d'informations d'identification GlobalProtect soumet les demandes de connexion sans délai.

1. À partir de la ligne de commande, entrez la commande **`regedit`** pour ouvrir l'Éditeur de registre Windows.
2. Dans le registre Windows, allez à`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`.
3. Cliquez avec le bouton droit sur **PreLogonState**, puis sélectionnez **New (nouveau)** > **DWORD (32-bit) Value Valeur NewDWORD (32 bits))**.
4. Cliquez avec le bouton droit sur **New Value #1 (Nouvelle valeur n°1)**, puis sélectionnez **Rename (Renommer)**.

   Saisissez la **LogonWaitTime (Durée d'attente de connexion à la session)**. Cliquez avec le bouton droit sur **LogonWaitTime (Durée d'attente de connexion à la session)**, puis sélectionnez **Modify (Modifier)**. Dans le champ **Value Data (Données de la valeur)**, définissez le nombre de secondes (la plage est de 5 à 30) pendant lesquelles les utilisateurs finaux doivent attendre pour se connecter à Windows avant d'établir une connexion tunnel. Cliquez sur **OK**.

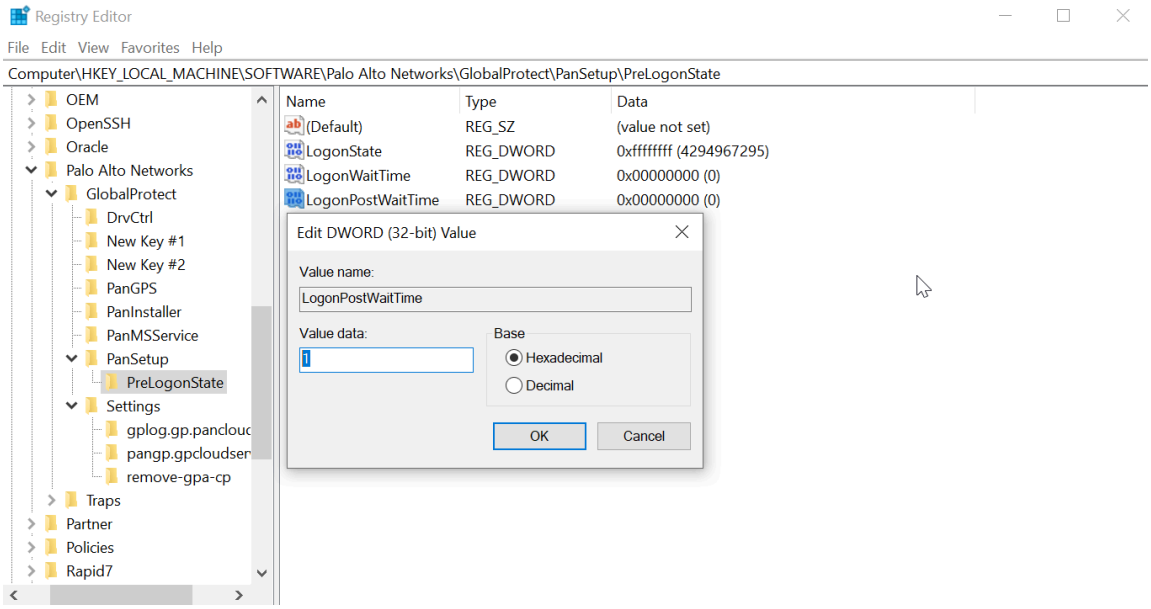


 ©2026 Palo Alto Networks, Inc.

5. Répétez les sous-étapes 1, 2 et 3 pour retarder le fournisseur d'informations d'identification GlobalProtect de soumettre la demande de connexion Windows une fois le tunnel établi.

   Saisissez **LogonPostWaitTime (Durée d'attente après la connexion à la session)**. Cliquez avec le bouton droit sur **LogonPostWaitTime (Durée d'attente après la connexion à la session)**, puis sélectionnez **Modify (Modifier)**. Dans le champ **Value data (Données de la valeur)**, définissez le nombre de secondes (la plage est de 3 à 10) que les utilisateurs finaux doivent attendre pour se connecter à Windows. Cliquez sur **OK**.

   *Vous devez d'abord entrer la durée (en secondes) pour **LogonWaitTime (Durée d'attente de connexion à la session)**, puis entrer la durée (en secondes) pour **LogonPostWaitTime (Durée d'attente après la connexion à la session)**.*



2. Appliquez le fournisseur d'informations d'identification GlobalProtect comme option de connexion par défaut pour Windows 10.

Lorsque GlobalProtect SSO est activé sur les appareils Windows, les utilisateurs peuvent avoir plus d'une option de connexion en plus d'utiliser les options du fournisseur d'informations d'identification GlobalProtect telles qu'une information d'identification tierce, une carte à puce, un code PIN Windows Hello, un mot de passe Windows Hello ou Windows Hello. Empreinte digitale. Les utilisateurs peuvent utiliser n'importe laquelle de ces options de connexion pour se connecter à leur appareil Windows et la définir comme option de connexion par défaut lors de la prochaine connexion Windows, rendant GlobalProtect SSO indisponible. Les utilisateurs doivent à nouveau basculer manuellement vers le fournisseur d'informations d'identification GlobalProtect pour activer GlobalProtect SSO. Lorsque le fournisseur d'informations d'identification GlobalProtect est activé comme option de connexion par défaut même lorsque les utilisateurs peuvent se connecter avec n'importe quelle autre option de connexion, l'option de connexion du fournisseur d'informations d'identification GlobalProtect est sélectionnée lors de la prochaine connexion Windows et pour les connexions suivantes.

Lorsque GlobalProtect est installé sur des périphériques Windows, les utilisateurs ne peuvent pas se connecter au périphérique en utilisant le nom d'utilisateur principal (UPN)

 ©2026 Palo Alto Networks, Inc.

*(par exemple, **username@domain**) lorsque le fournisseur d'informations d'identification GlobalProtect est sélectionné et que le périphérique est hors ligne.*

Suivez ces directives lorsque vous appliquez le fournisseur d'informations d'identification GlobalProtect comme option de signature par défaut sur les appareils Windows :

- *Lorsque l'application GlobalProtect est installée ou que l'authentification unique est activée, le fournisseur d'informations d'identification GlobalProtect est défini comme l'option de connexion par défaut pour tous les utilisateurs, même lorsque le paramètre **`MakeGPCPDefault`** est désactivé.*
- *Lorsque l'authentification unique est activée et que le paramètre **`MakeGPCPDefault`** est activé, les utilisateurs peuvent utiliser n'importe quelle option de connexion, telle qu'un fournisseur d'informations d'identification tiers, une carte à puce, un code PIN Windows Hello, un mot de passe Windows Hello ou une empreinte digitale Windows pour se connecter à leur appareil Windows. Quelle que soit l'option de connexion sélectionnée, le fournisseur d'informations d'identification GlobalProtect sera utilisé comme option de connexion par défaut lors de la prochaine connexion Windows.*
- *Lorsque l'authentification unique est activée et que le paramètre **`MakeGPCPDefault`** est désactivé ou vide, l'option de connexion sélectionnée par l'utilisateur sera utilisée par défaut lors de la prochaine connexion Windows.*
- *Lorsque l'authentification unique est désactivée, le fournisseur d'informations d'identification GlobalProtect n'est pas disponible. L'option de connexion par défaut de Windows fonctionnera comme prévu.*
- *La fonctionnalité Appliquer le fournisseur d'informations d'identification GlobalProtect en tant que connexion par défaut pour Windows 10 ne prend pas en charge l'option de connexion Autre utilisateur. Vous pouvez configurer l'option de connexion Autre utilisateur à l'aide de l'objet de stratégie de groupe (GPO) sur le périphérique Windows.*

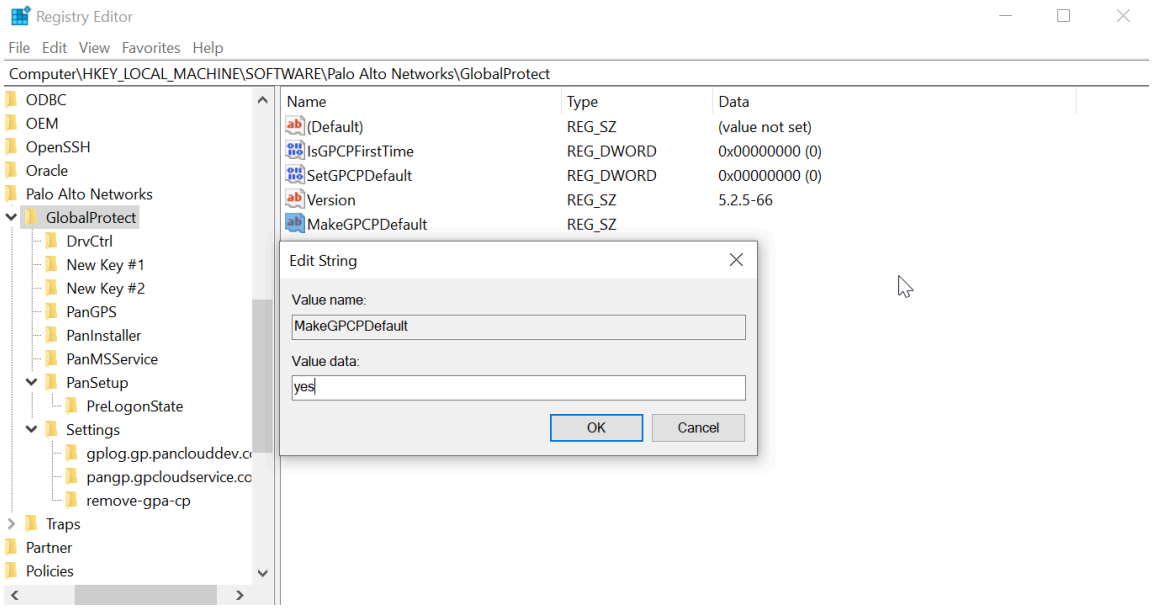
1. À partir de la ligne de commande, entrez la commande **`regedit`** pour ouvrir l'Éditeur de registre Windows.
2. Dans le registre Windows, accédez à :

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect
   ```
3. Cliquez avec le bouton droit sur le dossier **GlobalProtect**, puis sélectionnez **New (Nouveau)** > **String Value (valeur de la chaîne)** pour ajouter une nouvelle chaîne de valeur.
4. Entrez la valeur de chaîne **MakeGPCPDefault**. Cliquez avec le bouton droit sur **MakeGPCPDefault**, puis sélectionnez **Modify (Modifier)**.

   Dans le champ **Value data (Données de la valeur)**, saisissez **yes (oui)** pour permettre au fournisseur d'informations d'identification GlobalProtect d'être l'option de connexion par défaut lors de la prochaine connexion Windows. Si vous définissez les **Value data (données de la valeur)** sur **no (non)**, le paramètre **`MakeGPCPDefault`** est désactivé

 ©2026 Palo Alto Networks, Inc.

et l'option de connexion sélectionnée par l'utilisateur sera utilisée par défaut lors de la prochaine connexion Windows. Cliquez sur **OK**.



Englobement de l'ouverture de session unique pour les fournisseurs d'informations d'identification indépendantes sur les clients Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Sous les points de terminaison Windows 7, l'application GlobalProtect utilise le Framework de fournisseur d'informations d'identification Microsoft pour prendre en charge l'authentification unique (SSO). Avec SSO, le fournisseur d'accréditation GlobalProtect enveloppe le fournisseur natif authentique de Windows, ce qui permet à GlobalProtect d'utiliser les identifiants de connexion Windows pour s'authentifier automatiquement et se connecter au portail et à la passerelle GlobalProtect. De plus, l'englobement de l'ouverture de session unique permet aux utilisateurs de Windows 10 de mettre à jour leur mot de passe d'Active Directory (AD) au moyen du fournisseur d'informations d'identification GlobalProtect lorsque leur mot de passe expire ou lorsqu'un administrateur exige un changement de mot de passe à la prochaine ouverture de session.

Lorsque d'autres fournisseurs d'informations d'identification existent sur le point de terminaison, le fournisseur d'informations d'identification de GlobalProtect n'est pas en mesure de recueillir les informations d'identification de connexion Windows de l'utilisateur. Par conséquent, GlobalProtect ne parvient pas à se connecter automatiquement aux portails et à la passerelle GlobalProtect. Si l'ouverture de session unique échoue, vous pouvez identifier le fournisseur tiers d'informations d'identification, puis configurer l'application GlobalProtect pour envelopper ces informations d'identification tierces, ce qui permet aux utilisateurs d'authentifier avec succès Windows, GlobalProtect et le fournisseur d'informations d'identification tierce partie en utilisant uniquement leurs informations d'identification de connexion Windows.

 ©2026 Palo Alto Networks, Inc.

Facultativement, vous pouvez configurer Windows pour afficher des tuiles de connexion distinctes : une pour chaque fournisseur tiers d'informations d'identification et une autre pour la connexion native Windows . C'est utile lorsqu'un fournisseur tiers d'informations d'identification ajoute des fonctionnalités supplémentaires qui ne s'appliquent pas à GlobalProtect.

> *Si vous voulez supprimer le fournisseur d'informations d'identification de GlobalProtect de votre point de terminaison Windows, exécutez la commande* ***`GlobalProtectPanGPS.exe -u`*** *dans l'invite de commande.*

Utilisez le registre Windows ou le programme d'installation Windows (`msiexec`) pour permettre à GlobalProtect d'englober les informations d'identification indépendantes :

- Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le registre Windows
- Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le programme d'installation Windows

L'englobement d'ouverture de session unique GlobalProtect pour les informations d'identification indépendantes dépend des paramètres du fournisseur tiers d'informations d'identification. Dans certains cas, l'englobement d'ouverture de session unique GlobalProtect pourrait ne pas fonctionner correctement si la mise en œuvre du fournisseur tiers d'informations d'identification ne permet pas à GlobalProtect d'enrouler avec succès le fournisseur d'informations d'identification.

Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le registre Windows

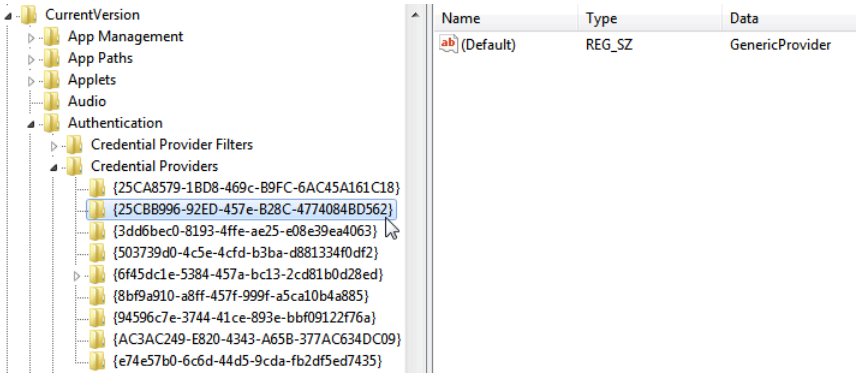
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Utilisez les étapes suivantes dans le registre Windows pour permettre à SSO d'enrouler les informations d'identification tierces sur les points de terminaison Windows.

 ©2026 Palo Alto Networks, Inc.

1. Ouvrez le registre Windows et localisez l'identificateur globalement unique (GUID) pour le fournisseur d'informations d'identification tiers que vous voulez envelopper.
   1. À partir de la ligne de commande, entrez la commande **`regedit`** pour ouvrir l'Éditeur de registre Windows.
   2. Accédez à l'emplacement du registre Windows suivant pour afficher la liste des fournisseurs d'accréditation actuellement installés :

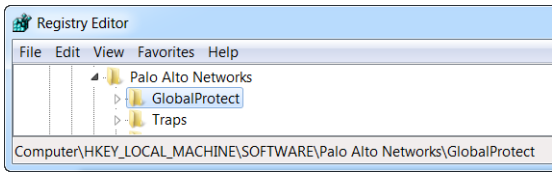
      `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers.`
   3. Copiez la clé GUID pour le fournisseur d'accréditation que vous désirez envelopper (y compris les accolades - {et} - à la fin du GUID) :



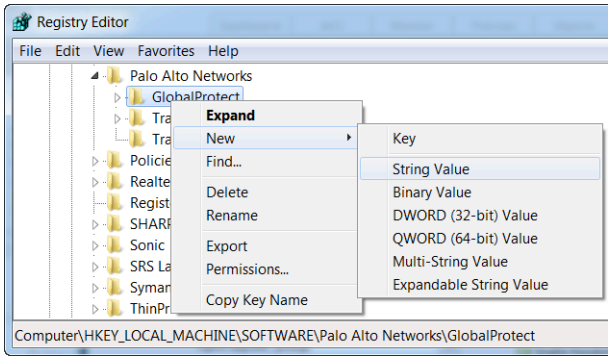
 ©2026 Palo Alto Networks, Inc.

2. Activez l'englobement d'ouverture de session unique pour les fournisseurs d'informations d'identification tiers en ajoutant le paramètre **`wrap-cp-guid`** au registre GlobalProtect.
   1. Accédez à l'emplacement du registre Windows suivant :

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\ GlobalProtect:
      ```

   2. Cliquez avec le bouton droit sur le dossier **GlobalProtect**, puis sélectionnez **New (Nouvelle)** > **String Value (Chaîne de valeur)** pour ajouter une nouvelle chaîne de valeur :

   3. Configurez les champs de la **String Value (Chaîne de valeur)** suivants :
      - **Name (Nom)** : **`wrap-cp-guid`**
      - **Value Data (Données de valeur)** :{<**`GUID de fournisseur d'informations d'identification indépendantes`**>}

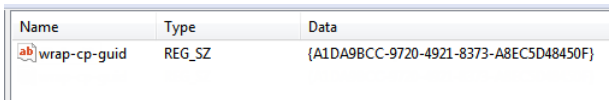
        *Pour le champ **Value Data (Données de valeur)**, la valeur de GUID que vous saisissez doit être entre accolades : { et }.*

        Voici un exemple de ce qu'un GUID du fournisseur tiers d'informations d'identification dans le champ de **Value Data (Données de valeur)** pourrait ressembler :

        ```
        {A1DA9BCC-9720-4921-8373-A8EC5D48450F}
        ```

 ©2026 Palo Alto Networks, Inc.

Pour la nouvelle **String Value (Valeur de chaîne)**, `wrap-cp-guid` s'affiche en tant que **Name (Nom)** de la valeur de chaîne et le GUID s'affiche en tant que **Value Data (Données de valeur)**.

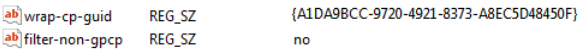


3. Étapes suivantes :

- Avec cette configuration, la mosaïque d'ouverture de session Windows native est affichée pour les utilisateurs à l'écran de connexion. Lorsque les utilisateurs cliquent sur le carreau et se connectent au système avec leurs informations d'identification de Windows, cette authentification unique authentifie les utilisateurs dans Windows, GlobalProtect et le fournisseur tiers d'informations d'identification.
- (Facultatif) Si vous souhaitez afficher plusieurs tuiles à l'écran de connexion (par exemple, la mosaïque native de Windows et la mosaïque du tiers fournisseur d'informations d'identification), passez à l'étape 4.
- (Facultatif) Si vous souhaitez affecter un fournisseur d'informations d'identification par défaut aux utilisateurs, passez à l'étape 5.
- (Facultatif) Si vous souhaitez masque la mosaïque d'un fournisseur tiers d'informations d'identification à partir de l'écran de connexion, passez à l'étape 6.

4. (Facultatif) Autorisez la présentation de la fenêtre du tiers fournisseur d'informations d'identification indépendantes aux utilisateurs à l'ouverture de session.

Ajoutez une deuxième **String Value (Valeur de chaîne)** avec le **Name (Nom)** **`filter-non-gpcp`** et entrez **`no`** pour la **Value data (Donnée de valeur)** de la chaîne :



Après avor ajouter cette valeur de chaîne aux paramètres de GlobalProtect, deux options d'ouverture de session sont présentées aux utilisateurs à l'écran de connexion Windows : la fenêtre Windows native et la fenêtre du fournisseur d'informations d'identification indépendantes.

 ©2026 Palo Alto Networks, Inc.

5. Affectez un fournisseur d'informations d'identificationpar défaut pour la connexion de l'utilisateur.
   1. Ouvrez le registre Windows afin de localiser l'identificateur globalement unique (GUID) pour le fournisseur d'informations d'identification tiers que vous voulez affecter en tant que fournisseur d'informations d'identification par défaut.
      1. À partir de la ligne de commande, entrez la commande `regedit` pour ouvrir l'Éditeur de registre Windows.
      2. Accédez à l'emplacement du registre Windows suivant pour afficher la liste des fournisseurs d'accréditation actuellement installés :

         `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers.`
      3. Copiez la clé GUID complète pour le fournisseur d'accréditation (y compris les accolades - {et} - à la fin du GUID) :
   2. Ouvrez l'Éditeur de politique de groupe local pour autoriser et affecter un fournisseur d'informations d'identification par défaut.
      1. À partir de la ligne de commande, entrez la commande `gpedit.msc` pour ouvrir l'Éditeur de politique de groupe local.
      2. Sélectionnez **Computer Configuration (Configuration de l'ordinateur)** > **Administrative Templates (Modèles administratifs)** > **System (Système)** > **Logon (Connexion)**.
      3. Sous **Setting (Paramètre)**, double-cliquez sur **Assign a default credential provider (Affecter un fournisseur d'informations d'identification par défaut)** pour ouvrir la fenêtre **Assign a default credential provider (Affecter un fournisseur d'informations d'identification par défaut)**.
      4. Définissez la politique sur **Enabled (Activé)**.
      5. Sous **Assign the following credential provider as the default credential provider (Affecter le fournisseur d'informations d'identification suivant en tant que fournisseur d'informations d'identification par défaut)**, entrez le GUID du fournisseur d'informations d'identification (copié du registre Windows).
      6. Cliquez sur **Apply (Appliquer)**, puis sur **OK** pour enregistrer vos modifications.

 ©2026 Palo Alto Networks, Inc.

6. (Facultatif) Masquez une mosaïque d'un fournisseur d'informations d'identification à l'écran de connexion Windows.
   1. Ouvrez le registre Windows pour localiser l'identificateur globalement unique (GUID) pour le fournisseur d'informations d'identification tiers que vous voulez masquer.
      1. À partir de la ligne de commande, entrez la commande `regedit` pour ouvrir l'Éditeur de registre Windows.
      2. Accédez à l'emplacement du registre Windows suivant pour afficher la liste des fournisseurs d'accréditation actuellement installés :

         ```
         HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion
         \Authentication\Credential Providers.
         ```
      3. Copiez la clé GUID complète pour le fournisseur d'accréditation que vous désirez masquer (y compris les accolades - {et} - à la fin du GUID).
   2. Ouvrez l'Éditeur de politique de groupe local pour masquer le fournisseur d'informations d'identification.
      1. À partir de la ligne de commande, entrez la commande `gpedit.msc` pour ouvrir l'Éditeur de politique de groupe local.
      2. Sélectionnez **Computer Configuration (Configuration de l'ordinateur)** > **Administrative Templates (Modèles administratifs)** > **System (Système)** > **Logon (Connexion)**.
      3. Sous **Setting (Paramètre)**, double-cliquez sur **Exclude credential providers (Exclure les fournisseurs d'informations d'identification)** pour ouvrir la fenêtre **Exclude credential providers (Exclure les fournisseurs d'informations d'identification)**.
      4. Définissez la politique sur **Enabled (Activé)**.
      5. Sous **Exclude the following credential providers (Exclure les fournisseurs d'informations d'identification suivants)**, saisissez le GUID du fournisseur d'informations d'identification que vous souhaitez masquer (copié du registre Windows).

         Pour masquer plusieurs fournisseurs d'informations d'identification, séparez chaque GUID au moyen d'une virgule.
      6. Cliquez sur **Apply (Appliquer)**, puis sur **OK** pour enregistrer vos modifications.

7. Finalisez vos changements.

   Une fois vos changements finalisés, redémarrez votre système pour que les changements prennent effet.

Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le programme d'installation Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

 ©2026 Palo Alto Networks, Inc.

Utilisez les étapes suivantes dans le programme d'installation Windows (Msiexec) pour permettre à l'ouverture de session unique d'englober les fournisseurs d'informations d'identification indépendantes sur les points de terminaison Windows 7.

Enroulez les informations d'identification tierces et affichez la mosaïque native aux utilisateurs lors de la connexion. Les utilisateurs peuvent cliquer sur la mosaïque pour se connecter au point de terminaison au moyen de leurs informations d'identification Windows natives. Grâce à cette ouverture de session unique, les utilisateurs peuvent d'authentifier sur Windows, sur GlobalProtect et sur le fournisseur d'informations d'identification indépendantes.

Utilisez la syntaxe suivante dans le programme d'installation Windows (Msiexec) :

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID=”{guid_value}”
 FILTERNONGPCP=”yes”
```

Dans la syntaxe ci-dessus, le paramètre **FILTERNONGPCP** simplifie l'authentification pour l'utilisateur en filtrant l'option d'ouverture de session sur le système à l'aide des informations d'identification tierces.

Si vous souhaitez permettre aux utilisateurs de se connecter au moyen des informations d'identification indépendantes, utilisez la syntaxe suivante dans le programme d'installation Windows (Msiexec) :

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID=”{guid_value}”
 FILTERNONGPCP=”no”
```

Dans la syntaxe ci-dessus, le paramètre **FILTERNONGPCP** est défini sur **“no”**, ce qui filtre la tuile d'ouverture de session des fournisseurs d'informations d'identification tiers, de sorte que seule la mosaïque native s'affiche. Dans ce cas, la mosaïque native de Windows et celle des fournisseurs d'informations d'identification tierces s'affichent aux utilisateurs lors de la connexion au point de terminaison Windows.

Déployer les paramètres d'application sur des points de terminaison MacOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Utilisez le fichier plist MacOS global (liste de propriétés) pour définir les paramètres de personnalisation de l'application GlobalProtect ou pour déployer les scripts sur les points de terminaison MacOS.

- Paramètres de l'application
- Scripts

 ©2026 Palo Alto Networks, Inc.

Déployer les paramètres d'application dans la Plist MacOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Vous pouvez définir les paramètres de personnalisation de l'application GlobalProtect dans le fichier plist MacOS global (liste de propriétés). Cela permet de déployer des paramètres d'application GlobalProtect sur des points de terminaison MacOS avant leur première connexion au portail GlobalProtect.

Sur les points de terminaison MacOS, les fichiers plist se trouvent dans `/Library/Preferences` ou dans `~/Library/Preferences`. Le tilde (~) indique que l'emplacement se trouve dans le dossier racine de l'utilisateur actuel. L'application GlobalProtect sur un point de terminaison MacOS vérifie tout d'abord les paramètres de plist GlobalProtect. Si la plist n'existe pas à cet emplacement, l'application GlobalProtect recherche les paramètres plist dans `~/Library/Preferences`.

Outre l'utilisation de la plist MacOS pour déployer les paramètres de l'application GlobalProtect, vous pouvez autoriser l'application GlobalProtect à collecter des informations de plist MacOS spécifiques auprès des points de terminaison. Vous pouvez ensuite surveiller les données et les ajouter à une règle de sécurité pour les utiliser en tant que critères de correspondance. Le trafic du point de terminaison correspondant aux paramètres de registre que vous définissez peut être mis en œuvre conformément à la règle de sécurité. En outre, vous pouvez configurer des vérifications personnalisées pour recueillir des données d'application et de traitement des points de terminaison.

1. Ouvrez le fichier plist GlobalProtect et recherchez les paramètres de personnalisation de l'application GlobalProtect.

   Utilisez Xcode ou un éditeur de plist alternatif pour ouvrir le fichier plist :

   ```
   /Library/Preferences/
   com.paloaltonetworks.GlobalProtect.settings.plist
   ```

   Ensuite, allez à :

   ```
   /Palo Alto Networks/GlobalProtect/Settings
   ```

   Si le dictionnaire `Settings` n'existe pas, créez-le. Ajoutez chaque clé au dictionnaire `Settings` en tant que chaîne.

2. Définissez le nom du portail.

   Si vous ne souhaitez pas que l'utilisateur final puisse saisir manuellement l'adresse du portail même pour la première connexion, vous pouvez pré-déployer l'adresse du portail via la plist. Dans le dictionnaire `PanSetup`, configurez une entrée correspondant à `Portal`.

3. Déployez divers paramètres au point de terminaison macOS, y compris la méthode de connexion utilisée pour l'application GlobalProtect.

   Consultez Paramètres d'application personnalisables. pour obtenir la liste complète des clés et des valeurs que vous pouvez configurer à l'aide du fichier plist macOS.

 ©2026 Palo Alto Networks, Inc.

4. (Facultatif) Si vous utilisez des extensions système et que vous devez passer aux extensions de noyau, définissez la valeur de **clé** sur **UseKextAnyway** dans la plist macOS (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) pour l'application GlobalProtect.

   Suivez ces instructions lorsque vous utilisez des extensions système et que vous devez passer aux extensions du noyau :

   - *Après avoir activé les extensions système, vous devez d'abord désinstaller l'application existante pour utiliser la clé plist **UseKextAnyway** afin d'activer les extensions du noyau sur macOS.*
   - *Vous avez ensuite la possibilité de revenir en arrière pour utiliser des extensions système. Vous devez supprimer la clé plist **UseKextAnyway** dans la plist macOS. Après avoir supprimé cette clé plist, vous devez redémarrer l'application GobalProtect pour que la modification prenne effet.*
   - *En passant aux extensions du noyau, vous ne pouvez plus utiliser les fonctionnalités Split DNS et Appliquer les connexions GlobalProtect avec les exclusions FQDN.*
   - *Si vous avez configuré des paramètres de tunnel fractionné en fonction de l'application sur des points de terminaison MacOS, tout le trafic basé sur Safari, le trafic Microsoft Teams ou le trafic Slack définis dans la configuration du tunnel fractionné sont supprimés. Nous vous recommandons d'utiliser Chrome au lieu de Safari afin que le trafic défini dans la configuration du tunnel fractionné ne soit pas supprimé. Tout le trafic créé sur la base de l'infrastructure WebKit tel que Safari, Microsoft Teams ou Slack peut avoir des problèmes lors de l'utilisation des extensions du noyau.*

   Vous devez spécifier **UseKextAnyway** comme clé plist avant d'installer l'application GlobalProtect 5.2.6 ou versions ultérieures ou de procéder à la mise à niveau d'une version antérieure vers l'application GlobalProtect 5.2.6 ou versions ultérieures exécutant Catalina 10.15.4 ou version ultérieure. Toutefois, si vous effectuez une mise à niveau à partir d'une version antérieure vers l'application GlobalProtect 5.2.6 ou des versions ultérieures exécutant macOS Big Sur 11 ou version ultérieure, vous devez activer les extensions système.

Déployer des scripts à l'aide de la Plist MacOS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

La première fois qu'un utilisateur se connecte à la passerelle GlobalProtect, l'application GlobalProtect télécharge le fichier de configuration et stocke les paramètres de l'application dans un fichier de propriétés MacOS (plist) GlobalProtect. En plus de vous servir de la plist Mac pour modifier les paramètres de l'application, vous l'utilisez pour déployer des scripts lorsque l'un ou l'autre des événements suivants survient : avant et après l'établissement du tunnel et avant la déconnexion du tunnel. Servez-vous du flux de travail suivant pour utiliser la plist pour déployer des scripts sur les points de terminaison MacOS.

Les paramètres de la plist MacOS qui vous permettent de déployer des scripts sont pris en charge sur les points de terminaison fonctionnant avec l'application GlobalProtect 2.3 ou une version ultérieure.

 ©2026 Palo Alto Networks, Inc.

1. (Points de terminaison sous Mac OS X 10.9 ou une version ultérieure) Videz la mémoire cache des paramètres. Cela empêche le système d'exploitation d'utiliser les préférences mises en cache après avoir apporté des modifications à la plist.

   Pour supprimer les préférences par défaut mises en cache, exécutez la commande **`killall cfprefsd`** à partir d'un terminal macOS.

2. Ouvrez le fichier de plist GlobalProtect et recherchez ou créez le dictionnaire GlobalProtect associé à l'événement de connexion ou de déconnexion. Le dictionnaire sous lequel vous ajouterez les paramètres détermine le moment où l'application GlobalProtect exécutera le(s) script(s).

   Utilisez Xcode ou un autre éditeur de fichiers plist pour ouvrir le fichier plist (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`) et accédez à l'un des emplacements de dictionnaire suivants :

   - `/PaloAlto Networks/GlobalProtect/Settings/pre-vpn-connect`
   - `/Palo Alto Networks/GlobalProtect/Settings/post-vpn-connect`
   - `/Palo Alto Networks/GlobalProtect/Settings/pre-vpn-disconnect`

     Si le dictionnaire `Settings` n'existe pas, créez-le. Puis, dans `Paramètres`, créez un nouveau dictionnaire correspondant à l'événement ou aux événements pour lesquels vous souhaitez exécuter les scripts.

3. Permettez à l'application GlobalProtect d'exécuter des scripts en créant une nouvelle `String` nommée **`command`**.

   La valeur indiquée ici devrait faire référence au script shell (et aux paramètres à transmettre au script) que vous souhaitez exécuter sur vos points de terminaison.

   Si la chaîne `command` n'existe pas encore, ajoutez-la au dictionnaire et indiquez le script et les paramètres dans le champ **Value (Valeur)**. Par exemple :

   ```
   $HOME/pre_vpn_connect.sh /Users/username username
   ```

   Les variables d'environnement sont prises en charge.

   Il est recommandé d'indiquer le chemin d'accès complet dans les commandes.

4. (Facultatif) Ajoutez les paramètres supplémentaires liés à la commande, y compris les privilèges d'administrateur, une valeur de délai pour le script, une valeur de somme de contrôle pour le fichier batch et un message d'erreur à afficher si l'exécution de la commande échoue.

   Créez ou modifiez d'autres chaînes dans la plist (`context`, `timeout`, `file`, `checksum` et/ou `error-msg`) et saisissez les valeurs correspondantes. Pour plus d'informations, consultez Paramètres d'application personnalisables.

5. Enregistrez les modifications apportées au fichier de plist.

   Enregistrez la plist.

 ©2026 Palo Alto Networks, Inc.

Déployer les paramètres de l'application sur les points de terminaison Linux

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Vous pouvez définir les paramètres de personnalisation de l'application GlobalProtect dans le fichier de configuration de pré-déploiement (`pangps.xml`). Cela permet de déployer des paramètres d'application GlobalProtect sur des points de terminaison Linux avant leur première connexion au portail GlobalProtect.

Sur les points de terminaison Linux, le fichier de configuration de pré-déploiement (`pangps.xml`) se trouve dans `/opt/paloaltonetworks/globalprotect`.

Le tableau suivant répertorie les paramètres de prédéploiement pour les points de terminaison Linux que vous pouvez ajouter au fichier `pangps.xml` pour personnaliser le comportement de l'application GlobalProtect et la façon dont l'utilisateur interagit avec l'application GlobalProtect.

Configuration de l'agent du portail	Linux	Par défaut
Méthode de connexion	**connect-method on-demand | user-logon (connexion-méthode à la demande | ouverture de session utilisateur)**	**user-logon**
Permettre à l'Utilisateur de modifier l'Adresse du portail	**Peut-il changer le portail oui | non**	**yes**
Permettre à l'utilisateur de continuer avec un certificat de serveur de portail invalide	**can-continue-if-portal-cert-invalid yes | no**	**yes**
Utiliser le navigateur par défaut pour l'authentification SAML	**default-browser yes | no (navigateur par défaut oui | non)**	**no**
Délai d'expiration de connexion au portail (sec.)	**portal-timeout (portail-expirationdélai) <portaltimeout>**	**5**
Délai d'expiration de connexion TCP (sec.)	**connect-timeout (connexion_expiratiodélai) <connect-timeout>**	**5**

 ©2026 Palo Alto Networks, Inc.

Configuration de l'agent du portail	Linux	Par défaut
Délai d'expiration de réception TCP (sec)	**receive-timeout (recevoir-expirationdélai)** <**receive-timeout**>	**30**
Pas sur le portail Ce paramètre est utilisé pour pré-déployer l'indicateur de vérification complète de la chaîne de certificats.	**full-chain-cert-verify** <**Settings**> **<full-chain-cert-verify>yes</full-chain-cert-verify>** **</Settings>**	S. O.
Pas sur le portail Ce paramètre indique l'adresse IP du portail par défaut (ou le nom d'hôte).	**Portal (Portail)**<**IPaddress**>	S. O.

Si vous avez déjà installé l'application GlobalProtect sur le point de terminaison Linux, suivez ces instructions :

1. *Modifiez le paramètre de prédéploiement que vous souhaitez modifier pour le fichier* `pangps.xml` *dans* `/opt/paloaltonetworks/globalprotect`.
2. *Redémarrez le point de terminaison Linux pour que les modifications de configuration de pré-déploiement prennent effet.*

Si vous installez l'application GlobalProtect pour la première fois, suivez ces instructions pour déployer divers paramètres sur le point de terminaison Linux.

1. Créez le fichier de configuration de prédéploiement `/opt/paloaltonetworks/globalprotect.xml`.
2. Ajoutez les paramètres de prédéploiement au fichier `pangps.xml`, y compris la méthode de connexion pour l'application GlobalProtect et le navigateur par défaut pour l'authentification SAML.

L'exemple suivant illustre la configuration XML des modifications de prédéploiement que vous avez déployées sur le point de terminaison Linux, y compris l'adresse IP du portail (ou le nom d'hôte) sous `<PanSetup>`.

```
<?xml version="1.0" encoding="UTF-8"?> <GlobalProtect>
       <Settings>           <connect-method>on-demand</connect-
method>           <can-continue-if-portal-cert-invalid>yes</
can-continue-if-portal-cert-invalid>           <can-change-
portal>no</can-change-portal>           <portal-timeout>100</
portal-timeout>           <connect-timeout>100</connect-
timeout>           <receive-timeout>100</receive-timeout>
```

 ©2026 Palo Alto Networks, Inc.

```
            <default-browser>yes</default-browser>       </Settings>
        <PanSetup>            <Portal>portal.acme.com</Portal>
        </PanSetup>       <PanGPS>       </PanGPS> </GlobalProtect>
```

3. Install the GlobalProtect app for Linux (Installez l'application GlobalProtect pour Linux.

Version CLI compatible avec distributeurs multiples de GlobalProtect pour Linux pour les distributeurs basés sur RPM et Debian

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect Application GlobalProtect 6.2.6 ou versions ultérieures Terminaux exécutant des distributeurs Linux basés sur RPM et Debian qui utilisent systemd comme ungestionnaire de système et de service.

Cette fonctionnalité offre aux utilisateurs Linux une expérience transparente de l'installation et de l'utilisation de GlobalProtect sur un plus large éventail de distributions Linux basées sur RPM et Debian. Cette flexibilité accrue permet aux utilisateurs Linux d'utiliser efficacement GlobalProtect sur différentes distributions qui peuvent ne pas avoir de support officiel, tout en permettant aux administrateurs de protéger rapidement les actifs importants.

La fonctionnalité de CLI compatible avec distributeurs multiples de GlobalProtect pour Linux pour RPM et de la fonctionnalité de distribution basée sur Debian est prise en charge sur les terminaux Linux exécutés sur GlobalProtect version 6.2.6 et ultérieure.

 ©2026 Palo Alto Networks, Inc.

Processus GlobalProtect à mettre sur liste blanche dans les déploiements EDR

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence de passerelle GlobalProtect

Pour garantir le bon fonctionnement de GlobalProtect, nous vous suggérons de configurer votre antivirus, EDR (Détection et réponse des terminaux) ou vos applications de pare-feu pour reconnaître les processus GlobalProtect comme sécurisés. Ces applications de sécurité peuvent parfois identifier à tort les processus GlobalProtect comme malveillants. Pour éviter cela, il est conseillé de mettre sur liste blanche ou de créer des exceptions de sécurité pour les processus GlobalProtect suivants avant l'installation.

Voici les processus GlobalProtect que vous devez mettre sur liste blanche dans vos déploiements EDR.

Processus macOS
`/Library/SystemExtensions/[UUID]/com.paloaltonetworks.GlobalProtect.client.extension.systemextension/Contents/MacOS/com.paloaltonetworks.GlobalProtect.client.extension`
`/Applications/GlobalProtect.app/Contents/Resources/PanGPS`
`/Applications/GlobalProtect.app/Contents/Resources/PanGpHip`
`/Applications/GlobalProtect.app/Contents/Resources/PanGpHipMp`
`/Applications/GlobalProtect.app/Contents/MacOS/GlobalProtect`
`/Applications/GlobalProtect.app/Contents/Resources/gp_support.sh`
`/Applications/GlobalProtect.app/Contents/Resources/systemext_gp.sh`
`/Applications/GlobalProtect.app/Contents/Resources/uninstall_gp.sh`
`/Applications/GlobalProtect.app/Contents/Resources/gplogin.bundle/Contents/MacOS/gplogin`

Processus Windows
`C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPA.exe`
`C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPS.exe`

 ©2026 Palo Alto Networks, Inc.

Processus Windows
C:\Program Files\Palo Alto Networks\GlobalProtect\PanGpHip.exe
C:\Program Files\Palo Alto Networks\GlobalProtect\PanGpHipMp.exe
C:\Program Files\Palo Alto Networks\GlobalProtect \wa_3rd_party_host_32.exe
C:\Program Files\Palo Alto Networks\GlobalProtect \wa_3rd_party_host_64.exe
C:\Program Files\Palo Alto Networks\GlobalProtect \PanVcrediChecker.exe
C:\Program Files\Palo Alto Networks\GlobalProtect\PanGPSupport.exe
C:\Windows\System32\PanPlapApp.exe

 ©2026 Palo Alto Networks, Inc.

VPN sans client GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

VPN sans client GlobalProtect offre un accès à distance sécurisé pour les applications Web d'entreprise courantes. Les utilisateurs ont l'avantage de profiter d'un accès sécurisé à partir de navigateurs Web sur lesquels SSL est activé sans installer le logiciel GlobalProtect. Cela s'avère utile lorsque vous devez activer l'accès à ces applications pour des partenaires ou des entrepreneurs ou que vous devez activer de manière sécurisée les ressources non gérées, y compris les points de terminaison personnels. Vous pouvez configurer la page d'accueil du portail GlobalProtect pour fournir un accès aux applications Web en fonction des utilisateurs et des groupes d'utilisateurs, et également autoriser l'authentification unique aux applications compatibles SAML.

Le VPN sans client fonctionne comme un proxy inverse qui modifie les pages web renvoyées par les applications web publiées. Il présente une version réécrite de ces pages aux utilisateurs distants. Lorsque les utilisateurs accèdent à ces URL, leurs demandes sont acheminées via le portail GlobalProtect. Ce qui conduit aux éléments suivants :

1. La protection généralement fournie par la politique de même origine ne s'applique pas aux pages accessibles via le VPN sans client, car le navigateur traite toutes les pages comme si elles provenaient de la même origine, indépendamment de leur origine réelle.
2. Le processus de réécriture de page peut entraîner un comportement différent de celui prévu pour JavaScript.

Par conséquent, si un utilisateur visite un site web compromis ou clique sur un lien d'hameçonnage, un attaquant distant pourrait potentiellement obtenir des jetons de session VPN et lire ou modifier le contenu (y compris les cookies, les scripts ou le code HTML) de tout site accessible via le VPN SSL sans client. Cela contourne effectivement les restrictions de la politique de même origine dans tous les navigateurs.

Par conséquent, la fonctionnalité VPN sans client ne garantit qu'un accès distant sécurisé à une seule application de confiance. Étant donné que la politique de même origine n'est pas appliquée, nous recommandons fortement de configurer l'accès uniquement à une page de confiance via le VPN sans client. Le VPN sans client ne doit jamais être utilisé pour accéder à plusieurs sites web différents sur Internet ou l'intranet. Si vous devez accéder à des sites web non fiables, utilisez Prisma Access Browser à la place.

Aperçu du VPN sans client

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Il est fortement recommandé d'accéder uniquement à des pages de confiance via le VPN sans client. Pour plus d'informations, consultez VPN sans client GlobalProtect.

Lorsque vous configurez VPN sans client GlobalProtect, les utilisateurs distants peuvent se connecter au portail GlobalProtect à l'aide d'un navigateur Web et lancer les applications Web que vous publiez pour les utilisateurs. En fonction des utilisateurs ou des groupes d'utilisateurs, vous pouvez autoriser les utilisateurs à accéder à un ensemble d'applications que vous mettez à leur disposition ou leur permettre d'accéder à des applications d'entreprise supplémentaires en entrant une URL d'application personnalisée.

> *Le VPN sans client n'est pas pris en charge sur les pare-feu avec plusieurs systèmes virtuels si le trafic VPN sans client doit traverser plusieurs systèmes virtuels.*

Une fois connectés au portail, les utilisateurs voient une page d'applications publiées présentant la liste des applications Web qu'ils peuvent lancer. Vous pouvez utiliser la page d'accueil des applications par défaut sur le portail GlobalProtect ou créer une page d'accueil personnalisée pour votre entreprise.

 ©2026 Palo Alto Networks, Inc.

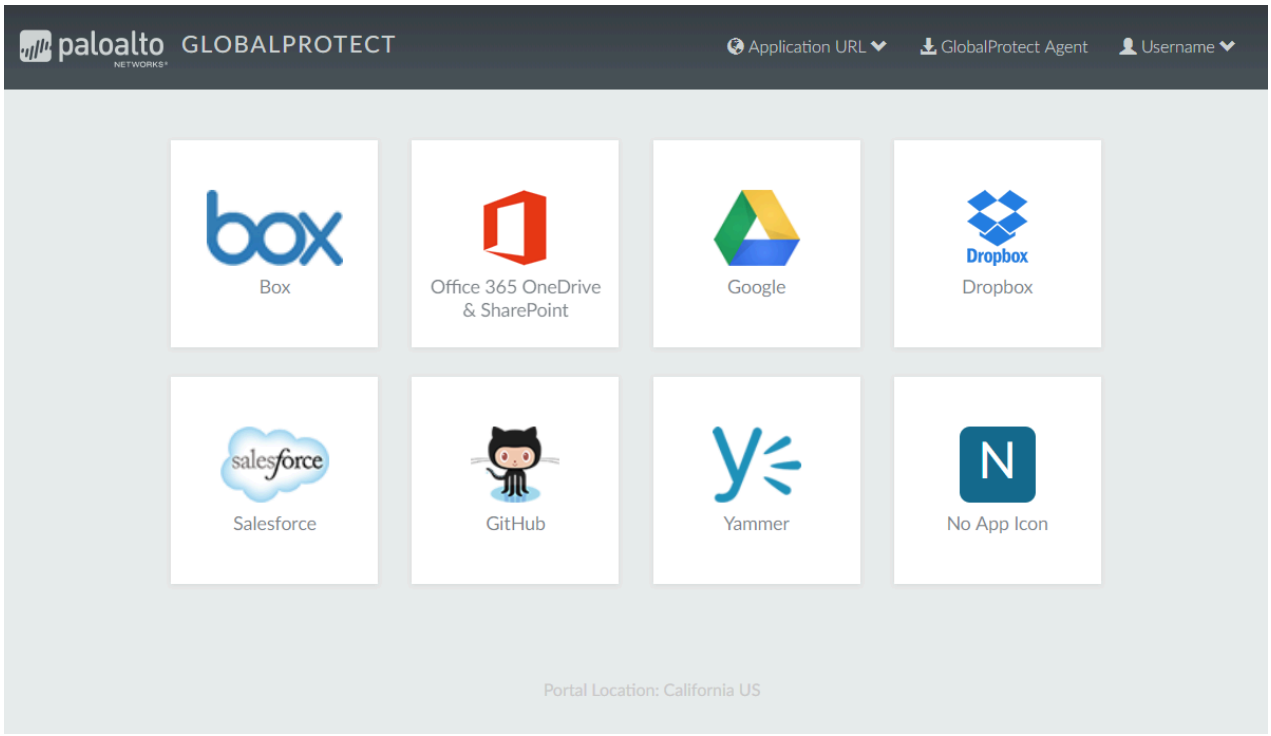


Illustration 3 : Page d'accueil des applications pour VPN sans client

Étant donné que cette page remplace la page d'accueil du portail par défaut, elle inclut un lien vers la page de téléchargement de l'application GlobalProtect. Si elle est configurée, les utilisateurs peuvent également sélectionner **Application URL (URL de l'application)** et entrez des URL pour lancer d'autres applications Web d'entreprise non publiées.

Lorsque vous ne configurez qu'une seule application Web (et désactivez l'accès aux applications non publiées), l'application se lance automatiquement dès que l'utilisateur se connecte, au lieu de rediriger l'utilisateur vers la page des applications publiées. Si vous ne configurez pas VPN sans

 ©2026 Palo Alto Networks, Inc.

client GlobalProtect, les utilisateurs verront la page de téléchargement du logiciel de l'application lors de la connexion au portail.

Lorsque vous configurez VPN sans client GlobalProtect, vous avez besoin de politiques de sécurité pour autoriser le trafic provenant des points de terminaison GlobalProtect vers la zone de sécurité associée au portail GlobalProtect qui héberge la page d'accueil des applications publiées et de politiques de sécurité pour autoriser le trafic utilisateur depuis la zone du portail GlobalProtect vers la zone de sécurité où sont hébergés les serveurs d'applications publiées. Les politiques de sécurité que vous définissez contrôlent les utilisateurs autorisés à utiliser chaque application publiée.

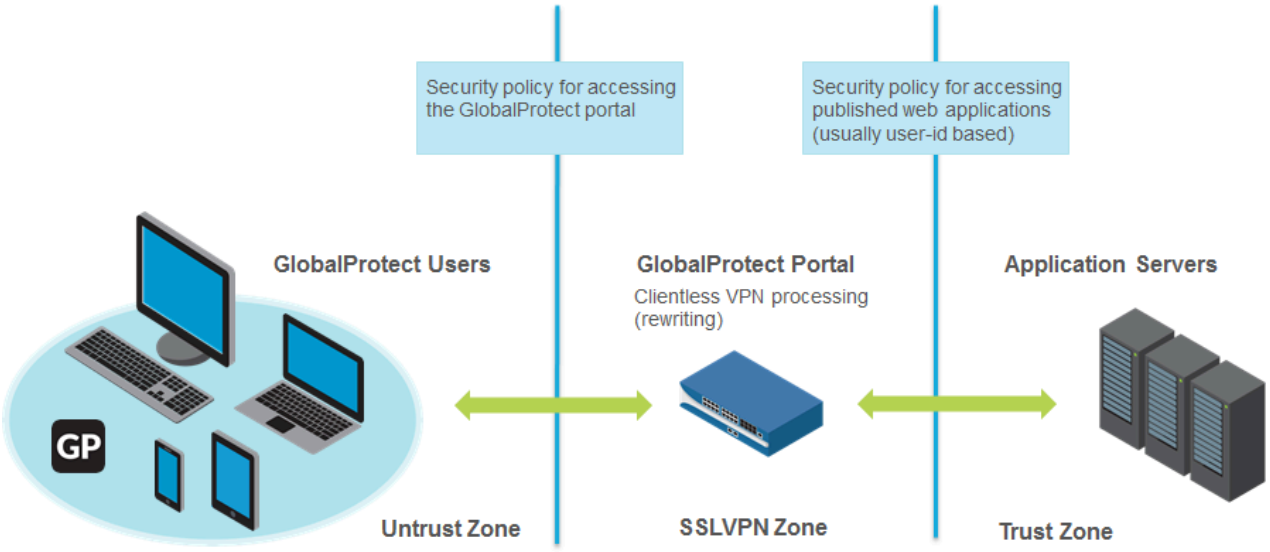


Illustration 4 : Zones et politique de sécurité pour VPN sans client

 ©2026 Palo Alto Networks, Inc.

Technologies prises en charge

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez configurer le portail GlobalProtect pour fournir un accès distant sécurisé aux applications Web d'entreprise communes. Pour obtenir de meilleurs résultats, assurez-vous de tester vos applications VPN sans client dans un environnement contrôlé avant de les déployer ou de les mettre à la disposition d'un grand nombre d'utilisateurs.

Les technologies d'application web suivantes ne sont pas compatibles :

- *Applications non web comme SSH, FTP, SMTP, Remote Desktop Protocol (protocole de prise de contrôle à distance des postes - RDP) etc.*
- *HTTP 2.0*
- *Encodages non UFT-8*
- *Déploiement IPv6*
- *Transactions multiples dans HTTP comme l'authentification NT LAN Manager (NTLM)*
- *Javascript ES6*
- *Les fichiers autres que HTML, Javascript et CSS ne sont pas réécrits (par exemple Flash, Java Applet, Microsoft Silverlight, PDF, XML, etc.)*
- *Autres technologies (par exemple, Microsoft Sliverlight ou XML/XSLT)*
- *Tous les encodages de contenu (par exemple, `Accept-Encoding : defalte, br`)*

TECHNOLOGIES	Version prise en charge
Technologies d'application Web	*Les fichiers encodés en UTF-16 ne sont pas pris en charge.* • HTML • HTML5 • HTML5-Web-Sockets • Javascript ES5 ou version antérieure • RDP, VNC, ou SSH • Les environnements Virtual Desktop Infrastructure (infrastructure de bureau virtuel ; VDI) et Virtual Machine (machine virtuelle ; VM), comme Citrix XenApp et XenDesktop et VMWare Horizon et vCenter, soutiennent l'accès nativement via HTML5. Vous pouvez utilisez RDP, VNC ouSSH sur ces

 ©2026 Palo Alto Networks, Inc.

TECHNOLOGIES	Version prise en charge
	machines via le VPN sans client sans exiger d'applications intergicielles tierces supplémentaires. • Dans les environnements qui ne comprennent pas de soutien natif pour HTML5 ou d'autres technologies d'application Web prises en charge par VPN sans client, vous pouvez utilisez des fournisseurs tiers, comme Thinfinity, à RDP via VPN sans client. • Adobe Flash—Avec le VPN sans client, les navigateurs peuvent servir du contenu qui utilise Adobe Flash, des documents Microsoft Word ou des PDF Adobe. Cependant, le VPN sans client ne peut réécrire des URL HTML ou des liens dans Adobe Flash, des documents Microsoft word ou des PDF Adobe, ce qui peut empêcher le contenu d'être affiché correctement. • Encodages de contenu (par exemple, `Accept-Encoding : gzip`)
Systèmes d'exploitation	• Windows • macOS • iOS • Android • Chrome • Linux
Navigateurs pris en charge	• Chrome • Microsoft Edge • Internet Explorer • Safari • Firefox
Méthodes d'authentification prises en charge	• Authentification locale • Authentification externe • LDAP • SAML • Kerberos • RADIUS ou TACACS+ • Authentification du certificat client • Authentification à deux facteurs

 ©2026 Palo Alto Networks, Inc.

Configurer le VPN sans client

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Il est fortement recommandé d'accéder uniquement à des pages de confiance via le VPN sans client. Pour plus d'informations, consultez VPN sans client GlobalProtect.

Pour configurer le VPN sans client GlobalProtect, suivez les étapes ci-dessous :

- Configurer le VPN sans client – Panorama
- Configurer le VPN sans client – SCM

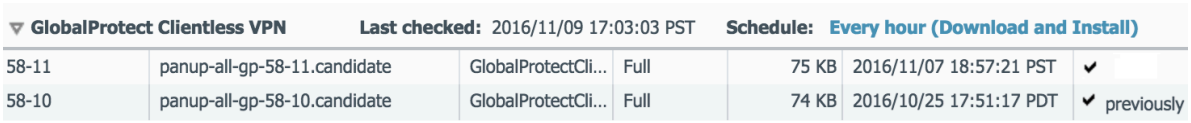
  L'adresse IP source du trafic VPN sans client (comme le voit l'application) correspondra à l'adresse IP de l'interface de sortie par laquelle le portail peut joindre l'application ou à l'adresse IP traduite lorsque la NAT source est en cours d'utilisation.

Configurer le VPN sans client – Panorama

Suivez les étapes ci-dessous pour configurer le VPN sans client dans Panorama.

1. Avant de commencer :

   - Installez un abonnement GlobalProtect sur le pare-feu qui héberge le VPN sans client depuis le portail GlobalProtect. Reportez-vous à Licences actives et abonnements.
   - Installez la dernière mise à jour dynamique du VPN sans client GlobalProtect (voir Installer les mises à jour de contenu et du logiciel) et définissez un calendrier d'installation des nouvelles mises à jour de contenu dynamiques. Il est recommandé de toujours installer les dernières mises à jour de contenu pour le VPN sans client GlobalProtect.



   - Il est recommandé de configurer un FQDN distinct pour le portail GlobalProtect qui héberge le VPN sans client. N'utilisez pas le même FQDN que l'interface Web PAN-OS.
   - Hébergez le portail GlobalProtect sur le port SSL standard (port TCP 443). Les ports non standard ne sont pas pris en charge.

 ©2026 Palo Alto Networks, Inc.

2. Configurez les applications disponibles avec VPN sans client GlobalProtect. Le portail GlobalProtect affiche ces applications sur la page d'accueil que les utilisateurs voient lorsqu'ils se connectent (page d'accueil des applications).
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Clientless Apps (Applications sans client)** et **Add (Ajouter)** une ou plusieurs applications. Spécifiez les éléments suivants pour chaque application :
      - **Name (Nom)** : saisissez un nom qui décrit l'application (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
      - **Location (Emplacement)** : (pour un pare-feu en mode systèmes virtuels multiples) le système virtuel (vsys) sur lequel les applications VPN sans client sont disponibles. Pour un pare-feu qui n'est pas en mode systèmes virtuels multiples, le champ **Location (Emplacement)** ne s'affiche pas.
      - **Application Home URL (URL d'accueil de l'application)** : l'URL à laquelle se trouve l'application Web (4,095 caractères maximum).
      - **Application Description (Description de l'application)** (Facultatif) : une brève description de l'application (255 caractères maximum).
      - **Application Icon (Icône de l'application)** (Facultatif : une icône pour identifier l'application sur la page d'application publiée. Vous pouvez parcourir pour télécharger l'icône.
   2. Cliquez sur **OK**.

3. (Facultatif) Créez des groupes pour gérer des ensembles d'applications Web.

   Les groupes d'applications sans client sont utiles si vous souhaitez gérer plusieurs ensembles d'applications et fournir un accès en fonction des groupes d'utilisateurs. Par exemple, des applications financières pour l'équipe G&A ou des applications de développeur pour l'équipe d'ingénierie.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Clientless App Groups (Groupes d'applications sans client)**. **Add (Ajoutez)** un nouveau groupe d'applications VPN sans client et spécifiez les éléments suivants :
      - **Name (Nom)** : saisissez un nom qui décrit le groupe d'applications (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
      - **Location (Emplacement)** : (pour un pare-feu en mode systèmes virtuels multiples) le système virtuel (vsys) sur lequel le groupe d'applications VPN sans client est disponible. Pour un pare-feu qui n'est pas en mode systèmes virtuels multiples, le champ **Location (Emplacement)** ne s'affiche pas.
   2. Dans la section **Applications**, **Add (Ajoutez)** les applications au groupe. Vous pouvez sélectionner dans la liste des applications VPN sans client existantes ou définir une **New Clientless App (Nouvelle application sans client)**.
   3. Cliquez sur **OK**.

 ©2026 Palo Alto Networks, Inc.

4. Configurez le portail GlobalProtect pour fournir le service VPN sans client.
   1. Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portal (Portail)**, puis sélectionnez une configuration de portail existante ou **Add (Ajouter)** une nouvelle. Reportez-vous à la rubrique Paramétrer l'accès au portail GlobalProtect.
   2. Dans l'onglet **Authentication (Authentification)**, vous pouvez :
      - (Facultatif Créez une nouvelle authentification client spécifique pour VPN sans client. Dans ce cas, choisissez **Browser (Navigateur)** comme **OS (Système d'exploitation)** pour **Client Authentication (Authentification client)**.
      - Utilisez une authentification client existante.
   3. Dans **Clientless (Sans client)** > **General (Général)**, sélectionnez **Clientless VPN (VPN sans client)** pour activer le service de portail et configurer les éléments suivants :
      - Spécifiez un **Hostname (Nom d'hôte)** (adresse IP ou FQDN) pour le portail GlobalProtect qui héberge la page d'accueil des applications. Ce nom d'hôte est utilisé pour réécrire les URL d'application. (Pour plus d'informations sur la réécriture des URL, reportez-vous à l'étape 8).

        Si vous utilisez la Traduction des adresses réseau (NAT) pour fournir un accès au portail GlobalProtect, l'adresse IP ou FQDN que vous saisissez doit correspondre à (ou se résoudre en) l'adresse IP NAT du portail GlobalProtect (l'adresse IP publique). Étant donné que les utilisateurs ne peuvent pas accéder au portail GlobalProtect sur un port personnalisé, le port pré-NAT doit également être le port TCP 443.
      - Spécifiez une **Security Zone (Zone de sécurité)**. Cette zone est utilisée comme zone source pour le trafic entre le pare-feu et les applications. Les règles de sécurité définies de cette zone vers la zone d'application déterminent à quelles applications les utilisateurs peuvent accéder.
      - Sélectionnez un serveur **DNS Proxy (Proxy DNS)** ou configurez un **New DNS Proxy (Nouveau proxy DNS)**. GlobalProtect utilisera ce proxy pour résoudre les noms d'application. Reportez-vous à DNS Proxy Object (Objet proxy DNS).
      - **Login Lifetime (Durée de vie de la connexion)** : spécifiez la durée de temps maximale (en heures ou en minutes) pendant laquelle une session VPN sans client est valide. La durée de la session typique est de 3 heures. La plage pour les heures est comprise entre 1 et 24, et celle pour les minutes est comprise entre 60 et 1 440. Après l'expiration de la session, les utilisateurs doivent se réauthentifier et démarrer une nouvelle session VPN sans client.
      - **Inactivity Timeout (Délai d'inactivité)** : spécifiez la durée de temps (en heures ou en minutes) pendant laquelle une session VPN sans client peut rester inactive. Le délai d'inactivité typique est de 30 minutes. La plage pour les heures est comprise entre 1 et 24, et celle pour les minutes est comprise entre 5 et 1 440. S'il n'y a pas d'activité utilisateur pendant la durée spécifiée, les utilisateurs doivent se réauthentifier et démarrer une nouvelle session VPN sans client.
      - **Max User (Nombre max. d'utilisateurs)** : spécifiez le nombre maximum d'utilisateurs pouvant se connecter simultanément au portail. Si aucune valeur n'est spécifiée, la capacité du point de terminaison est supposée. Si la capacité du point de terminaison est inconnue, une capacité de 50 utilisateurs est supposée. Lorsque le nombre maximum d'utilisateurs est atteint, les utilisateurs VPN sans client supplémentaires ne peuvent pas se connecter au portail.

 ©2026 Palo Alto Networks, Inc.

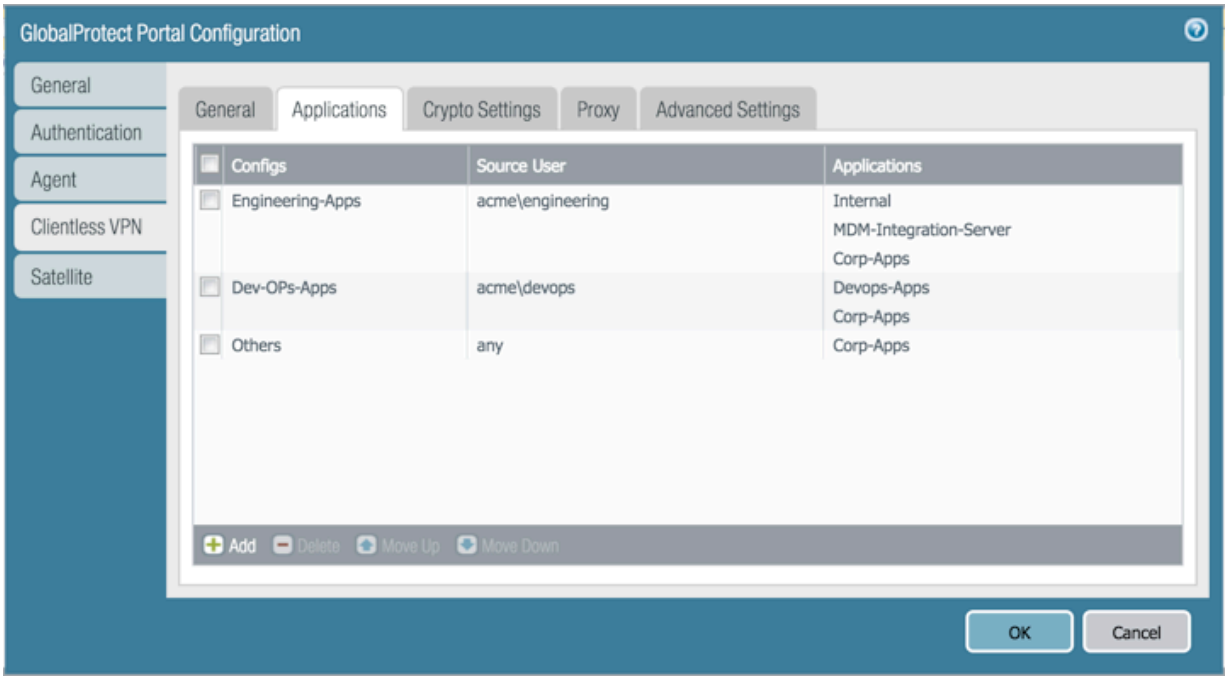
5. Mappez les utilisateurs et les groupes d'utilisateurs aux applications.

   Ce mappage contrôle les applications que les utilisateurs ou les groupes d'utilisateurs peuvent lancer à partir d'une session VPN sans client GlobalProtect.

   Le portail GlobalProtect utilise les paramètres de l'utilisateur / du groupe d'utilisateurs que vous avez indiqués pour déterminer la configuration qui doit être fournie à l'utilisateur VPN sans client GlobalProtect qui se connecte. Si vous avez plusieurs configurations, assurez-vous qu'elles sont correctement classées et mappées à toutes les applications requises, car le portail recherche une correspondance de configuration en commençant par le haut de la liste. Dès

 ©2026 Palo Alto Networks, Inc.

que le portail trouve une correspondance, il fournit la configuration associée à l'utilisateur VPN sans client GlobalProtect.



Publier une application pour un utilisateur / groupe d'utilisateurs ou leur permettre de lancer des applications non publiées n'implique pas qu'ils puissent accéder à ces applications. Vous utilisez les politiques de sécurité pour contrôler l'accès aux applications (publiées ou non).

*Vous devez configurer l'association de groupe (**Device [Périphérique]** > **User Identification [Identification utilisateur]** > **Group Mapping Settings [Paramètres du mappage de groupe]**) avant de pouvoir sélectionner les groupes.*

1. À l'onglet **Applications**, **Add (Ajoutez)** un **Applications to User Mapping (Mappage des applications aux utilisateurs)** pour faire correspondre les utilisateurs avec des applications publiées.
   - **Name (Nom)** : donnez un nom au mappage (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
   - **Display application URL address bar (Afficher la barre d'adresse URL d'application)** : sélectionnez cette option pour afficher une barre d'adresse URL d'application à partir de laquelle les utilisateurs peuvent lancer des applications qui ne sont pas publiées sur la page d'accueil des applications. Lorsque cette option est activée, les utilisateurs peuvent sélectionner la **Application URL (URL de l'application)**.

     Lorsque cette option est désactivée, **Application URL (URL de l'application)** n'apparaît pas sur la page de renvoi VPN sans client.
2. Spécifiez les **Source Users (Utilisateurs source)**. Vous pouvez **Add (Ajoutez)** des utilisateurs individuels ou des groupes d'utilisateurs auxquels appliquer la configuration

 ©2026 Palo Alto Networks, Inc.

d'application actuelle. Ces utilisateurs ont la permission de lancer les applications configurées à l'aide d'un VPN sans client GlobalProtect. En plus des utilisateurs et des groupes, vous pouvez spécifier quand ces paramètres sont applicables aux utilisateurs ou groupes :

- **any (tous)** : la configuration de l'application s'applique à tous les utilisateurs (pas besoin d'**Add (Ajouter)** des utilisateurs ou des groupes d'utilisateurs).
- **select (sélectionner)** : la configuration d'application s'applique uniquement aux utilisateurs et groupes d'utilisateurs que vous souhaitez **Add (Ajouter)** à cette liste.

3. **Add (Ajoutez)** des applications individuelles ou des groupes d'applications au mappage. Les **Source Users (Utilisateurs source)** que vous avez inclus à la configuration peuvent utiliser le VPN sans client GlobalProtect pour lier les applications que vous ajoutez.

6. Spécifiez les paramètres de sécurité pour une session VPN sans client.

1. À l'onglet **Crypto Settings (Paramètres crypto)**, spécifiez les algorithmes d'authentification et de chiffrement pour les sessions SSL entre le pare-feu et les applications publiées.
   - **Protocol Versions (Versions du protocole)** : sélectionnez les versions TLS/SSL minimales et maximales requises. Plus la version TLS est élevée, plus la connexion est sécurisée. Les choix comprennent **SSLv3**, **TLSv1.0**, **TLSv1.1** ou **TLSv1.2**.

     *La **Max Version (version max)** de TLS compatible avec Clientless VPN est TLSv1.2. **TLSv1.3** n'est actuellement pas compatible pour les connexions Clientless VPN.*
   - **Key Exchange Algorithms (Algorithmes d'échange de clés)** : sélectionnez les types d'algorithmes pris en charge pour l'échange de clés. Les choix sont les suivants : **RSA**, Diffie-Hellman (**DHE**) ou Diffie-Hellman basé sur les courbes elliptiques éphémères (**ECDHE**).
   - **Encryption Algorithms (Algorithmes de cryptage)** : sélectionnez les algorithmes de cryptage pris en charge. Nous recommandons **AES128** ou plus.
   - **Authentication Algorithms (Algorithmes d'authentification)** : sélectionnez les algorithmes d'authentification pris en charge. Les choix sont les suivants : **MD5**, **SHA1**, **SHA256** ou **SHA384**. Nous recommandons SHA256 ou plus.
2. Sélectionnez l'action à effectuer lorsque les problèmes suivants se produisent avec un certificat de serveur présenté par une application :
   - **Block sessions with expired certificate (Bloquer les sessions avec un certificat expiré)** : si le certificat du serveur a expiré, bloquez l'accès à l'application.
   - **Block sessions with untrusted issuers (Bloquer les sessions avec des émetteurs non approuvés)** : si le certificat du serveur est émis à partir d'une autorité de certification non approuvée, bloquez l'accès à l'application.
   - **Block sessions with unknown certificate status (Bloquer les sessions dont l'état du certificat est inconnu)** : si le service OCSP ou CRL renvoie un état de révocation de certificat `unknown (inconnu)`, bloquez l'accès à l'application.
   - **Block sessions on certificate status check timeout (Bloquer les sessions dont le délai d'attente de vérification de l'état du certificat a expiré)** : si l'état du certificat vérifie les délais avant de recevoir une réponse de tout service d'état du certificat, bloquez l'accès à l'application.

 ©2026 Palo Alto Networks, Inc.

7. (Facultatif) Spécifiez une ou plusieurs configurations de serveur proxy pour accéder aux applications.

   Seule l'authentification de base au proxy est prise en charge (nom d'utilisateur et mot de passe).

   Si les utilisateurs doivent accéder aux applications via un serveur proxy, indiquez un **Proxy Server (Serveur proxy)**. Vous pouvez ajouter plusieurs configurations de serveur proxy, une pour chaque ensemble de domaines.

   - **Name (Nom)** : une étiquette de 31 caractères maximum permettant d'identifier la configuration du serveur proxy. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
   - **Domains (Domaines)** : ajoutez les domaines servis par le serveur proxy. Vous pouvez utiliser un caractère générique (*) au début du nom de domaine pour indiquer plusieurs domaines.
   - **Use Proxy (Utiliser un proxy)** : sélectionnez pour affecter un serveur proxy afin de fournir l'accès aux domaines.
   - **Server (Serveur)** : spécifiez l'adresse IP ou le nom d'hôte du serveur proxy.
   - **Port** : spécifiez un port de communication avec le serveur proxy.
   - **User (Utilisateur)** et **Password (Mot de passe)** : spécifiez les informations d'identification **User (Utilisateur)** et **Password (Mot de passe)** nécessaires pour se connecter au serveur proxy. Saisissez à nouveau le mot de passe pour le vérifier.

8. (Facultatif) Spécifiez un traitement spécial pour les domaines d'application.

   Le VPN sans client agit comme un proxy inversé et modifie les pages Web renvoyées par les applications Web publiées. Il réécrit toutes les URL et présente une page réécrite aux utilisateurs distants de sorte que lorsqu'ils accèdent à l'une de ces URL, les requêtes passent par le portail GlobalProtect.

   Dans certains cas, l'application peut avoir des pages qui n'ont pas besoin d'être accessibles via le portail (par exemple, l'application peut inclure un code de titre de yahoo.finance.com). Vous pouvez exclure ces pages.

   À l'onglet **Advanced Settings (Paramètres avancés)**, **Add (Ajoutez)** des noms de domaine, des noms d'hôte ou des adresses IP pour **Rewrite Exclude Domain List (Réécrire la liste des domaines d'exclusion)**. Ces domaines sont exclus des règles de réécriture et ne peuvent pas être réécrits.

   Les chemins ne sont pas pris en charge dans les noms d'hôte et de domaine. Le caractère générique (*) pour les noms d'hôte et de domaine ne peut apparaître qu'au début du nom (par exemple, * .etrade.com).

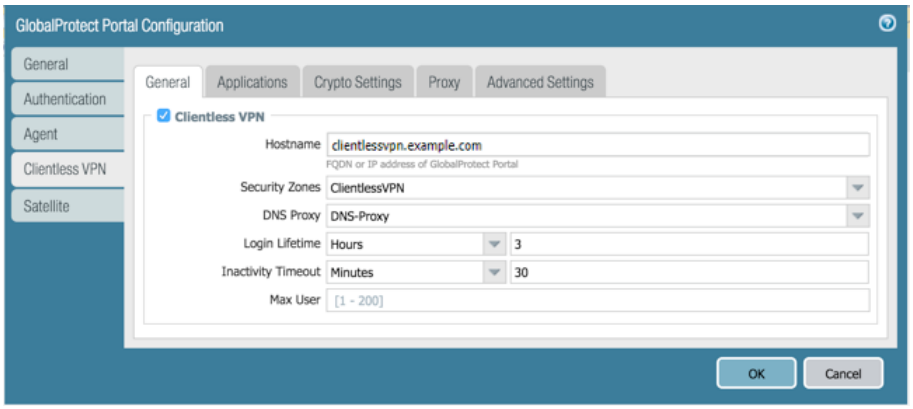
9. Enregistrez la configuration du portail.
   1. Cliquez deux fois sur **OK**.
   2. **Commit (Validez)** vos modifications.

 ©2026 Palo Alto Networks, Inc.

10. Configurez une Règle de politique de sécurité pour permettre aux utilisateurs d'accéder aux applications publiées.

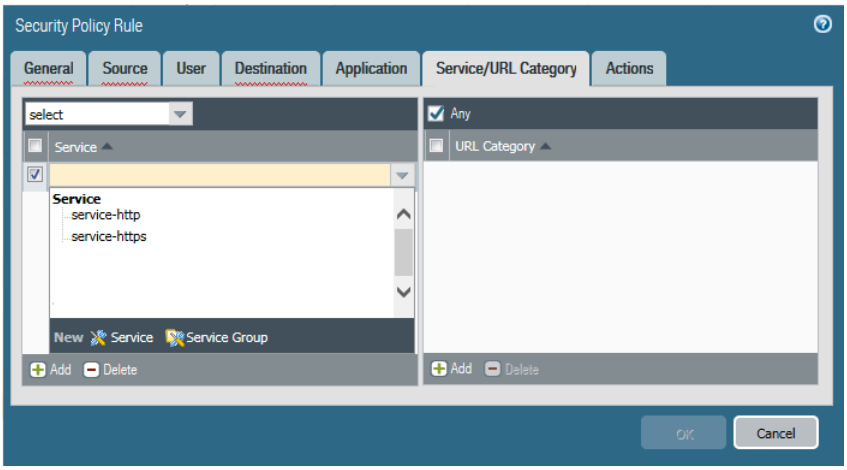
Vous avez besoin de politiques de sécurité pour les éléments suivants :

- Rendre le portail GlobalProtect qui héberge le VPN sans client accessible depuis Internet. Il s'agit du trafic depuis une zone non approuvée ou une zone Internet vers la zone où vous hébergez le portail VPN sans client.



- Autoriser les utilisateurs VPN sans client à accéder aux ressources de l'entreprise. Il s'agit du trafic depuis la zone VPN sans client vers la zone de confiance ou la zone de l'entreprise. Les politiques de sécurité que vous définissez contrôlent les utilisateurs autorisés à utiliser chaque application publiée. Pour la zone de sécurité où les serveurs des applications publiées sont hébergés, veillez à **Enable User Identification (Activer l'identification utilisateur)**.

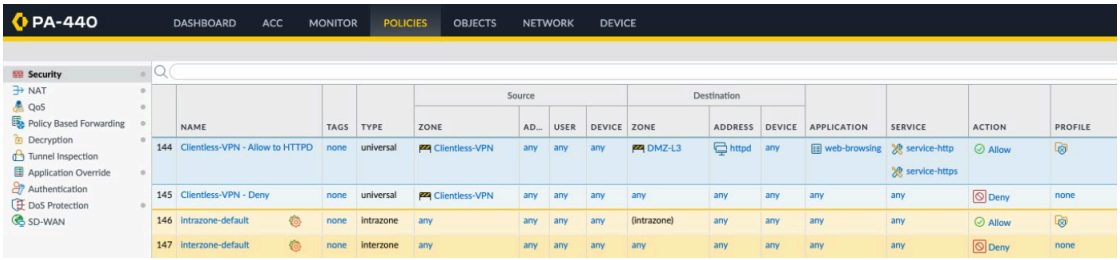
  Par défaut, **Service/URL** dans **Security Policy Rule (Règle de politique de sécurité)** est défini sur **application-default**. VPN sans client ne fonctionnera pas pour les sites HTTPS avec ce paramètre par défaut. Modifiez **Service/URL** pour inclure à la fois **service-http** et **service-https**.



- Configurez une politique pour bloquer explicitement tout le trafic provenant de la zone VPN sans client qui n'est pas explicitement autorisé par la politique. Cela garantira que le trafic n'est pas autorisé par inadvertance par d'autres politiques (par exemple, intrazone par

 ©2026 Palo Alto Networks, Inc.

défaut). Le VPN sans client n'est pas une méthode sécurisée pour naviguer sur plusieurs sites Internet ou intranet (voir notre avis PAN-SA-2025-0005 pour plus de détails).



- Lorsque vous configurez un serveur proxy pour accéder aux applications VPN sans client, veillez à inclure l'adresse IP et le port du proxy dans la définition de la politique de sécurité. Lorsque les applications sont accessibles via un serveur proxy, seules les politiques de sécurité définies pour l'adresse IP et le port du proxy sont appliquées.

11. (Facultatif) Pour configurer la page d'accueil du portail VPN sans client pour qu'elle affiche l'emplacement du portail auquel les utilisateurs du VPN sans client sont connectés, spécifiez l'emplacement physique du pare-feu sur lequel vous configurez le portail.

Lorsque les utilisateurs du VPN sans client constatent un comportement inhabituel, comme une piètre performance du réseau, ils peuvent donner les informations de cet emplacement à leur service d'assistance ou aux professionnels du Centre d'assistance pour qu'ils les aident avec la résolution du problème. Ils peuvent également utiliser ces informations sur l'emplacement pour déterminer leur proximité au portail. Selon leur proximité, ils peuvent évaluer s'ils doivent passer à un portail plus près.

Si vous ne spécifiez pas l'emplacement du portail, la page d'accueil du portail VPN sans client affiche un champ d'emplacement vide.

- **Dans la CLI** : Utilisez la commande de la CLI suivante pour spécifier l'emplacement physique du pare-feu sur lequel vous avez configuré le portail :

```
<username@hostname> définir le paramètre deviceconfig global-
protect location <location>
```

- **Dans l'API XML** : Utilisez la commande de l'API XML suivante pour spécifier l'emplacement physique du pare-feu sur lequel vous avez configuré le portail :
  - **périphériques** : nom du pare-feu sur lequel vous avez configuré le portail;
  - **emplacement** : emplacement du pare-feu sur lequel vous avez configuré le portail.

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

L'adresse IP source du trafic VPN sans client (comme le voit l'application) correspondra à l'adresse IP de l'interface de sortie par laquelle le portail peut joindre l'application ou à l'adresse IP traduite lorsque la NAT source est en cours d'utilisation.

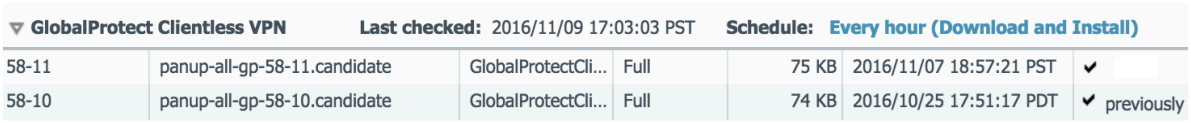
 ©2026 Palo Alto Networks, Inc.

Configurer le VPN sans client – SCM

Suivez les étapes ci-dessous pour configurer le VPN sans client dans Strata Cloud Manager.

1. Avant de commencer :

   - Installez un abonnement GlobalProtect sur le pare-feu qui héberge le VPN sans client depuis le portail GlobalProtect. Reportez-vous à Licences actives et abonnements.
   - Installez la dernière mise à jour dynamique du VPN sans client GlobalProtect (voir Installer les mises à jour de contenu et du logiciel) et définissez un calendrier d'installation des nouvelles mises à jour de contenu dynamiques. Il est recommandé de toujours installer les dernières mises à jour de contenu pour le VPN sans client GlobalProtect.



   - Il est recommandé de configurer un FQDN distinct pour le portail GlobalProtect qui héberge le VPN sans client. N'utilisez pas le même FQDN que l'interface Web PAN-OS.
   - Hébergez le portail GlobalProtect sur le port SSL standard (port TCP 443). Les ports non standard ne sont pas pris en charge.

2. Pour les étapes restantes, consultez GlobalProtect – VPN sans client.

 ©2026 Palo Alto Networks, Inc.

Résoudre les problèmes du VPN sans client

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Parce que cette fonctionnalité implique une réécriture dynamique des applications HTML, le contenu HTML de certaines applications peut ne pas réécrire correctement et interrompre l'application. Si des problèmes se produisent, utilisez les commandes du tableau suivant pour vous aider à identifier la cause probable :

Tableau 9 : Tableau : Statistiques du moteur de réécriture

Action (Action)	Commande
Commandes CLI	
Indique la version du contenu dynamique du VPN sans client utilisé Vous pouvez également afficher la version de mise à jour dynamique à partir de **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)** > **VPN GlobalProtect Clientless (VPN sans client GlobalProtect)**.	**show system setting ssl-decrypt memory** le proxy utilise le cache de certificats SSL de l'allocateur partagé : Entrées actuelles : 1 Allocated 1, Freed 0 Current CRE (61-62) : 3456 KB (Actual 3343 KB) Last CRE (60-47) : 3328 KB (Actual 3283 KB) Dans cet exemple, la mise à jour dynamique actuelle est la version 61-62 et la dernière mise à jour dynamique installée est la version 60-47.
Liste des utilisateurs actifs (actuels) de VPN sans client	**show global-protect-portal current-user portal GPClientlessPortal filter-user all-users** Portail GlobalProtect : GPClientlessPortal Vsys-Id : 1 User : paloaltonetworks.com\johndoe Session-id : 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0 Client-IP : 5.5.5.5 Inactivity Timeout : 1800 Seconds before inactivity timeout : 1750 Login Lifetime : 10800 Seconds

 ©2026 Palo Alto Networks, Inc.

Action (Action)	Commande
	before login lifetime : 10748 Total number of use r sessions: 1
Afficher les résultats de la résolution DNS Cela peut être utile pour déterminer s'il existe des problèmes de DNS. S'il y a un problème de DNS, vous remarquerez la requête sur un FQDN qui n'était pas résolvable dans la sortie CLI.	**show system setting ssl-decrypt dns-cache** Total d es entrées de cache DNS : 89 Site IP Expire(secs) Interface bugzilla.panw.local 10.0.2.15 querying 0 www.google.com 216.58.216.4 Expired 0 stats.g. doubleclick.net 74.125.199.154 Expired 0
Afficher toutes les sessions utilisateur de VPN sans client et les cookies stockés	**show system setting ssl-decrypt gp-cookie-cache** U ser: johndoe, Session-id: 1SU2vrPIDfdopGf-7gahMTC iX8PuL0S0, Client-ip: 199.167.55.50
Afficher les statistiques de réécriture Cela est utile pour identifier l'intégrité du moteur de réécriture de VPN sans client. Reportez-vous à Résoudre les problèmes du VPN sans client pour des informations sur les statistiques de réécriture et leur signification ou objectif.	**show system setting ssl-decrypt rewrite-stats** Rew rite Statistics initiate_connection : 11938 setup _connection : 11909 session_notify_mismatch : 1 r euse_connection : 37 file_end : 4719 packet : 174 257 packet_mismatch_session : 1 peer_queue_update _rcvd : 167305 peer_queue_update_sent : 167305 pe er_queue_update_rcvd_failure: 66 setup_connection _r : 11910 packet_mismatch_session_r : 22 pkt_no_ dest : 23 cookie_suspend : 2826 cookie_resume : 2 826 decompress : 26 decompress_freed : 26 dns_res olve_timeout : 27 stop_openend_response : 43 rece ived_fin_for_pending_req : 26 Destination Statist ics To mp : 4015 To site : 12018 To dp : 17276 Re turn Codes Statistics ABORT : 18 RESET : 30 PROTO COL_UNSUPPORTED : 7 DEST_UNKNOWN : 10 CODE_DONE : 52656 DATA_GONE : 120359 SWITCH_PARSER : 48 INSE RT_PARSER : 591 SUSPEND : 2826 Total Rewrite Byte s : 611111955 Total Rewrite Useconds : 6902825 To tal Rewrite Calls : 176545
Commandes de débogage	
Activer les journaux de débogage sur le pare-feu exécutant le	**debug dataplane packet-diag set log feature ssl a ll** **debug dataplane packet-diag set log feature misc all**

 ©2026 Palo Alto Networks, Inc.

Action (Action)	Commande
portail de VPN sans client	**debug dataplane packet-diag set log feature proxy all** **debug dataplane packet-diag set log feature flow basic** **debug dataplane packet-diag set log on**
Activer la capture de paquets sur le pare-feu exécutant le portail de VPN sans client	**debug dataplane packet-diag set capture username <*portal-username*>** **debug dataplane packet-diag set capture stage clientless-vpn-client file <*clientless-vpn-client-file*>** **debug dataplane packet-diag set capture stage clientless-vpn-server file <*clientless-vpn-server-file*>** **debug dataplane packet-diag set capture stage firewall file <*firewall-file*>** **debug dataplane packet-diag set capture stage receive file <*receive-file*>** **debug dataplane packet-diag set capture stage transmit file <*transmit-file*>** **debug dataplane packet-diag set capture on** *Lorsque vous exécutez les commandes de capture des paquets, une page de consentement s'afficher après que les utilisateurs finaux se connectent au portail VPN sans client, les informant ainsi que les paquets capturés lors de leur session d'utilisateur contiendront des données non chiffrées (en texte clair). Si les utilisateurs acceptent la session de capture des paquets, ils passent ensuite à la page d'accueil des applications, où la capture des paquets commence. Si les utilisateurs n'acceptent pas la session de capture des paquets, ils sont déconnectés du portail VPN sans client et doivent contacter un administrateur pour passer à une session utilisateur ordinaire (sans capture de paquets).* *Si vous exécutez des commandes de capture de paquets pour les sessions utilisateurs qui sont déjà en cours, ces utilisateurs sont automatiquement déconnectés du portail VPN sans client et doivent se reconnecter pour accepter ou refuser la session de capture de paquets.*
Montrer les fichiers de capture des paquets	**debug dataplane packet-diag show setting** -------- ---------- - Packet diagnosis setting: ---------- ---------- Packet filter Enabled: no Match pre-parsed packet: no ------ ---------- --- Logging Enabled: no Log-throttle: no Sync-log-by-ticks: yes Features: Counters: ---------- ---------- Pack

 ©2026 Palo Alto Networks, Inc.

Action (Action)	Commande
	et capture Enabled: yes Snaplen: 0 Username: test 1 Stage clientless-vpn-client: file client.pcap C aptured: packets - 3558 bytes - 11366322 Maximum: packets - 0 bytes - 0 Stage clientless-vpn-serve r: file server.pcap Captured: packets - 1779 byte s - 5651923 Maximum: packets - 0 bytes - 0 ------ ---------- ---
Exporter des fichiers de capture de paquets à un serveur Secure Copy (Copie sécurisée ; SCP)	**scp export filter-pcap** + remote-port SSH port num ber on remote host + source-ip Set source address to specified interface address * from from * to Destination (username@host:path) **scp export filte r-pcap from <*source-file*> to <*scp-server*> Destina tion (username@host:path)**

Tableau 10 : Tableau : Statistiques du moteur de réécriture

Statistiques	Description
initiate_connection_failure	L'initialisation de la connexion a échoué à l'hôte principal
setup_connection_failure	Échec de la configuration
setup_connection_duplicate	Il existe une session homologue en double
session_notify_mismatch	Session majoritairement invalide
packet_mismatch_session	Impossible de trouver la bonne session pour le paquet entrant
peer_queue_update_rcvd_failure	La session était invalide lors de la réception de la mise à jour de paquet par un homologue
peer_queue_update_sent_failure	Échec de l'envoi des mises à jour de paquets à l'homologue ou échec de l'envoi des mises à jour de longueur de file d'attente de paquets à l'homologue
exceed_pkt_queue_limit	Trop de paquets mis en file d'attente
proxy_connection_failure	La connexion proxy a échoué
setup_connection_r	Installation de la session homologue sur le serveur d'applications. Cette valeur doit correspondre aux valeurs de **initiate_connection** et **setup_connection**.

 ©2026 Palo Alto Networks, Inc.

Statistiques	Description
setup_connection_duplicate_r	Sessions en double déjà dans le proxy
setup_connection_failure_r	Échec de la configuration de la session homologue
session_notify_mismatch_r	Session homologue non trouvée
packet_mismatch_session_r	Session homologue non trouvée en essayant d'obtenir le paquet
exceed_pkt_queue_limit_r	Trop de paquets détenus
unknown_dest	Impossible de trouver l'hôte de destination
pkt_no_dest	Aucune destination pour ce paquet
cookie_suspend	Session suspendue pour récupérer les cookies
cookie_resume	Réponse reçue de MP avec des cookies mis à jour. Cette valeur correspond généralement à la valeur de cookie_suspend.
decompress_failure	Échec de la décompression
memory_alloc_failure	Échec de l'allocation de la mémoire
wait_for_dns_resolve	Session suspendue pour résoudre les requêtes DNS
dns_resolve_reschedule	Requête DNS replanifiée en raison de l'absence de réponse (réessayez avant l'expiration du délai)
dns_resolve_timeout	Délai d'expiration de la requête DNS
setup_site_conn_failure	Échec de la configuration de la connexion au site (proxy, DNS)
site_dns_invalid	La résolution DNS a échoué
multiple_multipart	Type de contenu en plusieurs parties traité
site_from_referer	Réception de l'hôte principal depuis le référent. Cela peut indiquer des échecs de réécriture de liens depuis Flash ou un autre contenu que VPN sans client ne réécrit pas.
received_fin_for_pending_req	Réception de FIN depuis le serveur pour une demande en attente du client
unmatched_http_state	Contenu HTTP inattendu Cela peut indiquer un problème d'analyse des en-têtes ou du corps HTTP.

©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

Informations sur l’hôte

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager) Pour le service de conformité de l’hôte : • NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l’abonnement Utilisateur mobile Pour le service de conformité de l’hôte : Licence d’abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 et versions ultérieures Moteur d’identité sur le cloud Certificat du périphérique

Même si vous disposez d'une sécurité stricte dans le périmètre de votre réseau d'entreprise, votre réseau est en réalité seulement aussi sécurisé que les terminaux qui y accèdent. Comme la main-d'œuvre est aujourd'hui de plus en plus mobile et qu'elle exige souvent un accès aux ressources d'entreprise depuis des lieux très variés : aéroports, salons de thé, hôtels, et depuis des terminaux très variés, provisionnés par la société et personnels, vous devez logiquement élargir votre sécurité de réseau à vos terminaux pour garantir la mise en œuvre d'une sécurité complète et cohérente. Pour appliquer la règle de politique de sécurité, vous pouvez configurer soit des Host Information Profiles (profils d’informations sur l’hôte - HIP) soit le Service de conformité de l’hôte (HCS) pour GlobalProtect :

- La fonctionnalité de profil d’informations sur l’hôte (HIP) GlobalProtect vous permet de collecter les informations sur l’état de sécurité de vos terminaux, par exemple si les derniers correctifs de sécurité et les dernières définitions d’antivirus sont installés, si le cryptage de disque est activé, si le terminal est débridé ou avec racine, ou s’il exécute un logiciel spécifique dont vous avez besoin au sein de votre organisation et de fonder votre décision pour autoriser ou interdire l’accès à un hôte spécifique en fonction de l’adhésion aux politiques de l’hôte que vous définissez.
- (À partir de PAN-OS 12.1.2)LeService de conformité de l’hôte pour GlobalProtect introduit un service hautement disponible et hébergé dans le cloud qui centralise l’évaluation de la posture des terminaux, la distribution et l’application des règles de politique de sécurité. Le HCS centralise la sécurité des terminaux en traitant des rapports HIP complets dans le cloud et en distribuant uniquement les données de conformité finales ou les verdicts aux produits abonnés comme les déploiements NGFW pour l’application des règles de politique, ce qui élimine le traitement redondant sur chaque pare-feu.

Host Information Profile (profil d’informations sur l’hôte - HIP) dans l’application de la politique de sécurité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l’abonnement Utilisateur mobile

L'une des fonctions de l'application GlobalProtect est de collecter les informations sur l'hôte sur lequel il fonctionne. L'application soumet ensuite ces informations sur l'hôte à la passerelle GlobalProtect dès que la connexion est établie. La passerelle fait correspondre ces informations brutes sur l'hôte soumises par l'application à tous les objets HIP et profils HIP que vous avez définis. Si elle trouve une correspondance, elle génère une entrée dans le journal des correspondances HIP. En outre, si elle trouve une correspondance de profil HIP dans une règle de politique, elle met en œuvre la politique de sécurité correspondante.

Les vérifications HIP sont effectuées lorsque l’application se connecte à la passerelle et les vérifications ultérieures sont effectuées toutes les heures pendant que l’agent GlobalProtect est connecté. L’agent GlobalProtect peut demander un rapport HIP à jour si la vérification HIP antérieure a changé. Seul le dernier rapport HIP est conservé sur la passerelle par terminal.

Assurer la conformité des terminaux avec les vérifications HIP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l’abonnement Utilisateur mobile

L'une des fonctions de l'application GlobalProtect est de collecter les informations sur l'hôte sur lequel il fonctionne. L'application soumet ensuite ces informations sur l'hôte à la passerelle GlobalProtect dès que la connexion est établie. La passerelle fait correspondre ces informations brutes sur l'hôte soumises par l'application à tous les objets HIP et profils HIP que vous avez définis. Si elle trouve une correspondance, elle génère une entrée dans le journal des correspondances HIP. En outre, si elle trouve une correspondance de profil HIP dans une règle de politique, elle met en œuvre la politique de sécurité correspondante.

Les vérifications HIP sont effectuées lorsque l’application se connecte à la passerelle et les vérifications ultérieures sont effectuées toutes les heures pendant que l’agent GlobalProtect est connecté. L’agent GlobalProtect peut demander un rapport HIP à jour si la vérification HIP antérieure a changé. Seul le dernier rapport HIP est conservé sur la passerelle par terminal.

 ©2026 Palo Alto Networks, Inc.

L'utilisation des profils d'informations sur l'hôte pour la mise en œuvre d'une stratégie active la sécurité granulaire qui garantit que les hôtes distants accédant à vos ressources vitales sont adéquatement maintenus et qu'ils respectent vos normes de sécurité avant de les autoriser à accéder à vos ressources réseau. Par exemple, avant d'autoriser l'accès à vos systèmes de données les plus sensibles, vous devrez vérifier que le cryptage de disque est activé sur les disques durs des hôtes accédant aux données. Vous pouvez mettre en œuvre cette stratégie en créant une règle de sécurité qui autorise l'accès à l'application uniquement si le cryptage de disque est activé sur le système de points de terminaison. En outre, pour les points de terminaison qui ne sont pas en conformité avec cette règle, vous pouvez créer un message de notification qui alerte les utilisateurs sur les motifs de l'interdiction d'accès et fournit des liens vers le partage de fichiers d'où ils peuvent accéder au programme d'installation pour le logiciel de chiffrement manquant (logiquement, pour autoriser l'utilisateur à accéder à ce partage de fichiers, vous devrez créer une règle de sécurité correspondante autorisant l'accès au partage spécifique pour les hôtes présentant cette correspondance de profil HIP spécifique).

Quelles sont les données que l'application GlobalProtect collecte ?

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Par défaut, l'application GlobalProtect collecte les données spécifiques des fournisseurs relatives aux offres groupées de sécurité pour les utilisateurs finaux qui fonctionnent sur le point de terminaison (compilation par le programme de partenariat global OPSWAT) et rapporte ces données sur la passerelle GlobalProtect pour la mise en œuvre d'une politique. Consultez le tableau Assistance OPSWAT GlobalProtect 5.1, Assistance OPSWAT GlobalProtect 5.2, Assistance OPSWAT GlobalProtect 6.0 ou Assistance OPSWAT GlobalProtect 6.1 pour plus d'informations sur les produits de fournisseurs tiers que GlobalProtect peut détecter à l'aide du OPSWAT SDK indiqué.

> *À partir de l'application GlobalProtect 5.2.6, la prise en charge du SDK OPSWAT V3 (fin de vie) sera supprimée et l'application GlobalProtect utilisera uniquement OPSWAT SDK V4. Les noms de fournisseurs et de produits sont basés sur OPSWAT SDK V4. La fonctionnalité de vérification HIP de l'application GlobalProtect 5.2.6 et versions ultérieures ne fonctionnera pas avec PAN-OS 8.0 (fin de vie) et les versions antérieures (fin de vie). La fonctionnalité de vérification HIP de l'application GlobalProtect 5.2.6 et versions ultérieures fonctionnera comme prévu avec PAN-OS 8.1 et les versions ultérieures.*

Comme les logiciels de sécurité doivent constamment évoluer pour garantir la protection de l'utilisateur final, vos licences de passerelle GlobalProtect vous permettent aussi d'obtenir des mises à jour dynamiques pour le fichier de données GlobalProtect avec les dernières versions de correctif et de logiciel qui sont disponibles pour chaque offre groupée.

Le fichier de données GlobalProtect contient la liste des produits anti-malware avec les listes correspondantes des versions historiques et des versions de mise à jour des définitions pour chaque produit. Le fichier de données GlobalProtect n'est pas utilisé pour renseigner les détails des produits tels que la liste des systèmes d'exploitation et des logiciels anti-malware lors de la

 ©2026 Palo Alto Networks, Inc.

configuration des objets HIP sur le pare-feu. Ces détails sont obtenus par le biais de mises à jour régulières du contenu des applications ou des menaces.

Par exemple, le fichier de données GlobalProtect est utilisé pour :

- Faites correspondre l'objet HIP pour la version de définition spécifiée du produit spécifique à l'aide de l'option **Within (À l'intérieur)**. Par exemple, **Within (À l'intérieur)** = 4, ce qui impliquerait la dernière version et trois versions ci-dessous seraient acceptables.
- Faites correspondre la dernière version du produit à l'aide de l'option **Within (À l'intérieur)**. Par exemple, **Within (À l'intérieur)** =1 (la seule option disponible est grisée pour la correspondance de version).

Pour pouvoir effectuer des comparaisons comme indiqué ci-dessus, le pare-feu doit disposer d'un fichier de données GlobalProtect à jour.

Le fichier de données GlobalProtect est utilisé pour des HIP Objects (Objets HIP) spécifiques lorsque vous utilisez la condition **Within (À l'intérieur)** lors de la configuration d'objets HIP sur le pare-feu.

L'application collecte par défaut des données sur les catégories d'informations suivantes pour permettre d'identifier l'état de sécurité de l'hôte :

Tableau 11 : Tableau : Catégories de collecte de données

Catégorie	Données collectées
Général	Informations sur l'hôte lui-même, incluant le nom d'hôte, le domaine de connexion, le système d'exploitation, la version de l'application, et, pour les systèmes Windows, le domaine auquel la machine appartient. *Pour le domaine des points de terminaison Windows, l'application GlobalProtect collecte le domaine défini pour `ComputerNameDnsDomain`, à savoir le domaine DNS assigné à l'ordinateur local ou le cluster associé à l'ordinateur local. Ces données sont affichées pour le **Domain (Domaine)** des points de terminaison Windows dans les détails du journal de correspondances HIP (**Monitor (Surveillance)** > **Logs (Journaux)** > **HIP Match (Correspondance HIP)**).*
Périphérique mobile	Informations concernant le périphérique mobile, notamment le nom du périphérique, le domaine de connexion, le système d'exploitation, la version de l'application et les informations sur le réseau auquel le périphérique est connecté. En outre, GlobalProtect recueille des informations permettant de déterminer si l'appareil est débridé (root ou jailbreak). *Pour recueillir les attributs des périphériques mobiles et les utiliser dans les politiques de mise en œuvre HIP, GlobalProtect a besoin d'un serveur MDM. À l'heure actuelle, GlobalProtect prend en charge l'intégration HIP via le serveur MDM Workspace ONE.*

 ©2026 Palo Alto Networks, Inc.

Catégorie	Données collectées
	Pour les périphériques gérés par Workspace ONE, les informations sur l'hôte collectées par l'application GlobalProtect peuvent être complétées par des informations supplémentaires collectées auprès du service Workspace ONE. Reportez-vous à la section Configurer l'agent User-ID Windows pour collecter des informations d'hôte pour connaître une liste d'attributs qui peuvent être récupérés à partir de Workspace ONE.
Gestion des correctifs	Informations relatives à tous les correctifs de logiciels de gestion qui sont activés et/ou installés sur l'hôte et indiquent s'il manque certains correctifs. *Si vous souhaitez configurer la valeur de **Severity (Gravité)** associée aux correctifs manquants en tant que condition de correspondance dans votre objet HIP, utilisez les mappages suivants entre les valeurs de gravité GlobalProtect et les cotes de gravité OPSWAT pour comprendre la signification de chacune des cotes :* • *Sur Panorama, sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** > **<hip-object>** > **Patch Management (Gestion des correctifs)** > **Criteria (Critères)**.* • *Sur Strata Cloud Manager (NGFW) :* 1. *Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Objects (Objets)** > **HIP Objects (Objets HIP)**.* 2. *Créez un objet HIP.* 3. *Sélectionnez ensuite **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)**.* 4. *Sur la page Ajouter une passerelle, sélectionnez **Advanced Settings (Paramètres avancés)** > **HIP Notifications (Notifications HIP)** > **Add HIP Notificaion (Ajouter une notification HIP)**.* • *Sur Strata Cloud Manager (Prisma Access) :* • 1. *Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)**.* 2. *Sur la page Paramètres globaux, sélectionnez **Add HIP Notification (Ajouter une notification HIP)**.*

 ©2026 Palo Alto Networks, Inc.

Catégorie	Données collectées
	Servez-vous des mappages suivants entre les valeurs de gravité GlobalProtect et les cotes de gravité d'OPSWAT pour comprendre la signification de chacune des valeurs : • ***0** : Faible* • ***1** : Modérée* • ***2** : Importante* • ***3** : Critique*
Pare-feu	Informations relatives à tous les pare-feu qui sont installés et/ou activés sur l'hôte.
Anti-logiciels malveillants	Informations relatives à tous les logiciels antivirus ou anti-espion qui sont activés et/ou installés sur le point de terminaison, indiquant si la protection en temps réel est activée, la version des définitions de virus, le dernier temps de balayage et le nom du fournisseur et du produit. GlobalProtect utilise la technologie OPSWAT pour détecter et évaluer les applications de sécurité tierces sur le point de terminaison. En intégrant le Framework OPSWAT OESIS, GlobalProtect vous permet d'évaluer l'état de conformité du point de terminaison. Par exemple, vous pouvez définir des objets HIP et des profils HIP qui vérifient la présence d'une version spécifique du logiciel antivirus à partir d'un fournisseur spécifique sur le point de terminaison et également s'assurer qu'il a les derniers fichiers de définition de virus. *OPSWAT ne parvient pas à détecter les informations **anti-logiciels malveillants** suivantes pour la fonctionnalité de sécurité Gatekeeper sur les terminaux macOS :* • *Engine Version (Version du moteur)* • *Definition Version (Version de la définition)* • *Date* • *Last scanned (Dernière analyse)*
Sauvegarde du disque	Informations indiquant si le logiciel de sauvegarde de disque est installé, le dernier temps de balayage, le nom du fournisseur et du produit du logiciel.
Cryptage du disque	Informations indiquant si le logiciel de cryptage de disque est installé, les disques et/ou les chemins qui sont configurés pour le cryptage, et le nom du fournisseur et du produit du logiciel. (Requires GlobalProtect app 5.2 (Nécessite l'application GlobalProtect 5.2)) Si vous souhaitez afficher l'état de chiffrement de tous les lecteurs et/ou chemins d'accès sur le

 ©2026 Palo Alto Networks, Inc.

Catégorie	Données collectées
	point de terminaison, vous devez entrer manuellement **All (Tous)** en tant que **Encrypted Locations (emplacements chiffrés)** lors de la création de l'objet HIP pour la catégorie **Disk Encryption (Chiffrement de disque)**. Pour vérifier si tous les lecteurs ou chemins d'accès sont chiffrés, vous devez définir les **Encrypted Locations (emplacements chiffrés)** sur **All (Tous)** et définir **State (état)** sur **Is encrypted (est chiffré)** dans la liste déroulante.
Prévention des pertes de données	Informations indiquant si le logiciel de prévention des pertes de données (DLP) est installé et/ou activé pour empêcher la sortie du réseau d'entreprise des informations d'entreprise sensibles ou leur stockage sur des supports potentiellement non sécurisés. Ces informations sont collectées uniquement auprès des points de terminaison Windows.
certificate	Informations sur le certificat machine installé sur le point de terminaison.
Vérifications personnalisées	Informations sur la présence de clés de registre spécifiques (Windows uniquement), de lits de propriétés (plist) (MacOs uniquement), listes de processus LINUX OU de processus du système d'exploitation ou de l'application utilisateur.

Vous pouvez exclure certaines catégories d'informations de la collecte sur certains hôtes pour économiser les cycles d'unité centrale et améliorer les temps de réponse. Pour ce faire, créez une configuration d'agent sur le portail, puis excluez les catégories qui ne vous intéressent pas

- sur Panorama, select **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **Data Collection (Collecte de données)**.
- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)** > **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)**.
- Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **<default>**. Sur la page Par défaut, sélectionnez **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)**.

Par exemple, si vous ne prévoyez pas de créer des politiques qui dépendent de l'exécution ou non de logiciel de sauvegarde du disque par les terminaux, vous pouvez exclure cette catégorie afin d'empêcher l'application de collection des informations sur la sauvegarde du disque.

Vous pouvez également exclure la collecte des informations sur les points de terminaison personnels afin de protéger la confidentialité des utilisateurs. Par exemple, vous pouvez exclure

 ©2026 Palo Alto Networks, Inc.

la liste des applications installées sur les points de terminaison qui ne sont pas gérés par un gestionnaire tiers des périphériques mobiles.

Quelles sont les données que l'application GlobalProtect collecte sur chaque système d'exploitation ?

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

L'application GlobalProtect collecte des données pour vous aider à identifier ou à récupérer le profil des informations de l'hôte (HIP) pour le périphérique afin de l'utiliser dans la HIP-based policy enforcement (application de la politique basée sur HIP).

Quelles sont les données que l'application GlobalProtect collecte dans Windows ?

Le tableau suivant décrit les données collectées par l'application GlobalProtect sur les périphériques Windows pour l'application de la politique basée sur HIP générée par le pare-feu.

Attribut de rapport HIP	Description
Report Generation Time (Heure de génération du rapport)	Date et heure auxquelles le rapport HIP a été généré.
User name (Nom d'utilisateur)	Le nom d'utilisateur qui est utilisé pour se connecter au VPN.
User IP Address (Adresse IP de l'utilisateur)	L'adresse IP du périphérique Windows de l'utilisateur.
Machine Name (Nom de la machine)	Nom de l'hôte et numéro de série du périphérique Windows.
Domain (Domaine)	Le champ est vide dans les périphériques Windows.
SYSTÈME D'EXPLOITATION	Nom de l'application et le nom du fournisseur de l'OS cible.
Host ID (ID d'hôte)	L'ID unique que GlobalProtect affecte afin d'identifier l'hôte. La valeur de l'ID de l'hôte est le GUIDE de la machine sur les périphériques Windows. Le GUIDE de la machine stocké dans le registre Windows (HKEY_Local_Machine\Software\Microsoft \Cryptography\MachineGuid)

 ©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
Client version (Version du client)	Numéro de version de l'application GlobalProtect actuellement installée.
Network interface (Interface réseau)	Les paramètres suivants sont identifiés pour l'interface du réseau : • **Interface**—Type de l'interface de réseau détectée sur le périphérique Windows. • **MAC Address (Adresse MAC)**—L'adresse MAC est l'identifiant unique du matériel attribué à chaque interface du réseau sur le périphérique Windows. • **IP Address (Adresse IP)**—L'adresse IP attribuée à chaque interface de réseau sur le périphérique Windows.
Anti-logiciels malveillants	Informations relatives à tous les logiciels antivirus ou anti-espion qui sont activés ou installés sur le périphérique, si la protection antivirus ou anti-espion en temps réel activée sur l'hôte, la version des définitions de virus, le dernier temps de balayage et le nom du fournisseur et du produit.
Sauvegarde du disque	Informations relatives au statut du disque de sauvegarde du périphérique telles que indiquer si logiciel de sauvegarde de disque est installé sur l'hôte, le dernier temps de balayage, le nom du fournisseur et du produit du logiciel.
Cryptage du disque	Informations au sujet du statut de cryptage du périphérique telle que indiquer si le logiciel de cryptage est installé sur l'hôte, le disque ou le chemin à vérifier pour que le cryptage du disque détermine une correspondance, l'état de l'emplacement crypté et le nom du fournisseur et du produit du logiciel. (Requires GlobalProtect app 5.2 (Nécessite l'application GlobalProtect 5.2)) Si vous souhaitez afficher l'état de chiffrement de tous les lecteurs ou chemins sur le point de terminaison, vous devez saisir manuellement **All (Tous)** comme **Encrypted Locations (Emplacements chiffrés)** lors de la création de l'objet HIP pour la catégorie **Disk Encryption (Chiffrement de disque)**. Pour vérifier si tous les lecteurs ou chemins d'accès sont chiffrés, vous devez définir les **Encrypted Locations (emplacements chiffrés)** sur **All (Tous)** et définir **State (état)** sur **Is encrypted (est chiffré)** dans la liste déroulante.
Gestion des correctifs	Informations relatives à tous les correctifs de logiciels de gestion qui sont activés ou installés sur l'hôte et si l'hôte a détecté qu'il manquait certains correctifs ainsi que la valeur de gravité indiquée. Consultez la catégorie Patch Management (gestion des correctifs) pour les informations sur chaque valeur.

©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
Pare-feu	Informations sur l'activation ou l'installation ou non du logiciel de pare-feu sur l'hôte.
Prévention des pertes de données	Informations indiquant le statut du logiciel de prévention des pertes de données (DLP) sur les périphériques Windows pour empêcher la sortie du réseau d'entreprise des informations d'entreprise ou leur stockage sur des supports potentiellement non sécurisés.
Vérifications personnalisées	Informations au sujet du Registre Windows collectées par l'application GlobalProtect depuis les périphériques Windows. Vous pouvez activer custom checks (vérifications personnalisées) pour collecter des données sur les périphériques Windows afin d'ordonner à l'appli de collecter des informations de registre spécifiques (Clés de registre et valeurs des clés de registre). Le type d'informations collectées peut inclure le fait qu'une application est installée sur le périphérique, ou des attributs spécifiques ou propriétés de cette application.

Quelles sont les données que l'application GlobalProtect collecte sur macOS ?

Le tableau suivant décrit les données collectées par l'application GlobalProtect sur les périphériques macOS pour l'application de la politique basée sur HIP générée par le pare-feu.

Attribut de rapport HIP	Description
Report Generation Time (Heure de génération du rapport)	Date et heure auxquelles le rapport HIP a été généré.
User name (Nom d'utilisateur)	Le nom d'utilisateur qui est utilisé pour se connecter au VPN.
User IP Address (Adresse IP de l'utilisateur)	L'adresse IP du périphérique macOS de l'utilisateur.
Machine Name (Nom de la machine)	Nom de l'hôte et numéro de série du périphérique MacOS.
Domain (Domaine)	Le champ est vide dans les périphériques MacOS.
SYSTÈME D'EXPLOITATION	Nom de l'application et le nom du fournisseur de l'OS cible.
Host ID (ID d'hôte)	L'ID unique que GlobalProtect affecte afin d'identifier l'hôte. La valeur de l'ID de l'hôte est l'adresse MAC de la première interface physique intégrée

 ©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
Client version (Version du client)	Numéro de version de l'application GlobalProtect actuellement installée.
Network interface (Interface réseau)	Les paramètres suivants sont identifiés pour l'interface du réseau : • **Interface**—Type de l'interface de réseau détectée sur le périphérique macOS. • **MAC Address (Adresse MAC)**—L'adresse MAC est l'identifiant unique du matériel attribué à chaque interface du réseau sur le périphérique macOS. • **IP Address (Adresse IP)**—L'adresse IP attribuée à chaque interface de réseau sur le périphérique macOS.
Anti-logiciels malveillants	Informations relatives à tous les logiciels antivirus ou anti-espion qui sont activés ou installés sur le périphérique, si la protection antivirus ou anti-espion en temps réel activée sur l'hôte, la version des définitions de virus, le dernier temps de balayage et le nom du fournisseur et du produit.
Sauvegarde du disque	Informations relatives au statut du disque de sauvegarde du périphérique telles que indiquer si logiciel de sauvegarde de disque est installé sur l'hôte, le dernier temps de balayage, le nom du fournisseur et du produit du logiciel.
Cryptage du disque	Informations au sujet du statut de cryptage du périphérique telle que indiquer si le logiciel de cryptage est installé sur l'hôte, le disque ou le chemin à vérifier pour que le cryptage du disque détermine une correspondance, l'état de l'emplacement crypté et le nom du fournisseur et du produit du logiciel. (Requires GlobalProtect app 5.2 (Nécessite l'application GlobalProtect 5.2)) Si vous souhaitez afficher l'état de chiffrement de tous les lecteurs ou chemins sur le point de terminaison, vous devez saisir manuellement **All (Tous)** comme **Encrypted Locations (Emplacements chiffrés)** lors de la création de l'objet HIP pour la catégorie **Disk Encryption (Chiffrement de disque)**. Pour vérifier si tous les lecteurs ou chemins d'accès sont chiffrés, vous devez définir les **Encrypted Locations (emplacements chiffrés)** sur **All (Tous)** et définir **State (état)** sur **Is encrypted (est chiffré)** dans la liste déroulante.
Chiffrement du disque HIP avec prise en charge de FileVault	Informations sur l'état du chiffrement du disque (chiffré ou déchiffré en fonction de l'état de FileVault) : activé, désactivé ou configuration différée. (Nécessite la version 6.4 de GlobalProtect)La fonctionnalité de chiffrement de disque GlobalProtect FileVault pour macOS

 ©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
	permet aux administrateurs de déterminer la posture du périphérique, en particulier l'état du chiffrement de disque basé sur l'état FileVault en plus du nom ou de l'emplacement du lecteur. Le rapport HIP inclut désormais des informations sur l'état du chiffrement du disque (chiffré ou déchiffré en fonction de l'état de FileVault) : activé, désactivé ou configuration différée. *Cette fonctionnalité est prise en charge sur les terminaux macOS Intel et ARM.* En vérifiant directement l'état de FileVault, cette amélioration résout les problèmes liés aux vérifications HIP non fiables causées par des lecteurs renommés par l'utilisateur ou des disques amovibles. Il garantit une vérification fiable du chiffrement du volume de démarrage, quel que soit le nom du lecteur. Le rapport HIP amélioré pour le chiffrement complet du disque contient désormais les informations suivantes : `<entry> <drive-name>état fdesetup</drive-name> </entry> <enc-state>chiffré</enc-state>`
Gestion des correctifs	Informations relatives à tous les correctifs de logiciels de gestion qui sont activés ou installés sur l'hôte et si l'hôte a détecté qu'il manquait certains correctifs ainsi que la valeur de gravité indiquée. Consultez la catégorie Patch Management (gestion des correctifs) pour les informations sur chaque valeur.
Pare-feu	Informations sur l'activation ou l'installation ou non du logiciel de pare-feu sur l'hôte.
Vérifications personnalisées	Informations au sujet de la liste de propriétés macOS (plist) collectée par l'application GlobalProtect depuis les périphériques macOS. Vous pouvez activer custom checks (vérifications personnalisées) pour collecter des données sur les périphériques macOS afin d'ordonner à l'appli de collecter des informations plist spécifiques (plist et clés plist). Le type d'informations collectées peut inclure le fait qu'une application est installée sur le périphérique, ou des attributs spécifiques ou propriétés de cette application.

Quelles sont les données que l'application GlobalProtect collecte dans Windows UWP ?

Le tableau suivant décrit les données collectées par l'application GlobalProtect sur les périphériques Windows UWP pour l'application de la politique basée sur HIP générée par le pare-feu.

 ©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
Report Generation Time (Heure de génération du rapport)	Date et heure auxquelles le rapport HIP a été généré.
User name (Nom d'utilisateur)	Le nom d'utilisateur qui est utilisé pour se connecter au VPN.
User IP Address (Adresse IP de l'utilisateur)	L'adresse IP du périphérique Windows UWP de l'utilisateur.
Machine Name (Nom de la machine)	Nom de l'hôte et numéro de série du périphérique Windows UWP.
Domain (Domaine)	Le champ est vide dans les périphériques Windows UWP.
SYSTÈME D'EXPLOITATION	Nom de l'application et le nom du fournisseur de l'OS cible.
Host ID (ID d'hôte)	L'ID unique que GlobalProtect affecte afin d'identifier l'hôte. La valeur de l'ID de l'hôte est le GUIDE sur les périphériques Windows UWP.
Client version (Version du client)	Numéro de version de l'application GlobalProtect actuellement installée.
Network interface (Interface réseau)	Les paramètres suivants sont identifiés pour l'interface du réseau : • **Interface**—Type de l'interface de réseau détectée sur le périphérique Windows UWP. • **MAC Address (Adresse MAC)**—L'adresse MAC est l'identifiant unique du matériel attribué à chaque interface du réseau sur le périphérique Windows UWP. • **IP Address (Adresse IP)**—L'adresse IP attribuée à chaque interface de réseau sur le périphérique Windows UWP.

Quelles sont les données que l'application GlobalProtect collecte sur Android ?

Le tableau suivant décrit les données collectées par l'application GlobalProtect sur les périphériques Android pour l'application de la politique basée sur HIP générée par le pare-feu.

L'application GlobalProtect pour Android sur un Chromebook utilise les mêmes attributs de rapport HIP.

 ©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
Report Generation Time (Heure de génération du rapport)	Date et heure auxquelles le rapport HIP a été généré.
User name (Nom d'utilisateur)	Le nom d'utilisateur qui est utilisé pour se connecter au VPN.
User IP Address (Adresse IP de l'utilisateur)	L'adresse IP du périphérique Android de l'utilisateur.
Machine Name (Nom de la machine)	Nom de l'hôte et numéro de série du périphérique Android.
Domain (Domaine)	Le champ est vide dans les périphériques Android.
Numéro de série	Numéro de série du périphérique Android.
Géré	Valeur qui indique si le périphérique Android est géré. Si cette valeur est réglée sur **Yes (oui)**, le périphérique est géré. Si cette valeur est réglée sur No (non), le périphérique n'est pas géré.
SYSTÈME D'EXPLOITATION	Nom de l'application et le nom du fournisseur de l'OS cible.
Host ID (ID d'hôte)	La chaîne alphanumérique unique d'une longueur de 16 caractères affectée par GlobalProtect pour identifier l'hôte. La valeur de l'ID de l'hôte est l'ID Android sur les périphériques Android.
Client version (Version du client)	Numéro de version de l'application GlobalProtect actuellement installée.
WiFi SSID	Informations spécifiques au sujet de la connectivité du réseau comme **WiFi SSID** sur les périphériques Android.
Network interface (Interface réseau)	Les paramètres suivants sont identifiés pour l'interface du réseau : • **Interface**—Type de l'interface de réseau détectée sur le périphérique Android. • **MAC Address (Adresse MAC)**—L'adresse MAC est l'identifiant unique du matériel attribué à chaque interface du réseau sur le périphérique Android. • **IP Address (Adresse IP)**—L'adresse IP attribuée à chaque interface de réseau sur le périphérique Android.

©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
Périphérique mobile	Informations concernant le mobile device (périphérique mobile), notamment le nom du périphérique, le domaine de connexion, le système d'exploitation, la version de l'application et le réseau auquel le périphérique est connecté.
Étiquettes	Étiquettes pour vous permettre de faire correspondre aux autres attributs fondés sur MDM.
Device Compliance (conformité du périphérique)	L'attribut **Rooted/Jailbroken (ancré/débridé)** est utilisé pour déterminer le statut de conformité du périphérique Android qui a été ancré ou débridé pour obtenir des privilèges administratifs. Les politiques de sécurité peuvent être supprimées ou contournées sur le système d'exploitation depuis un périphérique compromis.
MDM Attributes (attributs MDM)	Lorsque vous intégrez votre déploiement GlobalProtect avec un fournisseur MDM, l'application GlobalProtect pour les périphériques Android peut obtenir les attributs de données et étiquettes suivants du système MSDM : • **udid** Unique device identifier (UDID ; Identificateur de périphérique unique) du périphérique Android. • **managed-by-mdm** : Valeur qui indique si le périphérique Android est géré. Si cette valeur est réglée sur **Yes (oui)**, le périphérique Android est géré. Si cette valeur est réglée sur **No (non)**, le périphérique Android n'est pas géré. • **tag (étiquette)** : Étiquettes pour vous permettre de faire correspondre aux autres attributs fondés sur MDM. • **compliance (conformité)** : État de conformité qui indique si le périphérique Android est conforme aux politiques de conformité que vous avez définies. • **ownership (appartenance)** : Catégorie d'appartenance de l'appareil (par exemple, **Employee Owned (appartient à l'employé)**). Cette valeur est annexée à l'attribut **Tag (Étiquette)** indiqué dans le rapport HIP.

Quelles sont les données que l'application GlobalProtect collecte sur iOS ?

Le tableau suivant décrit les données collectées par l'application GlobalProtect sur les périphériques iOS pour l'application de la politique basée sur HIP générée par le pare-feu.

Attribut de rapport HIP	Description
Report Generation Time (Heure de génération du rapport)	Date et heure auxquelles le rapport HIP a été généré.

 ©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
User name (Nom d'utilisateur)	Le nom d'utilisateur qui est utilisé pour se connecter au VPN.
User IP Address (Adresse IP de l'utilisateur)	L'adresse IP du périphérique iOS de l'utilisateur.
Nom de la machine	Nom du périphérique attribué par l'utilisateur + identifierForVendor Le nom du périphérique attribué par l'utilisateur sera reporté en fonction de la version iOS du périphérique. • Dans iOS 15 et versions antérieures, la propriété name renvoie le nom du périphérique (par exemple, « iPhone d'Adam »). • Dans iOS 16 et versions ultérieures, la propriété name renvoie un nom de périphérique générique par défaut (par exemple, « iPhone »).
Domaine	Le champ est vide dans les périphériques iOS.
Numéro de série	Le champ est vide dans les périphériques iOS.
Géré	Valeur qui indique si le périphérique iOS est géré. Si cette valeur est réglée sur **Yes (oui)**, le périphérique est géré. Si cette valeur est réglée sur No (non), le périphérique n'est pas géré.
SYSTÈME D'EXPLOITATION	Nom de l'application et le nom du fournisseur de l'OS cible.
Host ID (ID d'hôte)	ID unique que GlobalProtect affecte afin d'identifier l'hôte. La valeur de l'ID de l'hôte est UDID sur les périphériques iOS.
Client version (Version du client)	Numéro de version de l'application GlobalProtect actuellement installée.
WiFi SSID	Informations au sujet de la connectivité du réseau comme **WiFi SSID** sur les périphériques iOS.
Network interface (Interface réseau)	Les paramètres suivants sont identifiés pour l'interface du réseau : • **Interface**—Type de l'interface de réseau détectée sur le périphérique iOS. • **MAC Address (Adresse MAC)**—L'adresse MAC est l'identifiant unique du matériel attribué à chaque interface du réseau sur le périphérique iOS.

©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
	• **IP Address (Adresse IP)**—L'adresse IP attribuée à chaque interface de réseau sur le périphérique iOS.
Périphérique mobile	Informations concernant le mobile device (périphérique mobile), notamment le nom du périphérique, le domaine de connexion, le système d'exploitation, la version de l'application et le réseau auquel le périphérique est connecté.
Device Compliance (conformité du périphérique)	Les attributs suivants sont utilisés pour déterminer le statut de conformité du périphérique iOS : • **Rooted/Jailbroken (ancré/débridé)** : Statut sur le périphérique iOS qui a été ancré ou débridé pour obtenir des privilèges administratifs. Les politiques de sécurité peuvent être supprimées ou contournées sur le système d'exploitation depuis un périphérique compromis. • **Disk Encryption Not Set (Cryptage du disque non défini)** : Statut sur le périphérique iOS qui est activé pour le cryptage du disque. • **Passcode Not Set (Code non défini)** : Statut sur le périphérique iOS qui n'est pas défini sur un code. • **Has Malware (contient un malware)** : statut sur le périphérique iOS qui a des applications infectées par un malware installé.
MDM Attributes (attributs MDM)	Lorsque vous intégrez votre déploiement GlobalProtect avec un fournisseur MDM, l'application GlobalProtect pour les périphériques iOS peut obtenir les attributs de données et étiquettes suivants du système MSDM : • **udid** Unique device identifier (UDID ; Identificateur de périphérique unique) du périphérique iOS. • **managed-by-mdm** : Valeur qui indique si le périphérique iOS est géré. Si cette valeur est réglée sur **Yes (oui)**, le périphérique iOS est géré. Si cette valeur est réglée sur **No (non)**, le périphérique iOS n'est pas géré. • **tag (étiquette)** : Étiquettes pour vous permettre de faire correspondre aux autres attributs fondés sur MDM. • État de conformité qui indique si le périphérique iOS est conforme aux politiques de conformité que vous avez définies. • **ownership (appartenance)** : Catégorie d'appartenance du périphérique iOS (par exemple, **Employee Owned (appartient à l'employé)**). Cette valeur est annexée à l'attribut **Tag (Étiquette)** indiqué dans le rapport HIP.

 ©2026 Palo Alto Networks, Inc.

Quelles sont les données que l'application GlobalProtect collecte sur Linux ?

Le tableau suivant décrit les données collectées par l'application GlobalProtect sur les périphériques LINUX pour l'application de la politique basée sur HIP générée par le pare-feu :

Attribut de rapport HIP	Description
Nom d'utilisateur	Le nom d'utilisateur qui est utilisé pour se connecter au VPN.
Adresse IP	L'adresse IP du périphérique Linux de l'utilisateur.
Generate Time (heure de génération)	Date et heure auxquelles le rapport HIP a été généré.
Infos sur l'hôte	Activez une ou plusieurs des options suivantes pour configurer les informations sur l'hôte : • **Managed (géré)** : Valeur qui indique si le périphérique Linux est géré. Si cette valeur est réglée sur **Yes (oui)**, le périphérique est géré. Si cette valeur est réglée sur No (non), le périphérique n'est pas géré. • **Serial Number (numéro de série)** : Numéro de série du périphérique Linux. • **Client Version (version client)** : Numéro de version de l'application GlobalProtect actuellement installée. • **OS** : nom d'application du système d'exploitation cible que vous souhaitez faire correspondre. • **OS Vendor (Fournisseur du système d'exploitation)** : nom du fournisseur du système d'exploitation cible que vous souhaitez faire correspondre. • **Domain (Domaine)** : le nom de domaine du périphérique Linux. • **Host Name (Nom de l'hôte)** : le nom de domaine du périphérique Linux. • **Host ID (ID de l'hôte)** : l'ID unique que GlobalProtect affecte afin d'identifier l'hôte. La valeur de l'ID d'hôte est l'identifiant de périphérique unique du produit (UUID) sur les périphériques Linux.
Network interface (Interface réseau)	Les paramètres suivants sont identifiés pour l'interface du réseau : • **Interface** : type d'interface réseau détecté sur le périphérique Linux. • **MAC Address (adresse MAC)**—L'adresse MAC est l'identifiant unique du matériel attribué à chaque interface du réseau sur le périphérique Linux.

©2026 Palo Alto Networks, Inc.

Attribut de rapport HIP	Description
	• **IP Address (adresse IP)** :L'adresse IP attribuée à chaque interface de réseau sur le périphérique Linux.
Anti-logiciels malveillants	Informations relatives à tous les logiciels antivirus ou anti-espion qui sont activés ou installés sur le périphérique, si la protection antivirus ou anti-espion en temps réel activée sur l'hôte, la version des définitions de virus, le dernier temps de balayage et le nom du fournisseur et du produit.
Sauvegarde du disque	Informations relatives au statut du disque de sauvegarde du périphérique telles que indiquer si logiciel de sauvegarde de disque est installé sur l'hôte, le dernier temps de balayage, le nom du fournisseur et du produit du logiciel.
Cryptage du disque	Informations au sujet du statut de cryptage du périphérique telle que indiquer si le logiciel de cryptage est installé sur l'hôte, le disque ou le chemin à vérifier pour que le cryptage du disque détermine une correspondance, l'état de l'emplacement crypté et le nom du fournisseur et du produit du logiciel. (Requires GlobalProtect app 5.2 (Nécessite l'application GlobalProtect 5.2)) Si vous souhaitez afficher l'état de chiffrement de tous les lecteurs ou chemins sur le point de terminaison, vous devez saisir manuellement **All (Tous)** comme **Encrypted Locations (Emplacements chiffrés)** lors de la création de l'objet HIP pour la catégorie **Disk Encryption (Chiffrement de disque)**. Pour vérifier si tous les lecteurs ou chemins d'accès sont chiffrés, vous devez définir les **Encrypted Locations (emplacements chiffrés)** sur **All (Tous)** et définir **State (état)** sur **Is encrypted (est chiffré)** dans la liste déroulante.
Pare-feu	Informations sur l'activation ou l'installation ou non du logiciel de pare-feu sur l'hôte.
Gestion des correctifs	Informations relatives à tous les correctifs de logiciels de gestion qui sont activés ou installés sur l'hôte et si l'hôte a détecté qu'il manquait certains correctifs ainsi que la valeur de gravité indiquée. Consultez la catégorie Patch Management (gestion des correctifs) pour les informations sur chaque valeur.
Vérifications personnalisées	Informations sur la liste des processus collectées par l'application GlobalProtect à partir des appareils Linux. Vous pouvez activer des custom checks (contrôles personnalisés) pour collecter des données à partir d'appareils Linux afin de demander à l'application de collecter des informations spécifiques pouvant inclure si une application est installée sur l'appareil, ou des attributs ou propriétés spécifiques de cette application.

 ©2026 Palo Alto Networks, Inc.

Comment la passerelle utilise-t-elle les informations sur l'hôte pour la mise en œuvre des politiques ?

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pendant que l'application récupère les informations indiquant les informations qui doivent être collectées dans la configuration de client téléchargée depuis le portail, vous définissez les attributs de l'hôte que vous souhaitez surveiller et/ou utiliser pour la mise en œuvre d'une politique en créant des objets HIP et des profils HIP sur la ou les passerelles :

- **Les objets HIP** : les critères de correspondance utilisés pour filtrer les informations sur l'hôte que vous souhaitez utiliser pour mettre en œuvre la politique à partir des données brutes signalées par l'application. Par exemple, alors que les données brutes sur l'hôte peuvent inclure des informations sur plusieurs modules antivirus installés sur le point de terminaison, vous n'êtes intéressé que par une application particulière dont vous avez besoin au sein de votre entreprise. Dans ce cas, créez un objet HIP qui doit correspondre à l'application spécifique que vous souhaitez mettre en œuvre.

  Pour définir les objets HIP dont vous avez besoin, vous devez déterminer comment vous allez utiliser les informations collectées sur l'hôte pour mettre en œuvre la stratégie. N'oubliez pas que les objets HIP forment simplement des blocs qui vous permettent de créer les profils HIP utilisés dans vos politiques de sécurité. Par conséquent, vous voudrez peut-être garder vos objets simples, en fonction d'une chose, comme la présence d'un type particulier de logiciel requis, l'appartenance à un domaine spécifique ou la présence d'un OS de terminaison spécifique. Ce faisant, vous avez la souplesse nécessaire pour créer une stratégie HIP enrichie très granulaire (et très puissante).
- **Profils HIP** : il s'agit d'une collecte d'objets HIP qui sont évalués ensemble, pour la surveillance ou la mise en œuvre des politiques de sécurité. Lors de la création de profils HIP, vous pouvez combiner des objets HIP précédemment créés (ainsi que d'autres profils HIP) à l'aide d'une logique booléenne, ainsi, lorsqu'un flux de trafic est évalué en fonction d'un profil HIP, il est mis en correspondance ou ou non. En cas de correspondance, la règle de politique correspondante est mise en œuvre. S'il n'y a pas de correspondance, le flux est évalué en fonction de la règle suivante, comme avec tout autre critère de correspondance de politique.

Contrairement au journal de trafic, qui créé une entrée de journal uniquement s'il existe une correspondance de politique, le journal des correspondances HIP génère une entrée dès que les données brutes soumises par une application correspondent à un objet HIP et/ou un profil HIP que vous avez définis. Cela fait du journal des correspondances HIP une ressource acceptable pour surveiller l'état des points de terminaison sur votre réseau au fil du temps, avant d'associer vos profils HIP aux politiques de sécurité, afin de vous aider à déterminer exactement les politiques que vous devez mettre en œuvre. Pour plus d'informations sur la création d'objets HIP et les profils HIP, consultez la section Configurez l'application de la stratégie basée sur HIP et utilisez-les comme critères de correspondance.

 ©2026 Palo Alto Networks, Inc.

De quelle manière les utilisateurs savent-ils si leurs systèmes sont conformes ?

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Par défaut, aucune information n'est fournie aux utilisateurs finaux sur les décisions de politique qui ont été prises à l'issue de la mise en œuvre d'une règle de sécurité activée par HIP. Toutefois, vous pouvez activer cette fonctionnalité en configurant les messages de notification HIP à afficher lorsqu'une correspondance de profil HIP particulier a été trouvée et/ou lorsqu'aucune correspondance n'a été trouvée.

La décision de savoir quand afficher un message (c'est-à-dire, s'il faut l'afficher lorsque la configuration de l'utilisateur correspond à un profil HIP dans la stratégie ou lorsqu'elle ne correspond pas) dépend en grande partie de votre politique et de quel point HIP (ou non-correspondance) signifie pour l'utilisateur. En effet, est-ce qu'une correspondance signifie qu'ils ont un accès complet à vos ressources réseau ? Ou cela signifie-t-il qu'ils ont un accès limité en raison de problèmes liés à la non-conformité ?

Par exemple, examinez les scénarios suivants :

- Vous créez un profil HIP qui correspond si l'antivirus d'entreprise et les progiciels anti-logiciel espion requis *ne sont pas* installés. Dans ce cas, vous pourriez créer un message de notification HIP pour les utilisateurs qui correspondent au profil HIP et leur indiquer qu'ils doivent installer le logiciel (et, facultativement, fournir un lien vers le partage de fichiers d'où ils peuvent accéder au programme d'installation pour le logiciel correspondant).
- Vous créez un profil HIP qui correspond si ces mêmes applications *sont* installées. Dans ce cas, vous pourriez créer le message destiné aux utilisateurs qui ne correspondent pas au profil, et les rediriger vers l'emplacement du module installé.

Reportez-vous à la section Configurez l'application de la stratégie basée sur HIP pour obtenir plus de détails sur la création d'objets et de profils HIP, et sur leur utilisation dans la définition de messages de notification HIP.

Comment obtenir une visibilité de l'état des points de terminaison ?

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Lorsqu'un point de terminaison se connecte à GlobalProtect, l'application présente ses données HIP à la passerelle. La passerelle utilise ensuite ces données pour déterminer les objets et/ou les profils HIP auxquels l'hôte correspond. Pour chaque correspondance, il génère une entrée

 ©2026 Palo Alto Networks, Inc.

dans le log de correspondances HIP. Contrairement au journal de trafic, qui créé une entrée de journal uniquement s'il existe une correspondance de politique, le journal des correspondances HIP génère une entrée dès que les données brutes soumises par une application correspondent à un objet HIP et/ou un profil HIP que vous avez définis. Cela fait du journal des correspondances HIP une ressource acceptable pour surveiller l'état des points de terminaison sur votre réseau au fil du temps, avant d'associer vos profils HIP aux politiques de sécurité, afin de vous aider à déterminer exactement les politiques que vous devez mettre en œuvre.

Étant donné qu'un log de correspondances HIP n'est généré que lorsque l'état de l'hôte correspond à un objet HIP que vous avez créé, pour obtenir une visibilité complète de l'état du point de terminaison, vous devrez peut-être créer plusieurs objets HIP afin de journaliser les correspondances HIP de points de terminaison conformes à un état particulier (à des fins de mise en œuvre de politiques de sécurité) ainsi que de points de terminaison non conformes (à des fins de visibilité). Par exemple, supposons que vous souhaitez empêcher un point de terminaison sur lequel aucun logiciel antivirus ou anti-espion n'est installé de se connecter au réseau. Dans ce cas, créez un objet HIP qui correspond aux hôtes sur lesquels un logiciel antivirus ou anti-espion spécifique est installé. En incluant cet objet dans un profil HIP et en l'associant à la règle de politique de sécurité qui autorise l'accès depuis votre zone VPN, vous vous assurez que seuls les hôtes protégés par un logiciel antivirus ou anti-espion peuvent se connecter.

Dans le présent exemple, vous ne seriez pas en mesure d'afficher les points de terminaison qui respectent cette exigence dans le journal de correspondance HIP. Si vous souhaitez consulter un journal des points de terminaison sur lesquels aucun logiciel antivirus ou anti-espion n'est installé afin de pouvoir suivre ces utilisateurs, vous pouvez également créer un objet HIP correspondant à la condition telle qu'un logiciel antivirus ou anti-espion n'est pas installé. Cet objet n'étant requis qu'à des fins de journalisation, vous ne devez pas nécessairement l'ajouter à un profil HIP ou l'associer à une règle de politique de sécurité.

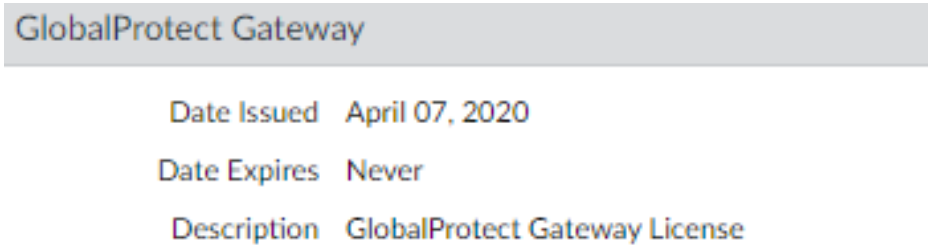
Configurer la mise en œuvre des politiques basées sur HIP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour autoriser l'utilisation des informations sur l'hôte pour la mise en œuvre d'une politique, vous devez exécuter les étapes suivantes. Consultez Quelles sont les données que l'application GlobalProtect collecte sur chaque système d'exploitation ? pour plus de détails sur les données qui sont collectées pour le périphérique.

 ©2026 Palo Alto Networks, Inc.

1. Vérifiez que les licences sont appropriées pour les vérifications HIP.



Pour utiliser la fonction HIP, vous devez acheter et installer une licence d'abonnement à GlobalProtect sur chaque passerelle qui effectuera des vérifications HIP. Pour vérifier le statut de vos licences sur chaque portail et passerelle, sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.

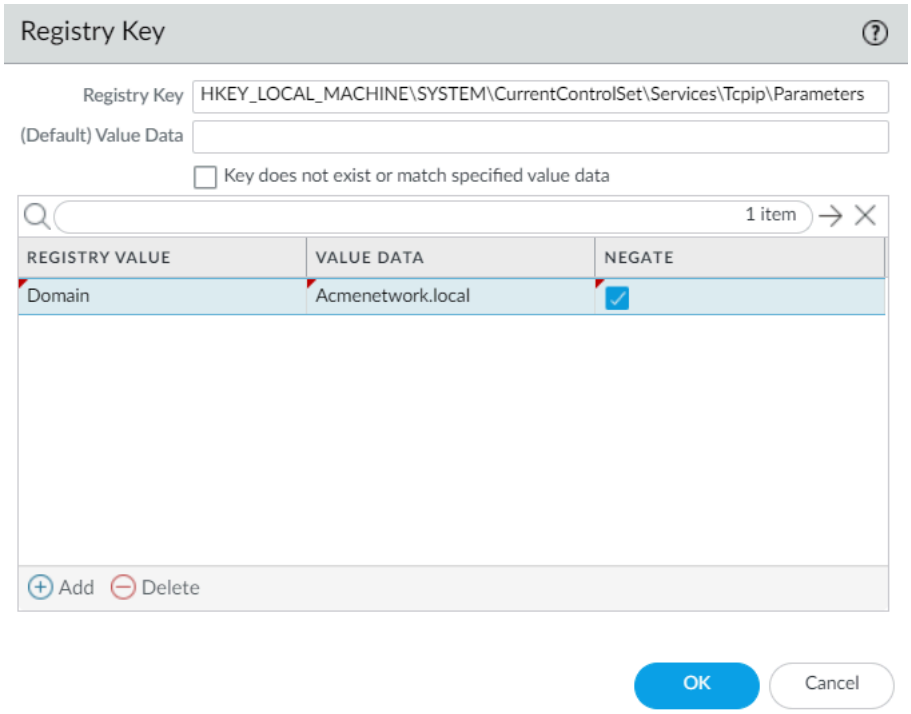
Contactez les ingénieurs commerciaux ou le revendeur de Palo Alto Networks si vous ne disposez pas des licences requises. Pour plus d'informations sur les licences, consultez À propos des Licences GlobalProtect.

2. (Facultatif) Définissez des informations personnalisées sur l'hôte que vous souhaitez que l'application collecte. Par exemple, si vous disposez d'applications non incluses dans les listes de fournisseurs et/ou de produits, qui sont requises pour la création d'objets HIP, vous

 ©2026 Palo Alto Networks, Inc.

pourriez créer une vérification personnalisée qui vous permet de déterminer si l'application est installée (a une clé de registre ou Plist correspondante) ou est en cours d'exécution.

Les étapes 2 et 3 présument que vous avez déjà configuré un portail GlobalProtect. Si vous n'avez pas encore configuré votre portail, reportez-vous à la section Paramétrer l'accès au portail GlobalProtect *pour des instructions.*



Si vous utilisez Strata Cloud Manager (NGFW), alors :

1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres d'application d'agent)**.
2. Sur la page Ajouter les paramètres d'application d'agent, sous **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Custom Checks (Vérifications personnalisées)**, modifiez les vérifications personnalisées.

Si vous utilisez Strata Cloud Manager (Prisma Access), alors :

1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs**

 ©2026 Palo Alto Networks, Inc.

mobiles) > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect).** > **App Settings (Paramètres de l'application)**.

2. Sélectionnez **Default (Par défaut)** > **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Custom Checks (Vérifications personnalisées)**.
   1. Sur le pare-feu qui héberge votre portail GlobalProtect (ou sur Panorama), sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
   2. Sélectionnez la configuration du portail que vous souhaitez modifier.
   3. À l'onglet **Agent**, sélectionnez la configuration de l'agent à laquelle vous souhaitez ajouter une vérification HIP personnalisée, ou **Add (Ajoutez)**-en une nouvelle.
   4. Sélectionnez **HIP Data Collection (Collecte de données HIP)**, puis activez l'option permettant la **Collect HIP Data (Collecte de données HIP)**.
   5. Sous **Custom Checks (Vérifications personnalisées)**, définissez les données suivantes que vous souhaitez recueillir auprès des hôtes exécutant cette configuration de l'agent :
      - **Pour recueillir des informations sur des clés de Registre spécifiques** : Sous l'onglet **Windows**, **Add (Ajoutez)** le nom d'une **Registry Key (Clé de registre**) pour laquelle collecter des données dans la zone des **Registry Key (clés de registre)**. Pour restreindre la collecte de données à une **Registry Value (Valeur de Registre)** spécifique, **Add (Ajoutez)**, puis définissez la valeur ou les valeurs de registre spécifiques. Cliquez sur **OK** pour enregistrer les paramètres.
      - **Pour collecter les informations sur les processus en cours d'exécution** : Sélectionnez l'onglet approprié (**Windows**, **Mac**, ou **Linux**) puis **Add (Ajouter)** un processus à la **Process List (Liste des processus)**. Saisissez le nom du processus sur lequel vous souhaitez que l'application collecte des informations. Vous pouvez éventuellement Configurer la correction du processus HIP pour résoudre les problèmes qui surviennent lors de la vérification du processus.
      - **Pour collecter les informations sur les listes de propriétés spécifique** : À l'onglet **Mac**, **Add (Ajoutez)** la **Plist** pour laquelle collecter des données. Pour restreindre la collecte de données à des valeurs clés précises, **Add (Ajoutez)** les valeurs des **Key (Clés)**. Cliquez sur **OK** pour enregistrer les paramètres.
   6. S'il s'agit d'une nouvelle configuration de l'agent, définissez les configurations de l'agent GlobalProtect selon vos besoins.
   7. Cliquez sur **OK** pour enregistrer la configuration.
   8. **Validez** les modifications.

3. (Facultatif) Excluez des catégories de la collecte.

Si vous utilisez Strata Cloud Manager (NGFW), alors :

1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device**

 ©2026 Palo Alto Networks, Inc.

(Périphérique) > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres d'application d'agent)**.

2. Sur la page Ajouter les paramètres d'application d'agent, sélectionnez **HIP Data Collecction (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Exclude Categories (Exclure les catégories)**.

Si vous utilisez Strata Cloud Manager (Prisma Access), alors :

1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)**.
2. Sélectionnez **Default (Par défaut** > **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Exclude Categories (Exclure les catégories)**.
    1. Sur le pare-feu qui héberge votre portail GlobalProtect (ou sur Panorama), sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
    2. Sélectionnez la configuration du portail que vous souhaitez modifier.
    3. Sous l'onglet **Agent**, sélectionnez la configuration de l'agent à partir de laquelle exclure les catégories, ou **Add (ajoutez)**-en une nouvelle.
    4. Sélectionnez **Data Collection (Collecte de données)**, puis vérifiez que l'option **Collect HIP Data (Collecter des données HIP)** est activée.
    5. Sous **Exclude Categories (Exclure les catégories)**, **Add (Ajoutez)** une nouvelle catégorie à exclure.
    6. Dans la liste déroulante, sélectionnez la **Category (Catégorie)** que vous souhaitez exclure.
    7. (Facultatif) Si vous souhaitez exclure des fournisseurs et/ou des produits spécifiques dans la catégorie sélectionnée au lieu d'exclure la catégorie entière, cliquez sur **Add (Ajouter)**. Dans la boîte de dialogue Edit Vendor (Modifier le fournisseur), sélectionnez le **Vendor (Fournisseur)** que vous souhaitez exclure, puis cliquez sur **Add (Ajouter)** pour exclure des produits spécifiques de ce fournisseur. Lorsque vous avez fini de définir ce fournisseur, cliquez sur **OK**. Vous pouvez ajouter de multiples fournisseurs et produits à la liste d'exclusion. Vous pouvez également Configurer les exceptions HIP pour la gestion des correctifs :
    8. Répétez les étapes 5 à 7 pour chaque catégorie que vous souhaitez exclure.
    9. S'il s'agit d'une nouvelle configuration de l'agent, définissez les configurations de l'agent GlobalProtect selon vos besoins.
    10. Cliquez sur **OK** pour enregistrer la configuration.
    11. **Validez** les modifications.

4. Créez les objets HIP pour filtrer les données brutes d'hôte collectées par l'application.

Pour définir les objets HIP dont vous avez besoin, vous devez déterminer comment vous allez utiliser les informations collectées sur l'hôte pour mettre en œuvre la stratégie. N'oubliez pas que les objets HIP forment simplement des blocs qui vous permettent de créer les profils HIP utilisés dans vos politiques de sécurité. Par conséquent, vous voudrez peut-être garder vos objets simples, en fonction d'un élément, comme la présence d'un type particulier de logiciel

 ©2026 Palo Alto Networks, Inc.

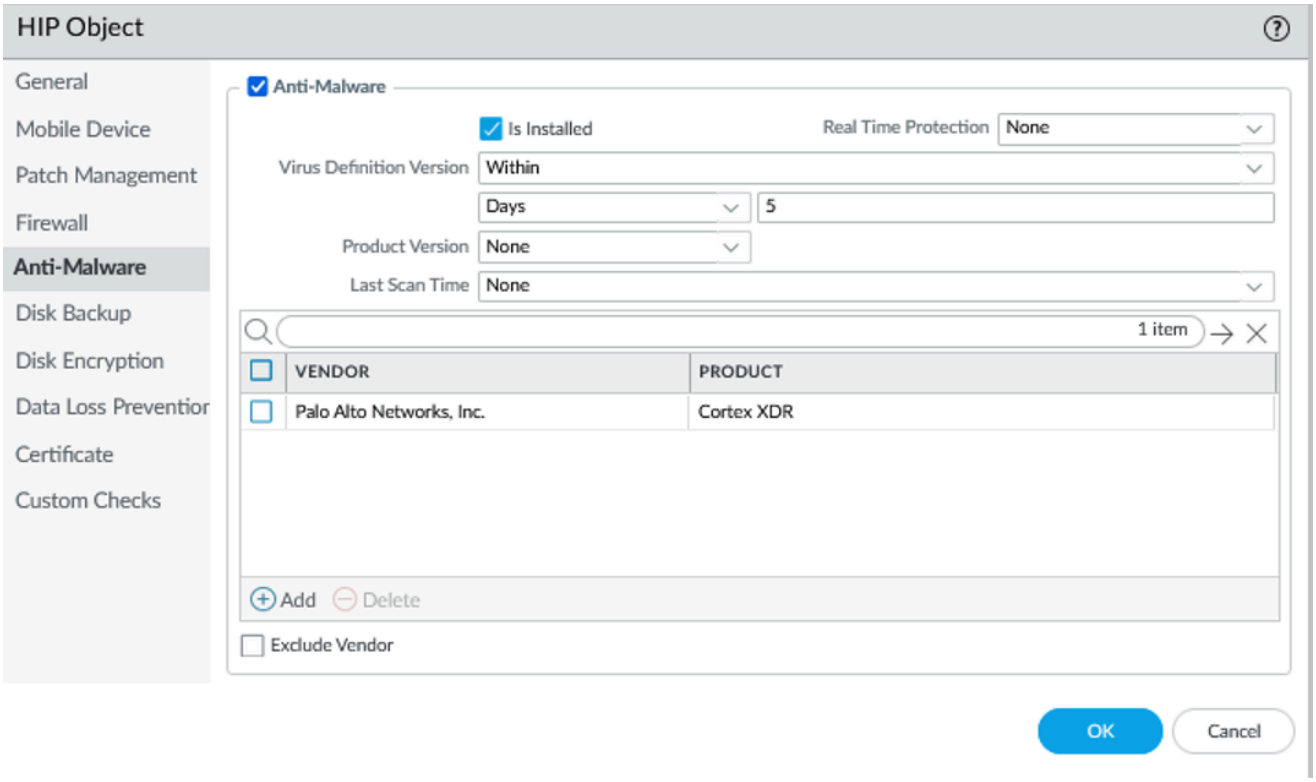
requis, l'appartenance à un domaine spécifique ou la présence d'un système d'exploitation spécifique. Ce faisant, vous aurez la souplesse nécessaire pour créer une stratégie HIP enrichie très granulaire (et très puissante).

Pour plus d'informations sur un champ ou une catégorie HIP spécifique, consultez la section Aide en ligne.

1. Ajoutez un nouvel objet HIP, effectuez l'une des actions suivantes :
   - Sur le pare-feu qui héberge vos passerelles GlobalProtect (ou sur Panorama si vous envisagez de partager les objets HIP entre de multiples passerelles), sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)**, puis **Add (Ajouter)** un nouvel objet HIP.
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **Objects (Objets)** > **HIP Objects (Objets HIP)** > **Add HIP Object (Ajouter un objet HIP)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Objects (Objets)** > **HIP Objects (Objets HIP)** > **Add HIP Object (Ajouter un objet HIP)**.
2. Saisissez un **Name (Nom)** pour l'objet.
3. Sélectionnez l'onglet correspondant à la catégorie d'informations sur l'hôte qui vous intéressent, puis cochez la case pour activer la mise en correspondance de l'objet avec la catégorie. Par exemple, pour créer un objet qui cherche des informations sur le logiciel anti-virus ou anti-espion, sélectionnez l'onglet **Anti-Malware (Anti-logiciels malveillants)**, puis cochez la case **Anti-Malware (Anti-logiciels malveillants)** pour activer les champs correspondants. Remplissez les champs pour définir les critères de correspondance souhaités. Par exemple, l'image suivante illustre comment créer un objet HIP qui correspondra si le logiciel antivirus AVAST est installé sur le point de terminaison, si la

 ©2026 Palo Alto Networks, Inc.

Real Time Protection (Protection en temps réel) est activée, et si des définitions de virus ont été mises à jour au cours des 5 derniers jours.



Répétez cette étape pour chaque catégorie que vous souhaitez faire correspondre dans cet objet. Pour plus d'informations, consultez le Tableau : Catégories de collecte de données.

4. (Facultatif) Configurez les étiquettes à faire correspondre à la catégorie de propriété ou à l'état de conformité du point de terminaison.

   Par exemple, vous pouvez créer une étiquette à faire correspondre aux points de terminaison appartenant aux employés, afin d'empêcher les utilisateurs d'accéder à des ressources réseau de nature délicate qui se trouvent sur leurs points de terminaison personnels.

   L'agent User-ID de Windows interroge le serveur MDM afin d'obtenir les informations suivantes :

   - État de conformité du périphérique mobile.
   - Groupe intelligent (catégorie de propriété) auquel le périphérique mobile appartient.

   L'agent User-ID convertit ces informations en des étiquettes qui sont intégrées au rapport HIP. Vous pouvez créer des objets HIP en fonction des valeurs de ces étiquettes afin d'appliquer les politiques de sécurité basées sur HIP aux points de terminaison de

 ©2026 Palo Alto Networks, Inc.

votre réseau. Pour obtenir de plus amples renseignements, reportez-vous à la section Configurer l'agent User-ID Windows pour collecter des informations d'hôte.

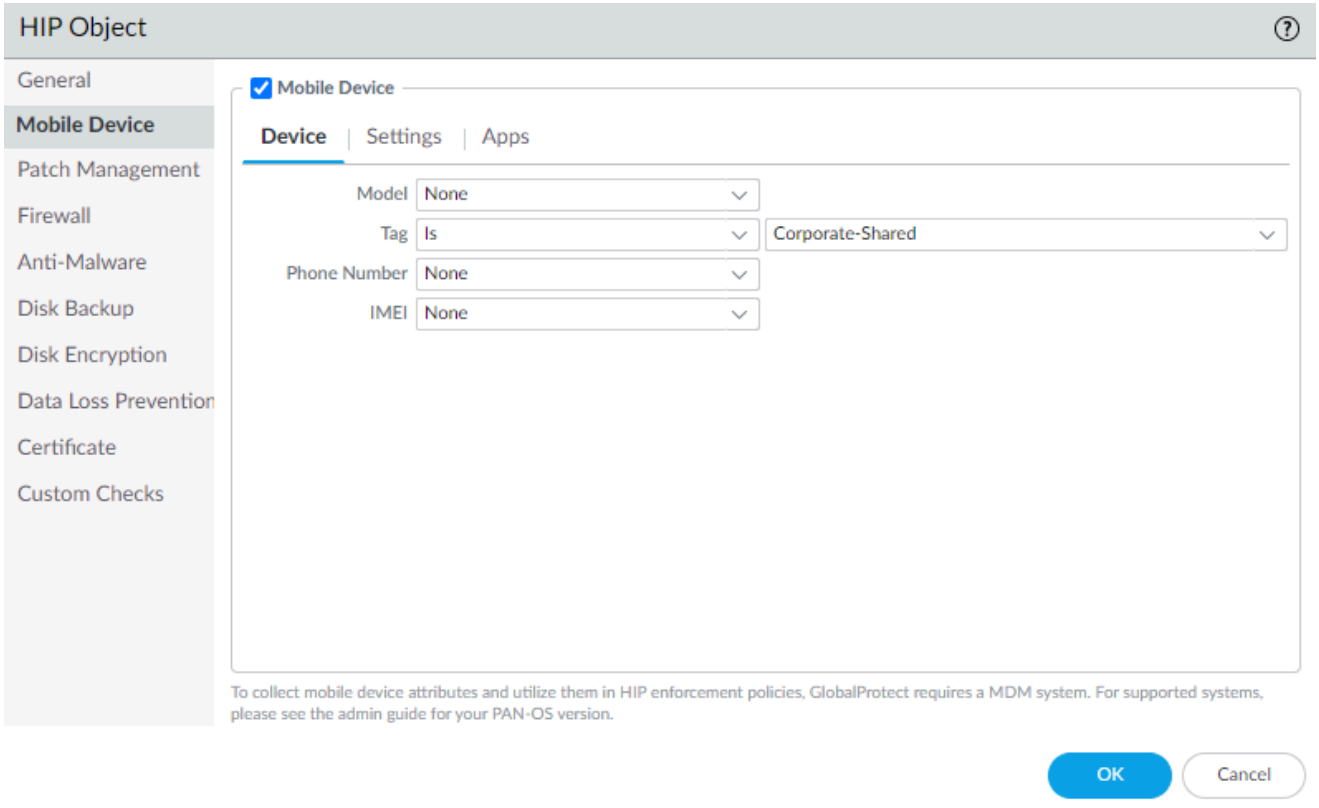
1. Cochez la case **Mobile Device (Périphérique mobile)** pour activer la configuration des paramètres du **Mobile Device (Périphérique mobile)**.
2. À l'onglet **Device (Périphérique)**, sélectionnez un opérateur de correspondance (comme **Contains (Contient)** ou **Is Not (N'est pas)**) dans la liste déroulante **Tag (Étiquette)**.
3. (Facultatif) Lorsque vous êtes invité à la faire, saisissez l'une des valeurs de catégorie de propriété suivantes :

   La catégorie de propriété indique la personne à qui le point de terminaison appartient.

   - **`Employee Owned (Appartient à l'employé)`**
   - **`Corporate-Dedicated (Dédié à l'entreprise)`**
   - **`Corporate-Shared (Partagé avec l'entreprise)`**
4. (Facultatif) Lorsque vous êtes invité à la faire, saisissez l'une des valeurs d'état de conformité suivantes :

   L'état de conformité indique si le point de terminaison est conforme aux politiques de sécurité que vous avez définies.

   - **`Compliant (Conforme)`**
   - **`NonCompliant (Non conforme)`**
   - **`NotAvailable (Indisponible)`**



 ©2026 Palo Alto Networks, Inc.

5. Cliquez sur **OK** pour enregistrer l'objet HIP.
6. Répétez ces étapes pour créer chaque objet HIP supplémentaire dont vous avez besoin.
7. **Validez** les modifications.

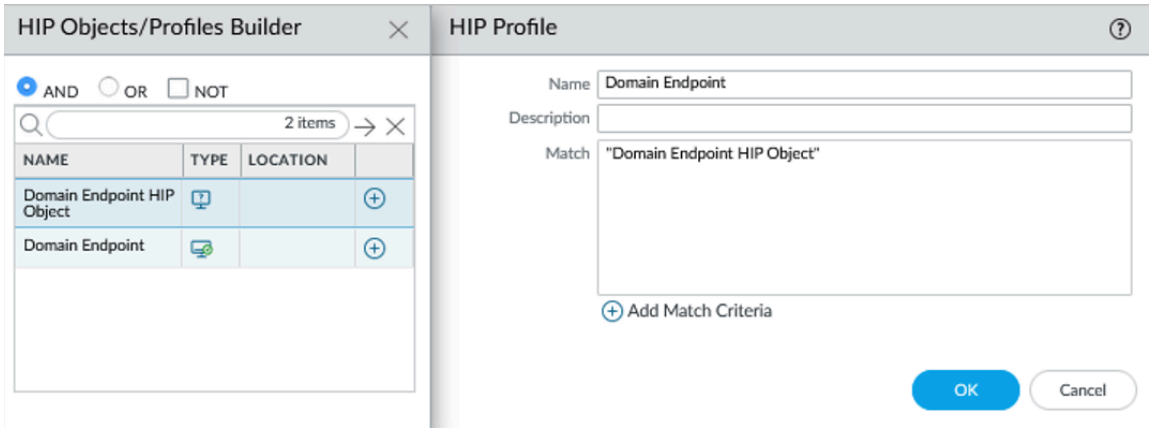
5. Créez les profils HIP que vous envisagez d'utiliser dans vos stratégies.

Lors de la création de profils HIP, vous pouvez combiner des objets HIP précédemment créés (ainsi que d'autres profils HIP) à l'aide d'une logique booléenne, notamment lorsqu'un flux de trafic est évalué en fonction d'un profil HIP auquel il correspond ou non. En cas de correspondance, la règle de politique correspondante est mise en œuvre ; sinon, le flux est évalué en fonction de la règle suivante, comme avec tout autre critère de la stratégie de correspondance.

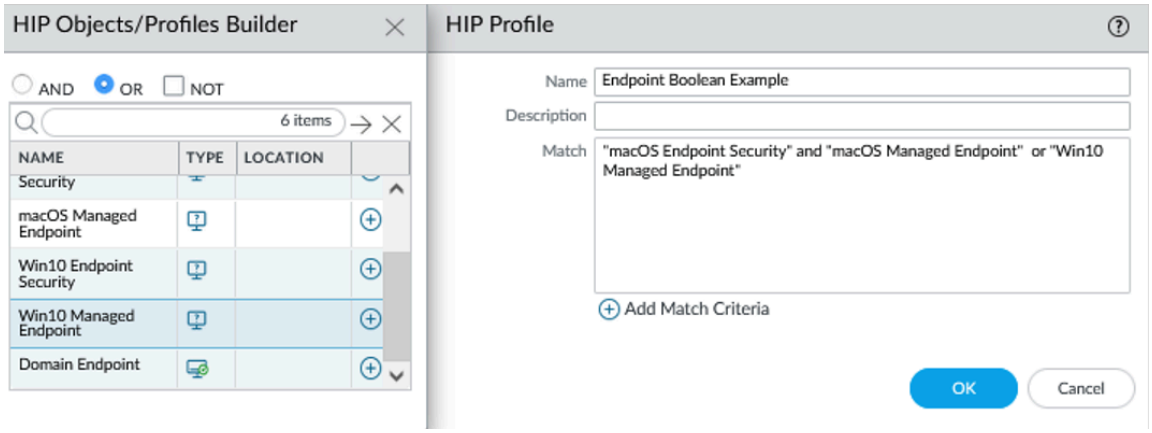
1. Ajoutez un nouveau profil HIP, effectuez l'une des actions suivantes :
   - Sur le pare-feu qui héberge vos passerelles GlobalProtect (ou sur Panorama si vous envisagez de partager les objets HIP entre de multiples passerelles), sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Profiles (Profils HIP)**, puis **Add (Ajouter)** un nouveau profil HIP.
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **Objects (Objets)** > **HIP Profiles (Profils HIP)** > **Add HIP Profile (Ajouter un profil HIP)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Objects (Objets)** > **HIP Profiles (Profils HIP)** > **Add HIP Profile (Ajouter un profil HIP)**.
2. Sur le pare-feu qui héberge vos passerelles GlobalProtect (ou sur Panorama si vous envisagez de partager les profils HIP entre de multiples passerelles), sélectionnez **Objets** > **GlobalProtect** > **Profils HIP**, puis **Ajoutez** un nouveau profil HIP.
3. Saisissez un **Name (Nom)** et une **Description** pour identifier le profil.
4. Cliquez sur **Add Match Criteria (Ajouter un critère de correspondance)** pour ouvrir le générateur de profils/d'objets HIP.
5. Sélectionnez le profil ou l'objet HIP que vous souhaitez utiliser comme critère de correspondance, puis cliquez sur l'icône d'ajout ( ) pour le déplacer vers la zone de texte **Match (Faire correspondre)** de la boîte de dialogue HIP Profile (Profil HIP). Si vous souhaitez que le profil HIP évalue l'objet comme correspondance uniquement lorsque

 ©2026 Palo Alto Networks, Inc.

le critère de l'objet n'est pas vrai pour un flux, vous devez cocher la case **NOT (NE PAS)** avant d'ajouter l'objet.



6. Continuez d'ajouter des critères de correspondance pour le profil que vous créez, en vous assurant de sélectionner la case d'option de l'opérateur booléen correspondant (**AND (ET)** ou **OR (OU)**) entre chaque ajout (et en cochant la case **NOT (NE PAS)**, le cas échéant). Le profil HIP peut contenir jusqu'à un maximum de 2048 caractères.
7. Si vous créez une expression booléenne complexe, vous devez ajouter manuellement les parenthèses aux bons endroits dans la zone de texte **Match (Faire correspondre)** pour que le profil HIP soit évalué à l'aide de la logique booléenne souhaitée. Par exemple, le profil HIP suivant correspond au trafic d'un hôte qui dispose du cryptage de disque FileVault (pour les systèmes d'exploitation macOS) ou TrueCrypt (pour les systèmes d'exploitation Windows), et appartient aussi au domaine requis et sur lequel un client antivirus Symantec est installé :



8. Lorsque vous avez ajouté tous vos critères de correspondance, cliquez sur **OK** pour enregistrer le profil.
9. Répétez ces étapes pour créer chaque profil HIP supplémentaire dont vous avez besoin.
10. **Validez** les modifications.

6. Vérifiez que les objets HIP et les profils HIP que vous avez créés correspondent à votre trafic GlobalProtect comme prévu.

   Songez à surveiller les objets et les profils HIP comme moyen de surveillance de l'état de sécurité et de l'activité des terminaux de vos hôtes. En surveillant les informations sur l'hôte dans le temps, vous pouvez mieux comprendre où se situent vos problèmes de sécurité et de

 ©2026 Palo Alto Networks, Inc.

conformité. Ces informations peuvent vous guider dans la création d'une politique utile. Pour plus de détails, voir la section Comment puis-je obtenir une visibilité de l'état des points de terminaison ?

Sur la (les) passerelle (s) que vos utilisateurs GlobalProtect utilisent pour se connecter, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **HIP match (Correspondance HIP)**. Ce journal présente toutes les correspondances identifiées par la passerelle lors de l'évaluation des données HIP brutes signalées par l'application par rapport aux objets HIP et aux profils HIP définis. Contrairement aux autres journaux, une correspondance HIP n'exige pas de correspondance de stratégie de sécurité pour l'ouverture de session.

RECEIVE TIME	SOURCE IPV4	SOURCE IPV6	SOURCE USER	MACHINE NAME	OPERATING SYSTEM	HIP	HIP TYPE
08/11 08:42:55			\casey	DESKTOP-	Windows	Domain Endpoint	profile
08/11 08:42:55			\casey	DESKTOP-	Windows	Windows Endpoint	object
08/11 08:42:37			pre-logon	DESKTOP-	Windows	Domain Endpoint	profile
08/11 08:42:36			pre-logon	DESKTOP-	Windows	Windows Endpoint	object
08/08 13:09:34			pre-logon	DESKTOP-	Windows	Domain Endpoint	profile
08/08 13:09:34			pre-logon	DESKTOP-	Windows	Windows Endpoint	object
08/08 13:07:38			pre-logon	DESKTOP-	Windows	Domain Endpoint	profile
08/08 13:07:38			pre-logon	DESKTOP-	Windows	Windows Endpoint	object
08/08 13:07:36			pre-logon	DESKTOP-	Windows	Domain Endpoint	profile
08/08 13:07:35			pre-logon	DESKTOP-	Windows	Windows Endpoint	object

7. Activez User-ID sur les zones source sur lesquelles se trouvent les utilisateurs GlobalProtect qui envoient des requêtes demandant des contrôles d'accès basés sur HIP. Vous devez activer User-ID, même si vous ne prévoyez pas d'utiliser la fonction d'identification de l'utilisateur ; sinon le pare-feu ne peut générer aucune entrée de journal de correspondances HIP.
   1. Sélectionnez **Network (Réseau)** > **Zones**.
   2. Cliquez sur le **Name (Nom)** de la zone dans laquelle vous souhaitez autoriser l'agent User-ID.
   3. **Enable User Identification (Activez l'identification de l'utilisateur)**, puis cliquez sur **OK (OK)**.

	NAME	TYPE	User-ID		
			ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS
☐	GlobalProtect	layer3	☑	any	none

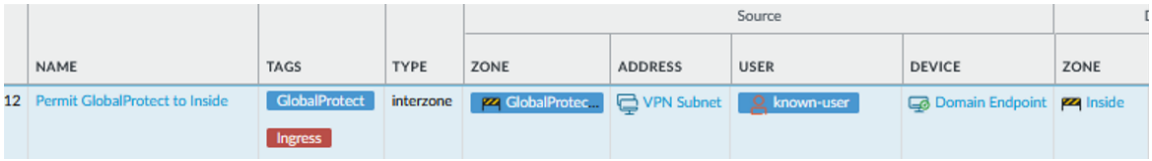
8. Créez les règles de sécurité activées par HIP sur vos passerelles.

L'idéal est de créer vos règles de sécurité et tester leur correspondance avec les flux attendus (d'après les critères source et de destination) avant d'ajouter vos profils HIP. Ainsi, vous êtes

 ©2026 Palo Alto Networks, Inc.

plus à même de déterminer l'inclusion appropriée des règles activées par HIP au sein de la stratégie.

1. Sélectionnez la règle de politique de sécurité à laquelle vous souhaitez ajouter un profil HIP. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez la règle à laquelle vous souhaitez ajouter un profil HIP.
   - Sur le pare-feu qui héberge vos passerelles GlobalProtect (ou sur Panorama), sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez la règle à laquelle vous souhaitez ajouter un profil HIP.
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > **Add Rule (Ajouter une règle)** > **Security Rule (Règle de sécurité)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > **Add Rule (Ajouter une règle)** > **Security Rule (Règle de sécurité)**.
2. Dans l'onglet **Source**, vérifiez que la **Source Zone (Zone Source)** est une zone pour laquelle vous avez activé l'User-ID.
3. Dans l'onglet **Sourcer** sous **Source Device (périphérique source)**, **Add (Ajoutez)** les **HIP Profiles (Profils HIP)** utilisés pour identifier les périphériques (vous pouvez ajouter un maximum de 63 profils HIP à une règle).
4. Cliquez sur **OK** pour enregistrer la règle.
5. **Validez** les modifications.



9. Ce sous-onglet vous permet de définir les messages de notification à afficher aux utilisateurs finaux lorsqu'une règle de sécurité dotée d'un profil HIP est mise en œuvre.

La décision relative au moment où vous souhaitez afficher un message (c'est-à-dire faut-il l'afficher lorsque la configuration de l'utilisateur correspond à un profil HIP dans la politique ou lorsqu'elle ne correspond pas), dépend en grande partie de votre politique et de la signification pour l'utilisateur d'une correspondance de profil HIP (ou non-correspondance). En effet, est-ce qu'une correspondance signifie qu'ils ont un accès complet à vos ressources réseau ? Ou cela signifie-t-il qu'ils ont un accès limité en raison de problèmes liés à la non-conformité ?

Par exemple, supposons que vous créez un profil HIP qui correspond si l'antivirus d'entreprise et les logiciels anti-spyware requis ne sont pas installés. Dans ce cas, vous pourriez créer un message de notification HIP pour les utilisateurs qui correspondent au profil HIP leur indiquant qu'ils doivent installer le logiciel. Sinon, si votre profil HIP correspond si ces

 ©2026 Palo Alto Networks, Inc.

mêmes applications sont installées, vous pouvez créer le message pour les utilisateurs qui ne correspondent pas au profil.

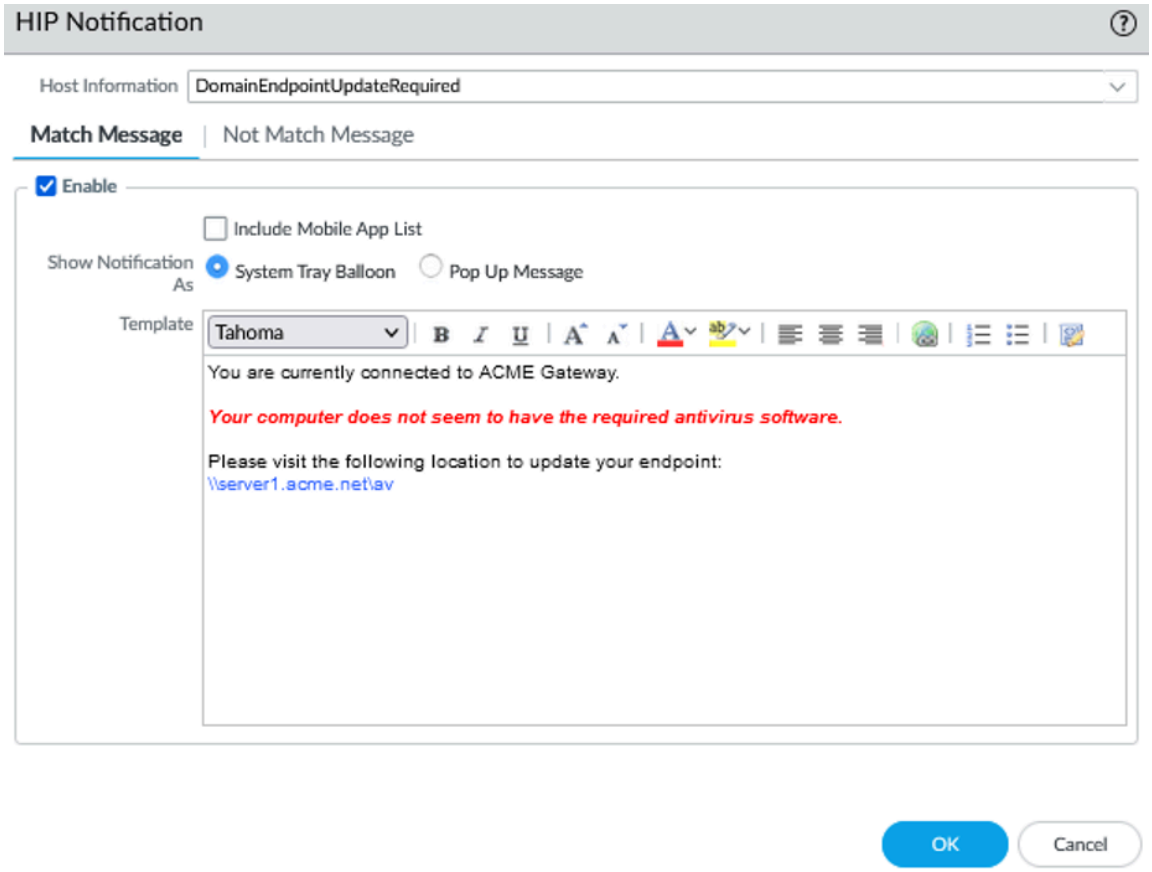
1. Créez des messages de notification HIP. Choisissez l'une des actions suivantes :
   - Sur Strata Cloud Manager (NGFW) :
     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Portals and Gateways (Portails et passerelles)** > **Gateways (Passerelles)**.
     2. Sur la page Ajouter une passerelle, sélectionnez **Advanced Settings (Paramètres avancés)** > **HIP Notifications (Notifications HIP)** > **Add HIP Notification (Ajouter une notification HIP)** et ajoutez un message de notification HIP

     .
   - Sur Strata Cloud Manager (Prisma Access) :
     1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access (Prisma Access)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **Global App Settings (Paramètres généraux de l'application)**.
     2. Sur la page Paramètres généraux, sélectionnez **Add HIP Notification (Ajouter une notification HIP)**, activez et ajoutez le message

     .
   - Sur le pare-feu qui héberge votre passerelle GlobalProtect, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**.
2. Sélectionnez la configuration de passerelle à laquelle vous souhaitez ajouter des messages de notification HIP.
3. Sélectionnez **Agent** > **HIP Notification (Notification HIP)**, puis cliquez sur **Add (Ajouter)**.
4. Sélectionnez le profil HIP auquel ce message s'applique dans la liste déroulante **Host Information (Informations sur l'hôte)**.
5. Selon que vous souhaitiez afficher le message lorsque le profil HIP correspondant est mis en correspondance ou lorsqu'il ne l'est pas, sélectionnez **Match Message (Faire correspondre le message)** ou **Not Match Message (Ne pas faire correspondre le message)**. Dans certains cas, vous pourriez créer des messages à la fois pour une correspondance et pour une non-correspondance, en fonction des objets que vous souhaitez faire correspondre et des objectifs que vous avez définis pour la stratégie.
6. **Enable (Activez)** l'option **Match Message (Faire correspondre le message)** ou **Not Match Message (Ne pas faire correspondre le message)**, puis choisissez si vous souhaitez afficher le message comme un **Pop Up Message (Message en incrustation)** ou comme une **System Tray Balloon (Bulle de la zone de notification)**.
7. Entrez le texte de votre message dans la zone **Template (Modèle)**, puis cliquez sur **OK**. La zone de texte fournit à la fois un affichage WYSIWYG du texte et un affichage HTML source, entre lesquels vous pouvez alterner à l'aide de l'icône **Source Edit (Modifier source)**. La barre d'outils fournit aussi diverses options pour le formatage de votre texte et pour la création des liens hypertextes vers des documents externes, par

 ©2026 Palo Alto Networks, Inc.

exemple un lien pour les utilisateurs directement vers l'URL de téléchargement pour un programme requis.



8. Répétez cette procédure pour chaque message que vous souhaitez définir.
9. **Validez** les modifications.

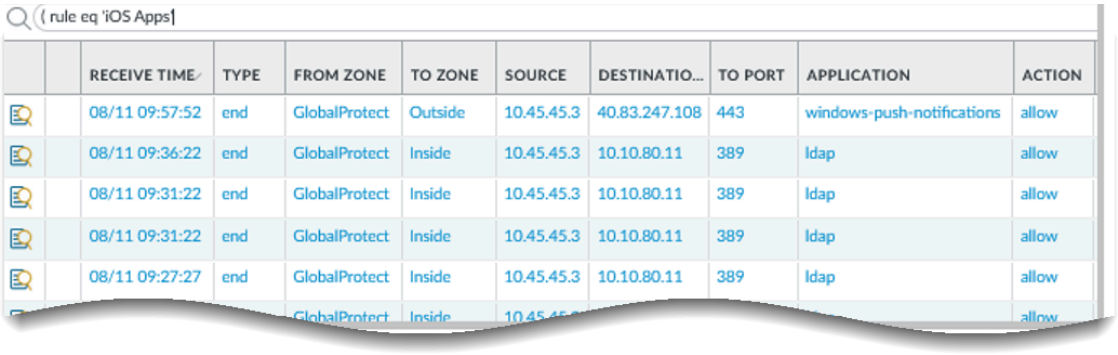
10. Vérifiez que vos profils HIP fonctionnent comme prévu.

Vous pouvez surveiller le trafic qui touche vos stratégies activées par HIP à l'aide du journal **Traffic (Trafic)** :

1. Sur le pare-feu qui héberge votre passerelle, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**.
2. Filtrez le journal pour afficher uniquement le trafic qui correspond à la règle qui contient le profil HIP que vous souhaitez surveiller. Par exemple, pour chercher le trafic qui

 ©2026 Palo Alto Networks, Inc.

correspond à une règle de sécurité nommée « Applications iOS » vous devrez saisir **(rule eq 'iOS Apps')** dans la zone de texte du filtre de la manière suivante :



Configurer les exceptions HIP pour la gestion des correctifs

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile Version de l'application GlobalProtect 6.2 ou ultérieure pour Windows, macOS, ou Linux Version de publication de contenu 8699-7991 ou ultérieure

Utilisez la procédure suivante pour configurer l'application GlobalProtect afin d'exempter des correctifs de sécurité spécifiques d'être signalés comme manquants dans le rapport HIP des terminaux pour éviter que le terminal échoue au contrôle HIP dans les cas où des mises à jour de correctifs se produisent fréquemment (par exemple, certaines entreprises mettent à jour leurs correctifs plusieurs fois par jour avec des mises à jour de menaces).

1. Configurer la mise en œuvre des politiques basées sur HIP.
2. Définissez les correctifs que vous souhaitez exclure du rapport HIP et la date jusqu'à laquelle les exclure.

   Si vous utilisez Strata Cloud Manager (NGFW), alors

   1. Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls**

 ©2026 Palo Alto Networks, Inc.

(Tous les pare-feu) > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)**.

2. Sur la page Ajouter les paramètres de l'application de l'agent, sous **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Exclude Categories (Exclure les catégories)**, modifiez les catégories à exclure.
3. Cliquez sur **Add (Ajouter)** et sélectionnez la **Category (Catégorie)** comme **Patch Management (Gestion des correctifs)** et ajoutez le **Vendor (Fournisseur)**.

Si vous utilisez Strata Cloud Manager (Prisma Access), alors :

1. Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **<default>**.
2. Sur la page par défaut, sélectionnez **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Exclude Categories (Exclure les catégories)** puis modifiez les catégories à exclure.
3. Cliquez sur **Add (Ajouter)** et sélectionnez la **Category (Catégorie)** comme **Patch Management (Gestion des correctifs)** et ajoutez le **Vendor (Fournisseur)**.

1. Sur le pare-feu qui héberge votre portail GlobalProtect (ou sur Panorama), sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez la configuration du portail que vous souhaitez modifier.
3. Sous l'onglet **Agent**, sélectionnez la configuration de l'agent à partir de laquelle exclure les catégories, ou **Add (ajoutez)**-en une nouvelle.
4. Sous **Exclude Categories (Exclure les catégories)**, **Add (Ajoutez)** une nouvelle catégorie à exclure.
5. Sélectionnez **patch-management (gestion des correctifs)** comme le **Vendor (Fournisseur)** puis **Add (Ajouter)** le fournisseur.
6. Spécifiez le nom ou le numéro du correctif <kb-article-id value> et éventuellement une date <MM/DD/YYYY> jusqu'à laquelle vous souhaitez exclure les mises à jour de correctifs du rapport HIP.

   Utilisez le format suivant :

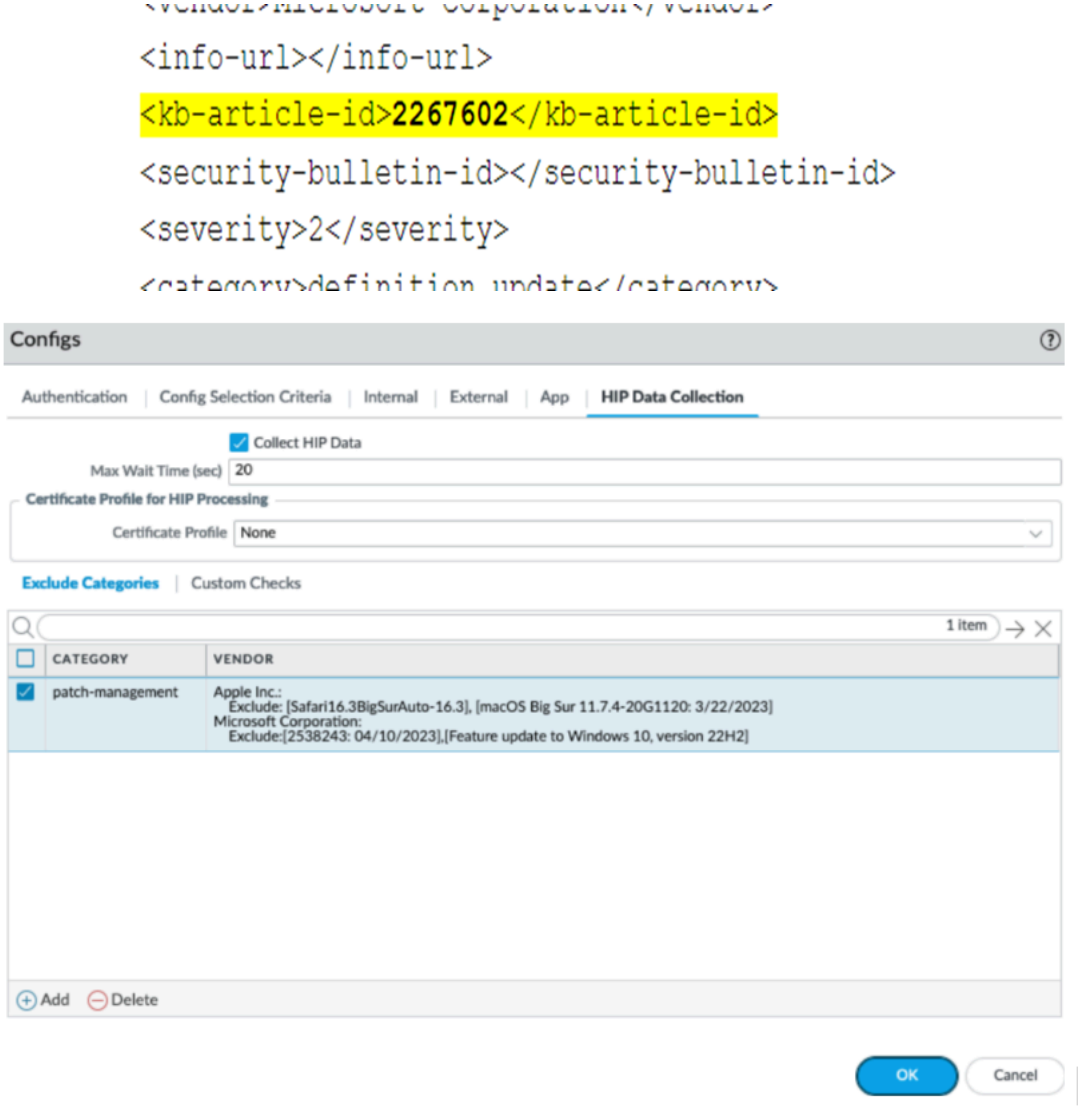
   `Exclure :[kb-article-id1 : MM/JJ/AAAA], [kb-article-id2 : MM/JJ/AAAA]`

   Où la valeur `kb-article` est le numéro de l'attribut, par exemple `<kb-article-id>2267602</kb-article-id>` et `MM/JJ/AAAA` spécifie la date jusqu'à laquelle le correctif est exclu du rapport HIP. Si vous ne fixez pas de date, le correctif sera exclu du

 ©2026 Palo Alto Networks, Inc.

rapport HIP indéfiniment. Si vous choisissez de définir une date, le correctif sera exclu jusqu'à la date spécifiée.

L'identifiant de l'article Kb doit être dans le même format que celui affiché dans les journaux, par exemple :



Répétez cette étape pour chaque correctif que vous souhaitez exclure du rapport HIP.

Si vous souhaitez exclure tous les correctifs d'un fournisseur spécifique, vous devez simplement exclure toute la catégorie au lieu de spécifier des correctifs précis.

3. Pour enregistrer les paramètres, cliquez sur **OK** puis **Commit (Valider)** vos modifications.

 ©2026 Palo Alto Networks, Inc.

Collecter des données d'application et de processus sur des points de terminaison

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Le registre Windows, mcOS plist et la liste de processus Linux peuvent être utilisés pour configurer et stocker des paramètres pour les systèmes d'exploitation respectivement Windows et MacOS, . Vous pouvez créer une vérification personnalisée qui vous permet de déterminer si une application est installée (a une clé de registre ou plist correspondante) ou est en cours d'exécution (a un processus en cours d'exécution en cours) sur un point de terminaison Windows, Linux ou MacOS. L'activation des vérifications personnalisées demande à l'application GlobalProtect de collecter des informations de registre spécifiques (clés de registre et valeurs de clé de registre de points de terminaison Windows) ou des informations de liste de préférences (plist) (plist et clés de plist de points de terminaison MacOS) ou a un processus correspondante (nom du processus des points de terminaison Linux). Les données que vous définissez pour être collectées dans une vérification personnalisée sont incluses dans les données brutes d'informations sur l'hôte collectées par l'application GlobalProtect, puis envoyées à la passerelle GlobalProtect lorsque l'application authentifie et se connecte à la passerelle. Pour plus d'informations sur la définition des paramètres d'application directement à partir du Registre Windows, de la liste globale de macOS ou de la configuration de prédéploiement Linux, voir Deploy App Settings Transparently (Déployer les paramètres de l'application de manière transparente).

Pour surveiller les données collectées avec des vérifications personnalisées, vous pouvez créer un objet HIP. Vous pouvez ensuite ajouter l'objet HIP à un profil HIP afin d'utiliser les données collectées pour mettre en correspondance les données et le trafic du point de terminaison, et mettre en œuvre des règles de sécurité. La passerelle utilise l'objet HIP (correspondant aux données définies dans la vérification personnalisée) pour filtrer les informations brutes sur l'hôte, envoyées par l'application. Lorsque la passerelle met en correspondance des données de point de terminaison et un objet HIP, une entrée du journal de correspondances HIP est générée pour les données. Le profil HIP permet également à la passerelle de mettre en correspondance les données collectées et une règle de sécurité. Si le profil HIP est utilisé en tant que critère d'une règle de politique de sécurité, la passerelle met en œuvre cette règle de sécurité sur le trafic correspondant.

Utilisez les étapes suivantes pour activer des vérifications personnalisées afin de collecter des données sur des points de terminaison Windows, MacOS ou Linux. Ce flux de travail présente également les étapes facultatives de création d'un objet HIP et d'un profil HIP pour une vérification personnalisée, ce qui vous permet d'utiliser des données de points de terminaison en tant que critères de correspondance de politiques de sécurité afin de surveiller, d'identifier et d'agir sur du trafic.

> *Sur les appareils Windows, macOS et Linux, lorsque vous configurez des **Custom Checks (vérifications personnalisées)** par exemple pour collecter des entrées de Registre ou de plist,*

 ©2026 Palo Alto Networks, Inc.

GlobalProtect masque ces informations dans le résumé du profil d'hôte de l'application GlobalProtect.

1. Activez l'application GlobalProtect pour collecter des informations de Registre Windows à partir de points de terminaison Windows, des informations plist à partir de points de terminaison macOS ou des informations de liste de processus à partir de points de terminaison Linux. Le type d'informations collectées peut inclure le fait qu'une application est installée ou non sur le point de terminaison, ou des attributs spécifiques ou propriétés de cette application.

   Si vous utilisez Strata Cloud Manager (NGFW) pour collecter des données d'application et de processus à partir des terminaux, alors

   1. Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres de l'application de l'agent)**.
   2. Sur la page Ajouter les paramètres de l'application de l'agent, sous **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Custom Checks (Vérifications personnalisées)**, modifiez les vérifications personnalisées.
   3. Cliquez sur **Add (Ajouter)** pour ajouter Windows (Clé de registre), Mac (Plist) ou Linux (Liste des processus).

   Si vous utilisez Strata Cloud Manager (Prisma Access), alors :

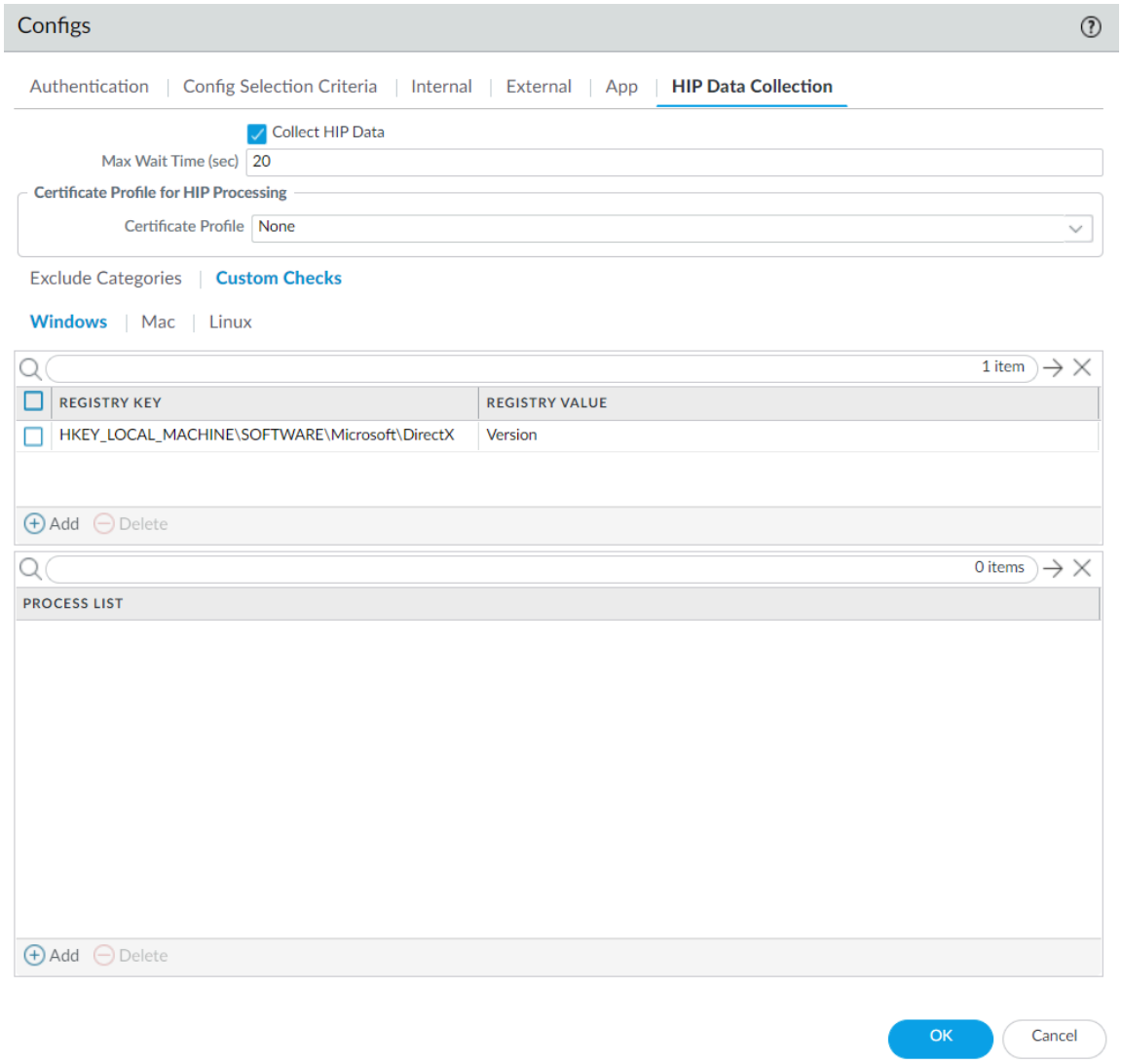
   1. Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **<default>**.
   2. Sur la page par défaut, sélectionnez **HIP Data Collection (Collecte de données HIP)** > **Show Advanced Options (Afficher les options avancées)** > **Custom Checks (Vérifications personnalisées)** puis modifiez les vérifications personnalisées.
   3. Cliquez sur **Add (Ajouter)** pour ajouter Windows (Clé de registre), Mac (Plist) ou Linux (Liste des processus).

   Collectez des données sur un point de terminaison Windows :

   1. Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
   2. Sélectionnez une configuration de portail existante ou **Add (Ajoutez)**-en une nouvelle.
   3. À l'onglet **Agent (Agent)**, sélectionnez la configuration de l'agent que vous souhaitez modifier (ou **Add (ajoutez)**-en une nouvelle).
   4. Sélectionnez **HIP Data Collection (Collecte de données HIP)**.
   5. Activez l'option **Collect HIP Data (Collecter les données HIP)** sur l'application GlobalProtect.
   6. Sélectionnez **Custom Checks (Vérifications personnalisées)** > **Windows (Windows)**, puis **Add (Ajoutez)** la **Registry Key (Clé de registre)** sur laquelle vous voulez collecter des

 ©2026 Palo Alto Networks, Inc.

renseignements. Si vous souhaitez limiter la collecte de données à une valeur contenue dans cette clé de registre, ajoutez la **Registry Value (Valeur de registre)** correspondante.

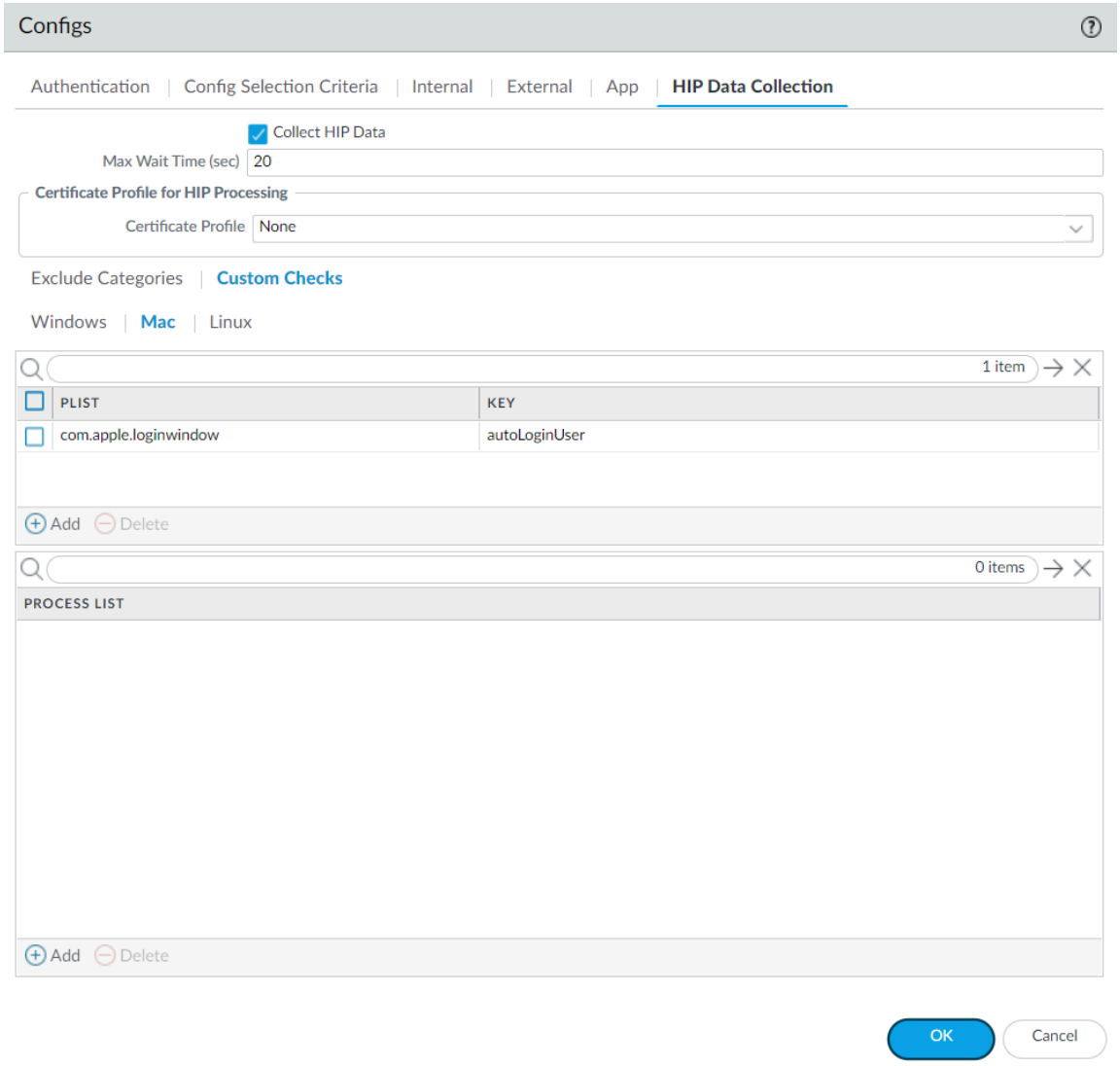


Collectez des données sur un point de terminaison MacOS :

1. Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez une configuration de portail existante ou **Add (Ajoutez)**-en une nouvelle.
3. À l'onglet **Agent (Agent)**, sélectionnez la configuration de l'agent que vous souhaitez modifier (ou **Add (ajoutez)**-en une nouvelle).
4. Sélectionnez **HIP Data Collection (Collecte de données HIP)**.
5. Activez l'option **Collect HIP Data (Collecter les données HIP)** sur l'application GlobalProtect.

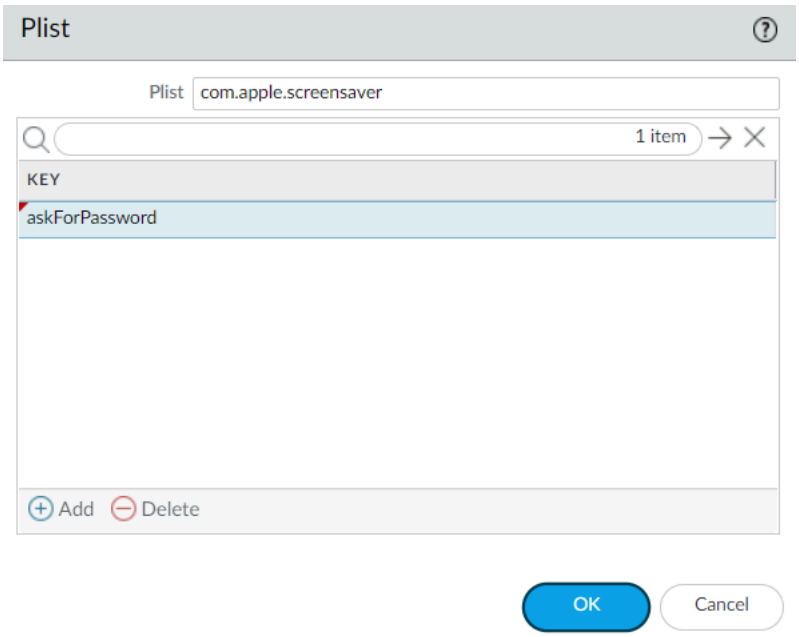
 ©2026 Palo Alto Networks, Inc.

6. Sélectionnez **Custom Checks (Vérifications personnalisées)** > **Mac (Mac)**, puis **Add (Ajoutez)** la **Plist (Plist)** sur laquelle vous souhaitez collecter des informations et la **Key (Clé)** de Plist correspondante pour déterminer si l'application est installée.



Par exemple, **Add (ajoutez)** la **Plist** **`com.apple.screensaver`** et la **Key (Clé)** **`askForPassword`** pour collecter des informations sur le fait qu'un mot de passe est requis pour réactiver le terminal macOS après le lancement de l'économiseur d'écran.

 ©2026 Palo Alto Networks, Inc.

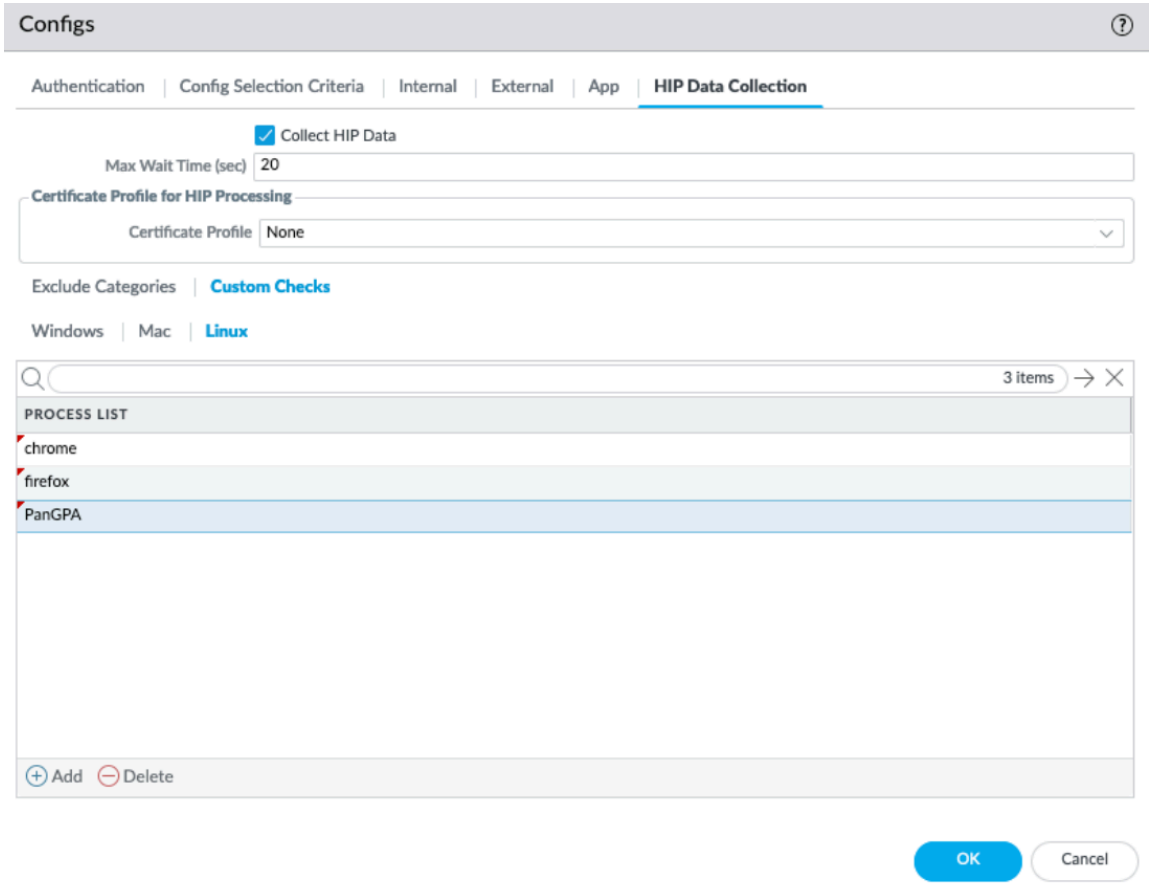


Collectez des données à partir d'un point de terminaison Linux :

1. Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez une configuration de portail existante ou **Add (Ajoutez)**-en une nouvelle.
3. À l'onglet **Agent (Agent)**, sélectionnez la configuration de l'agent que vous souhaitez modifier (ou **Add (ajoutez)**-en une nouvelle).
4. Sélectionnez **HIP Data Collection (Collecte de données HIP)**.
5. Activez l'option **Collect HIP Data (Collecter les données HIP)** sur l'application GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

6. Sélectionnez **Custom Checks (Vérifications personnalisées)** > **Linux**, puis **Add (Ajouter)** la **Process List (liste des processus)** sur laquelle vous souhaitez collecter des informations.



2. (Facultatif) Vérifiez si un processus spécifique est exécuté sur le point de terminaison.
   1. Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
   2. Sélectionnez une configuration de portail existante ou **Add (Ajoutez)**-en une nouvelle.
   3. À l'onglet **Agent (Agent)**, sélectionnez la configuration de l'agent que vous souhaitez modifier (ou **Add (ajoutez)**-en une nouvelle).
   4. Sélectionnez **HIP Data Collection (Collecte de données HIP)**.
   5. Activez l'option **Collect HIP Data (Collecter les données HIP)** sur l'application GlobalProtect.
   6. Sélectionnez **Custom Checks (Vérifications personnalisées)** > **Windows,**, **Mac**, ou **Linux.**
   7. **Add (Ajoutez)** le nom du processus sur lequel vous souhaitez collecter des informations dans la **Process List (Liste des processus)**.

3. Enregistrez la vérification personnalisée.

   Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.

4. (Optional (Facultatif)) Créez un objet HIP à faire correspondre à une clé de registre (Windows), une plist (MacOS) ou une liste de processus(Linux). Cela vous permet de filtrer

 ©2026 Palo Alto Networks, Inc.

les informations brutes sur l'hôte collectées de l'application GlobalProtect pour surveiller les données aux fins de la vérification personnalisée.

Avec un objet HIP défini pour les données de contrôle personnalisées, la passerelle correspond aux données brutes soumises par l'application à l'objet HIP, et une entrée de journal HIP correspondante est générée pour les données (**Monitor (Surveillance)** > **HIP Match (Correspondances HIP)**).

Pour les points de terminaison Windows, macOS et Linux :

1. Sélectionnez **Objects (Objects)** > **GlobalProtect (GlobalProtect)** > **HIP Objects (Objets HIP)**.
2. Sélectionnez un objet HIP existant ou **Add (Ajoutez)**-en un nouveau.
3. À l'onglet **Custom Checks (Vérifications personnalisées)**, cochez la case permettant d'activer les **Custom Checks (Vérifications personnalisées)**.

Pour les points de terminaison Windows uniquement :

1. Pour vérifier la présence d'une clé de registre précise sur les points de terminaison Windows, sélectionnez **Custom Checks (Vérifications personnalisées)** > **Registry Key (Clé de registre)**, puis **Add (Ajoutez)** la clé de registre pour la mise en correspondance. Lorsque vous êtes invité à le faire, entrez la **Registry Key (Clé de registre)**, puis configurez l'une des options suivantes :
   - Pour une mise en correspondre sur les données de valeur par défaut pour la clé de registre, saisissez les **(Default) Value Data (Données de valeur par défaut)**.
   - Pour faire correspondre des points de terminaison qui ne disposent pas de la clé de registre définie, sélectionnez **La clé n'existe pas ou ne correspond pas aux données de la valeur définies**.

   *Ne configurez pas les deux options **(Default) Value Data (Données de valeur par défaut)** et **Key does not exist or match the specified value data (La clé n'existe pas ou ne correspond pas aux données de la valeur définies)** simultanément.*

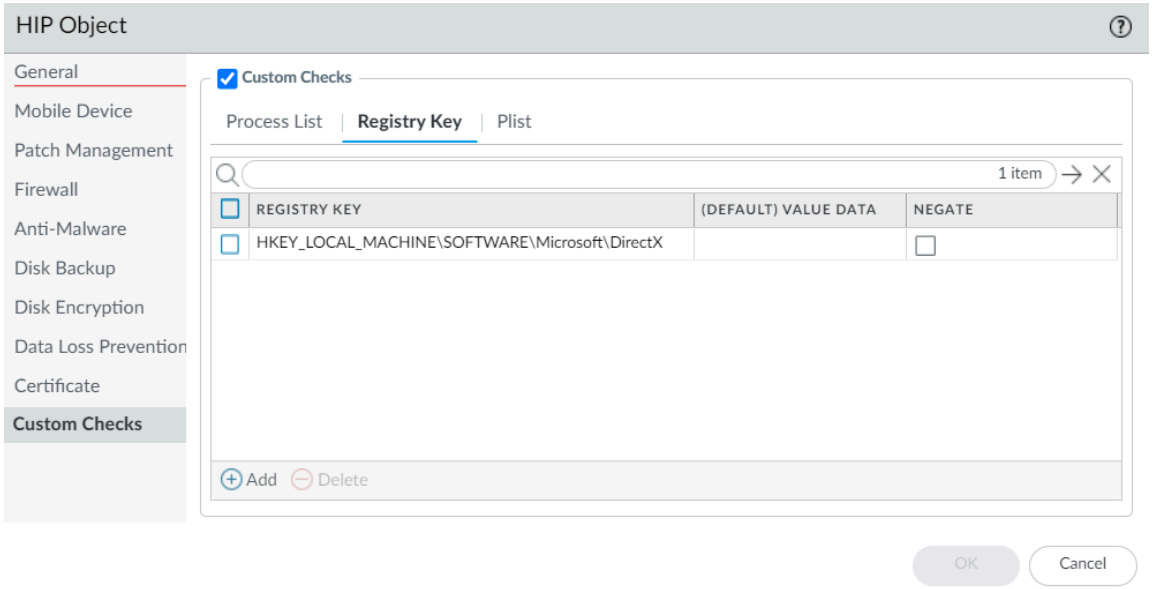
2. Pour faire correspondre à des valeurs spécifiques de la clé de registre, sélectionnez **Custom Checks (Vérifications personnalisées)** > **Registry Key (Clé de registre)**, puis **Add (Ajoutez)** la clé de registre pour la mise en correspondance. Lorsque vous êtes invité, entrez la **Registry Key (Clé de registre)**. Cliquez sur **Add (Ajouter)** et configurez l'une des options suivantes :
   - Pour la mise en correspondance avec des valeurs spécifiques de la clé de registre, saisissez la **Registry Value (Valeur de registre)** et les **Value Data (Données de valeur)**.

 ©2026 Palo Alto Networks, Inc.

- Pour la mise en correspondance des points de terminaison pour lesquels aucune valeur de registre n'est spécifiée, saisissez la **Registry Value (Valeur du registre)**, puis cochez la case **Negate (Refuser)**.

  *Pour utiliser cette option, ne saisissez aucune **Value Data (Donnée de valeur)** pour votre **Registry Key (Clé de registre)**.*

  Si vous ajoutez plus d'une valeur de registre à votre clé de registre, la passerelle GlobalProtect vérifie les points de terminaison pour toutes la valeurs de registre spécifiées.



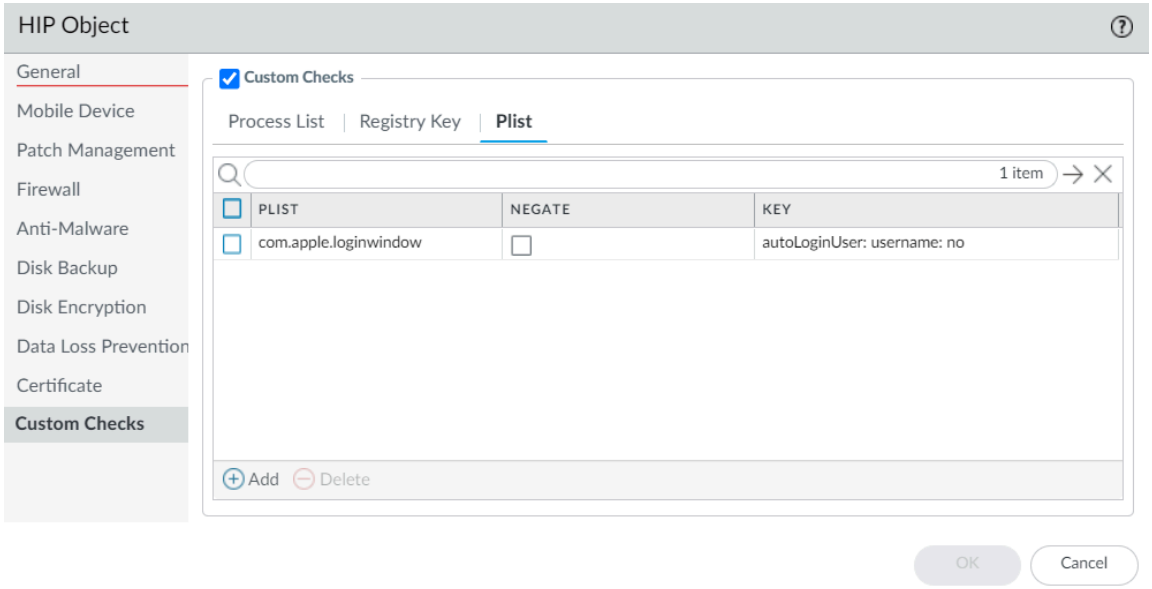
3. Cliquez sur **OK** pour enregistrer l'objet HIP. Vous pouvez **Commit (Valider)** les modifications pour consulter les données des journaux **HIP Match (Correspondances HIP)** au prochain archivage du périphérique, ou passer à l'étape 6.

Pour les points de terminaison MacOS uniquement :

1. Pour vérifier les points de terminaison macOS d'une plist spécifique, sélectionnez **Plist**, puis **Add (Ajoutez)** la plist que vous souhaitez vérifier. Lorsque vous êtes invité à le faire, saisissez le nom de la **Plist**. Si vous souhaitez mettre en correspondance des points de terminaison macOS qui ne disposent pas d'une plist définie, activez l'option **Plist does not exist (La Plist n'existe pas)**.
2. Pour la mise en correspondance de la paire clé-valeur au sein d'une plist, sélectionnez **Plist**, puis **Add (Ajoutez)** la plist que vous souhaitez vérifier. Lorsque vous êtes invité à le faire, saisissez le nom de la **Plist**, puis **Add (Ajoutez)** une **Key (Clé)** et la **Value (Valeur)**

 ©2026 Palo Alto Networks, Inc.

correspondante à faire correspondre. Par ailleurs, si vous souhaitez identifier des points de terminaison qui ne disposent pas d'une clé et d'une valeur spécifiques, vous pouvez sélectionner **Negate (Nier)** après avoir ajouté la **Key (Clé)** et la **Value (Valeur)**).



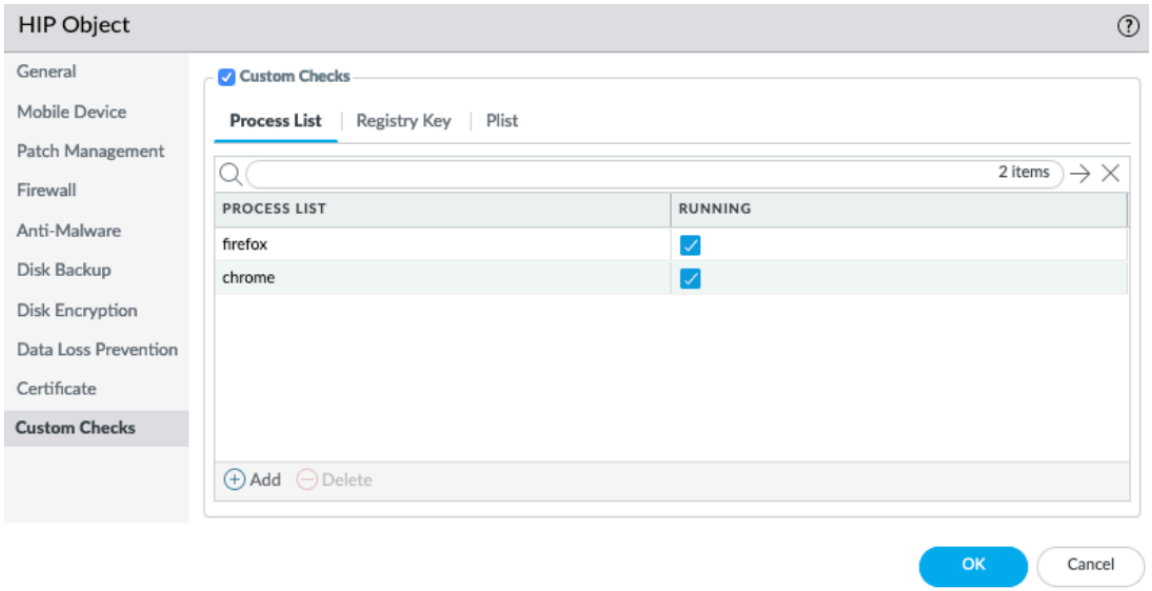
3. Cliquez sur **OK** pour enregistrer l'objet HIP. Vous pouvez **Commit (Valider)** les modifications pour consulter les données des journaux **HIP Match (Correspondances HIP)** au prochain archivage du périphérique, ou passer à l'étape 6.

Pour les points de terminaison Linux uniquement :

1. Pour vérifier si un processus spécifique s'exécute sur le point de terminaison Linux, sélectionnez **Process List (Liste des processus)**, puis **Add (Ajoutez)** le processus

 ©2026 Palo Alto Networks, Inc.

correspondant que vous souhaitez vérifier. Lorsque vous êtes invité à le faire, saisissez le nom de la **Process List (liste de processus)**.



2. Cliquez sur **OK** pour enregistrer l'objet HIP. Vous pouvez **Commit (Valider)** les modifications pour consulter les données des journaux **HIP Match (Correspondances HIP)** au prochain archivage du périphérique, ou passer à l'étape 6.

5. (Facultatif) Créez un profil HIP pour que l'objet HIP soit évalué par rapport au trafic.

Le profil HIP peut être ajouté à une stratégie de sécurité en tant que vérification supplémentaire pour le trafic correspondant à cette politique. Lorsque le trafic est mis en correspondance avec le profil HIP, la règle de stratégie de sécurité est mise en œuvre sur le trafic.

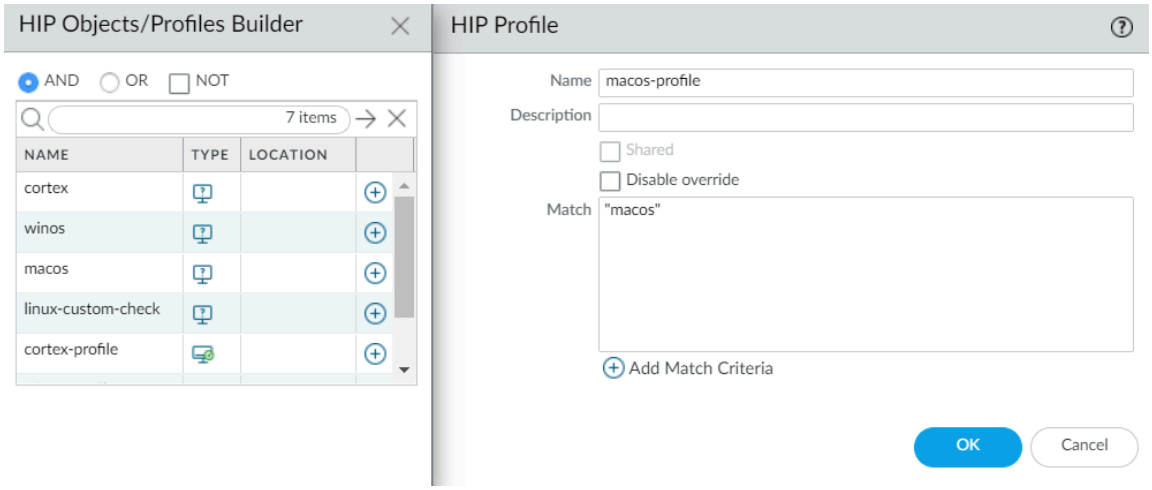
Pour plus de détails sur la création de profils HIP, voir Configurer un renforcement de stratégie basé sur HIP.

1. Créez un profil HIP, effectuez l'une des actions suivantes :
   - Sur le pare-feu qui héberge vos passerelles GlobalProtect (ou sur Panorama si vous envisagez de partager les objets HIP entre de multiples passerelles), sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Profiles (Profils HIP)**, puis **Add (Ajouter)** un nouveau profil HIP.
   - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **Objects (Objets)** > **HIP Profiles (Profils HIP)** > **Add HIP Profile (Ajouter un profil HIP)**.
   - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Objects (Objets)** > **HIP Profiles (Profils HIP)** > **Add HIP Profile (Ajouter un profil HIP)**.
2. Sélectionnez un profil HIP existant ou **Add (Ajoutez)**-en un nouveau.
3. Cliquez sur **Add Match Criteria (Ajouter un critère de correspondance)** pour ouvrir le générateur de profils/d'objets HIP.

 ©2026 Palo Alto Networks, Inc.

4. Sélectionnez le **HIP object (Objet HIP)** que vous souhaitez utiliser comme critère de correspondance, puis cliquez sur l'icône d'ajout (

) pour le déplacer vers la zone de texte **Match (Faire correspondre)** du profil HIP.
5. Après avoir ajouté les objets au nouveau profil HIP, cliquez sur **OK**, puis **Commit (Validez)** les changements.



6. Ajoutez le profil HIP à une politique de sécurité de sorte que les données collectées avec la vérification personnalisée puissent être utilisées pour faire correspondre et agir sur du trafic.

Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis sélectionnez une politique de sécurité existante ou **Add (Ajoutez)**-en une nouvelle. À l'onglet **User (Utilisateur)**, **Add (Ajoutez)** les **HIP Profiles (Profils HIP)** à la politique. Pour plus de détails sur les composants des stratégies de sécurité et l'utilisation de stratégies de sécurité pour faire correspondre et agir sur du trafic, reportez-vous à Stratégie de sécurité.

Si vous utilisez Strata Cloud Manager,

- Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **GlobalProtect** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > **Add Rule (Ajouter une règle)** > **Security Rule (Règle de sécurité)**.
- Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)** > **Add Rule (Ajouter une règle)** > **Security Rule (Règle de sécurité)**.

Configurer la correction du processus HIP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence d'abonnement GlobalProtect Licence pour utilisateurs mobiles de Prisma Access (à utiliser avec Prisma Access)

©2026 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	Version de l'application GlobalProtect 6.2 ou ultérieure pour Windows et macOS Version de publication de contenu 8699-7991 ou ultérieure

Procédez comme suit pour configurer l'application GlobalProtect de manière à exécuter un script de correction chaque fois qu'un terminal GlobalProtect échoue à une ou plusieurs vérifications de processus pour aider le terminal à récupérer les échecs d'une vérification HIP. Avec cette fonctionnalité activée, l'application GlobalProtect fournira un délai d'expiration spécifié dans lequel le terminal peut exécuter le script de correction s'il échoue à une vérification de processus. Après l'expiration du délai d'expiration, l'application GlobalProtect soumet à nouveau le rapport HIP.

1. Configurez des vérifications de processus personnalisées.

   Les scripts de correction que vous écrivez doivent vérifier si les processus que vous avez configurés dans les **Custom Checks (Vérifications personnalisées)** sont en cours d'exécution et, dans le cas contraire, exécuter le script et lancer le processus.

2. Configurez un délai de correction HIP sur le portail.

   1. Pour configurer un délai de correction de HIP, effectuez l'une des opérations suivantes :

      Sur Strata Cloud Manager (NGFW) :

      1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)** > **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres d'application d'agent)**.
      2. Sur la page Ajouter des paramètres d'application Agent, sélectionnez **App Configuration (Configuration d'application)** > **Show Advanced Options (Afficher les options avancées)**.
      3. Sous **Enforcement (Renforcement)**, configurez Délai d'expiration pour la correction du processus HIP, Tentatives de correction du processus HIP et Vérification de l'intégrité de la correction du processus HIP.

      Sur Strata Cloud Manager (Prisma Access) :

      1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)**

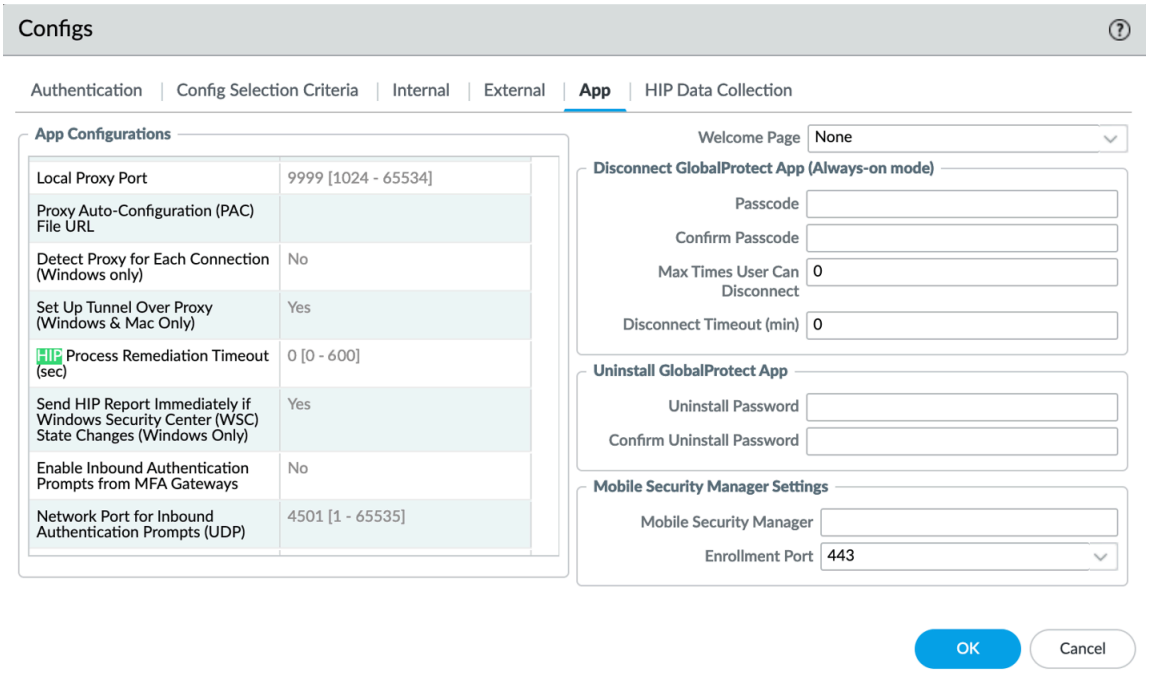
 ©2026 Palo Alto Networks, Inc.

> **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **<default>**.

2. Sur la page Par défaut, sélectionnez **App Configuration (Configuration de l'application)** > **Show Advanced Options (Afficher les options avancées)**.
3. Sous **Enforcement (Renforcement)**, configurez Délai d'expiration pour la correction du processus HIP, Tentatives de correction du processus HIP et Vérification de l'intégrité de la correction du processus HIP.

2. Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
3. Sélectionnez la configuration du portail à laquelle vous ajoutez la configuration de l'agent, puis sélectionnez l'onglet **Agent**.
4. Sélectionnez la configuration de l'agent que vous souhaitez modifier ou **Add (Ajouter)** une nouvelle.
5. Sélectionnez l'onglet **App (Applications)**.
6. Pour activer la fonctionnalité de correction de HIP, définissez un **HIP Remediation Process Timeout (sec) (Délai d'expiration du processus de correction HIP [sec])**.

   Par défaut, ce champ est défini sur 0, indiquant que la fonctionnalité est désactivée. Entrez une valeur comprise entre 1 et 600 secondes pour indiquer le temps que vous souhaitez accorder au script de correction pour se terminer.



7. Cliquez deux fois sur **OK** pour enregistrer les configurations de votre application et de votre portail.
8. **Commit (Validez)** les modifications.

3. Déployez le script de correction sur vos terminaux à l'aide de la Mobile Device Management (gestion des appareils mobiles - MDM).

Comme meilleure pratique, utilisez des formats standard pour les scripts que vous déployez (par exemple, déployer des scripts shell sur les terminaux macOS et des scripts batch sur

 ©2026 Palo Alto Networks, Inc.

les terminaux Windows). Le nom du script est sensible à la casse et doit utiliser le nom et l'emplacement prédéfinis comme suit :

- **Windows**

  Emplacement : `\Program Files\Palo Alto Networks\GlobalProtect\`

  Convention de dénomination : `hip-remediation-script.bat`

- **macOS**

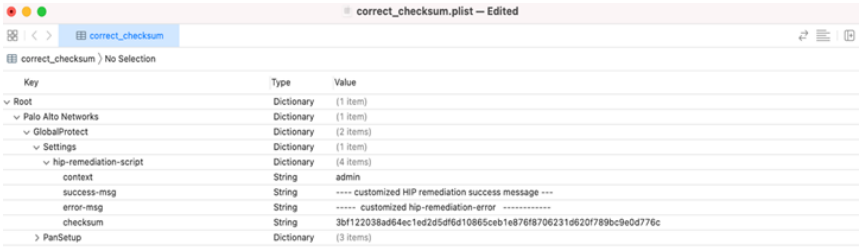
  Lieu : `/Applications/GlobalProtect.app/Contents/Resources/`

  Convention de dénomination : `hip-remediation-script.sh`

 ©2026 Palo Alto Networks, Inc.

4. (Facultatif) Personnalisez la façon dont le script s'exécute sur le terminal en définissant une somme de contrôle et/ou un message d'erreur personnalisé et en définissant le contexte dans lequel le script s'exécutera.

- **macOS**
  1. Calculer la somme de contrôle sha 256 : `shasum -a 256 hip-remediation-script.sh`.
  2. Modifiez les valeurs suivantes dans la liste au besoin :
     - `somme de contrôle` : spécifiez la somme de contrôle que vous avez générée
     - `erreur-msg` : saisissez le message d'erreur personnalisé que vous souhaitez afficher à l'utilisateur final lorsque la correction échoue
     - `success-msg` : saisissez le message d'erreur personnalisé que vous souhaitez afficher à l'utilisateur final lorsque la correction réussit
     - `context` : définissez sur **`admin`** ou **`user (utilisateur)`** pour spécifier le contexte dans lequel exécuter le script de correction. Par défaut, le script s'exécute dans le contexte utilisateur.
  3. Remplacez la liste GlobalProtect en copiant le fichier modified.plist pour écraser la liste par défaut : `sudo cp modified.plist /Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`.

  4. Arrêter/démarrer PanGPS :

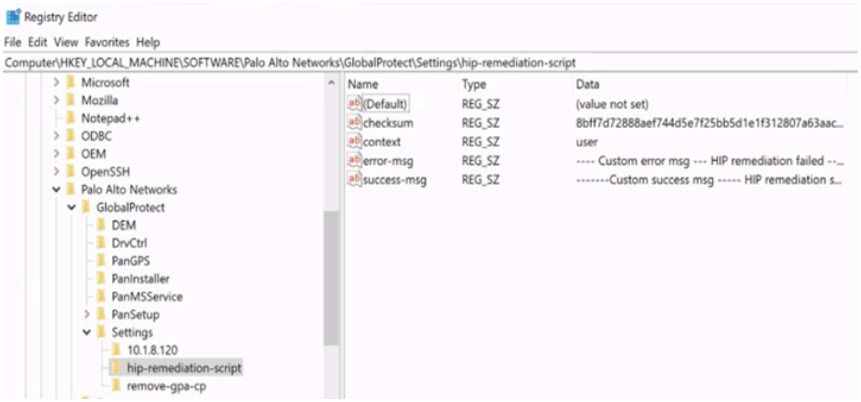
     ```
     launchctl stop com.paloaltonetworks.gp.pangps
     launchctl start com.paloaltonetworks.gp.pangps
     ```

- **Windows**
  1. Créez la somme de contrôle pour le script de correction : `certutil -hashfile hip-remediation-script.bat HASH256` .
  2. Déployez le paramètre de registre à l'aide de l'éditeur de Registre par défaut de Windows.

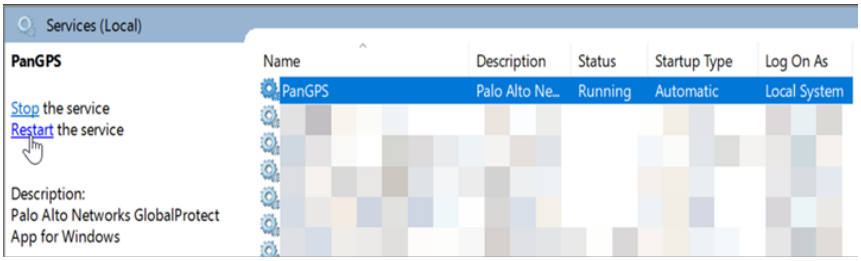
     Dans le Registre Windows, accédez à : **\HKEY_LOCAL_MACHINE > SOFTWARE> Palo Alto Networks > GlobalProtect > Settings > hip-remediation-script** et définissez les clés suivantes : dans le Registre Windows, accédez à : **\HKEY_LOCAL_MACHINE >**

 ©2026 Palo Alto Networks, Inc.

SOFTWARE> Palo Alto Networks > GlobalProtect > Settings > hip-remediation-script et définissez les clés suivantes :



- `somme de contrôle` : spécifiez la somme de contrôle que vous avez générée
- `erreur-msg` : saisissez le message d'erreur personnalisé que vous souhaitez afficher à l'utilisateur final lorsque la correction échoue
- `success-msg` : saisissez le message d'erreur personnalisé que vous souhaitez afficher à l'utilisateur final lorsque la correction réussit
- `contexte` : définissez sur **`admin`** ou **`user (utilisateur)`** pour spécifier le contexte dans lequel exécuter le script de correction. Par défaut, le script s'exécute dans le contexte utilisateur.

3. Pour redémarrer GlobalProtect, dans l'écran Services Windows, recherchez le service **PanGPS** et cliquez sur **Restart the service (Redémarrer le service)**.
4. 

Processus de correction HIP amélioré

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile PAN-OS 11.0.2 (ou une version ultérieure de PAN-OS) Application GlobalProtect 6.3.0 ou versions ultérieures Terminaux GlobalProtect fonctionnant sous Windows et macOS.

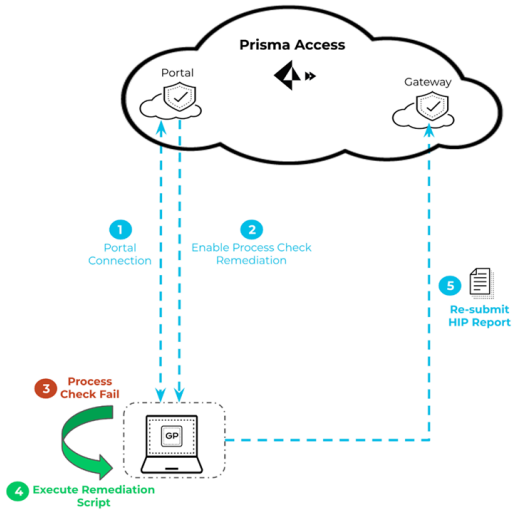
 ©2026 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	Version de publication de contenu 8833-8679 ou ultérieure

Vous pouvez désormais configurer l'application GlobalProtect pour relancer le script de correction HIP chaque fois que le terminal GlobalProtect échoue à la vérification du processus après avoir exécuté le processus de correction HIP configuré.

Avec cette fonctionnalité activée, l'application GlobalProtect relancera le script de correction HIP lorsque le processus échoue après le délai d'expiration de la période de correction HIP définie pour aider le terminal à se remettre d'un échec de vérification HIP. L'application relance le script de correction après un échec de vérification de processus basé sur le nombre de tentatives de processus de correction HIP que vous configurez via les paramètres de l'application du portail GlobalProtect.

Par exemple, si vous configurez le nombre de tentatives sur 3 et le délai d'expiration de la période de correction à 5 minutes dans la configuration du portail, alors chaque fois que le terminal échoue à la vérification du processus après avoir effectué le processus de correction, l'application exécute le script trois fois et attend jusqu'à 5 minutes avant de soumettre le rapport HIP.



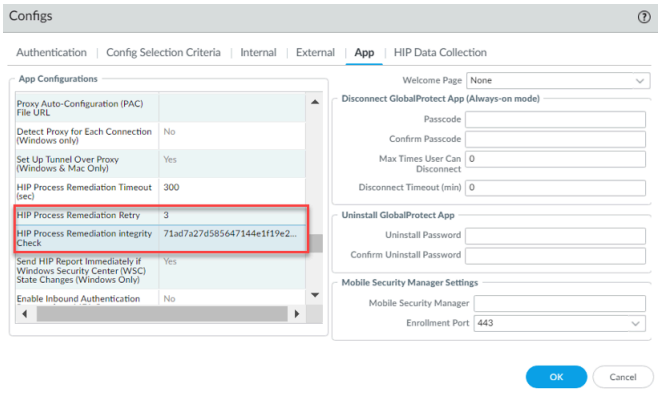
Utilisez la procédure suivante pour configurer le nombre de tentatives du processus de correction HIP :

1. Configurez des vérifications de processus personnalisées.

 ©2026 Palo Alto Networks, Inc.

2. Configurez un processus de correction HIP pour que l'application GlobalProtect exécute un script de correction chaque fois qu'un terminal GlobalProtect échoue à une ou plusieurs vérifications de processus pour aider le terminal à se remettre d'un échec de vérification HIP.
   1. Configurez un délai d'expiration de correction HIP sur le portail.
   2. Configurez une tentative de correction du processus HIP.
      1. Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**.
      2. Sélectionnez la configuration du portail à laquelle vous ajoutez la configuration de l'agent, puis sélectionnez l'onglet **Agent**.
      3. Sélectionnez la configuration de l'agent que vous souhaitez modifier ou **Add (Ajouter)** une nouvelle.
      4. Sélectionnez l'onglet **App (Applications)**.
      5. Pour activer la fonction de tentative de correction du processus HIP, configurez un nombre de **HIP Process Remediation Retry (Tentative de correction du processus HIP)**.

         Par défaut, ce champ est défini sur 0, indiquant que la fonctionnalité est désactivée. Entrez une valeur de 1 à 3 pour indiquer le nombre de fois que vous souhaitez exécuter le processus de correction HIP en cas d'échecs de vérification de processus.

         Cette fonctionnalité sera désactivée après la mise à niveau ou la rétrogradation des versions de l'application GlobalProtect.
      6. Dans le champ **HIP Process Remediation Integrity Check (Vérification de l'intégrité de la correction du processus HIP)**, spécifiez la somme de contrôle que vous avez généré pour le processus de correction HIP.
      7. Cliquez deux fois sur **OK** pour enregistrer les configurations de votre application et de votre portail.
      8. **Commit (Validez)** les modifications.

   Si vous utilisez Strata Cloud Manager, effectuez l'une des actions suivantes :

   Sur Strata Cloud Manager (NGFW) :

   1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **All Firewalls (Tous les pare-feu)**

 ©2026 Palo Alto Networks, Inc.

> **Device (Périphérique)** > **GlobalProtect** > **Agent Settings (Paramètres de l'agent)** > **Add Agent App Settings (Ajouter les paramètres d'application d'agent)**.

2. Sur la page Ajouter des paramètres d'application Agent, sélectionnez **App Configuration (Configuration d'application)** > **Show Advanced Options (Afficher les options avancées)**.
3. Sous **Enforcement (Renforcement)**, configurez Délai d'expiration pour la correction du processus HIP, Tentatives de correction du processus HIP et Vérification de l'intégrité de la correction du processus HIP.

Sur Strata Cloud Manager (Prisma Access) :

1. Sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de configuration)** > **Prisma Access** > **Mobile Users Container (Conteneur d'utilisateurs mobiles)** > **GlobalProtect** > **Setup (Configuration)** > **GlobalProtect App (Application GlobalProtect)** > **App Settings (Paramètres de l'application)** > **<default>**.
2. Sur la page Par défaut, sélectionnez **App Configuration (Configuration de l'application)** > **Show Advanced Options (Afficher les options avancées)**.
3. Sous **Enforcement (Renforcement)**, configurez Délai d'expiration pour la correction du processus HIP, Tentatives de correction du processus HIP et Vérification de l'intégrité de la correction du processus HIP.

3. Déployez le script de correction sur vos terminaux à l'aide de la Mobile Device Management (gestion des appareils mobiles - MDM).

Comme meilleure pratique, utilisez des formats standard pour les scripts que vous déployez (par exemple, déployer des scripts shell sur les terminaux macOS et des scripts batch sur les terminaux Windows). Le nom du script est sensible à la casse et vous devez utiliser le nom et l'emplacement prédéfinis comme suit :

- **Windows** :

  Emplacement : `\Program Files\Palo Alto Networks\GlobalProtect\`

  Convention de nommage : `hip-remediation-script.bat`

- **macOS** :

  Emplacement : `/Applications/GlobalProtect.app/Contents/Resources/`

  Convention de nommage : `hip-remediation-script.sh`

4. (Facultatif) Personnalisez la façon dont le script s'exécute sur le terminal en définissant une somme de contrôle et/ou un message d'erreur personnalisé et en définissant le contexte dans lequel le script s'exécutera.

5. Connectez l'application GlobalProtect et le script de correction HIP s'exécute automatiquement chaque fois que le terminal GlobalProtect échoue à la vérification du processus. Si la vérification du processus échoue même après l'exécution du script de correction, l'application relance le script de correction en fonction du nombre de tentatives configuré. Après les tentatives, l'application soumet le rapport de vérification HIP indépendamment de la réussite ou non de la vérification du processus.

 ©2026 Palo Alto Networks, Inc.

6. Affichez les journaux GlobalProtect pour consulter le journal `hip_remediation_script` et vérifier si le processus de correction HIP est réussi ou non.

   Le nom et les emplacements des journaux de correction pour

   - **Windows :** `%AppData%\Local\Palo Alto Networks\GlobalProtect \hip_remediation_scripts.log`
   - **macOS :** `~/Library/Logs/PaloAltoNetworks/GlobalProtect/ hip_remediation_scripts.log`

   Le `hip_remediation_scripts.log` fera partie du bundle de journaux GlobalProtect et sera collecté lorsque les utilisateurs initient la collecte de journaux via l'application GlobalProtect ou lorsque l'application envoie des journaux de diagnostic au service de journalisation Strata pour une analyse plus approfondie.

Redistribution des rapports HIP

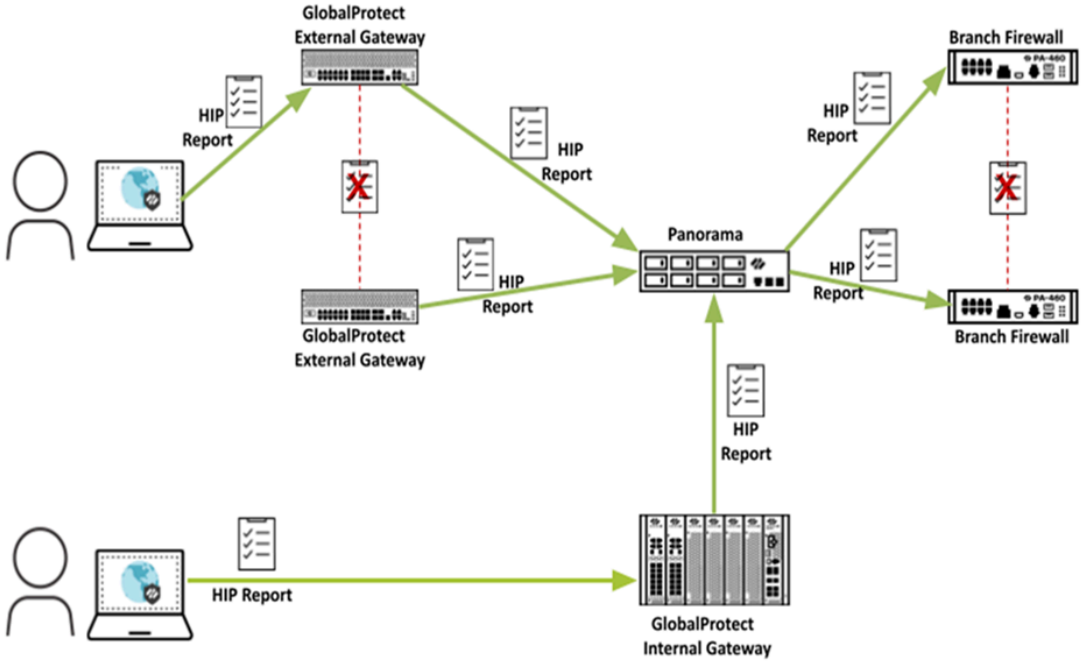
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile (Toutes les passerelles et tous les pare-feu GlobalProtect qui redistribuent les rapports HIP doivent avoir une licence GlobalProtect Gateway. Les périphériques Panorama qui redistribuent les rapports HIP ne nécessitent pas de licence de passerelle GlobalProtect.)

Pour garantir une application cohérente des politiques Host Information Profile (profil d'informations sur l'hôte - HIP) et simplifier la gestion des politiques, vous pouvez distribuer les rapports HIP de la passerelle interne ou externe GlobalProtect à d'autres pare-feu et appareils Panorama dans l'entreprise. La redistribution des rapports HIP peut s'avérer utile dans les situations suivantes :

- Vous voulez appliquer des politiques uniformes aux passerelles GlobalProtect internes et externes.
- Vous voulez appliquer des politiques HIP uniformes au trafic d'un utilisateur donné qui traverse plusieurs pare-feu.

Pour redistribution des rapports HIP, utilisez les mêmes recommandations de déploiement et les meilleures pratiques que vous utilisez pour redistribuer les informations d'User-ID. Gardez à l'esprit que les passerelles internes et externes GlobalProtect ne prennent pas en charge la redistribution HIP bidirectionnelle. Par conséquent, la meilleure pratique consiste à utiliser votre appareil Panorama comme point de redistribution. Dans ce déploiement, vous configureriez vos passerelles internes et externes pour envoyer les rapports HIP à Panorama, et Panorama les transférerait à vos pare-feu pour une application constante des politiques dans votre environnement.

 ©2026 Palo Alto Networks, Inc.



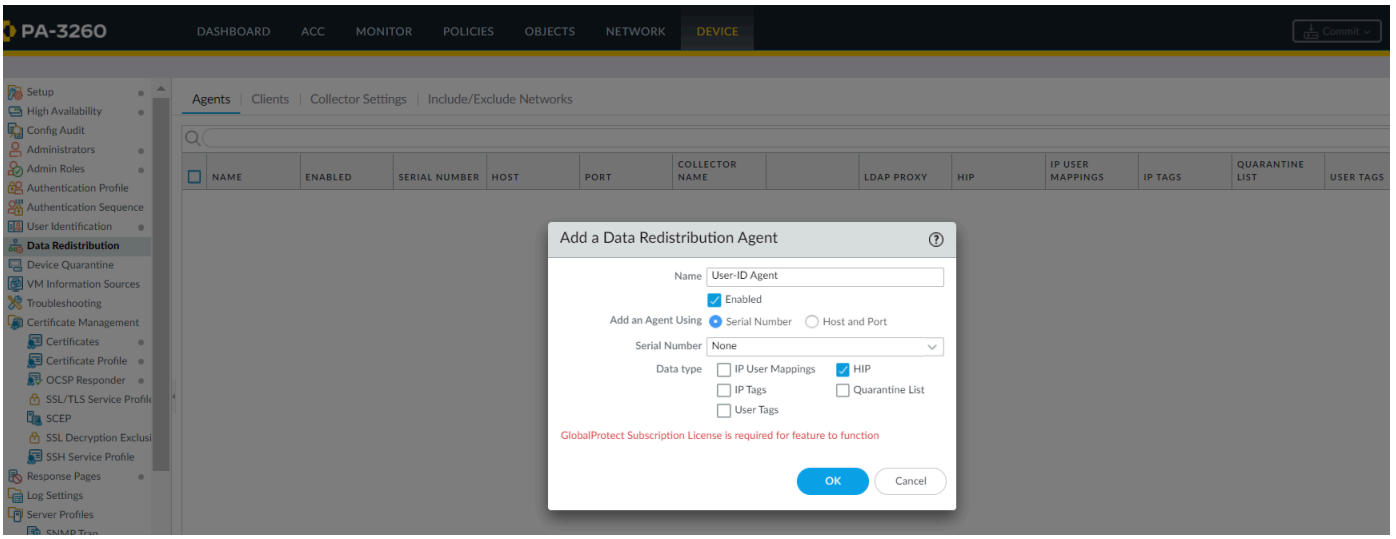
Utilisez les étapes suivantes pour configurer la redistribution des rapports HIP.

1. Configurer la mise en œuvre des politiques basées sur HIP pour vos passerelles et pare-feu.
2. Configurez la redistribution des rapports HIP.
   1. Pour configurer la redistribution des rapports HIP, effectuez l'une des actions suivantes :
      - Sur Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **All Firewalls (Tous les pare-feu)** > **Identity Services (Services d'identité)** > **Identity Redistribution (Redistribution d'identité)** > **Add Agent (Ajouter un agent)**.
      - Sur Strata Cloud Manager (Prisma Access), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access** > **Identity Services (Services d'identité)** > **Identity Redistribution (Redistribution d'identité)** > **Add Agent (Ajouter un agent)**.
      - Sur Panorama, sélectionnez **Device (Périphérique)** > **Agents** > **Data Redistribution (Redistribution des données)**.
   2. Sélectionnez un agent de redistribution des données existant ou **Add (Ajouter)** un nouveau.

      Il doit s'agir d'un pare-feu nouvelle génération Palo Alto Networks, d'une passerelle GlobalProtect ou d'un appareil Panorama.

 ©2026 Palo Alto Networks, Inc.

3. Sélectionnez **HIP Report (Rapport HIP)**.



4. Cliquez sur **OK**.

3. Si vous utilisez des pare-feu ou des passerelles GlobalProtect pour distributer les rapports HIP, assurez-vous que les paramètres de mappage des groupes sur les pare-feu ou les passerelles que vous utilisez pour redistribuer les rapports HIP correspondent aux attributs suivants sur les pare-feu ou passerelles sur lesquels User-ID est configuré.

   Si vous utilisez un appareil Panorama pour distribuer les rapports HIP, sautez cette étape.

- Configurez les attributs d'utilisateur sur les pare-feu ou passerelles de redistribution des rapports HIP pour qu'ils correspondent aux attributs d'utilisateur configurés sur les pare-feu ou passerelles utilisant User-ID.

  Par exemple, si les pare-feu ou passerelles utilisés pour la redistribution des rapports HIP possède un nom sAMAccountName de **Primary attribute (Attribut principal)** et d'un User Principal Name (Nom d'utilisateur principal ; UPN) de **Alternate Username (Nom d'utilisateur alternatif 1)**, assurez-vous de configurer les mêmes valeurs sur les pare-feu ou les passerelles sur lesquels vous avez configuré User-ID.

  > *Les attributs n'ont pas à être dans le même ordre ; par exemple, si le pare-feu de redistribution des rapports HIP comporte un sAMAccountName de **Primary attribute (Attribut principal)** et un UPN de **Alternate Username 1 (Nom d'utilisateur alternatif 1)**, vous pouvez configurer le pare-feu User-ID avec un sAMAccountName de **Alternate Username (Nom d'utilisateur alternatif)** et un UPN de **Primary attribute 1 (Attribut principal 1)**.*

- Si votre déploiement comporte des domaines d'utilisateur configurés dans son mappage de groupe, configurez les attributs des domaines d'utilisateur sur les pare-feu ou passerelles de redistribution des rapports HIP pour qu'ils correspondent aux attributs des domaines d'utilisateur configurés sur les pare-feu ou passerelles utilisant User-ID. Les attributs des domaines d'utilisateur doivent être les mêmes sur tous les pare-feu et passerelles.
- Configurez les groupes d'utilisateurs courants (les groupes d'utilisateurs sur les pare-feu et passerelles qui se connectent aux mêmes serveurs d'authentification et récupère les mêmes groupes d'utilisateurs) sur les pare-feu ou passerelles de redistribution des

 ©2026 Palo Alto Networks, Inc.

rapports HIP pour la mise en correspondance avec les groupes d'utilisateurs sur les pare-feu ou passerelles User-ID.

4. Redistribuez les rapports HIP sur vos appareils Panorama gérés, passerelles, pare-feu et systèmes virtuels en fonction des besoins de votre environnement.

   Gardez à l'esprit que les passerelles internes et externes GlobalProtect ne prennent pas en charge la redistribution HIP bidirectionnelle. Habituellement, les pare-feu non-passerelle agissent uniquement comme collecteurs. Même entre ces pare-feu et leurs collecteurs, la distribution HIP ne doit être qu'à sens unique.

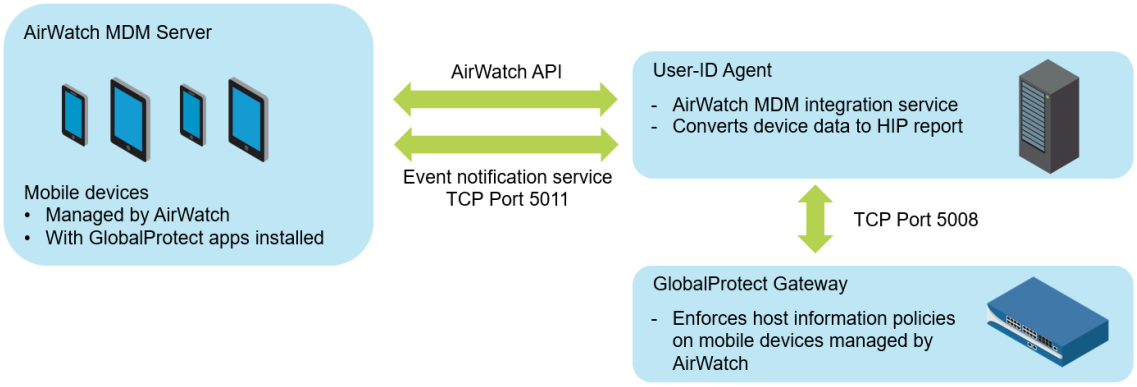
Configurer l'agent User-ID Windows pour collecter des informations d'hôte

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

User-ID basé sur Windows prend en charge le service d'intégration MDM Workspace ONE, permettant à GlobalProtect d'utiliser les informations d'hôte collectées par l'application pour appliquer des politiques basées sur HIP sur les périphériques gérés par Workspace ONE. Exécuté en tant qu'agent User-ID Windows, le service d'intégration MDM Workspace ONE utilise l'API Workspace ONE pour collecter des informations à partir de terminaux mobiles gérés par VMware Workspace ONE et traduire ces données en informations d'hôte.

Pour les terminaux Android gérés par Workspace ONE, cette fonctionnalité prend en charge les terminaux Android for Work, mais pas les autres types de terminaux Android.

- Aperçu de l'intégration MDM
- Informations collectées
- Configuration système requise
- Configurer GlobalProtect pour récupérer des informations d'hôte
- Résoudre les problèmes du service d'intégration MDM



 ©2026 Palo Alto Networks, Inc.

Aperçu de l'intégration MDM

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Le service d'intégration MDM inclus avec l'agent User-ID Windows effectue une requête HIP complète sur le serveur MDM Workspace ONE pour obtenir les informations complètes sur l'hôte d'un périphérique mobile. Les applications GlobalProtect sur les périphériques mobiles envoient également des informations HIP à la passerelle, qui fusionne les informations HIP provenant des applications GlobalProtect et du service d'intégration MDM. Lorsqu'un périphérique mobile exécutant l'application GlobalProtect est connecté à une passerelle GlobalProtect, GlobalProtect peut appliquer des politiques de sécurité avec des profils d'informations d'hôte.

Vous pouvez configurer le service d'intégration MDM pour extraire les informations du périphérique Workspace ONE à intervalles réguliers et pour transmettre ces informations aux passerelles GlobalProtect. En outre, le service peut surveiller les notifications d'événements Workspace ONE et récupérer les informations de périphérique mises à jour lorsque des événements Workspace ONE (comme des modifications de conformité) se produisent.

Informations collectées

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Le tableau suivant montre comment le service d'intégration MDM traduit les informations collectées à partir des terminaux gérés par Workspace ONE en attributs de rapport HIP. Le mappage se fait automatiquement.

Attributs de Workspace ONE	Attributs de rapport HIP
Informations sur le périphérique	
SerialNumber (Numéro de série)	serial-number
MacAddress (Adresse Mac)	wifimac
Imei	IMEI

©2026 Palo Alto Networks, Inc.

Attributs de Workspace ONE	Attributs de rapport HIP
OperatingSystem (Système d'exploitation)	version
Modèle	model
DeviceFriendlyName (Nom convivial du périphérique)	devname
IsSupervised (Est supervisé)	supervisé
Udid (Identificateur de périphérique unique)	udid
UserName (Nom d'utilisateur)	user
LastEnrolledOn (Dernière inscription)	enroll-time
Platform (Plateforme)	os
EnrollmentStatus (État de l'inscription)	managed-by-mdm
LastSeen (Vu pour la dernière fois)	last-checkin-time
ComplianceStatus (Agent User-ID 8.0.3 et ultérieur)	Compliant (Conforme) NonCompliant (Non conforme) NotAvailable (Indisponible)
Propriétaire (Agent User-ID 8.0.3 et ultérieur)	Employee Owned (Appartient à l'employé) Corporate-Dedicated (Dédié à l'entreprise) Corporate-Shared (Partagé avec l'entreprise)
Informations de sécurité	
DataProtectionEnabled (Protection des données activée)	disk-encrypted
IsPasscodePresent (Mot de passe présent)	passcode-set
IsPasscodeCompliant (Mot de passe conforme)	passcode-compliant
Informations sur le réseau	
DataRoamingEnabled (Itinérance de données activée)	data-roaming

©2026 Palo Alto Networks, Inc.

Attributs de Workspace ONE	Attributs de rapport HIP
GPS Coordinates (Coordonnées GPS)	
Latitude	latitude
Longitude	longitude
SampleTime (Temps d'échantillonnage)	last-location-time
Détails de l'application	
ApplicationName (Nom de l'application)	appname
Version	version
ApplicationIndentifier (Identificateur de l'application)	package

Configuration système requise

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Le service d'intégration MDM Workspace ONE nécessite les logiciels suivants :

Logiciels	Version minimale prise en charge
agent User-ID	8.0.1
PAN-OS	7.1.0
Application GlobalProtect pour Android	4.0.0
Application GlobalProtect pour iOS	4.0.1
Serveur Workspace ONE	8.4.7.0
Windows Server	2008 et 2012

 ©2026 Palo Alto Networks, Inc.

Logiciels	Version minimale prise en charge
	2016 avec agent User-ID 8.0.4 et PAN-OS 8.0.4

Configurer GlobalProtect pour récupérer des informations d'hôte

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Utilisez les instructions suivantes pour configurer GlobalProtect afin de récupérer les informations d'hôte à partir des périphériques gérés par Workspace ONE.

1. Installation de l'agent User-ID. L'agent User-ID doit se trouver dans un emplacement permettant des connexions sécurisées au système de gestion de périphériques mobiles (MDM) VMware Workspace ONE.

   Le service d'intégration MDM Workspace ONE est fourni avec l'agent User-ID basé sur Windows PAN-OS.

2. Configurez l'authentification SSL entre l'agent User-ID basé sur Windows et la passerelle GlobalProtect.

   Lorsque vous configurez l'authentification SSL, assurez-vous que :

   - Le certificat de serveur configuré sur l'agent User-ID basé sur Windows a le même nom commun (CN) que le nom d'hôte / l'adresse IP de l'hôte de l'agent User-ID.
   - Le certificat de serveur est approuvé par le pare-feu (inclus dans la liste des CA de confiance dans la configuration MDM du pare-feu).
   - Le certificat d'autorité de certification racine (CA) du certificat client MDM configuré sur le pare-feu doit être importé dans le magasin de confiance Windows du serveur Windows.

     1. Procurez-vous un certificat de serveur et une clé privée pour l'authentification entre l'agent User-ID basé sur Windows et la passerelle GlobalProtect. L'ensemble de

 ©2026 Palo Alto Networks, Inc.

certificats doit être au format PEM et contenir un certificat PEM, une chaîne de certificats complète et une clé privée.

2. Ouvrez l'agent User-ID Windows et sélectionnez **Server Certificate (Certificat de serveur)**.
3. **Add (Ajoutez)** le certificat du serveur.

- **Browse (Parcourez)** jusqu'au fichier de certificat et **Open (Ouvrez)** le fichier pour télécharger le certificat vers l'agent User-ID Windows.
- Saisissez un **Private Key Password (Mot de passe de clé privée)** au certificat.
- Cliquez sur **OK**.

L'agent vérifie que le certificat est valide et stocke le mot de passe de chiffrement de la clé privée dans le magasin d'informations d'identification Windows de la machine hôte.

Si l'installation est réussie, des informations détaillées sur le certificat (y compris le nom commun, la date d'expiration et l'émetteur) s'affichent dans l'onglet **Server Certificate (Certificat de serveur)**.

1. Redémarrez l'agent User-ID basé sur Windows.

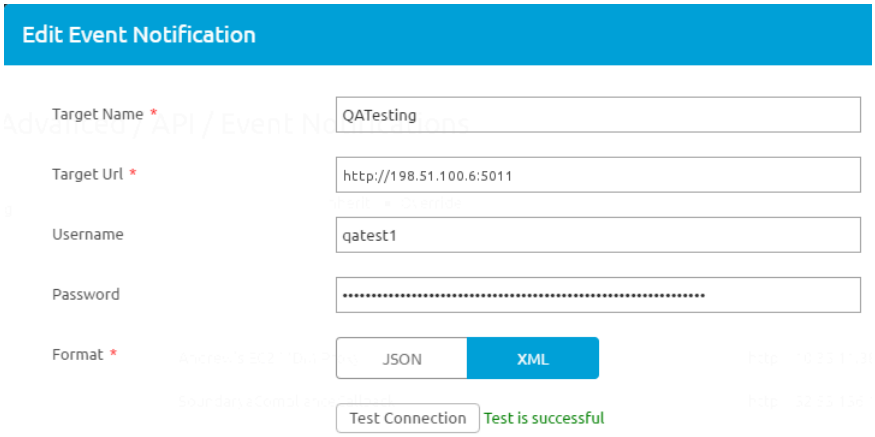
3. Configurez le service d'intégration MDM sur l'agent User-ID basé sur Windows.
   1. Sélectionnez **MDM Integration (Intégration MDM)** dans l'agent User-ID Windows.
   2. Spécifiez un **Gateway Connection TCP Port (Port TCP de connexion de passerelle** pour les communications TCP. L'agent User-ID basé sur Windows écoute sur ce port tous les messages liés à MDM. Le port par défaut est 5008. Pour changer de port, indiquez un chiffre entre 1 et 65 535.
   3. Dans l'onglet **Setup (Configuration)**, cliquez sur **Edit (Modifier)**.
   4. Choisissez **Workspace ONE** pour le **MDM Vendor (Fournisseur MDM)**.

4. Spécifiez les paramètres de la **MDM Event Notification (Notification d'événement MDM)** pour surveiller et collecter les événements Workspace ONE (par exemple, inscription d'un périphérique, retrait d'un périphérique et modifications de conformité). Lorsqu'un événement se produit, le service d'intégration MDM récupère les informations de périphérique mises à jour à partir de l'API Workspace ONE et transmet ces informations à toutes les passerelles GlobalProtect configurées.

   *Pour **MDM Event Notification (Notification d'événement MDM)**, assurez-vous que les valeurs que vous entrez ici sont également configurées dans la console Workspace ONE sous **Groups***

 ©2026 Palo Alto Networks, Inc.

& Settings (Groupes et paramètres) > All Settings (Tous les paramètres) > System (Système) > Advanced (Avancé) > API > Event Notifications (Notifications d'événement).



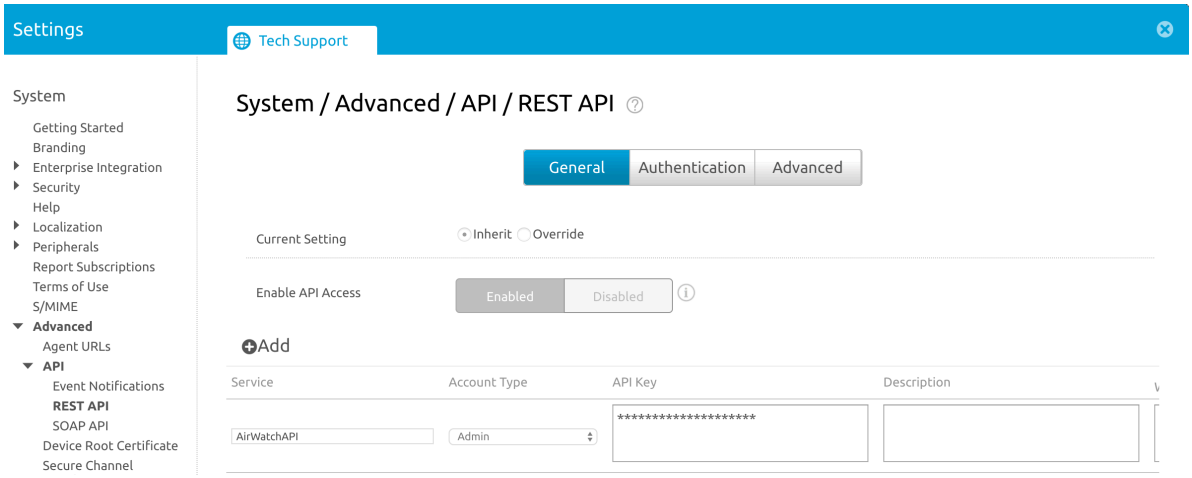
- Définissez le **TCP Port (Port TCP)** pour communiquer avec le service de notification d'événement. Utilisez ce format : **`http://<external_hostname>/<ip_address>:<port>`** où **`<ip-address>`** est l'adresse IP du service d'intégration MDM. Le port par défaut est 5011. Pour changer de port, indiquez un chiffre entre 1 et 65 535.
- Pour la notification d'événement, entrez les informations d'identification **Username (Nom d'utilisateur)** et **Password (Mot de passe)** nécessaires pour authentifier les demandes entrantes.
- Entrer les adresses **Permitted IP (IP autorisées)** pour accéder aux événements MDM. Il s'agit d'une liste d'adresses IP, séparées par des virgules, à partir de laquelle les événements MDM sont publiés. Par exemple, l'adresse IP du serveur Workspace ONE. Contactez votre équipe d'assistance Workspace ONE pour obtenir des instructions sur les adresses IP à spécifier.

5. Ajoutez les paramètres **MDM API Authentication (Authentification API MDM)** pour vous connecter à l'API Workspace ONE.

- Saisissez la **Server Address (Adresse du serveur)** du serveur MDM Workspace ONE auquel l'agent User-ID basé sur Windows se connectera. Par exemple, **`api.awmdm.com`**.
- Saisissez les informations d'identification **Username (Nom d'utilisateur)** et **Password (Mot de passe)** nécessaires pour accéder à l'API MDM Workspace ONE.
- Saisissez le **Tenant Code (Code du locataire)**. Il s'agit d'un numéro de code hexadécimal unique requis pour accéder à l'API MDM Workspace ONE. Sur la console Workspace ONE,

 ©2026 Palo Alto Networks, Inc.

vous pouvez trouver le code du locataire dans la section **System (Système)** > **Advanced (Avancé)** > **API** > **REST API (API REST)** > **API Key (Clé API)**.



- Entrer le **Mobile Device State Retrieval Interval (Intervalle de récupération de l'état du périphérique mobile)**. Ce paramètre contrôle la fréquence à laquelle les informations d'hôte sont récupérées des périphériques gérés par Workspace ONE. L'intervalle par défaut est de 30 minutes. Pour changer d'intervalle, indiquez un chiffre entre 1 et 600.

6. **Commit (Validez)** vos modifications.

7. Cliquez sur **Test Connection (Tester la connexion)** pour vous assurer que l'agent User-ID basé sur Windows peut se connecter à l'API Workspace ONE.

 ©2026 Palo Alto Networks, Inc.

8. Configurez la passerelle GlobalProtect pour communiquer avec le service d'intégration MDM afin de récupérer les rapports HIP pour les périphériques gérés par Workspace ONE.
   1. Dans l'interface Web PAN-OS, sélectionnez **Network (Réseau)** > **GlobalProtect** > **MDM**.
   2. **Add (Ajoutez** les informations suivantes à propos du service d'intégration MDM.

   - **Name (Nom)** : donnez un nom au service d'intégration MDM (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
   - (Facultatif) Sélectionnez le système virtuel auquel la passerelle appartient.
   - **Server (Serveur)** : saisissez l'adresse IP ou le FQDN de l'interface sur le service d'intégration MDM Workspace ONE où la passerelle se connecte pour récupérer les rapports HIP. Assurez-vous de disposer d'un itinéraire de service sur cette interface.
   - **Connection Port (Port de connexion)** : saisissez le port de connexion sur lequel le service d'intégration MDM écoute les demandes de rapport HIP. Le port par défaut est 5008. Pour changer de port, indiquez un chiffre entre 1 et 65 535.
   - **Client Certificate (Certificat client)** : choisissez le certificat client de la passerelle à présenter au service d'intégration MDM lors de l'établissement d'une connexion HTTPS. Vous pouvez choisir un certificat client dans la liste déroulante ou en importer un nouveau. Le **Certificate Purpose (Objectif du certificat)** doit indiquer qu'il s'agit d'un certificat d'authentification client.

     Le certificat d'autorité de certification (CA) racine du certificat client doit être importé dans le magasin de confiance Windows du serveur Windows sur lequel l'agent User-ID est installé.

     1. **Add (Ajoutez)** le certificat CA racine associé au certificat de serveur installé sur l'hôte du service d'intégration MDM. Vous avez besoin du certificat CA racine et du certificat de serveur pour établir une connexion sécurisée entre la passerelle et le service d'intégration MDM. Vous pouvez choisir un certificat CA racine dans la liste déroulante, ou *Import (Importer)* un nouveau certificat.
     2. Cliquez sur **OK**.
     3. **Commit (Validez)** vos modifications.

9. Vérifiez votre connexion pour vous assurer que les données du périphérique Workspace ONE sont transférées vers GlobalProtect.
   1. Ouvrez l'agent User-ID Windows et sélectionnez **MDM Integration (Intégration MDM)** > **Mobile Devices (Périphériques mobiles)**. Vous devriez voir une liste d'ID de périphérique et de noms d'utilisateur uniques pour tous les périphériques gérés par Workspace ONE.
   2. (Facultatif) Vous pouvez **Filter (Filtrer)** la liste pour trouver un **Mobile Device (Périphérique mobile** spécifique.
   3. (Facultatif). Sélectionnez un périphérique dans la liste des ID de périphériques et cliquez sur **Retrieve Device State (Récupérer l'état du périphérique)** pour extraire les dernières informations sur le périphérique et voir comment il mappe les profils d'informations d'hôte sur la passerelle GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Résoudre les problèmes du service d'intégration MDM

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Suivez ces instructions si vous rencontrez des problèmes avec les notifications d'événements ou si vous ne parvenez pas à vous authentifier auprès de l'API REST Workspace ONE.

Les notifications d'événements provenant du serveur MDM Workspace ONE ne sont pas reçues par le service d'intégration MDM.

1. Définissez l'option **Debug (Déboguer)** (dans le menu **File (Fichier)**) sur **Debug (Déboguer)** ou **Verbose (Commentaires)**.
2. Allez dans le dossier d'installation de l'agent User-ID sur le serveur Windows, puis ouvrez le fichier `MaDebug`. Recherchez des messages similaires au suivant :

```
L'adresse x.x.x.x n'est pas dans la liste IP autorisée pour
 les notifications d'événements.
```

3. Ajoutez cette adresse IP en tant qu'adresse **Permitted IP (IP autorisée)** (**MDM Integration (Intégration MDM)** > **Setup (Configuration)** > **Permitted IP (IP autorisée)**).

L'authentification à l'API REST Workspace ONE a échoué.

Assurez-vous que :

- Les informations d'identification utilisées pour le service d'intégration MDM pour s'authentifier auprès du service MDM Workspace ONE sont valides.
- Le compte utilisateur utilisé pour accéder à l'API REST Workspace ONE possède des autorisations d'accès API et des autorisations en lecture seule (au minimum) sur les données pour les périphériques mobiles et les utilisateurs gérés par Workspace ONE.
- Le **Tenant Code (Code du locataire)** (clé API) est correctement associé au compte utilisateur. Retirez toutes les clés API inutilisées.

Périphériques en quarantaine utilisant les informations de l'hôte

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect vous permet d'ajouter des périphériques compromis à la liste de quarantaine soit manually (manuellement) ou automatically (automatiquement). Après avoir mis le périphérique

 ©2026 Palo Alto Networks, Inc.

en quarantaine, vous pouvez block users from logging into the network (bloquer la connexion des utilisateurs au réseau) depuis ce périphérique en utilisant GlobalProtect. Vous pouvez aussi restreindre le trafic vers un périphérique compromis, depuis un périphérique compromis ou les deux. Si vous utilisez un appareil Panorama, vous pouvez aussi redistribute the quarantined device information (redistribuer les informations du périphérique en quarantaine) vers les autres pare-feux nouvelle génération. Utilisez les sujets suivants pour apprendre comment mettre un périphérique en quarantaine, y compris les exigences de licence d'abonnement à GlobalProtect et comment redistribuer les informations de quarantaine.

Aperçu de l'identification et mise en quarantaine des périphériques compromis et Exigences de la licence

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect vous permet de bloquer facilement des périphériques compromis sur votre réseau en identifiant un périphérique compromis par son Host ID (ID d'hôte) et, en option, le numéro de série de son adresse IP source. Cette capacité est préférable au blocage d'un terminal compromis depuis un réseau sur la base de son adresse IP car si l'adresse IP d'un périphérique change (par exemple si l'utilisateur déplace son terminal du travail à son domicile), les politiques de sécurité basées sur les adresses IP pourraient autoriser le terminal à accéder à nouveau au réseau.

Après avoir identifié un périphérique comme étant compromis (par exemple, si un périphérique a été infecté par un malware et effectue des commande d'exécution et des actions de contrôle), vous pouvez manuellement ajouter l'ID de l'hôte à une liste de quarantaine et configurer GlobalProtect afin d'empêcher les utilisateurs de se connecter à la passerelle GlobalProtect depuis un périphérique en quarantaine. Vous pouvez aussi mettre le périphérique en quarantaine automatiquement à l'aide des log forwarding profiles (profils de transfert de journaux) et les politiques de sécurité ou HIP match (correspondance HIP) log settings (paramètres des journaux).

> *À partir de la version Android 8.0, l'application GlobalProtect est incapable de récupérer le numéro de série du périphérique car l'application GlobalProtect n'est pas l'application propriétaire du périphérique ou l'application propriétaire du profil. Dans ce cas, vous pouvez utiliser ANDROID_ID comme numéro de série du périphérique. ANDROID_ID est spécifique à une application sur un périphérique Android et l'ID peut changer lors de la réinitialisation de votre périphérique Android aux paramètres d'usine.*

Avant de commencer à mettre des périphériques en quarantaine, veillez à ce que les utilisateurs de GlobalProtect utilisent au minimum la version 5.1 de l'application GlobalProtect. De plus, veillez à ce qu'une licence d'abonnement valide à GlobalProtect soit présente sur le pare-feu afin que le pare-feu puisse ajouter des périphériques compromis à la liste de quarantaine. Les exigences de licence d'abonnement GlobalProtect pour cette fonctionnalité sont appliquées tel que cela est décrit dans la liste suivante.

- Le pare-feu a besoin d'une licence d'abonnement GlobalProtect afin d'ajouter, manuellement ou automatiquement, des périphériques à la liste de quarantaine. Vous recevez le message d'erreur suivant si vous essayez d'ajouter un périphérique sans licence : `Le périphérique`

 ©2026 Palo Alto Networks, Inc.

```
ne peut pas être mis en quarantaine. Vous devez posséder un
abonnement valide à GlobalProtect pour ajouter un périphérique à la
liste de quarantaine.
```

Cependant, vous pouvez supprimer les périphériques en quarantaine de la liste de quarantaine sans licence.

- Si votre licence d'abonnement GlobalProtect expire, la liste de quarantaine est conservée et n'est pas supprimée.

  GlobalProtect vérifie la licence toutes les heures.

- Si vous ne possédez pas de licence GlobalProtect valide et qu'une des conditions suivantes est vraie, votre pare-feu ou Panorama affiche un message d'avertissement lorsque vous effectuez la modification :
  - Vous avez sélectionné **Quarantine List (Liste de quarantaine)** dans un agent de redistribution des données.
  - Vous avez sélectionné **Quarantine (Quarantaine)** en tant qu'action intégrée du **Log Forwarding Profile (profil de transfert des journaux)**.

Afficher les informations du périphérique en quarantaine

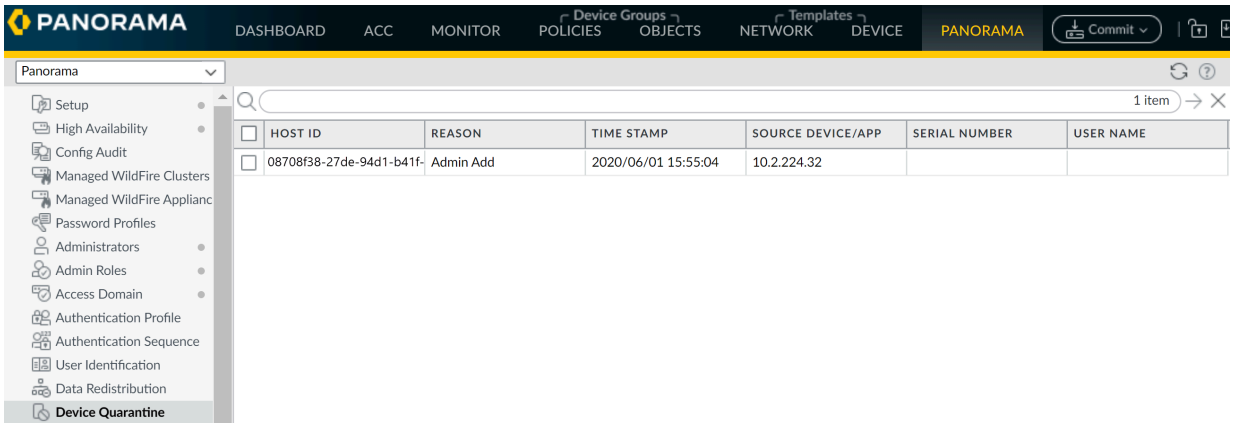
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous affichez les informations du périphérique en quarantaine depuis la page **Device Quarantine**. L'emplacement de la page est différent si vous l'affichez depuis un pare-feu nouvelle génération ou un appareil Panorama.

- Dans les pare-feux nouvelle génération, affichez la liste des périphériques en quarantaine en sélectionnant **Device (périphérique)** > **Device Quarantine (Quarantaine des périphériques)**.

 ©2026 Palo Alto Networks, Inc.

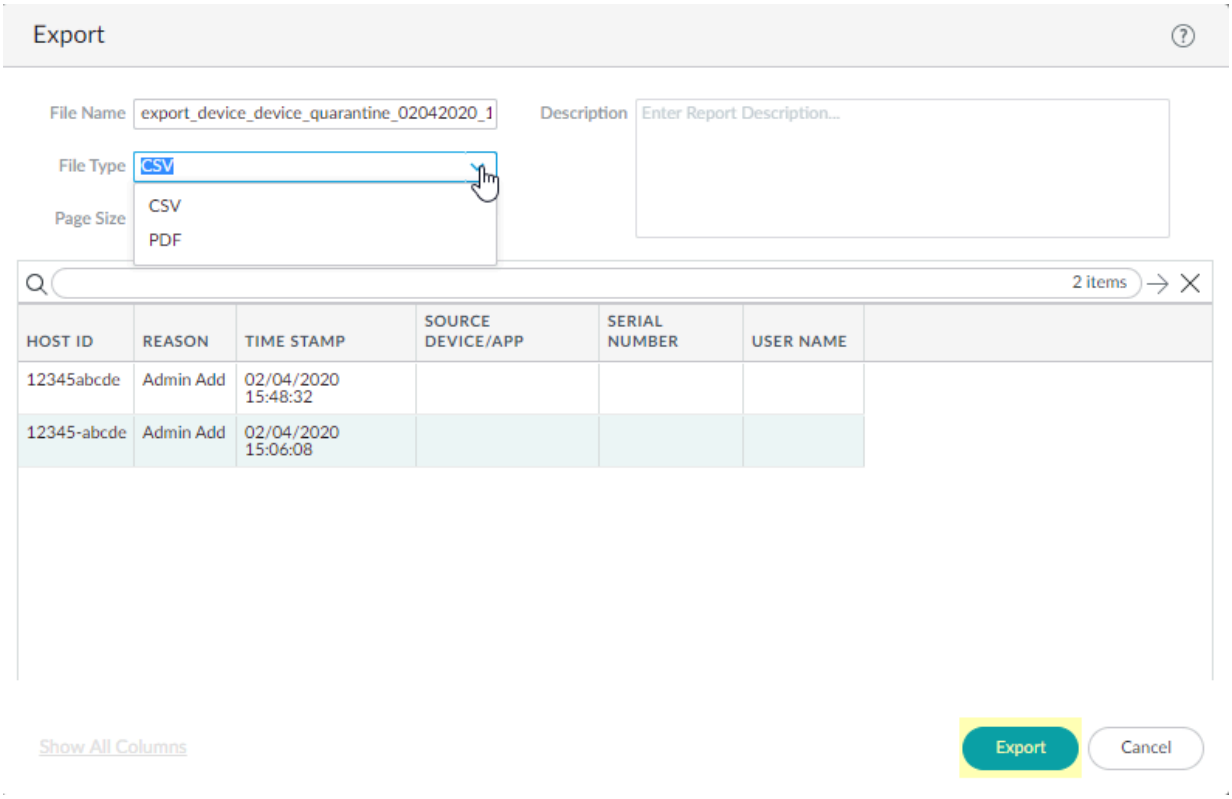
- Pur la appareils Panorama affichez **Device (Périphérique)** > **Device Quarantine (Quarantaine des périphériques)** en sélectionnant **Panorama** > **Device Quarantine (Quarantaine des périphériques)**.



- Vous pouvez également voir l'activité de quarantaine de GlobalProtect depuis ACC. L'onglet**GlobalProtect Quarantine Activity (Activité de quarantaine GlobalProtect)** dans l'ACC contient un plan, **GlobalProtect Quarantine Activity (Activité de quarantaine GlobalProtect)**, qui affiche un résumé des périphériques qui ont été mis en quarantaine. Utilisez le bouton en haut du tableau pour afficher les périphériques mis en quarantaine selon les actions qui ont amené GlobalProtect à mettre le périphérique en quarantaine, la raison pour laquelle GlobalProtect a mis le périphérique en quarantaine et l'emplacement des périphériques mis en quarantaine.

 ©2026 Palo Alto Networks, Inc.

- Pour exporter la liste des périphériques en quarantaine à un fichier pdf ou csv, sélectionnez **PDF/CSV**en bas de la page **Device Quarantine (Quarantaine des périphériques)** pour ouvrir la page **Export (Exporter)** page.



Ajouter et supprimer manuellement des périphériques de la liste de quarantaine

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

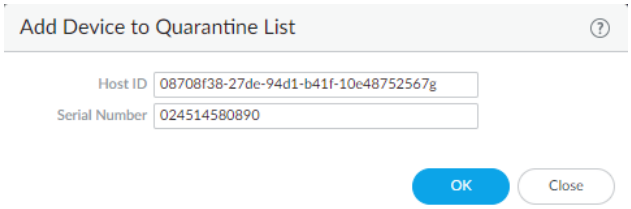
Vous pouvez ajouter une périphérique manuellement depuis les pages de quarantaine, depuis les jounaux GlobalProtect, Threat (Menace), Traffic (Trafic), ou Unified (Unifié) ou en utilisant un API. Vous pouvez aussi supprimer manuellement le périphérique depuis les pages de quarantaine tel que cela est indiqué dans les étapes suivantes.

Pour ajouter manuellement un périphérique à la liste de quarantaine de la page**Device Quarantine (Quarantaine des périphériques)**, sélectionnez **Device (Périphérique)** > **Device**

 ©2026 Palo Alto Networks, Inc.

Quarantine (Quarantaine des périphériques) ou **Panorama** > **Device Quarantine (Quarantaine des périphériques)** et **Add (Ajoutez)** le périphérique.

Ajoutez le **Host ID (ID d'hôte)** et, en option, le **Serial Number (numéro de série)** du périphérique. GlobalProtect utilise l'ID de l'hôte pour identifier le périphérique.



pour ajouter un périphérique à la liste de quarantaine depuis les journaux GlobalProtect, Threat (Menace), Traffic (Trafic), ou Unified (Unifié) , respectez les étapes suivantes.

1. (journaux Menace, Trafic et Unifiés uniquement) Pour ajouter des informations aux jounaux de Trafic, Menace et Unifié, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajouter)** une règle de politique de sécurité ; puis sélectionnez **Quarantine (Quarantaine)** en tant que **Source Device (Périphérique source)** pour le trafic **Source**.

   Un ID d'hôte est nécessaire pour ajouter un périphérique à la liste de quarantaine. Lorsqu'un utilisateur se connecte au réseau avec l'application GlobalProtect, GlobalProtect ajoute automatiquement les informations de l'ID d'hôte du terminal connecté au journal GlobalProtect. La valeur d'ID hôte varie selon le type de point de terminaison :

   - Windows – GUIDE machine stocké dans le registre Windows (HKEY_Local_Machine \Software\Microsoft\Cryptography\MachineGuid)
   - macOS – Adresse MAC de la première interface de réseau physique intégrée
   - Android – ID Android
   - iOS – UDID
   - Chrome – La chaîne alphanumérique unique d'une longueur de 32 caractères affectée par GlobalProtect.

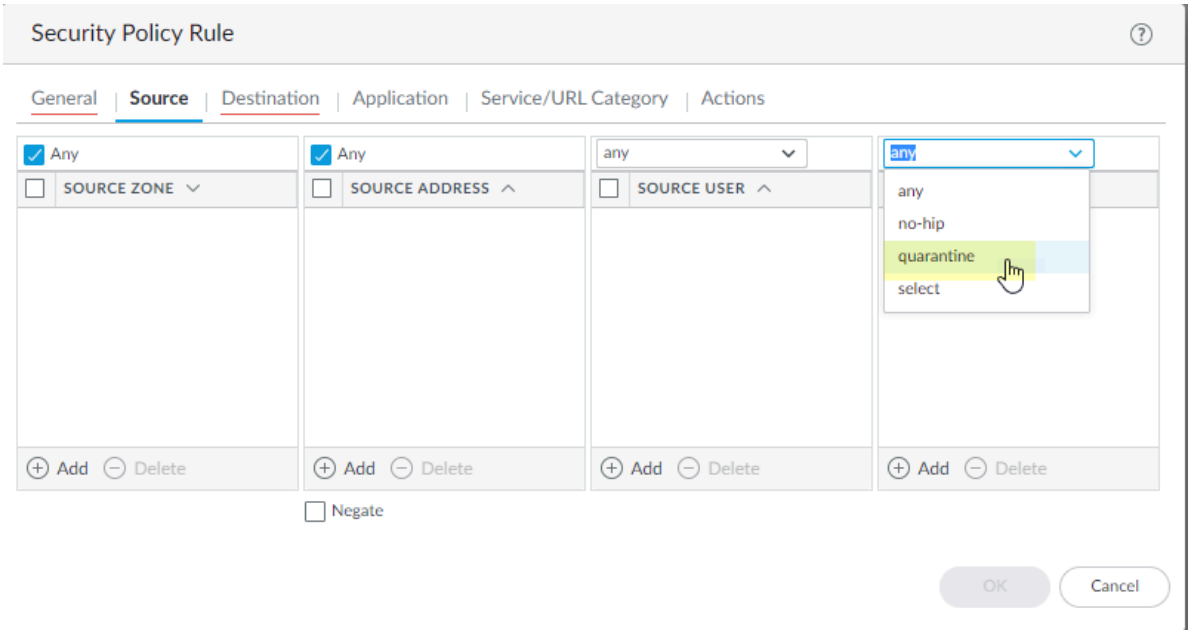
   Si vous ne connaissez pas l'ID d'hôte, vous pouvez associer l'User-ID à l'ID d'hôte dans les journaux de correspondance HIP :

   - Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **HIP Match (Correspondance HIP)**.
   - Filtrez les journaux de correspondance HIP pour l'utilisateur source associé au point de terminaison.

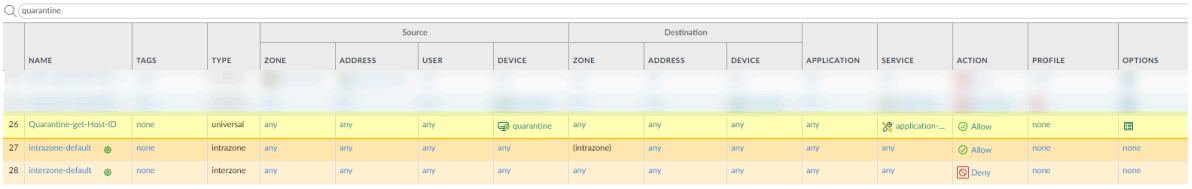
 ©2026 Palo Alto Networks, Inc.

- Ouvrez le journal de correspondance HIP et identifiez l'ID d'hôte sous **OS (Système d'exploitation)** > **Host ID (ID d'hôte)** et éventuellement le nom d'hôte sous **Host Information (Informations de l'hôte)** > **Machine Name (Nom de la machine)**.

Pour que GlobalProtect ajoute automatiquement les informations de l'ID d'hôte aux journaux de Trafic, Menace ou Unifié, vous devez ajouter une règle de politique qui a sélectionné **Quarantine (Quarantaine)** pour le trafic source.



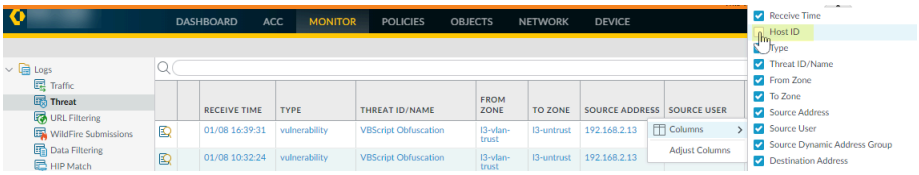
Afin d'être sûr que vous ajoutez l'ID d'hote pour tous les périphériques que vous voulez mettre en quarantaine (manuellement ou automatiquement), créez une politique de sécurité qui autorise tout le trafic et indiquez ***Quarantine (Quarantaine)*** *comme* ***Source Device (périphérique source)****. L'ordre dans lequel vous placez cette politique dans la liste des politiques n'a pas d'importance pour son fonctionnement.*



 ©2026 Palo Alto Networks, Inc.

2. Faites un clic droit sur le **Host ID (ID d'hôte)** associé au périphérique et cliquez sur **Block Device (bloquez le périphérique)**.

Si la colonne**Host ID (ID de l'hôte)** ne s'affiche pas, sélectionnez l'en-tête de n'importe quelle colonne puis sélectionnez le champ **Host ID (ID d'hôte)** pour afficher l'ID d'hôte.



Pour créez un APOI afin d'ajouter manuellement des périphériques, consultez les instructions dans le PAN-OS and Panorama API Usage Guide (Guide d'utilisation de PAN-OS et de l'API Panorama).

Une fois que votre administrateur a restauré le périphérique, vous pouvez le supprimer de la liste en sélectionnant **Device** > **Device Quarantine (Quarantaine du périphérique)** pour les pare-feux nouvelle génération ou **Panorama** > **Device Quarantine (quarantaine des périphériques)** pour les périphériques Panorama, en sélectionnant un ou plusieurs périphérique puis **Delete (supprimer)**.

Mettre automatiquement un périphérique en quarantaine

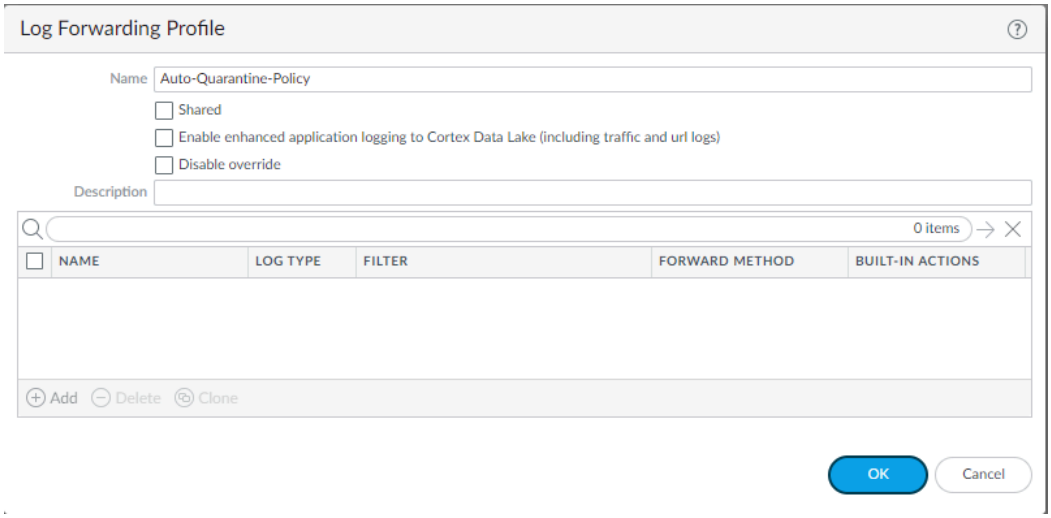
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez aussi mettre le périphérique en quarantaine automatiquement à l'aide du profil de transfert de journaux et d'une politique de sécurité ou des paramètres de correspondance HIP.

 ©2026 Palo Alto Networks, Inc.

Pour mettre un périphérique en quarantaine en utilisant un profil de transfert des journaux, respectez les étapes suivantes.

1. Sélectionnez **Object (Objet)** > **Log Forwarding (transfert des journaux)** et soit **Add (Ajouter)** un nouveau log forwarding profile (profil de transfert des journaux) ou sélectionnez un profil existant pour le modifier.



2. **Add (Ajoutez)** une **Log Forwarding Profile Match List (Liste de correspondance de profil de transfert des journaux)** et dans la partie **Built-in Actions (Actions intégrées)** sélectionnez **Quarantine (Quarantaine)**.

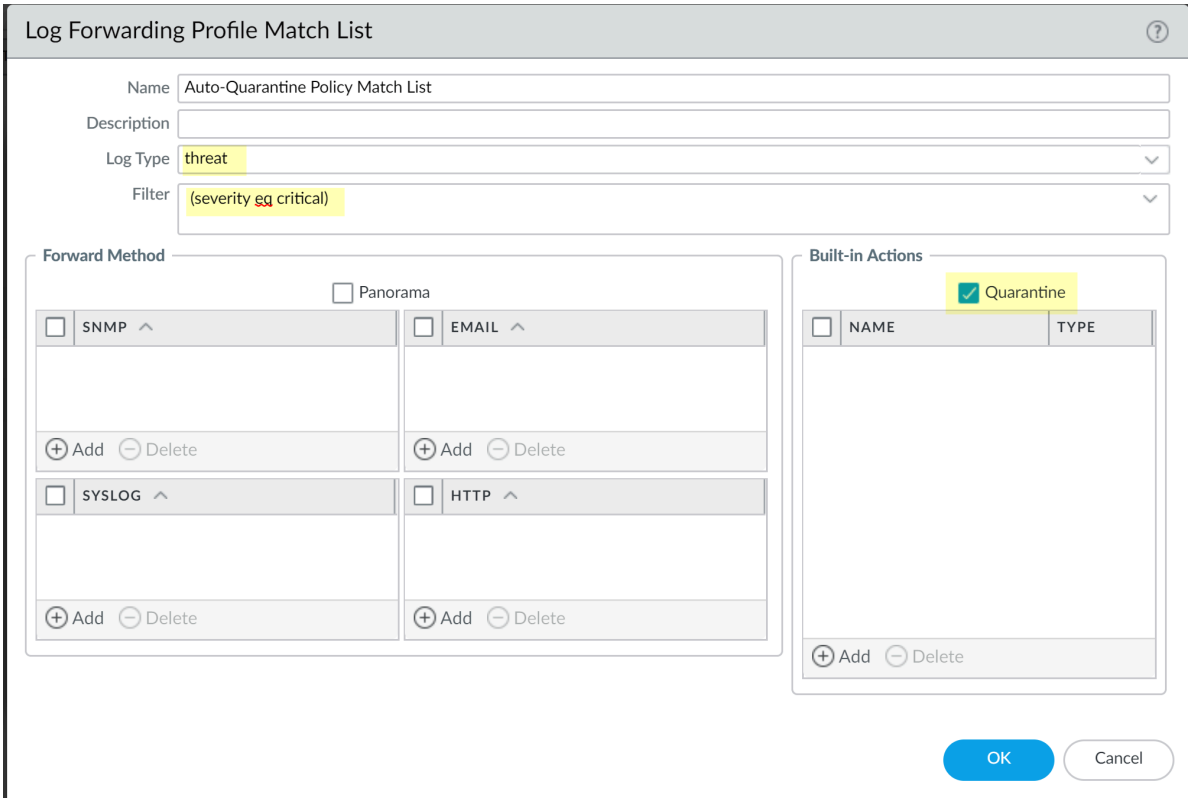
   Indiquez un **Log Type (type de journal)** entre **GlobalProtect**, **Threat (Menace)**, ou **Traffic (Trafic)**.

   > *Si vous indiquez un **Log Type (Type de journal)** entre**Threat (Menace)** ou **Traffic (Trafic)**, veillez à ce qu'un ID d'hôte soit associé avec un périphérique en créant une règle de politique de sécurité qui a **Quarantine (Quarantaine)** en tant que **Source Device (Périphérique source)** pour le trafic **Source** afin d'ajouter l'ID d'hôte. Sans ID d'hôte, vous ne pouvez pas ajouter de périphérique à la liste de quarantaine.*

   L'exemple suivant utilise un **Log type (type de journal)** de **Threat (Menace)** et une gravité de niveau critique. Une fois que vous avez ajouté ce profil à une politique de sécurité et que

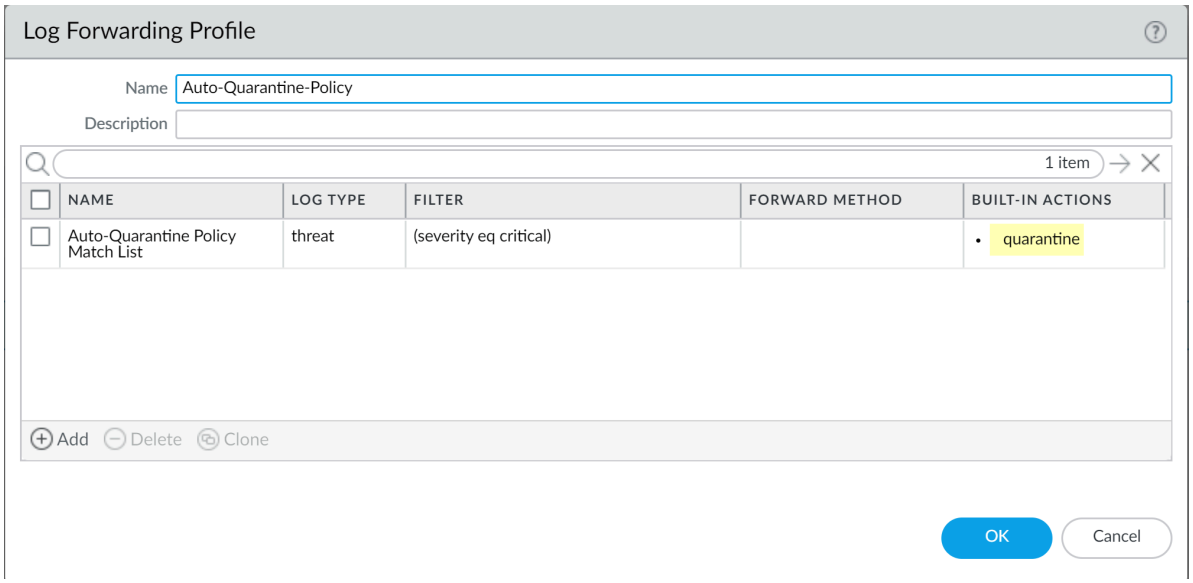
 ©2026 Palo Alto Networks, Inc.

ces critères correspondent, le pare-feu ajoute les périphériques depuis lesquels ce trafic arrive à la liste de quarantaine.

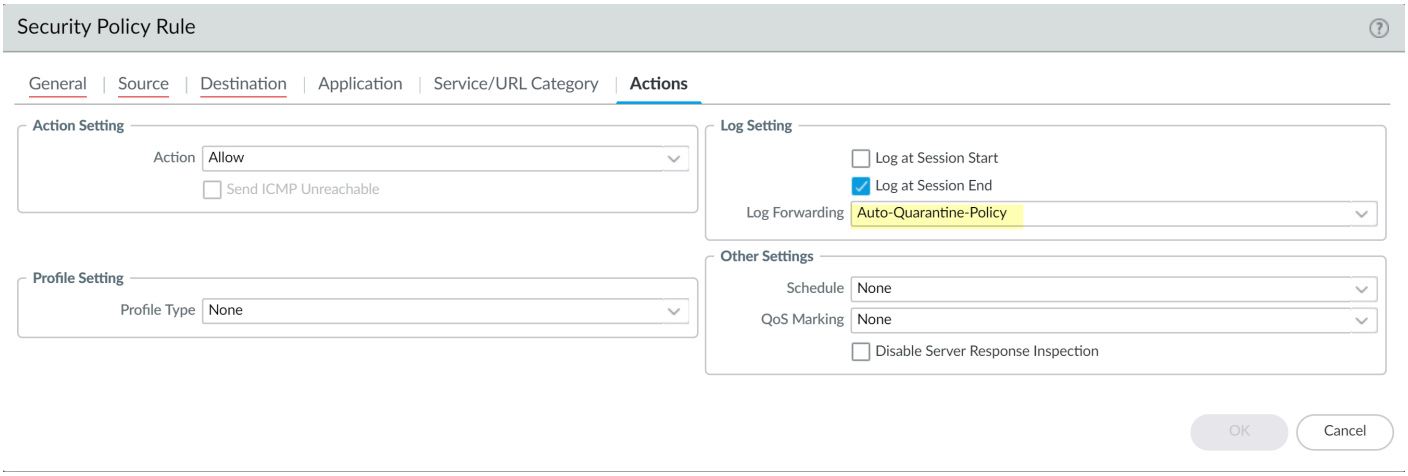


Une fois que vous avez ajouté la liste de correspondance, le profil de transfert des journaux affiche **Quarantine (Quarantaine)** sous **Built-In Actions (Actions intégrées)**

 ©2026 Palo Alto Networks, Inc.



3. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et **Add (Ajoutez)** une politique de sécurité.
4. Sélectionnez **Actions** puis sélectionnez le profil de **Log Forward (Transfert de journaux)** que vous avez créé.

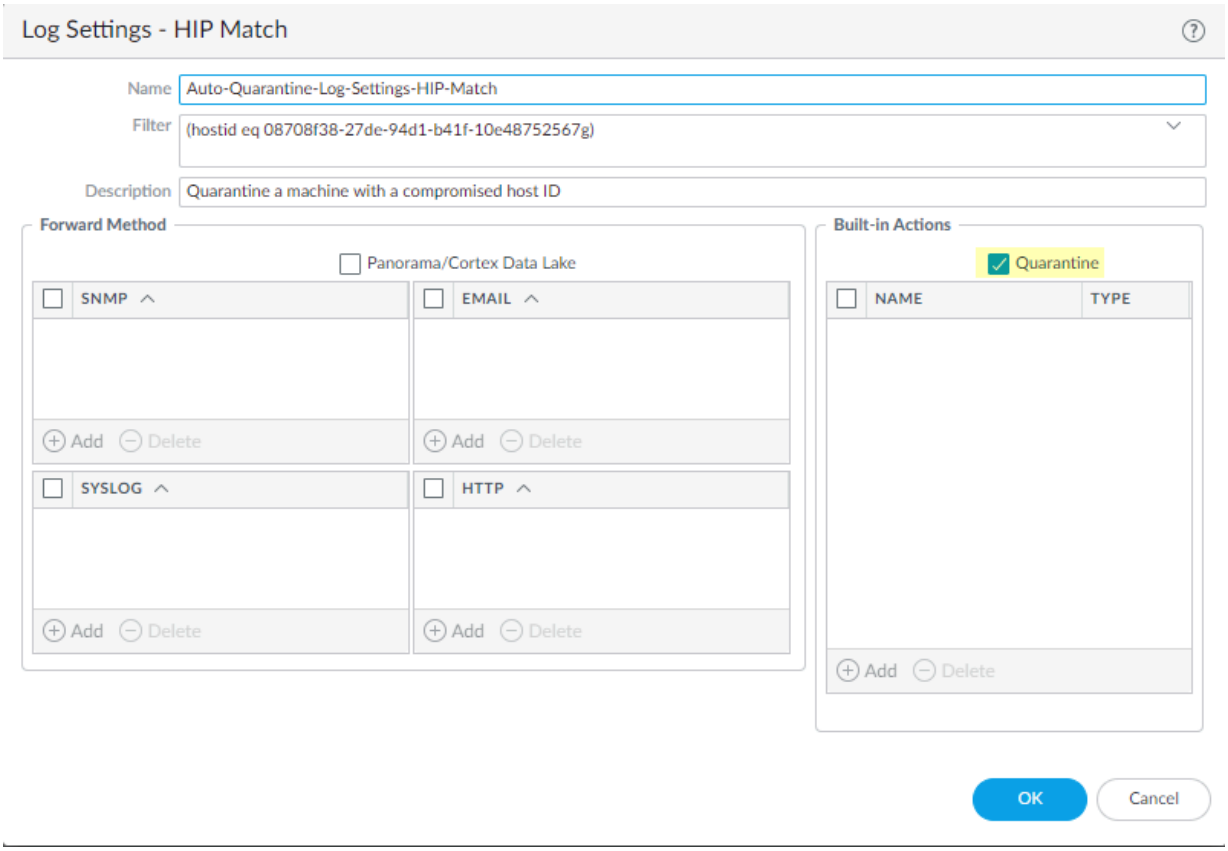


Pour mettre automatiquement un périphérique en quarantaine en utilisant les paramètre de journal de correspondance HIP, sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** > **HIP Match (correspondance HIP)** et**Add (Ajouter)** un paramètre de journal avec des **Built-In Actions (Actions intégrées)** de **Quarantine (Quarantaine)**.

Le paramètre de journal suivant à un **Filter (filtre)** avec une ID d'hôte de 08708f38-27de-94d1-b41f-10e48752567g. Si les journaux de correspondance HIP trouvent une correspondance pour cet ID d'hôte, ce paramètre de journal ajoute ce périphérique à la

 ©2026 Palo Alto Networks, Inc.

liste de quarantaine. Contrairement au profil de transfert des journaux, vous n'avez pas besoin de joindre ce paramètre de journal à une politique de sécurité pour qu'il prenne effet.



Utiliser GlobalProtect et les politiques de sécurité pour bloquer l'accès aux périphériques en quarantaine.

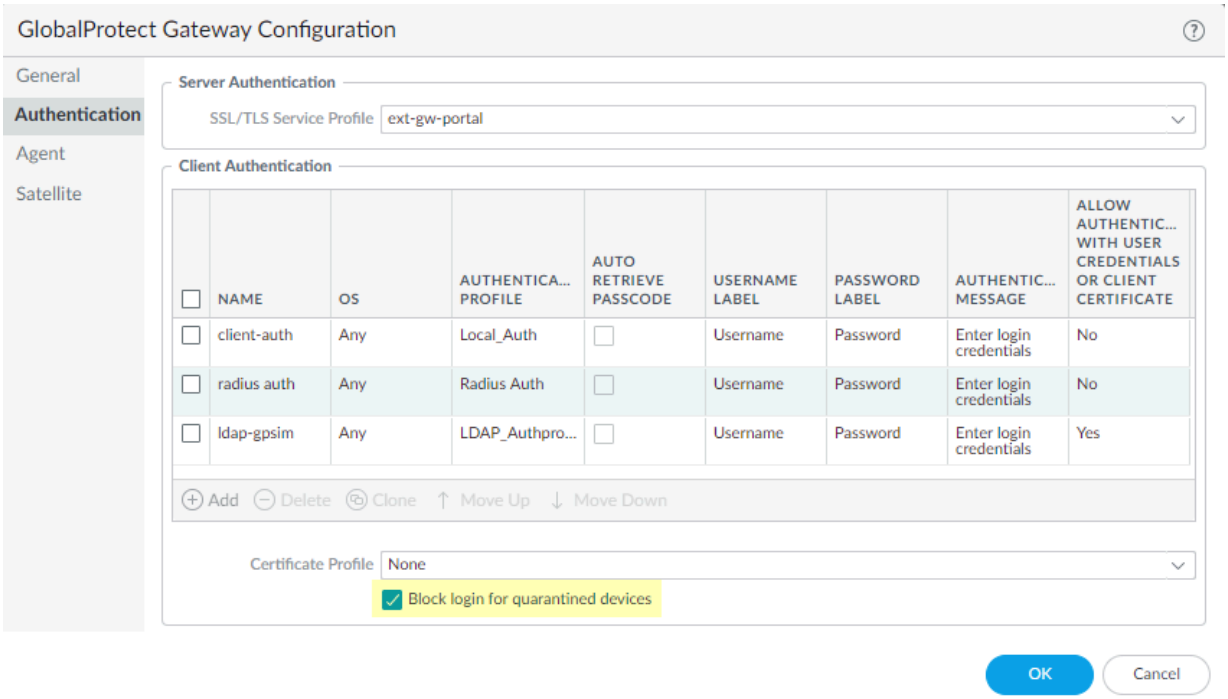
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Vous pouvez empêcher les utilisateurs de se connecter à GlobalProtect depuis un périphérique en quarantaine en configurant l'authentification de la passerelle. De plus, vous pouvez empêcher un périphérique en quarantaine d'envoyer ou de recevoir du trafic sur le réseau en indiquant

 ©2026 Palo Alto Networks, Inc.

des options dans la règle de politique de sécurité. Utilisez les tâches suivantes pour bloquer des utilisateurs de GlobalProtect ou gérez l'accès au réseau pour un périphérique en quarantaine.

Pour empêcher des utilisateurs de se connecter à GlobalProtect depuis un périphérique en quarantaine, configurez l'authentification de passerelle GlobalProtect (**Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > ***gateway-configuration (Configuration de passerelle)*** > **Authentication (Authentification)**) et sélectionnez **Block login for quarantined devices (Bloquer la connexion pour les périphériques en quarantaine)**.



Si un utilisateur essaye de se connecter depuis un périphérique en quarantaine à une passerelle qui a activé **Block login for quarantined devices (Bloquer la connexion pour les périphériques en quarantaine)**, l'application GlobalProtect prévient l'utilisateur que le périphérique est en quarantaine et que l'utilisateur ne peut pas se connecter depuis ce périphérique. Si ce paramètre n'est pas activé, l'utilisateur reçoit la notification mais peut se connecter depuis ce périphérique.

Pour bloquer l'accès à un périphérique en quarantaine en utilisant une règle de politique de sécurité, indiquez **Quarantine (Quarantaine)** pour la source ou la destination du trafic ; ensuite, indiquez une action qui bloque le périphérique en quarantaine.

Indiquer **Quarantine (Quarantaine)** dans une règle de politique de sécurité signifie que la règle utilise des périphériques dans la liste de quarantaine comme critères de correspondance, que vous indiquiez **Quarantine (Quarantaine)** en tant que **Source device (périphérique source)**

 ©2026 Palo Alto Networks, Inc.

pour le trafic **Source** ou le **Destination Device** pour le trafic **Destination**. Les exemples suivants montrent un **Device (périphérique)** source de **Quarantine (Quarantaine)** une adresse IP de destination du serveur HQ et une action de **Deny (Refuser)**. Avec cette règle de politique de sécurité, tous les périphériques de la liste de quarantaine ne pourront pas accéder au serveur HQ.

	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION
26	Block-quarantined-devices-from-HQ-server	none	universal	any	any	any	quarantine	any	HQ-server	any	any	any	Deny
27	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	any	Allow
28	interzone-default	none	interzone	any	any	any	any	any	any	any	any	any	Deny

Pour qu'un périphérique en quarantaine soit valide dans une politique sur un pare-feu, un utilisateur GlobalProtect doit réussir à se connecter à GlobalProtect depuis le périphérique en quarantaine et le pare-feu doit être au courant de cet événement de connexion. Si le pare-feu est configuré en tant que passerelle GlobalProtect, l'utilisateur peut se connecter à cette passerelle depuis le périphérique en quarantaine pour valider le périphérique dans la politique. Après que l'utilisateur ait réussi à se connecter à une passerelle depuis un périphérique en quarantaine, la passerelle applique la politique et vous pouvez redistribute the quarantined device information (redistribuer les informations du périphérique en quarantaine) *et pour qu'elles soient appliquées dans une politique sur un pare-feu ou une passerelle de votre réseau. Si la connexion de l'utilisateur est bloquée sur la passerelle (par exemple, si vous avez sélectionné **Block login for quarantined devices (Bloquer la connexion pour les périphériques en quarantaine)** dans la configuration de passerelle), cette connexion n'est pas comptabilisée dans les connexions réussies.*

Redistribuer les informations du périphériques en quarantaine depuis Panorama

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama) • Prisma Access (géré par Panorama)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Si vous gérez vos pare-feu nouvelle génération à l'aide d'un périphérique Panorama, vous pouvez créer une liste de quarantaine pour tous les pare-feux dans **Panorama** > **Device Quarantine (Quarantaine des périphériques)** et distribuez ces informations à vos pare-feux gérés. Vous redistribuez les informations de quarantaine des périphériques de la même façon que vous redistribute User-ID information (redistribuez des informations sur l'ID de l'utilisateur). Respectez les étapes suivantes pour redistribuer les informations de quarantaine depuis Panorama.

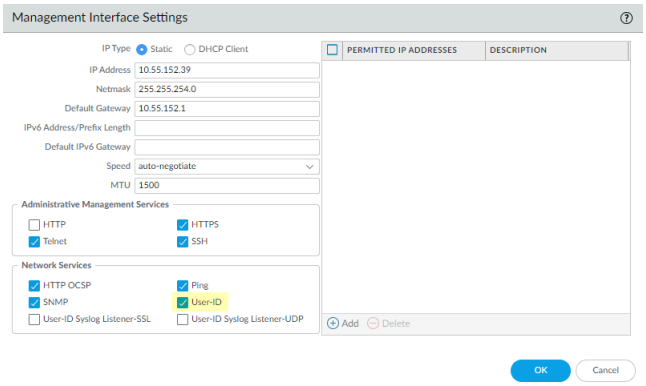
1. Activez User-ID sur le serveur de l'agent si vous ne l'avez pas déjà fait.

   - Si le serveur de l'agent de redistribution utilise l'interface de gestion, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Interfaces** > **Management (Gestion)** et sélectionnez **User-ID**.

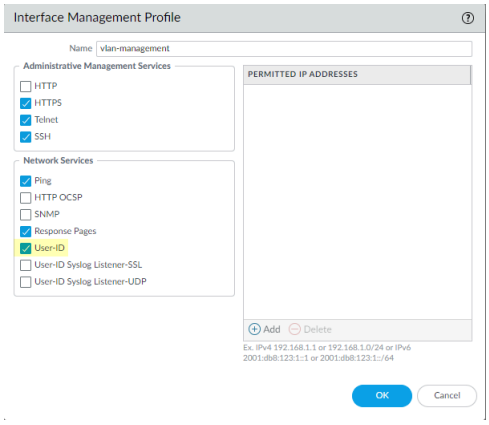
     Si vous vous utilisez Strata Cloud Manager (NGFW), sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la**

 ©2026 Palo Alto Networks, Inc.

configuration) > All Firewalls (Tous les pare-feu) > Devices (Périphériques) > Interfaces > Add Interface (Ajouter un interface) > Interface



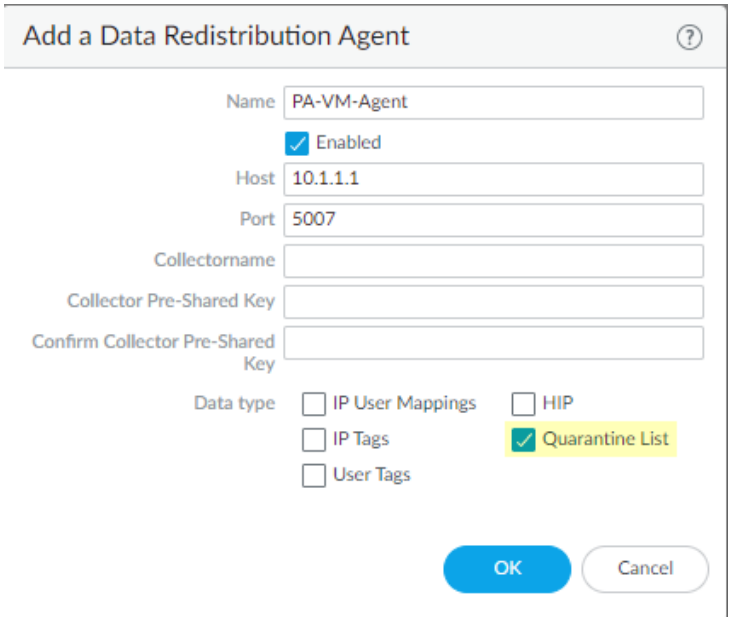
- Si l'agent de redistribution utilise une interface sur le plan de données (par exemple, une interface Ethernet ou VLAN), sélectionnez **Network (Réseau)** > **Interface Mgmt (Gestion des interfaces)**, sélectionnez un profil de gestion existant ou **Add (Ajoutez)** un nouveau et sélectionnez **User-ID**.



 ©2026 Palo Alto Networks, Inc.

2. Pour créer un agent de redistribution des données, sélectionnez **Panorama** > **Data Redistribution (Redistribution des données)** et **Add (Ajoutez)** l'agent.

L'exemple suivant montre un agent de redistribution des données dans lequel Panorama distribue les informations de la **Quarantine List (Liste de quarantaine)** au pare-feu avec une adresse IP de 10.1.1.1 utilisant le port 5007.



Résoudre les problèmes HIP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Les problèmes HIP surviennent généralement lorsque l'évaluation de la posture du terminal de l'application GlobalProtect (produits installés, vérifications personnalisées, paramètres de chiffrement et de sauvegarde, etc.) ne correspond pas aux objets et profils HIP attendus, ce qui fait correspondre le trafic provenant du client GlobalProtect à des politiques de sécurité inattendues. Des problèmes HIP se produisent également lorsque les fournisseurs ne sont pas pris en charge par le module OPSWAT utilisé par l'application GlobalProtect pour HIP. Lorsque l'évaluation de l'application GlobalProtect ne correspond pas à HIP du côté de la passerelle GlobalProtect, les utilisateurs finaux bénéficient d'un accès limité ou d'aucun accès en fonction de la politique de sécurité configurée. Les problèmes HIP se situent le plus souvent du côté du client, par exemple lorsque le module OPSWAT n'évalue pas correctement certains produits ou certaines versions. Les problèmes du côté de la passerelle GlobalProtect sont principalement des objets et profils HIP configurés de manière incorrecte, ou des problèmes de redistribution HIP.

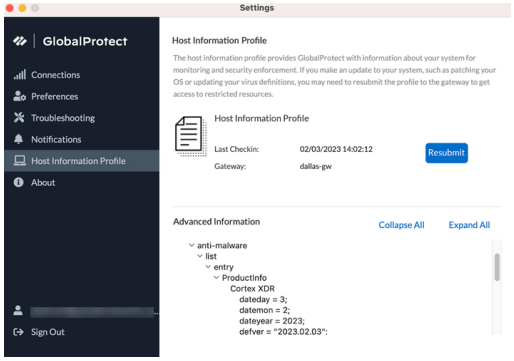
Suivez les étapes suivantes pour identifier ou déterminer si un problème HIP se situe du côté du client GlobalProtect ou du côté du pare-feu ou de la passerelle GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

1. Assurez-vous que l'application GlobalProtect n'a aucun problème pour identifier les attributs ou logiciels HIP spécifiques, tels que : pare-feu, anti-malware, et plus encore.

   En prenant comme exemple l'anti-malware, chaque version de l'application GlobalProtect possède une base de données OPSWAT fixe. Si un nouveau produit ou une nouvelle version anti-malware est disponible, l'application GlobalProtect actuellement installée pourrait ne pas être en mesure de le détecter ou, dans certains cas, ses fonctionnalités de détection pourraient être réduites. Reportez-vous au graphique OPSWAT des produits pris en charge pour vérifier si un nouveau produit anti-malware est pris en charge. S'il est pris en charge, mais n'est pas détecté, vous pouvez essayer d'installer la dernière application GlobalProtect.

   1. Depuis l'application GlobalProtect, sélectionnez **Settings (Paramètres)** > **Host Information Profile (Profil d'informations sur l'hôte)**.
   2. Vérifiez la catégorie HIP exacte.

   3. Si le produit anti-malware est non identifié, essayez d'installer une nouvelle version de l'application GlobalProtect contenant une version mise à jour de la base de données OPSWAT si disponible. Vous pouvez également essayer de consulter les notes sur la version de l'application GlobalProtect. Lorsque l'application GlobalProtect est mise à jour, les notes de version de la nouvelle version listent les produits anti-malware pour lesquels la capacité de détection OPSWAT est mise à jour ou corrigée en fonction des problèmes signalés par les clients.

2. Assurez-vous que l'application GlobalProtect a envoyé le rapport HIP avec les informations sur la posture du terminal.

   1. Affichez et collectez les journaux d'application GlobalProtect.
   2. Vérifiez si l'application GlobalProtect a transmis le rapport au pare-feu de la passerelle GlobalProtect après s'être bien connectée.

      - Si le processus HIP se bloque sur l'application GlobalProtect, cela peut finalement entraîner la déconnexion de l'application en raison de l'expiration du délai d'inactivité si la version de PAN-OS est 10.0 ou inférieure (qui devrait être actualisé à chaque message hipreportcheck.esp).
      - Parfois, un retard dans la finalisation du rapport HIP provient de l'évaluation des Patches manquants (PanGpHipMp) car ce processus prend du temps. Gardez à l'esprit qu'un rapport HIP partiel est envoyé après le « Temps d'attente max » configuré (par défaut 20 s), et le rapport complet est envoyé lorsqu'il est prêt.

 ©2026 Palo Alto Networks, Inc.

3. Assurez-vous que la passerelle ou le pare-feu a reçu le rapport HIP.
   1. Vérifiez si l'échange de rapports HIP s'est produit en vérifiant **Monitor (Surveiller)** > **Logs (Journaux)** > **GlobalProtect** sur la passerelle. Si oui, vous pouvez également vérifier les éléments suivants :
      - Recherchez les objets et profils HIP correspondants dans **Monitor (Surveiller)** > **Logs (Journaux)** > **HIP**.
      - Cliquez sur la loupe pour chaque objet ou profil pour voir le rapport complet.
   2. Si vous êtes un client Prisma Access, les journaux sont transmis par défaut à CDL. Affichez les journaux dans la **Log Viewer (Visionneuse de journaux)** intégrée dans la plateforme SASE ou dans l'option **Explore (Explorer)** intégrée dans CDL. Plus de détails sur Explorer.
   3. Si vous êtes un client NGFW, vérifiez si le pare-feu a reçu le rapport HIP de l'application GlobalProtect en exécutant les commandes suivantes à partir du pare-feu :

      L'exemple suivant fournit les détails sur le nom de l'ordinateur (PAN00965), le nom du profil HIP (Hip-Profile), la Condition de correspondance, utilisateur (admin), et IP allouée (172.24.10.1). Le format du nom d'utilisateur peut être différent (adresse e-mail, nom d'utilisateur, netbios\nom_d'utilisateur). Si vous ne tapez pas le bon format de nom d'utilisateur, la sortie sera vide. Dans le résultat, recherchez les profils HIP configurés pour le PC PAN00965.

      ```
      > show user hip-report computer PAN00965 user admin ip
      172.24.10.1
      ```

      ```
      <?xml version="1.0" encoding="UTF-8"?> <hip-report> <user-
      name>admin</user-name> <host-name>PAN00965</host-name> <ip-
      address>172.24.10.1</ip-address> <generate-time>10/29/2012
       16:51:17</generate-time> <categories> <entry name="host-
      info"> <client-version>1.1.7-11</client-version> <os>Microsoft
       Windows 7 Enterprise Edition Service Pack 1, 32-bit</os>
       <os-vendor>Microsoft</os-vendor> <host-name>PAN00965</host-
      name> <network-interface> <entry name="{7383A4FF-0140-4E4C-
      B70F-0D30438851C9}"> <description>PANGP Virtual Ethernet
       Adapter</description> <mac-address>02-50-41-00-00-01</
      mac-address> <ip-address> <entry name="172.24.10.1"/>
       </ip-address> </entry> <entry name="firewall"> <list>
       <entry> <ProductInfo> <Prod name="Microsoft Windows
       Firewall" version="7" vendor="Microsoft Corp."> </Prod> <is-
      enabled>yes</is-enabled> </ProductInfo> </entry> </list> </
      entry> <entry name="disk-backup"> <list> <entry> <ProductInfo>
      ```

   4. En cas de retard dans l'envoi du rapport HIP par l'application GlobalProtect, la passerelle utilisera le fichier cache (hip_report_base) jusqu'à ce que le nouveau rapport soit envoyé et que les politiques soient traitées en fonction du nouveau rapport.

   Si vous ne voyez pas le rapport sur le pare-feu après le temps d'attente maximal ou les informations de **Monitor (Surveiller)** > **Logs (Journaux)** > **GlobalProtect**, consultez les journaux de l'application Global Protect pour voir si l'application a essayé d'envoyer le rapport HIP. Le fait de sélectionner **Refresh Connection (Actualiser la connexion)** sur le client peut aider en cas de blocage, mais cela ne déterminera pas la raison de l'échec.

 ©2026 Palo Alto Networks, Inc.

4. Assurez-vous que l'utilisateur final de l'application GlobalProtect correspond au profil HIP correct, sur la base du rapport HIP envoyé.

 ©2026 Palo Alto Networks, Inc.

Service de conformité de l'hôte

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

Le service de conformité de l'hôte (HCS) pour GlobalProtect introduit un service hautement disponible et hébergé dans le cloud qui centralise l'évaluation de la posture des terminaux, la distribution et l'application des règles de politique de sécurité.

Le HCS centralise la sécurité des terminaux en traitant des rapports HIP complets dans le cloud et en distribuant uniquement les données de conformité finales ou les verdicts aux produits abonnés comme les déploiements NGFW pour l'application des règles de politique, ce qui élimine le traitement redondant sur chaque pare-feu.

L'application GlobalProtect continue d'envoyer des rapports de conformité des hôtes aux passerelles GlobalProtect, mais les passerelles envoient désormais ces rapports au HCS hébergé dans le cloud, si le HCS est activé. Le HCS traite les rapports HIP dans le cloud, effectue l'évaluation par rapport à vos politiques de sécurité définies, et les convertit en verdicts de conformité et envoie ces verdicts au pare-feu nouvelle génération.

La fonctionnalité HCS améliore considérablement la redistribution HIP pour les déploiements GlobalProtect à grande échelle. Elle répond aux défis des mises à jour d'informations sur les hôtes retardées et des problèmes d'évolutivité.

HCS pour GlobalProtect fournit :

- Configuration simplifiée des objets de conformité des hôtes et des profils de conformité des hôtes.
- Amélioration de l'évolutivité et de la rentabilité pour la redistribution HIP, éliminant le besoin d'une infrastructure supplémentaire sur site.

Utilisez la procédure suivante pour configurer le HCS pour GlobalProtect comme indiqué dans trois sections :

1. Activer le service de conformité de l'hôte
2. Configurer la redistribution du cloud
3. Configurer la politique de sécurité basée sur les services de conformité des hôtes

Avant de commencer :

- Assurez-vous que Portails GlobalProtect et Configurer une passerelle GlobalProtect sont configurés.

 ©2026 Palo Alto Networks, Inc.

Activer le service de conformité de l'hôte

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

1. Sur le ou les pare-feu hébergeant la ou les passerelles GlobalProtect, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **PAN-OS Edge Services Settings (Paramètres des services Edge PAN-OS)**.

2. Cochez la case **Enable Cloud Host Compliance Service (Activer le service de conformité de l'hôte cloud)** pour vous connecter aux services cloud. L'état de la **Connection (Connexion)** indique si le HCS est activé ou non. Vérifiez si l'indicateur d'état devient **Green (Vert)**, confirmant une connexion réussie au cloud.

   Par défaut, HCS est désactivé.

   Voici les différents états de connexion :

   - **Gray (Gris)** : Le service n'est pas activé.
   - **Green (Vert)** : Le service est activé et correctement connecté au cloud.
   - **Red (Rouge)** : Le service est activé et correctement connecté au cloud.
     1. Vérifiez la validité du certificat du périphérique pour le pare-feu sur lequel le HCS est activé.
     2. Vérifiez le cloud FQDN. Contactez l'équipe d'assistance pour résoudre ce problème.

     *Si votre périphérique est dans une configuration High Availability (haute disponibilité - HA), la connexion HCS pour le périphérique actif-secondaire/passif s'affichera en état **Not Connected (Non connecté)** (**Red [Rouge]**). Il s'agit d'un comportement attendu qui est accompagné du*

 ©2026 Palo Alto Networks, Inc.

message ***Device is not Active/Primary (Le périphérique n'est pas actif/principal)*** *sur la page* ***Monitor (Surveiller > Host Compliance (Conformité de l'hôte)***.

Notez le comportement suivant concernant HCS dans un environnement HA :

- **Active-Active Mode (Mode active/active)** : La synchronisation des verdicts se produit dans une seule direction, du périphérique principal au périphérique secondaire. Cela garantira que le périphérique secondaire, qui traite également le trafic, dispose de verdicts à jour.
- **Active-Passive Mode (Mode active-passive)** : La synchronisation continue avec le périphérique passif ne se produit pas. En cas de basculement, le périphérique nouvellement actif télécharge automatiquement l'ensemble complet des verdicts depuis le cloud.

La synchronisation **Active-Active** se fait dans la mesure du possible et nécessite que les configurations des périphériques soient maintenues synchronisées entre les homologues HA. Si les politiques ne sont pas cohérentes entre les périphériques, la synchronisation des verdicts peut échouer ou fonctionner de manière imprévisible. C'est une limitation connue de la fonctionnalité.

Configurer la redistribution du cloud

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

L'application GlobalProtect envoie un rapport HIP à la passerelle GlobalProtect. Pour que le HCS reçoive ce rapport HIP, vous devez configurer la passerelle GlobalProtect pour transférer le rapport HIP. Une fois configurée, la passerelle GlobalProtect partage automatiquement tous les HCP et HCO avec le HCS pour chaque système virtuel (vsys).

Vous devez activer **Contributing (Contribuant)** les rapports HIP sur le pare-feu de la passerelle pour envoyer des rapports HIP au service hébergé dans le cloud. En fonction des HCP et HCO configurés, une correspondance HIP sera évaluée sous la forme d'un verdict HIP.

Activer la contribution des rapports HIP à HCS pour les pare-feu passerelles

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures

 ©2026 Palo Alto Networks, Inc.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	Moteur d'identité sur le cloud Certificat du périphérique

1. Sur le ou les pare-feu hébergeant la ou les passerelles GlobalProtect, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Cloud Redistribution (Redistribution cloud)**.
2. Dans l'onglet **Contribution**, cliquez sur **Add (Ajouter)**.
3. Sélectionnez **HIP Report (Rapport HIP)** dans le menu déroulant et cochez la case **Enabled (Activé)**.

   - *La fonctionnalité de contribution est applicable uniquement aux pare-feu passerelles.*
   - *Dans l'onglet **Contribution**, **Enable Segment (Activer le segment)** n'est pas disponible pour la version PAN-OS 12.1. Ceci est réservé à un usage futur uniquement.*
4. Cliquez sur **OK**.

Activer la réception des verdicts HIP du HCS

Les verdicts HIP sont reçus à la fois pour les pare-feu passerelles et non passerelles.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

Vous devez activer la fonctionnalité **Receiving HIP verdicts (Réception de verdicts HIP)** pour permettre au pare-feu de recevoir des verdicts HIP évalués du HCS par vsys. En fonction des verdicts HIP, les règles de politique de sécurité configurées peuvent être appliquées avec des HCP qui contrôlent le trafic.

1. Sur le ou les pare-feu hébergeant la ou les passerelles GlobalProtect, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Cloud Redistribution (Redistribution cloud)**.
2. Dans l'onglet **Receiving (Réception)**, cliquez sur **Add (Ajouter)**.
3. Sélectionnez **HIP Verdict (Verdict HIP)** dans le menu déroulant et cochez la case **Enabled (Activé)**.

 ©2026 Palo Alto Networks, Inc.

4. Cliquez sur **OK**.

Configurer CIE pour HCS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

Vous devez affecter des pare-feu aux segments souscrits dans CIE et, lors de l'affectation des types de données, vous pouvez configurer les **HIP Reports (Rapports HIP)** au segment associé sous la section **Segment to Contribute Data (Segment auquel fournir des données)**.

Vous pouvez également activer les **HIP Verdicts (Verdicts HIP)** dans la section **Segment to Receive Data From (Segments à partir desquels recevoir des données)** des données.

Après avoir affecté le pare-feu, vous pouvez afficher les configurations HIP pour les segments associés tels que le nombre de rapports HIP.

Le **HIP Verdict (Verdict HIP)** et le **HIP Report (rapport HIP)** sont également affichés sur les informations de segment

Les informations de mappage sont affichées sur la page **Mappings & Tags (Mappages et étiquettes)** sur CIE. Pour afficher les informations relatives aux types de données, dans l'application CIE, sélectionnez **User Context (Contexte de l'utilisateur)** > **Mappings & Tags (Mappages de contexte utilisateur et étiquettes)**.

Configurer la politique de sécurité basée sur les services de conformité des hôtes

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud

 ©2026 Palo Alto Networks, Inc.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	Certificat du périphérique

Pour activer l'utilisation de HCP dans l'application des règles de politique de sécurité, vous devez exécuter les procédures suivantes :

- Objet de conformité de l'hôte : Vous commencez par créer des HCO individuels pour chaque vérification de sécurité spécifique que vous souhaitez effectuer. Par exemple, vous pouvez créer un objet pour vérifier Windows 10, un autre pour un antivirus à jour, et un troisième pour le chiffrement du disque.
- Créer un profil de conformité de l'hôte avec les objets de conformité de l'hôte : Vous créez ensuite un HCP en utilisant un ou plusieurs HCO. Par exemple, vous pouvez créer un profil « Périphériques Windows conformes » qui exige qu'un périphérique corresponde aux trois critères suivants : Windows 10 ET antivirus à jour ET chiffrement de disque.
- Activation de User-ID : Vous devez activer l'User-ID afin que le pare-feu génère des journaux de correspondance HIP.
- Appliquer le profil de conformité de l'hôte à une politique de sécurité : Vous devez ajouter le HCP comme critère de correspondance dans vos règles de politique de sécurité. Par exemple, vous pouvez créer une règle qui dit : « Si un appareil correspond au profil HIP « Périphériques Windows conformes », alors, autorisez-le à accéder à nos serveurs internes ».
- Définir les notifications de conformité d'hôte GlobalProtect : Vous pouvez définir les messages de notification à afficher aux utilisateurs finaux lors de l'application d'une règle de politique de sécurité avec un HCP.
- (Facultatif)Configurer l'itinéraire de service pour HCS : Vous pouvez configurer l'itinéraire de service uniquement dans les scénarios où le trafic HCS doit être acheminé séparément de l'interface de gestion, ou lorsque l'interface de gestion n'a pas de connexion à Internet.
- Vérifier que vos profils HIP fonctionnent comme prévu : Vous pouvez surveiller le trafic qui touche vos règles de politique de sécurité activées par le profil de conformité des hôtes en utilisant le journal du trafic.
- Vérification des détails des services de conformité de l'hôte : Vous pouvez voir l'état de connexion HCS, les détails du verdict, les détails HCP ajoutés aux règles de politique de sécurité.

Objet de conformité de l'hôte

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

 ©2026 Palo Alto Networks, Inc.

HCO (Host Compliance Object pour Objet de conformité de l'hôte) est un contrôle de sécurité spécifique et granulaire que le pare-feu effectue sur un périphérique essayant de se connecter à votre réseau. L'application GlobalProtect installée sur les terminaux collecte ces informations et les signale au pare-feu. Les HCO ne sont pas utilisés directement dans les règles de politique de sécurité. Au lieu de cela, ils sont ajoutés pour créer des HCP, qui sont ensuite appliqués aux règles de politique de sécurité.

Vous pouvez créer un ou plusieurs HCO qui définissent les critères spécifiques d'un périphérique conforme (par exemple, la vérification de logiciels spécifiques, de niveaux de correctifs, etc.).

1. Sur le ou les pare-feu hébergeant la ou les passerelles GlobalProtect, sélectionnez **Objects (Objets)** > > **Host Compliance Objects (Objets de conformité de l'hôte)**, puis **Add (Ajouter)** un nouveau HCO.
2. Saisissez un **Name (Nom)** et une **Description** pour l'objet.
3. Définissez les critères d'hôte spécifiques que vous souhaitez vérifier en sélectionnant :
   - **Catégorie** : Sélectionnez le type de vérification (par exemple, antivirus, pare-feu, gestion des correctifs).
   - **Attribute (Attribut)** : Définissez les détails spécifiques à évaluer (par exemple, la version du produit, le dernier temps d'analyse).
   - **Operator (Opérateur)** : Définissez la logique de comparaison (par exemple, est, n'est pas, contient, est supérieur, inférieur, supérieur égal et inférieur).
   - **Operating System (Système d'exploitation)** : Choisissez le système d'exploitation (par exemple, Windows, macOS) et la version à vérifier.

     *L'opérateur des versions « Within »/« Not Within » N n'est pas pris en charge pour l'attribut « Product Version » ou « Virus Definition Version » pour la catégorie **Anti-Malware**.*
4. Cliquez sur **OK** pour créer le HCO.
5. Répétez ces étapes pour créer chaque HCO supplémentaire dont vous avez besoin.
6. **Commit (Validez)** les modifications.

Comparaison des objets HIP et des configurations HCO

La section suivante compare les configurations des objets HIP et des HCO par catégorie.

Informations sur l'hôte

Objet HIP (informations sur l'hôte)

HCO (informations sur l'hôte)

Informations réseau

Objet HIP (informations réseau)

HCO (informations réseau)

 ©2026 Palo Alto Networks, Inc.

Périphérique mobile
Objet HIP (périphérique mobile)

Périphérique mobile

Gestion des correctifs
Objet HIP (gestion des correctifs)

HCO (gestion des correctifs)

Pare-feu
Objet HIP (pare-feu)

HCO (pare-feu)

Anti-logiciels malveillants
Objet HIP (anti-malware)

HCO (anti-malware)

Sauvegarde du disque
Objet HIP (sauvegarde du disque)

HCO (sauvegarde du disque)

Cryptage du disque
Objet HIP (chiffrement du disque)

HCO (chiffrement du disque)

Prévention des pertes de données
Objet HIP (prévention des pertes de données)

HCP (prévention des pertes de données)

certificate
Objet HIP (certificat)

 ©2026 Palo Alto Networks, Inc.

HCO (mauvais certificat)

Vérifications personnalisées (registre de clés)

Objet HIP (vérifications personnalisées [registre de clés])

HCO (vérifications personnalisées [registre de clés])

Vérifications personnalisées (Plist)

Objet HIP (vérifications personnalisées [Plist])

HCO (vérifications personnalisées [Plist])

Vérifications personnalisées (liste de processus)

Objet HIP (vérifications personnalisées [liste de processus])

HCO (vérifications personnalisées [liste de processus])

Créer un profil de conformité de l'hôte avec les objets de conformité de l'hôte

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

Vous pouvez créer un HCP que vous prévoyez d'utiliser dans vos règles de politique de sécurité en ajoutant des HCO existants que vous avez créés pour vos terminaux. Le HCP agit alors comme une condition de correspondance dans les règles de votre politique de sécurité.

HCP utilise un ou plusieurs HCO pour définir une liste de contrôle de sécurité pour votre pare-feu. Lorsqu'un périphérique se connecte, le pare-feu effectue une correspondance HIP pour vérifier que le périphérique répond à tous les critères définis dans le HCP.

Sur la base de ces informations, le pare-feu applique automatiquement des règles de sécurité pour autoriser ou interdire l'accès à l'utilisateur GlobalProtect, garantissant que seuls les terminaux conformes peuvent se connecter.

Lorsqu'un flux de trafic est évalué par rapport à une politique de sécurité, il est comparé au profil de conformité de l'hôte :

 ©2026 Palo Alto Networks, Inc.

- **S'il y a une correspondance** : La règle de politique de sécurité correspondante est appliquée.
- **S'il n'y a pas de correspondance** : Le flux est évalué par rapport à la règle suivante dans la séquence, comme pour tout autre critère de correspondance de politique de sécurité.

Pour configurer un HCP :

1. Sur le ou les pare-feu hébergeant la ou les passerelles GlobalProtect, sélectionnez **Objects (Objets)** > **Host Compliance Profile (Profil de conformité de l'hôte)**, puis **Add (Ajouter)** le HCO que vous avez créé.
2. Saisissez un **Name (Nom)** et une **Description** pour identifier le HCP.
3. Cliquez sur **Add Match Criteria (Ajouter des critères de correspondance)** pour ouvrir le **Host Compliance Object/Profiles Builder (Objets de conformité de l'hôte/Créateur de profil)** et ajouter les critères de correspondance requis pour le profil. Si vous souhaitez que le HCP évalue l'objet comme correspondance uniquement lorsque le critère de l'objet n'est pas vrai pour un flux, vous devez cocher la case **NOT (NE PAS)** avant d'ajouter l'objet.
4. Continuez à ajouter des critères de correspondance pour le profil que vous créez. Assurez-vous de sélectionner le bouton radio approprié (**AND or OR [ET ou OU]**) entre chaque ajout (et, encore une fois, en utilisant la case à cocher **NO (NON)** le cas échéant.
5. Lorsque vous avez ajouté tous vos critères de correspondance, cliquez sur **OK** pour enregistrer le profil.
6. Répétez ces étapes pour créer chaque HCP supplémentaire dont vous avez besoin. Le nombre maximum de HCP supportés est de 127. Il s'agit du nombre maximal de HCP que vous pouvez ajouter à une politique de sécurité.
7. **Commit (Validez)** les modifications.

Activation de User-ID

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

Activez User-ID sur les zones source sur lesquelles se trouvent les utilisateurs GlobalProtect qui envoient des requêtes demandant des contrôles d'accès basés sur HIP. Vous devez activer User-ID, sinon le pare-feu ne peut pas générer d'entrées de journal de correspondance HIP.

1. Sélectionnez **Network (Réseau)** > **Zones**

 ©2026 Palo Alto Networks, Inc.

2. Cliquez sur le Nom de la zone dans laquelle vous souhaitez autoriser l'agent User-ID.

3. **Enable User Identification (Activez l'identification de l'utilisateur)**, puis cliquez sur **OK (OK)**.

Appliquer le profil de conformité de l'hôte à une politique de sécurité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

Vous pouvez ajouter le HCP à une politique de sécurité et créer les règles de sécurité activées par le HCP sur votre ou vos passerelles.

Il est recommandé de créer vos règles de politique de sécurité et de vérifier qu'elles correspondent aux flux attendus (en fonction des critères de source et de destination) avant d'ajouter vos HCP. Ainsi, vous êtes plus à même de déterminer l'inclusion appropriée des règles activées par HCP au sein de la politique de sécurité.

1. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et sélectionnez la règle à laquelle vous souhaitez ajouter un profil HCP.

2. Dans l'onglet **Source**, vérifiez que la zone source est une zone pour laquelle vous avez activé User-ID.

3. Dans l'onglet **Source** sous **Source Device (Périphérique source)**, **Add (Ajouter)** le HCP utilisé pour identifier les périphériques (vous pouvez ajouter un maximum de 127 HCP à une règle).

4. Cliquez sur **OK** pour enregistrer la règle.

Définir les notifications de conformité d'hôte GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

 ©2026 Palo Alto Networks, Inc.

Les notifications de conformité d'hôte aident à guider vos utilisateurs vers la conformité de sécurité en fournissant des alertes utiles et exploitables. La décision d'afficher une notification lorsque le périphérique d'un utilisateur correspond à un profil HIP, ou lorsqu'il ne correspond pas, doit être basée sur ce que vous voulez que l'utilisateur effectue.

Si votre profil HIP est configuré pour trouver des périphériques non conformes (par exemple, il correspond lorsque le logiciel antivirus est manquant), alors vous devez afficher la notification sur une correspondance pour indiquer à l'utilisateur comment résoudre le problème. Toutefois, si votre profil identifie des périphériques entièrement conformes, vous devez afficher la notification pour les utilisateurs qui ne correspondent pas, car ce sont eux qui doivent prendre des mesures correctives.

1. Sur le pare-feu qui héberge votre passerelle GlobalProtect, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**.
2. Sélectionnez la configuration de passerelle à laquelle vous souhaitez ajouter des messages de notification HIP.
3. Sélectionnez **Agent** > **HIP Notification (Notification HIP)**, puis cliquez sur **Add (Ajouter)**.
4. Sélectionnez le HCOP auquel ce message s'applique dans la liste déroulante **Host Information (Informations sur l'hôte)**.
5. Selon que vous souhaitiez afficher le message lorsque le profil HIP correspondant est mis ou non en correspondance, sélectionnez **Match Message (Message de correspondance)** ou **Not Match Message (Message de non-correspondance)**. Dans certains cas, vous pourriez créer des messages à la fois pour une correspondance et pour une non-correspondance, en fonction des objets que vous souhaitez faire correspondre et des objectifs que vous avez définis pour la politique de sécurité.
6. **Enable (Activez)** l'option **Match Message (Faire correspondre le message)** ou **Not Match Message (Ne pas faire correspondre le message)**, puis choisissez si vous souhaitez afficher le message comme un **Pop Up Message (Message en incrustation)** ou comme une **System Tray Balloon (Bulle de la zone de notification)**.
7. Entrez le texte de votre message dans la zone **Template (Modèle)**, puis cliquez sur **OK**.
8. Répétez cette procédure pour chaque message que vous souhaitez définir.
9. **Commit (Validez)** les modifications.

Configurer l'itinéraire de service pour HCS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures

 ©2026 Palo Alto Networks, Inc.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	Moteur d'identité sur le cloud Certificat du périphérique

Cette procédure n'est requise que dans les scénarios où le trafic HCS doit être acheminé séparément de l'interface de gestion, ou lorsque l'interface de gestion ne dispose pas de connexion Internet.

La configuration de l'itinéraire de service est une étape facultative pour HCS.

Vous devez configurer les itinéraires de service pour modifier l'interface que le pare-feu utilise pour envoyer des requêtes à HCS.

1. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Services** et dans la section Fonctionnalités des services, cliquez sur **Service Route Configuration (Configuration de l'itinéraire de service)**.
2. Sélectionnez **Host Compliance Cloud Service (Service cloud de conformité de l'hôte)** et cliquez sur **OK**.
3. **Commit (Validez)** les modifications.

Vérifier que vos profils HIP fonctionnent comme prévu

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

Vous pouvez surveiller le trafic qui touche vos politiques de sécurité activées par HCP à l'aide du journal **Traffic (Trafic)** :

1. Sur le pare-feu qui héberge votre passerelle, sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)** > **Traffic (Trafic)**.
2. Filtrez le journal pour afficher uniquement le trafic correspondant à la règle avec le HCP que vous souhaitez afficher et surveiller.

 ©2026 Palo Alto Networks, Inc.

Vérification des détails des services de conformité de l'hôte

Pour afficher les détails, sur le pare-feu qui héberge votre passerelle, sélectionnez **Monitor (Surveiller)** > **Host Compliance (Conformité de l'hôte)**.

Un HCP doit être joint à une politique de sécurité pour que les verdicts HIP soient visibles sur la page ***Monitor (Surveiller)*** > ***Host Compliance ()Conformité de l'hôte***

- La section **Host Compliance Cloud Service (Service cloud de conformité de l'hôte)** indique si le HCS est activé ou non et l'état de la connexion (en gris, vert ou rouge).
- La section **Hosts per Host Compliance Profile in Security Policy (Hôtes par profil de conformité d'hôte dans la politique de sécurité)** affiche la correspondance HCP par ID d'hôte.
- La section **Inventoruy (Inventaire)** affiche tous les HCP utilisés dans les politiques de sécurité indépendamment de la correspondance HCP.

Mise à niveau et migration

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

Pour des mises à niveau réussies de redistribution HIP, l'ordre standard est de mettre à niveau Panorama en premier, suivi des pare-feu de passerelle et enfin des pare-feu non-passerelle. Ce principe s'applique à diverses topologies, tant au sein des déploiements simples que multi-niveaux (*GW→collecteurs FW→ pare-feux de bord*). La séquence reste la même : les passerelles avant les pare-feu périphériques, les mises à niveau des pare-feu collecteurs étant facultatives.

Vous devez suivre la mise à niveau des composants de manière séquentielle comme indiqué dans le tableau :

Catégorie	Séquence de mise à niveau
Grande entreprise avec NGFW	**1.** Panorama **2.** Pare-feu de passerelle **3.** Pare-feu non-passerelle
Petites entreprises	**1.** Pare-feu de passerelle **2.** Pare-feu non-passerelle

 ©2026 Palo Alto Networks, Inc.

Étapes post-mise à niveau pour la configuration de redistribution :

Quel que soit le modèle de déploiement, il est recommandé de conserver toutes les configurations d'agent de redistribution existantes après une mise à niveau. Cela est nécessaire pour prendre en charge un éventuel retour à une version qui repose sur la logique de redistribution HIP. Conserver la configuration simplifie le processus de retour en arrière, élimine le besoin de reconfiguration manuelle et prévient les interruptions de service liées au rapport HIP.

Après la mise à niveau, le système met automatiquement à jour les objets HIP existants en nouveaux HCO et HCP. Ces nouveaux objets sont uniquement à titre de référence et peuvent être identifiés par le nom d'objet HIP d'origine dans leur champ de description. Votre configuration HIP d'origine n'est pas impactée. Vous devez examiner ces exemples pour apprendre le nouveau cadre, puis créer manuellement vos propres HCO et HCP. Une fois votre nouvelle configuration en place, vous devez supprimer les objets de référence générés automatiquement.

Lors d'une mise à niveau, le système effectue automatiquement :

- **Crée de nouveaux objets :** Chacun de vos objets HIP existants est automatiquement converti en un ou plusieurs nouveaux HCO.
- **Ajoute une référence :** Pour une traçabilité facile, le nom de l'objet HIP d'origine est ajouté au **champ de description** de chaque nouveau HCO créé à partir de celui-ci.
- **Regroupe les objets :** Tous les HCO générés à partir d'un seul objet HIP sont ensuite regroupés avec une condition **ET** à l'intérieur d'un nouveau HCP correspondant.
- **Préserve la configuration d'origine :** Ce processus de conversion n'a aucun impact sur vos objets HIP d'origine et vos profils HIP. Ils restent intacts et continuent de fonctionner jusqu'à ce que vous décidiez de les modifier.

Vous devez créer manuellement une nouvelle configuration, puis supprimer les objets de référence générés automatiquement. Suivez ces étapes

1. Examinez les HCO et HCP générés automatiquement. Analysez comment le nouveau cadre HCS représente la logique de vos anciens objets HIP.
2. Créez manuellement vos propres HCO et HCP en fonction des exigences de sécurité de votre organisation.
3. Une fois que vous avez mis en œuvre la nouvelle configuration HCS, vous devez supprimer les HCO et HCP générés automatiquement par le système pour éviter toute confusion.

Comportement de migration des objets HIP par emplacement

Lors de la migration, les objets HIP existants sont convertis en nouveaux HCO et HCP. Leur emplacement et la convention de nommage des nouveaux objets dépendent de leur portée d'origine :

- **Groupes de périphériques :** Les objets HIP configurés au sein d'un groupe d'appareils spécifique seront migrés en tant que nouveaux objets au sein de ce même groupe d'appareils. Les noms de ces nouveaux objets auront comme préfixe *DG-*.

- **Portée partagée :** Les objets HIP de la portée « Partagée » seront migrés dans la portée « Partagée ». Les noms de ces nouveaux objets auront comme préfixe *CMS-*.

 ©2026 Palo Alto Networks, Inc.

- **Specific Vsys: (Vsys spécifique :)** Les objets HIP configurés pour un système virtuel spécifique (vsys) seront migrés au sein de ce même vsys. Les noms auront comme préfixe par *vsysX-*, où *X* est l'ID du vsys (par exemple, *vsys1-*).

- **Local Firewall/Vsys: (Pare-feu local/Vsys :)** Les objets HIP configurés directement sur un pare-feu local (non hérités de Panorama) seront migrés au sein de leurs vsys respectifs. Les noms de ces nouveaux objets auront comme préfixe *Local-*

.

Les HCP nouvellement créés seront placés au même endroit (par exemple, Groupe d'appareils, Partagé ou vsys) que les HCO qu'ils contiennent.

Scénario de rétrogradation

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

La rétrogradation serait restreinte si HCP est utilisé dans la politique de sécurité ou la notification HIP dans la passerelle.

Après avoir désactivé le HCS, vous pouvez suivre la procédure standard pour rétrograder le PAN-OS à la version souhaitée. Notez les éléments suivants avant de rétrograder la version du PAN-OS avec HCS à une version inférieure :

- Vous ne pouvez pas désactiver le HCS si un HCP est activement utilisé dans une politique de sécurité. Vous devez d'abord retirer le HCP de toutes les règles de sécurité associées avant de pouvoir désactiver le service.
- Vous ne pouvez pas créer un HCP ou un HCO si un autre objet dans le groupe existe déjà avec le même nom exact.
- Un HCP ne peut pas être supprimé s'il est activement affecté à une notification HIP. Vous devez d'abord retirer le HCP de la notification HIP avant de pouvoir le supprimer.
- Un HCP ne peut pas être supprimé tant qu'il est référencé dans une politique de sécurité. Vous devez d'abord retirer le HCP de chaque règle de sécurité qui l'utilise.

Restriction de rétrogradation en raison de l'utilisation de HCP dans la notification HIP

Restriction de rétrogradation en raison de l'utilisation de HCO dans la notification HIP

Restriction de rétrogradation en raison de HCP dans la politique de sécurité

 ©2026 Palo Alto Networks, Inc.

Lorsque vous poussez une configuration depuis Panorama vers un pare-feu exécutant une version de PAN-OS qui ne prend pas en charge le HCS, vous pouvez vous attendre au comportement suivant :

- Tous les HCP et HCO existants seront supprimés de la configuration du pare-feu lors de l'opération de transmission. Il en va de même pour la configuration de l'agent de redistribution du cloud.
- La validation et la transmission échouent si un HCP est encore activement utilisé dans une politique de sécurité ou une notification HIP.

Pour garantir une rétrogradation réussie et éviter les échecs de configuration, il est recommandé qu'avant de procéder à la rétrogradation, vous effectuiez les actions suivantes :

- Dans votre politique de sécurité, supprimez toutes les règles qui utilisent un HCP pour l'application.
- Dans vos notifications HIP GlobalProtect, supprimez toutes les références aux HCP.

Limitations

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence d'abonnement GlobalProtect Application GlobalProtect 6.0 ou versions ultérieures PAN-OS 12.1.2 ou versions ultérieures Moteur d'identité sur le cloud Certificat du périphérique

- L'HCO actuel a une limitation lors de la vérification des rapports HIP contenant une liste d'éléments, où chaque élément a plusieurs attributs. Il n'est pas possible de créer une seule règle qui vérifie une combinaison spécifique d'attributs pour un seul élément dans cette liste.

Par exemple, dans la catégorie Anti-Malware, vous ne pouvez pas créer un seul HCO pour vérifier si le fournisseur Microsoft Defender a spécifiquement défini la protection en temps réel sur « Oui ». Vous ne pouvez créer que des objets séparés : un pour vérifier si un produit installé provient de Microsoft et un autre pour vérifier si un produit a la protection en temps réel activée. Le système ne peut pas établir de corrélation entre ces deux conditions pour la même instance de produit.

- Cette limitation sur la corrélation d'attributs spécifiques s'applique aux catégories HIP suivantes :
  - Anti-Malware (par exemple, corréler un fournisseur spécifique avec son dernier temps d'analyse ou l'état de protection en temps réel)
  - Gestion des correctifs (par exemple, corréler un correctif spécifique avec sa gravité)
  - Sauvegarde de disque (par exemple, corréler un fournisseur spécifique avec son dernier temps de sauvegarde)

 ©2026 Palo Alto Networks, Inc.

- Pour une connectivité HCS fiable, l’interface de gestion et l’interface de données (utilisée pour les routes de service) doivent être configurées avec des adresses IP statiques. L’utilisation d’IP dynamiques attribuées par DHCP entraînera des échecs de connexion.
- La connectivité HCS n’est pas prise en charge avec IPv6.

 ©2026 Palo Alto Networks, Inc.

Surveillance et dépannage de GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

La surveillance centralisée d'un déploiement GlobalProtect est une fonction administrative critique requise pour faire respecter la politique de sécurité, garantir la fiabilité de la connexion pour les utilisateurs distants et effectuer un dépannage opérationnel. Ce chapitre détaille les procédures pour utiliser les plateformes de Palo Alto Networks pour une surveillance efficace de GlobalProtect et fournit des conseils pour résoudre les problèmes courants.

En exploitant les journaux de GlobalProtect, vous pouvez obtenir la visibilité nécessaire pour surveiller l'activité des utilisateurs, diagnostiquer les échecs de connexion, auditer la conformité des terminaux à l'aide des données du Host Information Profile (profil d'informations sur l'hôte - HIP) et enquêter sur les événements de sécurité.

Vous pouvez surveiller GlobalProtect en utilisant :

- **Service de journalisation Strata** : Fournit une solution de journalisation centralisée basée sur le cloud pour une visibilité complète sur l'ensemble de votre déploiement GlobalProtect.
- **Journaux PAN-OS GlobalProtect** : Permet la surveillance et l'analyse directes des événements GlobalProtect depuis le pare-feu local ou l'interface de gestion Panorama.

Ce chapitre fournit également des informations sur la collecte de journaux, des conseils de diagnostic et de dépannage pour résoudre les problèmes courants rencontrés avec l'application GlobalProtect, les portails et les passerelles. Vous pouvez apprendre à interpréter les fichiers journaux, à diagnostiquer les problèmes d'authentification, à résoudre les erreurs courantes côté application telles que les échecs de connexion ainsi que les problèmes liés au portail et à la passerelle GlobalProtect.

Surveillance de GlobalProtect à l'aide du service de journalisation Strata

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

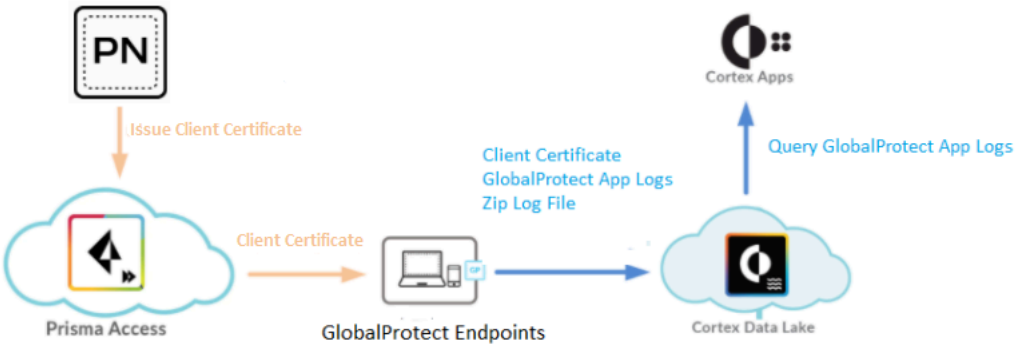
Avec Prisma Access et les déploiements de pare-feu de nouvelle génération, vous pouvez désormais résoudre rapidement les problèmes de connexion, de performances et d'accès des utilisateurs mobiles. L'application GlobalProtect peut désormais être configurée pour envoyer des journaux de dépannage et de diagnostic du terminal de l'utilisateur final au Service de journalisation Strata pour une analyse plus approfondie. En utilisant cette fonctionnalité, lorsque l'utilisateur final signale un problème à partir de l'application GlobalProtect (à la demande de l'utilisateur), l'application peut générer et envoyer un rapport complet et facile à lire pour vous aider à identifier rapidement la cause première du problème de l'utilisateur final distant. En outre, l'application GlobalProtect peut exécuter des tests de diagnostic de bout en bout pour sonder l'état et les performances de la connexion réseau et les performances d'applications Web spécifiques à partir du point de terminaison de l'utilisateur final distant. Il en résulte une résolution plus rapide des problèmes de l'utilisateur final distant, permet une productivité accrue et optimise l'expérience utilisateur pour l'utilisateur final distant.

Les utilisateurs finaux peuvent désormais signaler un problème depuis leur terminal directement au Service de journalisation Strata auquel l'administrateur peut accéder sans collecter et envoyer manuellement les journaux de l'application GlobalProtect, par exemple par e-mail ou en les stockant sur un lecteur cloud. Si les utilisateurs finaux consentent à exécuter des tests de diagnostic et à inclure des journaux de diagnostic sur l'application GlobalProtect, l'ensemble de journaux de dépannage et les journaux de diagnostic sont envoyés au Service de journalisation Strata à partir de leur terminal afin que vous puissiez les consulter facilement à l'aide de l'application Explore sur le hub. Si les utilisateurs finaux ne consentent pas à exécuter des tests de diagnostic et à inclure des journaux de diagnostic et des journaux de dépannage dans l'application GlobalProtect, seuls les rapports de dépannage sans l'ensemble de journaux de dépannage sont envoyés au Service de journalisation Strata à partir de leur terminal pour une analyse plus approfondie.

Par exemple, si vous souhaitez exécuter des tests de diagnostic pour les URL de destination HTTPS qui peuvent contenir des adresses IP ou des noms de domaine complets (par exemple, https://10.10.10.10/resource.html, https://webserver/file.pdf ou https://google.com) afin de déterminer s'il existe un problème de latence ou de performances réseau, vous pouvez configurer ces URL de destination HTTPS qui sont essentielles à la productivité de votre utilisateur final en activant la collecte du journal des applications GlobalProtect pour le dépannage sur le portail. Par défaut, la collecte des journaux d'application GlobalProtect pour le dépannage est désactivée et, par conséquent, les utilisateurs finaux ne peuvent pas envoyer les journaux de dépannage et de diagnostic au Service de journalisation Strata à partir de leur terminal. Ils devraient collecter et envoyer manuellement les journaux de l'application GlobalProtect à l'administrateur à des fins de dépannage et de débogage.

 ©2026 Palo Alto Networks, Inc.

Le diagramme suivant illustre le workflow (flux de travail) pour l'envoi des rapports de dépannage et des journaux de diagnostic de l'application GlobalProtect du terminal de l'utilisateur final au Service de journalisation Strata :



Avant de commencer à activer la collecte de journaux d'application GlobalProtect pour le dépannage et d'afficher les enregistrements de journal de dépannage et de diagnostic de l'application GlobalProtect sur l'application Explorer, suivez ces recommandations pour communiquer :

- Achetez une licence de service de journalisation Strata pour le volume de journaux dans votre déploiement GlobalProtect et connectez-vous à l'application Explore sur le hub.
- Utilisez l'infrastructure de journalisation du Service de journalisation Strata pour gérer le mécanisme de livraison des journaux de dépannage et de diagnostic de l'application GlobalProtect.
- Utilisez le Cortex Sizing Calculator (calculateur de dimensionnement Cortex) pour calculer la quantité de stockage dont vous avez besoin dans le Service de journalisation Strata.
- Procurez-vous le plug-in Panorama et Cloud Services et upgrade (effectuez une mise à niveau) vers le plug-in cloud services version 1.8, le plug-in cloud services 2.0 Preferred ou le plug-in cloud services 2.0 Innovation.
- Récupérez le certificat du service de journalisation Strata.
- Achetez et installez une licence d'abonnement GlobalProtect sur chaque passerelle.
- Enable the GlobalProtect app log collection for troubleshooting (Activez la collection de journaux d'application GlobalProtect pour le dépannage) sur le portail GlobalProtect.

Liste de vérification Collecte de journaux de l'application GlobalProtect pour le dépannage

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Utilisez le flux de travail suivant pour activer la collecte de journaux d'applications GlobalProtect pour le dépannage :

©2026 Palo Alto Networks, Inc.

Avec Cloud Managed Prisma Access, vous pouvez activer la collecte de journaux pour le dépannage *de l'application GlobalProtect en utilisant l'application Prisma Access sur le hub pour générer le certificat et l'importer automatiquement afin que l'application puisse s'authentifier avec Strata Logging Service pour la collecte de journaux.*

Étape 1 : Dans Panorama, autorisez GlobalProtect à communiquer avec Cortex Data Lake Strata Logging Service

Avec le plug-in Cloud Services 2.0 Innovation, si vous avez un déploiement qui utilise Prisma Access ou le pare-feu de nouvelle génération, vous devez utiliser l'interface Web Panorama pour configurer la connectivité GlobalProtect.

Générez un certificat client utilisé pour établir une connexion entre l'application GlobalProtect et Strata Logging Service.

Lecertificat **globalprotect_app_log_cert** est automatiquement exporté à partir du magasin de certificats Panorama, puis automatiquement importé dans le modèle Panorama où réside la configuration du portail GlobalProtect.

Créez ou modifiez la configuration existante de GlobalProtect agent configuration (agent GlobalProtect) pour un groupe spécifique d'utilisateurs.

Sélectionnez le certificat **globalprotect_app_log_cert** comme certificat client dans la configuration du portail GlobalProtect.

Avec le plug-in Cloud Services 1.8 et le plug-in Cloud Services 2.0 Preferred, vous devez utiliser les commandes pour configurer la connectivité GlobalProtect.

Générez un certificat client utilisé pour établir une connexion entre l'application GlobalProtect et Strata Logging Service.

Exportez le certificat **`gp_app_log_cert`** depuis le magasin de certificats Panorama.

Importez le certificat **`gp_app_log_cert`** dans le modèle Panorama où réside la configuration du portail GlobalProtect.

Créez ou modifiez la configuration existante de GlobalProtect agent configuration (agent GlobalProtect) pour un groupe spécifique d'utilisateurs.

Sélectionnez le certificat **gp_app_log_cert** comme certificat client dans la configuration du portail GlobalProtect.

Étape 2 : Configurez les paramètres de collecte de journaux d'applications GlobalProtect

Activez la collecte de journaux d'applications GlobalProtect pour le dépannage sur le portail GlobalProtect.

Configurez les URL de destination basées sur HTTPS qui peuvent contenir des adresses IP ou des noms de domaine complets sur le portail GlobalProtect. Plus tard, ces URL de destination basées sur HTTPS sont utilisées pour lancer des tests de performances pour la vérification.

 ©2026 Palo Alto Networks, Inc.

Étape 3 : Signalez un problème depuis l'application GlobalProtect pour Windows, macOS, iOS, Android et Linux

Ouvrez l'application GlobalProtect.

Signalez un problème à partir de GlobalProtect à partir du point de terminaison de l'utilisateur final.

(Optional (Facultatif)) Autorisez l'application GlobalProtect à exécuter des tests de diagnostic et de performances supplémentaires à la fois à l'intérieur et à l'extérieur du tunnel, et envoyez également l'ensemble de journaux de dépannage avec les rapports de problème à la demande de l'utilisateur.

Étape 4 : Affichez les journaux de dépannage et de diagnostic de l'application GlobalProtect sur l'application Explore

Affichez l'enregistrement du journal de dépannage ou de diagnostic téléchargé sur Strata Logging Service.

Consultez les détails dans les journaux pour vous aider à identifier la cause racine et à résoudre les problèmes de connectivité, d'accès au réseau ou de performances.

Configurer la connectivité GlobalProtect vers Strata Logging Service

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Vous devez configurer la connectivité GlobalProtect afin que l'application GlobalProtect puisse s'authentifier auprès de Strata Logging Service pour la collecte des journaux. Un seul certificat client est utilisé par client. Par exemple, tous les points de terminaison des utilisateurs finaux hébergés par un client Prisma Access obtiendront le même certificat poussé à partir de la configuration du portail. Le certificat client est valable 1 an. L'application GlobalProtect utilise le certificat client et l'instance Strata Logging Service pour envoyer les journaux de dépannage de l'application GlobalProtect à Strata Logging Service.

Sur la base de la version du plug-in Cloud Services, vous devez configurer la connectivité GlobalProtect à Strata Logging Service à l'aide de l'interface de ligne de commande (CLI) ou de l'interface Web Panorama qui gère Prisma Access :

- Configurer la connectivité GlobalProtect à Strata Logging Service (Plug-in Cloud Services 2.0 Innovation)
- Configurer la connectivité GlobalProtect à Strata Logging Service (Plug-in Cloud Services 1.8 et 2.0 préféré)

  *Avec Cloud Managed Prisma Access, vous pouvez activer la collecte de journaux pour le dépannage de l'application GlobalProtect en utilisant l'application Prisma Access sur le hub pour générer le certificat et l'importer automatiquement afin que l'application puisse s'authentifier avec Strata Logging Service pour la collecte de journaux. Le certificat s'affiche automatiquement dans la page **Certificate Management (Gestion des certificats)** et est poussé en tant que certificat client vers le portail Prisma Access.*

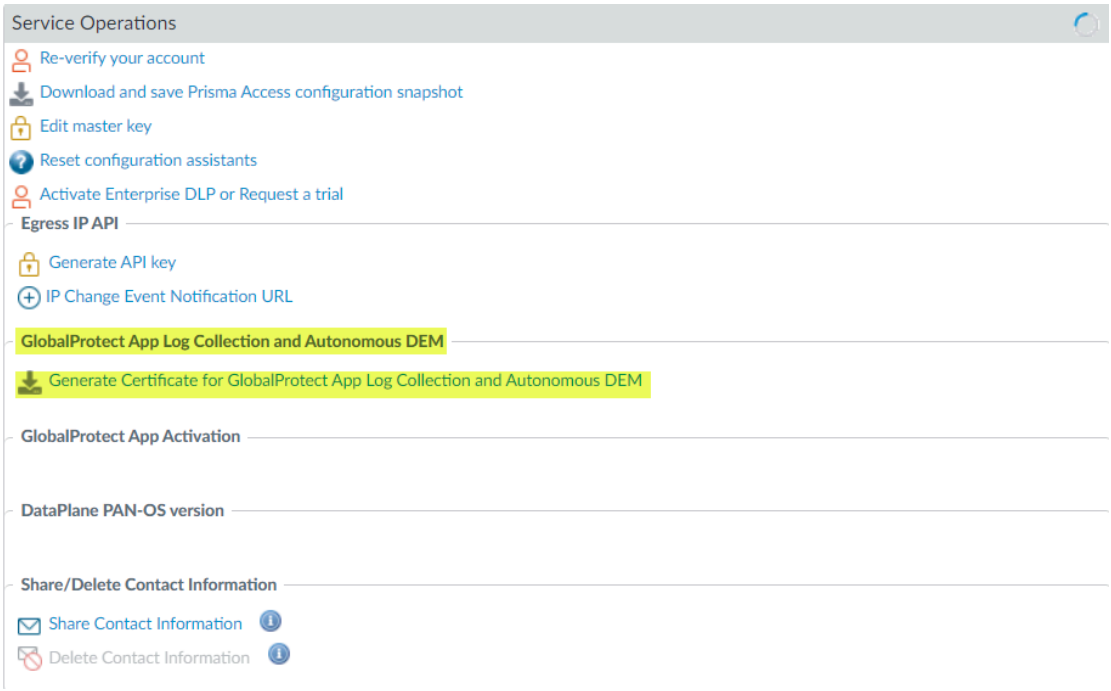
 ©2026 Palo Alto Networks, Inc.

Configurer la connectivité GlobalProtect à Strata Logging Service (Plug-in Cloud Services 2.0 Innovation)

Avec le plug-in Cloud Services 2.0 Innovation, si vous disposez d'un déploiement qui utilise Prisma Access ou le pare-feu de nouvelle génération, vous devez utiliser l'interface Web Panorama pour configurer la connectivité GlobalProtect afin que l'application GlobalProtect puisse s'authentifier auprès de Strata Logging Service pour la collecte de journaux.

1. Utilisez l'Estimateur de service de journalisation Strata pour calculer la quantité de stockage dont vous avez besoin dans Strata Logging Service.

2. Générez un certificat client utilisé pour établir une connexion entre l'application GlobalProtect et Strata Logging Service.
   1. Utilisez l'interface Web Panorama qui gère Prisma Access pour générer un certificat client.
      1. Connectez-vous au Panorama qui gère Prisma Access.
      2. Sélectionnez **Panorama** > **Cloud Services (Services Cloud)** > **Configuration** > **Service Setup (Configuration du service)**.
      3. Sélectionnez **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM (Générer un certificat pour Collecte de journaux de l'application GlobalProtect et DEM autonome)**.



      4. Pour les déploiements Prisma Access, cliquez sur **Oui** pour générer un certificat client.

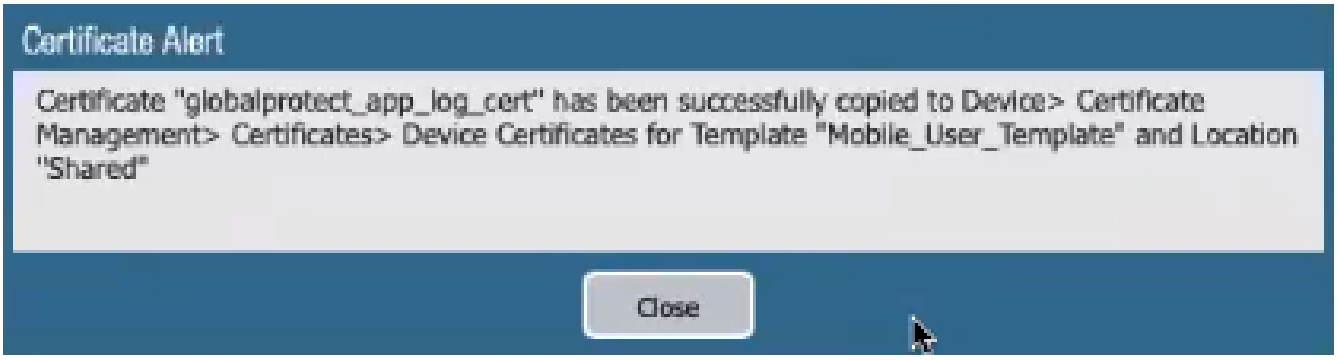
         Si vous configurez Prisma Access pour gérer un seul client, le certificat **`globalprotect_app_log_cert`** est automatiquement importé dans le **Mobile_User_Template** et l'emplacement **Shared (partagé)**.

         Si vous configurez Prisma Access pour manage multiple tenants (gérer plusieurs locataires),le certificat **`globalprotect_app_log_cert`** est automatiquement

 ©2026 Palo Alto Networks, Inc.

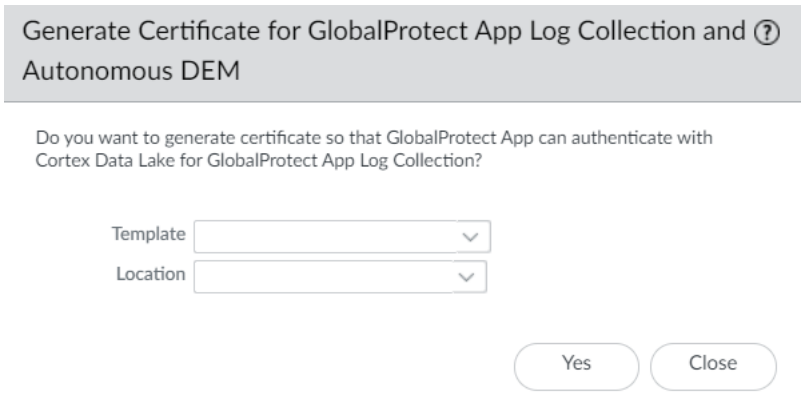
importé dans le deuxième modèle d'utilisateur mobile après le premier **mu-tpl-***tenant (locataire)* nommé. Le certificat **`globalprotect_app_log_cert`** est importé dans les locataires supplémentaires.

Une fois que le certificat **`globalprotect_app_log_cert`** a été généré et téléchargé dans **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (certificats)**, vous recevez un message de réussite. Le **Mobile_User_Template** est sélectionné automatiquement en tant que **Template (Modèle)** et **Shared (Partagé)** est sélectionné automatiquement en tant que**Location (Emplacement)**.



5. Dans les déploiements de pare-feu de nouvelle génération, sélectionnez n'importe quel **Template (modèle)** dans la liste déroulante et **Location (Emplacement)** dans la liste déroulante.

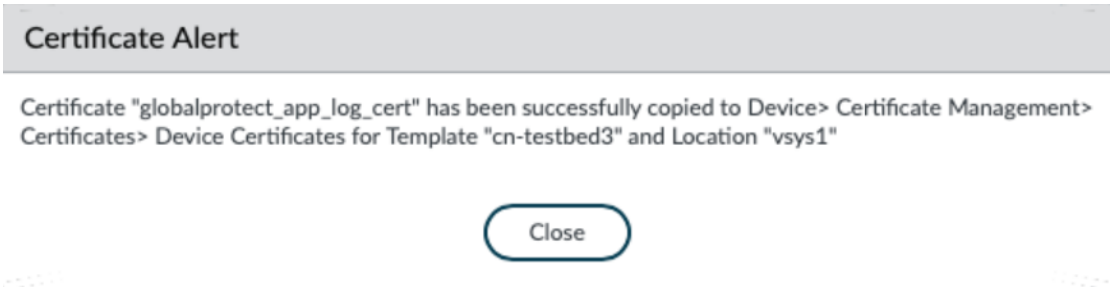
   Cliquez sur **Yes (Oui)** pour générer un certificat client.



   Une fois que le certificat **`globalprotect_app_log_cert`** a été généré et téléchargé dans **Device (périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Certificates Device (Périphérique des certificats)**, vous recevez un message de réussite. Le modèle affecté est sélectionné

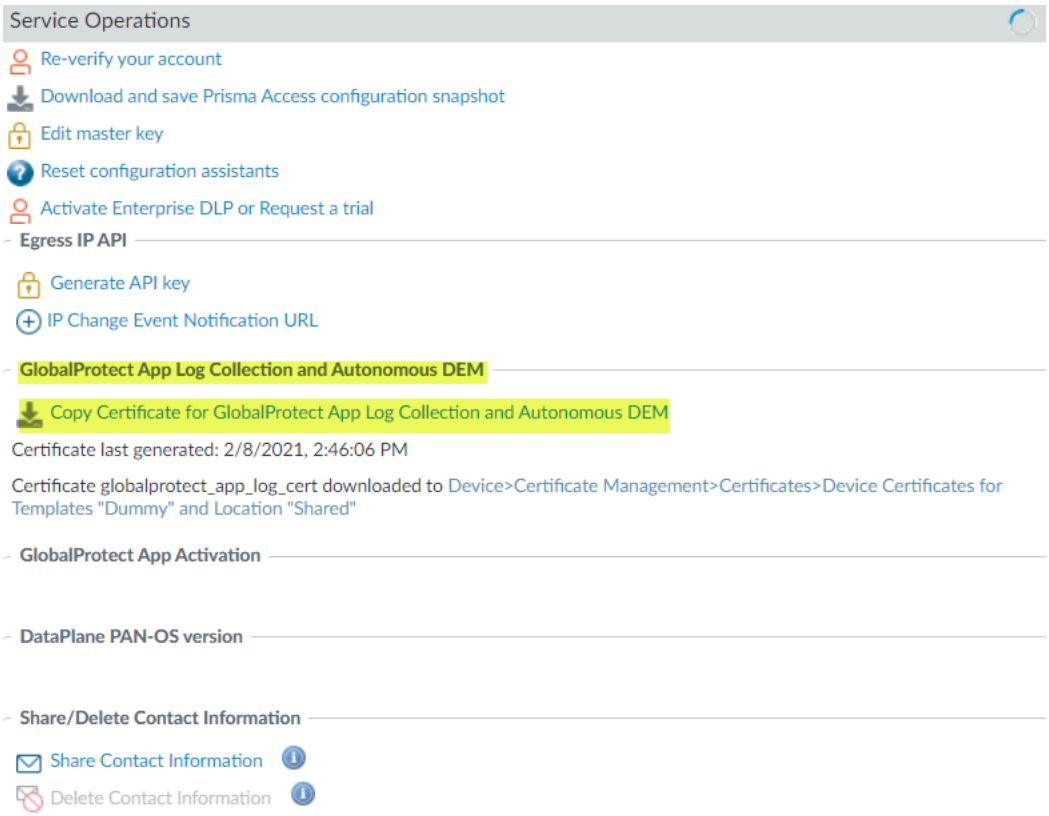
 ©2026 Palo Alto Networks, Inc.

automatiquement en tant que **Template (modèle)** et l'emplacement attribué est sélectionné automatiquement en tant que **Location (Emplacement)**.



6. (Facultatif) Dans les déploiements de pare-feu de nouvelle génération, copiez le certificat **`globalprotect_app_log_cert`** vers un autre modèle et un autre emplacement.

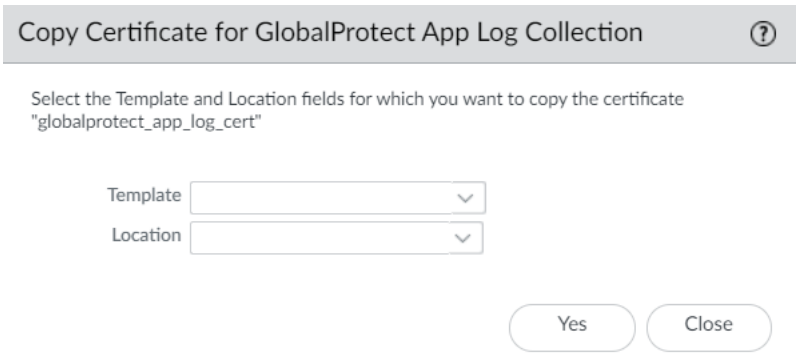
   Sélectionnez **Copy Certificate for GlobalProtect App Log Collection and Autonomous DEM (Copier le certificat pour la collecte de journaux de l'application GlobalProtect et DEM autonome)**.



   Sélectionnez un autre **Template (modèle)** dans la liste déroulante et **Location (Emplacement)** dans la liste déroulante.

   Cliquez sur **Yes (Oui)** pour générer un certificat client.

 ©2026 Palo Alto Networks, Inc.



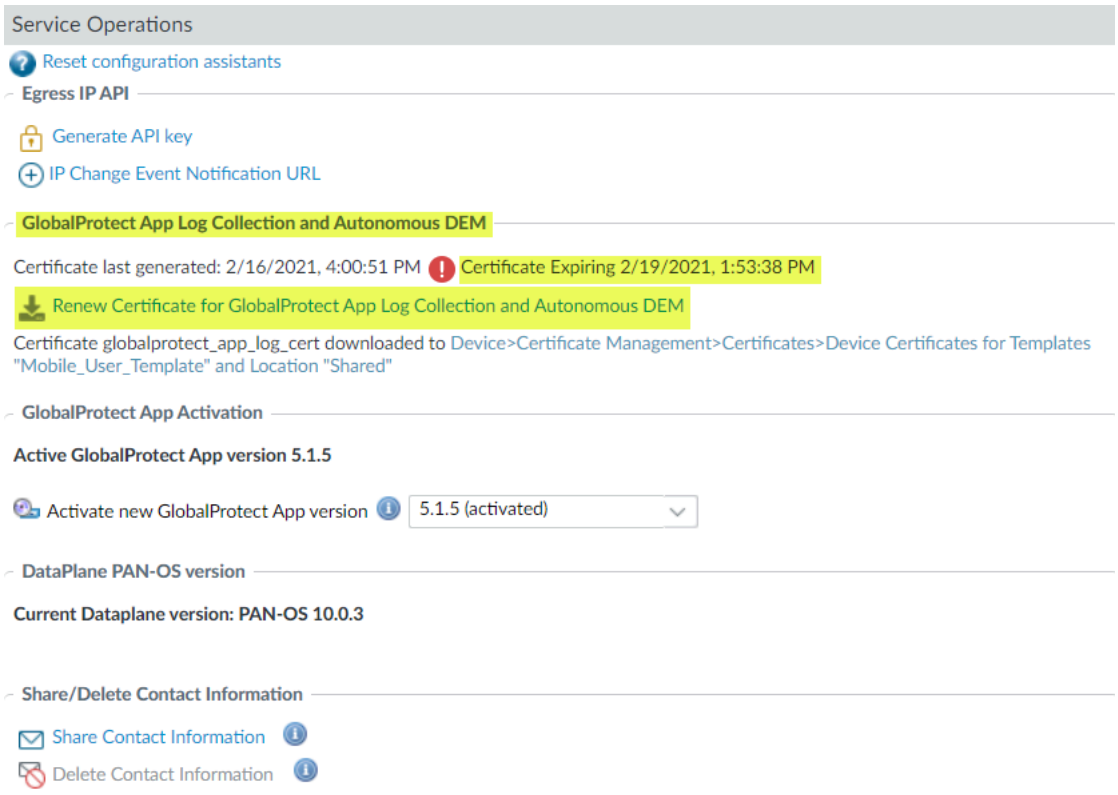
Une fois que le certificat **`globalprotect_app_log_cert`** a été généré et téléchargé dans **Device (périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Certificates Device (Périphérique des certificats)**, vous recevez un message de réussite. Le modèle affecté est sélectionné automatiquement en tant que **Template (modèle)** et l'emplacement attribué est sélectionné automatiquement en tant que **Location (Emplacement)**.

 ©2026 Palo Alto Networks, Inc.

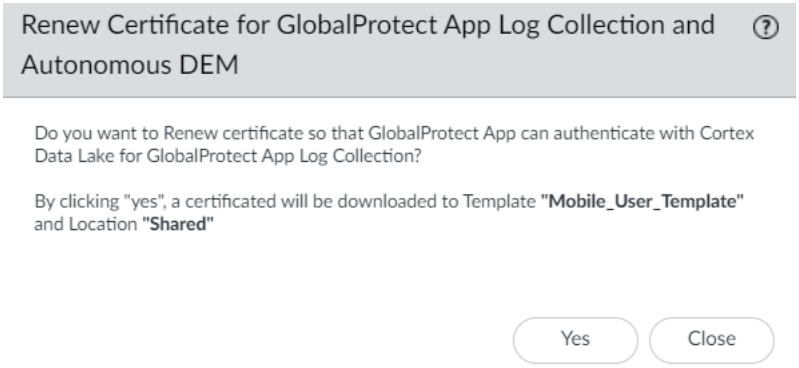
3. (Optional (Facultatif)) Demandez un nouveau certificat client avant l'expiration du certificat.

Le certificat client a une durée de vie de 1 an.

1. Dans Panorama, sélectionnez **Panorama** > **Cloud Services (Services Cloud)** > **Configuration** > **Tenants (Locataires)**
2. Sélectionnez le client que vous avez créé dans la liste déroulante **Tenant (Locataire)**.
3. Sélectionnez **Panorama** > **Cloud Services (Services Cloud)** > **Configuration** > **Service Setup (Configuration du service)**.
4. Sélectionnez **Renew Certificate for GlobalProtect App Log Collection and Autonomous DEM (Renouveler le certificat pour la collecte de journaux de l'application GlobalProtect et DEM Autonome)**.



5. Cliquez sur **Oui** pour renouveler et télécharger un autre certificat client. Le modèle affecté est associé automatiquement en tant que **Template (modèle)** et l'emplacement attribué est associé automatiquement en tant que**Location (Emplacement)**.



 ©2026 Palo Alto Networks, Inc.

4. Créez ou modifiez la configuration existante de GlobalProtect agent configuration (agent GlobalProtect) pour un groupe spécifique d'utilisateurs.

Pour activer la collecte de journaux d'application GlobalProtect à des fins de dépannage, vous devez définir la configuration de l'agent pour qu'un groupe spécifique d'utilisateurs envoie les journaux à Strata Logging Service.

1. Dans Panorama, sélectionnez **Network (réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez la **Mobile_User_Template** dans la liste déroulante **Template (Modèle)**.

   Si vous configurez un déploiement qui inclut plusieurs instances de Prisma Access sur un seul Panorama(multi-tenancy (mutualisation)), vous pouvez sélectionner un autre modèle associé à la configuration.
3. Sélectionnez **GlobalProtect_Portal** pour modifier la configuration du portail Prisma Access.
4. Sélectionnez l'onglet **Agent.**
5. Sélectionnez l'onglet **Agent** et sélectionnez la configuration de l'agent.
6. Sélectionnez **Local** (par défaut) et **DEFAULT (PAR DÉFAUT)globalprotect_app_log_cert** dans la liste déroulante **Client Certificate (Certificat client)**.

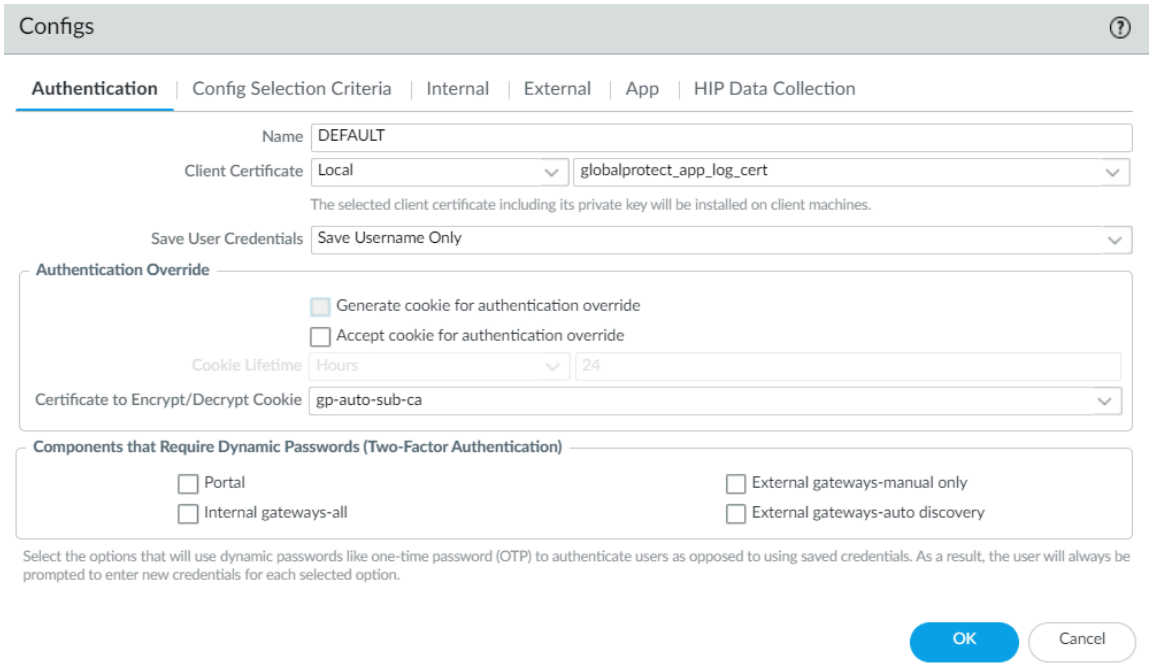
   Après avoir « Activer la collecte de journaux Autonomous DEM et GlobalProtect pour le dépannage » et poussé **globalprotect_app_log_cert** vers la machine client, un certificat CA racine, deux CA intermédiaires et un certificat client, émis par Palo Alto Networks, sont installés dans le magasin personnel de l'utilisateur.

   Palo Alto Networks génère automatiquement le certificat client Strata Logging Service, donc le certificat CA racine et le certificat CA intermédiaire doivent être détenus par Palo Alto Networks. Palo Alto Networks peut ajouter le certificat racine à la configuration du portail afin que le client GlobalProtect puisse l'installer en tant que CA racine de confiance sur la machine s'il souhaite le faire.

   *Étant donné que le **Client Certificate (certificat client)** est utilisé pour pousser le certificat Strata Logging Service, vous ne pouvez pas pousser le certificat client pour vous authentifier sur le portail ou la passerelle à l'aide d'un type de certificat **Local***

 ©2026 Palo Alto Networks, Inc.

(par défaut) ou d'un protocole Simple Certificate Enrollment Protocol (protocole simple d'enregistrement de certificat - SCEP).



Configurer la connectivité GlobalProtect à Strata Logging Service (Plug-in Cloud Services 1.8 et 2.0 préféré)

Avec le plug-in Cloud Services 1.8 et 2.0 Preferred, vous devez utiliser les commandes pour configurer la connectivité GlobalProtect afin que l'application GlobalProtect puisse s'authentifier auprès de Strata Logging Service pour la collecte des journaux.

1. Utilisez l'Estimateur de service de journalisation Strata pour calculer la quantité de stockage dont vous avez besoin dans Strata Logging Service.

 ©2026 Palo Alto Networks, Inc.

2. Générez un certificat client utilisé pour établir une connexion entre l'application GlobalProtect et Strata Logging Service.
   1. Ouvrez une session CLI avec des privilèges d'administrateur, en utilisant la même adresse IP que celle que vous utilisez pour vous connecter au Panorama qui gère Prisma Access.
   2. Saisissez la commande**request plugins cloud_services gpclient_cert fetch**, comme illustré dans l'exemple suivant :

      ```
      admin-Panorama>requête de plugins cloud_services gpclient_cert
       fetch Succès Importation réussie de globalprotect_gp_log_cert
       dans la configuration candidate
      ```

      Si un certificat client est déjà généré, la sortie de la commande est la suivante :

      ```
      admin-Panorama> demande de plugins cloud_services
       gpclient_cert fetch le certificat existe et n'est pas expiré
      ```
   3. Validez vos modifications sur Panorama.
   4. Vérifiez l'état du certificat client en entrant la commande suivante :

      ```
      admin-Panorama> demande de plugins cloud_services
       gpclient_cert status  le certificat
       globalprotect_app_log_cert est valide jusqu'au 22 oct.
       21:55:39 2021 GMT
      ```
3. Exportez le certificat **gp_app_log_cert** depuis le magasin de certificats Panorama.
   1. Dans Panorama, sélectionnez **Panorama** > **Certificate Management (Gestion des certificats)** > **Certificates (certificats)**sélectionnez le certificat **gp_app_log_cert**, et **Export Certificate (Exporter le certificat)**.
   2. Sélectionnez **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat chiffrés (PKCS12)** dans la liste déroulante **File Format (Format de fichier)** pour exporter le certificat et la clé privée dans un seul fichier.
   3. Saisissez une **Passphrase (phrase secrète)** et **Confirm Passphrase (confirmer la phrase secrète)** pour importer la clé de certificat.
   4. Cliquez sur **OK (OK)** pour enregistrer le certificat/fichier de clé sur votre ordinateur.
4. Importez le certificat **gp_app_log_cert** dans le modèle Panorama où réside la configuration du portail GlobalProtect.

   Si vous configurez Prisma Access pour gérer un seul client, vous devez importer le certificat **gp_app_log_cert** dans le **Mobile_User_Template**.

   Si vous configurez Prisma Access pour manage multiple tenants (gérer plusieurs locataires),vous devez importer le certificat **gp_app_log_cert** dans le deuxième modèle

 ©2026 Palo Alto Networks, Inc.

d'utilisateur mobile créé automatiquement après le premier **mu-tpl-***tenant (locataire)* nommé. Vous devez importer le certificat **`gp_app_log_cert`** dans les clients supplémentaires.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis cliquez sur **Import (Importer)**.
2. Comme **Certificate Type (Type de certificat)**, sélectionnez **Local**.
3. Entrez **`gp_app_log_cert`** comme **Certificate Name (nom du certificat)**.
4. **Browse (Recherchez)** le fichier de certificat que vous avez exporté.
5. Saisissez la **Passphrase (Phrase secrète)** et **Confirm Passphrase (Confirmez la phrase secrète)** utilisée pour chiffrer la clé privée.
6. Cliquez sur **OK** pour importer le certificat.

5. Créez ou modifiez la configuration existante de GlobalProtect agent configuration (agent GlobalProtect) pour un groupe spécifique d'utilisateurs.

Pour activer la collecte de journaux d'application GlobalProtect à des fins de dépannage, vous devez définir la configuration de l'agent pour qu'un groupe spécifique d'utilisateurs envoie les journaux à Strata Logging Service.

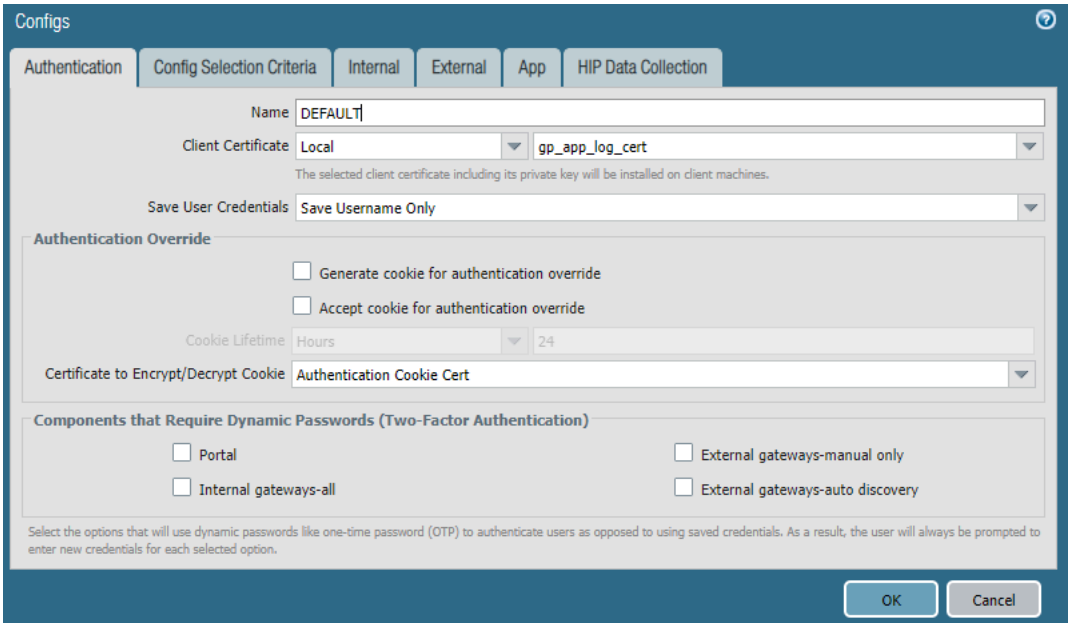
1. Dans Panorama, sélectionnez **Network (réseau)** > **GlobalProtect** > **Portals (Portails)**.
2. Sélectionnez la **Mobile_User_Template** dans la liste déroulante **Template (Modèle)**.

   Si vous configurez un déploiement qui inclut plusieurs instances de Prisma Access sur un seul Panorama(multi-tenancy (mutualisation)), vous pouvez sélectionner un autre modèle associé à la configuration.
3. Sélectionnez **GlobalProtect_Portal** pour modifier la configuration du portail Prisma Access.
4. Sélectionnez l'onglet **Agent.**
5. Sélectionnez l'onglet **Agent** et sélectionnez la configuration de l'agent **DEFAULT (PAR DÉFAUT)**.
6. Sélectionnez **Local** (par défaut) et **gp_app_log_cert** dans la liste déroulante **Client Certificate (Certificat client)**.

   *Étant donné que le **Client Certificate (certificat client)** est utilisé pour pousser le certificat Strata Logging Service, vous ne pouvez pas pousser le certificat client pour vous authentifier sur le portail ou la passerelle à l'aide d'un type de certificat **Local***

 ©2026 Palo Alto Networks, Inc.

(par défaut) ou d'un protocole Simple Certificate Enrollment Protocol (protocole simple d'enregistrement de certificat - SCEP).



Configurer les paramètres de collecte des journaux de l'application sur le portail GlobalProtect

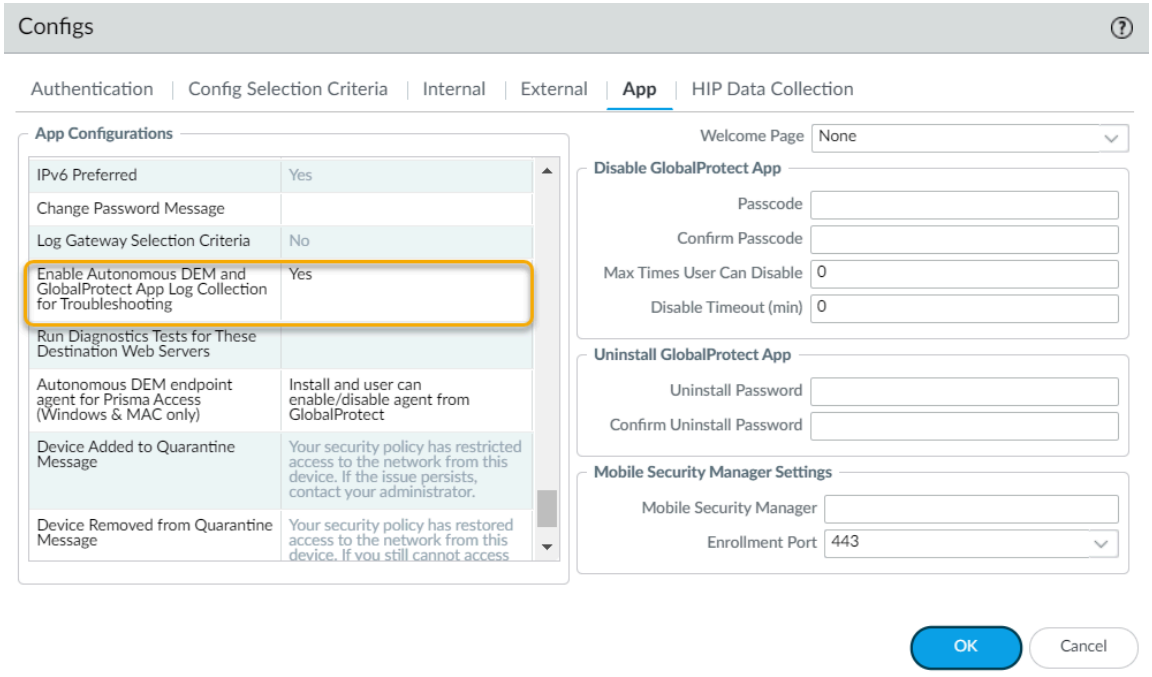
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Vous devez activer l'application GlobalProtect pour afficher l'option **Report an Issue (Signaler un problème)** sur l'application GlobalProtect pour permettre aux utilisateurs finaux d'envoyer les journaux de dépannage et de diagnostic de l'application GlobalProtect directement depuis leur terminal vers l'instance du service de journalisation Strata associée au déploiement Prisma Access pour plus de détails.

1. Activez la collecte de journaux d'applications GlobalProtect pour le dépannage sur le portail GlobalProtect.
   1. Dans Panorama, sélectionnez **Networks (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***GlobalProtect_Portal*** > **Agent *DEFAULT (PAR DÉFAUT)*** > **App** > **Enable Autonomous DEM and GlobalProtect Log Collection for Troubleshooting (Activer le DEM autonome et la collecte de journaux GlobalProtect pour le dépannage)**.
   2. Définissez **Enable Autonomous DEM and GlobalProtect Log Collection for Troubleshooting (Activer DEM autonome et Collecte de journaux GlobalProtect pour le dépannage)** sur **Yes (Oui)** pour permettre à l'application GlobalProtect d'afficher l'option **Report an issue (Signaler un problème)** sur l'application GlobalProtect afin de permettre aux utilisateurs finaux d'envoyer les journaux de dépannage et de diagnostic directement ay service de journalisation Strata. Vous devez configurer le certificat Strata Logging Service qui est poussé depuis le portail en tant que certificat client pour afficher

 ©2026 Palo Alto Networks, Inc.

l'option **Report an issue (Signaler un problème)**. Ce certificat est utilisé pour que le client s'authentifie auprès de Strata Logging Service lors de l'envoi des journaux. Lorsque ce paramètre est défini sur **No (Non)** (par défaut), l'application GlobalProtect n'affiche pas l'option **Report an issue (Signaler un problème)** et les utilisateurs finaux ne peuvent pas envoyer les journaux de dépannage et de diagnostic à Strata Logging Service.



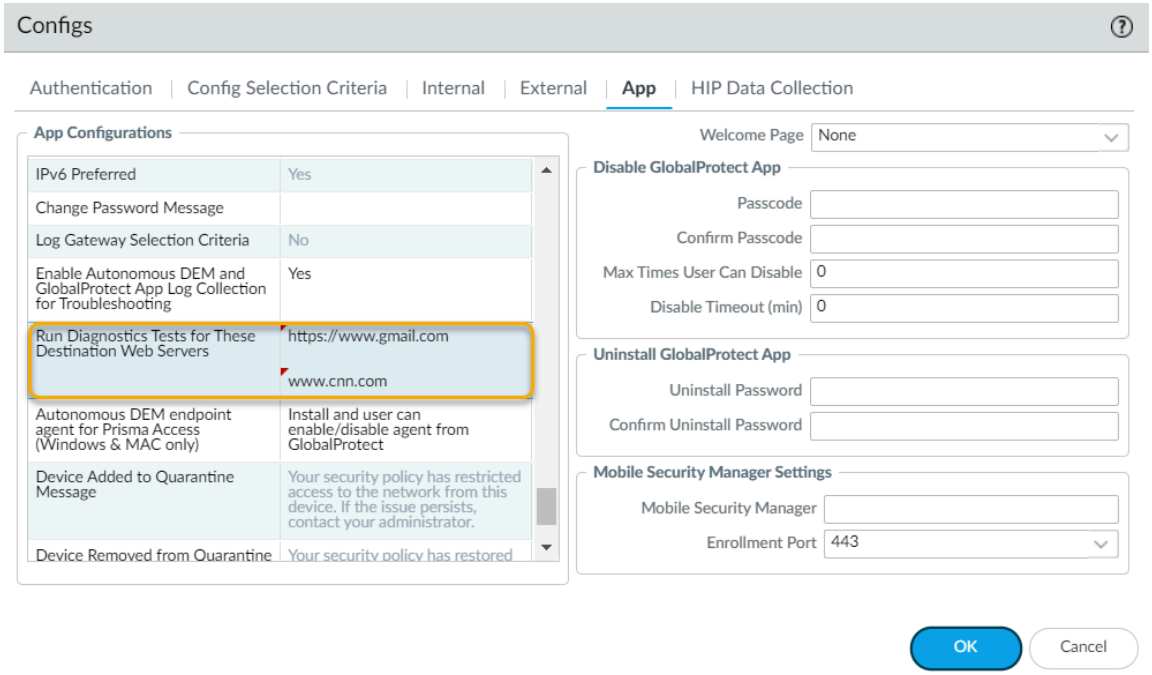
2. Configurez les URL de destination basées sur HTTPS qui peuvent contenir des adresses IP ou des noms de domaine complets sur le portail GlobalProtect. Plus tard, ces URL de destination basées sur HTTPS sont utilisées pour lancer des tests de performances pour la vérification.

   1. Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***GlobalProtect_Portal*** > **Agent** ***DEFAULT (PAR DÉFAUT)*** > **App** > **Run Diagnostics Tests for These Destination Web Servers (Exécuter des tests de diagnostic pour ces serveurs Web de destination)**.
   2. Spécifiez jusqu'à dix URL de destination HTTPS pouvant contenir des adresses IP ou des noms de domaine complets (par exemple, https://10.10.10.10/resource.html, https://webserver/file.pdf ou https:// google.com) pour **Run Diagnostics Tests for These Destination Web Servers (exécuter des tests de diagnostic pour ces serveurs Web de destination sur le portail GlobalProtect)**. Pour vous aider à identifier avec précision les résultats de vitesse de téléchargement, vous pouvez spécifier un emplacement de fichier de téléchargement ayant la taille appropriée. Par exemple, la taille du fichier peut aller de 10 Mo à 50 Mo pour calculer la vitesse de téléchargement suffisante. Cependant, ce calcul n'est pas vrai pour la limitation de taille de la page Web pour récupérer et télécharger le fichier qui peut prendre moins d'une seconde, ce qui n'est pas une taille d'échantillon suffisante pour déterminer des résultats de vitesse de téléchargement élevés. Ce champ est vide par défaut.

      Les URL de destination HTTPS qui peuvent contenir des adresses IP ou des noms de domaine complets que vous fournissez sont utilisées uniquement lorsque **Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting (Activer DEM autonome et Collecte de journaux de l'application GlobalProtect App pour le**

 ©2026 Palo Alto Networks, Inc.

dépannage) est défini sur **Yes (Oui)** et lorsque les diagnostics sont effectués. Ces URL de destination basées sur HTTPS ne sont pas utilisées lorsque l'application GlobalProtect crée des rapports de dépannage en cas de problème. Utilisez des virgules, des points-virgules ou des lignes distinctes pour séparer plusieurs noms de domaine complets (par exemple, google.com, gmail.com).



Afficher les journaux de dépannage et de diagnostic de l'application GlobalProtect sur l'application Explore

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d’abonnement GlobalProtect

Vous devez utiliser la fonctionExplore (Explorer) l’application pour afficher tous les rapports de dépannage et les journaux de diagnostics de l’application GlobalProtect qui sont transférés à Strata Logging Service depuis le terminal de l’utilisateur final. Les details within the GlobalProtect app troubleshooting and diagnostic logs (détails contenus dans les journaux de dépannage et de diagnostic de l'application GlobalProtect) vous aident à identifier la cause première et à résoudre les problèmes de connectivité, d'accès au réseau ou de performances.

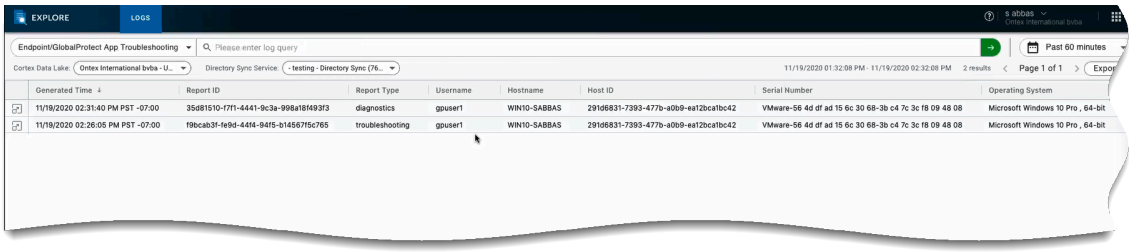
1. Récupérez les enregistrements des dépannages et les journaux de l’application GlobalProtect transférés à Strata Logging Service.
   1. Connectez-vous au hub (plate-forme) de Palo Alto Networks et sélectionnez **Explore (Explorer)**.
   2. Sélectionnez **Endpoint/GlobalProtect App Troubleshooting (Dépannage du terminal/de l’application GlobalProtect)**.

 ©2026 Palo Alto Networks, Inc.

2. Affichez la totalité de l'enregistrement de dépannages ou journaux de diagnostics.
   1. Cliquez sur l'icône

      à côté de la ligne.

      Vous pouvez modifier les champs qui s'affichent dans le log table (tableau des journaux), leur ordre, les champs qui sont épinglés et utiliser la fonction de Recherche pour trouver rapidement des champs spécifiques dans les journaux de dépannage du terminal de l'utilisateur final. Par exemple, vous pouvez récupérer le numéro de série du terminal, le nom d'hôte, le nom d'utilisateur ou l'ID d'hôte unique du terminal.

   2. Vérifiez la totalité de l'enregistrement de dépannages et journaux de diagnostics dans la fenêtre **Log Details (détails du journal)**. L'enregistrement du journal peut uniquement inclure des informations de dépannage ou un journal de diagnostic basé sur le consentement de l'utilisateur.

      Les champs des journaux individuels sont regroupés de façon logique. Si vous n'avez pas activé l'application pour effectuer des tests de diagnostic et pour inclure les journaux de diagnostic, les champs du journal des groupes **Endpoint State (état du terminal)**, **GlobalProtect App Health (santé de l'application GlobalProtect)**, **Gateway Network Impairments (Faiblesses du réseau de la passerelle),** et **App Access Performance (Performance d'accès de l'appli)** sont vides.
   3. (Optional (Facultatif)) Si les utilisateurs finaux ont consenti à exécuter des tests de diagnostic sur l'application GlobalProtect, cliquez sur **Debug Logs (Journaux de débogage)** pour télécharger les fichiers journaux de débogage GlobalProtect sur votre bureau pour une analyse plus approfondie.

      Vous pouvez décompresser les fichiers journaux de débogage GlobalProtect à partir du package zip `reportid_GlobalProtectLogs.zip`. Vous pouvez saisir les critères

 ©2026 Palo Alto Networks, Inc.

de recherche **reportid** dans le champ Search pour trouver rapidement le package zip `reportid_GlobalProtectLogs.zip`.

Détails dans les journaux de dépannage et de diagnostic de l'application GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d’abonnement GlobalProtect

Utilisez les rubriques suivantes pour vous aider à identifier la cause première des problèmes de connectivité, d'accès au réseau ou de performances rencontrés par les utilisateurs finaux en affichant l'intégralité de l'enregistrement du journal de dépannage et de diagnostic dans la fenêtre **Log Details (Détails du journal)** :

- Informations générales des journaux
- Détails du journal du portail
- Détails du journal de la passerelle
- Détails du journal du réseau
- Détails du journal d'état du point de terminaison
- Détails du journal de santé de l'application GlobalProtect
- Altérations du réseau de passerelle
- Performances d'accès aux applications

Informations générales des journaux

Le tableau suivant décrit les champs des journaux individuels dans le groupe logique **General (Général)** du journal **Endpoint/GlobalProtect App Troubleshooting (Dépannage du terminal/de l’application GlobalProtect)**.

 ©2026 Palo Alto Networks, Inc.

Champ de journal	Description
Generated Time (Heure de génération)	Date et heure auxquelles le journal a été généré sur le terminal de l'utilisateur. Cette chaîne affiche une valeur d'horodatage au format UTC (par défaut).
ID du rapport	Identifiant unique attribué par l'application GlobalProtect au rapport.
Type de rapport	Identifie le type de rapport de dépannage ou de diagnostic généré à partir du point de terminaison de l'utilisateur final.
Nom d'utilisateur	Nom d'utilisateur utilisé pour se connecter à GlobalProtect.
Nom d'hôte	Nom d'hôte (adresse IP ou nom de domaine complet) pour le point de terminaison de l'utilisateur final.
ID d'hôte	L'ID unique que GlobalProtect affecte afin d'identifier l'hôte.
Numéro de série	Numéro de série du terminal de l'utilisateur.
Système d'exploitation	Type d'OS du terminal de l'utilisateur final sur lequel l'application GlobalProtect est déployée.
Locale (localisation)	Langage du système du terminal de l'utilisateur final sur lequel l'application GlobalProtect est déployée.
GlobalProtect Version (Version de GlobalProtect)	Numéro de la version de l'application GlobalProtect.
Error Stage (Etape d'erreur)	Identifie à quelle étape dans le flux de connexion GlobalProtect comme la connexion préalable au portail, la passerelle, get-config ou découverte du réseau l'erreur de portail ou passerelle s'est produite.
Message d'erreur	Le dernier message d'erreur qui a déclenché la génération du rapport. Le même message d'erreur s'affiche dans l'application GlobalProtect.
Error Details (Détails de l'erreur)	D'autres informations vous aident à identifier la cause de l'erreur afin de résoudre les problèmes

©2026 Palo Alto Networks, Inc.

Champ de journal	Description
	de connectivité, accès au réseau et performance depuis le terminal de l'utilisateur final.
Error Generated Time (Heure de génération de l'erreur)	Heure à laquelle le journal a été généré sur le terminal de l'utilisateur. Cette chaîne affiche une valeur d'horodatage au format UTC (par défaut).
Host Time Offset (Décalage de l'heure de l'hôte)	Décalage de fuseau horaire par rapport au méridien de Greenwich (GMT) en minutes de l'hôte. Par exemple, la valeur de `-420` s'affiche pour le fuseau horaire PST lorsque l'heure d'été est activée.

Détails du journal du portail

Le tableau suivant décrit les champs des journaux individuels dans le groupe logique du **Portal (portail)** du journal **Endpoint/GlobalProtect App Troubleshooting (Dépannage du terminal/de l'application GlobalProtect)**.

Champ de journal	Description
Adresse du portail	Portail GlobalProtect auquel l'utilisateur final s'est connecté en dernier.
Portal Reachable (Portail atteignable)	Lorsque le portail est atteignable et accepté dans la requête de connexion TCP.
Portal SSL Certificate Valid (Certificat SSL valide du portail)	Si le certificat du serveur de portail est valide.
Portal Authentication (Portail d'authentification)	La méthode d'authentification utilisée pour établir une connexion avec le portail (par exemple l'authentification du certificat du client, nom d'utilisateur/mot de passe ou SAML).
Portal Status (Statut du portail)	Si l'application GlobalProtect est en mesure d'établir une connexion avec le portail.
Cached Configuration (Configuration en cache)	Si la configuration du portail mis en cache local est utilisée (par exemple, lorsque le portail est inaccessible).
Configuration Refresh (Actualisation de la configuration)	Si la connexion au portail GlobalProtect est automatiquement utilisée pour l'actualisation de la configuration.

©2026 Palo Alto Networks, Inc.

Champ de journal	Description
Last Connect Time (Dernière heure de connexion)	La dernière fois où l'utilisateur final s'est connecté au portail. Cette chaîne affiche une valeur d'horodatage au format UTC (par défaut).

Détails du journal de la passerelle

Le tableau suivant décrit les champs des journaux individuels dans le groupe logique **Gateway (Passerelle)** du journal **Endpoint/GlobalProtect App Troubleshooting (Dépannage du terminal/de l'application GlobalProtect)**.

Champ de journal	Description
Gateway Address (Adresse de la passerelle)	Passerelle GlobalProtect à laquelle l'utilisateur final s'est connecté en dernier ou a tenté de se connecter en fonction des rapports d'échec de connexion à la passerelle.
Emplacement	Emplacement de la passerelle GlobalProtect à laquelle l'utilisateur final s'est connecté. Vous pouvez également utiliser ces informations sur l'emplacement pour déterminer la proximité des utilisateurs finaux avec la passerelle. Si vous ne spécifiez pas l'emplacement de la passerelle, l'application Explore affiche un champ d'emplacement vide.
Gateway Reachable (Passerelle atteignable)	Lorsque la passerelle est atteignable et acceptée dans la requête de connexion TCP.
Attempted Gateways (Passerelles tentées)	Liste des passerelles tentées avant de se connecter à une passerelle spécifique.
Gateway SSL Certificate Valid (Certificat SSL valide de la passerelle)	Si le certificat du serveur de passerelle est valide pour permettre à l'application GlobalProtect de se connecter à une passerelle.
Gateway Authentication (Authentification de la passerelle)	La méthode d'authentification comme l'authentification du certificat du client, nom d'utilisateur/mot de passe ou SAML qui est utilisée pour établir une connexion avec la passerelle.
Gateway Status (état de la passerelle)	Si l'application GlobalProtect est en mesure d'établir une connexion avec la passerelle. **Connected (Connecté)** indique une connexion VPN réussie. **Disconnected (Déconnecté)**

 ©2026 Palo Alto Networks, Inc.

Champ de journal	Description
	indique que l'utilisateur final n'est pas connecté. **RestoringVPN connection (Restauration de la connexion VPN)** indique que GlobalProtect a tenté de rétablir la connexion après la déconnexion du tunnel.
IPSec Enabled (IPSec activé)	IPSec est activé pour sécuriser les tunnels VPN entre l'application GlobalProtect et la passerelle.
IPSec Failure Reason (Motif de l'échec IPSec)	Informations sur l'échec d'une connexion tunnel IPSec infructueuse. Par exemple, lorsque le port 4501 est spécifié pour UDP et bloqué, la connexion IPSec ne peut pas être établie.
SSL Failure Reason (Motif de l'échec SSL)	Informations sur l'échec d'une connexion tunnel SSL infructueuse. Par exemple, le tunnel SSL n'a pas réussi à établir une connexion ou le délai d'attente keepalive s'est déconnecté après l'établissement de la connexion du tunnel.
Fallback to SSL Reason (Motif du basculement vers SSL)	Informations sur l'application GlobalProtect pour se rabattre sur un tunnel SSL lorsque le tunnel IPSec ne peut pas être établi.
DLSA Status (Etat DLSA)	Si l'option **No direct access to local network (Pas d'accès direct au réseau local)** est activée.
Logout Time (Durée de verrouillage)	La dernière fois que l'utilisateur final s'est déconnecté avec succès de la passerelle. Cette chaîne affiche une valeur d'horodatage au format UTC (par défaut).
Tunnel Rename (Renommer le tunnel)	(Windows only (Windows uniquement)) Indique si le tunnel de pré-ouverture de session a été renommé en tunnel utilisateur.

Détails du journal du réseau

Le tableau suivant décrit les champs des journaux individuels dans le groupe logique duNetwork (réseau) du journal **Endpoint/GlobalProtect App Troubleshooting (Dépannage du terminal/de l'application GlobalProtect)**.

Champ de journal	Description
Network Access (Accès au réseau)	Si l'accès au réseau est disponible.

 ©2026 Palo Alto Networks, Inc.

Champ de journal	Description
Type	Type de connectivité réseau telle qu'Ethernet, WiFi ou réseau étendu sans fil (WWAN) sur le point de terminaison de l'utilisateur final.
Internet Access (Accès Internet)	Si l'accès Internet est disponible sur le point de terminaison de l'utilisateur final.
Internal Network (Réseau interne)	Si le point de terminaison de l'utilisateur final se trouve sur le réseau interne.
portail captif	Si le portail captif est détecté afin que l'utilisateur final doive se connecter à un portail captif pour accéder à Internet.
Proxy Server (Serveur proxy)	Nom d'hôte du serveur proxy si le proxy est configuré.
Dual Stack Tunnel Interface (Interface de tunnel à double pile)	Si le réseau à double pile de l'interface du tunnel est activé.
DNS Reachable (DNS accessible)	Si les serveurs DNS sont configurés pour l'accès à Internet et accessibles via l'adaptateur physique.
Portal/Gateway Latency (Latence du portail/passerelle)	Le nombre de millisecondes avant l'expiration de la connexion TCP pour le portail ou la passerelle en raison de l'absence de réponse.
GlobalProtect MTU	La valeur **GlobalProtect MTU** qui est utilisée par l'application pour l'adaptateur virtuel (voir GlobalProtect App Customization (Personnalisation de l'application GlobalProtect)).

Détails du journal d'état du point de terminaison

Le tableau suivant décrit les champs des journaux individuels dans le groupe logique **Endpoint state (état du point de terminaison)** du journal **Endpoint/GlobalProtect App Troubleshooting (Dépannage du terminal/de l'application GlobalProtect)**.

> *Si vous n'avez pas activé l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, les champs de journal sont vides pour le groupe **Endpoint State (état du point de terminaison)**.*

 ©2026 Palo Alto Networks, Inc.

Champ de journal	Description
CPU Usage (Utilisation du processeur)	Pourcentage de CPU utilisé sur le point de terminaison de l'utilisateur final.
GlobalProtect CPU Usage (Utilisation du processeur GlobalProtect)	Le pourcentage de CPU utilisé par l'application GlobalProtect.
Total memory (Mémoire totale)	Mémoire totale en Go.
Memory Usage (Utilisation de la mémoire)	Pourcentage de la mémoire totale utilisée sur le point de terminaison de l'utilisateur final.
GlobalProtect Memory Usage (Utilisation de la mémoire GlobalProtect)	Le pourcentage de la mémoire totale utilisée par l'application GlobalProtect.
Total Disk Space (Espace disque total)	L'espace disque total utilisé sur le point de terminaison de l'utilisateur final.
Disk Available (Disque disponible)	Espace disque total disponible sur le point de terminaison de l'utilisateur final.

Détails du journal de santé de l'application GlobalProtect

Le tableau suivant décrit les champs des journaux individuels dans le groupe logique **GlobalProtect App Health (intégrité de l'application GlobalProtect)** du journal **Endpoint/ GlobalProtect App Troubleshooting (Dépannage du terminal/de l'application GlobalProtect)**.

> *Si vous n'avez pas activé l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, les champs de journal sont vides pour le groupe **GlobalProtect App Heath (intégrité de l'application GlobalProtect)**.*

Champ de journal	Description
Install History (Historique d'installation)	Si l'application GlobalProtect a été installée pour la première fois, mise à niveau vers une version plus récente ou rétrogradée vers une version précédente. Si les utilisateurs finaux effectuent une mise à niveau depuis l'application GlobalProtect 5.2.5 vers une version plus récente, **Install History (historique d'installation)** affiche qu'ils ont mis à niveau depuis l'application GlobalProtect 5.2.5. Si les utilisateurs finaux effectuent une mise à niveau de l'application GlobalProtect 5.2.4 vers 5.2.5,**Install History (historique d'installation)** affiche **Fresh Install (Nouvelle installation)**. Si les utilisateurs finaux passent d'une version plus récente telle que l'application GlobalProtect 5.2.6 à 5.2.5, **Install History (historique d'installation)**

 ©2026 Palo Alto Networks, Inc.

Champ de journal	Description
	affiche qu'ils sont passés de l'application GlobalProtect 5.2.6 à 5.2.5. Si les utilisateurs finaux passent à des versions antérieures de l'application (5.2.4 et versions antérieures), la fonctionnalité Collecte de journaux de l'application GlobalProtect pour dépannage n'est pas prise en charge.
Enforcer Status (Statut de l'exécutant)	Si les connexions GlobalProtect pour l'accès au réseau sont activées ou désactivées sur le portail GlobalProtect mais pas appliquées sur le portail (voir GlobalProtect App Customization (Personnalisation de l'application GlobalProtect)).
Privilèges	(masOS only (macOS uniquement)) Si les utilisateurs finaux disposent de privilèges pour effectuer des tâches telles que activation des system extensions (extensions système) pour configurer un tunnel divisé en fonction du domaine et de l'application de destination et pour appliquer les connexions GlobalProtect pour l'accès au réseau sans nécessiter d'extensions de noyau.
App Tampered (Application falsifiée)	(Windows and macOS only (Windows et macOS uniquement)) Si les fichiers d'application GlobalProtect sont altérés ou modifiés sur le point de terminaison de l'utilisateur final.
Jailbroken Status (État de jailbreak)	(iOS and Android only (iOS et Android uniquement)) Si ces points de terminaison d'utilisateur final ont subis un jailbreak.
Last HIP Report Time (Heure du dernier rapport HIP)	Dernière fois que le rapport d'informations sur l'hôte (HIP) a été envoyé. Cette chaîne affiche une valeur d'horodatage au format UTC (par défaut).
Last Logout Time (Heure de la dernière déconnexion)	Dernière fois que l'application GlobalProtect s'est déconnectée. Cette chaîne affiche une valeur d'horodatage au format UTC (par défaut).
Disable History (Désactiver l'historique)	Nombre de fois répertorié lorsque les utilisateurs finaux ont activé ou désactivé l'application GlobalProtect. Cette chaîne affiche une valeur d'horodatage au format UTC (par défaut).
Split-tunnel Configuration (Configuration de tunnel séparé)	(Windows and macOS only (Windows et macOS uniquement)) Type de capacité de tunnel divisé configurée en fonction d'une route d'accès, d'un

©2026 Palo Alto Networks, Inc.

Champ de journal	Description
	domaine de destination, d'une application et d'une application de streaming vidéo HTTP/HTTPS.
Crash history (Historique des plantages)	(Windows and macOS only (Windows et macOS uniquement)) Nombre d'horodatages qui correspondent aux plantages de l'application GlobalProtect (le cas échéant).

Altérations du réseau de passerelle

Le tableau suivant décrit les champs des journaux individuels dans le groupe logique **Gateway Network Impairments (altérations du réseau de passerelle)** du journal **Endpoint/GlobalProtect App Troubleshooting (Dépannage du terminal/de l'application GlobalProtect)**.

*Si vous n'avez pas activé l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, les champs de journal sont vides pour le groupe **Gateway Network Impairments (altérations du réseau de passerelle)**.*

Pour que l'application GlobalProtect exécute des tests de diagnostic de bout en bout pour tester les défaillances du réseau, la passerelle GlobalProtect doit être autorisée à envoyer des requêtes ping ICMP.

Champ de journal	Description
Latence	Latence mesurée entre le point de terminaison de l'utilisateur final et la passerelle Prisma Access en millisecondes.
Jitter	Gigue qui est mesurée entre le point de terminaison de l'utilisateur final et la passerelle Prisma Access sur une période de temps en millisecondes.
Perte de paquets	Pourcentage de perte de paquets utilisé pour mesurer le nombre de paquets envoyés sur un réseau qui n'ont pas réussi à atteindre la destination de la passerelle Prisma Access. Les requêtes ping ICMP doivent être autorisées sur l'interface de passerelle.

Performances d'accès aux applications

Vous pouvez spécifier jusqu'à dix URL de destination HTTPS pouvant contenir des adresses IP ou des noms de domaine complets (par exemple, https://10.10.10.10/resource.html, https://webserver/file.pdf ou https : //google.com) pour lesquelles vous souhaitez run diagnostic tests (exécuter des tests de diagnostic) en configurant le portail GlobalProtect.

*Si vous avez configuré le split tunneling pour inclure ou exclure le trafic en fonction des itinéraires d'accès **Split Tunnel (tunnel séparé)** > **Access Route (Itinéraire d'accès)** ou en fonction du*

 ©2026 Palo Alto Networks, Inc.

*domaine ou de l'application de destination (**Split Tunnel (tunnel séparé)** > **Domain et Application (Domaine et application)**) et exécuter des tests de diagnostic et vérifier les tests de performances à l'intérieur ou à l'extérieur du tunnel, split tunneling a priorité sur la table de routage et les routes plus spécifiques ont priorité sur la route par défaut.*

Pour que l'application GlobalProtect exécute des tests de diagnostic de bout en bout pour sonder les performances d'accès, les limitations suivantes s'appliquent :

- Sur iOS, les tests de performances du serveur incluent uniquement les métriques testées via l'adaptateur physique.
- Sur iOS 14 ou version ultérieure, les tests d'itinéraire de trace ne sont pas pris en charge.
- Le serveur Web doit autoriser les requêtes ping ICMP pour les tests de latence, de gigue et de perte de paquets.

Le tableau suivant décrit les champs des journaux individuels dans le groupe logique **App Access Performance (Performance de l'accès à l'application)** du journal **Endpoint/GlobalProtect App Troubleshooting (Dépannage du terminal/de l'application GlobalProtect)**.

*Si vous n'avez pas activé l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, le champ de journal est vide pour le groupe **App Access Performance (Performance d'accès à l'application)**.*

Champ de journal	Description
Server Performance (Performances du serveur)	Les données de performances du serveur sont testées à partir du point de terminaison de l'utilisateur final pour chaque application/serveur Web HTTPS de destination que vous avez configurée sur le portail. Les métriques réseau suivantes sont testées via l'adaptateur physique et à l'extérieur du tunnel : • `out_latency (latence de sortie)` : latence mesurée en millisecondes entre le point de terminaison de l'utilisateur final et pour chaque application/serveur Web HTTPS de destination via l'adaptateur physique. • `out_jitter (gigue de sortie)` : gigue mesurée sur une période de temps en millisecondes entre le point de terminaison de l'utilisateur final et pour chaque application/serveur Web HTTPS de destination via l'adaptateur physique. • `out__packet_loss (perte de paquets en sortie)` : pourcentage de perte de paquets utilisé pour mesurer le nombre de paquets envoyés sur un réseau qui n'ont pas réussi à atteindre chaque destination/applications/serveurs Web HTTPS via l'adaptateur physique. • `out_tcp_connect_time` : temps de connexion TCP mesuré au serveur via l'adaptateur physique. • `out_first_byte_time` : temps jusqu'au premier octet mesuré en millisecondes pour se connecter au serveur via l'adaptateur physique. Sur les points de terminaison macOS, le temps jusqu'au premier octet est calculé lorsque le client GlobalProtect a reçu l'heure du certificat du serveur et le temps de traitement de l'API.

 ©2026 Palo Alto Networks, Inc.

Champ de journal	Description
	• `out_download_size` : taille du fichier en octets téléchargé depuis l'adaptateur physique. • `out_download_speed` : vitesse mesurée en Kbit/s à laquelle le fichier est téléchargé à partir de l'adaptateur physique. Nous vous recommandons d'utiliser un fichier binaire pour tester la vitesse de téléchargement au lieu d'utiliser la page Web. • `out_trace_route` : résultat de la route de trace configurée sur la destination via l'adaptateur physique.
Server Performance (Performances du serveur)	Les données de performances du serveur sont testées à partir du point de terminaison de l'utilisateur final pour chaque application/serveur Web HTTPS de destination que vous avez configurée sur le portail. Les métriques réseau suivantes sont testées via le tunnel GlobalProtect : • `in_latency (latence d'entrée)` : latence mesurée en millisecondes entre le point de terminaison de l'utilisateur final et pour chaque destination/applications/serveurs Web HTTPS via le tunnel GlobalProtect. • `in_jitter (gigue d'entrée)` : gigue qui est mesurée sur une période de temps en millisecondes entre le point de terminaison de l'utilisateur final et pour chaque destination/applications/serveurs Web HTTPS via le tunnel GlobalProtect. • `in__packet_loss (perte de paquets en entrée)` : pourcentage de perte de paquets utilisé pour mesurer le nombre de paquets envoyés sur un réseau qui n'ont pas réussi à atteindre chaque destination/applications/serveurs Web HTTPS via le tunnel GlobalProtect. • `in_tcp_connect_time` : temps de connexion TCP mesuré au serveur via le tunnel GlobalProtect. • `in_first_byte_time` : temps jusqu'au premier octet mesuré en millisecondes pour se connecter au serveur via le tunnel GlobalProtect. Sur les points de terminaison macOS, le temps jusqu'au premier octet est calculé lorsque le client GlobalProtect a reçu l'heure du certificat du serveur et le temps de traitement de l'API. • `in_download_size` : taille du fichier en octets téléchargé depuis le tunnel GlobalProtect. • `in_download_speed` : vitesse mesurée en Kbit/s à laquelle le fichier est téléchargé depuis le tunnel GlobalProtect. Nous vous recommandons d'utiliser un fichier binaire pour tester la vitesse de téléchargement au lieu d'utiliser la page Web. • `in_trace_route` : résultat de la route de trace configurée sur la destination via le tunnel GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Surveillance de GlobalProtect à l'aide de PAN-OS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Les journaux GlobalProtect dans PAN-OS offrent une vue détaillée et en temps réel de la sécurité et de l'état opérationnel de votre environnement d'accès à distance. En enregistrant chaque étape du cycle de vie de la connexion GlobalProtect, ces journaux fournissent la visibilité nécessaire pour résoudre les problèmes opérationnels, auditer l'activité des utilisateurs et vérifier l'application des politiques de sécurité. Ce chapitre explique comment accéder et interpréter les journaux GlobalProtect directement via l'interface web de PAN-OS.

Vous pouvez utiliser les journaux GlobalProtect pour :

- **Le dépannage** : Identifier et résoudre les problèmes de connexion ou de performance des utilisateurs.
- **L'audit des utilisateurs** : Suivre l'activité des utilisateurs pour les examens de sécurité et la vérification de la conformité.
- **L'application des politiques** : Confirmer que les politiques de sécurité sont correctement appliquées au trafic à distance.

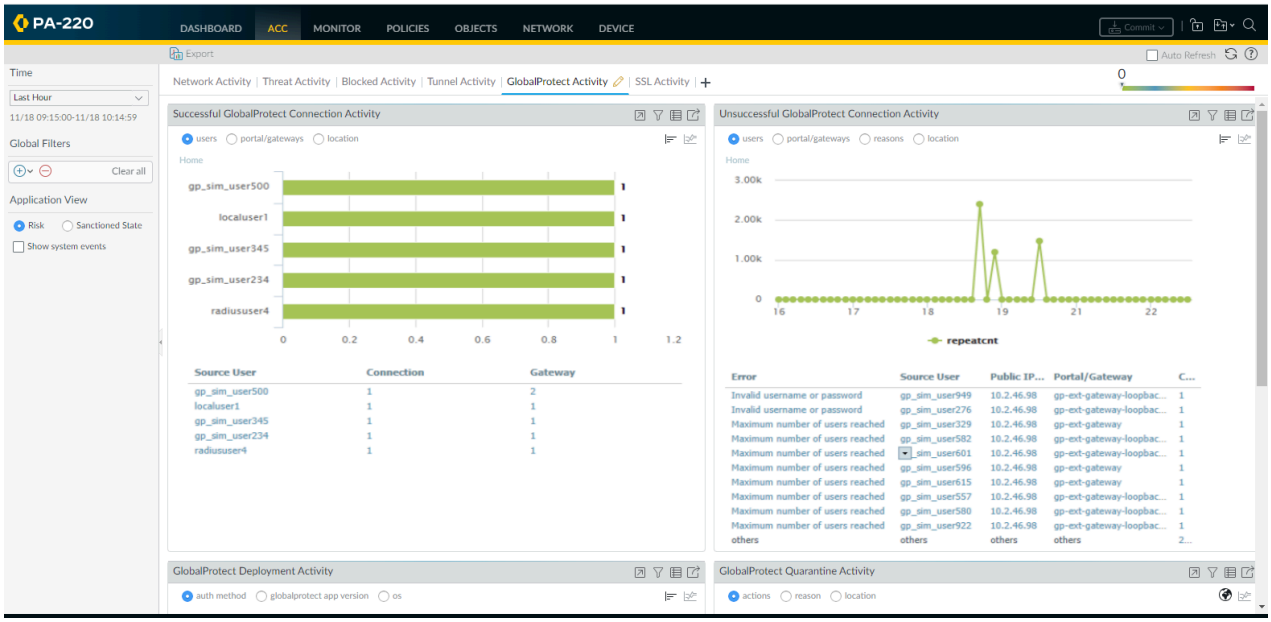
Ces fonctionnalités sont disponibles pour tout pare-feu de nouvelle génération Palo Alto Networks déployé en tant que passerelle ou portail GlobalProtect.

Afficher un affichage graphique de l'activité des utilisateurs de GlobalProtect dans PAN-OS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Application Command Center (Centre de commande des applications - ACC) dans PAN-OS affiche une vue graphique de l'activité des utilisateurs dans votre déploiement GlobalProtect sur l'onglet Activité GlobalProtect.

 ©2026 Palo Alto Networks, Inc.



Les graphiques et diagrammes d'activité GlobalProtect sont interactifs et prennent en charge une fonctionnalité d'exploration similaire à d'autres graphiques et diagrammes de l'ACC.

1. Dans PAN-OS, sélectionnez **ACC** > **GlobalProtect Activity (Activité GlobalProtect)**.

2. Affichez les graphiques comme suit :

   - **Successful GlobalProtect Connection Activity (Réussite de l'activité de connexion à GlobalProtect)** : affiche un tableau des activités de connexion GlobalProtect sur la période de temps sélectionnée. Utilisez la touche à bascule qui se trouve au haut du tableau pour faire basculer les statistiques de connexion selon les utilisateurs, les portails et les passerelles et l'emplacement.
   - **Unsuccessful GlobalProtect Connection Activity (Échec de l'activité de connexion à GlobalProtect)** : affiche un tableau des activités de connexion GlobalProtect sur la période de temps sélectionnée. Utilisez la touche à bascule qui se trouve au haut du tableau

 ©2026 Palo Alto Networks, Inc.

pour faire basculer les statistiques de connexion selon les utilisateurs, les portails et les passerelles et l'emplacement. Pour vous aider à identifier et à résoudre les problèmes de connexion, vous pouvez également afficher le tableau ou le graphique des motifs. Pour ce tableau, l'ACC indique l'erreur, l'utilisateur source, l'adresse IP publique et les autres informations qui vous aident à identifier et à résoudre le problème rapidement.

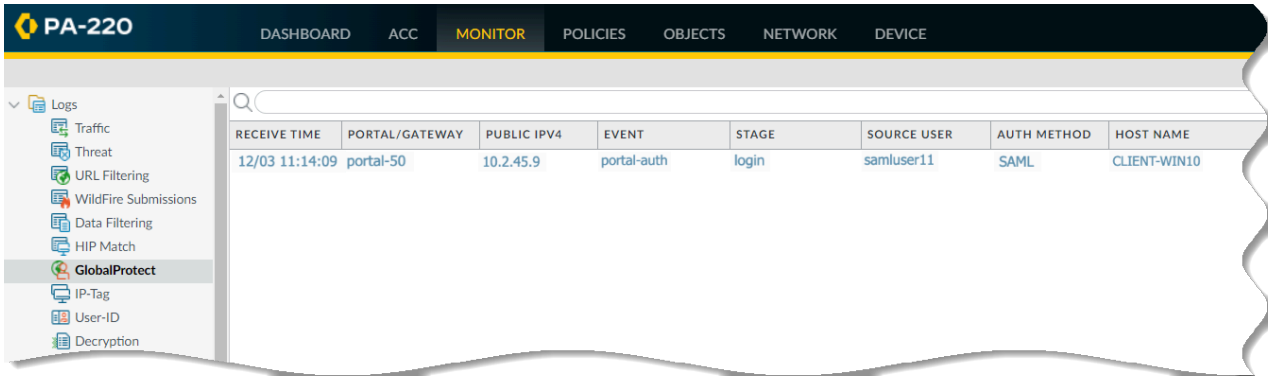
- **GlobalProtect Deployment Activity (Activité de déploiement GlobalProtect)** : résumé de l'affichage graphique de votre déploiement. Utilisez la touche à bascule au haut du tableau pour consulter la distribution des utilisateurs par méthode d'authentification, la version de l'application GlobalProtect et la version du système d'exploitation.

Afficher tous les journaux GlobalProtect sur une page dédiée dans PAN-OS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

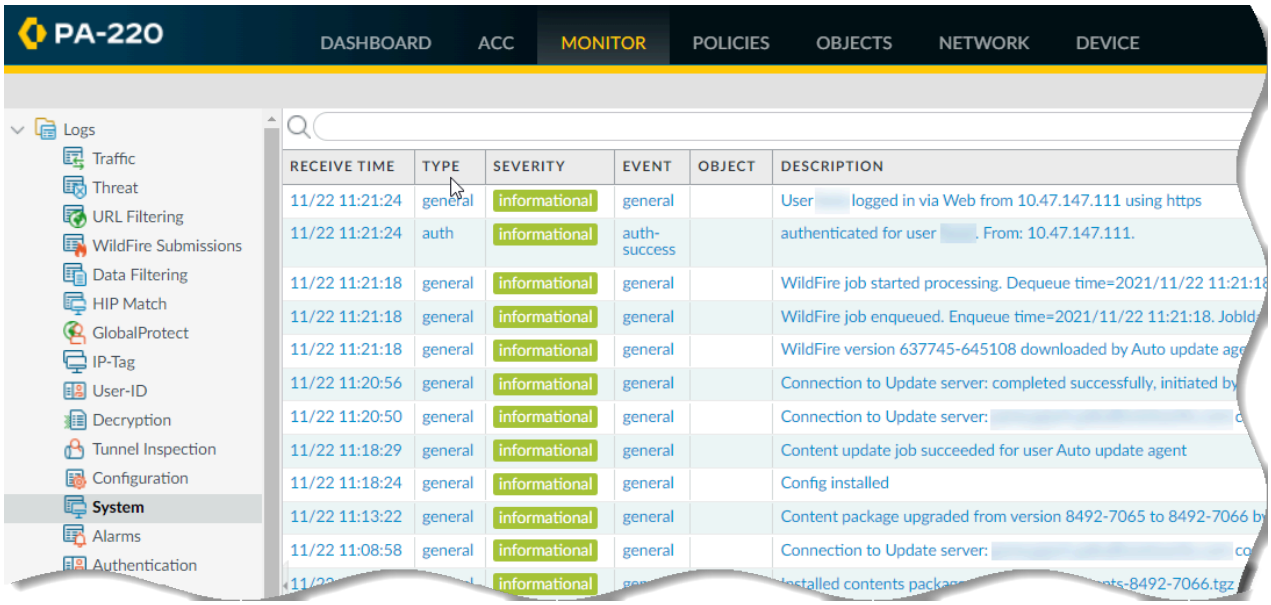
Dans PAN-OS, les journaux GlobalProtect ont une page dédiée qui vous permet de consulter les événements GlobalProtect en un seul endroit. La catégorie de journal dédiée à GlobalProtect élimine le besoin d'utiliser des requêtes de journal complexes pour localiser les journaux GlobalProtect. Vous pouvez également trier, filtrer et interroger les journaux GlobalProtect.

La page des journaux GlobalProtect affiche des informations qui incluent la méthode d'authentification. La capture d'écran suivante montre un exemple de journaux dans la page **Monitor (Surveiller)** > **Logs (Journaux)** > **GlobalProtect** ; notez la **Auth Method (Méthode d'authentification)** de **SAML**.



Cependant, les journaux d'événements d'authentification GlobalProtect restent dans **Monitor (Surveiller)** > **Logs (Journaux)** > **System (Système)**.

 ©2026 Palo Alto Networks, Inc.



1. Dans PAN-OS, sélectionnez **Monitor (Surveiller)** > **Logs (Journaux)**.
2. Afficher les journaux suivants :
   - LSVPN/SATELLITE événements
   - Journaux du portail et passerelles GlobalProtect
   - Journaux du VPN sans client
   - Journaux système liés à GlobalProtect.

Descriptions des événements pour les journaux GlobalProtect dans PAN-OS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Utilisez les descriptions suivantes pour vous aider à identifier les événements du portail GlobalProtect, de la passerelle ou du VPN sans client lors de la consultation des journaux GlobalProtect dans PAN-OS à **Monitor (Surveiller)** > **Logs (Journaux)** > **GlobalProtect** :

- Détails des événements du portail
- Détails des événements de la passerelle
- Détails de l'événement VPN sans client

©2026 Palo Alto Networks, Inc.

Détails des événements du portail

Le tableau suivant décrit les événements de journal liés au portail GlobalProtect.

Événement	Description
portal-auth	Indique une étape d'authentification du portail GlobalProtect. Affichez l'état pour les résultats.
portal-gen-cookie	Indique un événement de génération de cookie de remplacement d'authentification du portail GlobalProtect. Affichez l'état pour les résultats.
portal-getconfig	Indique un événement du portail GlobalProtect pour générer la configuration du client GlobalProtect, comme la configuration d'application dynamique ou la liste des passerelles.
portal-prelogin	Indique un événement de pré-connexion du portail GlobalProtect. Dans le cadre de l'événement, le client GlobalProtect effectue les actions suivantes : • Certificat : valide si un certificat client est valide. • SAML : génère une demande SAML et l'envoie à un client GlobalProtect. • Kerbero : déclenche un processus d'authentification Kerberos.

Détails des événements de la passerelle

Le tableau suivant décrit les événements de journal liés à la passerelle GlobalProtect.

Événement	Description
gateway-agent-msg	Indique un événement de passerelle GlobalProtect pour un message reçu du client GlobalProtect, tel que le message de raison de désactivation du client GlobalProtect.
gateway-auth	Indique l'étapde d'authentification de la passerelle GlobalProtect. Affichez l'état pour les résultats.
gateway-config-release	Indique un événement de passerelle GlobalProtect pour la publication de configuration, tel que la suppression de l'ip

 ©2026 Palo Alto Networks, Inc.

Événement	Description
	de mappage d'utilisateur ou la suppression du tunnel.
gateway-connected	Indique un événement de passerelle GlobalProtect pour une connexion réussie du client GlobalProtect en mode tunnel ou non-tunnel.
gateway-framed-ip	Indique un événement de passerelle GlobalProtect où la passerelle a récupéré une adresse IPv4 encadrée de RADIUS pour un client GlobalProtect.
gateway-getconfig	Indique un événement de passerelle GlobalProtect pour générer la configuration du client GlobalProtect, telle que la segmentation de tunnel, l'IP virtuelle ou les informations sur le tunnel.
gateway-hip-check	Indique un événement de passerelle GlobalProtect pour confirmer si un rapport HIP GlobalProtect a été mis à jour ou non, et pour rafraîchir l'ip de mappage d'utilisateur. Référez-vous à la description pour les informations sur la latence signalée. Les exemples incluent des éléments tels que le rapport HIP n'est pas nécessaire ou le rapport HIP est nécessaire.
gateway-hip-report	Indique un événement de passerelle GlobalProtect pour confirmer si un rapport HIP a été reçu d'un client GlobalProtect, pour mettre à jour l'ip de mappage d'utilisateur, et pour appliquer la politique HIP.
gateway-inheritance	Indique un événement de passerelle GlobalProtect dans lequel une passerelle GlobalProtect utilise une adresse IP dynamique et où l'adresse IP a changé.
gateway-logout	Indique un événement de passerelle GlobalProtect pour une déconnexion du client GlobalProtect.
gateway-prelogin	Indique un événement de passerelle GlobalProtect. Dans le cadre de l'événement, le client GlobalProtect effectue les actions suivantes :

 ©2026 Palo Alto Networks, Inc.

Événement	Description
	• Certificat : valide si un certificat client est valide. • SAML : génère une demande SAML et l'envoie à un client GlobalProtect. • Kerbero : déclenche un processus d'authentification Kerberos.
gateway-register	Indique que des informations utilisateur du client GlobalProtect, comme le nom d'utilisateur, le nom de domaine, le nom de l'ordinateur, l'identifiant de l'hôte, le numéro de série, l'IP publique ou l'heure de connexion, sont ajoutées sur la passerelle.
gateway-setup-ipsec	Indique un événement de passerelle GlobalProtect pour la configuration d'un tunnel VPN IPSec.
gateway-setup-ssl	Indique un événement de passerelle GlobalProtect pour la configuration d'un tunnel VPN SSL.
gateway-switch-to-ssl	Indique un changement de tunnel de passerelle GlobalProtect de l'IPSec vers le SSL, considérant que le tunnel IPSec a échoué.
gateway-tunnel-latency	Indique la latence de la passerelle GlobalProtect fournie par un client GlobalProtect. Référez-vous à la description pour les informations sur la latence signalée, telles que la latence pré-tunnel : 10 ms ou latence post-tunnel : 1 ms
quarantine-add	Indique un événement de passerelle GlobalProtect pour un client GlobalProtect, confirmant que le client est ajouté à la liste de quarantaine.
quarantine-delete	Indique un événement de passerelle GlobalProtect pour un client GlobalProtect, confirmant que le client est retiré de la liste de quarantaine.

Détails de l'événement VPN sans client

Le tableau suivant décrit les événements de journal liés au VPN sans client GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Événement	Description
clientlessvpn-login	Indique un événement de portail GlobalProtect pour la connexion VPN sans client GlobalProtect.
clientlessvpn-logout	Indique un événement de portail GlobalProtect pour la déconnexion VPN sans client GlobalProtect.
clientlessvpn-prelogin	Indique un événement de portail GlobalProtect pour le VPN sans client GlobalProtect. Dans le cadre de l'événement, les éléments suivants se produisent : • Certificat : valider si un certificat client est valide. • SAML : générer une demande SAML et l'envoyer à un client GlobalProtect. • Kerbero : déclencher un processus d'authentification Kerberos.

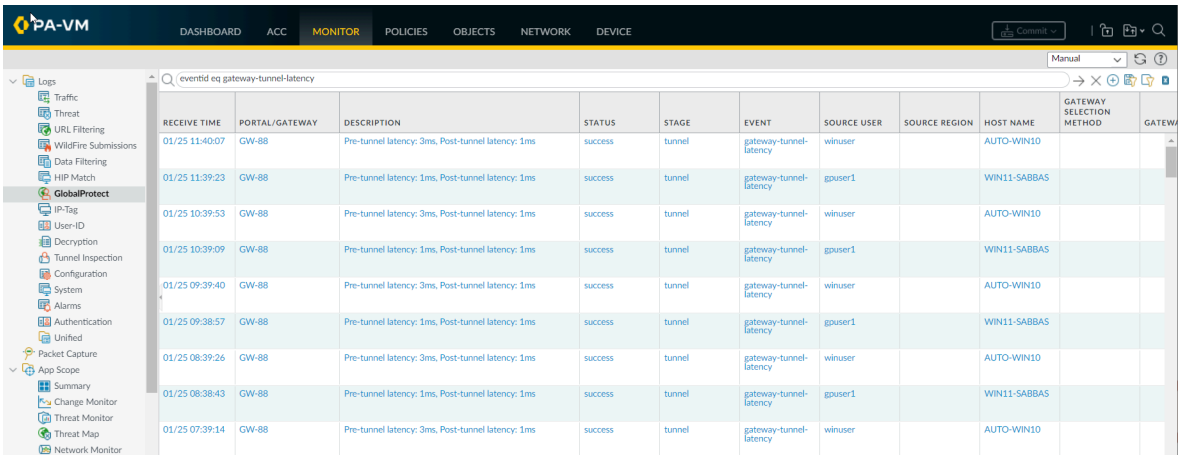
Filtrer les journaux GlobalProtect pour la latence de la passerelle dans PAN-OS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Pour vous aider à résoudre les problèmes de connexion et de performance pour un utilisateur spécifique, GlobalProtect collecte et rapporte des informations de télémétrie sur la latence entre la passerelle GlobalProtect et le terminal. Avec ces informations, vous pouvez identifier la passerelle à laquelle l'utilisateur est connecté, l'étape actuelle de la connexion et des statistiques sur la latence réseau avant et après le tunnel.

- Les mesures de latence avant le tunnel sont basées sur l'établissement de connexion OpenSSL. Le temps est mesuré depuis le SYN initial jusqu'à ce que l'établissement de la connexion en trois étapes TCP soit terminée.
- Les mesures de latence après le tunnel sont prises après l'établissement du tunnel. Le temps est mesuré pour le temps de trajet aller-retour (RTT) d'un seul maintien de tunnel à partir d'une sonde ICMP. Le temps après le tunnel est souvent plus rapide, car il mesure uniquement le maintien et non l'ensemble de l'établissement de la connexion TCP.

 ©2026 Palo Alto Networks, Inc.



1. Dans PAN-OS, sélectionnez **Monita (Surveiller)** > **Logs (Journaux)** > **GlobalProtect**.
2. Filtrez pour **`eventid eq gateway-tunnel-latency`** dans les journaux GlobalProtect.

Restreindre l'accès aux journaux GlobalProtect dans PAN-OS

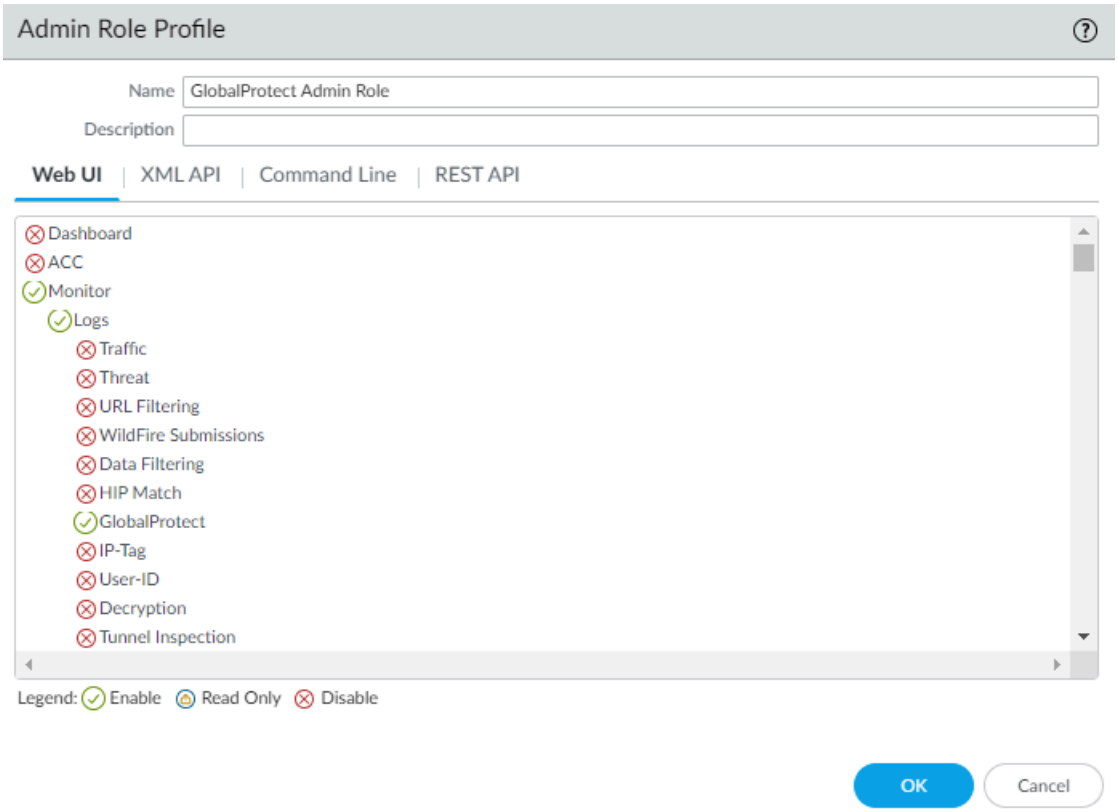
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Si l'accès aux journaux et aux données GlobalProtect est une préoccupation (comme pour la conformité réglementaire ou les préoccupations de confidentialité des données), vous pouvez restreindre l'accès à ces journaux dans PAN-OS.

1. Dans PAN-OS, créez un profil de rôle admin.
2. Spécifiez le rôle **admin GlobalProtect**.

 ©2026 Palo Alto Networks, Inc.

3. Sélectionnez **Monitor (Surveiller)**, **Logs (Journaux)** et **GlobalProtect** pour activer, désactiver ou fournir un accès en lecture seule aux journaux GlobalProtect.



Transférer les journaux GlobalProtect vers un service externe dans PAN-OS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

Dans PAN-OS, vous pouvez transférer les journaux GlobalProtect vers un service externe tel qu'un récepteur syslog ou un système de billets. Dans les situations où certaines équipes de votre entreprise peuvent être plus efficaces en surveillant uniquement les journaux GlobalProtect qui concernent leurs activités, vous pouvez créer des filtres de transfert en fonction des attributs des journaux GlobalProtect. Par exemple, vous pouvez filtrer par :

- Événements d'authentification GlobalProtect générés par GlobalProtect (type eq globalprotect)

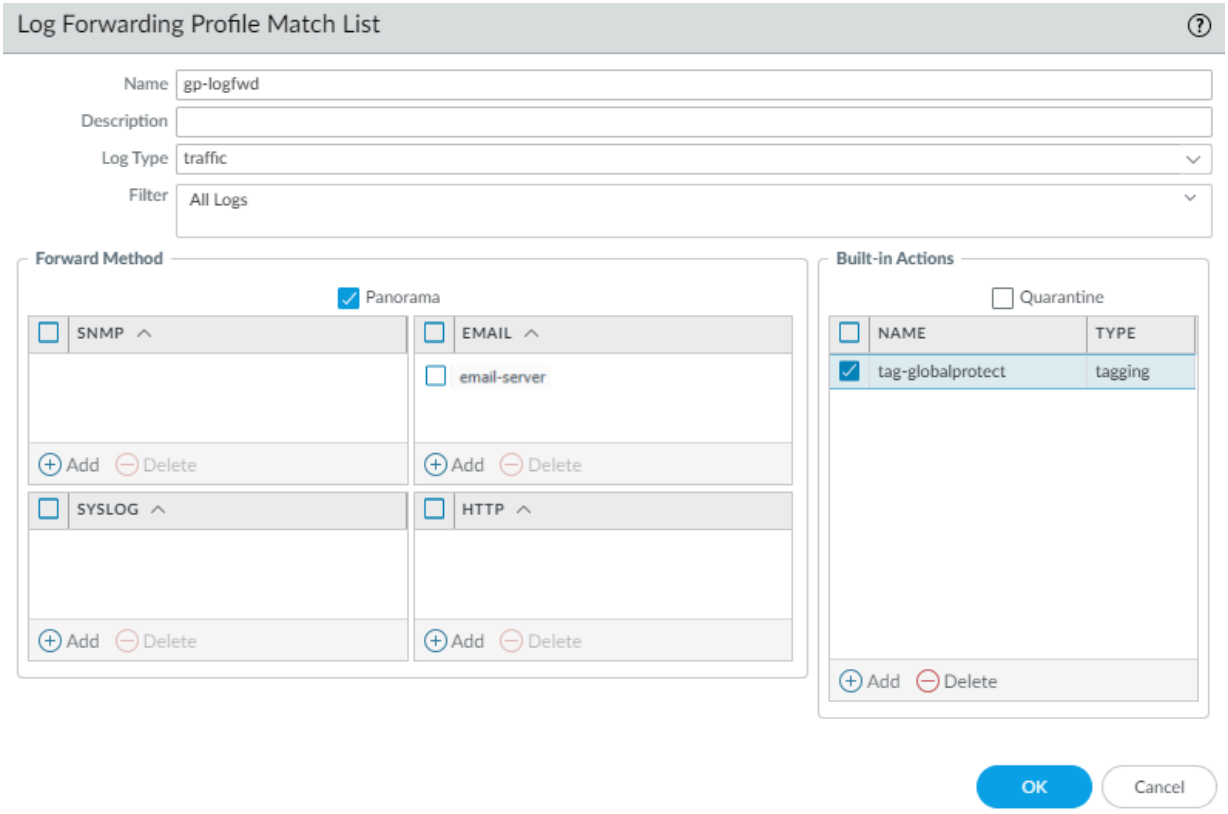
  Les événements d'authentification GlobalProtect générés par le service d'authentification (type eq auth) restent dans **Monitor (Surveiller)** > **Logs (Journaux)** > **System (Système)**.
- Tous les autres événements GlobalProtect (non-authentification)

Les pare-feu Palo Alto Networks transfèrent les journaux GlobalProtect en utilisant le format suivant. Pour simplifier l'analyse, le délimiteur est une virgule ; chaque champ est une chaîne Comma-Separated Valeur (Valeur séparée par une virgule ; CSV).

 ©2026 Palo Alto Networks, Inc.

Format : domain, receive_time, serial, seqno, actionflags, type, subtype, config_ver, time_generated, vsys, eventid, stage, auth_method, tunnel_type, srcuser, srcregion, machinename, public_ip, public_ipv6, private_ip, private_ipv6, hostid, serialnumber, client_ver, client_os, client_os_ver, repeatcnt, reason, error, opaque, status, location, login_duration, connect_method, error_code, portal

1. Dans PAN-OS, configurer le transfert de journaux pour les journaux GlobalProtect.
2. Configurez un profil de serveur pour chaque service externe qui recevra des informations des journaux.
3. Configurez les destinations pour les journaux GlobalProtect.



Vous pouvez également ajouter ou supprimer des balises d'une adresse IP source ou destination dans une entrée de journal.

4. Validez et vérifiez vos modifications.

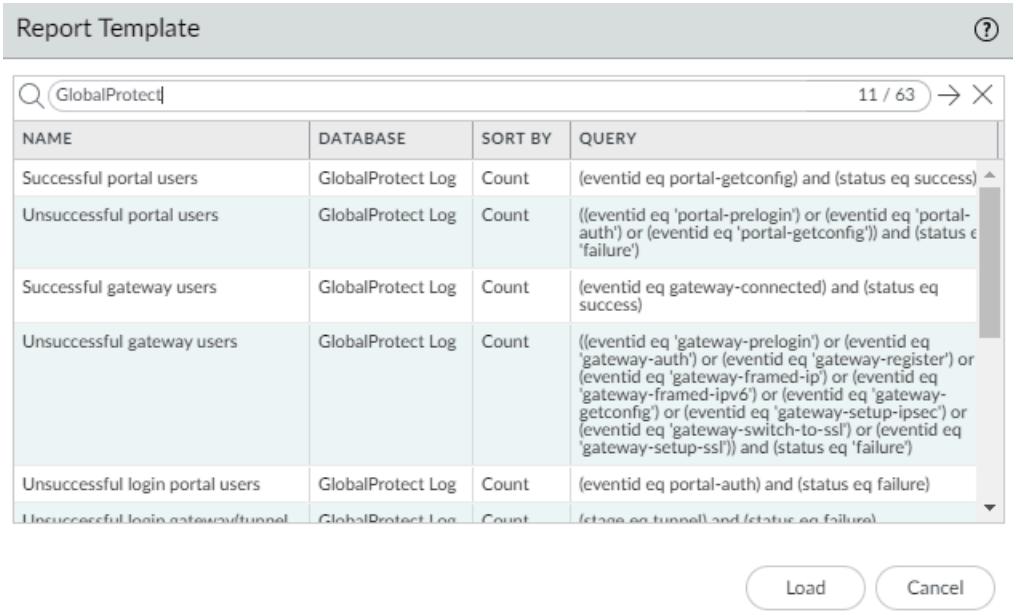
Configuration de rapports personnalisés pour GlobalProtect dans PAN-OS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect

 ©2026 Palo Alto Networks, Inc.

Vous pouvez configurer des rapports personnalisés que le pare-feu génère immédiatement (à la demande) ou selon la planification (chaque nuit).

1. Dans PAN-OS, générez un rapport personnalisé pour GlobalProtect.
2. Sélectionnez **Monitor (Surveiller)** > **Manage Custom Reports (Gérer les rapports personnalisés)**.
3. Cliquez sur **Add (Ajouter)**, puis saisissez un **Name (Nom)** pour le rapport.
4. Pour qu'un rapport se base sur un modèle prédéfini, cliquez sur **Load Template (Charger un modèle)** et sélectionnez un modèle. Vous pouvez ensuite modifier le modèle et l'enregistrer sous un rapport personnalisé.



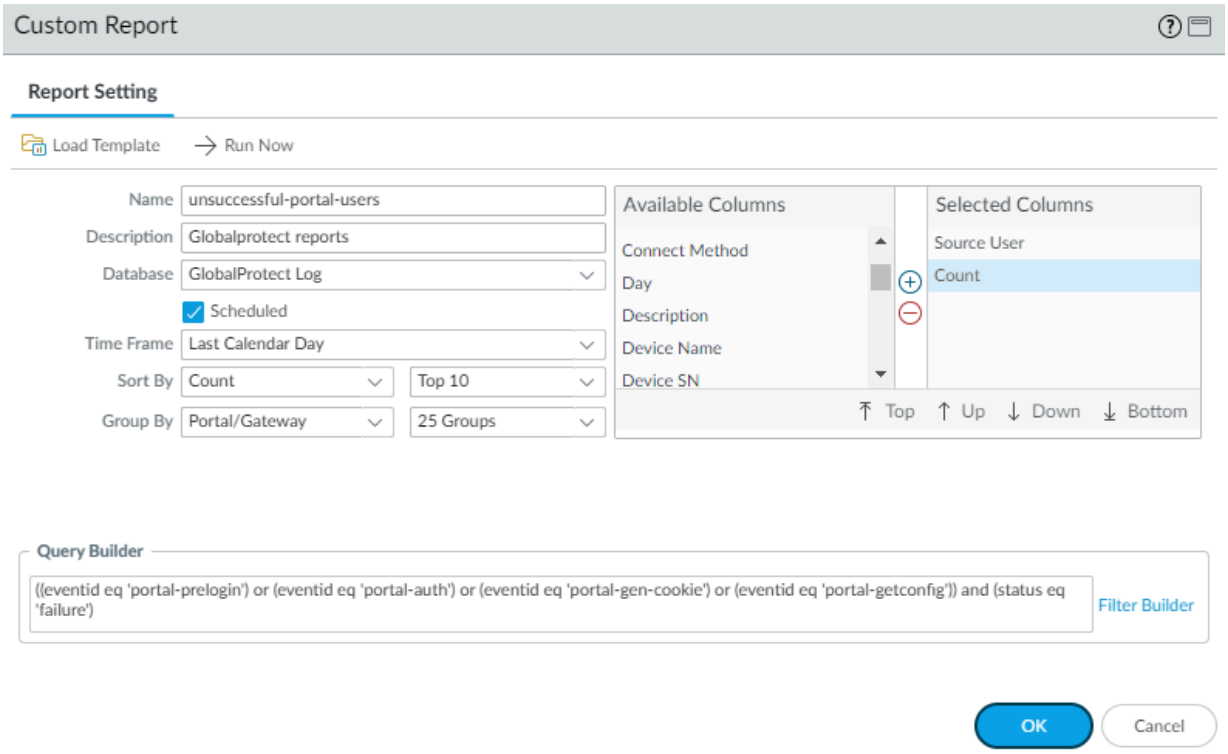
5. Si vous choisissez de créer le rapport à partir de zéro, sélectionnez la base de données que vous souhaitez utiliser pour le rapport comme **Device GlobalProtect Log (Journal GlobalProtect du périphérique)**.
6. Cochez la case **Scheduled (Planifié)** pour exécuter le rapport de nuit. Le rapport peut alors être affiché dans la colonne **Reports (Rapports)** située sur le côté.
7. Définissez les critères de filtrage. Sélectionnez le **Time Frame (Calendrier)**, l'ordre **Sort By (Trier par)**, **la préférence Group By (Regrouper par)**, puis sélectionnez les colonnes qui doivent s'afficher dans le rapport.
8. (Facultatif) Sélectionnez les attributs **Query Builder (Générateur de requêtes)**, si vous souhaitez encore affiner les critères de sélection. Pour générer une requête de rapport, indiquez les options suivantes et cliquez sur **Add (Ajouter)**. Répétez ces différentes étapes, le cas échéant, pour formuler une requête complète.
   - **Connector (Connecteur)** : sélectionnez le connecteur (et/ou) devant précéder l'expression que vous ajoutez.

 ©2026 Palo Alto Networks, Inc.

- **Negate (Refuser)** : cochez cette case pour interpréter la requête en tant que refus. Si, par exemple, vous avez choisi de mettre en correspondance les entrées des 24 dernières heures et/ou provenant de la zone non approuvée, l'option de refus renvoie des entrées en dehors des 24 dernières heures et/ou ne provenant pas de la zone non approuvée.
- **Attribute (Attribut)** : sélectionnez un élément de donnée. Les options disponibles dépendent du choix de base de données.
- **Operator (Opérateur)** : sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les options disponibles dépendent du choix de base de données.
- **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre.

Par exemple, pour créer un rapport pour les utilisateurs du portail GlobalProtect qui ont échoué à se connecter, utilisez une requête similaire à la suivante :

```
((eventid eq 'portal-prelogin') or (eventid eq 'portal-auth') ou
(eventid eq 'portal-gen-cookie') ou (eventid eq 'portal-getconfig'))
et (status eq 'failure')
```



9. Pour tester les paramètres de rapport, sélectionnez **Run Now (Lancer l'exécution)**. Modifiez les paramètres si nécessaire pour modifier les informations qui figurent dans le rapport.

10. Cliquez sur **OK** pour enregistrer le rapport personnalisé.

©2026 Palo Alto Networks, Inc.

Exigences de GlobalProtect pour les périphériques IoT

Où puis-je l'utiliser ?	De quoi ai-je besoin ?

• NGFW (géré par Panorama ou Strata Cloud Manager)
• Prisma Access (géré par Panorama ou Strata Cloud Manager)
• L'un des systèmes d'exploitation suivants :
  • Android
  • Raspbian
  • Ubuntu
  • Windows 10 IoT Entreprise
	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile
	PAN-OS 10.1 ou version ultérieure

GlobalProtect pour l'IoT vous permet de sécuriser le trafic qui provient de vos périphériques IoT en appliquant à ces derniers vos politiques de sécurité. Une fois que vous avez configuré GlobalProtect pour l'IoT, l'application GlobalProtect s'authentifie auprès du portail ou des passerelles GlobalProtect au moyen de certificats client et, éventuellement, d'un nom d'utilisateur et d'un mot de passe. Une fois l'authentification réussie, l'application GlobalProtect établit un tunnel IPSEC. En cas d'échec d'une connexion IPSec, vous pouvez configurer l'application GlobalProtect pour qu'elle bascule vers un tunnel SSL. Reportez-vous à la grille de compatibilité Palo Alto Networks pour obtenir une liste des fonctionnalités prises en charge par système d'exploitation pour les périphériques IoT.

Les exigences du système IdO sont les suivantes :

- 128 Mo de RAM
- 4 Go de stockage
- x86 et processeur ARMv7 ou ARMv5
- Installation utilisant des packages d'application snap à partir de la CLI ou de WebDM

Configuration des portails et des passerelles GlobalProtect pour les périphériques IoT

Où puis-je l'utiliser ?	De quoi ai-je besoin ?

• NGFW (géré par Panorama ou Strata Cloud Manager)
• Prisma Access (géré par Panorama ou Strata Cloud Manager)
• L'un des systèmes d'exploitation suivants :
  • Android
  • Raspbian
  • Ubuntu
  • Windows 10 IoT Entreprise
	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

1. Configurez les passerelles GlobalProtect pour qu'elles prennent en charge l'application GlobalProtect pour l'IdO.
   1. Effectuez les tâches préalables à la configuration de la passerelle GlobalProtect.

      Obligatoire uniquement sur NGFW (géré par Panorama ou Strata Cloud Manager)Créez les interfaces (et zones) pour le pare-feu sur lequel vous prévoyez de configurer chaque passerelle. Pour les passerelles qui exigent des connexions en tunnel, vous devez configurer à la fois l'interface physique et l'interface virtuelle de tunnel. Voir Créer des interfaces et des zones pour GlobalProtect

      Configuration des certificats de serveur de passerelle et du profil de service SSL/TLS requis pour que l'application GlobalProtect puisse établir une connexion SSL avec la passerelle. Voir Activer SSL entre les composants GlobalProtect.

      Définition des profils d'authentification et/ou des profils de certificat qui seront utilisés pour authentifier les utilisateurs GlobalProtect. Reportez-vous à la section Authentification de l'utilisateur GlobalProtect.
   2. Installez un abonnement à GlobalProtect pour chaque passerelle qui prend en charge l'application GlobalProtect pour IoT. Si vous utilisez Prisma Access, l'abonnement à GlobalProtect n'est pas nécessaire.
   3. Personnalisez la configuration de la passerelle pour vos périphériques IoT :

      Lorsque vous configurez une passerelle, vous pouvez spécifier les paramètres d'authentification du client qui s'appliquent spécialement à l'IoT. Par exemple, vous

 ©2026 Palo Alto Networks, Inc.

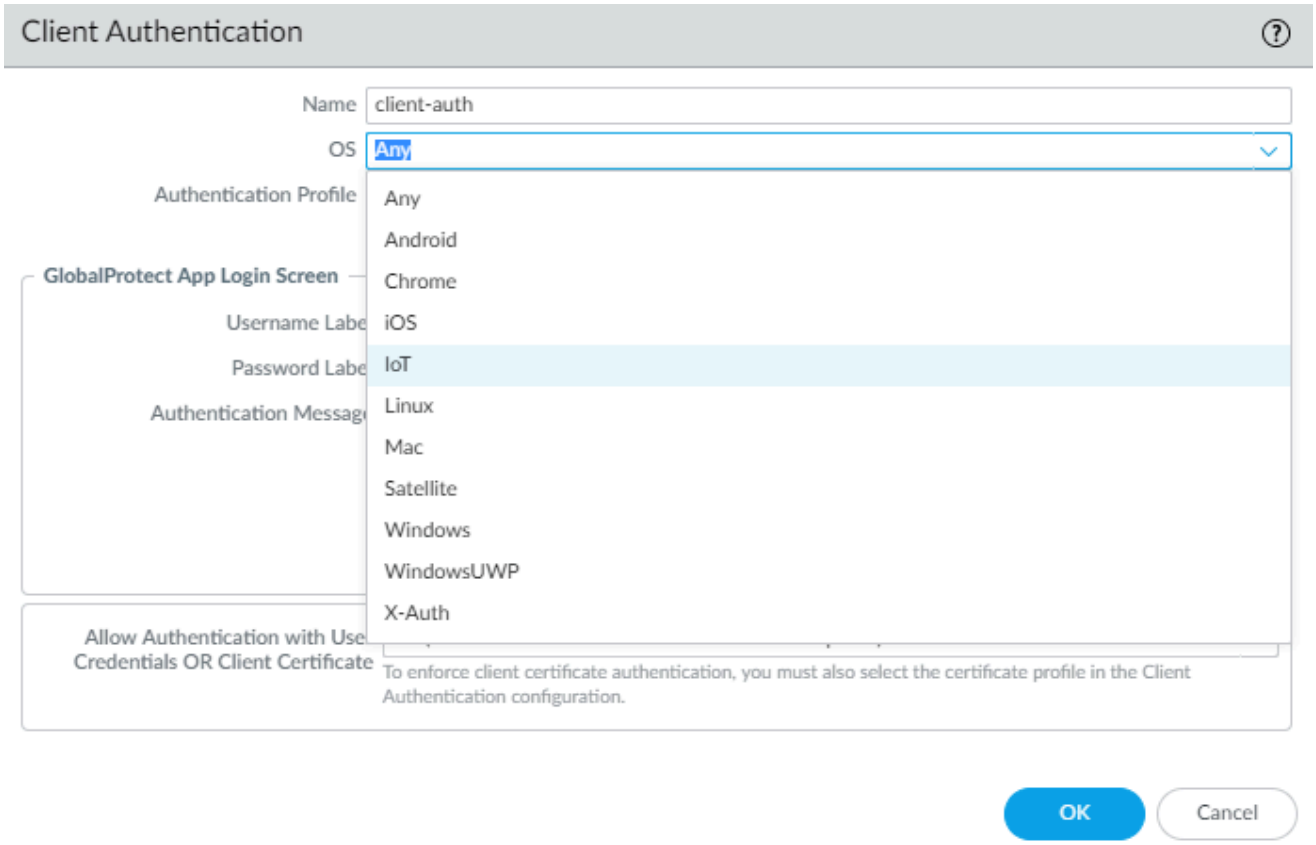
pouvez configurer l'utilisation à deux facteurs sur les terminaux Windows et macOS et l'authentification basée sur des certificats pour les périphériques IoT.

Vous pouvez également configurer les paramètres réseau et client pris en charge (comme les pools d'adresses IP, les itinéraires d'accès et la séparation des tunnels) pour les périphériques IoT.

1. Effectuez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**, puis sélectionnez ou **Add (Ajouter)** une configuration de passerelle.
   - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)Device Settings (Paramètres du périphérique)** > **GlobalProtect**, puis sélectionnez ou **Add (Ajouter)** une configuration de passerelle.
2. Ajoutez une configuration d'authentification du client pour les périphériques IoT :
   1. Sélectionnez **Authentification** et **Ajoutez** une nouvelle configuration d'authentification du client.
   2. Donnez un **Nom** à la configuration, définissez le **système d'exploitation** sur **IoT**, spécifiez le **Profil d'authentification** à utiliser pour l'authentification des utilisateurs

 ©2026 Palo Alto Networks, Inc.

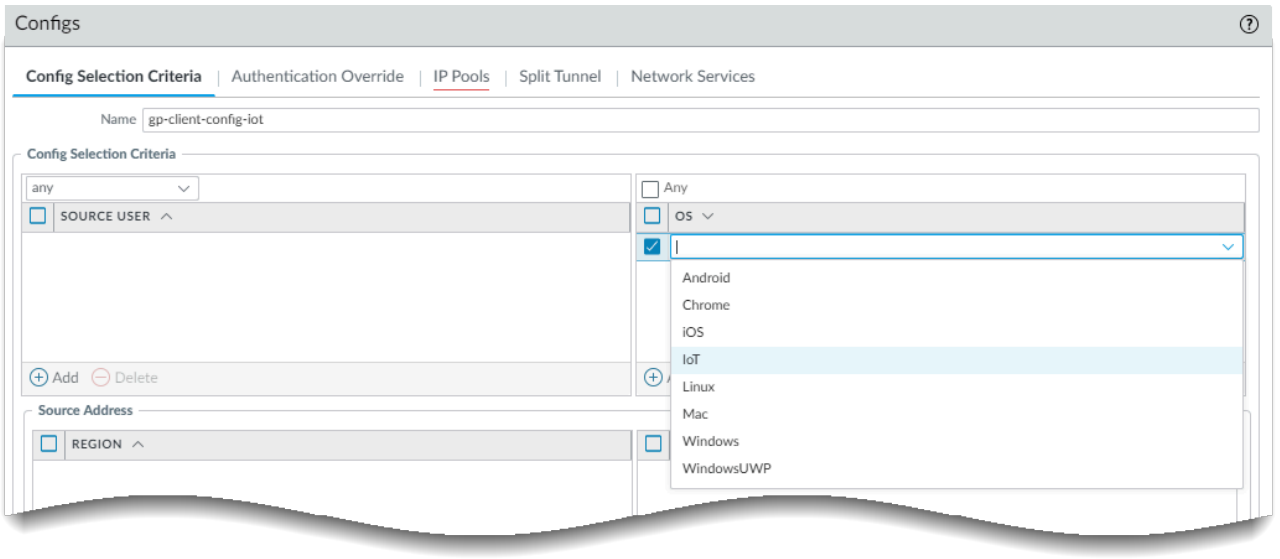
sur cette passerelle. Choisissez un profil qui permet l'authentification du certificat client.



3. Cliquez sur **OK**.

3. Pour configurer des paramètres client précis qui s'appliquent uniquement aux terminaux IoT, configurez une nouvelle configuration de paramètres client :
   1. Sélectionnez **Agent**, puis **Ajoutez** une nouvelle configuration de paramètres client.
   2. Configurez les paramètres d'authentification du client comme désiré,
   3. Sélectionnez **Utilisateur/Groupe d'utilisateurs**, puis **Ajoutez** un système d'exploitation et sélectionnez **IoT**.

©2026 Palo Alto Networks, Inc.



4. Cliquez sur **OK**.
4. Cliquez sur **OK**.
5. **Commit (Validez)** la configuration.

2. Configurez le portail pour qu'il prenne en charge l'application GlobalProtect pour les périphériques IoT.

Pour prendre en charge les périphériques IoT, vous devez configurer au moins une passerelle à laquelle l'application GlobalProtect peut se connecter et configurer les paramètres du portail et de l'application. Le portail envoie les informations de configuration et les informations sur les passerelles disponibles à l'application. Après avoir reçu la configuration du portail GlobalProtect, l'application découvre les passerelles qui sont répertoriées dans la configuration du client et sélectionne la passerelle qui convient le mieux. Utilisez le workflow suivant pour configurer le portail GlobalProtect pour qu'il prenne en charge l'application GlobalProtect pour les périphériques IoT.

1. Si vous ne l'avez pas encore fait, effectuez les tâches préalables à la configuration du portail GlobalProtect.

   Obligatoire uniquement sur NGFW (géré par Panorama ou Strata Cloud Manager)

   Création des interfaces (et des zones) pour le pare-feu sur laquelle vous envisagez de configurer le portail. Voir Créer des interfaces et des zones pour GlobalProtect

   Configuration du certificat de serveur du portail, du certificat de serveur de passerelle, des profils de service SSL/TLS et, facultativement, de certains certificats clients à déployer pour les utilisateurs finaux afin d'activer les connexions SSL/TLS mutuelles avec les services GlobalProtect™ Voir Activer SSL entre les composants GlobalProtect.

   Définition des profils d'authentification facultatifs et des profils de certificats que le portail peut utiliser pour authentifier les utilisateurs GlobalProtect. Reportez-vous à la section Authentification de l'utilisateur GlobalProtect.

   Configurer une passerelle GlobalProtect et comprendre Priorité de passerelle dans une configuration de passerelle multiple.

 ©2026 Palo Alto Networks, Inc.

2. Définissez les paramètres du client pour que les périphériques IoT s'authentifient auprès du portail.
   1. Effectuez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**, puis sélectionnez ou **Add (Ajouter)** une configuration de passerelle.
      - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)Device Settings (Paramètres du périphérique)** > **GlobalProtect**, puis sélectionnez ou **Add (Ajouter)** une configuration de portail.
   2. Configurez les paramètres d'authentification du client qui s'appliquent aux périphériques IoT lorsque les utilisateurs accèdent au portail :
      1. Sélectionnez **Authentification** et **Ajoutez** une nouvelle configuration d'authentification du client.
      2. Donnez un **Nom** à la configuration, définissez le **système d'exploitation** sur **IoT**, spécifiez le profil d'authentification à utiliser pour l'authentification des utilisateurs sur ce portail. Choisissez un profil qui permet l'authentification du certificat client.
3. Personnalisez une configuration d'agent pour les périphériques IoT.

   Le choix de modifier une configuration existante ou d'en créer une nouvelle dépend de votre environnement. Par exemple, si vous utilisez des passerelles propres au système d'exploitation ou que vous souhaitez collecter des informations sur l'hôte qui sont propres aux périphériques IoT, envisagez de créer une nouvelle configuration d'agent.

   Pour obtenir de plus amples renseignements sur les fonctionnalités prises en charge, reportez-vous à la grille de compatibilité Palo Alto Networks pour obtenir une liste des fonctionnalités prises en charge par système d'exploitation pour les périphériques IoT.

   1. Définissez les configurations de l'agent GlobalProtect :
   2. Sélectionnez **Agent**, puis sélectionnez une configuration d'agent de portail existante ou **Ajoutez**-en une nouvelle.
   3. Configurez les paramètres d'authentification du client applicables aux périphériques IoT.
   4. Sélectionnez **Utilisateur/Groupe d'utilisateurs**, puis Ajoutez un **Système d'exploitation** et sélectionnez **IoT**.
   5. Spécifiez les passerelles externes auxquelles les utilisateurs possédant cette configuration peuvent se connecter.
   6. (Facultatif) Sélectionnez **Application**, puis personnalisez les paramètres du portail qui s'appliquent à l'application GlobalProtect pour IoT L'application GlobalProtect rejette les paramètres qui ne s'appliquent pas à l'IoT. Reportez-vous à la grille de compatibilité Palo Alto Networks pour obtenir une liste des fonctionnalités prises en charge par système d'exploitation pour les périphériques IoT.
   7. Cliquez deux fois sur **OK**.
   8. **Commit (Validez)** la configuration.
4. Appliquez les politiques sur les périphériques IoT (**Objets** > **GlobalProtect** > **Objets HIP**).

   Vous pouvez désormais créer de nouveaux objets HIP au moyen des informations sur l'hôte qui sont propres aux périphériques IoT et les utiliser pour faire correspondre les

 ©2026 Palo Alto Networks, Inc.

conditions dans tous les profils HIP. Vous pouvez ensuite utiliser un profil HIP comme condition de correspondance dans une règle de politique pour appliquer la politique de sécurité correspondante.

1. Sélectionnez **Général** > **Informations sur l'hôte** > **Système d'exploitation**.
2. Sélectionnez **Contient** > **IoT**.
3. Cliquez sur **OK**.
4. Créez des objets HIP, au besoin.
5. Configurez la mise en œuvre des politiques basées sur HIP.

3. Installez et configurez l'application GlobalProtect pour IoT.

Utilisez les instructions fournies pour le système d'exploitation de votre périphérique IoT.

- Installation GlobalProtect pour IoT sur Android
- Installation GlobalProtect pour IoT sur Raspbian
- Installation GlobalProtect pour IoT sur Ubuntu
- Installation GlobalProtect pour IoT sur Windows

 ©2026 Palo Alto Networks, Inc.

Installation GlobalProtect pour IoT sur Android

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Système d'exploitation Android	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Pour utiliser GlobalProtect pour l'IoT sur des périphériques Android, vous devez intégrer la configuration de l'application et de GlobalProtect à l'image du système d'exploitation Android en une application système. Pour que GlobalProtect puisse fonctionner en mode sans tête, vous devez déployer un fichier de préconfiguration avec le package de l'application GlobalProtect.

1. Ajoutez GlobalProtect.apk en tant qu'application système préconstruite dans votre image de système d'exploitation Android.
   1. À partir du site de support, sélectionnez **Mises à jour** > **Mises à jour logicielles**, puis téléchargez le paquet GlobalProtect APK.
   2. Décodez le fichier APK dans le répertoire `android_src_tree_root/packages/app/`.

      Le décodeur décompresse l'application dans un dossier GlobalProtect.
   3. Dans le dossier GlobalProtect, créez le fichier `Android.mk`. Ce fichier définit les sources et les annuaires partagés que le décodeur utilisera pour bâtir le système.

      Modifiez le fichier afin qu'il inclut ce qui suit :

      ```
      LOCAL_PATH := $(call my-dir) include $(CLEAR_VARS)
       LOCAL_MODULE_TAGS := optional LOCAL_MODULE := GlobalProtect
       LOCAL_SRC_FILES := $(LOCAL_MODULE).apk LOCAL_MODULE_CLASS :=
       APPS LOCAL_MODULE_SUFFIX := $(COMMON_ANDROID_PACKAGE_SUFFIX)
       LOCAL_CERTIFICATE := PRESIGNED include $(BUILD_PREBUILT)
      ```
   4. Pour tout fichier MK supplémentaire sous `android_src_tree_root/vendor/`, ajoutez la ligne suivante :

      ```
      PRODUCT_PACKAGES += GlobalProtect
      ```
   5. Ajoutez libgpjni.so au dossier `/system/lib` ou `/system/lib64`, selon l'architecture du processeur prise en charge par le périphérique IoT. Le fichier libgpjni.so peut être extrait du répertoire lib après que le fichier GlobalProtect.apk a été décodé par ApkTool.

 ©2026 Palo Alto Networks, Inc.

2. Modifiez le code source du cadre d'applications Android afin de préautoriser la fenêtre de demande d'autorisation pour la connexion VPN.

Modifiez le fichier `android_src_tree_root/frameworks/base/services/core/java/com/android/server/connectivity/Vpn.java` pour qu'il comprennent le segment de code suivant :

```
private boolean isVpnUserPreConsented(String packageName) { if
 (“com.paloaltonetworks.globalprotect”.equals(packageName))
{ Log.v(TAG, "IoT, isVpnUserPreConsented always true");
 return true; } AppOpsManager appOps = (AppOpsManager)
 mContext.getSystemService(Context.APP_OPS_SERVICE); //
 Verify that the caller matches the given package
 and has permission to activate VPNs. return
 appOps.noteOpNoThrow(AppOpsManager.OP_ACTIVATE_VPN,Binder.getCallingUid(),
 packageName) == AppOpsManager.MODE_ALLOWED; } }
```

3. Personnalisez le comportement d'Android pour qu'il supprime l'icône de GlobalProtect dans la barre de notification d'Android 8.0 et les versions ultérieures.

Modifiez le fichier `android_src_tree_root/frameworks/base/services/core/java/com/android/server/connectivity/Vpn.java` pour qu'il comprennent le segment de code qui suit.

```
if ( r.packageName.equals("com.paloaltonetworks.globalprotect") )
 { Slog.d(TAG, "not to show the foreground service running
 notification for IoT"); } else { r.postNotification(); }
```

4. Configurez les paramètres VPN que vous souhaitez prédéployer sur les périphériques IdO Android.
   1. Créez un fichier de configuration (`globalprotect.conf`) au format suivant et modifiez l'adresse IP du portail GlobalProtect et les paramètres d'authentification, soit : nom d'utilisateur et mot de passe ou le chemin du certificat client (client-cert-path) et le fichier de la phrase secrète (client-cert-passphrase).

      Authentification basée sur le nom d'utilisateur et le mot de passe

      ```
      <?xml version="1.0" encoding="UTF-8"?> <GlobalProtect>
       <PanSetup> <Portal>192.168.1.23</Portal> </PanSetup>
       <Settings> <head-less>yes</head-less> <os-type>IoT</os-type>
       <username>user1</username> <password>mypassw0rd</password>
       <log-path-service>/home/gptest/Desktop/data/gps</log-path-
      service> <log-path-agent>/home/gptest/Desktop/data/gpadata</
      log-path-agent> </Settings> </GlobalProtect>
      ```

      Authentification basée sur le certificat client

      ```
      <?xml version="1.0" encoding="UTF-8"?> <GlobalProtect>
       <PanSetup> <Portal>192.168.1.23</Portal> </
      PanSetup> <Settings> <head-less>yes</head-less> <os-
      type>IoT</os-type> <client-cert-path>/home/gptest/
      ```

 ©2026 Palo Alto Networks, Inc.

```
Desktop/data/pan_client_cert.pfx</client-cert-path>
 <client-cert-passphrase>/home/gptest/Desktop/data/
pan_client_cert_passcode.dat</client-cert-passphrase>
 <username>user1</username> <password>paloalto</password>
 <log-path-service>/home/gptest/Desktop/data/gps</log-path-
service> <log-path-agent>/home/gptest/Desktop/data/gpadata</
log-path-agent> </Settings> </GlobalProtect>
```

2. Encodez le fichier `globalprotect.conf` au format Base64 et enregistrez-le dans le répertoire `android_src_tree_root/system/config/`.

   Si vous le souhaitez, vous pouvez enregistrer le fichier dans un autre emplacement. Vous devez cependant modifier l'emplacement de cette configuration dans le fichier `android_src_tree_root/assets/gp_conf_location.txt`.

5. Créez un fichier APK GlobalProtect.

6. Signez le fichier APK GlobalProtect.

7. Transmettez le nouveau système d'exploitation aux périphériques Android dans l'image système, puis transmettez le nouveau système d'exploitation aux périphériques Android.

 ©2026 Palo Alto Networks, Inc.

Installation GlobalProtect pour IoT sur Raspbian

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Système d'exploitation Raspbian	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Effectuez les étapes suivantes pour installer GlobalProtect pour IoT sur des périphériques Raspbian.

GlobalProtect pour IoT sur Raspbian et Ubuntu ne supporte uniquement une architecture basée sur ARM.

1. À partir du site de support, sélectionnez **Mises à jour** > **Mises à jour logicielles**, puis téléchargez le package GlobalProtect correspondant à votre système d'exploitation.
2. Installez l'application GlobalProtect pour IoT.

   À partir du périphérique IdO, utilisez la commande **`sudo dpkg -i GlobalProtect_deb_arm<version>.deb`** pour installer le logiciel.

   ```
   sudo dpkg -i GlobalProtect_deb_arm-5.1.0.0-84.deb
   ```

   *Pour désinstaller le logiciel, utilisez la commande **`sudo dpkg -P globalprotect`**.*
3. Configurez les paramètres VPN que vous souhaitez prédéployer sur les périphériques IoT Raspbian.
   1. Dans le chemin `client-cert`, importez le certificat au format pcks12 et enregistrez le fichier en y ajoutant l'extension .pfx (par exemple, **pan_client_cert.pfx**).
   2. Dans le chemin `passphrase du certificat client`, enregistrez le fichier du code secret en ajoutant l'extension .dat extension (par exemple, **pan_client_cert_passcode.dat**)
   3. Dans le chemin `log-path-service`, si vous n'utilisez pas le chemin par défaut pour PanGPS (par exemple, `/opt/paloaltonetworks/globalprotect`), assurez-vous que le dossier-chemin `log-setting (paramètre du journal)` a les mêmes privilèges que le dossier globalprotect, qui se trouve sous `opt/paloaltonetworks`.
   4. Créez le fichier de configuration prédéploiement (`/opt/paloaltonetworks/globalprotect/pangps.xml`) au format suivant et modifiez l'adresse IP du portail GlobalProtect et les paramètres d'authentification, soit : nom d'utilisateur et mot de passe ou le chemin du certificat client (**`client-cert-path`**) et le fichier de la phrase secrète (**`client-cert-passphrase`**). Vous pouvez également spécifier un dossier

 ©2026 Palo Alto Networks, Inc.

facultatif dans lequel stocker vos journaux de service GlobalProtect (**log-path-service**) et d'agent (**log-path-agent**).

```
<?xml version="1.0" encoding="UTF-8"?> <GlobalProtect> <PanSetup>
 <Portal>192.168.1.160</Portal> //adresse du portail pré-déployé
 </PanSetup> <PanGPS> </PanGPS> <Settings> <portal-timeout>5</
portal-timeout> <connect-timeout>5</connect-timeout> <receive-
timeout>30</receive-timeout> <os-type>IoT</os-type> //type de
 système d'exploitation pré-déployé pour l'IdO. Si cette balise
 n'est pas présente, GP détectera automatiquement le type de
 système d'exploitation. <head-less>oui</head-less> //mode sans
 tête pré-déployé <username>abc</username> //nom d'utilisateur
 pré-déployé optionnel <password>xyz</password> //mot de passe
 pré-déployé optionnel <client-cert-path>cli_cert_path</client-
cert-path> //chemin de certificat client pré-déployé optionnel(p12)
 <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase> //chemin de fichier de phrase de passe de certificat
 client pré-déployé optionnel <log-path-service>/tmp/gps</log-
path-service> //dossier journal pré-déployé optionnel pour PanGPS
 <log-path-agent>/tmp/gpa</log-path-agent> //dossier journal pré-
déployé optionnel pour PanGPA et GlobalProtect CLI </Settings> </
GlobalProtect>
```

4. Recommencez le processus GlobalProtect pour que la configuration de prédéploiement prenne effet.

5. Une fois que vous avez déployé le périphérique IoT, vous pouvez collecter les journaux selon vos besoins à l'aide de la commande **globalprotect collect-log**.

```
user@raspbianhost:~/Desktop/data$ globalprotect collect-
log Le fichier de support est enregistré dans /home/
gptest/.GlobalProtect/GlobalProtectLogs.tgz
```

6. (Facultatif) Si la méthode d'authentification est une combinaison nom d'utilisateur/mot de passe et certificat de client, assurez-vous que le **Nom commun** du certificat de client correspond au nom d'utilisateur.

 ©2026 Palo Alto Networks, Inc.

Installation GlobalProtect pour IoT sur Ubuntu

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager) • Système d'exploitation Ubuntu	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Effectuez les étapes suivantes pour installer GlobalProtect pour IoT sur des périphériques Ubuntu.

GlobalProtect pour IoT sur Raspbian et Ubuntu ne supporte uniquement une architecture basée sur ARM.

1. À partir du site de support, sélectionnez **Mises à jour** > **Mises à jour logicielles**, puis téléchargez le package GlobalProtect correspondant à votre système d'exploitation.
2. Installez l'application GlobalProtect pour IoT.

   À partir du périphérique IdO, utilisez la commande **ARM** pour installer le logiciel.

   ```
   $ ./gp_install.sh --help Usage: $ sudo ./gp_install [--cli-only |
    --arm | --help] --cli-only: CLI Only --arm: ARM no options: UI
   ```

   *Pour désinstaller ultérieurement le logiciel, utilisez la commande **ARM** :*

   ```
   $ ./gp_uninstall.sh --help Usage: $ sudo ./gp_uninstall [--
   cli-only | --arm | --help] --cli-only: CLI Only --arm: ARM no
    options: UI
   ```

3. Configurez les paramètres VPN que vous souhaitez pré-déployer sur les périphériques IoT Ubuntu.
   1. Dans le chemin `client-cert`, importez le certificat au format pcks12 et enregistrez le fichier en y ajoutant l'extension .pfx (par exemple, **pan_client_cert.pfx**).
   2. Dans le chemin `passphrase du certificat client`, enregistrez le fichier du code secret en ajoutant l'extension .dat extension (par exemple, **pan_client_cert_passcode.dat**)
   3. Dans le chemin `log-path-service`, si vous n'utilisez pas le chemin par défaut pour PanGPS (par exemple, `/opt/paloaltonetworks/globalprotect`), assurez-vous que le dossier-chemin `log-setting (paramètre du journal)` a les mêmes privilèges que le dossier globalprotect, qui se trouve sous `opt/paloaltonetworks`.
   4. Créez le fichier de configuration prédéploiement (`/opt/paloaltonetworks/globalprotect/pangps.xml`) au format suivant et modifiez l'adresse IP du portail GlobalProtect et les paramètres d'authentification, soit : nom d'utilisateur et mot de passe ou le chemin du certificat client (**`client-cert-path`**) et le fichier de la phrase

 ©2026 Palo Alto Networks, Inc.

secrète (**client-cert-passphrase**). Vous pouvez également spécifier un dossier facultatif dans lequel stocker vos journaux de service GlobalProtect (**log-path-service**) et d'agent (**log-path-agent**).

```
<?xml version="1.0" encoding="UTF-8"?> <GlobalProtect> <PanSetup>
 <Portal>192.168.1.160</Portal> //adresse du portail pré-déployé
 </PanSetup> <PanGPS> </PanGPS> <Settings> <portal-timeout>5</
portal-timeout> <connect-timeout>5</connect-timeout> <receive-
timeout>30</receive-timeout> <os-type>IoT</os-type> //type de
 système d'exploitation pré-déployé pour l'IdO. Si cette balise
 n'est pas présente, GP détectera automatiquement le type de
 système d'exploitation. <head-less>oui</head-less> //mode sans
 tête pré-déployé <username>abc</username> //nom d'utilisateur
 pré-déployé optionnel <password>xyz</password> //mot de passe
 pré-déployé optionnel <client-cert-path>cli_cert_path</client-
cert-path> //chemin de certificat client pré-déployé optionnel(p12)
 <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase> //chemin de fichier de phrase de passe de certificat
 client pré-déployé optionnel <log-path-service>/tmp/gps</log-
path-service> //dossier journal pré-déployé optionnel pour PanGPS
 <log-path-agent>/tmp/gpa</log-path-agent> //dossier journal pré-
déployé optionnel pour PanGPA et GlobalProtect CLI </Settings> </
GlobalProtect>
```

4. Recommencez le processus GlobalProtect pour que la configuration de prédéploiement prenne effet.

5. Une fois que vous avez déployé le périphérique IoT, vous pouvez collecter les journaux selon vos besoins à l'aide de la commande **globalprotect collect-log**.

```
user@linuxhost:~$ globalprotect collect-log Le fichier de
 support est enregistré dans /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

6. (Facultatif) Si la méthode d'authentification est une combinaison nom d'utilisateur/mot de passe et certificat de client, assurez-vous que le **Nom commun** du certificat de client correspond au nom d'utilisateur.

 ©2026 Palo Alto Networks, Inc.

Installation GlobalProtect pour IoT sur Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager) • IdO sur le système d'exploitation Windows	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Les périphériques exécutant Windows 10 IoT peuvent utiliser l'application GlobalProtect. Utilisez la méthode de distribution de votre organisation, comme Microsoft System Center Configuration Manager (SCCM), pour déployer et installer l'application GlobalProtect sur vos périphériques IoT exécutant Windows 10 IoT Enterprise.

Le déploiement Windows IoT GlobalProtect prend en charge l'authentification basée sur les certificats. Vous devez installer le certificat utilisé aux fins d'authentification sur chaque périphérique IoT dans le magasin local de la machine. Si un périphérique IoT possède plusieurs certificats avec la même CA racine, GlobalProtect utilise le premier certificat du magasin local du périphérique IoT pour l'authentification. Assurez-vous que vos certificats sont placés dans le bon ordre sur vos périphériques.

Les sections suivantes décrivent l'installation de l'application GlobalProtect sur les périphériques exécutant Windows IoT :

- Téléchargez le fichier MSIEXEC sur le périphérique IoT et installez-le
- Modifiez les clés de registre sur le périphérique IoT (à la demande ou toujours actif)
- Modifiez les clés de registre sur le périphérique IoT (Toujours actif avec préouverture de session)

Téléchargez le fichier MSIEXEC sur le périphérique IoT et installez-le

Vous pouvez télécharger le fichier `msiexec.exe` sur vos périphériques IoT pour installer l'application GlobalProtect pour la méthode de connexion **À la demande** ou **Toujours active**. Vous utilisez la même méthode pour déployer le fichier msiexec.exe que sur un périphérique autre que IoT.

Modifiez les clés de registre sur le périphérique IoT (à la demande ou toujours actif)

Vous devez indiquer IoT en tant que type de système d'exploitation et sans tête comme type de périphérique et spécifier l'adresse du portail. Vous pouvez également spécifier un nom d'utilisateur et un mot de passe. Si vous ne spécifiez pas de nom d'utilisateur et de mot de passe, GlobalProtect utilise alors l'authentification basée sur un certificat.

 ©2026 Palo Alto Networks, Inc.

Vous pouvez utiliser les méthodes d'installation suivantes pour la méthode de connexion **à la demande** ou **toujours active** :

- Spécifiez le type de système d'exploitation (Requis) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\Settings`

  Nom : type de système d'exploitation

  Type : REG_SZ

  Données : IoT
- Spécifiez un périphérique IoT sans tête (requis) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\Settings`

  Nom : sans tête

  Type : REG_SZ

  Données : oui
- Spécifiez l'adresse du portail (requis) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\PanSetup`

  Name (Nom) : Portail

  Type : REG_SZ

  Données : Saisissez l'adresse IP ou le FQDN du portail GlobalProtect.
- Spécifiez le nom d'utilisateur (facultatif) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\Settings`

  Nom : nom d'utilisateur

  Type : REG_SZ

  Données : Entrez le nom d'utilisateur à utiliser avec le périphérique IoTO.
- Spécifiez le mot de passe (facultatif) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\Settings`

  Nom : mot de passe

  Type : REG_SZ

  Données : Entrez le mot de passe à utiliser avec le périphérique IoT.

 ©2026 Palo Alto Networks, Inc.

Modifiez les clés de registre sur le périphérique IoT (Toujours actif avec préouverture de session)

Vous devez spécifier l'adresse du portail, le délai d'expiration de la préouverture de session et la valeur de service uniquement. Vous devez supprimer la valeur de GlobalProtect pour empêcher le périphérique IoT de lancer automatiquement l'interface de l'application lors du redémarrage du système. Un tunnel VPN de pré-ouverture de session n'associe pas le nom d'utilisateur parce que l'utilisateur ne s'est pas connecté.

Vous pouvez utiliser les méthodes d'installation suivantes pour la méthode de connexion **Préouverture de session (Toujours actif)** :

- Spécifiez l'adresse du portail (requis) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\PanSetup`

  Name (Nom) : Portail

  Type : REG_SZ

  Données : Saisissez l'adresse IP ou le FQDN du portail GlobalProtect.
- Spécifiez la valeur de préouverture de session (requis) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\PanSetup`

  Name (Nom) : Préouverture de session

  Type : REG_SZ

  Données : 1
- Spécifiez la valeur de service uniquement (requis) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks \GlobalProtect\Settings`

  Nom : service uniquement

  Type : REG_SZ

  Données : oui
- Supprimez la valeur de GlobalProtect (requis) :

  Sous-clé de registre : `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\Run`

  Name (Nom) : GlobalProtect

  Type : REG_SZ

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

Certification FIPS-CC de GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect 6.0.7 ou une version ultérieure de 6.0.x. Pour iOS et Android, application GlobalProtect pour les gouvernements 6.0.7 ou une version ultérieure de l'application GlobalProtect pour les gouvernements 6.0.x. Mode FIPS-CC pour GlobalProtect sur Windows et macOS, périphériques basés sur ARM fonctionnant sous Windows et macOS, iOS, Android et Linux.

L'application GlobalProtect™ pour Windows et macOS, les périphériques basés sur ARM fonctionnant sous Windows, et macOS, iOS, Android,et Linux fournit un mode FIPS-CC qui peut être activé et qui intègre les exigences des Critères communs (CC) et de la Federal Information Processing Standard (norme fédérale de traitement de l'information) (FIPS 140-3).

Vous pouvez consulter la page d'état pour suivre l'état de la certification FIPS et CC.

Ces certifications de sécurité garantissent un ensemble standard d'assurances et de fonctionnalités de sécurité. Elles sont souvent requises par les agences gouvernementales américaines et d'autres industries régies à l'échelle nationale et internationale. Pour obtenir de plus amples précisions sur les certifications de produits et les validations de tiers, reportez-vous à la page consacrée aux certifications de Palo Alto Networks.

Reportez-vous aux sections suivantes pour des informations sur la configuration et le dépannage de l'application GlobalProtect pour les terminaux Windows et macOS, les périphériques basés sur ARM fonctionnant sous Windows, et macOS, iOS, Android,et Linux en mode FIPS-CC :

- Activation et vérification du mode FIPS-CC
- Fonctions de sécurité FIPS-CC

Activation et vérification du mode FIPS-CC

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect 6.0.7 ou une version ultérieure de 6.0.x. Pour iOS et Android, application GlobalProtect pour les gouvernements 6.0.7 ou une version ultérieure de l'application GlobalProtect pour les gouvernements 6.0.x. Mode FIPS-CC pour GlobalProtect sur Windows et macOS, périphériques basés sur ARM fonctionnant sous Windows et macOS, iOS, Android et Linux.

Vous pouvez activer et vérifier le mode FIPS-CC pour l'application FIPS-CC.

- Pour les terminaux Windows
- Pour les terminaux MacOS
- Utiliser Workspace ONE sur les terminaux iOS
- Sur les terminaux Linux avec Ubuntu ou RHEL
- Utiliser Microsoft Intune sur les terminaux Android

  L'application GlobalProtect mode FIPS-CC est prise en charge sur les plateformes x86 et ARM.

  Nous vous recommandons d'activer le mode FIPS-CC sur le portail/passerelle GlobalProtect afin d'exploiter de manière efficace le mode FIPS-CC sur les terminaux.

  Pour modifier le registre Windows ou la plist MacOs, vous devez avoir un compte administrateur dans Windows ou MacOS.

- Windows
- macOS
- Linux (Red Hat)
- iOS
- Android

 ©2026 Palo Alto Networks, Inc.

Activer et vérifier le mode FIPS-CC sur les terminaux Windows

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect 6.0.7 ou une version ultérieure de 6.0.x. Mode FIPS-CC pour GlobalProtect sous Windows et les périphériques basés sur ARM fonctionnant sous Windows.

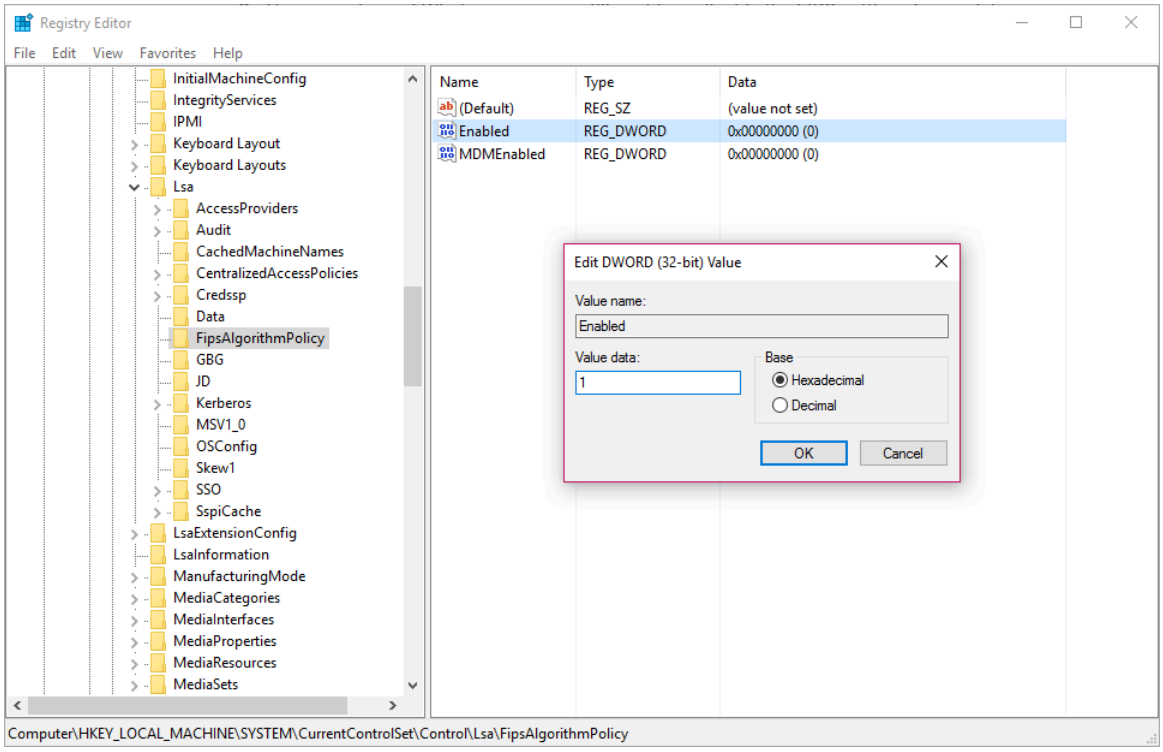
Sur les points de terminaison Windows, utilisez les étapes suivantes pour activer et vérifier le mode FIPS-CC pour GlobalProtect™ à l'aide du registre Windows :

©2026 Palo Alto Networks, Inc.

1. Activez le mode FIPS-CC pour le système d'exploitation Windows.

   Pour activer le mode FIPS-CC pour GlobalProtect, vous devez d'abord activer le mode FIPS-CC pour le système d'exploitation Windows.

   1. Lancez l'invite de commande.
   2. Entrez **`regedit`** pour ouvrir le registre Windows.
   3. Dans le registre Windows, accédez à : `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\`.
   4. Cliquez avec le bouton droit sur la valeur **Enabled (Activé)** du registre et **Modify (Modifiez)**-la.
   5. Pour activer le mode FIPS, définissez les **Value Data (Données de valeur)** sur **1**. La valeur par défaut de **`0`** indique que le mode FIPS est désactivé.



   6. Cliquez sur **OK**.
   7. Redémarrez votre point de terminaison.

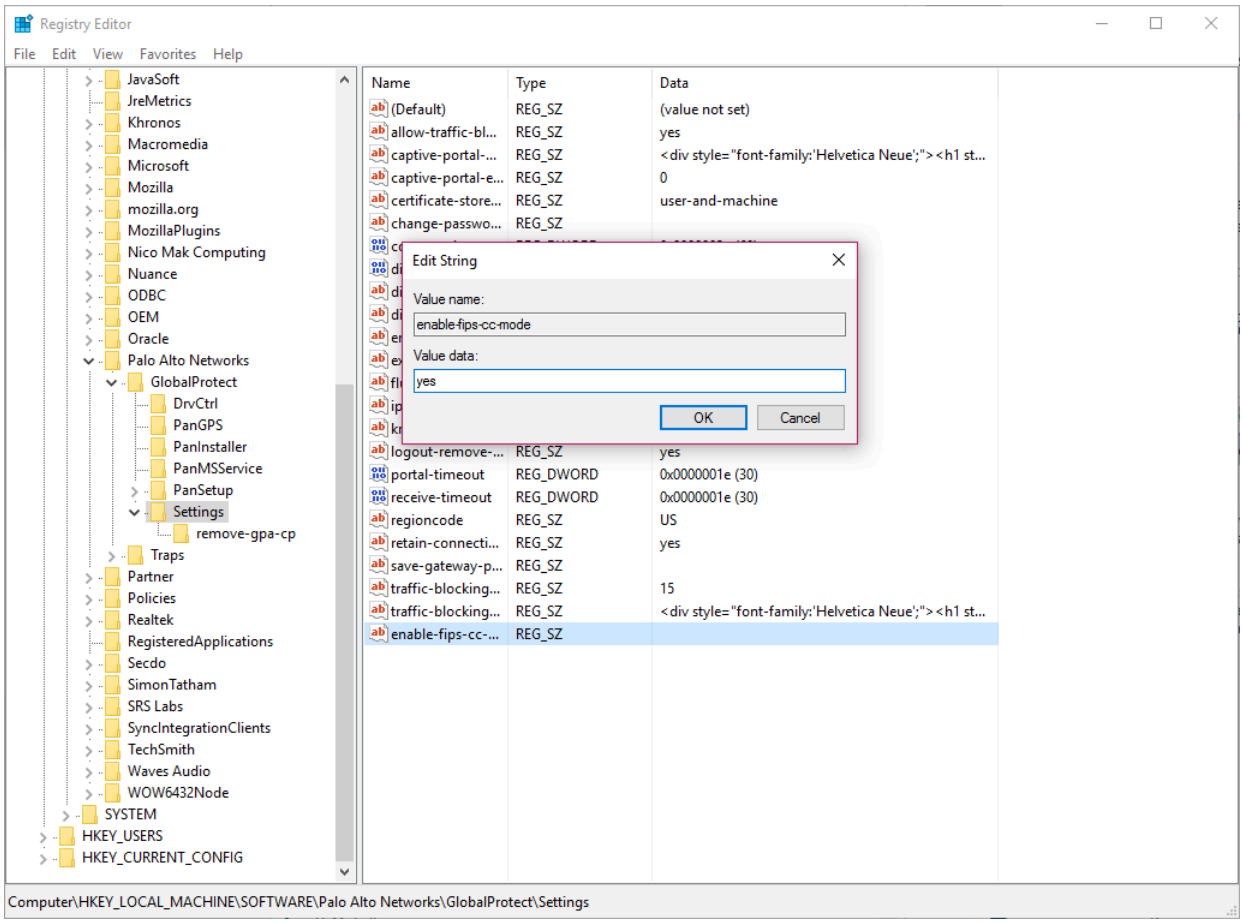
2. Activez le mode FIPS-CC pour GlobalProtect.

   Vous ne pouvez désactiver le mode FIPS-CC après l'avoir activé. Pour exécuter GlobalProtect en mode non-FIPS-CC, les utilisateurs finaux doivent désinstaller et réinstaller l'application

 ©2026 Palo Alto Networks, Inc.

GlobalProtect. Tous les paramètres du mode FIPS-CC sont ainsi supprimés du registre Windows.

1. Lancez l'invite de commande.
2. Entrez **`regedit`** pour ouvrir le registre Windows.
3. Dans le registre Windows, accédez à : `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\`.
4. Cliquez sur **Edit (Modifier)**, puis sélectionnez **New (Nouveau)** > **String Value (Valeur de chaîne)**.
5. Lorsque vous êtes invité à le faire, spécifiez le **Name (Nom)** de la nouvelle valeur du registre en tant que **`enable-fips-cc-mode`**.
6. Cliquez avec le bouton droit sur la nouvelle valeur du registre et **Modify (Modifiez)**-la.
7. Pour activer le mode FIPS-CC, définissez les **Value Data (Données de valeur)** sur **`yes`**.
8. Cliquez sur **OK**.

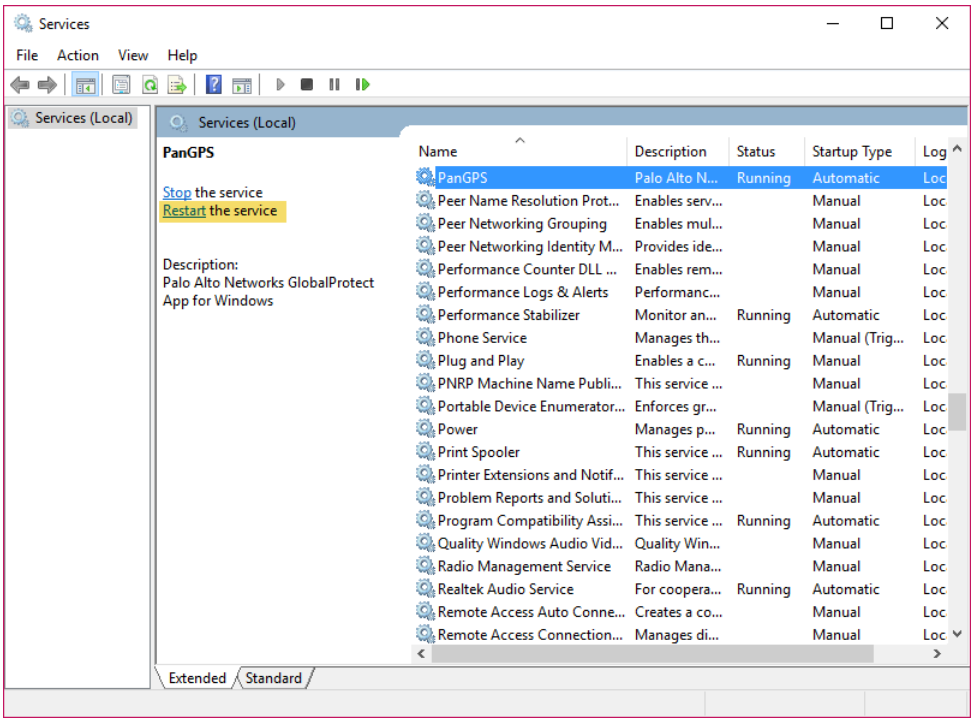


 ©2026 Palo Alto Networks, Inc.

3. Redémarrez GlobalProtect.

Pour permettre à l'application GlobalProtect d'être lancée en mode FIPS-CC, vous devez redémarrer GlobalProtect à l'aide de l'une des méthodes suivantes :

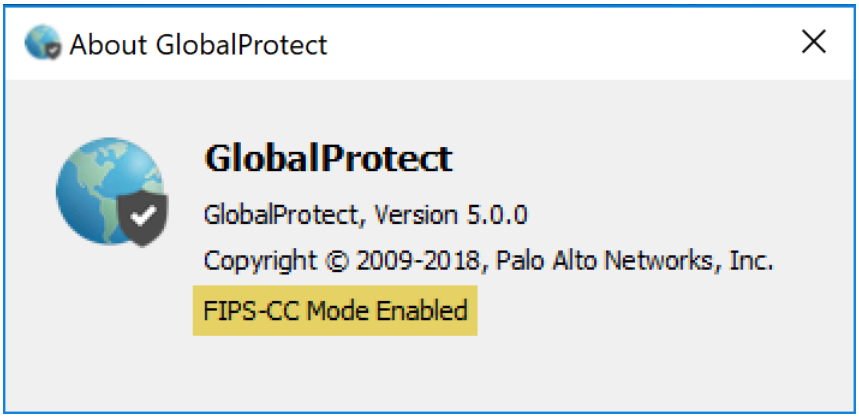
- Redémarrez votre point de terminaison.
- Relancez l'application GlobalProtect et le service GlobalProtect (PanGPS) :
  1. Lancez l'invite de commande.
  2. Entrez **`services.msc`** pour ouvrir le gestionnaire des Windows Services.
  3. Dans la liste des Services, sélectionnez **PanGPS**.
  4. **Restart (Redémarrez)** le service.

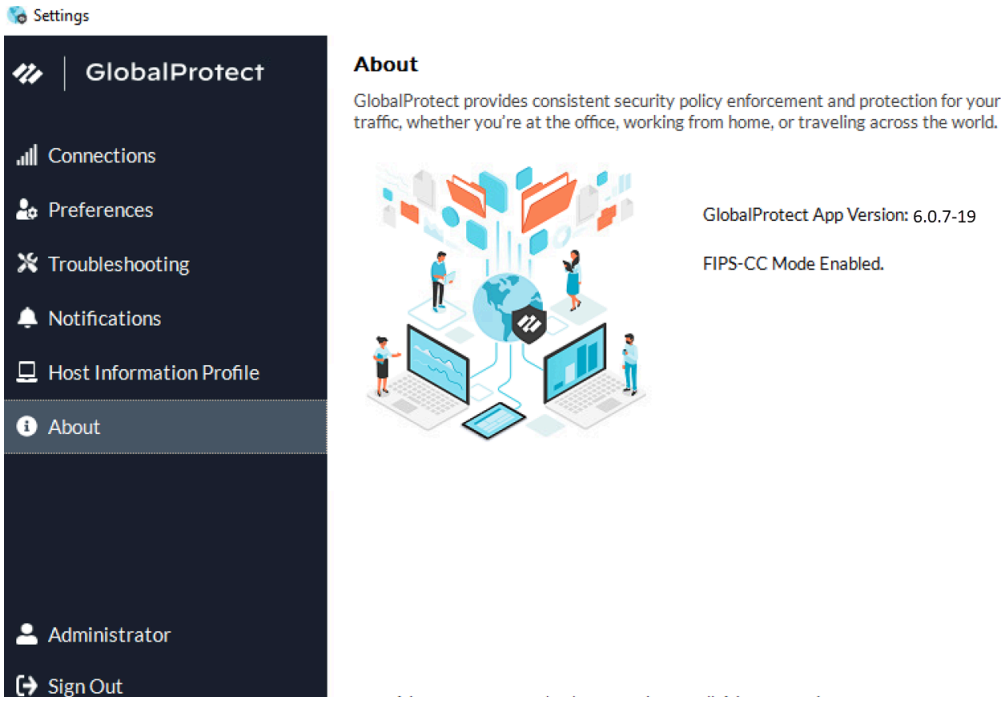


4. Sinon, vous pouvez activer le mode FIPS-CC en utilisant la syntaxe msiexec suivante via le programme d'installation Microsoft Windows (Msiexec) : **`msiexec /i GlobalProtect64.msi ENABLEFIPSCCMODE=YES`**

 ©2026 Palo Alto Networks, Inc.

5. Vérifiez que le mode FIPS-CC est activé sur l'application GlobalProtect.
   1. Lancez l'application GlobalProtect.
   2. À partir du panneau d'état, ouvrez le dialogue des paramètres ( ).
   3. Sélectionnez **About (À propos)**.
   4. Vérifiez que le mode FIPS-CC est activé. Si le mode FIPS-CC est activé, la boîte de dialogue About (À propos) affiche l'état `FIPS-CC Mode Enabled`.





6. Affichez les journaux pour consulter les journaux de l'application GlobalProtect liés au mode FIPS-CC sur les terminaux Windows.

7. Affichez, collectez et envoyez les journaux à l'administrateur pour déboguer et résoudre les problèmes liés au mode FIPS-CC sur les périphériques Windows.

©2026 Palo Alto Networks, Inc.

Activer et vérifier le mode FIPS-CC sur les terminaux macOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect 6.0.7 ou une version ultérieure de 6.0.x. Mode FIPS-CC pour GlobalProtect sur les périphériques macOS et ARM fonctionnant sur macOS.

Sur les points de terminaison MacOS, utilisez les étapes suivantes pour activer et vérifier le mode FIPS-CC pour GlobalProtect™ à l'aide de la plist MacOS (liste des propriétés) :

Pour activer le mode FIPS-CC pour GlobalProtect, vous devez d'abord activer le mode FIPS-CC pour le système d'exploitation macOS. Par défaut, le mode FIPS pour le système d'exploitation macOS est activé automatiquement sur les points de terminaison exécutant macOS 10.8 ou toutes versions ultérieures.

1. Ouvrez le fichier plist GlobalProtect et recherchez les paramètres de personnalisation GlobalProtect.
   1. Lancez un éditeur de plist, comme Xcode.
   2. Dans l'éditeur de plist, ouvrez le fichier de la plist suivant : `/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`.
   3. Trouvez le dictionnaire des paramètres GlobalProtect : `/Palo Alto Networks/GlobalProtect/Settings`.

      Si le dictionnaire des paramètres n'existe pas, créez-le. Vous pouvez ajouter chaque clé au dictionnaire des paramètres en tant que chaîne.

 ©2026 Palo Alto Networks, Inc.

2. Activez le mode FIPS-CC pour GlobalProtect.

   Vous ne pouvez désactiver le mode FIPS-CC après l'avoir activé. Pour exécuter GlobalProtect en mode non-FIPS-CC, les utilisateurs finaux doivent désinstaller et réinstaller l'application GlobalProtect. Tous les paramètres du mode FIPS-CC sont ainsi supprimés de la plist MacOS.

   Dans le dictionnaire des paramètres, ajoutez la paire clé-valeur suivant pour activer le mode FIPS-CC :

   <key>enable-fips-cc-mode</key>

   <string>yes</string>

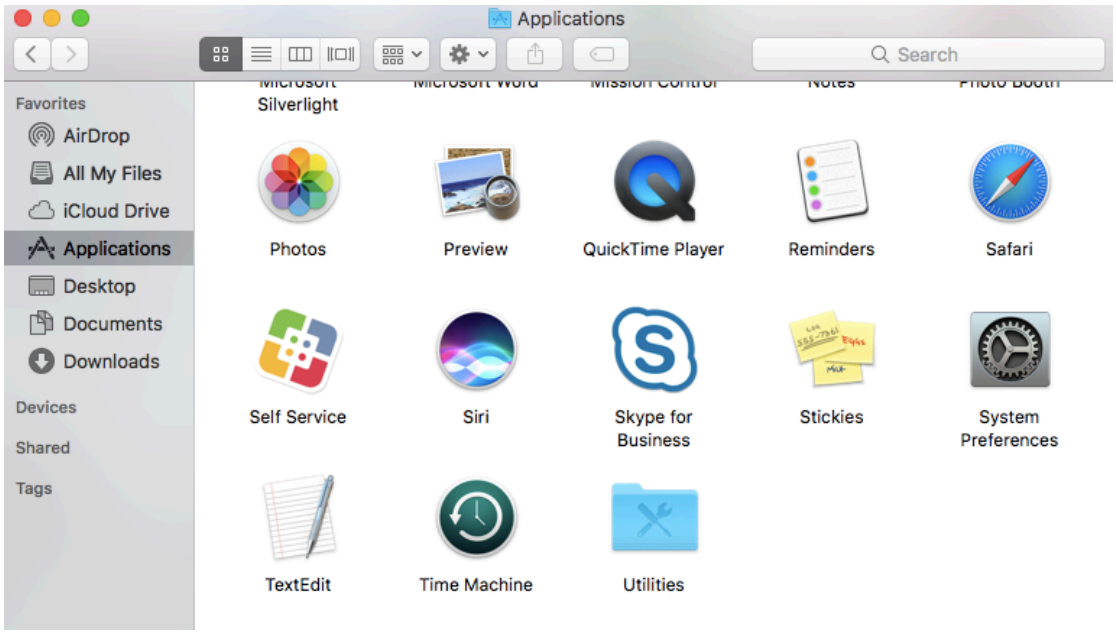
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>Palo Alto Networks</key>
        <dict>
                <key>GlobalProtect</key>
                <dict>
                        <key>PanGPS</key>
                        <dict>
                                <key>UserProfileType</key>
                                <integer>0</integer>
                                <key>disable-globalprotect</key>
                                <integer>0</integer>
                        </dict>
                        <key>PanSetup</key>
                        <dict>
                                <key>CurrentVersion</key>
                                <string>6.0.5-27</string>
                                <key>InstallHistory</key>
                                <string>Fresh Install</string>
                                <key>PreviousVersion</key>
                                <string></string>
                        </dict>
                        <key>Settings</key>
                        <dict>
                                <key>enable-fips-cc-mode</key>
                                <string>yes</string>
                                <key>disable-globalprotect</key>
                                <integer>0</integer>
                        </dict>
                </dict>
        </dict>
</dict>
</plist>
~
```

 ©2026 Palo Alto Networks, Inc.

3. Redémarrez GlobalProtect.

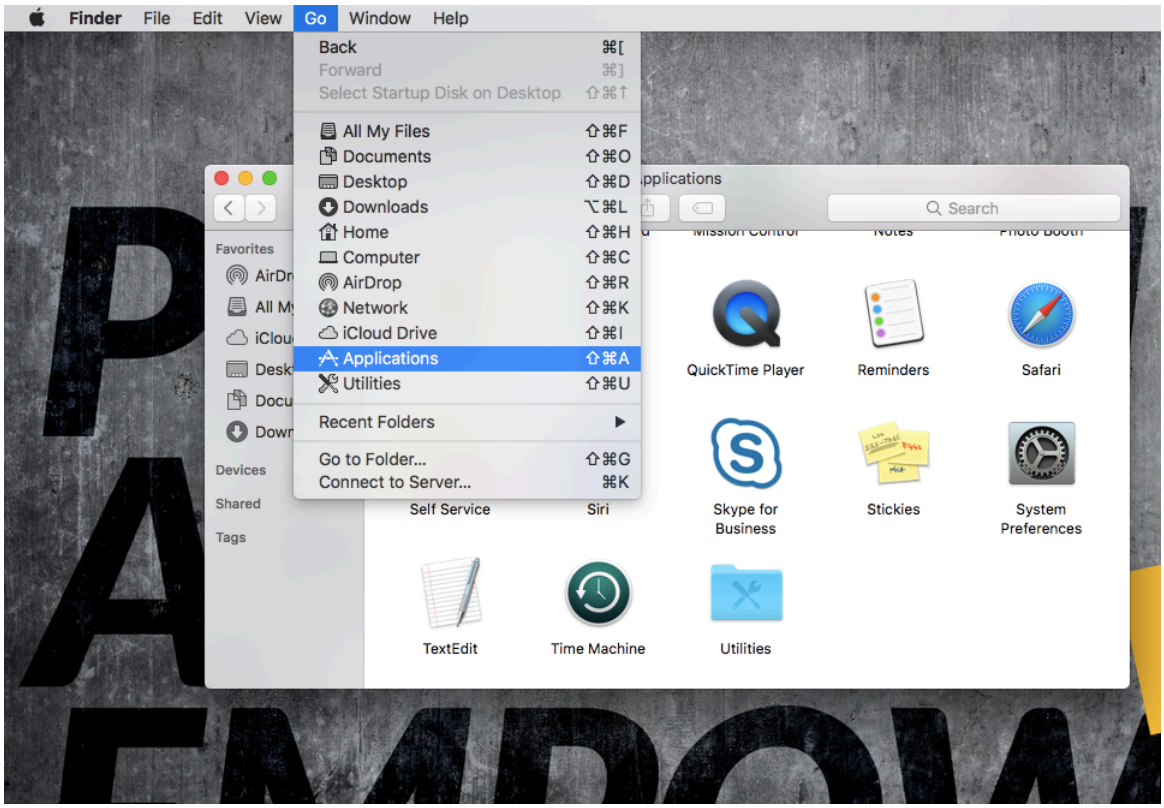
Pour permettre à l'application GlobalProtect d'être lancée en mode FIPS-CC, vous devez redémarrer GlobalProtect à l'aide de l'une des méthodes suivantes :

- Redémarrez votre point de terminaison.
- Relancez l'application GlobalProtect et le service GlobalProtect (PanGPS) :
  1. Lancez le Finder.
  2. Ouvrer le dossier des applications :
     - Dans la barre latérale du Finder, sélectionnez **Applications**.



     - Si vous ne voyez pas **Applications** dans la barre latérale du Finder, sélectionnez **Go (Aller)** > **Applications** dans la barre de menu du Finder.

 ©2026 Palo Alto Networks, Inc.



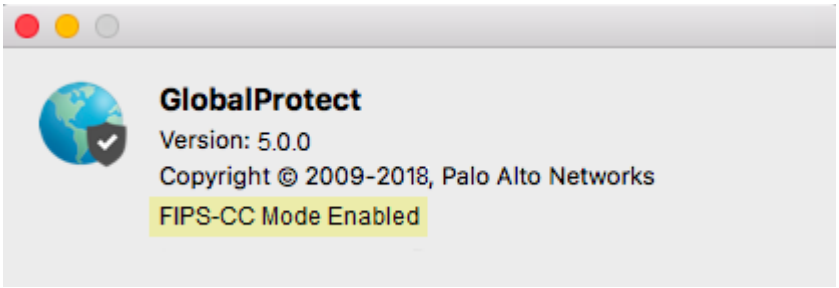
*Pour afficher **Applications** dans la barre latérale du Finder, sélectionnez **Finder** > **Preferences (Préférences)** dans la barre de menu du Finder. Dans les préférences du Finder, sélectionnez **Sidebar (Barre latérale)**, puis cochez l'option permettant d'afficher **Applications.***

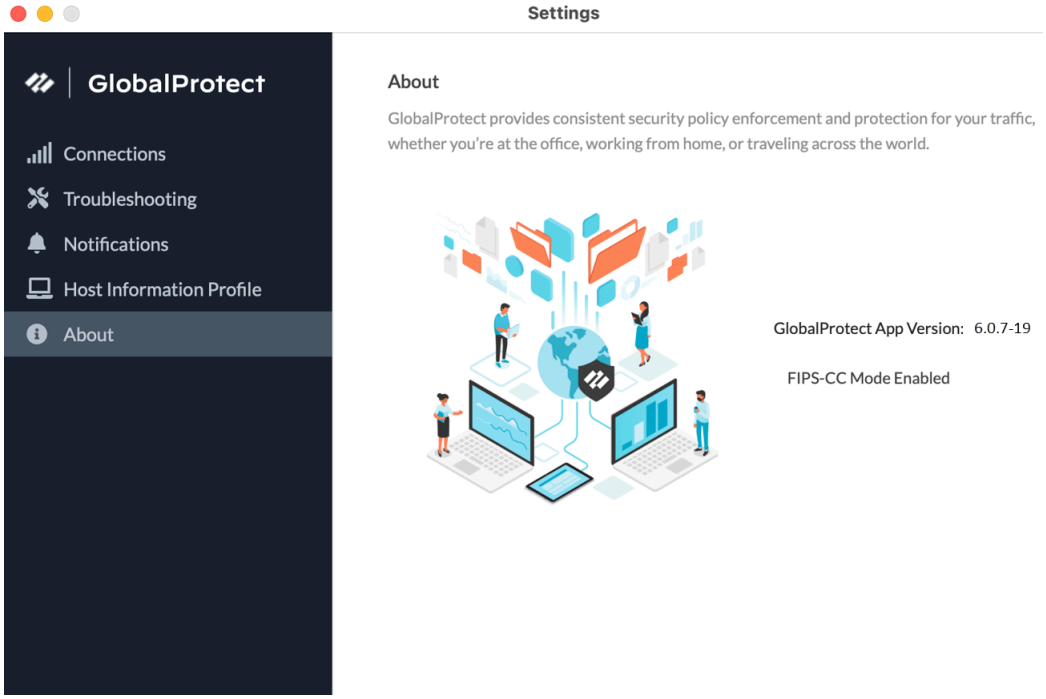
3. Ouvrer le dossier des utilitaires.
4. Lancez le Terminal.
5. Exécutez les commandes suivantes :

```
username>$ launchctl unload -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist username>$
 launchctl unload -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangps.plist username>$
 launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangps.plist username>$
 launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangpa.plist
```

 ©2026 Palo Alto Networks, Inc.

4. Vérifiez que le mode FIPS-CC est activé sur l'application GlobalProtect.
   1. Lancez l'application GlobalProtect.
   2. À partir du panneau d'état, ouvrez le dialogue des paramètres (⚙).
   3. Sélectionnez **About (À propos)**.
   4. Vérifiez que le mode FIPS-CC est activé. Si le mode FIPS-CC est activé, la boîte de dialogue About (À propos) affiche l'état `FIPS-CC Mode Enabled`.





5. Affichez les journaux pour consulter les journaux de l'application GlobalProtect liés au mode FIPS-CC sur les terminaux exécutant macOS.

6. Affichez, collectez et envoyez les journaux à l'administrateur pour déboguer et résoudre les problèmes liés au mode FIPS-CC sur les périphériques exécutant macOS.

 ©2026 Palo Alto Networks, Inc.

Activer et vérifier le mode FIPS-CC à l'aide de Workspace ONE sur les terminaux iOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect pour les gouvernements 6.0.7 ou une version ultérieure de l'application GlobalProtect pour les gouvernements 6.0.x. Mode FIPS-CC pour GlobalProtect sur des périphériques basés sur ARM fonctionnant sur iOS.

Utilisez les étapes suivantes pour activer et vérifier le mode FIPS-CC pour GlobalProtectTM sur les terminaux iOS à l'aide de Workspace ONE.

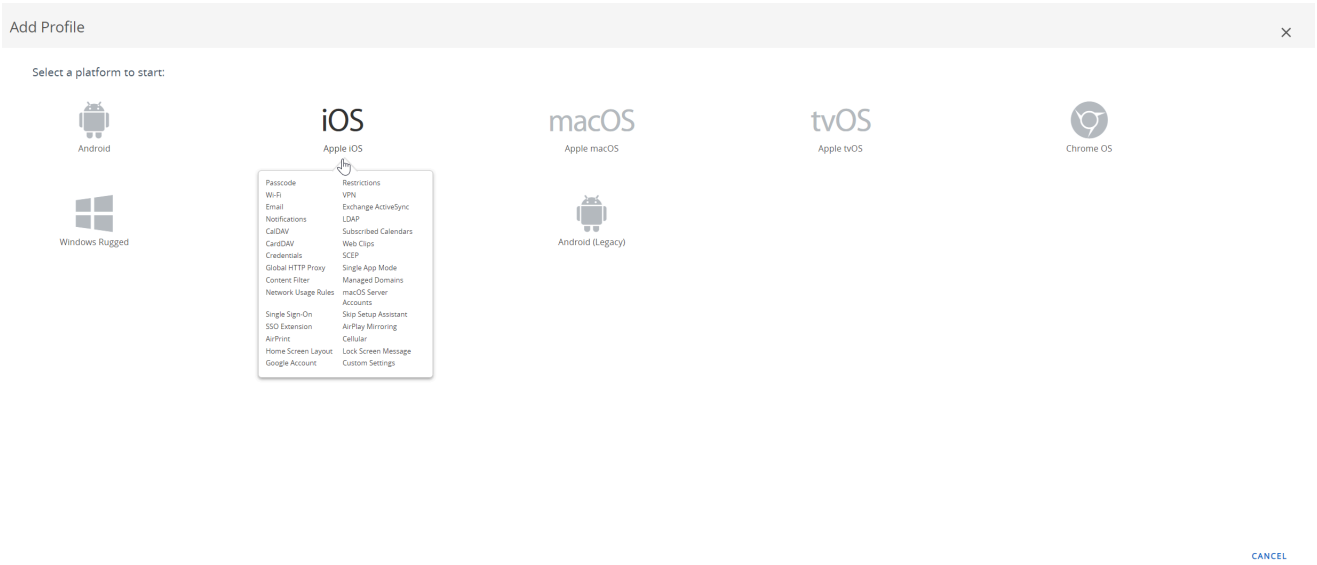
Pour activer FIPS-CC pour les terminaux iOS et Android, vous devez utiliser la version GlobalProtect GlobalProtect pour les gouvernements. Contactez le support Palo Alto et créez un cas pour accéder à la version GlobalProtect pour les gouvernements, qui est distribuée de manière privée.

©2026 Palo Alto Networks, Inc.

1. Activez le mode FIPS sur les terminaux iOS.
   1. Configurer Workspace ONE pour les terminaux iOS. pour les terminaux iOS.
   2. Téléchargez l'application GlobalProtect pour les terminaux iOS et déployez l'application mobile GlobalProtect à l'aide de Workspace ONE.
   3. Depuis la console AirWatch, modifiez un profil Apple iOS existant ou ajoutez-en un nouveau.

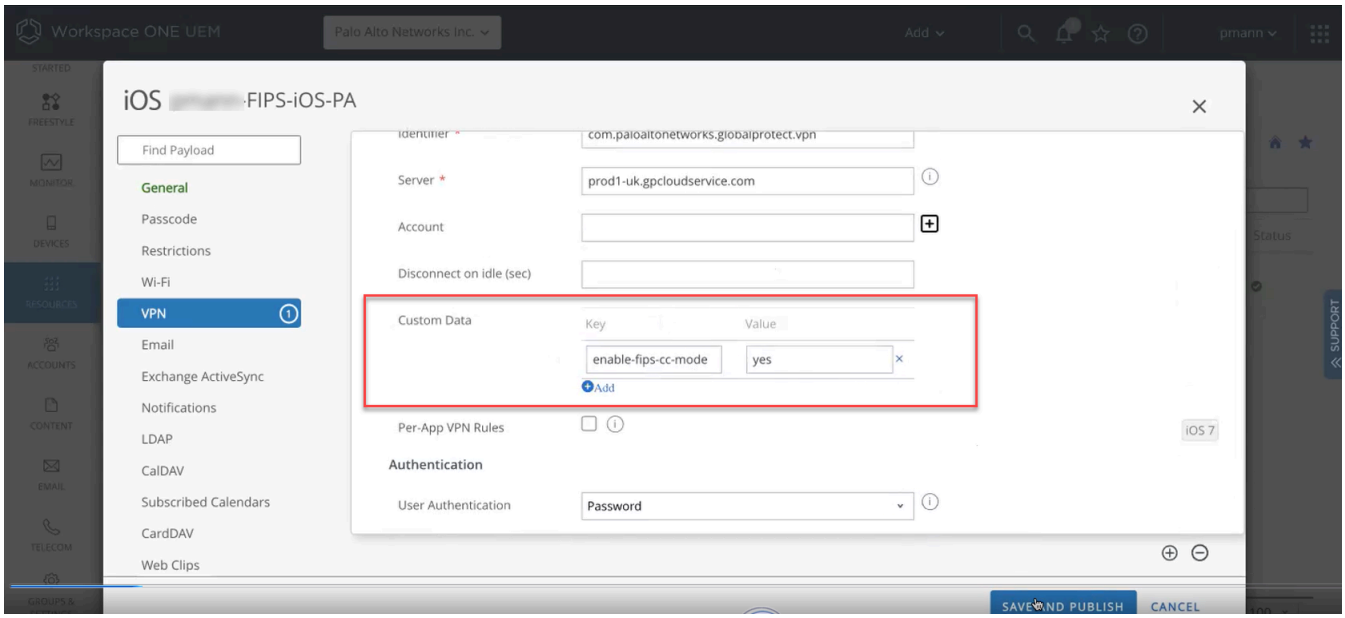
      Pour ajouter un nouveau profil :

      - Sélectionnez **Resources (Ressources)** > **Profiles & Baselines (Profils et références)** > **Profiles (Profils)** > **ADD (AJOUTER)**, puis **Add profile (Ajouter un profil)**.
      - Sélectionnez **iOS** à partir de la liste de la plateforme.



      - Sélectionnez **Device Profile (Profil du périphérique)** dans la fenêtre **Select Context (Sélectionner le contexte)**.
   4. Sur la page **Resources (Ressources)** > **Profiles & Baselines (Profils et références)** > **Profiles (Profils)**, sélectionnez le `<iOS profile>` pour lequel vous souhaitez activer le mode FIPS-CC.
   5. Configurez les paramètres General (Général), VPN et Credentials (Informations d'identification) (Facultatif) pour les `<iOS profile>` que vous souhaitez créer.
   6. Sur la page VPN, sous **Custom Data (Données personnalisées)** :
      - Spécifiez la valeur de la **Key (Clé)** comme `enable-fips-cc-mode`.
      - Définissez la **Value (Valeur)** sur `Yes (Oui)`.

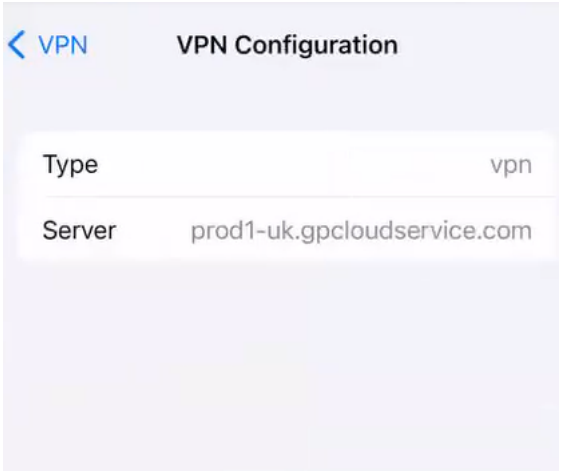
 ©2026 Palo Alto Networks, Inc.



7. **Save & Publish (Enregistrer et publier)** vos modifications.

   Après avoir activé le mode FIPS-CC sur la console Workspace ONE, la console transmet la configuration du mode FIPS-CC mise à jour aux terminaux iOS.

8. Assurez-vous que la configuration mise à jour est transmise de la console aux terminaux iOS. Sur le terminal iOS, sélectionnez **Settings (Paramètres)** > **General (Général)** > **VPN & Device Management (VPN et gestion des périphériques)** > **VPN**. L'écran **VPN Configuration (Configuration VPN)** affiche la dernière configuration. La capture d'écran suivante montre un exemple de configuration VPN.



 ©2026 Palo Alto Networks, Inc.

2. Vérifiez que le mode FIPS-CC est activé sur l'application GlobalProtect.
   1. Lancez l'application GlobalProtect.
   2. À partir du panneau d'état, ouvrez le dialogue des paramètres (⚙).
   3. Sélectionnez **About (À propos)**.
   4. Vérifiez que le mode FIPS-CC est activé. Si le mode FIPS-CC est activé, la boîte de dialogue About (À propos) affiche l'état `FIPS-CC Mode Enabled`.

   Si le mode FIPS-CC n'a pas pu être activé avec succès, la boîte de dialogue À propos affiche le statut `FIPS-CC Mode Failed (Échec du mode FIPS-CC)`.

 ©2026 Palo Alto Networks, Inc.

Vous ne pouvez pas désactiver le mode FIPS-CC sur les terminaux iOS. Pour désactiver le mode FIPS-CC, vous devez supprimer le périphérique iOS du profil de configuration respectif via la console Workspace ONE.

3. Affichez les journaux pour consulter les journaux de l'application GlobalProtect liés au mode FIPS-CC sur les terminaux iOS.
4. Affichez, collectez et envoyez les journaux à l'administrateur pour déboguer et résoudre les problèmes liés au mode FIPS-CC sur les périphériques iOS.

Activer le mode FIPS sur les terminaux Linux avec Ubuntu ou RHEL

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect 6.0.7 ou une version ultérieure de 6.0.x.

 ©2026 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	Mode FIPS-CC pour GlobalProtect sur des périphériques basés sur ARM fonctionnant sur Linux.

Utilisez les étapes suivantes pour activer et vérifier le mode FIPS-CC pour GlobalProtectTM sur les terminaux Linux exécutant Ubuntu ou les plateformes Red Hat Enterprise Linux (RHEL) 8.1.

1. Assurez-vous que le mode FIPS-CC est désactivé sur les terminaux Linux avec Ubuntu ou Red Hat Enterprise Linux (RHEL) 8.1.
2. Installez l'application GlobalProtect sur votre terminal Linux.
3. (Facultatif) Si un certificat client est utilisé pour l'authentification, installez et configurez le certificat client.
4. Modifiez `pangps.xml` pour activer le mode FIPS-CC.

   Sur les points de terminaison Linux, le fichier de configuration de pré-déploiement (`pangps.xml`) se trouve dans `/opt/paloaltonetworks/globalprotect`.

   Dans le fichier `pangps.xml`, sous `Settings (Paramètres)`, ajouter `<enable-fips-cc-mode>yes</enable-fips-cc-mode>`

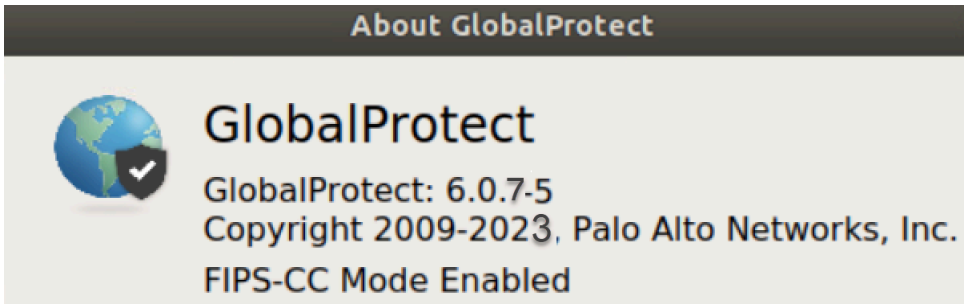
   Par exemple :

   ```
   <?xml version="x.x" encoding="UTF-8"?><GlobalProtect> <Settings>
    <enable-fips-cc-mode>yes</enable-fips-cc-mode> <disable-
   globalprotect>0</disable-globalprotect> </Settings>
   ```

5. Activez le mode FIPS-CC sur le terminal Linux avec Ubuntu ou Red Hat Enterprise Linux (RHEL) 8.1.
6. Redémarrez le point de terminaison Linux pour que les modifications de configuration de pré-déploiement prennent effet.

 ©2026 Palo Alto Networks, Inc.

7. Vérifiez que le mode FIPS-CC est activé sur l'application GlobalProtect.
   1. Lancez l'application GlobalProtect.
   2. À partir du panneau d'état, ouvrez le dialogue des paramètres (⚙).
   3. Sélectionnez **About (À propos)**.
   4. Vérifiez que le mode FIPS-CC est activé. Si le mode FIPS-CC est activé, la boîte de dialogue About (À propos) affiche l'état **FIPS-CC Mode Enabled**. Pour la version CLI, vous pouvez utiliser la commande CLI `globalprotect show --version`.



   Si le mode FIPS-CC n'a pas pu être activé avec succès, la boîte de dialogue À propos affiche le statut **FIPS-CC Mode Failed (Échec du mode FIPS-CC)**.

8. Affichez les journaux pour consulter les journaux de l'application GlobalProtect liés au mode FIPS-CC sur les terminaux Linux.

9. Affichez, collectez et envoyez les journaux à l'administrateur pour déboguer et résoudre les problèmes liés au mode FIPS-CC sur les périphériques Linux.

Activer et vérifier le mode FIPS-CC en utilisant Microsoft Intune sur des terminaux Android

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect pour les gouvernements 6.0.7 ou une version ultérieure de l'application GlobalProtect pour les gouvernements 6.0.x.

 ©2026 Palo Alto Networks, Inc.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	Mode FIPS-CC pour GlobalProtect sur des périphériques basés sur ARM fonctionnant sous Android.

Utiliser les étapes suivantes pour activer et vérifier le mode FIPS-CC pour GlobalProtect™ sur des terminaux Android en utilisant Microsoft Intune

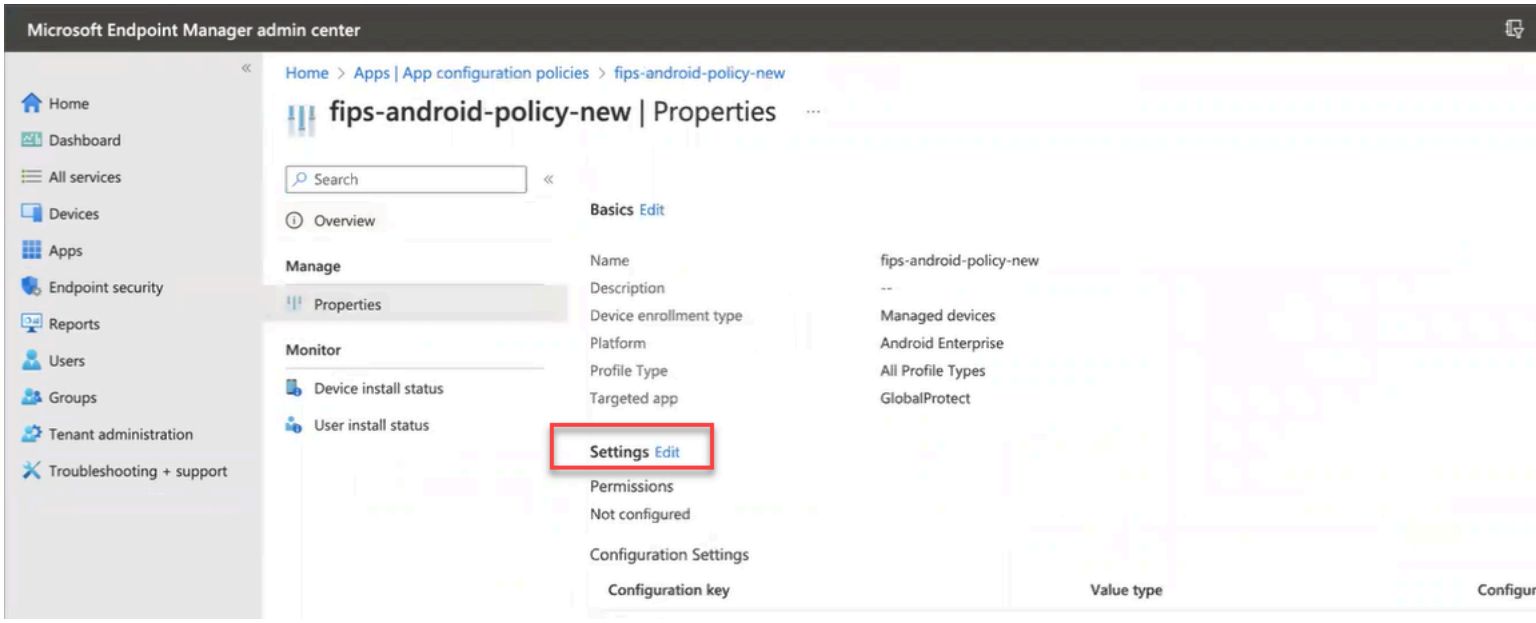
Pour activer FIPS-CC pour les terminaux iOS et Android, vous devez utiliser la version GlobalProtect GlobalProtect pour les gouvernements. Contactez le support Palo Alto et créez un cas pour accéder à la version GlobalProtect pour les gouvernements, qui est distribuée de manière privée.

 ©2026 Palo Alto Networks, Inc.

1. Activez le mode FIPS sur les terminaux Android.
   1. Téléchargement de l'application GlobalProtect pour Android et Déployer l'application GlobalProtect sur des terminaux Android en utilisant Microsoft Intune :
   2. Depuis la console Microsoft Intune, ajoutez **Configuration Settings (Paramètres de configuration)** pour activer le mode FIPS-CC.

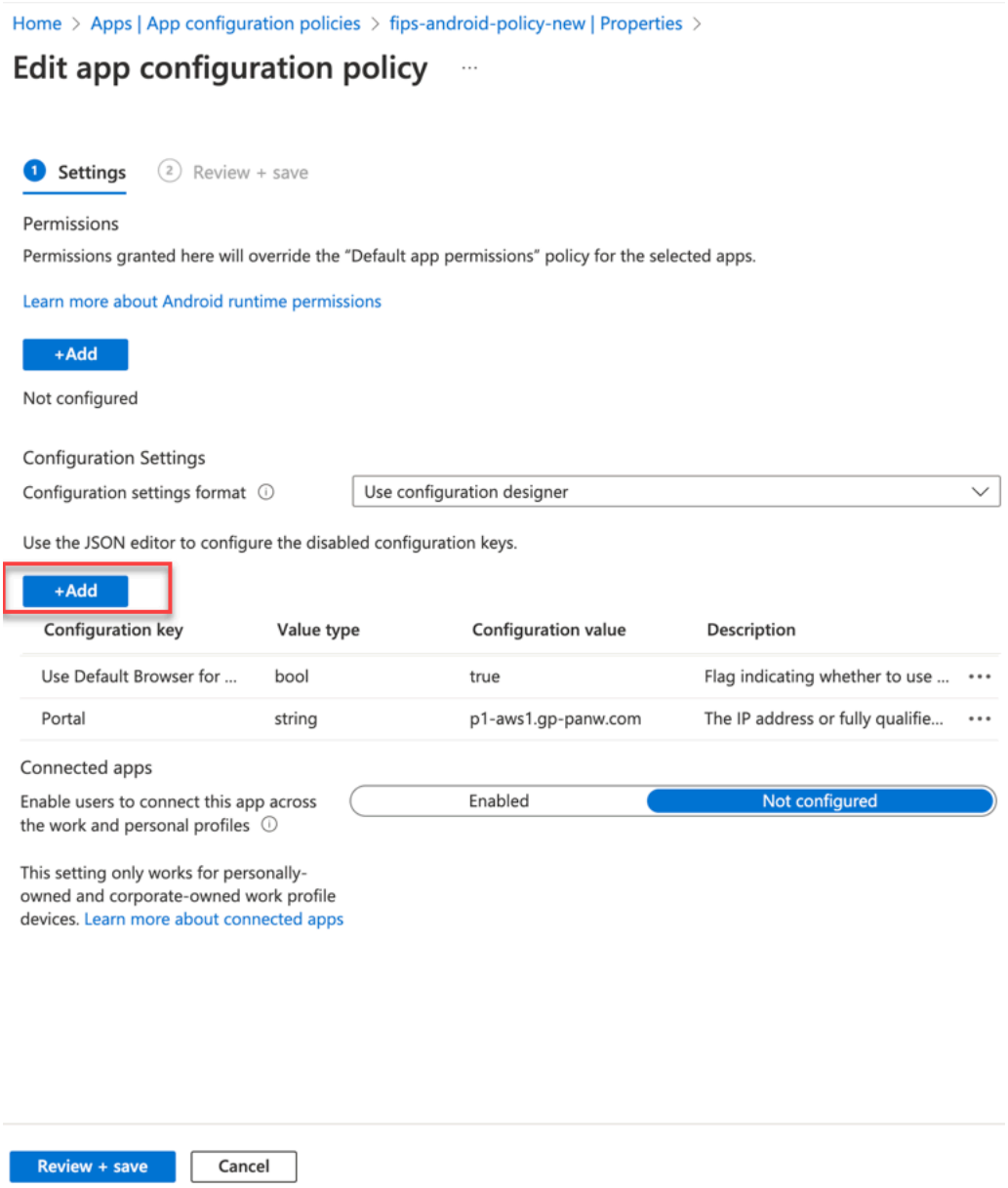
      Pour ajouter des paramètres de configuration pour `Enable fips-cc-mode` :

      1. Sélectionnez **APPS** > **Policy (Politique)** > **App configuration policies (Politiques de configuration des applications)** > **<policy>** > **Properties (Propriétés)**.
      2. **Edit (Modifier)** les **Settings (Paramètres)**.



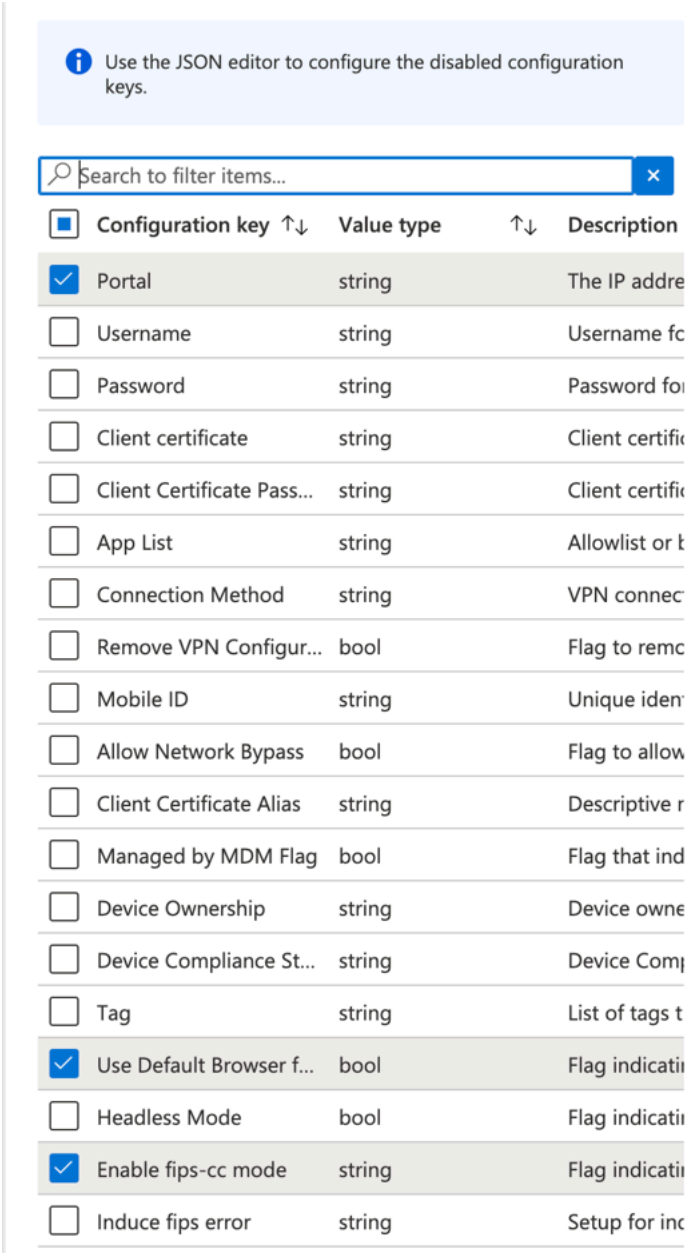
   3. Sur la page Modifier les politiques de configuration des applications, **Add** les **Configuration Settings (Paramètres de configuration)** pour activer le mode FIPS-CC.

 ©2026 Palo Alto Networks, Inc.



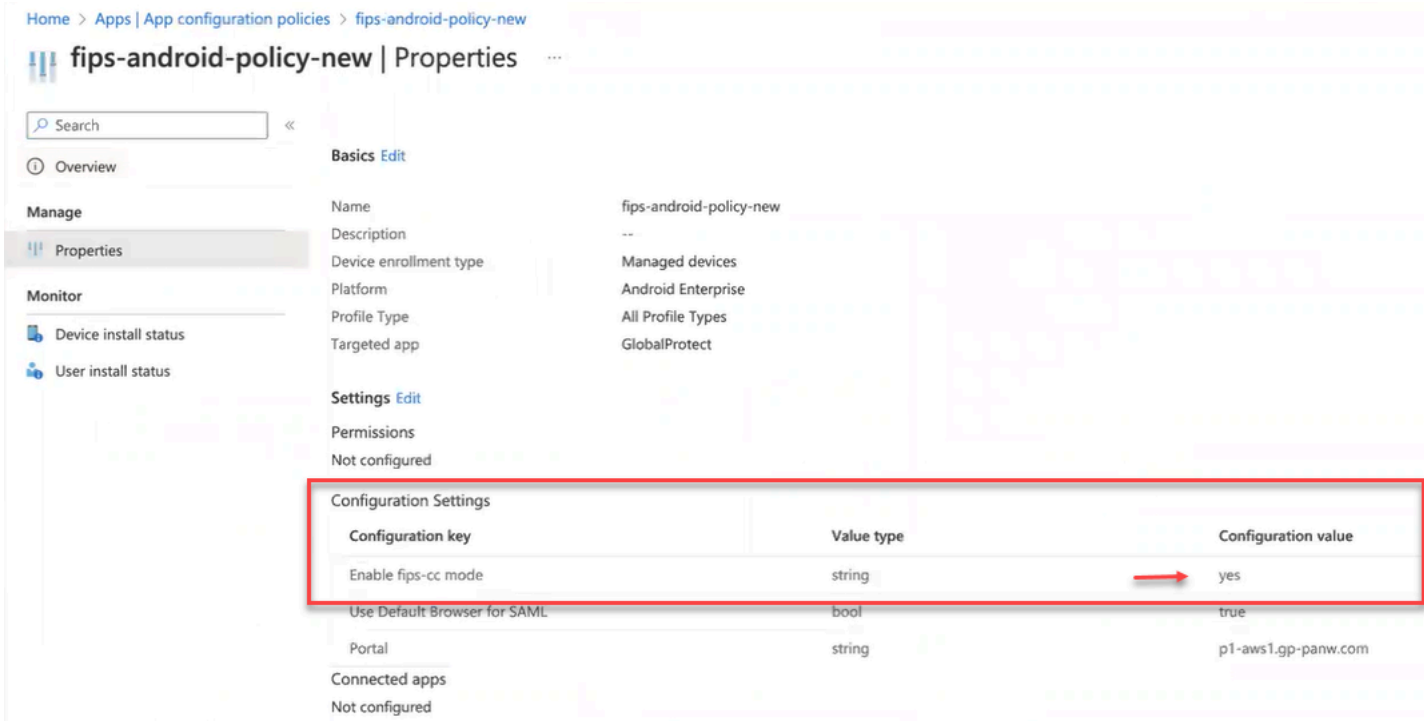
4. Dans la liste des clés de configuration, sélectionnez **Enable fips-cc mode (Activer le mode fips-cc)**.

©2026 Palo Alto Networks, Inc.

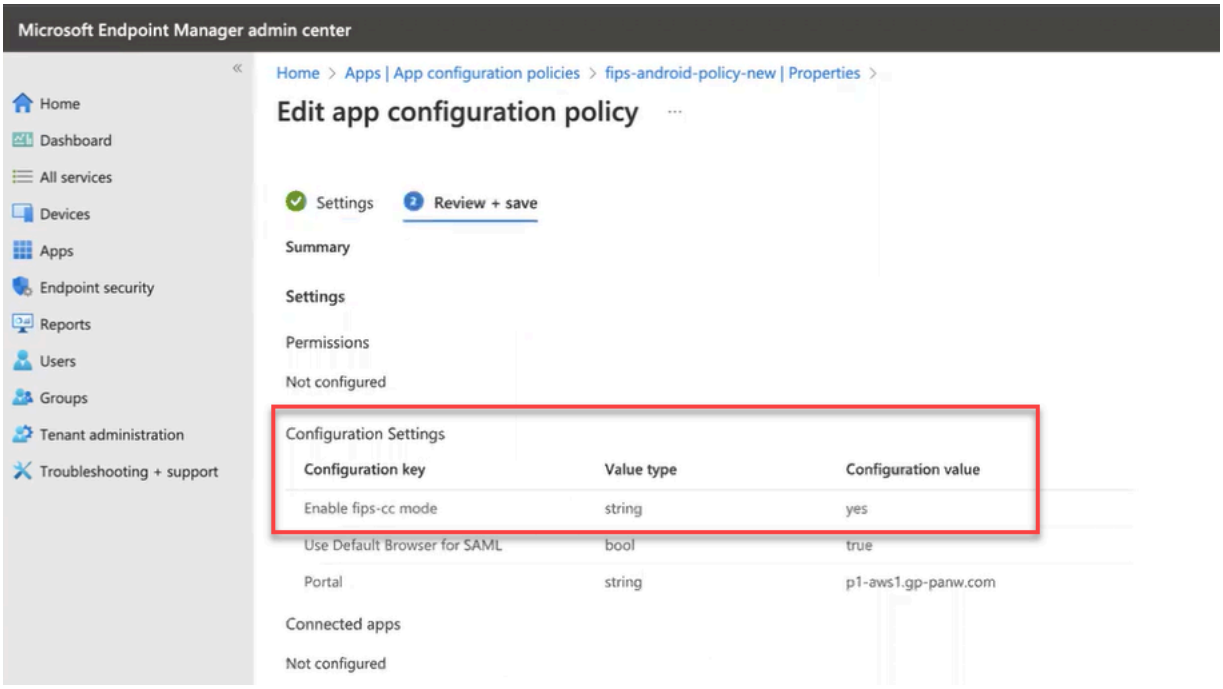


5. Définissez la **Configuration Value (Valeur de configuration)** sur **Yes (Oui)** pour la clé de configuration **Enable fips-cc mode (Activer le mode fips-cc)**.

 ©2026 Palo Alto Networks, Inc.



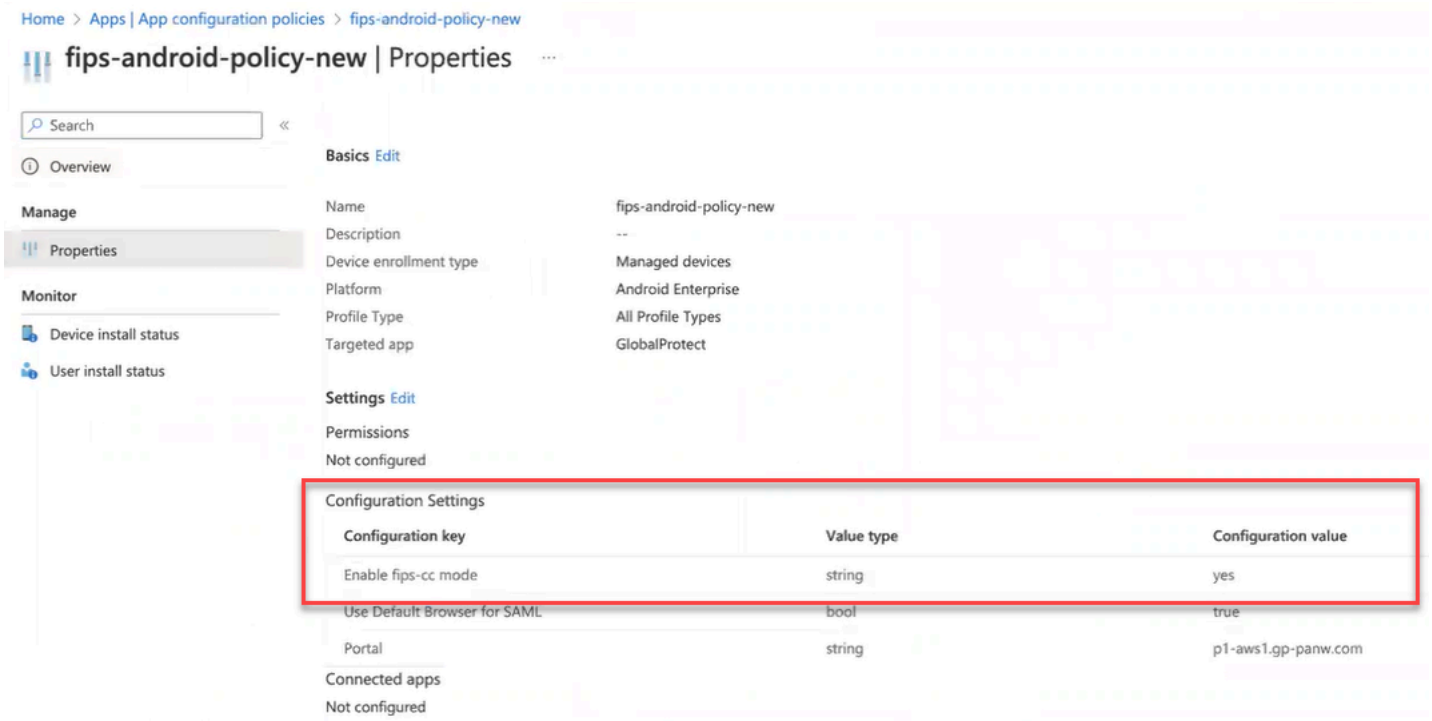
6. Cliquez sur **Review and Save (Réviser et enregistrer)**. La page Modifier les politiques de configuration des applications affiche les nouveaux paramètres de configuration `Enable-fips-cc-mode` ajoutés.



Le paramètre de configuration pour activer le mode fips-cc est également affiché dans la zone des paramètres de configuration (**APPS** > **Policy (Politique)** > **App configuration**

 ©2026 Palo Alto Networks, Inc.

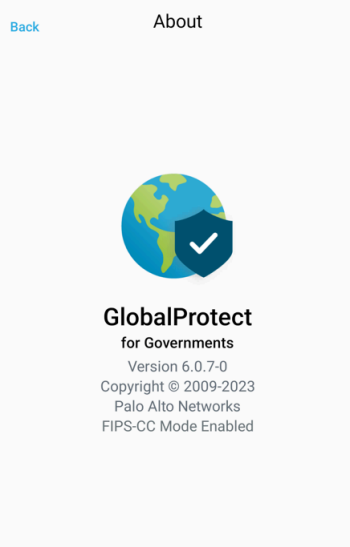
policies (Politiques de configuration des applications) > <policy> > Properties (Propriétés).



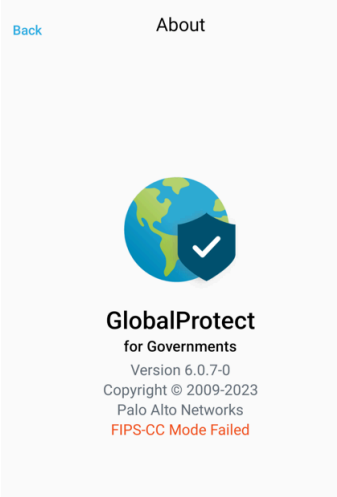
Après avoir activé le mode FIPS-CC sur la console Microsoft Intune et synchronisé le périphérique avec Microsoft Intune, la console pousse la configuration mise à jour du mode FIPS-CC vers les terminaux Android.

©2026 Palo Alto Networks, Inc.

2. Vérifiez que le mode FIPS-CC est bien activé sur un terminal Android.
   1. Lancez l'application GlobalProtect.
   2. À partir du panneau d'état, ouvrez le dialogue des paramètres (⚙).
   3. Sélectionnez **About (À propos)**.
   4. Vérifiez que le mode FIPS-CC est activé. Si le mode FIPS-CC est activé, la boîte de dialogue About (À propos) affiche l'état `FIPS-CC Mode Enabled`.



Si le mode FIPS-CC n'a pas pu être activé avec succès, la boîte de dialogue À propos affiche le statut `FIPS-CC Mode Failed (Échec du mode FIPS-CC)`.



3. Affichez les journaux pour consulter les journaux de l'application GlobalProtect liés au mode FIPS-CC sur les terminaux Android.

4. Affichez, collectez et envoyez les journaux à l'administrateur pour déboguer et résoudre les problèmes liés au mode FIPS-CC sur les périphériques Android.

 ©2026 Palo Alto Networks, Inc.

Fonctions de sécurité FIPS-CC

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect 6.0.7 ou une version ultérieure de 6.0.x. Pour iOS et Android, application GlobalProtect pour les gouvernements 6.0.7 ou une version ultérieure de l'application GlobalProtect pour les gouvernements 6.0.x. Mode FIPS-CC pour GlobalProtect sur Windows et macOS, périphériques basés sur ARM fonctionnant sous Windows et macOS, iOS, Android et Linux.

Lorsque vous activez le mode FIPS-CC pour GlobalProtect, les fonctions de sécurité suivantes sont appliquées à toutes les applications GlobalProtect gérées sur les terminaux Windows, macOS, iOS, Android et Linux :

- Vous devez configurer la passerelle pour chiffrer tous les tunnels VPN entre l'application GlobalProtect et les passerelles à l'aide de TLS ou IPSec.
- Lors de la configuration d'un tunnel VPN IPSec sur la passerelle, vous devez sélectionner une option suite de cryptage présentée lors de la configuration IPSec.
- Lorsque vous configurez un tunnel VPN IPSec sur la passerelle, vous pouvez spécifier l'un des algorithmes de chiffrement suivants :
  - AES-CBC-128 (avec l'algorithme d'authentification HMAC-SHA-1)
  - AES-GCM-128
  - AES-GCM-256
- Les certificats du serveur et clients doivent utiliser l'un des algorithmes de signature suivants :
  - RSA 2048 bit (ou plus grand)
  - ECDSA P-256
  - ECDSA P-384
  - ECDSA P-521

  De plus, vous devez utiliser un algorithme de hachage de signature SHA-256, SHA-384 ou SHA-512.

 ©2026 Palo Alto Networks, Inc.

- L'application GlobalProtect appliquera des vérifications strictes de vérification X.509v3 sur le certificat du serveur.
  - Les vérifications sont basées sur les exigences de validation et d'authentification des certificats FIA_X509_EXT.1 et FIA_X509_EXT.2 de NIAP.

 ©2026 Palo Alto Networks, Inc.

Résolution des problèmes du mode FIPS-CC

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (géré par Panorama)	Licence d'abonnement GlobalProtect™ PAN-OS 8.1 ou une version ultérieure de PAN-OS. Application GlobalProtect 6.0.7 ou une version ultérieure de 6.0.x. Pour iOS et Android, application GlobalProtect pour les gouvernements 6.0.7 ou une version ultérieure de l'application GlobalProtect pour les gouvernements 6.0.x. Mode FIPS-CC pour GlobalProtect sur Windows et macOS, périphériques basés sur ARM fonctionnant sous Windows et macOS, iOS, Android et Linux.

La section suivante décrit les problèmes éventuels du mode FIPS-CC et les solutions correspondantes. Si vous éprouvez des problèmes qui ne sont pas décrits ci-dessous, veuillez communiquer avec votre administrateur GlobalProtect™ pour obtenir de l'aide relativement à leur résolution.

Affichez la page d'état pour suivre l'état des FIPS et CC.

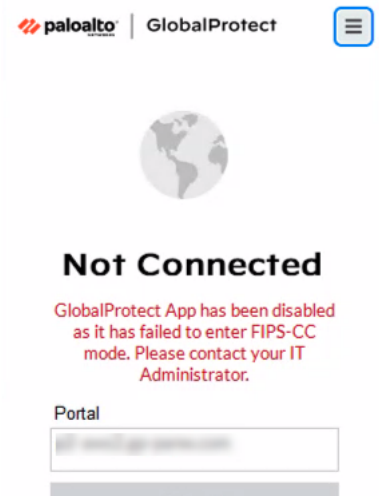
- **Problème :**

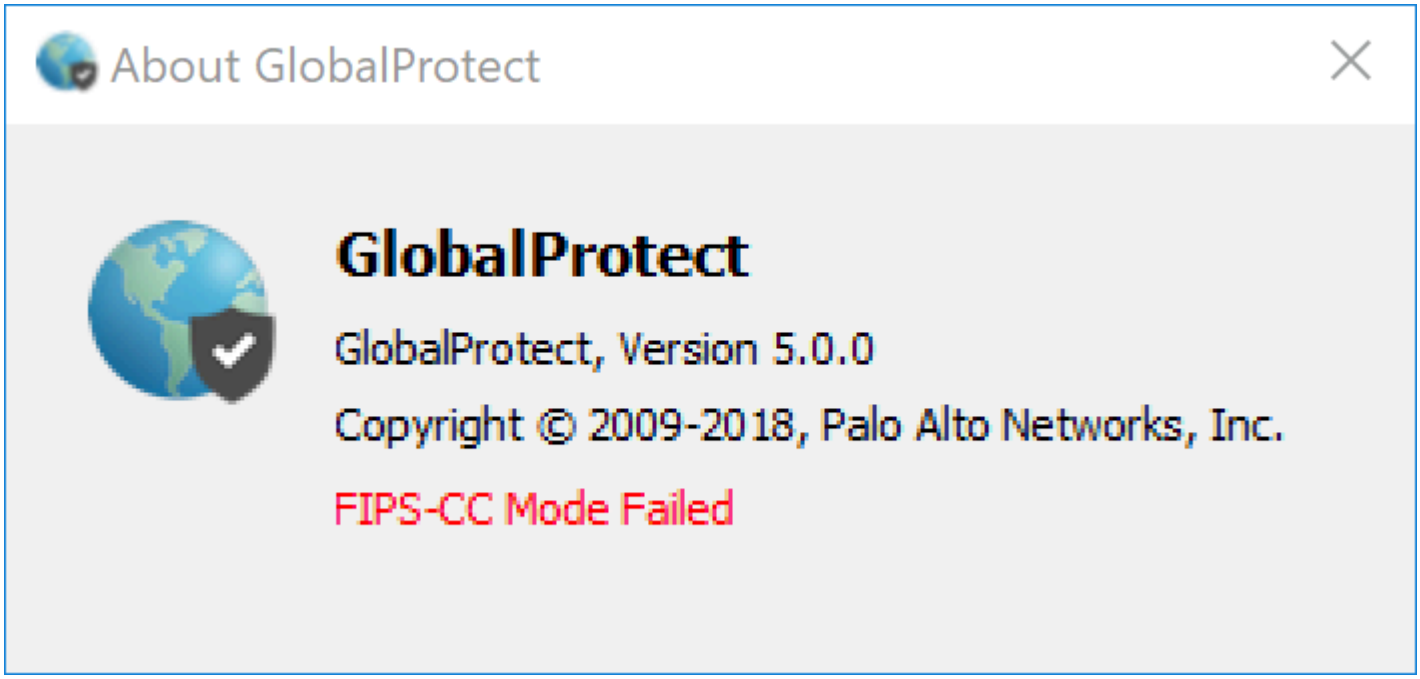
  L'application GlobalProtect n'arrive pas à initialiser le mode FIPS-CC en raison de l'échec d'un test d'intégrité ou d'un test automatique à la mise sous tension (POST) FIPS.

  - **Description :** Après avoir activé le mode FIPS-CC, l'application GlobalProtect effectue les tests automatiques à la mise sous tension (POST) FIPS et les tests d'intégrité lors de l'initialisation des applications et des redémarrages des systèmes ou des applications. En cas

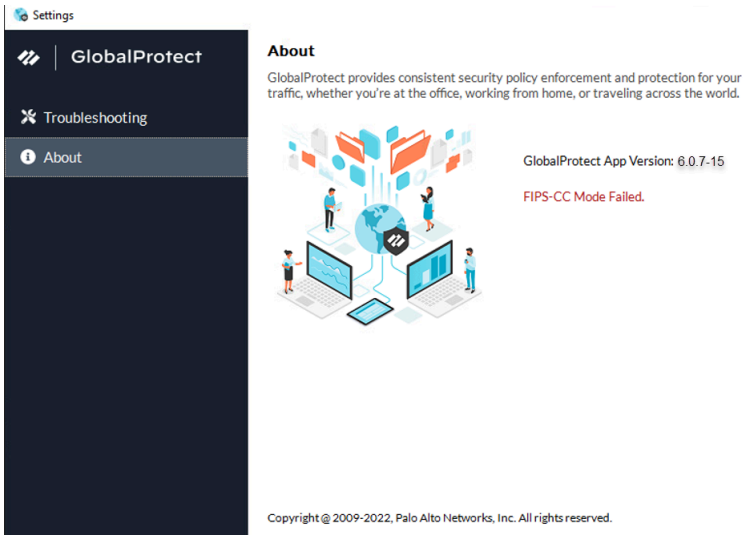
©2026 Palo Alto Networks, Inc.

d'échec de l'un de ces tests, l'application GlobalProtect est désactivée et le fenêtre About (À propos) affiche le message d'erreur `FIPS-CC Mode Failed` :





 ©2026 Palo Alto Networks, Inc.



  - **Resolution: (Résolution :)** Redémarrez l'application pour supprimer la condition d'erreur. Si le problème persiste, désinstallez l'application, puis réinstallez-la.

- **Problème :**

  L'application GlobalProtect n'arrive pas à établir une connexion au mode FIPS-CC en raison de l'échec d'un test automatique des conditions FIPS.

  - **Description :** Après l'initialisation de l'application GlobalProtect en mode FIPS-CC, elle effectue les tests automatiques des conditions FIPS. En cas d'échec des tests automatiques, l'application GlobalProtect met fin à la session et demeure déconnectée.
    - **Resolution: (Résolution :)** Pour établir une connexion à GlobalProtect, vous devez vous réauthentifier auprès du portail GlobalProtect et activez de nouveau le mode FIPS-CC.

  *Si GlobalProtect n'arrive pas à s'initialiser ou de se connecter en mode FIPS-CC, vous pouvez accéder à l'onglet **Troubleshooting (Résolution des problèmes)** du panneau des paramètres GlobalProtect pour afficher et collecter les journaux à des fins de résolution des problèmes. Tous les autres onglets demeurent indisponibles tant que GlobalProtect n'est pas connecté.*

Les tableaux suivants répertorient les messages d'erreur affichés lorsque la validation des certificats échoue pour les plateformes Windows et macOS. Les administrateurs peuvent afficher les messages d'erreur pour le dépannage et la résolution des problèmes.

Validation certification FIPS-CC	Messages d'erreur
Certificat d'autorité de certification racine fiable introuvable.	Échec de la validation du certificat X.509v3 : Le certificat de portail n'est pas signé par une autorité de certification de confiance.
Certificat CA expiré.	Échec de la validation du certificat X.509v3 : Le certificat du portail n'est pas dans sa période de validité.

 ©2026 Palo Alto Networks, Inc.

Validation certification FIPS-CC	Messages d'erreur
Certificat CA révoqué.	Échec de la validation du certificat X509v3. Certificat révoqué.
Indicateur CA basicConstraints du certificat CA introuvable.	**Windows** : Échec de la validation du certificat X.509v3. Indicateur basicConstraints du certificat CA introuvable ou invalide. **macOS** : Extension des contraintes de base requise par la politique, mais non présente.
Indicateur CA basicConstraints du certificat CA défini sur « Faux ».	BasicConstraintsCA = 0;StatusCodes = ("-2147408893")
EC Paramètre Explicite manquant.	Erreur FIPS-CC : Certificat de mode FIPS-CC non conforme. Certificat ECDSA avec paramètres EC explicites.
CA intermédiaire avec des contraintes de base manquantes.	**Windows** : Échec de la validation du certificat X.509v3. Indicateur basicConstraints du certificat CA introuvable ou invalide. **macOS** : Extension des contraintes de base requise par la politique, mais non présente.
Certificat CA sans but de signature CA en intermédiaire.	**Windows** : Échec de la validation du certificat X509v3. Indicateur basicConstraints du certificat CA introuvable ou invalide. **macOS** : Utilisation de clé non valide pour la politique.
Certificat CA sans but de signature CA.	**Windows** : Échec de la validation du certificat X.509v3. Champ caSigning manquant dans la chaîne CA. **macOS** : Échec de la validation du certificat X.509v3. Certificat de CA racine approuvé introuvable. KeyUsage = 0;StatusCodes = ("-2147408890")
Validation de certificat pour certificat révoqué.	Échec de la validation du certificat X.509v3 : Le certificat n'est pas conforme à la norme FIPS. Veuillez accéder aux journaux du système pour plus d'informations.
Validation du certificat avec un certificat sans bit d'utilisation de clé cRLsign défini.	Échec de la validation du certificat X.509v3. Absence de l'objet CRL Sign dans le champ KeyUsage (étendu).

©2026 Palo Alto Networks, Inc.

Validation certification FIPS-CC	Messages d'erreur
Validation du certificat (OCSP) pour le certificat client GlobalProtect révoqué	La connexion a échoué : Un certificat valide est nécessaire à des fins d'authentification. Si le problème persiste, veuillez contacter votre administrateur.
Validation de certificat (OCSP) pour un certificat manquant à des fins de signature OCSP	Échec de la validation du certificat de signature OCSP X.509v3. Champ d'utilisation de clé étendue manquant.
Validation de certificat avec OCSP lorsque le serveur est injoignable.	Échec de la validation du certificat X509v3. Lecture/accès pour OCSP ou CRL a échoué.

Validation du certificat du serveur	Messages d'erreur
Pris en charge SHA-256, SHA-384, and SHA-512 only. La connexion échoue si un autre algorithme est utilisé (par exemple MD5). Les certificats avec SHA-1 ne sont pas autorisés.	Échec de la pré-connexion au <portal> avec la valeur de retour 0(0).
Clé RSA : Échec lorsque la longueur est inférieure à 2048	Échec de la pré-connexion au <portal> avec la valeur de retour 0(0).
Clé ECDSA : Défaillance lorsque la longueur n'est pas P-256/384/521.	Échec de la pré-connexion au <portal> avec la valeur de retour 0(0).
Échec de l'exposant de clé RSA.	**Windows** : Erreur FIPS-CC : Certificat de mode FIPS-CC non conforme. **macOS** : CSSMERR_CSP_UNSUPPORTED_KEY_SIZE
Le certificat serveur a expiré.	Échec de la validation du certificat X.509v3 : Le certificat du portail n'est pas dans sa période de validité.
Certificat serveur (OCSP) révoqué.	Échec de la validation du certificat X509v3. Certificat révoqué.
Échec de connexion lorsque le champ Utilisation étendue de la clé est manquant dans le certificat serveur.	Échec de la pré-connexion au <portal> avec la valeur de retour 0(0).

 ©2026 Palo Alto Networks, Inc.

Validation du certificat du serveur	Messages d'erreur
Échec de connexion lorsque le but de l'authentification du serveur est manquant dans le champ Clé étendue utilisée.	Échec de la pré-connexion au <portal> avec valeur de retour 0(0).

Les tableaux suivants répertorient les messages d'erreur affichés lorsque la validation du certificat échoue pour la plateforme iOS. Dans certains cas, les messages d'erreur affichés sont légèrement différents des messages d'erreur attendus tels qu'indiqués dans le tableau. Les administrateurs peuvent afficher les messages d'erreur pour le dépannage et la résolution des problèmes.

Validation certification FIPS-CC	Messages d'erreur
Utilisation clé manquante Objectif de signature CA.	Impossible de construire un certificat de chaîne à racine.
Clé RSA : Échec lorsque la longueur est inférieure à 2048. Un ou plusieurs certificats utilisent un algorithme de signature faible.	
Clé RSA : défaillance lorsque le certificat serveur 1 024 bits est utilisé. Un ou plusieurs certificats utilisent une taille de clé faible.	
Champ Utilisation étendue de la clé manquant.	Échec de la validation du certificat X.509v3. Champ Utilisation de clé la étendue manquant.
Le certificat de serveur de vérification doit avoir serverAuth dans EKU.	Exigences politiques non respectées.
La vérification du certificat client doit avoir clientAuth dans EKU.	Échec de la validation du certificat X.509v3. Le certificat CA « Signature CA » est absent, mais basicConstraints peut être valide ou non.
Le chemin de certification mène à une racine non fiable ou un certificat CA dans le chemin a expiré ou a été révoqué.	Échec de la validation du certificat X509v3. Certificat de CA racine approuvé introuvable.
Contraintes de base manquantes	Échec de la validation du certificat X509v3. Certificat de CA racine approuvé introuvable.

 ©2026 Palo Alto Networks, Inc.

Validation certification FIPS-CC	Messages d'erreur
Indicateur basicConstraints du certificat CA non défini sur True.	Impossible de construire un certificat de chaîne à racine.
Certificat expiré	Un ou plusieurs certificats ont expiré ou ne sont pas encore valides.
Certificat révoqué	Un ou plusieurs certificats ont expiré ou ne sont pas encore valides.
Algorithme faible utilisé	Un ou plusieurs certificats utilisent un algorithme de signature faible .
Champ de signature CA manquant	Exigences de la politique non respectées.
Lecture/accès pour la CRL	Échec de la validation du certificat X509v3. Lecture/accès pour OCSP ou CRL a échoué.
Lecture/accès pour échec OCSP	Échec de la validation du certificat X509v3. Lecture/accès pour OCSP ou CRL a échoué.
La validation du certificat OCSP a échoué.	Échec de la validation du certificat X509v3. Certificat révoqué.
Objectif de signature OCSP manquant dans le champ ExtendedKeyUsage .	Échec de la validation du certificat de signature OCSP X.509v3. Champ Utilisation de clé la étendue manquant.
Validation du certificat OCSP pour le certificat client GlobalProtect révoqué	Échec de la validation du certificat X509v3. Certificat révoqué.
Certificat révoqué : certificat serveur (OCSP)	Échec de la validation du certificat X509v3. Certificat révoqué.

 ©2026 Palo Alto Networks, Inc.

 ©2026 Palo Alto Networks, Inc.

Cryptographie de GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect prend en charge les modes de tunnel IPsec et SSL. GlobalProtect prend également en charge la possibilité d'activer et de demander à l'application GlobalProtect de toujours tenter d'établir un tunnel IPsec avant de revenir au tunnel SSL. Avec un tunnel IPsec, l'application GlobalProtect utilise SSL/TLS pour échanger les algorithmes de chiffrement et d'authentification et les clés. La sélection de la suite de chiffrement utilisée par GlobalProtect pour sécuriser le tunnel SSL/TLS dépend des éléments suivants :

- **Versions SSL/TLS acceptées par la passerelle** : le portail et les passerelles GlobalProtect peuvent restreindre la liste des suites de chiffrement disponibles pour l'application en utilisant les profils SSL/TLS. Sur le pare-feu, créez le profil SSL/TLS en spécifiant le certificat et les versions de protocole autorisées, et associez-le au portail et à la passerelle GlobalProtect.
- **Algorithme du certificat de serveur de la passerelle** : le système d'exploitation du point de terminaison détermine les suites de chiffrement que l'application GlobalProtect inclut dans son message Client Hello. Tant que l'application GlobalProtect inclut la suite de chiffrement que la passerelle préfère utiliser, la passerelle sélectionnera cette suite de chiffrement pour la session SSL. L'ordre des suites de chiffrement dans le message Client Hello n'a aucune incidence sur la sélection de la suite de chiffrement : La passerelle sélectionne la suite de chiffrement en fonction du profil de service SSL/TLS et de l'algorithme du certificat de serveur de passerelle et sa liste préférée. Vous sélectionnez le profil de service dans la configuration de l'authentification de la passerelle GlobalProtect.

Échange de chiffrement entre l'application GlobalProtect et la passerelle

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

La figure suivante montre l'échange de chiffrement entre les passerelles GlobalProtect et les applications GlobalProtect lors de la création du tunnel VPN.

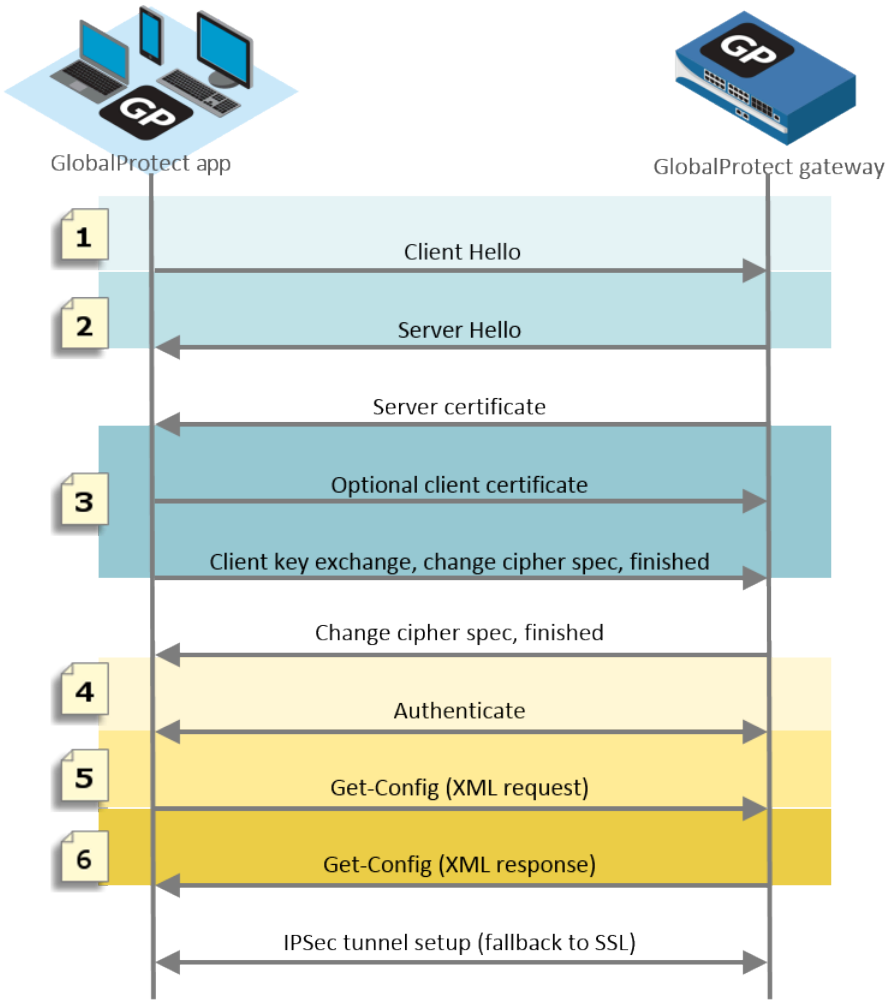


Illustration 5 : Échange de chiffrement entre l'application et la passerelle

Le tableau suivant décrit ces étapes plus en détail.

©2026 Palo Alto Networks, Inc.

Tableau 12 : Échange de chiffrement entre l'application et la passerelle

Étape de communication	Description
1. Hello client	L'application propose une liste de suites de chiffrement en fonction du système d'exploitation du point de terminaison.
2. Hello serveur	La passerelle sélectionne la suite de chiffrement proposée par l'application. Lors de la sélection des chiffrements pour configurer le tunnel, la passerelle ignore à la fois le nombre et l'ordre des suites de chiffrement proposées par l'application et s'appuie plutôt sur les versions SSL/TLS et l'algorithme du certificat de serveur de passerelle et sa liste préférée (tel que décrit à la section À propos de la sélection de chiffrement GlobalProtect).
3. Certificat client facultatif	La passerelle peut éventuellement demander à l'application un certificat client à utiliser pour approuver l'identité de l'utilisateur ou du point de terminaison.
4. Session SSL	Après la configuration de la session SSL/TLS, l'application s'authentifie auprès de la passerelle et demande la configuration de la passerelle (Get-Config-Request). Pour demander la configuration, l'application propose les algorithmes de chiffrement et d'authentification et d'autres paramètres tels que l'adresse IP préférée pour l'interface du tunnel. La passerelle répond à la demande et sélectionne l'algorithme de chiffrement et d'authentification à utiliser en fonction de la configuration du profil Crypto IPSec GlobalProtect (Get-Config-Response).

Le tableau suivant présente un exemple d'échange de chiffrement entre une application sur un point de terminaison MacOS et la passerelle.

Tableau 13 : Exemple : Échange de chiffrement pour les postes de travail macOS

Étape de communication	Exemple : postes de travail macOS
1. Hello client	TLS 1.2 37 suites de chiffrement ()
2. Hello serveur	• Lorsque GlobalProtect utilise un certificat ECDSA et que TLS 1.2 est accepté, la session SSL utilise ECDSA-AES256-CBC-SHA. • Lorsque GlobalProtect utilise un certificat RSA et que TLS 1.2 est accepté, la session SSL utilise RSA-AES256-CBC-SHA256.

 ©2026 Palo Alto Networks, Inc.

Étape de communication	Exemple : postes de travail macOS
3. Certificat client facultatif	Certificats clients signés avec ECDSA ou RSA et utilisant SHA1, SHA256 ou SHA384

4. Session SSL	• La session SSL utilise ECDSA-AES256-CBC-SHA ou RSA-AES256-CBC-SHA256
	• Get-Config-Request
	  • Chiffrement : AES-256-GCM, AES-128-GCM, AES-128-CBC
	  • Authentification : type de système d'exploitation et SHA1, adresse IP préférée, etc.
	• Get-Config-Response
	  • SPI client à serveur et serveur à client, clés de chiffrement et clés d'authentification
	  • Type de tunnel, ports, mode tunnel segmenté, IP et DNS, etc.

 ©2026 Palo Alto Networks, Inc.

Fonctions cryptographiques de l’application GlobalProtect

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l’abonnement Utilisateur mobile

L'application GlobalProtect utilise la bibliothèque OpenSSL 1.0.1h pour établir une communication sécurisée avec le portail GlobalProtect et les passerelles GlobalProtect. Le tableau suivant répertorie chaque fonction d'application GlobalProtect qui nécessite une fonction cryptographique et les clés cryptographiques utilisées par l'application GlobalProtect :

Fonction crypto	Clé	Usage
WinHTTP (Windows) et NSURLConnection (MacOS) AES256-SHA	Clé dynamique négociée entre l'application GlobalProtect et le portail et/ou la passerelle GlobalProtect pour établir une connexion HTTPS.	Utilisée pour établir la connexion HTTPS entre l'application GlobalProtect et le portail et/ou la passerelle GlobalProtect pour l'authentification.
OpenSSL AES256-SHA	Clé dynamique négociée entre l'application GlobalProtect et le portail et/ou la passerelle GlobalProtect pendant la négociation SSL.	Utilisée pour établir la connexion SSL entre l'application GlobalProtect et la passerelle GlobalProtect pour l'envoi du rapport HIP, la négociation de tunnel SSL et la découverte réseau.
Cryptage et authentification IPSec aes-128-sha1, aes-128-cbc, aes-128-gcm, and aes-256-gcm	Clé de session envoyée par la passerelle GlobalProtect.	Utilisée pour définir le tunnel IPSec entre l'application GlobalProtect et la passerelle GlobalProtect. Utilisez l'algorithme le plus fort supporté par votre réseau (AES-GCM est recommandé). Pour assurer l’intégrité des données et la protection d’authenticité, le chiffrement AES-128-CBC requiert l’algorithme d’authentification SHA1. Étant donné que les algorithmes de chiffrement

 ©2026 Palo Alto Networks, Inc.

Fonction crypto	Clé	Usage
		AES-GCM (AES-128-GCM et AES-256-GCM) fournissent nativement la protection d'intégrité ESP, l'algorithme d'authentification SHA1 est ignoré pour ces chiffres, même s'il est nécessaire pendant la configuration.

 ©2026 Palo Alto Networks, Inc.

Suites de chiffrement TLS prises en charge par les applications GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Les sections suivantes fournissent des exemples de ciphers TLS pris en charge sur les applications GlobalProtect installées sur divers systèmes d'exploitation des terminaux. Les listes ne sont pas exhaustives pour tous les systèmes d'exploitation pris en charge.

Les renégociations (sécurisées ou non sécurisées) ne sont pas prises en charge.

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison MacOS

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison MacOS	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)

 ©2026 Palo Alto Networks, Inc.

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison MacOS	
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
	TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
	TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_RSA_WITH_RC4_128_MD5 (0x0004)

Chiffrements TLS ajoutés à la prise en charge de TLSv 1.3 pour les applications GlobalProtect sur les terminaux macOS	
TLS_AES_128_GCM_SHA256	TLS_CHACHA20_POLY1305_SHA256
TLS_AES_256_GCM_SHA384	

Chiffrements TLS pris en charge par les agents GlobalProtect sur les terminaux Windows 7

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Windows 10	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)

 ©2026 Palo Alto Networks, Inc.

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Windows 10	
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Chiffrements TLS ajoutés à la prise en charge de TLSv 1.3 pour les applications GlobalProtect sur les terminaux Windows 11	
TLS_AES_128_GCM_SHA256	TLS_CHACHA20_POLY1305_SHA256
TLS_AES_256_GCM_SHA384	

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Android 6.0.1

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Android 6.0.1	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)

 ©2026 Palo Alto Networks, Inc.

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Android 6.0.1	
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison iOS 10.2.1

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison iOS 10.2.1	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

 ©2026 Palo Alto Networks, Inc.

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison iOS 10.2.1	
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Chiffrements TLS pris en charge par les applications GlobalProtect sur les Chromebooks

Chiffrements TLS pris en charge par les applications GlobalProtect sur les Chromebooks (Chrome OS 55.0.2883)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0085)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x0068)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)

 ©2026 Palo Alto Networks, Inc.

Chiffrements TLS pris en charge par les applications GlobalProtect sur les Chromebooks (Chrome OS 55.0.2883)	
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
TLS_DH_DSS_WITH_AES_256_CBC_SHA (0x0036)	TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4)
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0)
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0086)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_DH_RSA_WITH_AES_128_CBC_SHA256 (0x003f)	TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e)	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)	TLS_RSA_WITH_IDEA_CBC_SHA (0x0007)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x0031)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DH_DSS_WITH_AES_128_CBC_SHA (0x0030)	TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)	TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)	TLS_RSA_WITH_RC4_128_SHA (0x0005)
TLS_DH_RSA_WITH_SEED_CBC_SHA (0x0098)	TLS_RSA_WITH_RC4_128_MD5 (0x0004)
TLS_DH_DSS_WITH_SEED_CBC_SHA (0x0097)	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)

©2026 Palo Alto Networks, Inc.

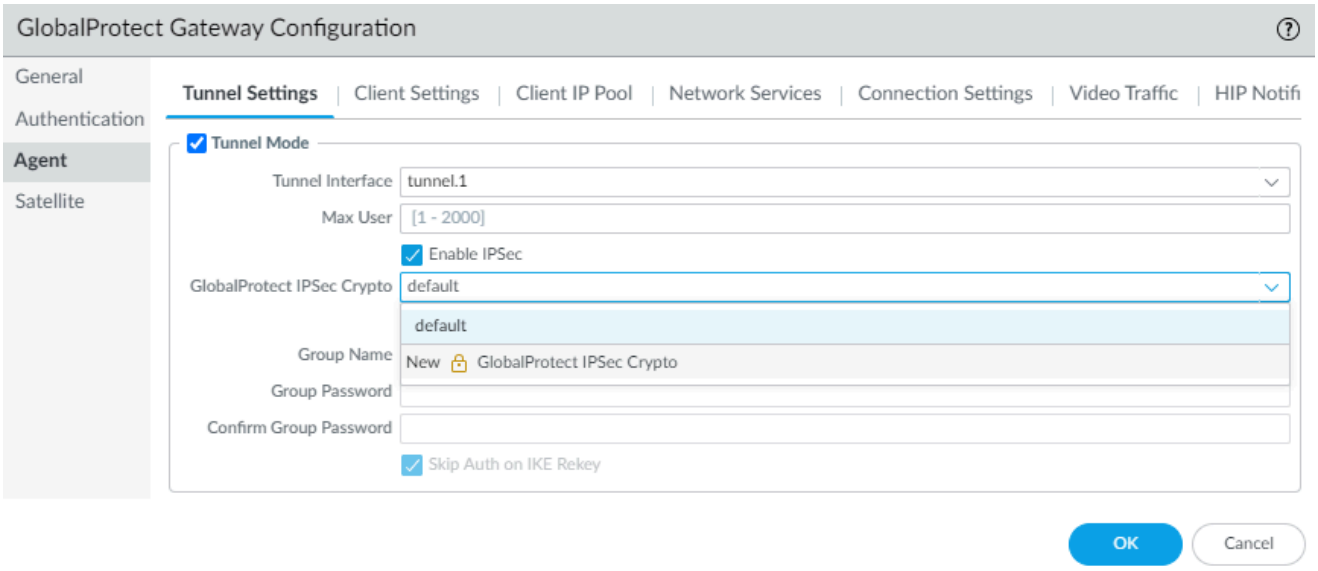
Chiffrements TLS pris en charge par les applications GlobalProtect sur les Chromebooks (Chrome OS 55.0.2883)	
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0043)	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA (0x0010)
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0042)	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA (0x000d)
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)	TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_DH_RSA_WITH_DES_CBC_SHA (0x000f)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)	TLS_DH_DSS_WITH_DES_CBC_SHA (0x000c)
	TLS_RSA_WITH_DES_CBC_SHA (0x0009)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

 ©2026 Palo Alto Networks, Inc.

Chiffrements utilisés pour configurer les tunnels IPsec

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect peut restreindre et/ou définir un ordre préférentiel pour l'algorithme de chiffrement et d'authentification que l'application GlobalProtect peut utiliser pour le tunnel IPsec. Les algorithmes et les préférences sont définis dans le profil **GlobalProtect IPSec Crypto (Crypto IPSec GlobalProtect)** que vous avez configuré lors de l'établissement du tunnel pour la passerelle GlobalProtect (**Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > **<gateway-config>** > **GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect)** > **Agent** > **Tunnel Settings (Paramètres de tunnels)**).



Lorsque l'application GlobalProtect établit une session SSL avec une passerelle GlobalProtect, la suite de chiffrement utilisée pour cette session SSL est régie par le profil SSL/TLS configuré sur la passerelle et le type d'algorithme utilisé par le certificat de passerelle. Une fois la session SSL établie, l'application GlobalProtect lance une configuration de tunnel VPN en demandant la configuration via SSL.

En utilisant la même session SSL, la passerelle GlobalProtect répond avec les algorithmes de chiffrement et d'authentification, les clés et les SPI que l'application doit utiliser pour configurer le tunnel IPsec.

> *AES-GCM est recommandé pour des exigences plus sécurisées. Pour assurer l'intégrité des données et la protection d'authenticité, le chiffrement AES-128-CBC requiert l'algorithme d'authentification SHA1. Étant donné que les algorithmes de chiffrement AES-GCM (AES-128-GCM et AES-256-GCM) fournissent nativement la protection d'intégrité ESP, l'algorithme d'authentification SHA1 est ignoré pour ces Ciphers, même s'il est nécessaire pendant la configuration.*

 ©2026 Palo Alto Networks, Inc.

Le profil **Crypto IPSec GlobalProtect** que vous configurez sur la passerelle détermine l'algorithme de cryptage et d'authentification utilisé pour configurer le tunnel IPsec. La passerelle GlobalProtect répond avec le premier algorithme de chiffrement correspondant répertorié dans le profil qui correspond à la proposition de l'application.

L'application GlobalProtect tente ensuite de configurer un tunnel en fonction de la réponse de la passerelle.

 ©2026 Palo Alto Networks, Inc.

API SSL

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW géré par Panorama	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

GlobalProtect utilise à la fois OpenSSL et les API système natives pour effectuer les connexions SSL. Les opérations telles que la mesure de la latence de la passerelle GlobalProtect (utilisée par GlobalProtect pour sélectionner la meilleure passerelle), la déconnexion de la passerelle et la transmission du message et du rapport de vérification HIP sont toutes effectuées via des sessions SSL configurées à l'aide de la bibliothèque OpenSSL. Les opérations telles que la pré-connexion à la passerelle, la connexion et get-config sont effectuées via des sessions SSL configurées à l'aide de l'API système native.

 ©2026 Palo Alto Networks, Inc.

Configurations rapides GlobalProtect

Les sections suivantes fournissent des instructions pas à pas pour la configuration de certains déploiements GlobalProtect™ communs :

- VPN d'accès à distance (Profil d'authentification)
- VPN d'accès à distance (profil de certificat)
- VPN d'accès à distance avec l'authentification à deux facteurs
- Configuration de VPN toujours active
- VPN d'accès à distance avec pré-ouverture de session
- Configuration de plusieurs passerelles GlobalProtect
- GlobalProtect pour l'archivage HIP interne et l'accès basé sur l'utilisateur
- Configuration mixte de passerelles internes et externes
- Portail captif et application de GlobalProtect pour l'accès au réseau
- GlobalProtect sur les PC Cloud Windows 365

Reportez-vous à l'article de la base de données de connaissances à l'adresse https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClGYCA0 pour des informations sur la façon dechange the Active Directory password using GlobalProtect (modifier le mot de passe de l'annuaire à l'aide de GlobalProtect).

VPN d'accès à distance (Profil d'authentification)

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans le VPN GlobalProtect pour l'accès à distance, le portail GlobalProtect et la passerelle sont configurés sur **ethernet1/2**, il s'agit donc de l'interface physique où les utilisateurs GlobalProtect se connectent. Dès qu'un utilisateur se connecte et s'authentifie au portail et à la passerelle, le point de terminaison établit un tunnel depuis sa carte virtuelle, à laquelle une adresse IP a été assignée dans le pool d'adresses IP associé à la configuration de tunnel.2 de passerelle : 10.31.32.3-10.31.32.118 dans cet exemple. Comme les tunnels VPN GlobalProtect se terminent dans une zone **`corp-vpn`** séparée, vous avez une visibilité du trafic de connexion ainsi que la capacité à personnaliser les politiques de sécurité pour les utilisateurs distants.

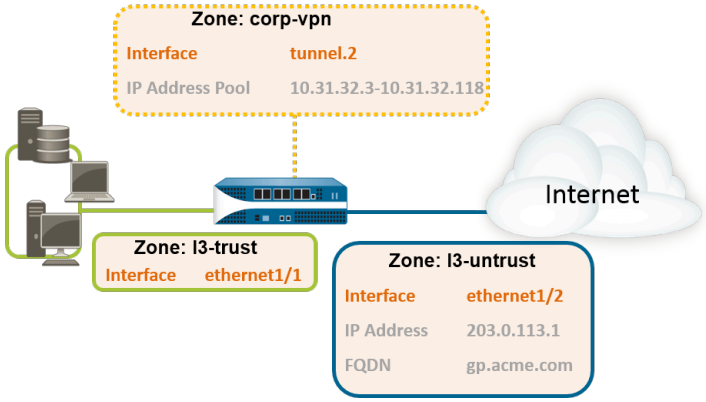


Illustration 6 : VPN GlobalProtect pour l'accès à distance

1. (Requis uniquement sur NGFW géré par Panorama ou Strata Cloud Manager)Créez des interfaces et des zones pour GlobalProtect.

   *Utilisez le routeur virtuel **default (par défaut)** pour toutes les configurations d'interface pour éviter d'avoir à créer un routage inter-zone.*

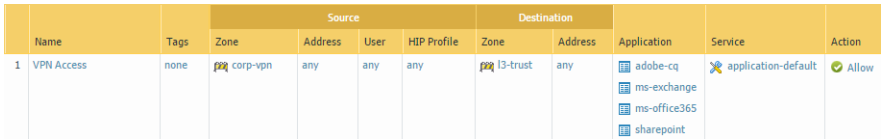
   - Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**. Configurez **ethernet1/2** en tant qu'interface de Couche 3 comportant une adresse IP 203.0.113.1, puis affectez-la à la **Security Zone (Zone de sécurité)** **`l3-untrust`** et au **Virtual Router (Routeur virtuel)** par défaut.
   - Créez un dossier « A » DNS qui mappe l'adresse IP **`203.0.113.1`** en **`gp.acme.com.`**
   - Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** et **Add (Ajouter)** une interface **tunnel.2**. **Add (Ajoutez)** l'interface de tunnel à une nouvelle **Security Zone (Zone**

 ©2026 Palo Alto Networks, Inc.

de sécurité) nommée **`corp-vpn`**, puis affectez-la au **`Virtual Router (Routeur virtuel)`** par défaut.

- Activez l'identification de l'utilisateur sur la zone **`corp-vpn`**.

2. Créez des politiques de sécurité pour autoriser le flux de trafic entre la zone **`corp-vpn`** et la zone **`l3-trust`**, ce qui autorise l'accès à vos ressources internes.
   1. Choisissez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajouter)** une nouvelle règle.
      - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** puis **Add (Ajouter)** une nouvelle règle.
      - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** puis **Add (Ajouter)** une nouvelle règle.
   2. Pour cet exemple, vous devriez définir la règle avec les paramètres suivants :
      - **Name (Nom)** (onglet **General (Général)**) : accès VPN
      - **Source Zone (Zone source)** (onglet **Source**) : corp-vpn
      - **Destination Zone (Zone de destination)** (onglet **Destination**) : l3-trust



3. Utilisez l'une des méthodes suivantes pour obtenir un certificat de serveur pour l'interface qui héberge le portail GlobalProtect et la passerelle :

- (Recommandé)Importez un certificat de serveur d'une autorité de certification tierce reconnue.
- Utilisez l'autorité de certification racine sur le portail pour générer un certificat de serveur auto-signé.

Gérez les certificats comme suit :

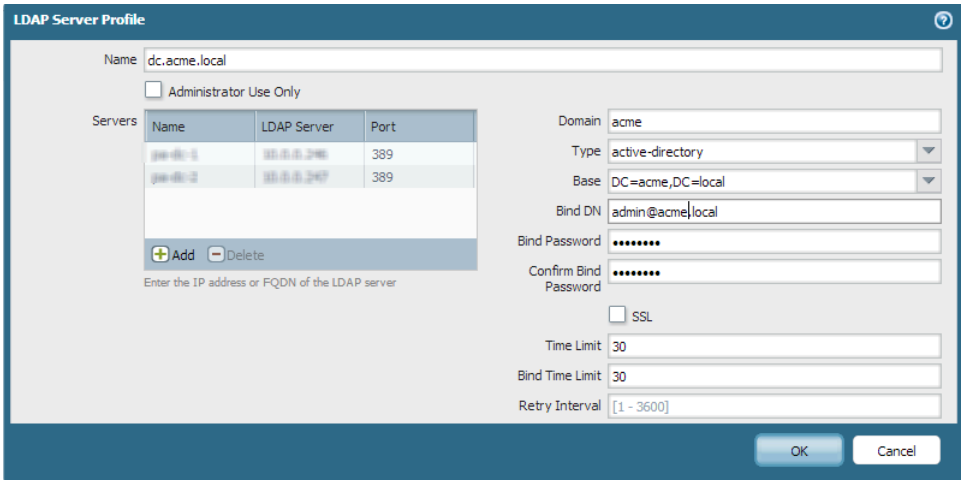
- Obtenez un certificat de serveur. Comme le portail et la passerelle sont sur la même interface, le même certificat de serveur peut être utilisé pour les deux composants.
- Le CN du certificat doit correspondre au FQDN, `gp.acme.com`.
- Pour permettre aux utilisateurs de se connecter au portail sans recevoir d'erreur de certificat, utilisez un certificat de serveur généré par une AC publique.

4. Créez un profil de serveur pour se connecter au serveur LDAP.

Le profil de serveur indique au pare-feu comment se connecter au service d'authentification. Les méthodes d'authentification locale, RADIUS, Kerberos, SAML et LDAP sont prises en

 ©2026 Palo Alto Networks, Inc.

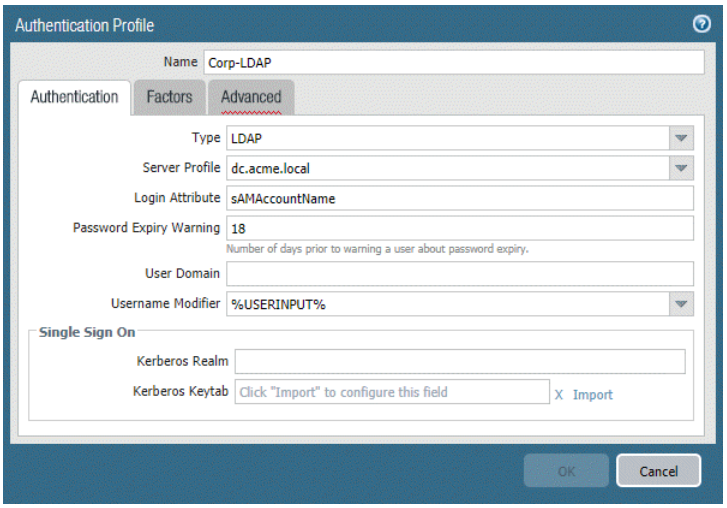
charge. Cet exemple décrit un profil d'authentification LDAP pour authentifier les utilisateurs par rapport à Active Directory.



5. (Facultatif) Créez un profil d'authentification.

Ajoutez le profil de serveur TACACS+ à un profil d'authentification :

- Sur Panorama, sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**.
- Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication Profiles (Profils d'authentification)**.
- Dans Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication Profiles (Profils d'authentification)** puis **Add (Ajouter)** une nouvelle règle.



 ©2026 Palo Alto Networks, Inc.

6. Configurez une passerelle GlobalProtect avec la configuration suivante.

   Interface : **`ethernet1/2`**

   Adresse IP : **`203.0.113.1`**

   Server Certificate (Certificat Serveur) - **`GP-server-cert.pem publié par GoDaddy`**

   Authentication Profile (Profil d'authentification) : **`Corp-LDAP`**

   Tunnel Interface (Interface de tunnel) : **`tunnel.2`**

   IP Pool (Pool d'adresses IP) : **`10.31.32.3 - 10.31.32.118`**

7. Configurez un Portails GlobalProtect avec la configuration suivante :
   1. Paramétrer l'accès au portail GlobalProtect:

      Interface : **`ethernet1/2`**

      Adresse IP : **`203.0.113.1`**

      Server Certificate (Certificat Serveur) - **`GP-server-cert.pem publié par GoDaddy`**

      Authentication Profile (Profil d'authentification) : **`Corp-LDAP`**
   2. Définir les configurations d'authentification client GlobalProtect:

      Connect Method (Méthode de Connexion) : **`On-demand`** (connexion manuelle initiée par l'utilisateur)

      External Gateway Address (Adresse de passerelle externe) : **`gp.acme.com`**

8. Déployer le logiciel de l'application GlobalProtect. Suivez la procédure visant à héberger les mises à jour de l'application sur le portail.

9. (Facultatif) Activez l'utilisation de l'application mobile GlobalProtect.

   Achetez et installez un abonnement à GlobalProtect (**Device (Périphérique)** > **Licenses (Licences)**) pour activer l'utilisation de l'application.

10. Enregistrez la configuration GlobalProtect.

    Cliquez sur **Commit (Valider)**.

 ©2026 Palo Alto Networks, Inc.

VPN d'accès à distance (profil de certificat)

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Avec l'authentification de certificat, l'utilisateur doit présenter un certificat client valide qui l'identifie auprès du portail GlobalProtect ou de la passerelle. Afin de vérifier qu'un certificat de client est valide, le portail ou la passerelle vérifie si le client détient la clé privée du certificat en utilisant le message de vérification du certificat échangé au cours de la communication SSL. De plus, le certificat du client est signé par l'autorité de certification (CA) indiquée dans le champ **Issuer (émetteur)** de la chaîne de certificat. En plus du certificat lui-même, le portail ou la passerelle peut utiliser un profil de certificat pour déterminer si l'utilisateur qui a envoyé le certificat est l'utilisateur auquel le certificat a été délivré.

Lorsqu'il est utilisé en tant que procédure d'authentification unique, le certificat que l'utilisateur présente doit contenir le nom d'utilisateur dans l'un des champs du certificat ; en général le nom d'utilisateur correspond au nom commun (NC) dans le champ Sujet du certificat.

Dès que l'authentification a réussi, l'application GlobalProtect établit un tunnel avec la passerelle et une adresse IP lui est assignée depuis la réserve IP dans la configuration de tunnel de passerelle. Pour soutenir la mise en œuvre d'une politique basée sur l'utilisateur lors des sessions depuis la zone **`corp-vpn`**, le nom d'utilisateur figurant sur le certificat est mappé en l'adresse IP assignée par la passerelle. Si une stratégie de sécurité requiert un nom de domaine en plus du nom d'utilisateur, la valeur de domaine spécifiée dans le profil de certificat est ajoutée au nom d'utilisateur.

 ©2026 Palo Alto Networks, Inc.

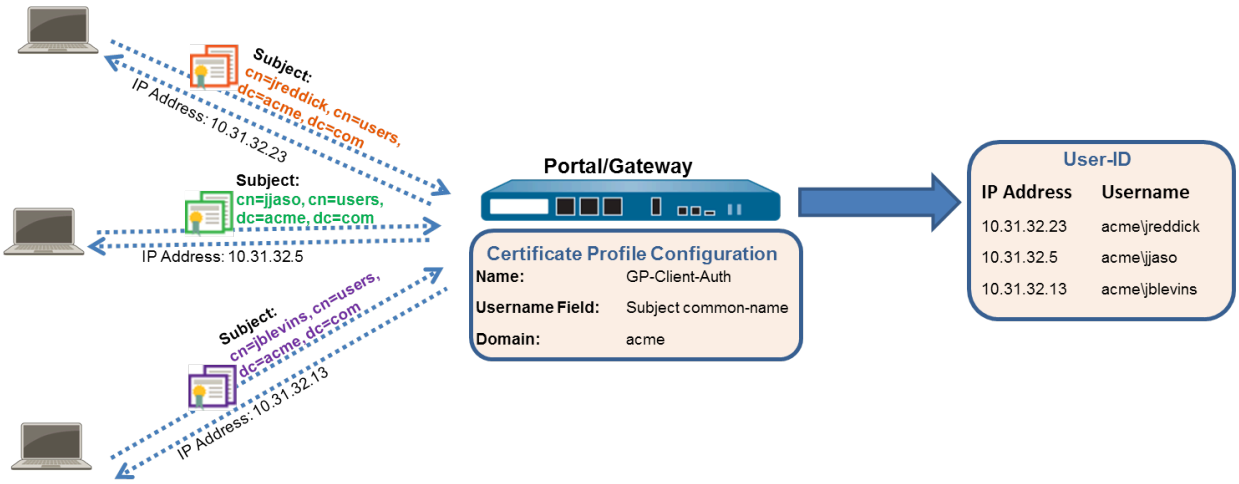


Illustration 7 : Configuration de l'authentification du certificat client GlobalProtect

Cette configuration rapide utilise la même topologie que VPN GlobalProtect pour l'accès à distance. L'unique différence de configuration est que, à la place de l'authentification des utilisateurs sur un serveur d'authentification externe, cette configuration utilise l'authentification du certificat client uniquement.

1. (Requis uniquement sur NGFW géré par Panorama ou Strata Cloud Manager)Créez des interfaces et des zones pour GlobalProtect.

   *Utilisez le routeur virtuel **default (par défaut)** pour toutes les configurations d'interface pour éviter d'avoir à créer un routage inter-zone.*

   - Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**. Configurez **ethernet1/2** en tant qu'interface de Couche 3 comportant une adresse IP **`203.0.113.1`**, puis affectez-la à la **Security Zone (Zone de sécurité)** **`l3-untrust`** et au **Virtual Router (Routeur virtuel)** par défaut.
   - Créez un dossier « A » DNS qui mappe l'adresse IP **`203.0.113.1`** en **`gp.acme.com.`**
   - Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** et **Add (Ajouter)** une interface **tunnel.2**. Add (Ajoutez) l'interface de tunnel à une nouvelle **Security Zone (Zone de sécurité)** nommée `corp-vpn`, puis affectez-la au **Virtual Router (Routeur virtuel)** par défaut.
   - Activez l'identification de l'utilisateur sur la zone **`corp-vpn`**.

 ©2026 Palo Alto Networks, Inc.

2. Créez des politiques de sécurité pour autoriser le flux de trafic entre la zone **`corp-vpn`** et la zone **`l3-trust`**, ce qui autorise l'accès à vos ressources internes.
   1. Choisissez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajouter)** une nouvelle règle.
      - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** puis **Add (Ajouter)** une nouvelle règle.
      - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** puis **Add (Ajouter)** une nouvelle règle.
   2. Sélectionnez **Policies (Politiques)** > **Security (Securité)**, puis **Add (Ajoutez)** une nouvelle règle.
   3. Pour cet exemple, vous devriez définir la règle avec les paramètres suivants :
      - **Name (Nom)** (onglet **General (Général)**) : **`VPN Access`**
      - **Source Zone (Zone source)** (onglet **Source**) : **`corp-vpn`**
      - **Destination Zone (Zone de destination)** (onglet **Destination**) : **`l3-trust`**

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	VPN Access	none	corp-vpn	any	any	any	l3-trust	any	adobe-cq ms-exchange ms-office365 sharepoint	application-default	Allow

3. Utilisez l'une des méthodes suivantes pour obtenir un certificat de serveur pour l'interface qui héberge le portail GlobalProtect et la passerelle :

- (Recommandé) Importez un certificat de serveur depuis une AC indépendante tierce reconnue.
- Utilisez l'autorité de certification racine sur le portail pour générer un certificat de serveur auto-signé.

Gérez les certificats comme suit :

- Obtenez un certificat de serveur. Comme le portail et la passerelle sont sur la même interface, le même certificat de serveur peut être utilisé pour les deux composants.
- Le CN du certificat doit correspondre au FQDN, `gp.acme.com`.
- Pour permettre aux utilisateurs de se connecter au portail sans recevoir d'erreur de certificat, utilisez un certificat de serveur généré par une AC publique.

4. Émettez des certificats clients pour les clients GlobalProtect et les points de terminaison.
   1. Utilisez votre ICP d'entreprise ou une AC publique pour générer un certificat client unique pour chaque utilisateur GlobalProtect.
   2. Installez les certificats dans le magasin de certificats personnel sur les points d'extrémité.

 ©2026 Palo Alto Networks, Inc.

5. Créer un profil de certificat client.
   1. Choisissez l'une des actions suivantes :
      - Dans Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**. **Add (Ajoutez)** un nouveau profil de certificat, puis saisissez un **Name (Nom)** de profil, comme **`GP-client-cert`**.
      - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**. **Add (Ajoutez)** un nouveau profil de certificat, puis saisissez un **Name (Nom)** de profil, comme **`GP-client-cert`**.
      - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**. **Add (Ajoutez)** un nouveau profil de certificat, puis saisissez un **Name (Nom)** de profil, comme **`GP-client-cert`**.
   2. Sélectionnez **Subject (Sujet)** dans la liste déroulante **Username Field (Champ Nom d'utilisateur)**.
   3. Dans la zone **CA Certificates (Certificats de l'autorité de certification)**, **Add (Ajoutez)** le certificat de l'autorité de certification qui a délivré les certificats du client. Cliquez deux fois sur **OK**.

6. Configurer une passerelle GlobalProtect.

   Consultez le diagramme de la topologie illustré dans VPN GlobalProtect pour l'accès à distance.

   Add (Ajouter) une passerelle avec la configuration suivante :

   Interface : **`ethernet1/2`**

   Adresse IP : **`203.0.113.1`**

   Server Certificate (Certificat Serveur) - **`GP-server-cert.pem publié par GoDaddy`**

   Certificate Profile (Profil du certificat) : **`GP-client-cert`**

   Tunnel Interface (Interface de tunnel) : **`tunnel.2`**

   IP Pool (Pool d'adresses IP) : **`10.31.32.3 - 10.31.32.118`**

 ©2026 Palo Alto Networks, Inc.

7. Configurez les portails GlobalProtect.
   1. Paramétrer l'accès au portail GlobalProtect:

      Interface : `ethernet1/2`

      Adresse IP : `203.0.113.1`

      Server Certificate (Certificat Serveur) - `GP-server-cert.pem publié par GoDaddy`

      Certificate Profile (Profil du certificat) : `GP-client-cert`
   2. Définir les configurations Agent GlobalProtect:

      Connect Method (Méthode de Connexion) : `On-demand` (connexion manuelle initiée par l'utilisateur)

      External Gateway Address (Adresse de passerelle externe) : `gp.acme.com`
8. Déployer le logiciel de l'application GlobalProtect.

   Sélectionnez **Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)** . Suivez la procédure visant à héberger les mises à jour de l'application sur le portail.
9. (Facultatif) Activez l'utilisation de l'application mobile GlobalProtect.

   Achetez et installez un abonnement à GlobalProtect (**Device (Périphérique)** > **Licenses (Licences)**) pour activer l'utilisation de l'application.
10. Enregistrez la configuration GlobalProtect.

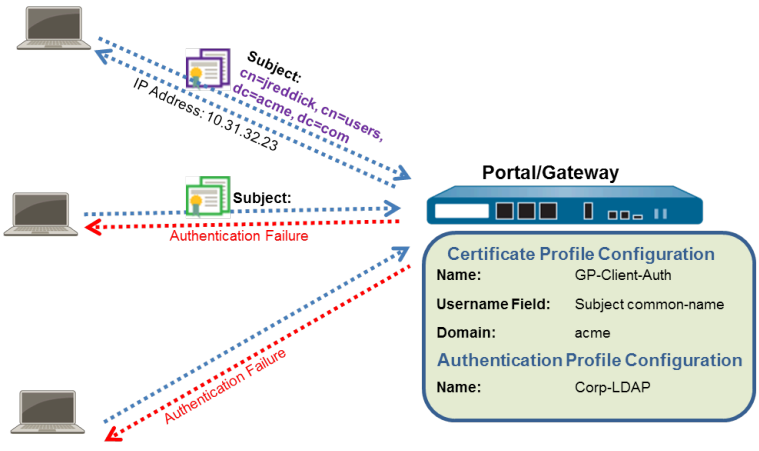
    Cliquez sur **Commit (Valider)**.

 ©2026 Palo Alto Networks, Inc.

VPN d'accès à distance avec l'authentification à deux facteurs

Si vous configurez un portail GlobalProtect ou une passerelle avec un profil d'authentification et un profil de certificat (qui, ensemble, peuvent fournir une authentification à deux facteurs), l'utilisateur final s'authentifier par les deux profils avant d'obtenir l'accès. Pour l'authentification du portail, cela signifie que les certificats doivent être pré-déployés sur les points de terminaison avant leur connexion initiale au portail. En outre, les certificats présentés par un utilisateur doivent correspondre à ce qui est défini dans le profil de certificat.

- Si le profil de certificat ne prévoit pas un champ Nom d'utilisateur (le **Username Field (Champ Nom d'utilisateur)** est défini sur **None (Aucun)**), le certificat client n'exige pas de nom d'utilisateur. Dans ce cas, l'utilisateur doit fournir le nom d'utilisateur lorsqu'il s'authentifie par rapport au profil d'authentification.
- Si le profil de certificat indique un champ Nom d'utilisateur, le certificat que l'utilisateur présente doit contenir un nom d'utilisateur dans le champ correspondant. Par exemple, si le profil de certificat indique que le champ Nom d'utilisateur est le **Subject (Sujet)**, le certificat présenté par le client doit contenir une valeur dans le champ Nom commun ; sinon, l'authentification échouera. En outre, lorsque le champ Nom d'utilisateur est requis, la valeur figurant dans le champ Nom d'utilisateur du certificat est automatiquement renseignée par le nom d'utilisateur si l'utilisateur tente de saisir des informations d'identification pour s'authentifier sur le profil d'authentification. Si vous ne souhaitez pas forcer les utilisateurs à s'authentifier avec un nom d'utilisateur figurant sur le certificat, ne prévoyez pas de champ Nom d'utilisateur dans le profil de certificat.



Cette configuration rapide utilise la même topologie que VPN GlobalProtect pour l'accès à distance. Toutefois, dans cette configuration, les utilisateurs doivent s'authentifier par rapport à un profil de certificat et un profil d'authentification. Pour plus d'informations sur un type spécifique d'authentification à deux facteurs, reportez-vous aux rubriques suivantes :

- Activer l'authentification à deux facteurs à l'aide de profils de certificat et d'authentification
- Activer l'authentification à deux facteurs basée sur les mots de passe à usage unique (MPUU)
- Activer l'authentification à deux facteurs basée sur les cartes à puce intelligentes
- Activer l'authentification à deux facteurs basée sur une application de jetons logiciels

 ©2026 Palo Alto Networks, Inc.

Utilisez la procédure suivante pour configurer l'accès distant VPN au moyen de l'authentification à deux facteurs.

1. (Requis uniquement sur NGFW géré par Panorama ou Strata Cloud Manager)Créez des interfaces et des zones pour GlobalProtect.

   *Utilisez le routeur virtuel **default (par défaut)** pour toutes les configurations d'interface pour éviter d'avoir à créer un routage inter-zone.*

   - Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**. Configurez **ethernet1/2** en tant qu'interface de **Layer3 (Couche 3)** comportant une adresse IP **`203.0.113.1`**, puis affectez-la à la **Security Zone (Zone de sécurité)** **`l3-untrust`** et au **Virtual Router (Routeur virtuel)** par défaut.
   - Créez un dossier « A » DNS qui mappe l'adresse IP **`203.0.113.1`** en **`gp.acme.com`**.
   - Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** et **Add (Ajouter)** une interface **tunnel.2**. Add (Ajoutez) l'interface de tunnel à une nouvelle **Security Zone (Zone de sécurité)** nommée **`corp-vpn`**, puis affectez-la au **Virtual Router (Routeur virtuel)** par défaut.
   - Activez l'identification de l'utilisateur sur la zone **`corp-vpn`**.

2. Créez des politiques de sécurité pour autoriser le flux de trafic entre la zone **`corp-vpn`** et la zone **`l3-trust`**, ce qui autorise l'accès à vos ressources internes.

   1. Choisissez l'une des actions suivantes :
      - Sur Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis **Add (Ajouter)** une nouvelle règle.
      - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** puis **Add (Ajouter)** une nouvelle règle.
      - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** puis **Add (Ajouter)** une nouvelle règle.
   2. Pour cet exemple, vous devriez définir la règle avec les paramètres suivants :
      - **Name (Nom)** (onglet **General (Général)**) : **`VPN Access`**
      - **Source Zone (Zone source)** (onglet **Source**) : **`corp-vpn`**
      - **Destination Zone (Zone de destination)** (onglet **Destination**) : **`l3-trust`**

 ©2026 Palo Alto Networks, Inc.

3. Utilisez l'une des méthodes suivantes pour obtenir un certificat de serveur pour l'interface qui héberge le portail GlobalProtect et la passerelle :

   - (Recommandé)Importez un certificat de serveur d'une autorité de certification tierce reconnue.
   - Utilisez l'autorité de certification racine sur le portail pour générer un certificat de serveur auto-signé.

   Gérez les certificats comme suit :

   - Obtenez un certificat de serveur. Comme le portail et la passerelle sont sur la même interface, le même certificat de serveur peut être utilisé pour les deux composants.
   - Le CN du certificat doit correspondre au FQDN, **`gp.acme.com`**.
   - Pour permettre aux utilisateurs de se connecter au portail sans recevoir d'erreur de certificat, utilisez un certificat de serveur généré par une AC publique.

4. Émettez des certificats clients pour les clients GlobalProtect et les points de terminaison.
   1. Utilisez votre ICP d'entreprise ou une AC publique pour générer un certificat client unique pour chaque utilisateur GlobalProtect.
   2. Installez les certificats dans le magasin de certificats personnel sur les points d'extrémité.

5. Créer un profil de certificat client.
   1. Choisissez l'une des actions suivantes :
      - Dans Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**. **Add (Ajoutez)** un nouveau profil de certificat, puis saisissez un **Name (Nom)** de profil, comme **`GP-client-cert`**.
      - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**. **Add (Ajoutez)** un nouveau profil de certificat, puis saisissez un **Name (Nom)** de profil, comme **`GP-client-cert`**.
      - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**. **Add (Ajoutez)** un nouveau profil de certificat, puis saisissez un **Name (Nom)** de profil, comme **`GP-client-cert`**.
   2. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**. **Add (Ajoutez)** un nouveau profil de certificat, puis saisissez un **Name (Nom)** de profil, comme **`GP-client-cert`**.
   3. Indiquez dans quel emplacement le nom d'utilisateur qui sera utilisé pour authentifier l'utilisateur final peut être récupéré :
      - **Auprès de l'utilisateur** : Si vous souhaitez que l'utilisateur final fournisse un nom d'utilisateur lorsqu'il s'authentifie sur le service indiqué dans le profil d'authentification, sélectionnez **None (Aucun)** comme **Username Field (Champ Nom d'utilisateur)**.
      - **Sur le certificat** : Si vous souhaitez extraire le nom d'utilisateur du certificat, sélectionnez **Subject (Sujet)** comme **Username Field (Champ Nom d'utilisateur)**. Si

 ©2026 Palo Alto Networks, Inc.

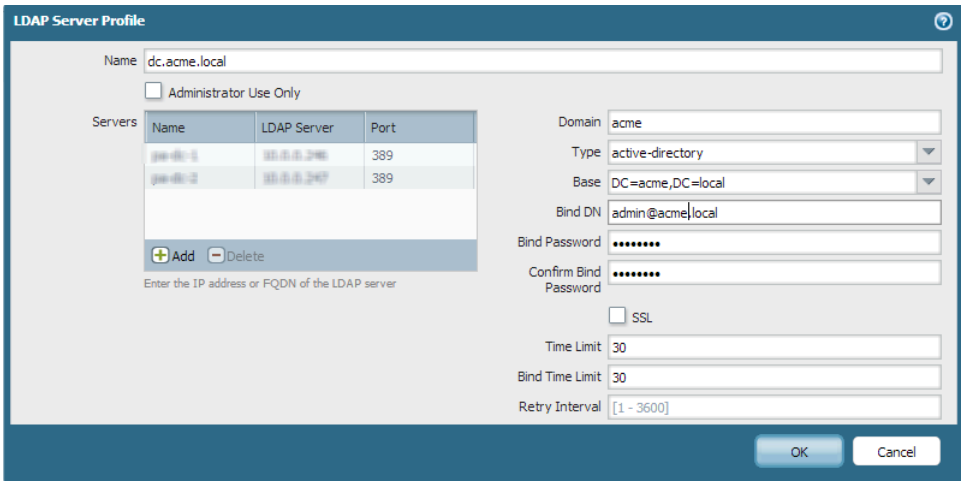
vous utilisez cette option, le NC contenu dans le certificat sera automatiquement renseigné dans le champ Nom d'utilisateur lorsque l'utilisateur est invité à ouvrir une session sur le portail/passerelle. L'utilisateur devra se connecter en utilisant ce même nom d'utilisateur.

4. Dans la zone **CA Certificates (Certificats de l'autorité de certification)**, **Add (Ajoutez)** le certificat de l'autorité de certification qui a délivré les certificats du client. Cliquez deux fois sur **OK**.

6. Créez un profil de serveur.

Le profil de serveur indique au pare-feu comment se connecter au service d'authentification. Les méthodes d'authentification locale, RADIUS, Kerberos, SAML et LDAP sont prises en charge. Cet exemple décrit un profil d'authentification LDAP pour authentifier les utilisateurs par rapport à Active Directory.

Créez le profil serveur pour la connexion au serveur LDAP (**Device (Périphérique)** > **Server Profiles (Profils Serveur)** > **LDAP**).

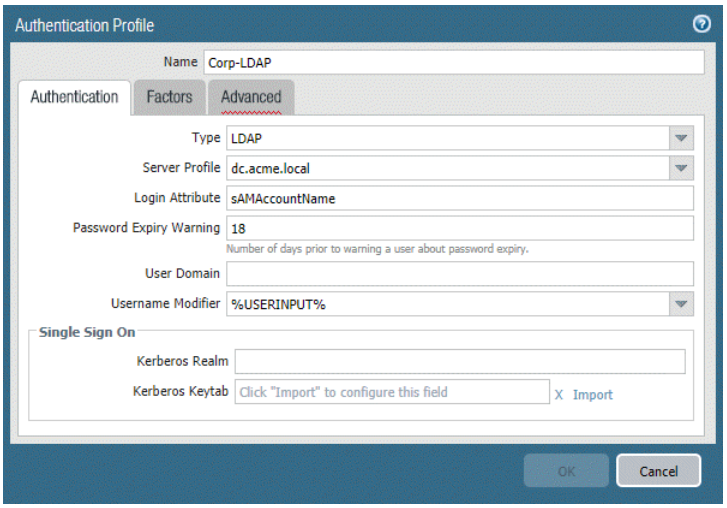


 ©2026 Palo Alto Networks, Inc.

7. (Facultatif) Créez un profil d'authentification.

Ajoutez le profil de serveur TACACS+ à un profil d’authentification :

- Sur Panorama, sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d’authentification)**.
- Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d’identité)** > **Authentication Profiles (Profils d’authentification)**.
- Dans Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d’identité)** > **Authentication Profiles (Profils d’authentification)** puis **Add (Ajouter)** une nouvelle règle.



8. Configurez une passerelle GlobalProtect avec la configuration suivante.

Consultez le diagramme de la topologie illustré dans VPN GlobalProtect pour l’accès à distance.

Interface : **`ethernet1/2`**

Adresse IP : **`203.0.113.1`**

Server Certificate (Certificat Serveur) - **`GP-server-cert.pem publié par GoDaddy`**

Certificate Profile (Profil du certificat) : **`GP-client-cert`**

Authentication Profile (Profil d’authentification) : **`Corp-LDAP`**

Tunnel Interface (Interface de tunnel) : **`tunnel.2`**

IP Pool (Pool d'adresses IP) : **`10.31.32.3 - 10.31.32.118`**

 ©2026 Palo Alto Networks, Inc.

9. Configurez un Portails GlobalProtect avec la configuration suivante :

   Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**, puis **Add (Ajouter)** la configuration suivante :

   1. Paramétrer l'accès au portail GlobalProtect:

      Interface : **`ethernet1/2`**

      Adresse IP : **`203.0.113.1`**

      Server Certificate (Certificat Serveur) - **`GP-server-cert.pem publié par GoDaddy`**

      Certificate Profile (Profil du certificat) : **`GP-client-cert`**

      Authentication Profile (Profil d'authentification) : **`Corp-LDAP`**

   2. Définir les configurations Agent GlobalProtect:

      Connect Method (Méthode de Connexion) : **`On-demand`** (connexion manuelle initiée par l'utilisateur)

      External Gateway Address (Adresse de passerelle externe) : **`gp.acme.com`**

10. Déployer le logiciel de l'application GlobalProtect.

    Suivez la procédure visant à héberger les mises à jour de l'application sur le portail.

11. (Facultatif) Déployez les paramètres d'agent de manière transparente.

    Comme autre procédure possible pour le déploiement des paramètres de l'application à partir de la configuration du portail, vous pouvez définir les paramètres directement dans le registre Windows ou la plist macOS globale. Parmi les exemples de paramètres que vous pouvez déployer, mentionnons l'indication de l'adresse IP du portail ou l'activation de GlobalProtect pour initier un tunnel VPN avant qu'un utilisateur ne se connecte au point de terminaison et au portail GlobalProtect. Sur les points de terminaison Windows uniquement, vous pouvez également configurer les paramètres à l'aide du programme d'installation Windows.

12. (Facultatif) Activez l'utilisation de l'application mobile GlobalProtect.

    Achetez et installez un abonnement à GlobalProtect pour activer l'utilisation de l'application.

13. Enregistrez la configuration GlobalProtect.

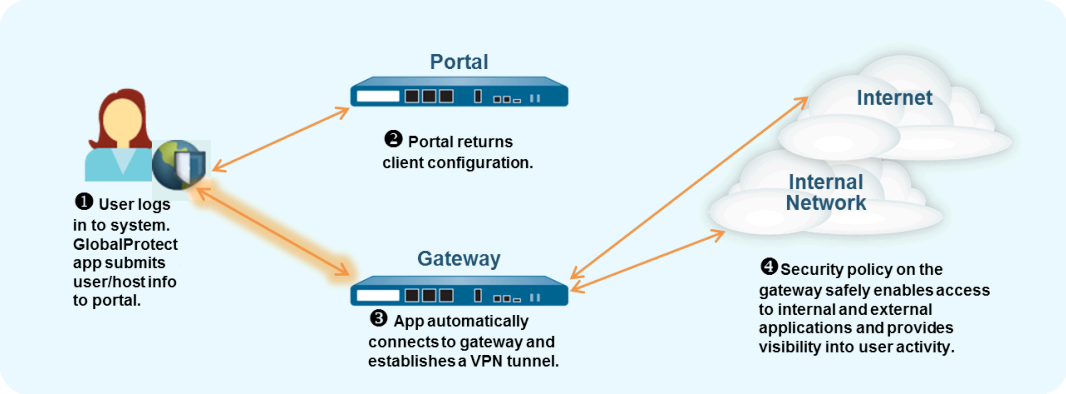
    Cliquez sur **Commit (Valider)**.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect : configuration de VPN toujours activée

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans une configuration GlobalProtect « toujours active », l'application se connecte au portail GlobalProtect dès l'ouverture de session de l'utilisateur pour soumettre les informations sur l'utilisateur et sur l'hôte et recevoir la configuration de client. Puis, l'application se connecte automatiquement et établit un tunnel VPN vers la passerelle qui a été précisée dans la configuration client transmise par le portail, comme l'illustre l'image suivante :



Pour faire basculer l'une des configurations VPN d'accès à distance suivantes sur une configuration toujours active, vous pouvez changer la méthode de connexion :

- VPN d'accès à distance (Profil d'authentification)
- VPN d'accès à distance (profil de certificat)
- VPN d'accès à distance avec l'authentification à deux facteurs

Utilisez les étapes suivantes pour basculer une configuration VPN d'accès à distance sur une configuration toujours active.

- GlobalProtect : configuration de VPN toujours activée – Panorama
- GlobalProtect : configuration de VPN toujours activée – SCM

©2026 Palo Alto Networks, Inc.

VPN d'accès à distance avec pré-ouverture de session

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

La pré-ouverture de session est une méthode de connexion qui établit un tunnel VPN avant qu'un utilisateur ne se connecte. Le but de la pré-ouverture de session est d'authentifier le point de terminaison (pas l'utilisateur), puis d'activer les scripts de domaine et d'autres tâches de votre choix à exécuter dès que le point de terminaison est activé. Les certificats machine permettent au point de terminaison d'établir un tunnel VPN à la passerelle GlobalProtect. Une pratique courante pour les administrateurs informations consiste à installer le certificat de machine tout en mettant en scène le point de terminaison pour l'utilisateur.

Un tunnel VPN de pré-ouverture de session n'a aucune association de nom d<utilisateur parce que l'utilisateur ne s'est pas connecté. Pour autoriser le point de terminaison à accéder aux ressources de la zone de confiance, vous devez créer des stratégies de sécurité qui correspondent à l'utilisateur pré-ouverture de session. Ces stratégies doivent autoriser l'accès uniquement aux services de base pour le démarrage du système, par exemple DHCP, DNS, des services Active Directory spécifiques, des antivirus ou des services de mise à jour du système d'exploitation. Une fois que l'utilisateur s'est authentifié auprès de la passerelle, l'application GlobalProtect réaffecte le tunnel VPN à cet utilisateur (le mappage d'adresses IP sur le pare-feu passe du point de terminaison de pré-ouverture de session à l'utilisateur authentifié).

En tant que meilleure pratique, vous devez créer des stratégies de sécurité pour autoriser l'accès à uniquement des services spécifiques (par exemple, DHCP, DNS, des services Active Directory spécifiques ou des services de mise à jour du système d'exploitation) qui sont suffisants pour l'authentification de la machine et pour activer les services qui sont nécessaires pour le réseau de l'entreprise. Nous vous recommandons de créer des stratégies de sécurité pour refuser aux utilisateurs avant la connexion l'accès à d'autres ressources et applications.

Suivez ces directives si le point de terminaison de l'utilisateur est perdu ou volé :

- *Vous devez révoquer le certificat d'ordinateur qui est délivré au point de terminaison pour la pré-connexion. Une fois le certificat de la machine révoqué pour la méthode de connexion avant ouverture de session, vous ne pouvez pas utiliser le certificat pour vous authentifier auprès du portail et de la passerelle car l'authentification au point de terminaison a échoué et le point de terminaison ne peut pas se connecter au réseau d'entreprise.*
- *Vous pouvez mettre en quarantaine les points de terminaison perdus ou volés en les ajoutant à la liste de quarantaine, empêcher les utilisateurs de se connecter au réseau à partir de ce point de terminaison et empêcher les connexions VPN à partir de ces points de terminaison compromis.*
- *Vous devez désactiver le compte d'ordinateur de point de terminaison volé dans Active Directory pour bloquer les connexions VPN des comptes d'ordinateur désactivés en fonction de la présence du numéro de série du point de terminaison. Lorsque cette fonctionnalité est*

 ©2026 Palo Alto Networks, Inc.

utilisée, les tentatives d'authentification du compte d'ordinateur désactivé échoueront lors de la tentative d'empêcher les connexions VPN du point de terminaison perdu ou volé.

L'écran de connexion du fournisseur d'informations d'identification de GlobalProtect pour les points de terminaison Windows 7 et Windows 10 affiche également l'état de la connexion pré-ouverture de session avant que l'utilisateur ne se connecte, ce qui permet aux utilisateurs finaux de déterminer s'ils peuvent accéder aux ressources du réseau lors de la connexion. Si l'application GlobalProtect détecte qu'un point de terminaison est interne, l'écran de connexion indique **Internal (Interne)** comme état de connexion pré-ouverture de session. Si l'application GlobalProtect détecte qu'un point de terminaison est externe, l'écran de connexion indique **Connected (Connecté)** ou **Not Connected (Non connecté)** comme état de connexion pré-ouverture de session.

Les points de terminaison Windows se comportent différemment des points de terminaison macOS en ce qui a trait à la pré-ouverture de session. Avec les points de terminaison MacOS, le tunnel créé pour la pré-connexion est déchiré et un nouveau tunnel est créé lorsque l'utilisateur se connecte.

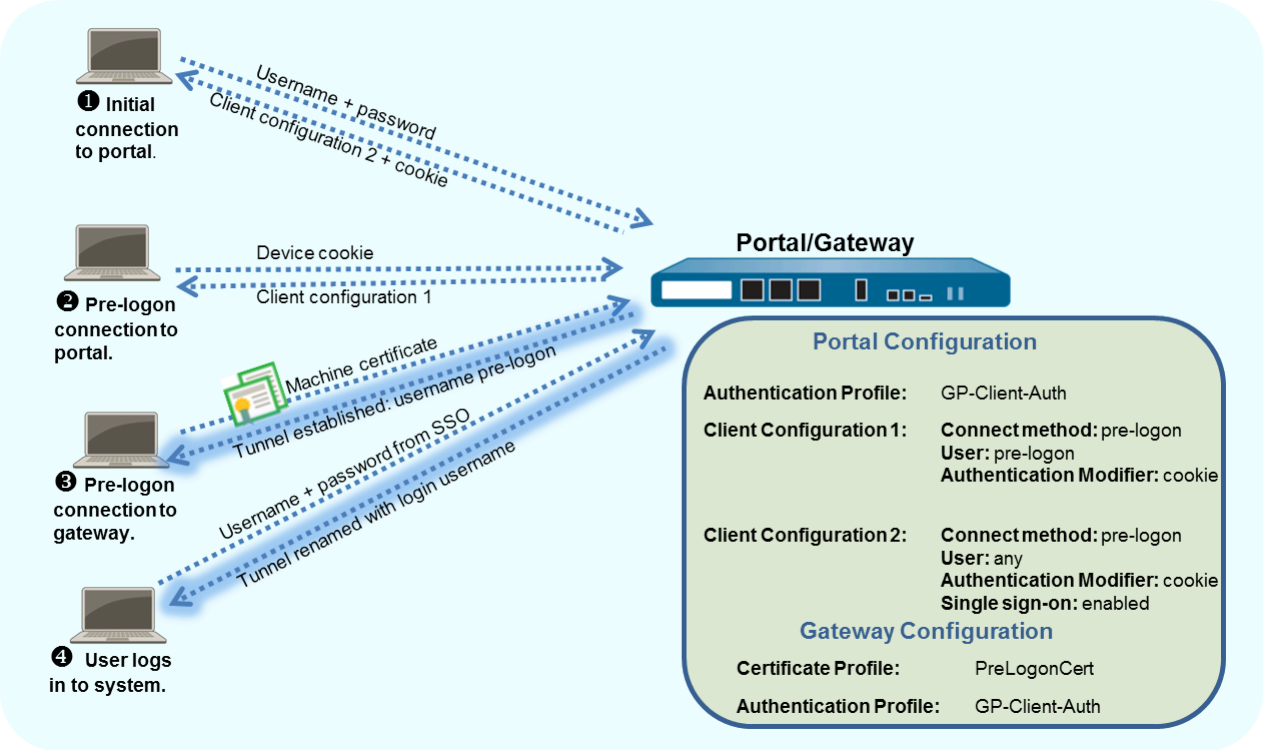
Lorsqu'un utilisateur demande une nouvelle connexion, le portail authentifie l'utilisateur à l'aide d'un profil d'authentification. Le portail peut également utiliser un profil de certificat facultatif qui valide le certificat client (si la configuration comprend un certificat client). Dans ce cas, le certificat doit identifier l'utilisateur. Après l'authentification, le portail détermine si la configuration GlobalProtect du point de terminaison est actuelle. Si la configuration du portail a changé, elle insère une configuration de mise à jour vers le point de terminaison.

Si la configuration sur le portail ou une passerelle comprend l'authentification basée sur des cookies, le portail ou la passerelle installe un cookie crypté sur le point de terminaison. Par la suite, le portail ou la passerelle utilise le cookie pour authentifier les utilisateurs et actualise la configuration de l'agent. Si un profil de configuration de l'agent comprend la méthode de connexion avant ouverture de session en plus de l'authentification cookie, les composants GlobalProtect peuvent utiliser le cookie pour la pré-ouverture de session.

Si les utilisateurs ne se connectent jamais à un point de terminaison (par exemple, un point de terminaison sans affichage) ou qu'une connexion de pré-ouverture de session est requise sur un système sur lequel un utilisateur n'a jamais ouvert de session, vous pouvez laisser le point de terminaison lancer un tunnel de pré-connexion sans avoir été connecté au portail pour télécharger la configuration de pré-connexion. Pour ce faire, vous devez remplacer ce comportement par défaut en créant des entrées dans le registre Windows ou la plist Macos.

Le point de terminaison GlobalProtect se connecte alors au portail indiqué dans la configuration, s'authentifie en présentant son certificat machine (tel qu'il figure dans un profil de certificat configuré sur la passerelle), puis établit le tunnel VPN. Lorsque l'utilisateur final ouvre ultérieurement une session sur la machine, et si la Single Sign-On (ouverture de session unique ; SSO) est activée dans la configuration de l'agent, le nom de l'utilisateur et le mot de passe sont saisis lorsque l'utilisateur se connecte. Si SSO n'est pas activé dans la configuration du client ou que SSO n'est pas pris en charge sur le point de terminaison (par exemple, s'il s'agit d'un système macOS), les informations d'identification de l'utilisateur doivent être stockées dans l'application (c'est-à-dire que l'option **Save User Credentials (Sauvegarder les informations d'identification des utilisateurs)** doit être mise sur **Yes (Oui)**). Une fois l'authentification réussie sur la passerelle, le tunnel est renommé (Windows) ou recréé (macOS) et la politique basée sur l'utilisateur et le groupe peut être mise en œuvre.

 ©2026 Palo Alto Networks, Inc.



Cet exemple utilise la topologie GlobalProtect illustrée dans VPN GlobalProtect pour l'accès à distance.

1. (Requis uniquement sur NGFW géré par Panorama ou Strata Cloud Manager)Créez des interfaces et des zones pour GlobalProtect.

   *Utilisez le routeur virtuel **default (par défaut)** pour toutes les configurations d'interface pour éviter d'avoir à créer un routage inter-zone.*

   - Pour cet exemple, sélectionnez l'onglet **Network (Réseau)** > **Interfaces** > **Ethernet**, puis configurez les paramètres suivants :

     1. Sélectionnez **ethernet1/2**.
     2. Sélectionnez **Layer 3 (Couche 3)** dans la liste déroulante **Interface Type (Type d'interface)**.
     3. À l'onglet **Config (Configuration)**, **Assign interface to (Affecter l'interface à) Virtual Router (Routeur virtuel)** par défaut et à la **`Security Zone (Zone de sécurité)`** **l3-untrust**.
     4. À l'onglet **IPv4**, cliquez sur **Add (Ajouter)** pour sélectionner l'adresse **`IP 203.0.113.1`** (ou l'objet qui mappe **`203.0.113.1`**) ou pour ajouter une **New Address (Nouvelle adresse)** dans le but de créer un nouveau mappage d'objets et d'adresses (laissez le

 ©2026 Palo Alto Networks, Inc.

type d'adresse sur **Static (Statique)**). Par exemple, créez un dossier « A » DNS qui mappe l'adresse IP **`203.0.113.1`** en **`gp.acme.com`**.

- Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** et **Add (Ajouter)** une nouvelle interface de tunnel.
  1. Comme **Interface Name (Nom de l'interface)**, saisissez **`tunnel.2`**.
  2. À l'onglet **Config (Configuration)**, **Assign Interface To (Affectez l'interface à)** une nouvelle **Security Zone (Zone de sécurité)** nommée **`corp-vpn`** et au **Virtual Router (Routeur virtuel)** par défaut.
- Activez l'identification de l'utilisateur sur la zone **`corp-vpn`**.

2. Créez les règles de politique de sécurité.

Cette configuration requiert les stratégies suivantes (**Policies (Politiques)** > **Security (Sécurité)**) :

1. **Add (Ajoutez)** une règle qui autorise l'accès aux utilisateurs en pré-ouverture de session aux services de base requis pour le point de terminaison, tels que les services d'authentification, DNS, DHCP et Microsoft Updates.

   Vous devez vous assurer que toutes les règles de stratégie de sécurité sont correctement configurées pour permettre aux utilisateurs de pré-ouverture de session d'accéder uniquement aux services requis pour le point de terminaison.
2. **Add (Ajoutez)** une règle pour refuser l'accès aux utilisateurs en pré-ouverture de session à toutes les autres destinations et applications.
3. **Add (Ajoutez)** les règles supplémentaires permettant aux divers utilisateurs ou groupes d'utilisateurs d'accéder à des destinations ou à des applications données. Suivez les recommandations des Meilleures pratiques de politique de sécurité de la passerelle Internet pour créer ces règles.

3. Utilisez l'une des méthodes suivantes pour obtenir un certificat de serveur pour l'interface qui héberge le portail GlobalProtect et la passerelle:

- (Recommandé)Importez un certificat de serveur d'une autorité de certification tierce reconnue.
- Utilisez l'autorité de certification racine sur le portail pour générer un certificat de serveur auto-signé.

Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion de Certificat)** > **Certificates (Certificats)** pour gérer les certificats avec les critères suivants :

- Obtenez un certificat de serveur. Comme le portail et la passerelle sont sur la même interface, le même certificat de serveur peut être utilisé pour les deux composants.
- Le CN du certificat doit correspondre au FQDN, **`gp.acme.com`**.
- Pour permettre aux points de terminaison de se connecter au portail sans recevoir d'erreur de certificat, utilisez un certificat de serveur généré par une AC publique.

 ©2026 Palo Alto Networks, Inc.

4. Générez un certificat machine pour chaque système client qui se connecte à GlobalProtect, puis importez le certificat dans le magasin de certificats personnels sur chaque machine.

   Même si vous pouvez générer des certificats auto-signés pour chaque système client, selon la procédure recommandée, vous devez utiliser votre propre infrastructure à clés publiques (ICP) pour générer et distribuer les certificats à vos points de terminaison.

   1. Émettez des certificats clients pour les clients GlobalProtect et les points de terminaison.
   2. Installez les certificats dans le magasin de certificats personnel sur les points d'extrémité. (Sans le magasin de l'ordinateur local sur les points de terminaison Windows ou dans System Keychain sur les points de terminaison MacOS)

5. Importez le certificat AC racine de confiance à partir de l'AC ayant généré les certificats machines sur le portail et les passerelles :

   Vous n'avez pas besoin d'importer la clé privée.

   1. Téléchargez le certificat AC au format Base64.
   2. Suivez les étapes suivantes pour importer le certificat sur chaque pare-feu hébergeant un portail ou une passerelle :

      1. Effectuez l'une des actions suivantes :

         - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importer)** un nouveau certificat.
         - Sur Strata Cloud Manager, sélectionnez **Manage Configuration (Gérer la configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** et **Import (Importer)** un certificat.
         - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)Objects (Objets)** > **Certificate Management (Gestion des certificats)** et **Import (Importer)** le certificat.

      2. Saisissez un **Certificate Name (Nom de certificat)** qui identifie le certificat comme étant votre certificat CA client.
      3. **Browse (Accédez)** au **Certificate File (Fichier du certificat)** que vous avez téléchargé de l'AC.
      4. Définissez le **File Format (Format du fichier)** sur **Base64 Encoded Certificate (PEM) (Certificat codé en base-64 (PEM))**.
      5. Cliquez sur **OK** pour enregistrer votre certificat.
      6. Sous l'onglet **Device Certificates (Certificats de périphérique)**, sélectionnez le certificat que vous venez d'importer.
      7. Cochez la case **Trusted Root CA (CA racine de confiance)**, puis cliquez sur **OK**.

6. Sur chaque pare-feu hébergeant une passerelle GlobalProtect, créez un profil de certificat pour identifier le certificat de l'AC pour valider les certificats de machine.

   Si vous envisagez d'utiliser l'authentification du certificat client pour authentifier les utilisateurs lorsqu'ils se connectent au système, assurez-vous que le certificat AC qui génère les certificats

 ©2026 Palo Alto Networks, Inc.

clients est référencé dans le profil de certificat en plus du certificat AC qui a généré les certificats machines s'ils sont différents.

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Device (Périphérique)** > **Certificates (Certificats)** > **Certificate Management (Gestion de Certificats)** > **Certificate Profile (Profil de certificat)**, puis **Add (Ajouter)** un nouveau profil de certificat.
   - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** > **Certificate Profiles (Profils de certificat)** et puis **Add (Ajouter)** un nouveau profil de certificat.
   - Sur Strata Cloud Manager, sélectionnez **ConfigurationNGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Certificate Management (Gestion des certificats)** > **Certificate Profiles (Profils de certificat)** et puis **Add (Ajouter)** un nouveau profil de certificat.
2. Saisissez un **Name (Nom)** pour identifier le profil, par exemple **`PreLogonCert`**.
3. Définissez le champ **Username (Nom d'utilisateur)** sur **None (Aucun)**.
4. (Facultatif) Si vous devez aussi utiliser l'authentification du certificat client pour authentifier les utilisateurs dès l'ouverture de session, ajoutez le certificat AC qui a généré les certificats clients s'il est différent de celui qui a généré les certificats machines.
5. Dans le champ **CA Certificates (Certificats de l'autorité de certification)**, **Add (Ajoutez)** le certificat de l'autorité de certification.
6. Sélectionnez le **CA Certificate (Certificat de l'autorité de certification)** racine de confiance que vous avez importé à l'étape 5, puis cliquez sur **OK**.
7. Cliquez sur **OK** pour enregistrer le profil.

7. Configurer une passerelle GlobalProtect.

Consultez le diagramme de la topologie illustré dans VPN GlobalProtect pour l'accès à distance.

Même si vous devez créer un profil de certificat pour l'accès pré-ouverture de session sur la passerelle, vous pouvez utiliser soit l'authentification du certificat client soit l'authentification

 ©2026 Palo Alto Networks, Inc.

basée sur le profil d'authentification pour les utilisateurs connectés. Dans cet exemple, le profil LDAP utilisé est le même que celui qui est utilisé pour authentifier les utilisateurs sur le portail.

1. Choisissez l'une des actions suivantes :
   - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**.
   - Dans Strata Cloud Manager, sélectionnez **Manage Configuration (Gérer la configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device Settings (Paramètres du périphérique)** > **Gateways (Passerelles)**.
   - Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **ConfigurationNGFW and Prisma Access (NGFW et Prisma Access)** > **Device Settings (Paramètres du périphérique)** > **Gateways (Passerelles)**.
2. **Add (Ajouter)** la configuration de passerelle suivante :

   Interface : **`ethernet1/2`**

   Adresse IP : **`203.0.113.1`**

   Server Certificate (Certificat Serveur) - **`GP-server-cert.pem publié par GoDaddy`**

   Certificate Profile (Profil de certificat) : **`PreLogonCert`**

   Authentication Profile (Profil d'authentification) : **`Corp-LDAP`**

   Tunnel Interface (Interface de tunnel) : **`tunnel.2`**

   IP Pool (Pool d'adresses IP) : **`10.31.32.3 - 10.31.32.118`**
3. **Commit (Validez)** la configuration de passerelle.

 ©2026 Palo Alto Networks, Inc.

8. Configurez les portails GlobalProtect.

   Configurez les détails du **Device (périphérique)** (paramètres de réseautage, le profil du service d'authentification et le certificat pour le serveur d'authentification).

   1. Choisissez l'une des actions suivantes :
      - Dans Panorama, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**.
      - Dans Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device Settings (Paramètres du périphérique)** > **Gateways (Passerelles)**.
      - Dans Strata Cloud Manager, sélectionnez **ConfigurationNGFW and Prisma Access (NGFW et Prisma Access)** > **Device Settings (Paramètres du périphérique)** > **Gateways (Passerelles)**.
   2. **Add (Ajouter)** la configuration de portail suivante :
      - Paramétrer l'accès au portail GlobalProtect
      - **Interface** : **`ethernet1/2`**
      - **Adresse IP** : **`203.0.113.1`**
      - **Server Certificate (Certificat Serveur)** - **`GP-server-cert.pem publié par GoDaddy`**
      - **Certificate Profile (Profil de certificat)** : **`None`**
      - **Authentication Profile (Profil d'authentification)** : `Corp-LDAP`

9. Définissez les configurations de l'agent GlobalProtect pour les utilisateurs pré-logon et pour les utilisateurs enregistrés.

   Vous devez créer des règles de stratégie de sécurité pour refuser l'accès aux services non requis pour les utilisateurs de pré-connexion et autoriser uniquement l'accès aux services qui sont obligatoires pour les utilisateurs de pré-connexion.

   Utilisez une configuration unique si vous souhaitez que les utilisateurs pré-ouverture de session accèdent aux mêmes passerelles avant et après leur connexion.

   Pour diriger les utilisateurs pré-ouverture de session vers différentes passerelles avant et après leur connexion, créez deux profils de configuration. Dans ce premier **User/User Group (utilisateur/groupe d'utilisateurs)** de la configuration, sélectionnez le filtre **pre-logon (pré-ouverture de session)**. Avec la pré-ouverture de session, le portail authentifie d'abord le point de terminaison (et non l'utilisateur) pour établir une connexion, même si le paramètre de pré-ouverture de session est associé à l'utilisateur. Par la suite, le portail authentifie l'utilisateur lorsqu'il se connecte.

   Une fois que le portail authentifie l'utilisateur, il déploie la deuxième configuration. Dans ce cas, **User/User Group (utilisateur/groupe d'utilisateurs)** est **any (tout)**.

   Le mieux est d'activer la SSO dans la deuxième configuration afin que le nom d'utilisateur correct soit signalé immédiatement à la passerelle lorsque l'utilisateur se connecte au point

 ©2026 Palo Alto Networks, Inc.

*de terminaison. Si SSO n'est pas activé, le nom d'utilisateur enregistré dans le panneau paramètres de l'**agent** est utilisé.*

Add (Ajouter) l'une des configurations suivantes :

- Utiliser la même passerelle avant et après les utilisateurs pré-logon :

  Use single sign-on (Utiliser l'ouverture de session unique) : **`enabled`**

  Connect Method (Méthode de connexion) : **`pré-connexion`**

  External Gateway Address (Adresse de passerelle externe) : **`gp1.acme.com`**

  User/User Group (Utilisateur / groupe d'utilisateurs) : **`any`**

  Authentication Override (Surpasser l'authentification) : authentification par cookie pour l'authentification transparente des utilisateurs et pour actualiser la configuration
- Utilisez des passerelles distinctes pour les utilisateurs avant et après leur ouverture de session :

  Première configuration de l'agent :

  Connect Method (Méthode de connexion) : **`pré-connexion`**

  External Gateway Address (Adresse de passerelle externe) : **`gp1.acme.com`**

  User/User Group (Utilisateur/Groupe d'utilisateurs) : **`pré-ouverture de session`**

  Authentication Override (Surpasser l'authentification) : authentification par cookie pour l'authentification transparente des utilisateurs et pour actualiser la configuration

  Deuxième configuration de l'agent :

  Use single sign-on (Utiliser l'ouverture de session unique) : **`enabled`**

  Connect Method (Méthode de connexion) : **`pré-connexion`**

  External Gateway Address (Adresse de passerelle externe) : **`gp2.acme.com`**

  User/User Group (Utilisateur / groupe d'utilisateurs) : **`any`**

  Authentication Override (Surpasser l'authentification) : authentification par cookie pour l'authentification transparente des utilisateurs et pour actualiser la configuration

  Vérifiez que la configuration en pré-ouverture de session est la première affichée dans la liste des configurations. Si tel n'est pas le cas, sélectionnez-la et cliquez sur **Move Up (Remonter)**.

10. Enregistrez la configuration GlobalProtect.

    Cliquez sur **Commit (Valider)**.

11. (Facultatif) Si les utilisateurs ne se connecteront jamais à un point de terminaison (par exemple, un point de terminaison sans tête) ou qu'une connexion en mode pré-ouverture de

 ©2026 Palo Alto Networks, Inc.

session est nécessaire sur un système auquel un utilisateur ne s'est jamais connecté, créez l'entrée `Prelogon` du registre sur le point de terminaison.

Vous devez également redéployer l'adresse IP du portail par défaut.

Pour plus d'informations sur les paramètres du Registre, consultez déploiement de paramètres de l'application de manière transparente.

1. Accédez à l'emplacement du registre Windows suivant pour afficher la liste des paramètres GlobalProtect :
   `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`
2. Sélectionnez **Edit (Modifier)** > **New (Nouveau)** > **String Value (Valeur de chaîne)** pour créer les entrées de registre suivantes :
   - Créez une **String Value (Valeur de chaîne)** nommée **`Prelogon`** avec une valeur de **1**. Ce paramètre permet à GlobalProtect d'initier une connexion avant que l'utilisateur ne se connecte au point de terminaison.
   - Créez une **String Value (Valeur de chaîne)** nommée **`Portal`** qui indique l'adresse IP ou le nom d'hôte du portail par défaut du point de terminaison GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

Connexion préouverture de session initiée par l'utilisateur

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Terminaux Windows 10 ou ultérieurs Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Permettez aux utilisateurs finaux d'initier manuellement la connexion VPN d'accès à distance avec pré-ouverture de session GlobalProtect sur les terminaux Windows 10. La préouverture de session initiée par l'utilisateur nécessite l'utilisation de l'option **Use Single Sign-On (Ouverture de session unique)** dans la configuration de votre portail. Dans ce déploiement, les utilisateurs peuvent initier la connexion de préouverture de session uniquement lorsque leur terminal nécessite un accès au réseau d'entreprise avant la connexion, par exemple lorsque de nouveaux employés se connectent au réseau à distance pour la première fois ou lorsque les administrateurs doivent se connecter à distance et résoudre les problèmes sur le terminal. Pour initier la connexion de préouverture de session, les utilisateurs doivent **Start GlobalProtect Connection (Démarrer la connexion GlobalProtect)** à partir de l'écran de connexion du fournisseur d'informations d'identification GlobalProtect après le démarrage du terminal.

*Si les utilisateurs ne parviennent pas à établir la connexion de pré-ouverture de session à l'aide de cette option, l'état de la connexion de préouverture de session reste **Déconnecté**.*

Lorsque les utilisateurs se déconnectent de leur terminal, le tunnel VPN n'est pas renommé du tunnel utilisateur vers le tunnel de préouverture de session. À la place, le tunnel se déconnecte.

Utilisez les étapes suivantes pour permettre aux utilisateurs d'initier manuellement la connexion de préouverture de session :

Vous pouvez configurer cette option uniquement dans le Registre Windows. Cette configuration peut être effectuée manuellement après l'installation de GlobalProtect ou pré-déployée dans l'image Windows qui inclut le logiciel GlobalProtect.

1. Configurer le VPN d'accès à distance avec préouverture de session

   Utilisez l'une des options suivantes pour configurer le VPN d'accès à distance avec préouverture de session :

   - Si votre utilisateur final se connecte au portail GlobalProtect avant d'utiliser cette fonctionnalité (par exemple, un employé existant qui s'est déjà connecté à GlobalProtect),

 ©2026 Palo Alto Networks, Inc.

vous pouvez configurer un VPN d'accès à distance avec préouverture de session dans la configuration du portail.

Pour permettre aux utilisateurs d'initier manuellement la connexion de préouverture de session, vous devez configurer les options suivantes dans la configuration de votre portail :

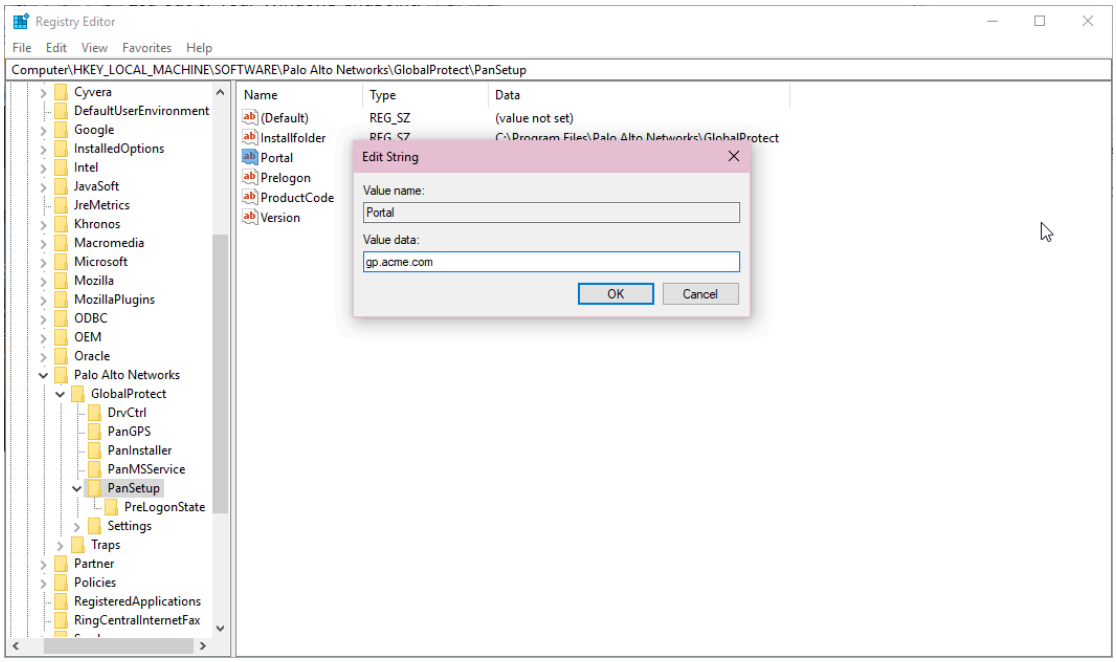
- Spécifiez une **IP address (Adresse IP)** de portail.
- Définissez la GlobalProtect **Connect Method (Méthode de connexion GlobalProtect)** sur **Pre-logon (Always On) (Préouverture de session [Toujours activée])** ou **Pre-logon then On-demand (Préouverture de session puis À la demande** (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **App (Application)**).
- Définissez l'option **Use Single Sign-On (Utiliser l'ouverture de session unique)** sur **Yes (Oui)** pour permettre à GlobalProtect d'utiliser les informations d'identification de connexion Windows pour authentifier automatiquement les utilisateurs lors de la connexion Active Directory (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **App (Application)**).

- Si votre utilisateur final ne se connectera pas au portail GlobalProtect avant d'utiliser cette fonctionnalité (par exemple, un nouvel employé qui se connecte au réseau à distance pour la première fois), vous devez pré-déployer les paramètres de préouverture de session dans le Registre Windows :

  1. À partir de votre terminal Windows, lancez l'invite de commande.
  2. Entrez **`regedit`** pour ouvrir le registre Windows.
  3. Dans le registre Windows, accédez à : `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup\`.

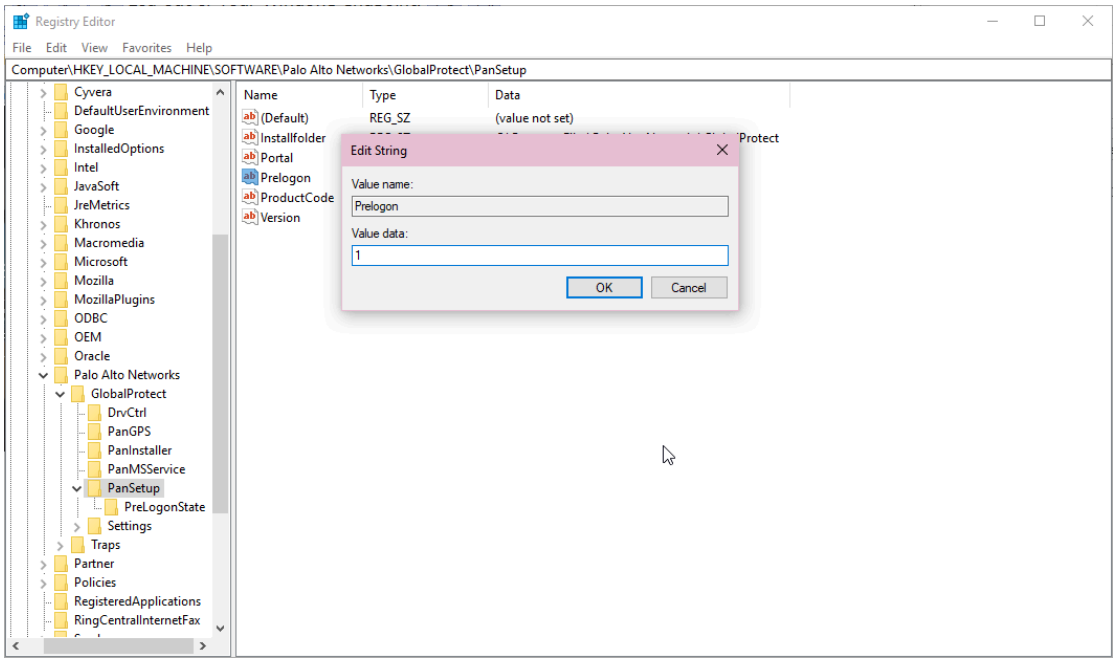
 ©2026 Palo Alto Networks, Inc.

4. Spécifiez une adresse de portail :
   1. Dans la liste des options PanSetup, faites un clic droit sur **Portal (Portail)**, puis sélectionnez **Modify... (Modifier...)** pour mettre à jour l'adresse du portail.
   2. Saisissez l'adresse du portail dans le champ **Value data (Données de valeur)**.



   3. Cliquez sur **OK** pour enregistrer vos modifications.
5. Activez la préouverture de session :
   1. Dans la liste des options PanSetup, faites un clic droit sur **Prelogon (Préouverture de session)**, puis sélectionnez **Modify... (Modifier...)**.
   2. Pour activer la préouverture de session, définissez les **Value data (Données de valeur)** sur **1**.

 ©2026 Palo Alto Networks, Inc.



Pour Désactiver la préouverture de session, définissez les ***Value data (Données de valeur)*** *sur* ***0***.

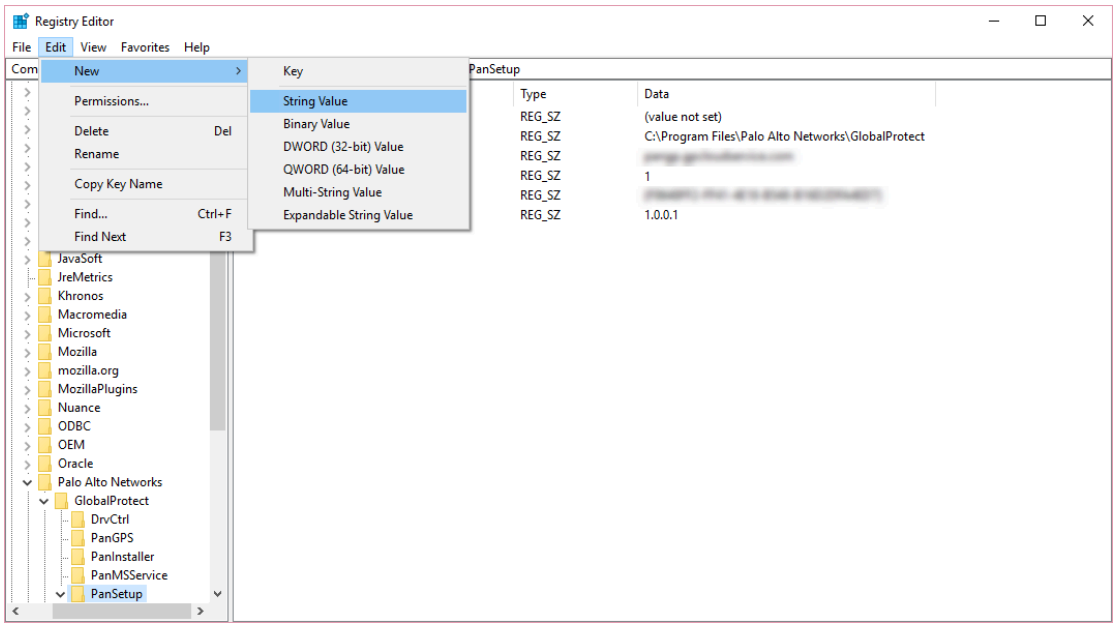
3. Cliquez sur **OK** pour enregistrer vos modifications.

6. Activer l'ouverture de session unique (SSO) :

   Lorsque vous activez l'ouverture de session unique, GlobalProtect utilise les informations d'identification de connexion Windows pour authentifier automatiquement les utilisateurs lors de la connexion Active Directory.

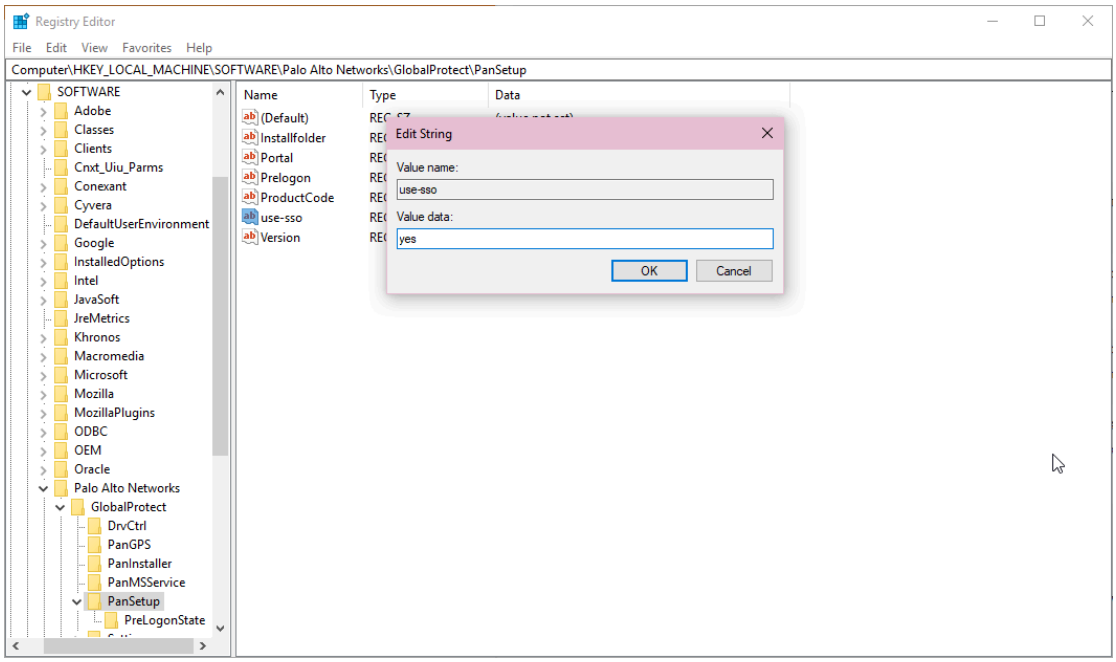
   1. Sélectionnez **Edit (Modifier)** > **New (Nouveau)** > **String Value (Valeur de chaîne)** pour ajouter l'option d'utilisation de l'ouverture de session unique.

 ©2026 Palo Alto Networks, Inc.



2. Lorsque vous y êtes invité, définissez le **Name (Nom)** sur **`use-sso (utiliser le sso)`**.
3. Faites un clic droit sur **Use-SSO (Utiliser SSO)**, puis sélectionnez **Modify... (Modifier...)** pour mettre à jour les paramètres d'ouverture de session unique.
4. Pour activer l'ouverture de session unique, définissez les **Value data (Données de valeur)** sur **`yes (oui)`**

 ©2026 Palo Alto Networks, Inc.

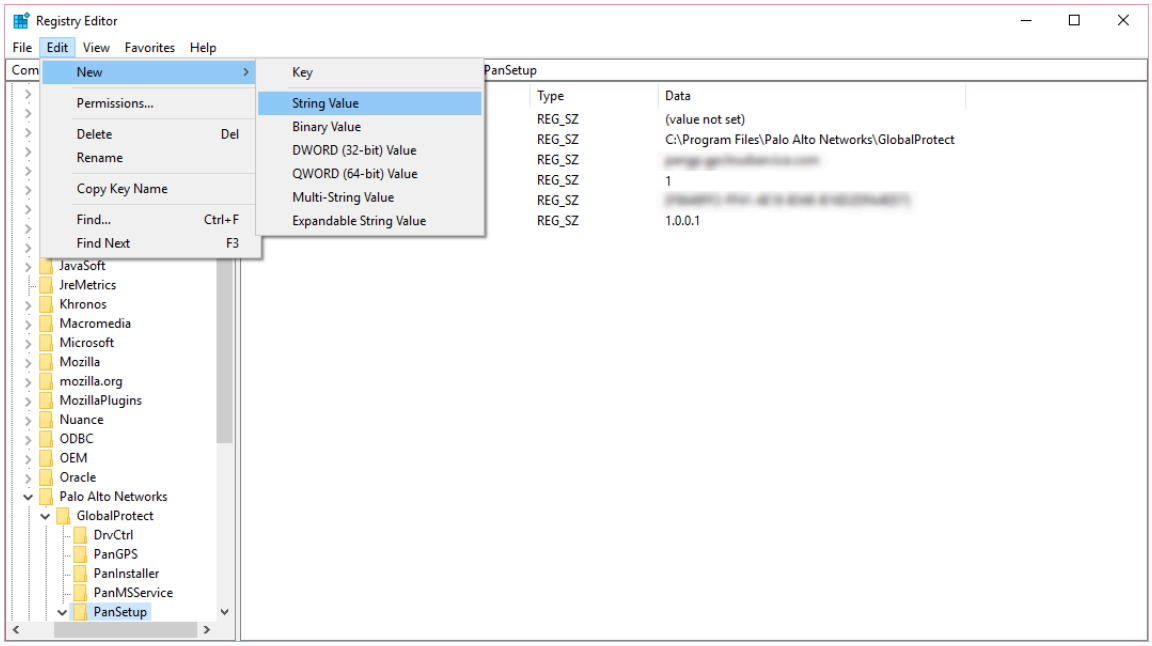


Pour désactiver l'ouverture de session unique, définissez les ***Value data (Données de valeur)*** *sur* ***no (non)***.

5. Cliquez sur **OK** pour enregistrer vos modifications.

 ©2026 Palo Alto Networks, Inc.

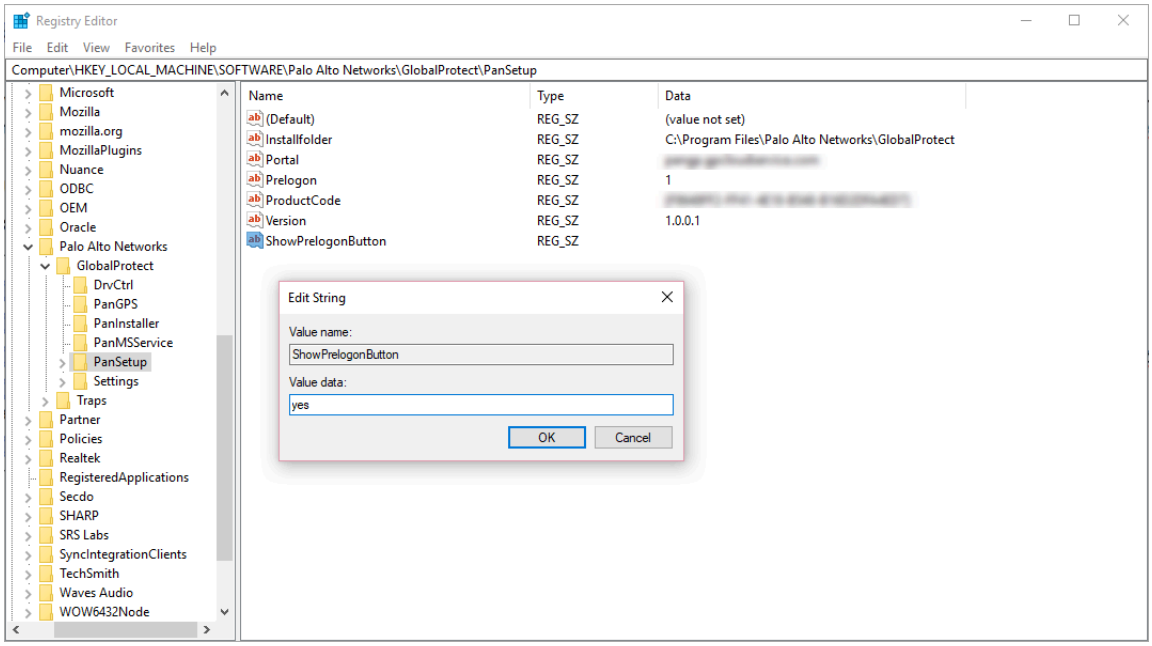
2. Dans le Registre Windows, activez l'option permettant d'afficher le bouton **Start GlobalProtect Connection (Démarrer la connexion GlobalProtect)** sur l'écran de connexion du fournisseur d'informations d'identification GlobalProtect.
   1. À partir de votre terminal Windows, lancez l'invite de commande.
   2. Entrez **`regedit`** pour ouvrir le registre Windows.
   3. Dans le registre Windows, accédez à : `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup\`.
   4. Sélectionnez **Edit (Modifier)** > **New (Nouveau)** > **String Value (Valeur de chaîne)** pour ajouter l'option d'affichage du bouton.



5. Lorsque vous y êtes invité, définissez le **Name (Nom)** sur **`ShowPrelogonButton (Afficher le bouton de préouverture de session)`**.

 ©2026 Palo Alto Networks, Inc.

6. Faites un clic droit sur **ShowPrelogonButton (Afficher le bouton de préouverture de session)**, puis sélectionnez **Modify... (Modifier...)** pour mettre à jour les paramètres d'affichage du bouton.
7. Pour permettre au fournisseur d'informations d'identification GlobalProtect d'afficher le bouton **Start GlobalProtect Connection (Démarrer la connexion GlobalProtect)**, définissez les **Value data (Données de valeur)** sur **`yes (oui)`**.



*Pour désactiver l'option **ShowPrelogonButton (Afficher le bouton de préouverture de session)**, définissez les **Value data (Données de valeur)** sur **`no (non)`**. Vous pouvez également faire un clic droit sur **ShowPrelogonButton (Afficher le bouton de préouverture de session)** pour **Delete (Supprimer)** l'option.*

8. Cliquez sur **OK** pour enregistrer vos modifications.

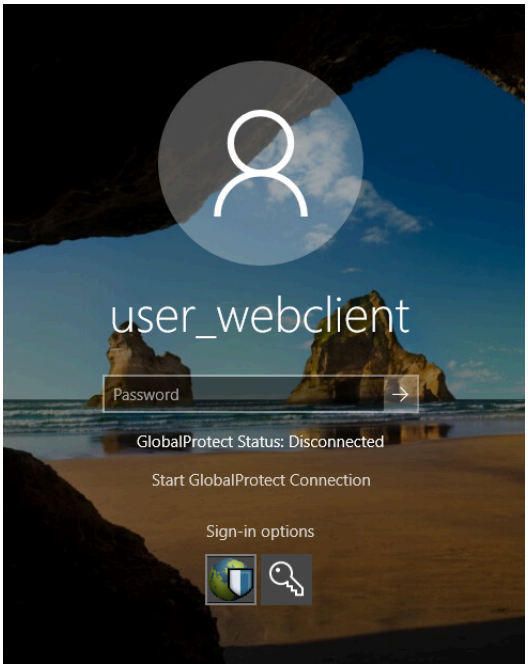
3. Vérifiez que le fournisseur d'informations d'identification GlobalProtect affiche le bouton **Start GlobalProtect Connection (Démarrer la connexion GlobalProtect**) afin que les utilisateurs puissent initier la connexion de préouverture de session manuellement.

Selon l'option que vous avez utilisée pour configurer le VPN d'accès à distance avec pré-ouverture de session (étape 1), utilisez l'une des options suivantes pour vérifier que le fournisseur d'informations d'identification GlobalProtect affiche le bouton **Start GlobalProtect Connection (Démarrer la connexion)** :

- Si vous avez configuré un VPN d'accès à distance avec préouverture de session sur votre pare-feu, suivez les étapes suivantes pour vérifier que le bouton s'affiche :
  1. À partir de votre terminal Windows, lancez l'application GlobalProtect.
  2. **Connectez-vous** à GlobalProtect pour télécharger la configuration de l'agent de portail que vous avez configurée à l'étape 1.
  3. Redémarrez votre terminal Windows.
  4. Lorsque l'écran de connexion du fournisseur d'informations d'identification GlobalProtect s'affiche, assurez-vous que le bouton **Start GlobalProtect Connection**

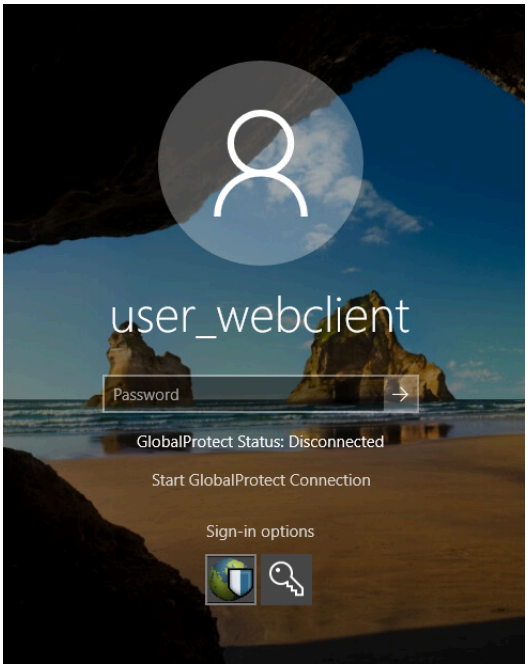
 ©2026 Palo Alto Networks, Inc.

(Démarrer la connexion GlobalProtect) s'affiche et que l'état de la connexion de préouverture de session est **Disconnected (Déconnecté)**.



- Si vous avez pré-déployé les paramètres de préouverture de session dans le Registre Windows, suivez les étapes suivantes pour vérifier que le bouton s'affiche :

  1. Redémarrez votre terminal Windows.
  2. Lorsque l'écran de connexion du fournisseur d'informations d'identification GlobalProtect s'affiche, assurez-vous que le bouton **Start GlobalProtect Connection (Démarrer la connexion GlobalProtect)** s'affiche et que l'état de la connexion de préouverture de session est **Disconnected (Déconnecté)**.



 ©2026 Palo Alto Networks, Inc.

Configuration de plusieurs passerelles GlobalProtect

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans la Topologie Passerelle Multiple GlobalProtect ci-dessous, une deuxième passerelle externe est ajoutée à la configuration. Dans cette topologie, vous devez configurer un pare-feu supplémentaire pour héberger la deuxième passerelle GlobalProtect. Lorsque vous ajoutez les configurations client qui doivent être déployées par le portail, vous pouvez également indiquer des passerelles différentes pour des configurations client différentes ou autoriser l'accès à toutes les passerelles.

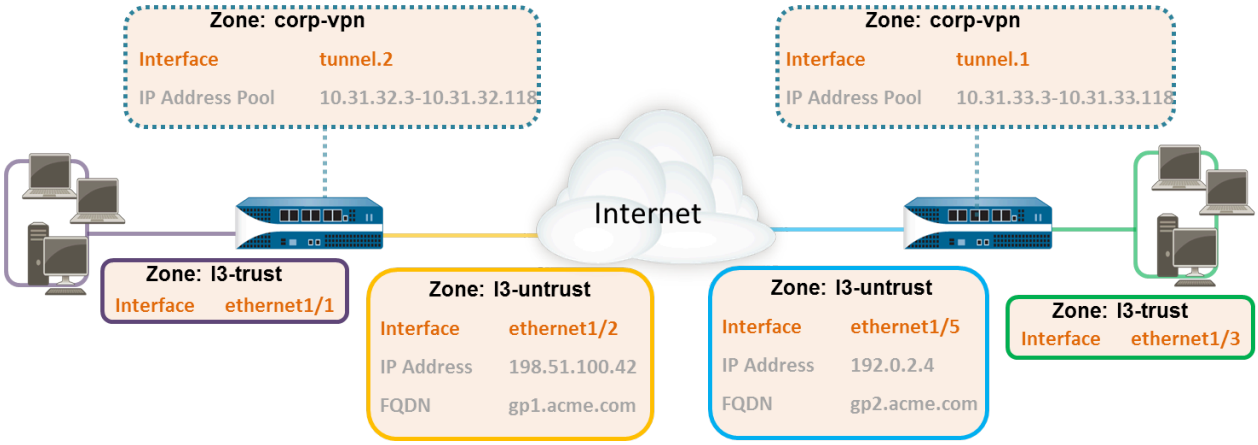


Illustration 8 : Topologie de multiples passerelles GlobalProtect

Si une configuration client contient plusieurs passerelles, l'application tente de se connecter à toutes les passerelles répertoriées dans sa configuration client. L'application utilise ensuite la priorité et le temps de réponse pour déterminer à quelle passerelle elle se connectera. L'application se connecte à une passerelle prioritaire inférieure si le temps de réponse pour la passerelle prioritaire supérieure est supérieur au temps de réponse moyen entre toutes les passerelles. Pour plus d'informations, consultez priorité de passerelle dans une configuration de passerelles multiples.

©2026 Palo Alto Networks, Inc.

1. (Requis uniquement sur NGFW géré par Panorama ou Strata Cloud Manager)Créez des interfaces et des zones pour GlobalProtect.

   Dans cette configuration, vous devez configurer des interfaces sur chaque pare-feu hébergeant une passerelle.

   *Utilisez le routeur virtuel **default (par défaut)** pour toutes les configurations d'interface pour éviter d'avoir à créer un routage inter-zone.*

   Sur le pare-feu hébergeant le portail /la passerelle (gw1) :

   - Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, puis sélectionnez **ethernet1/2**.
   - Configurez **ethernet1/2** en tant qu'interface de Couche 3 comportant une adresse IP **`198.51.100.42`**, puis affectez-la à la **Security Zone (Zone de sécurité)** **`l3-untrust`** et au **Virtual Router (Routeur virtuel)** **`default`** (par défaut).
   - Créez un dossier « A » DNS qui mappe l'adresse IP **`198.51.100.42`** en **`gp1.acme.com`**.
   - Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel**, puis **Add (Ajouter)** une interface **`tunnel.2`**. Ajoutez l'interface à une nouvelle **Security Zone (Zone de sécurité)** appelée **`corp-vpn`**. Assignez-la au **Virtual Router (Routeur virtuel)** **`default`** (par défaut).
   - Activez l'identification de l'utilisateur sur la zone **`corp-vpn`**.

   Sur le pare-feu hébergeant la seconde passerelle (gw2) :

   - Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet (Ethernet)**, puis sélectionnez **ethernet1/5**.
   - Configurez **ethernet1/5** en tant qu'interface de Couche 3 comportant une adresse IP **`192.0.2.4`**, puis affectez-la à la **Security Zone (Zone de sécurité)** **`l3-untrust`** et au **Virtual Router (Routeur virtuel)** **`default`** (par défaut).
   - Créez un dossier « A » DNS qui mappe l'adresse IP **`192.0.2.4`** en **`gp2.acme.com`**.
   - Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel**, puis **Add (Ajouter)** une interface **`tunnel.1`**. Ajoutez l'interface à une nouvelle **Security Zone (Zone de sécurité)** appelée **`corp-vpn`**. Assignez-la au **Virtual Router (Routeur virtuel)** par défaut.
   - Activez l'identification de l'utilisateur sur la zone **`corp-vpn`**.

2. Achetez et installez un abonnement à GlobalProtect sur chaque passerelle si vos utilisateurs finaux utiliseront l'application GlobalProtect sur leurs points de terminaison mobiles ou si vous prévoyez d'utiliser la politique de sécurité HIP.

   Après avoir acheté l'abonnement à GlobalProtect et reçu votre code d'activation, installez la licence sur le pare-feu hébergeant le portail.

3. Sur chaque pare-feu hébergeant une passerelle GlobalProtect, créez des politiques de sécurité.

   Cette configuration nécessite des règles de sécurité pour autoriser le flux de trafic entre la zone **`corp-vpn`** et la zone **`l3-trust (l3-de confiance)`** pour fournir l'accès à vos ressources internes (**Policies (Politiques)** > **Security (Sécurité)**).

 ©2026 Palo Alto Networks, Inc.

4. Utilisez les recommandations suivantes pour obtenir des certificats de serveur pour chaque interface qui héberge le portail GlobalProtect et les passerelles GlobalProtect :

   - (Sur le pare-feu hébergeant le portail ou le portail / la passerelle) Importez un certificat de serveur à partir d'une AC tierce reconnue.
   - (Sur un pare-feu n'acceptant qu'une passerelle) Utilisez l'autorité de certification racine sur le portail pour générer un certificat de serveur auto-signé.

   Sur chaque pare-feu hébergeant un portail ou une passerelle/portail ou une passerelle, sélectionnez **Device (Périphériques)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** pour gérer les certificats comme suit:

   - Obtenez un certificat de serveur pour l'interface hébergeant le portail/gw1. Comme le portail et la passerelle sont sur la même interface, vous devez utiliser le même certificat de serveur. Le CN du certificat doit correspondre au FQDN, `gp1.acme.com`. Pour permettre aux points de terminaison de se connecter au portail sans recevoir d'erreur de certificat, utilisez un certificat de serveur généré par une AC publique.
   - Obtenez un certificat de serveur pour l'interface hébergeant gw2. Comme cette interface héberge uniquement une passerelle, vous pouvez utiliser un certificat auto-signé. Le CN du certificat doit correspondre au FQDN, `gp.acme.com`.

5. Définissez comment vous authentifierez les utilisateurs sur le portail et les passerelles.

   Vous pouvez utiliser toutes les combinaisons de profils de certificat et/ou de profils d'authentification nécessaires pour garantir la sécurité de votre portail et passerelles. Les portails et les passerelles individuelles peuvent aussi utiliser des schémas d'authentification différents. Reportez-vous aux sections suivantes pour les instructions pas à pas :

   - Configurer l'authentification externe (profil d'authentification)
   - Configurer l'authentification du certificat client (profil de certificat)
   - Configurer l'authentification à deux facteurs (Jeton ou basé sur un MPUU)

   Vous devez ensuite référencer le profil de certificat et/ou les profils d'authentification que vous définissez dans les configurations de portail et de passerelle.

 ©2026 Palo Alto Networks, Inc.

6. Configurer une passerelle GlobalProtect.

   L'exemple suivant illustre la configuration de GP1 et GP2 affichée dans la topologie de passerelles multiples GlobalProtect.

   Sur le pare-feu qui héberge gp1, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**. Configurez les paramètres des passerelles comme suit :

   Interface : **`ethernet1/2`**

   Adresse IP : **`198.51.100.42`**

   Certificat du serveur : **`GP1-server-cert.pem issued by GoDaddy`**

   Tunnel Interface (Interface de tunnel) : **`tunnel.2`**

   IP Pool (Pool d'adresses IP) : **`10.31.32.3 - 10.31.32.118`**

   Sur le pare-feu qui héberge gp2, sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)**. Configurez les paramètres des passerelles comme suit :

   Interface : **`ethernet1/2`**

   Adresse IP : **`192.0.2.4`**

   Server Certificate (Certificat de serveur) : **`certificat auto-signé, GP2-server-cert.pem`**

   Tunnel Interface (Interface de tunnel) : **`tunnel.1`**

   IP Pool (Pool d'adresses IP) : **`10.31.33.3 - 10.31.33.118`**

7. Configurez les portails GlobalProtect.

   Configurez les paramètres du portail comme suit :

   1. Paramétrer l'accès au portail GlobalProtect:

      Interface : **`ethernet1/2`**

      Adresse IP : **`198.51.100.42`**

      Certificat du serveur : **`GP1-server-cert.pem issued by GoDaddy`**

   2. Définir les configurations Agent GlobalProtect:

      Le nombre de configurations de client que vous créez dépend de vos conditions d'accès spécifique, indiquant notamment si vous exigez une politique basée sur l'utilisateur/groupe et/ou la mise en œuvre d'une politique activée par HIP.

8. Déployer l'agent logiciel GlobalProtect.

   Dans cet exemple, suivez la procédure visant à héberger les mises à jour de l'application sur le portail.

9. Enregistrez la configuration GlobalProtect.

   Commit (Validez) la configuration sur le pare-feu hébergeant le portail et la ou les passerelle(s).

 ©2026 Palo Alto Networks, Inc.

GlobalProtect pour l'archivage HIP interne et l'accès basé sur l'utilisateur

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Lorsqu'elle est utilisée en association avec l'ID utilisateur et/ou les archivages HIP, une passerelle interne procure une méthode sécurisée et précise d'identification et de contrôle du trafic par utilisateur et/ou état du périphérique, remplaçant d'autres services de contrôle d'accès réseau (NAC). Les passerelles internes sont utiles dans des environnements fragiles qui exigent un accès authentifié aux ressources vitales.

Dans une configuration avec seulement des passerelles internes, tous les points de terminaison doivent être configurés avec une connexion utilisateur (Toujours activée)) ; le mode à la demande n'est pas pris en charge. Il est également recommandé de configurer toutes les configurations client pour utiliser l'ouverture de session unique. De même, comme les hôtes internes n'ont pas besoin d'établir une connexion tunnel avec la passerelle, l'adresse IP de la carte réseau physique sur le point de terminaison est utilisée.

Dans cette configuration rapide, les passerelles internes appliquent des stratégies basées sur le groupe qui permettent aux utilisateurs du groupe Engineering d'accéder au contrôle interne interne et aux bases de données de bogues et aux utilisateurs du groupe Finance aux applications CRM. Tous les utilisateurs qui se sont authentifiés ont accès aux ressources Web internes. En outre, les profils HIP configurés sur la passerelle vérifient chaque hôte pour garantir la conformité aux conditions de maintenance interne, par exemple si les derniers correctifs de sécurité sont installés, si le cryptage de disque est activé, ou si le logiciel requis est installé.

 ©2026 Palo Alto Networks, Inc.

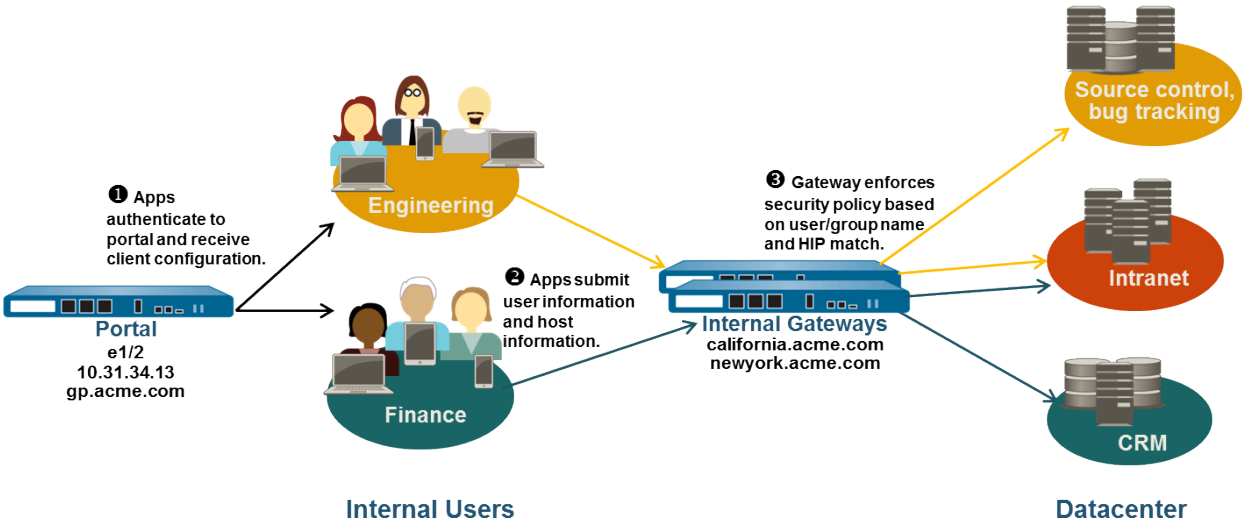


Illustration 9 : Configuration de passerelles internes GlobalProtect

Utilisez les étapes suivantes pour configurer une passerelle interne GlobalProtect.

1. (Requis uniquement sur NGFW géré par Panorama ou Strata Cloud Manager)Créez des interfaces et des zones pour GlobalProtect.

   Dans cette configuration, vous devez configurer des interfaces sur chaque pare-feu hébergeant un portail et/ou une passerelle. Comme cette configuration utilise des passerelles internes uniquement, vous devez configurer le portail et les passerelles sur des interfaces sur le réseau interne.

   > *Utilisez le routeur virtuel **default (par défaut)** pour toutes les configurations d'interface pour éviter d'avoir à créer un routage inter-zone.*

   Sur chaque pare-feu hébergeant un portail/passerelle :

   1. Sélectionnez un port Ethernet pour héberger le portail/passerelle, puis configurez une interface de couche 3 avec une adresse IP dans **`l3-trust` Security Zone (Zone de sécurité)** (**Network [Réseau]** > **Interfaces** > **Ethernet**).
   2. **Activer l'identification de l'utilisateur** sur la zone **`l3-de confiance`**.

 ©2026 Palo Alto Networks, Inc.

2. Si vos utilisateurs doivent utiliser l'application GlobalProtect sur leurs périphériques mobiles ou si vous envisagez d'utiliser une politique de sécurité activée par HIP, achetez et installez un abonnement à GlobalProtect pour chaque pare-feu hébergeant une passerelle interne.

Après avoir acheté les abonnements à GlobalProtect et reçu votre code d'activation, installez les abonnements à GlobalProtect sur les pare-feu hébergeant les passerelles.

Contactez les ingénieurs commerciaux ou le revendeur de Palo Alto Networks si vous ne disposez pas des licences requises.

3. Obtenez les certificats de serveur pour le portail GlobalProtect et chaque passerelle GlobalProtect.

Pour se connecter au portail pour la première fois, les points de terminaison doivent valider le certificat AC racine utilisé pour générer le certificat de serveur du portail. Vous pouvez soit utiliser un certificat auto-signé sur le portail et déployer le certificat AC racine sur les points de terminaison avant la première connexion au portail, soit obtenir un certificat de serveur pour le portail auprès d'une AC de confiance.

Vous pouvez utiliser des certificats auto-signés sur les passerelles.

La marche à suivre recommandée est la suivante :

1. Sur le pare-feu hébergeant le portail :
    1. Importez un certificat de serveur d'une autorité de certification tierce bien connue.
    2. Créer le certificat AC racine pour générer les certificats AC auto-signés pour les composants GlobalProtect.
    3. Utilisez l'autorité de certification racine sur le portail pour générer un certificat de serveur auto-signé. Répétez cette étape pour chaque passerelle.
2. Sur chaque pare-feu hébergeant une passerelle interne, Déployez les certificats de serveur auto-signés.

4. Définissez comment vous authentifierez les utilisateurs sur le portail et les passerelles.

Vous pouvez utiliser toutes les combinaisons de profils de certificat et/ou de profils d'authentification nécessaires pour garantir la sécurité de votre portail et passerelles. Les portails et les passerelles individuelles peuvent aussi utiliser des schémas d'authentification différents. Reportez-vous aux sections suivantes pour les instructions pas à pas :

- Configurer l'authentification externe (profil d'authentification)
- Configurer l'authentification du certificat client (profil de certificat)
- Configurer l'authentification à deux facteurs (Jeton ou basé sur un MPUU)

Vous devez ensuite référencer le profil de certificat et/ou les profils d'authentification que vous avez définis dans les configurations de portail et de passerelle.

 ©2026 Palo Alto Networks, Inc.

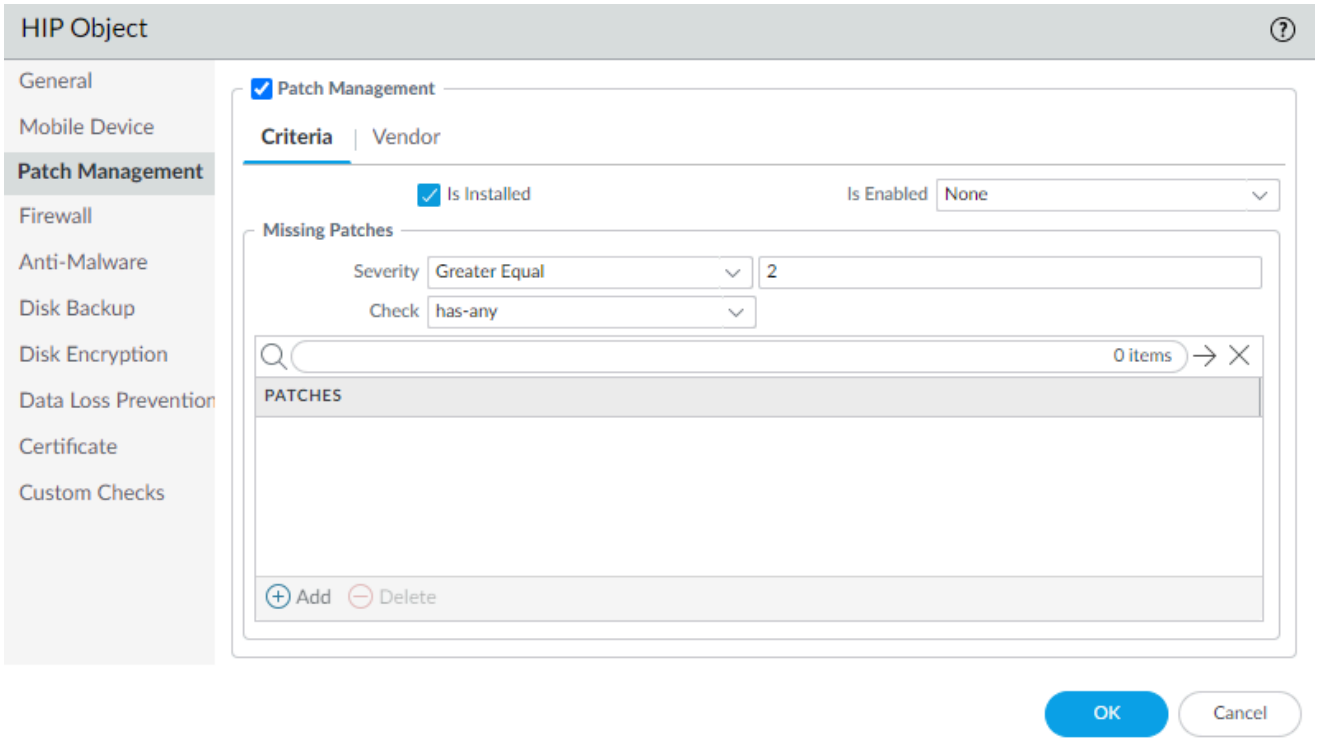
5. Créez les profils HIP dont vous avez besoin pour mettre en œuvre les politiques de sécurité sur l'accès passerelle.

   Reportez-vous à la section Informations de l'hôte pour plus d'informations sur les correspondances HIP.

   1. Créez les objets HIP pour filtrer les données brutes d'hôte collectées par l'application. Par exemple, si vous souhaitez empêcher les utilisateurs qui n'ont pas mis les correctifs requis à jour de se connecter, vous pouvez créer un objet HIP pour que le logiciel de

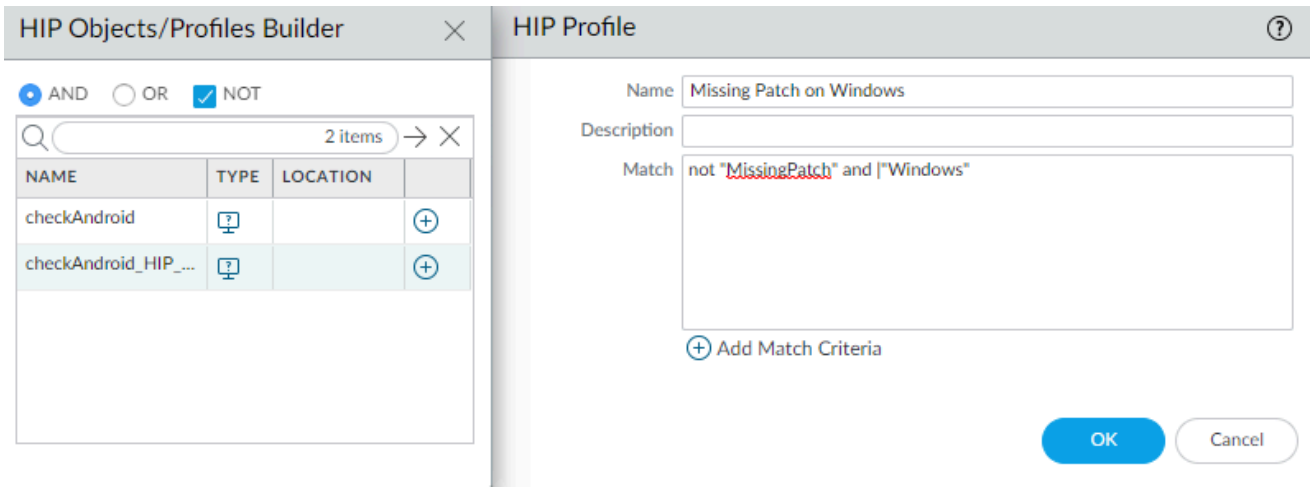
 ©2026 Palo Alto Networks, Inc.

gestion des correctifs soit installé et que tous les correctifs avec une gravité donnée soient mis à jour.



2. Créez les profils HIP que vous envisagez d'utiliser dans vos stratégies.

   Par exemple, si vous souhaitez garantir que seuls les utilisateurs Windows dont les correctifs sont à jour peuvent accéder à vos applications internes, vous pourriez associer le profil HIP suivant qui correspond aux hôtes à qui il NE manque PAS de correctif :



 ©2026 Palo Alto Networks, Inc.

6. Configurez les passerelles internes avec les paramètres suivants.

   - **Interface**
   - **Adresse IP**
   - **Certificat du serveur**
   - **Authentication Profile (Profil d'authentification)** et/ou **Configuration Profile (Profil de configuration)**

   Prenez note qu'il n'est pas nécessaire de configurer les paramètres du client dans les configurations de passerelle (sauf si vous souhaitez paramétrer des notifications HIP) parce que les connexions tunnel ne sont pas requises. Reportez-vous à la section Configurez une passerelle GlobalProtect pour obtenir des instructions étape par étape sur la création des configurations de passerelle.

7. Configurez les portails GlobalProtect.

   *Bien que toutes les configurations précédentes puissent utiliser une méthode de connexion de l'**User-logon (Always On) (Connexion utilisateur (Toujours activée))** ou **On-demand (Manual user initiated connection) (sur-demande (connexion manuelle initiale))**, une configuration de passerelle interne doit toujours être activée et nécessite donc une méthode de connexion de l'**User-logon (Always On) (Connexion utilisateur (Toujours activée))**.*

   Configurez le portail comme suit :

   1. Paramétrer l'accès au portail GlobalProtect:

      Interface : **`ethernet1/2`**

      IP Address (Adresse IP) : **`10.31.34.13`**

      Certificat du serveur : **`GP-server-cert.pem issued by GoDaddy`** avec **`CN=gp.acme.com`**
   2. Définir les configurations d'authentification client GlobalProtect:

      Use single sign-on (Utiliser l'ouverture de session unique) : **`enabled`**

      Connect Method (Méthode de connexion) : **`User-logon (Always On)`**

      Internal Gateway Address (Adresse de passerelle interne) : **`california.acme.com, newyork.acme.com`**

      User/User Group (Utilisateur / groupe d'utilisateurs) : **`any`**
   3. **Commit (Valider)** la configuration de portail.

8. Déployer le logiciel de l'application GlobalProtect.

   Sélectionnez **Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)** .

   Dans cet exemple, utilisez la procédure pour héberger les mises à jour de l'application sur le portail.

 ©2026 Palo Alto Networks, Inc.

9. Créez les règles de sécurité activées par HIP et/ou basées sur l'utilisateur/groupe sur vos passerelles.

Ajoutez les règles de sécurité suivantes pour cet exemple :

1. Choisissez l'une des actions suivantes :
   - Sur Panorama, sélectionnez **Policies (Politiques)** > **Security (Securité)**, puis **Add (Ajouter)** une nouvelle règle.
   - Sur Strata Cloud Manager, sélectionnez **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** puis **Add (Ajouter)** une nouvelle règle.
   - Sur Strata Cloud Manager, sélectionnez **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** puis **Add (Ajouter)** une nouvelle règle.
2. Dans l'onglet **Source**, définissez la **Source Zone (Zone source)** sur **l3-trust (l3-de confiance)**.
3. Dans l'onglet **User (Utilisateur)**, ajoutez le profil HIP et l'utilisateur/groupe à faire correspondre.
   - Cliquez sur **Add (Ajouter)** dans la section **HIP Profiles (Profils HIP)**, puis sélectionnez le profil HIP **MissingPatch (Correctif manquant)**.
   - **Add (Ajoutez)** le groupe **Source User (Utilisateur source)** (Finance ou Ingénierie en fonction de la règle que vous créez).
4. Cliquez sur **OK** pour enregistrer la règle.
5. **Commit (Validez)** la configuration de passerelle.

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	CRM access	none	l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	
2	Eng access	none	l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	

 ©2026 Palo Alto Networks, Inc.

Configuration mixte de passerelles internes et externes

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans une configuration mixte de passerelles internes et externes GlobalProtect, vous pouvez configurer des passerelles distinctes pour l'accès VPN et pour l'accès à vos ressources internes sensibles. Avec cette configuration, l'application GlobalProtect effectue la détection des hôtes internes pour déterminer si elle est sur le réseau interne ou externe. Si l'application détermine qu'elle est sur le réseau externe, elle tentera de se connecter aux passerelles externes répertoriées dans sa configuration de client et établit ensuite une connexion avec la passerelle offrant le niveau de priorité optimal et le temps de réponse le plus court.

> *Si vous configurez toutes les passerelles externes comme des passerelles manuelles uniquement, mais la méthode de connexion GlobalProtect en tant que* ***User-Logon (Always On) (Connexion utilisateur (Toujours activée))*** *ou* ***Pre-Logon (Always On) (Pré-connexion (toujours activée))****, l'application GlobalProtect ne se connecte pas automatiquement aux passerelles externes. GlobalProtect demeure à l'état* ***Not Connected (Non connecté)*** *jusqu'à ce que l'utilisateur externe établisse une connexion manuelle à la passerelle. Ce comportement vous permet de déployer GlobalProtect afin de dériver User-ID pour les utilisateurs internes tout en prenant le comportement de VPN* ***On-Demand (À la demande)*** *pour les utilisateurs externes.*

Comme les politiques de sécurité sont définies séparément sur chaque passerelle, vous avez un contrôle granulaire sur les ressources auxquelles vos utilisateurs externes et internes ont accès. En outre, vous avez aussi un contrôle granulaire sur les passerelles auxquelles les utilisateurs ont accès en configurant le portail pour déployer différentes configurations de client basées sur l'utilisateur ou l'appartenance à un groupe ou sur les correspondances de profil HIP.

Dans cet exemple, les portails et les trois passerelles (une externe et deux internes) sont déployés sur des pare-feu distincts. La passerelle externe à gpvpn.acme.com permet l'accès VPN à distance au réseau d'entreprise tandis que les passerelles internes permettent un accès granulaire aux ressources sensibles de centre de données basé sur l'appartenance à un groupe. En outre, les archivages HIP sont utilisés pour garantir que les hôtes accédant au centre de données sont à jour des correctifs de sécurité.

 ©2026 Palo Alto Networks, Inc.

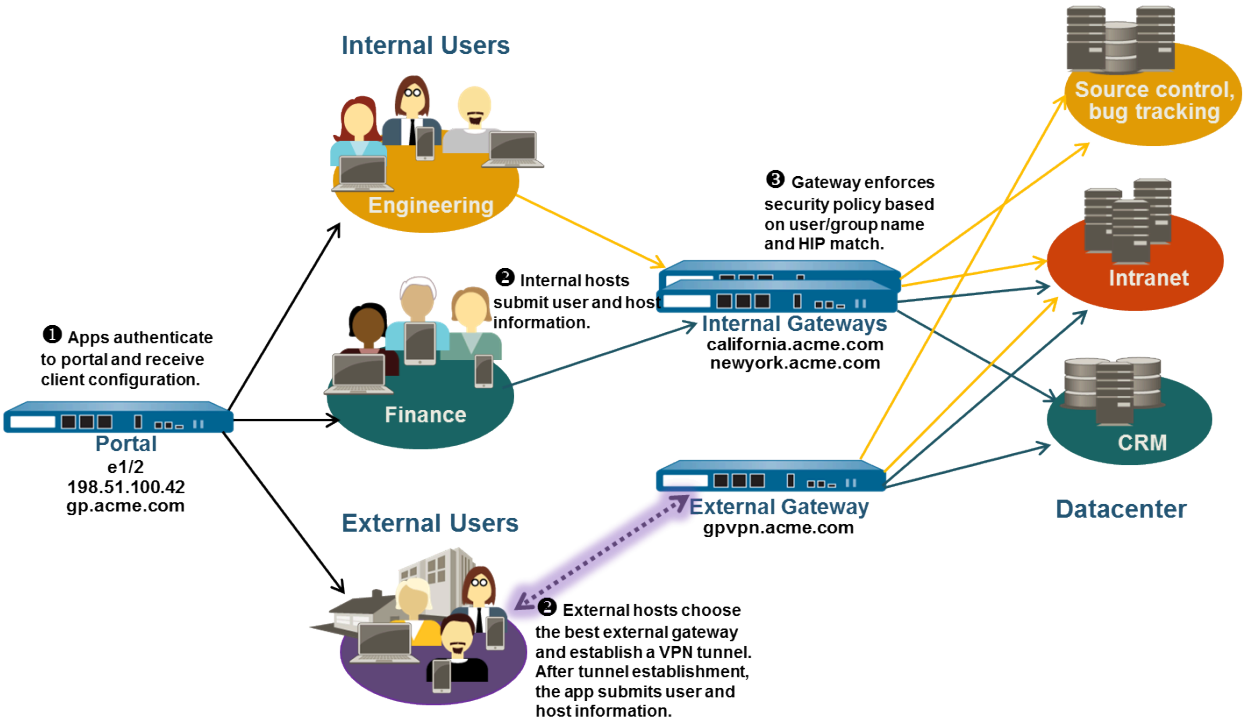


Illustration 10 : Déploiement de GlobalProtect avec des passerelles internes et externes

Utilisez les étapes suivantes pour configurer un mélange de passerelles GlobalProtect internes et externes.

 ©2026 Palo Alto Networks, Inc.

1. (Requis uniquement sur NGFW géré par Panorama ou Strata Cloud Manager)Créez des interfaces et des zones pour GlobalProtect.

Dans cette configuration, vous devez configurer des interfaces sur le pare-feu hébergeant un portail et chaque pare-feu hébergeant une passerelle.

N'attachez pas de profil de gestion d'interface qui autorise HTTP, HTTPS, Telnet ou SSH sur l'interface où vous avez configuré un portail ou une passerelle GlobalProtect, car cela permet d'accéder à votre interface de gestion depuis Internet. Suivez les Meilleures pratiques pour sécuriser l'accès administratif *afin de vous assurer que vous sécurisez l'accès administratif à vos pare-feu d'une manière qui empêchera la réussite des attaques.*

*Utilisez le routeur virtuel **default (par défaut)** pour toutes les configurations d'interface pour éviter d'avoir à créer un routage inter-zone.*

Sur le pare-feu hébergeant la passerelle du portail (gp.acme.com) :

- Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, puis configurez **ethernet1/2** en tant qu'interface Ethernet de Couche 3 avec l'adresse IP **`198.51.100.42`**. Affectez-le à la **Security Zone (Zone de sécurité)** **`l3-untrust`** et au **Virtual Router (Routeur virtuel)** par défaut.
- Créez un dossier « A » DNS qui mappe l'adresse IP 198.51.100.42 en gp.acme.com.
- Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** et **Add (Ajouter)** une interface **`tunnel.2`**. Affectez-le à une nouvelle **Security Zone (Zone de sécurité)** appelée `corp-vpn` et au **Virtual Router (Routeur virtuel)** par défaut.
- Activez l'identification de l'utilisateur sur la zone corp-vpn.

Sur le pare-feu hébergeant la passerelle externe (gpvpn.acme.com) :

- Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, puis configurez **ethernet1/5** en tant qu'interface ethernet de Couche 3 avec l'adresse IP **`192.0.2.4`**. Affectez-le à la

 ©2026 Palo Alto Networks, Inc.

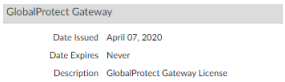
Security Zone (Zone de sécurité) **`l3-untrust`** et au **Virtual Router (Routeur virtuel)** par défaut.

- Créez un dossier « A » DNS qui mappe l'adresse IP 192.0.2.4 en gpvpn.acme.com.
- Sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Tunnel** et **Add (Ajouter)** une interface **`tunnel.3`**. Affectez-le à une nouvelle **Security Zone (Zone de sécurité)** appelée `corp-vpn` et au **Virtual Router (Routeur virtuel)** par défaut.
- Activez l'identification de l'utilisateur sur la zone corp-vpn.

Sur le pare-feu hébergeant les passerelles externes (california.acme.com et newyork.acme.com) :

- Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**, puis configurez une interface Ethernet de Couche 3 avec des adresses IP sur le réseau interne. Affectez-les à la **Security Zone (Zone de sécurité)** **`l3-trust`** et au **Virtual Router (Routeur virtuel)** par défaut.
- Créez un dossier « A » DNS qui mappe les adresses IP internes california.acme.com et newyork.acme.com.
- Activez l'identification de l'utilisateur sur la zone l3-de confiance.

2. Achetez et installez un abonnement à GlobalProtect pour chaque pare-feu hébergeant une passerelle (interne ou externe) si vos utilisateurs doivent utiliser l'application GlobalProtect sur leurs points de terminaison mobiles ou si vous envisagez d'utiliser une politique de sécurité activée par HIP.



Après avoir acheté les abonnements à GlobalProtect et reçu votre code d'activation, installez les abonnements à GlobalProtect sur les pare-feu hébergeant les passerelles.

Contactez les ingénieurs commerciaux ou le revendeur de Palo Alto Networks si vous ne disposez pas des licences requises.

 ©2026 Palo Alto Networks, Inc.

3. Obtenez les certificats de serveur pour le portail GlobalProtect et chaque passerelle GlobalProtect.

   Pour se connecter au portail pour la première fois, les points de terminaison doivent valider le certificat AC racine utilisé pour générer le certificat de serveur du portail.

   Vous pouvez utiliser des certificats auto-signés sur les passerelles et déployer le certificat AC racine sur les applications dans la configuration de client. L'idéal consiste à générer tous les certificats sur le pare-feu hébergeant le portail et à les déployer sur les passerelles.

   La marche à suivre recommandée est la suivante :

   1. Sur le pare-feu hébergeant le portail :
      1. Importez un certificat de serveur d'une autorité de certification tierce bien connue.
      2. Créer le certificat AC racine pour générer les certificats AC auto-signés pour les composants GlobalProtect.
      3. Utilisez l'autorité de certification racine sur le portail pour générer un certificat de serveur auto-signé. Répétez cette étape pour chaque passerelle.
   2. Sur chaque pare-feu hébergeant une passerelle interne :
      - Déployez les certificats de serveur auto-signés.

4. Définissez votre méthode d’authentification des utilisateurs sur le portail et les passerelles.

   Vous pouvez utiliser toutes les combinaisons de profils de certificat et/ou de profils d'authentification pour garantir la sécurité de votre portail et de vos passerelles. Les portails et les passerelles individuelles peuvent aussi utiliser des schémas d'authentification différents. Reportez-vous aux sections suivantes pour les instructions pas à pas :

   - Configurer l'authentification externe (profil d'authentification)
   - Configurer l'authentification du certificat client (profil de certificat)
   - Configurer l'authentification à deux facteurs (Jeton ou basé sur un MPUU)

   Vous devez ensuite référencer le profil de certificat et/ou les profils d'authentification que vous avez définis dans les configurations de portail et de passerelle.

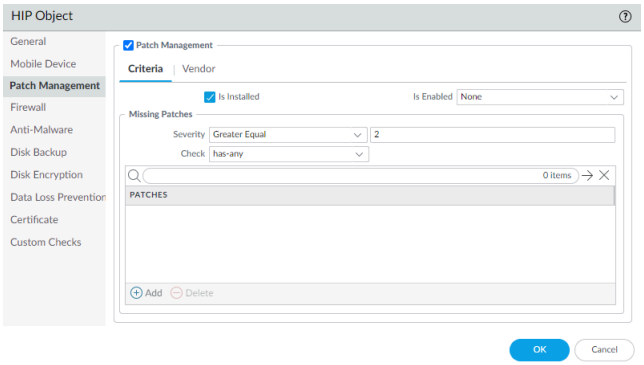
5. Créez les profils HIP dont vous aurez besoin pour mettre en œuvre une politique de sécurité sur l'accès passerelle.

   Reportez-vous à la section Informations de l’hôte pour plus d'informations sur les correspondances HIP.

   1. Créez les objets HIP pour filtrer les données brutes d'hôte collectées par l’application. Par exemple, si vous souhaitez empêcher les utilisateurs qui ne sont pas à jour avec les correctifs requis, vous pouvez créer un objet HIP pour que le logiciel de gestion des

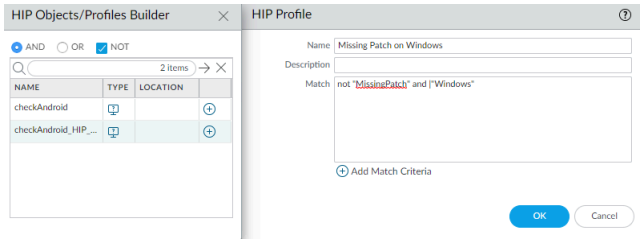
 ©2026 Palo Alto Networks, Inc.

correctifs soit installé et que tous les correctifs avec une gravité donnée soient mis à jour.



2. Créez les profils HIP que vous envisagez d'utiliser dans vos stratégies.

   Par exemple, si vous souhaitez garantir que seuls les points de terminaison Windows dont les correctifs sont à jour peuvent accéder à vos applications internes, vous pourriez associer le profil HIP suivant qui correspond aux hôtes à qui il NE manque PAS de correctif :



6. Configurez les passerelles internes.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)** et **Add (Ajoutez)** les configurations de passerelle possédant les paramètres suivants :

- **Interface**
- **Adresse IP**
- **Certificat du serveur**
- **Authentication Profile (Profil d'authentification)** et/ou **Configuration Profile (Profil de configuration)**

Remarquez qu'il n'est pas nécessaire de configurer les paramètres d'authentification client sous l'onglet Authentification de la passerelle (sauf si vous souhaitez configurer des notifications HIP), car les connexions tunnel ne sont pas requises. Reportez-vous à la section Configurez une passerelle GlobalProtect pour obtenir des instructions étape par étape sur les configurations d'une passerelle.

7. Configurez les portails GlobalProtect.

Même si cet exemple décrit comment créer une configuration de client unique qui sera déployée sur toutes les applications, vous pourriez également créer des configurations distinctes pour des utilisateurs différents et les déployer en fonction du nom de l'utilisateur/

 ©2026 Palo Alto Networks, Inc.

groupe et/ou du système d'exploitation des points de terminaison que l'application logiciel/application exécute.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)** et **Add (Ajoutez)** la configuration de portail suivante :

1. Paramétrer l'accès au portail GlobalProtect:

   Interface : **`ethernet1/2`**

   Adresse IP : **`198.51.100.42`**

   Certificat du serveur : **`GP-server-cert.pem issued by GoDaddy`** avec **`CN=gp.acme.com`**
2. Définir les configurations d'authentification client GlobalProtect:

   Internal Host Detection (Détection d'hôte interne) : **`enabled`**

   Use single sign-on (Utiliser l'ouverture de session unique) : **`enabled`**

   Connect Method (Méthode de connexion) : **`User-logon (Always On)`**

   External Gateway Address (Adresse de passerelle externe) : **`gpvpn.acme.com`**

   Internal Gateway Address (Adresse de passerelle interne) : **`california.acme.com, newyork.acme.com`**

   Utilisateur/Groupe d'utilisateurs : tous
3. **Commit (Valider)** la configuration de portail.

8. Déployer le logiciel de l'application GlobalProtect.

Dans cet exemple, utilisez la procédure pour héberger les mises à jour de l'application sur le portail.

9. Créez des règles de politique de sécurité sur chaque passerelle pour autoriser l'accès en toute sécurité aux applications aux utilisateurs de votre VPN.

- Créez des politiques de sécurité (**Policies (Politiques)** > **Security (Sécurité)**) pour autoriser le flux de trafic entre la zone corp-vpn et la zone l3-de confiance.
- Créez des règles de sécurité activées par HIP et basées sur l'utilisateur/groupe pour autoriser un accès granulaire à vos ressources de centre de données internes.
- Pour la visibilité, créez des règles qui autorisent tous les utilisateurs à accéder par la navigation Web à la zone l3-non approuvée, en utilisant les profils de sécurité par défaut pour vous protéger contre les menaces connues.

			Source				Destination					
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	CRM access	none	corp-vpn l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	✓	none
2	Eng access	none	corp-vpn l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	✓	none
3	GP access	none	corp-vpn l3-trust	any	any	any	l3-untrust	any	web-browsing	application-default	✓	

 ©2026 Palo Alto Networks, Inc.

10. Enregistrez la configuration GlobalProtect.

Commit (Validez) vos configurations de portail et de passerelle.

 ©2026 Palo Alto Networks, Inc.

Portail captif et application de GlobalProtect pour l'accès au réseau

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Dans le plupart des cas, les utilisateurs mobiles se connectent aux réseaux Wi-Fi sur lesquels un portail captif a été activé, comme les réseaux Wi-Fi des cafés, des aéroports et des hôtels. L'accès Internet n'est disponible qu'une fois que les utilisateurs se sont connectés au portail captif. Les utilisateurs peuvent se connecter via une page de connexion au portail captif qui s'affiche dans un navigateur ou d'un assistant du portail captif fondé sur le système d'exploitation qui utilise les identifiants, comme votre nom et votre adresse électronique. Avec cette configuration, vous pouvez restreindre la durée de temps pendant laquelle les utilisateurs sont connectés au portail captif. Si l'utilisateur réussit à se connecter et que l'Internet est accessible, l'application GlobalProtect établit automatiquement une connexion. Si l'utilisateur n'arrive pas à se connecter au cours de la période de temps précisée, tout le trafic est bloqué.

Pour réduire davantage le risque d'exposer votre réseau à des menaces de sécurité, vous pouvez également Application de GlobalProtect pour l'accès au réseau. Lorsque vous activez cette option, GlobalProtect bloque tout le trafic du réseau jusqu'à ce que l'application se connecte à une passerelle GlobalProtect. Tout le trafic doit passer par le tunnel VPN à des fins d'inspection et d'application de la politique, ce qui vous permet de préserver une visibilité et un contrôle intégraux du trafic de vos utilisateurs.

Selon la présence d'un portail captif et la nécessité de disposer d'une connexion GlobalProtect pour accéder au réseau, les utilisateurs doivent suivre un flux de travail spécifique pour accéder au réseau :

portail captif	Application de GlobalProtect pour l'accès au réseau	Flux de production
Oui	Oui	Si la connexion à GlobalProtect est requise pour accéder au réseau et que vos utilisateurs finaux doivent également se connecter à un portail captif pour accéder à l'Internet, ils doivent suivre les étapes suivantes pour accéder au réseau : **1.** Se connecter au réseau Wi-Fi. Une fois que vous êtes connecté au réseau Wi-Fi, GlobalProtect détecte automatiquement le portail captif. Si votre administrateur configure un message de

 ©2026 Palo Alto Networks, Inc.

portail captif	Application de GlobalProtect pour l'accès au réseau	Flux de production
		détection du portail captif, l'application GlobalProtect vous avise que vous devez vous connecter au portail captif pour accéder au réseau. *Les administrateurs peuvent également configurée la durée après laquelle le message de détection du portail captif s'affiche.* **2.** Utilisez l'une des options suivantes pour vous connecter au portail captif : • Ouvrez un navigateur Web pour vous connecter à la page de connexion du portail captif. • Connectez-vous au système d'exploitation du point de terminaison par l'intermédiaire de l'assistant intégré au portail captif. Si la connexion au portail captif réussit, l'Internet devient accessible et l'application GlobalProtect se connecte automatiquement. Si l'application ne se connecte pas automatiquement et que votre administrateur configure un message de notification de blocage du trafic pour indiquer que vous devez vous connecter à GlobalProtect pour accéder au réseau, ce message s'affiche jusqu'à ce que la connexion soit établie. *Les administrateurs peuvent également configurée la durée après laquelle le message de notification du blocage du trafic s'affiche.* Si la connexion au portail captif échoue et que la page de connexion au portail captif expire ou que GlobalProtect n'arrive pas à établir une connexion, vous accès au réseau sera bloqué. Pour rétablir la connexion au portail et relancer la durée de connexion au portail captif, lancez l'application GlobalProtect, puis sélectionnez **Refresh Connection (Actualiser la connexion)** dans le menu des paramètres de l'application ( ).
Oui	Non	Si vos utilisateurs finaux doivent se connecter à un portail captif pour accéder à l'Internet, mais que la connexion GlobalProtect n'est pas requise pour accéder au réseau, ils doivent suivre les étapes suivantes pour accéder au réseau :

 ©2026 Palo Alto Networks, Inc.

portail captif	Application de GlobalProtect pour l'accès au réseau	Flux de production
		1. Se connecter au réseau Wi-Fi. Une fois que vous êtes connecté au réseau Wi-Fi, GlobalProtect détecte automatiquement le portail captif. 2. Utilisez l'une des options suivantes pour vous connecter au portail captif : • Ouvrez un navigateur Web pour vous connecter à la page de connexion du portail captif. • Connectez-vous au système d'exploitation du point de terminaison par l'intermédiaire de l'assistant intégré au portail captif. Si la connexion réussit et que l'Internet devient accessible, l'application GlobalProtect se connecte automatiquement.
Non	Oui	Si la connexion à GlobalProtect est requise pour accéder au réseau, mais que vos utilisateurs finaux n'ont pas à se connecter à un portail captif pour accéder à l'Internet, ils doivent se connecter au réseau Wi-Fi. Une fois le Wi-Fi connecté et l'Internet accessible, l'application GlobalProtect se connecte automatiquement. Si l'application ne se connecte pas automatiquement et que votre administrateur configure un message de notification de blocage du trafic pour indiquer que vous devez vous connecter à GlobalProtect pour accéder au réseau, ce message s'affiche jusqu'à ce que la connexion soit établie. Si GlobalProtect n'arrive pas à établir une connexion, vous n'aurez pas accès au réseau. Vous devez rétablir la découverte du réseau en vous déconnectant, puis en vous reconnectant au réseau Wi-Fi, en redémarrant votre point de terminaison ou en actualisant la connexion à GlobalProtect.

Utilisez les étapes suivantes pour personnaliser les paramètres du portail captif et pour indiquer si la connexion à GlobalProtect est requise pour accéder au réseau :

*Configurez l'option **Enforce GlobalProtect for Network Access (Appliquer GlobalProtect pour l'accès au réseau)** uniquement si vous connectez GlobalProtect au moyen de la méthode de connexion toujours active.*

1. Paramétrer l'accès au portail GlobalProtect.
2. Définir les configurations de l'agent GlobalProtect.

 ©2026 Palo Alto Networks, Inc.

3. Personnaliser l'application GlobalProtect.

- Pour vous assurer que la connexion à GlobalProtect est toujours active, définissez la **Connect Method (Méthode de connexion)** sur **User-logon (Always On) (Ouverture de session utilisateur [Toujours active])**.
- Si vos utilisateurs doivent se connecter à un portail captif pour accéder à l'Internet, vous pouvez personnaliser les paramètres du portail captif en configurant les options suivantes :
  - Dans le champ **Captive Portal Exception Timeout (sec) (Délai d'envoi d'une exception dans le portail captif (secondes))**, saisissez la période de temps (en secondes) au cours de laquelle les utilisateurs peuvent se connecter au portail captif (la plage est comprise entre 0 et 3 600 secondes ; la valeur par défaut est de 0 seconde). Si les utilisateurs ne se connectent pas au cours de cette période, la page de connexion au portail captif expire et les utilisateurs ne peuvent pas utiliser le réseau.

    Pour le portail captif de navigateur intégré, le délai d'exception recommandé pour le portail captif (en seconde) est de 0 car le trafic du portail captif de navigateur intégré est implicitement autorisé.
  - Pour que l'application GlobalProtect informe les utilisateurs de la détection d'un portail captif, définissez l'option **Display Captive Portal Detection Message (Afficher le message de détection du portail captif)** sur **Yes (Oui)**.
    - Dans le champ **Captive Portal Notification Delay (sec) (Délai de notification du portail captif (secondes))**, saisissez la période de temps (en secondes) à l'issue de laquelle l'application GlobalProtect affiche le message de détection du portail captif (la plage est comprise entre 0 et 120 secondes ; la valeur par défaut est de 5 secondes). GlobalProtect lance la minuterie après que le portail captif a été détecté, mais avant que l'Internet devienne accessible.
    - Personnalisez le **Captive Portal Detection Message (Message de détection du portail captif)** qui s'affiche lorsque GlobalProtect détecte un portail captif.
- Pour forcer tout le trafic du réseau à passer par le tunnel VPN de GlobalProtect, configurez les options suivantes :
  - Définissez l'option **Enforce GlobalProtect for Network Access (Appliquer GlobalProtect pour l'accès au réseau.)** sur **Yes (Oui)**.
  - Pour que l'application GlobalProtect avise les utilisateurs qu'une connexion à GlobalProtect est requise pour accéder au réseau, définissez l'option **Display Traffic Blocking Notification Message (Afficher le message de notification de blocage du trafic)** sur **Yes (Oui)**. L'application GlobalProtect affiche ce message lorsque l'Internet devient accessible, mais avant l'établissement de la connexion à GlobalProtect.
    - Dans le champ **Traffic Blocking Notification Delay (sec) (Délai de notification du blocage du trafic (secondes))**, saisissez la période de temps (en secondes) à l'issue de laquelle l'application GlobalProtect affiche le message notification de blocage du trafic (la plage est comprise entre 5 et 120 secondes ; la valeur par défaut est de 15 secondes). GlobalProtect initie cette minuterie lorsque l'Internet devient accessible.
    - Personnalisez le **Traffic Blocking Notification Message (Message de notification de blocage du trafic)** qui s'affiche lorsque la connexion à GlobalProtection est requise pour accéder au réseau. Ce message doit contenir 512 caractères maximum.

 ©2026 Palo Alto Networks, Inc.

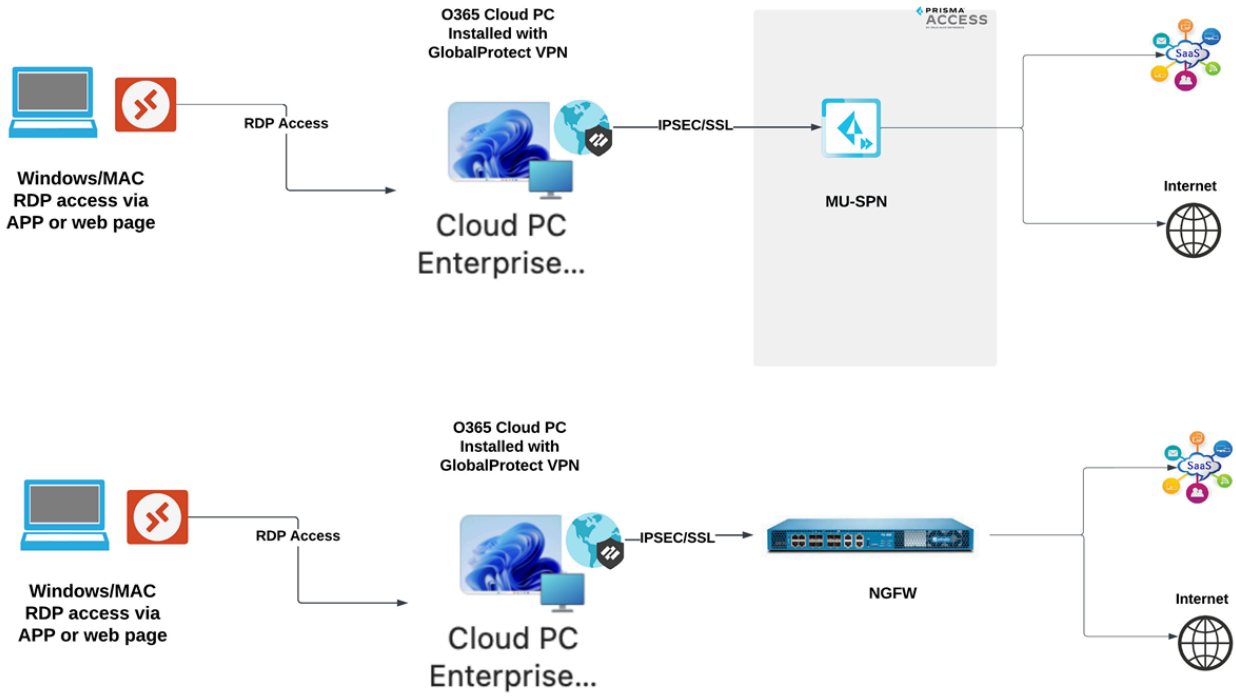
4. **Validez** les modifications.

 ©2026 Palo Alto Networks, Inc.

GlobalProtect sur les PC Cloud Windows 365

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (géré par Panorama ou Strata Cloud Manager) • Prisma Access (géré par Panorama ou Strata Cloud Manager)	GlobalProtect 6.2.6-c857 et versions ultérieures 6.2.x ou 6.3.2 et versions ultérieures 6.3.x Licence de passerelle GlobalProtect ou licence Prisma Access avec l'abonnement Utilisateur mobile

Un PC Cloud Windows 365 est une machine virtuelle qui offre une expérience de bureau Windows dans le cloud. Vous pouvez déployer GlobalProtect sur les PC Cloud pour renforcer la sécurité réseau des environnements de bureau virtuels basés sur le Cloud. Les utilisateurs Windows et macOS peuvent se connecter au PC cloud via le protocole RDP (Remote Desktop), leur permettant d'accéder à des applications privées hébergées dans le cloud. GlobalProtect achemine le trafic réseau via Prisma Access, offrant une défense supplémentaire contre les accès non autorisés et les menaces.



Suivez les étapes ci-dessous pour déployer GlobalProtect sur un PC Cloud Windows 365 :

1. Préparez le contenu de l'application Win32 pour le chargement.

   Au cours de cette étape, vous configurez les paramètres du client GlobalProtect et préparez le package d'installation.

 ©2026 Palo Alto Networks, Inc.

2. Ajoutez l'application Win32 à Microsoft Intune.

Au cours de cette étape, vous ajoutez l'application GlobalProtect à Intune et configurez les paramètres de déploiement. Le système pousse ensuite l'installation GlobalProtect vers les PC Cloud désignés en fonction des paramètres et des groupes que vous avez spécifiés. L'application GlobalProtect est installée lorsque le PC Cloud reçoit et traite cette instruction de déploiement d'Intune.

Il est recommandé de régler le **User Switch Tunnel Rename Timeout (Délai d'expiration pour renommer le tunnel de bascule d'utilisateur)** sur la valeur maximale pour éviter que GlobalProtect soit déconnecté lorsque le tunnel RDP est déconnecté ou fermé. La plage de valeurs de **User Switch Tunnel Rename Timeout (Délai d'expiration pour renommer le tunnel de bascule d'utilisateur)** est la suivante :

- Versions 6.2.x de GlobalProtect jusqu'à la version 6.2.8 : 0 à 600 secondes
- GlobalProtect version 6.2.8 et suivantes : 0 à 7 200 secondes

Pour un flux RDP ininterrompu entre l'hôte et le PC cloud, vous devez exclure le trafic réseau Microsoft de l'une des manières suivantes :

- Exclure Wildcard FQDN (*.wvd.microsoft.com) et les étiquettes du service Windows Virtual Desktop. Vous pouvez obtenir des informations IP pour l'étiquette de service Windows Virtual Desktop manuellement avec le fichier Azure IP Ranges JSON. Pour plus d'informations, reportez-vous à Plages d'adresses IP Azure et balises de service : Cloud public. Vous pouvez également utiliser un script PowerShell pour obtenir les IP dans un format CSV.

  Comme le nombre d'adresses IP dépasse 200 entrées, vous devrez peut-être utiliser une segmentation du tunnel avancée. Il est recommandé de configurer le contournement avec des FQDN génériques, car les FQDN ne changent pas au fil du temps. Vous pouvez également ajouter d'autres terminaux de service à votre chemin optimisé. Pour plus d'informations, reportez-vous à la Configuration réseau requise pour Microsoft. Si votre solution ne prend pas en charge les noms de domaine complets génériques, vous pouvez utiliser des adresses IP pour la configuration de contournement. Actuellement, Microsoft ne fournit que des adresses IP pour la connectivité RDP.

 ©2026 Palo Alto Networks, Inc.

- Exclure les voies d'accès et domaines suivants :
  - Liste d'exclusion de l'exécutant :
    - 40.64.144.0/20
    - 20.202.0.0/16
    - 51.5.0.0/16
    - *.wvd.microsoft.com
  - Liste d'exclusion de la segmentation du tunnel :
    - 40.64.144.0/20
    - 20.202.0.0/16
    - 51.5.0.0/16
    - *.wvd.microsoft.com

    Le tableau ci-dessous fournit plus de détails sur la liste d'exclusion :

Type de contournement	Valeur	Description	Notes
FQDN	FQDN *.wvd.microsoft.com	Contournement RDP basé sur TCP	TCP uniquement (le ou les sous-réseaux UDP doivent être ajoutés selon les besoins)
IP	40.64.144.0/20	Contournement RDP basé sur TCP	La plage IP devrait être pleinement utilisée d'ici la fin de janvier 2025 (consolidation à partir de ~380 /32 s actuels)
IP	20.202.0.0/16	Contournement RDP basé sur UDP via TURN (Courant)	Les relais TURN sont actuellement utilisés et seront interrompus une fois le sous-réseau 51.5.0.0/16 utilisé.
IP	51.5.0.0/16	Contournement RDP basé sur UDP via TURN (Actuel)	Utilisation future (arrivée prévue : début 2025) –Nouveau Infrastructure dédiée

 ©2026 Palo Alto Networks, Inc.

Type de contournement	Valeur	Description	Notes
			TURN à Windows 365/AVD

Vérifiez auprès de Microsoft si des sous-réseaux ou des domaines supplémentaires sont nécessaires pour exclure le trafic RDP.

TURN le trafic pour RDP Shortpath contournera la configuration de la segmentation du tunnel et par la suite, pour appliquer la configuration de la segmentation du tunnel, vous devez implémenter la politique de sécurité pour bloquer les sessions à travers le tunnel.

3. Examinez les journaux d'événements sur l'hôte Windows et les journaux d'applications gérées sur Intune pour confirmer que l'application GlobalProtect a bien été déployée sur le PC Cloud.

Fonctionnalités et limites prises en charge

Pour une liste des fonctionnalités GlobalProtect prises en charge sur les PC Cloud Windows 365, consultez la matrice de compatibilité.

Se connecter avant identification n'est pas pris en charge sur les PC Cloud Windows 365. En effet, la session Remote Desktop Protocol (protocole de prise de contrôle à distance des postes - RDP) vers le PC Cloud est établie à l'aide d'informations d'identification pré-authentifiées, permettant à l'utilisateur de se connecter directement sans utiliser l'écran de connexion Windows. De plus, la session RDP se ferme dès que l'utilisateur se déconnecte. C'est le comportement attendu de l'architecture des PC Cloud Microsoft. Étant donné que l'option Se connecter avant identification nécessite l'écran de connexion Windows pour fonctionner, il n'est pas compatible dans cet environnement.

Préouverture de session est pris en charge sur le PC Cloud Windows 365 pour les scénarios suivants :

- Redémarrage du PC Cloud – après un redémarrage, le PC Cloud établit le tunnel de préouverture de session jusqu'à ce que l'utilisateur se connecte.
- Déconnexion du PC Cloud – lorsque l'utilisateur est déconnecté du PC, le tunnel de préouverture de session est établi et reste connecté jusqu'à ce que l'utilisateur se reconnecte.

La déconnexion du PC Cloud ou la fermeture de la fenêtre du PC Cloud sont traitées comme des événements de verrouillage. En conséquence, GlobalProtect continue d'utiliser le tunnel d'ouverture de session utilisateur et ne passe pas au tunnel de pré-ouverture de session. Ceci est le comportement attendu.

 ©2026 Palo Alto Networks, Inc.