Guide de l'administrateur GlobalProtect

Version 9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

June 4, 2020

Table of Contents

Vue d'ensemble de GlobalProtect

Que ce soit en effectuant une vérification du courrier électronique depuis le domicile ou une mise à jour des documents de l'entreprise depuis un aéroport, la majorité des employés d'aujourd'hui travaillent à l'extérieur du périmètre physique de l'entreprise. La mobilité de cette main-d'œuvre accroît la productivité et la flexibilité tout en introduisant simultanément des risques significatifs pour la sécurité. Chaque fois que des utilisateurs quittent le bâtiment avec leurs ordinateurs portables ou leurs téléphones intelligents, ils contournent le pare-feu de l'entreprise et les politiques associées, qui sont conçues pour protéger aussi bien l'utilisateur que le réseau. GlobalProtect™ résout les défis de sécurité introduits par les utilisateurs nomades en élargissant les mêmes politiques basées sur pare-feu de nouvelle génération qui sont mises en œuvre à l'intérieur du périmètre physique à tous les utilisateurs, quelle que soit leur localisation.

Les sections suivantes fournissent des informations conceptuelles sur l'offre promotionnelle GlobalProtect de Palo Alto Networks et décrivent les composants et les différents scénarios de déploiement de GlobalProtect :

- À propos des composants GlobalProtect
- Quelles sont les versions de système d'exploitation prises en charge par GlobalProtect ?
- Quelles fonctionnalités GlobalProtect supporte-t-il ?
- À propos des Licences GlobalProtect

À propos des composants GlobalProtect

GlobalProtect propose une infrastructure complète pour la gestion de votre personnel mobile pour permettre un accès sécurisé à tous vos utilisateurs, indépendamment des points de terminaison qu'ils utilisent ou de l'endroit où ils se trouvent. L'infrastructure inclut les composants suivants'A0;:

- Portail GlobalProtect
- Passerelles GlobalProtect
- Application GlobalProtect

Portail GlobalProtect

Le portail GlobalProtect fournit les fonctions de gestion de votre infrastructure GlobalProtect. Chaque point de terminaison qui fait partie du réseau GlobalProtect reçoit des informations de configuration du portail, notamment des informations disponibles sur les passerelles ainsi que les certificats clients pouvant être requis pour se connecter aux passerelles GlobalProtect. De plus, le portail contrôle le comportement et la distribution du logiciel de l'application GlobalProtect à la fois sur les points de terminaison Windows et MacOS (sur les terminaux mobiles: l'application GlobalProtect est distribuée via l'App Store de Apple pour les terminaux iOS, via Google Play pour les terminaux Android et Chromebooks, via le Microsoft Store pour les terminaux Windows 10 UWP). Si vous utilisez la fonction Profil d'informations sur l'hôte (HIP), le portail définit aussi les informations qui devront être collectées auprès de l'hôte, notamment les informations personnalisées dont vous avez besoin. Vous pouvez Paramétrer l'accès au portail GlobalProtect sur l'interface de n'importe quel pare-feu de dernière génération Palo Alto Networks.

Passerelles GlobalProtect

Les passerelles GlobalProtect permettent la mise en œuvre de la sécurité du trafic depuis les applications GlobalProtect. En outre, si la fonction HIP est activée, la passerelle génère un rapport HIP à partir des données brutes sur l'hôte que les applications soumettent et peut utiliser ces informations dans la mise en œuvre des politiques. Vous pouvez configurer différents Types de passerelles pour fournir à vos utilisateurs distants un accès au réseau privé virtuel (VPN) et/ou une mise en œuvre de la sécurité, ou pour appliquer une politique de sécurité pour l'accès aux ressources internes.

Vous pouvez Configurer une passerelle GlobalProtect sur l'interface de n'importe quel pare-feu de dernière génération Palo Alto Networks. 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.

Application GlobalProtect

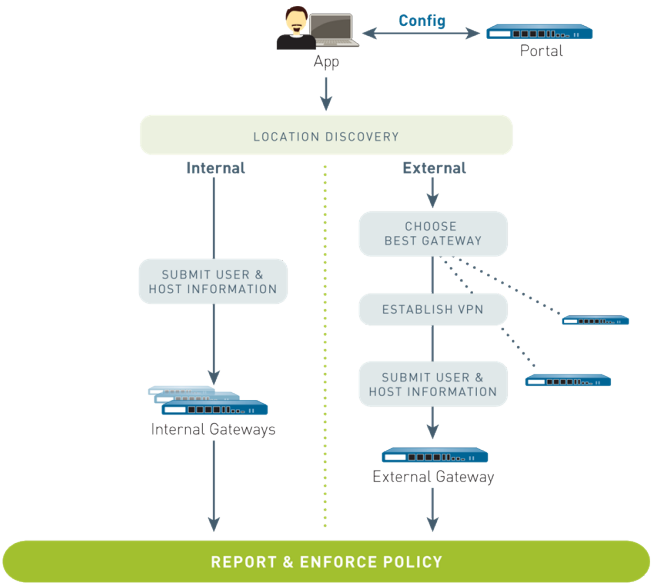
Le logiciel de l'application GlobalProtect fonctionne sur les points de terminaison des utilisateurs finaux et permet l'accès à vos ressources réseau via les portails et passerelles GlobalProtect que vous avez déployés.

L'application GlobalProtect pour les points de terminaison Windows et MacOS se déploie depuis le portail GlobalProtect. Vous pouvez configurer le comportement de l'application, par exemple, les onglets que les utilisateurs peuvent voir dans la ou les configuration(s) du client que vous définissez sur le portail. Voir Définir les configurations de l'application GlobalProtect, Personnaliser l'application GlobalProtect et Déployer le logiciel de l'application GlobalProtect pour plus de détails.

L'application GlobalProtect pour les terminaux mobiles (iOS, Android et Windows UWP) est disponible sur le magasin officiel du terminal, soit l'App Store de Apple pour iOS, Google Play pour Android et le Microsoft Store pour Windows UWP. Vous pouvez éventuellement Déployer l'application mobile GlobalProtect à l'aide de AirWatch, un système de gestion des points de terminaison mobile tiers.

Voir la section Quelles versions d'OS sont prises en charge par GlobalProtect ? pour obtenir plus de détails.

Le schéma suivant illustre la façon dont les portails, passerelles et applications GlobalProtect fonctionnent ensemble pour activer l'accès sécurisé à tous vos utilisateurs, indépendamment des points de terminaison qu'ils utilisent ou de l'endroit où ils se trouvent.



Quelles sont les versions de système d'exploitation prises en charge par GlobalProtect ?

L'application GlobalProtect est prise en charge sur les ordinateurs de bureau, les ordinateurs portatifs, les tablettes et les téléphones intelligents les plus courants. Nous vous recommandons de configurer GlobalProtect sur les pare-feu exécutant PAN-OS 6.1 ou une version ultérieure et de demander à vos utilisateurs finaux d'installer uniquement les versions prises en charge de l'application GlobalProtect sur leurs points de terminaison. La version minimale de l'application GlobalProtect varie selon le système d'exploitation. Pour déterminer la version minimale de l'application GlobalProtect pour un système d'exploitation spécifique, reportez-vous aux rubriques suivantes dans la matrice de compatibilité Palo Alto Networks® :

- Où puis-je installer l'application GlobalProtect?
- Quels clients X-Auth IPsec sont supportés ?

Les versions antérieures de l'app GlobalProtect sont toujours prises en charge sur les systèmes d'exploitation et les versions Pan-OS avec lesquelles elles ont été livrées. Pour connaître la version minimale de PAN-OS prise en charge, reportez-vous aux notes de publication de l'application GlobalProtect correspondant à la version spécifique sur le site des Software Updates (Mises à jour logicielles).

À propos des Licences GlobalProtect

Si vous souhaitez utiliser GlobalProtect pour fournir une solution d'accès à distance sécurisée ou un réseau privé virtuel (VPN) via des passerelles internes/externes uniques ou multiples, vous n'avez pas besoin de disposer de licences GlobalProtect. Cependant, pour utiliser certaines fonctionnalités plus avancées (comme les vérifications HIP et les mises à jour de contenu associées, la prise en charge de l'application mobile GlobalProtect ou la prise en charge d'IPv6), vous devez acheter un abonnement annuel à GlobalProtect. Cette licence doit être installée sur chaque pare-feu exécutant une ou plusieurs passerelles qui :

- effectuent des vérifications HIP ;
- prennent en charge l'application GlobalProtect pour les points de terminaison mobiles ;
- prennent en charge l'application GlobalProtect pour les points de terminaison Linux ;
- fournissent des connexions IPv6 ;
- segmentent les tunnels en fonction du domaine de destination, du nom de processus d'application ou de l'application de diffusion vidéo en continu HTTP/HTTPS.

Pour le VPN sans client GlobalProtect, vous devez également installer un abonnement GlobalProtect sur le pare-feu qui héberge le VPN sans client du portail GlobalProtect. Vous avez également besoin des mises à jour dynamiques de **GlobalProtect Clientless VPN (VPN sans client GlobalProtect)** pour utiliser cette fonctionnalité.

Fonctionnalité	Abonnement requis ?
Passerelle externe unique (Windows et MacOS)	—
Passerelles internes uniques ou multiples	—
Passerelles externes multiples	—
Périphériques Internet des objets (IoT)	—
Archivages HIP	✓
Configurations d'agent fondées sur le certificat machine du terminal, numéro de série du terminal et paramètres du logiciel et de l'application (un abonnement à GlobalProtect n'est requis que lors d'une utilisation avec des vérifications HIP)	✓
Application des politiques basées sur HIP en fonction de l'état du terminal	✓
Application pour les points de terminaison exécutant Windows et MacOS.	—
Application mobile pour les points de terminaison exécutant iOS, Android, Chrome OS et les applications UWP de Windows 10.	✓
Application pour les points de terminaison exécutant Linux.	✓

Fonctionnalité	Abonnement requis ?
IPv6 pour les passerelles externes	✓
IPv6 pour les passerelles internes (changement apporté au comportement par défaut—à compter de la version 4.1.3 de l'application GlobalProtect, un abonnement GlobalProtect n'est pas nécessaire pour ce cas d'utilisation)	—
VPN sans client	✓
Segmentation des tunnels en fonction du domaine de destination, du processus client ou de l'application de diffusion vidéo en continu.	✓

Reportez-vous à la section Activer les licences pour plus d'informations sur l'installation de licences sur le pare-feu.

Mise en route

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

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?

Pour plus d'informations sur les portails et les passerelles, consultez les composants GlobalProtect.

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

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.

STEP 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 (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.

STEP 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`**.

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

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

Activer SSL entre les composants GlobalProtect

Toutes les interactions entre les composants GlobalProtect se produisent sur une connexion SSL/TLS. C'est pourquoi vous devez générer et/ou installer les certificats requis avant de configurer chaque composant pour que vous puissiez référencer le ou les certificats approprié(s) 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

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.
- **Autorité de certification d'entreprise** : Si vous avez déjà votre propre AC d'entreprise, vous pouvez utiliser cette AC 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 AC auto-signé sur le portail et l'utiliser pour générer des certificats pour tous les composants GlobalProtect. Toutefois, cette solution est moins sécurisée que les autres options et par conséquent, elle n'est pas recommandée. Si vous choisissez néanmoins cette option, les utilisateurs finaux verront une erreur de certificat 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

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/procédures recommandés
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.

certificate	Usage	Génération de processus/procédures recommandés
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 AC racine utilisé pour générer le certificat du serveur de portail à tous les points de terminaison qui exécutent l'application GlobalProtect. L'exportation de 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.

certificate	Usage	Génération de processus/procédures recommandés
		• 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 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 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

certificate	Usage	Génération de processus/procédures recommandés
		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.

Déployer les certificats de serveur sur les composants GlobalProtect

Le tableau suivant 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 bien connue.

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. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importez)** un nouveau certificat.
2. Utilisez le type de certificat **Local (local)** (par défaut).
3. Saisissez un **Certificate Name (Nom de certificat)**.
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 AC racine pour générer les certificats AC auto-signés pour les composants GlobalProtect.

  Créez le certificat AC 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. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Generate (Générez)** 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 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 SCEP (Single Certificate Enrollment Protocol) pour demander un certificat de serveur auprès de votre AC d'entreprise.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Generate (Générez)** 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 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.

- Utilisez le protocole SCEP pour demander un certificat de serveur à partir de votre AC Enterprise.

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.*

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. 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.
    2. (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.

3. 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/`**).
4. Saisissez une chaîne (jusqu'à 255 caractères de longueur) dans le champ **CA-IDENT Name (Nom AC-IDENT)** pour identifier le serveur SCEP.
5. 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.
6. 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 Identifier (Identificateur de ressource uniforme)** pour identifier la ressource à partir duquel le client obtiendra le certificat.
7. 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.
8. 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)**).
9. (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 ».
10. Activer l'authentification SSL mutuelle entre le serveur SCEP et le portail GlobalProtect.
11. Cliquez sur **OK**, puis **Commit (validez)** la configuration.

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)**. Ce nom ne peut 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.

- Affectez le certificat de serveur que vous avez importé ou généré à un profil de service SSL/TLS.
  1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL/TLS Service Profile (Profil de service SSL/TLS)** et **Add (Ajoutez)** un nouveau profil 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.

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

- Déployez 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 AC auto-signés, vous devez distribuer le certificat AC racine aux clients finaux dans les configurations de client du portail.*

Exportez le certificat à partir du portail :

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**.
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.

Importez le certificat sur la passerelle:

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importez)** le certificat.
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.

Authentification

Le portail GlobalProtect™ et la passerelle doivent authentifier les utilisateurs finaux avant d'autoriser l'accès aux ressources GlobalProtect. Vous devez configurer des mécanismes d'authentification avant de configurer le portail et la passerelle. Les sections suivantes décrivent les mécanismes d'authentification pris en charge et les procédures pour les configurer :

- À propos de l'authentification de l'utilisateur GlobalProtect
- Configurer l'authentification externe
- Configurer l'authentification du certificat client
- Configurer l'authentification à deux facteurs
- Configurer l'authentification pour les points de terminaison strongSwan Ubuntu et CentOS
- Configurer GlobalProtect pour faciliter les notifications d'authentification multifacteur
- Activer la transmission des ASV vers un serveur RADIUS
- Activer le mappage des groupes

À propos de l’authentification de l’utilisateur GlobalProtect

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.

- Méthodes d’authentification GlobalProtect prises en charge
- Comment l’application sait-elle quelles sont les informations d’identification elle doit fournir ?

Méthodes d’authentification GlobalProtect prises en charge

Les rubriques suivantes décrivent les méthodes d’authentification que GlobalProtect prend en charge et fournit des directives d’utilisation pour chaque méthode.

- Authentification locale
- Authentification externe
- Authentification du certificat client
- Authentification à deux facteurs
- Authentification multifacteur pour les applications non basées sur un navigateur
- Ouverture de session unique

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 très petits déploiements.

Authentification externe

Les fonctions d’authentification de l’utilisateur sont réalisées par les services LDAP, Kerberos, TACACS +, SAML ou RADIUS externes (incluant la prise en charge des mécanismes d’authentification basée sur jeton à deux facteurs tels que l’authentification avec mot de passe à usage unique (MPUU)). Pour activer l'authentification externe :

- Créez un profil de serveur avec des paramètres d'accès au service d'authentification externe.
- Créez un profil d'authentification qui se réfère au profil du serveur.
- Spécifiez l'authentification du client dans les configurations portail et passerelle et spécifiez éventuellement l'OS du point de terminaison qui utilisera ces paramètres.

Vous pouvez utiliser des profils d'authentification différents pour chaque composant GlobalProtect. Voir Configuration de l'authentification externe pour les instructions. Consultez accès distant VPN (profil d'authentification) pour une configuration d'exemple.

Si vous configurez le portail ou la passerelle pour l'authentification des utilisateurs au moyen de l'authentification SAML, les utilisateurs qui utilisent l'application GlobalProtect 4.1.8 ou toute version ultérieure n'auront pas la possibilité de Sign Out (Se déconnecter) de l'application si vous désactivez la déconnexion unique (SLO). Les utilisateurs qui utilisent l'application GlobalProtect 4.1.9 ou une version ultérieure auront la possibilité de se Sign Out (Déconnecter) de l'application, peu importe si la SLO est activée ou désactivée.

Si vous configurez le portail ou la passerelle pour l'authentification des utilisateurs au moyen de l'authentification Kerberos, 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 de cette méthode d'authentification.

Si vous n'autorisez pas l'application GlobalProtect à Save User Credentials (Enregistrer les informations d'identification de l'utilisateur) (Network (Réseau) > GlobalProtect > Portals (Portails) > <portal-config> (<configuration du portail>) > Agent > <agent-config> (<configuration de l'agent>) > Authentication (Authentification)), les utilisateurs n'auront pas la possibilité de se Sign Out (Déconnecter) de l'application s'ils s'authentifient avec succès à l'aide de l'authentification LDAP, TACACS+ ou RADIUS.

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.

- 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. 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).

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 mot de passe ponctuel en plus des informations d'identification de connexion 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.

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.

Authentification multifacteur pour les applications non basées sur un navigateur

(Windows et macOS uniquementPour 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.

Ouverture de session unique

(Windows uniquement) Lorsque vous activez la Single Sign-On (ouverture de session unique - SSO), 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. 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.

Si vous activez l'ouverture de session unique, les utilisateurs qui utilisent l'application GlobalProtect 4.1.9 ou toute version ultérieure n'auront pas la possibilité de Sign Out (Se déconnecter) de l'application s'ils s'authentifient avec succès au moyen de la SSO.

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

Par défaut, l'application GlobalProtect tente d'utiliser les mêmes informations d'identification d'ouverture de session pour la passerelle qui est utilisée pour la connexion au portail. Dans le cas le plus simple, où la passerelle et le portail utilisent les mêmes profils d'authentification et/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.

Il existe deux options pour modifier le comportement d'authentification par défaut de l'application afin que l'authentification soit à la fois plus forte et plus rapide :

- Authentification par cookie sur le portail ou la passerelle
- Transfert d'informations d'identification vers certaines ou toutes les passerelles

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, après cinq jours, l'utilisateur a tenté de se connecter au portail, le cookie d'authentification serait toujours valide. Cependant, si après cinq jours, l'utilisateur a tenté de se connecter à la passerelle, la passerelle évalue la durée de vie des cookies et détermine qu'elle 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/ou 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.

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

Lorsque vous configurez GlobalProtect pour utiliser des certificats clients pour l'authentification sur des points de terminaison MacOS ou Windows, GlobalProtect doit présenter un certificat client valide pour s'authentifier auprès du portail et/ou 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, voir Sélection de certificat par 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 point de terminaison. 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 ces paramètres et d'autres paramètres que vous pouvez configurer pour personnaliser votre application, voir la section Personnaliser l'agent GlobalProtect.

Configurer l’authentification externe

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.

Pour plus d'informations, consultez Méthodes d'authentification GlobalProtect supportées.

Les options de configuration de l’authentification externe incluent :

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

Configurer l’authentification LDAP

Les organisations utilisent souvent LDAP comme service d’authentification et référentiel central pour les informations d’utilisateur. Il peut également être utilisé pour stocker les informations de rôle pour les utilisateurs de l’application.

STEP 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. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils serveur)** > **LDAP**, puis **Add (Ajoutez)** un profil 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 de certificats)** > **Certificates (Certificats)** > **Device 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.

STEP 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 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 pré-connexion, les utilisateurs ne peuvent accéder à GlobalProtection lorsque leur mot de passe est expiré.

7. Spécifiez le **User Domain (Domaine d'utilisateur)** et le **Username Modifier (Modificateur d'utilisateur)**. Le point de terminaison combine les valeurs **User Domain (Domaine utilisateur)** et **Username Modifier (Modificateur du nom d'utilisateur)** 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 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**.

STEP 3 | Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**.

Configurer l'authentification SAML

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.

STEP 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 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. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils de serveur)** > **SAML Identity Provider (Fournisseur d'identité SAML)**.
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. (Recommandé) 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.

STEP 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 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. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentication)**, puis **Add (Ajoutez)** 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. Reportez-vous à Authentification SAML 2.0 pour plus de détails.
   - 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.

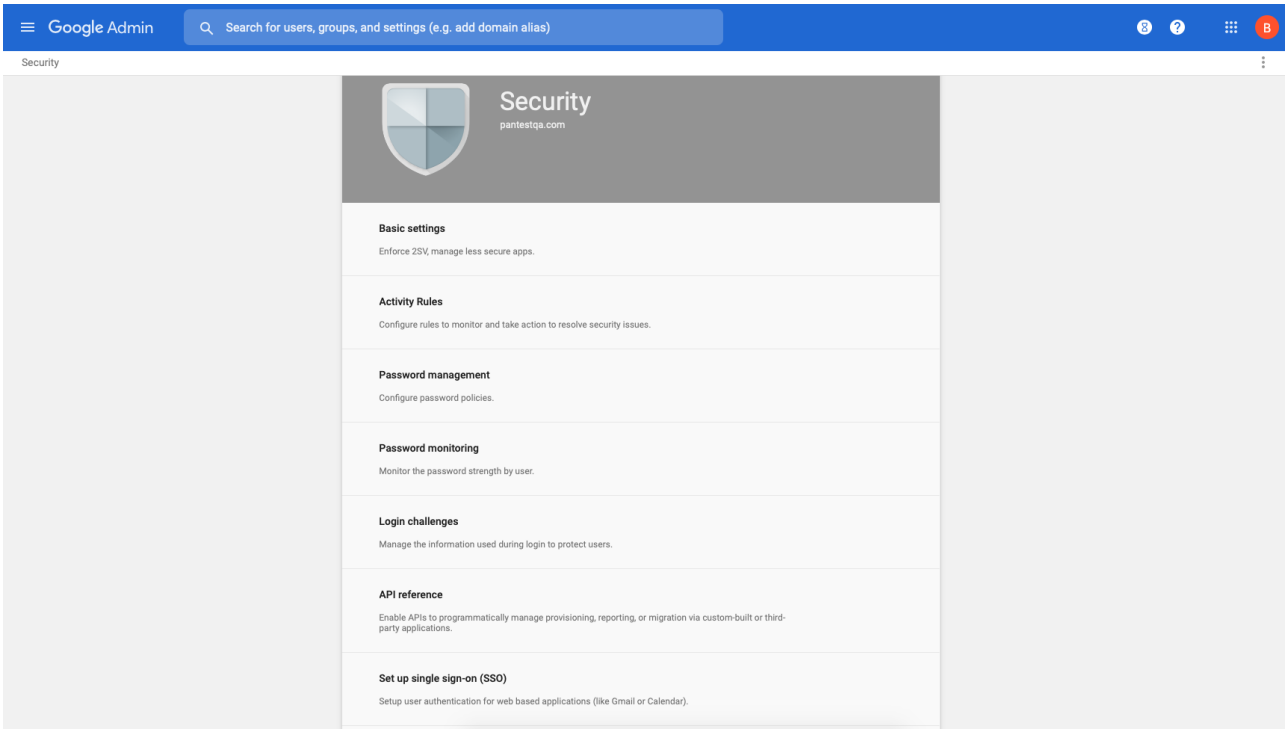
   Assurez-vous que le nom d'utilisateur qui figure dans la **Allow List (Liste d'autorisations)** correspond au nom d'utilisateur renvoyé par le serveur de l'IdP SAML.
8. Cliquez sur **OK**.

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

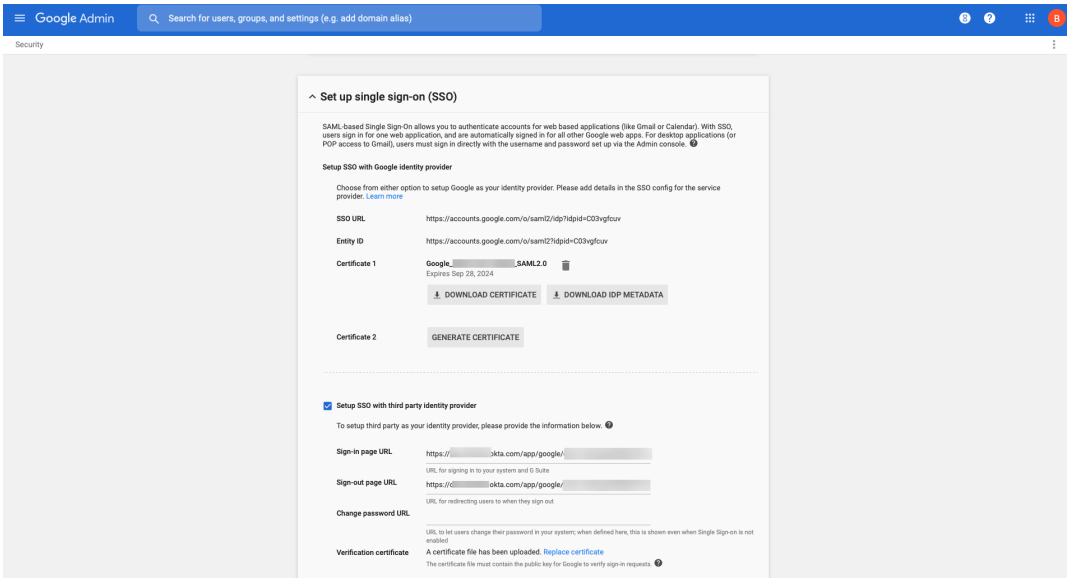
STEP 4 | (Chromebook uniquement) Activez le SSO SAML pour les Chromebook.

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

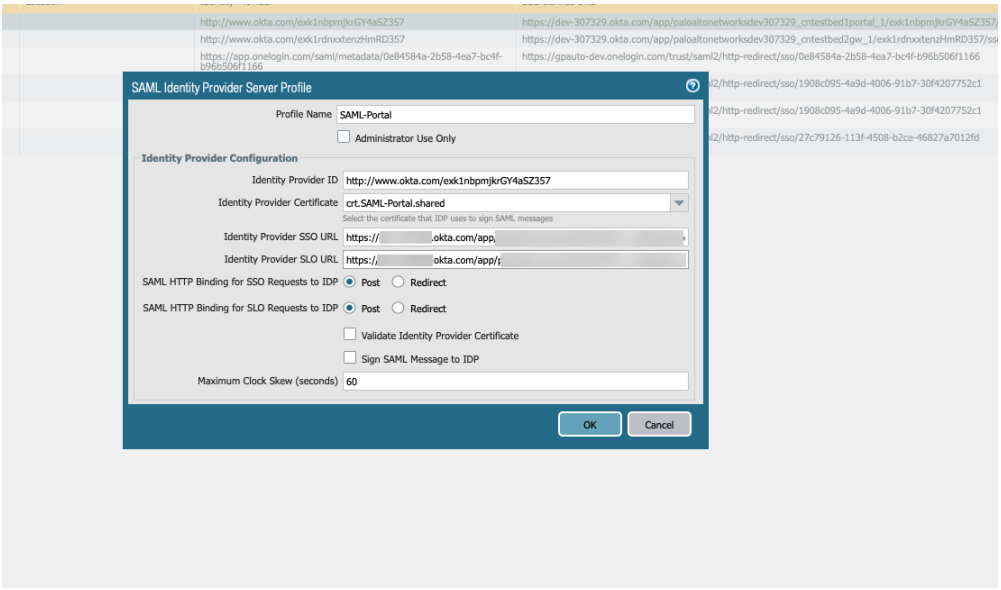
1. Connectez-vous à la console Google Admin, puis sélectionnez **Sécurité**.



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 **Configurer l'ouverture de session unique SSO auprès d'un fournisseur d'identité tiers**, puis spécifiez la **Page d'URL de connexion** et la **page d'URL de déconnexion** et chargez un **certificat de vérification** valide.



4. Configurez le fournisseur d’identité SAML dans GlobalProtect.
    1. Dans la console GlobalProtect, sélectionnez **Périphérique** > **Profils de serveur** > **Fournisseur d’identité SAML**.
    2. Faites correspondre les valeurs que vous avez saisies pour l’IdP dans la console Google Admin.



Configurer l’authentification Kerberos

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.

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.

STEP 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.

1. Sélectionnez **Device (Périphérique)** > **Server Profiles (Profils serveur)** > **Kerberos (Kerberos)**, puis **Add (Ajoutez)** 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.

STEP 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 mot de passe expiré sans l'intervention d'un administrateur, songez à utiliser un VPN d'accès distant avec pré-connexion.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis **Add (Ajoutez)** un nouveau profil.
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 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.
   - 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.
   - **Import (Importez)** un fichier **Kerberos Keytab (Keytab Kerberos)**. Lorsque vous y êtes invité, **Browse (Parcourez)** pour trouver le fichier keytab, puis cliquez sur **OK**. 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.
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 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.
7. Cliquez sur **OK**.

STEP 3 | Commit (Validez) la configuration.

Cliquez sur **Commit (Valider)**.

Configurer l'authentification RADIUS ou TACACS+

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.

STEP 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. Sélectionnez **Device (Périphérique)** > **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 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.

STEP 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. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis **Add (Ajoutez)** un nouveau profil.
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 (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**.

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

Configurer l'authentification du certificat client

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.

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

Déployer des certificats clients partagés pour l'authentification

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.

STEP 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.

STEP 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

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).

STEP 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 **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.

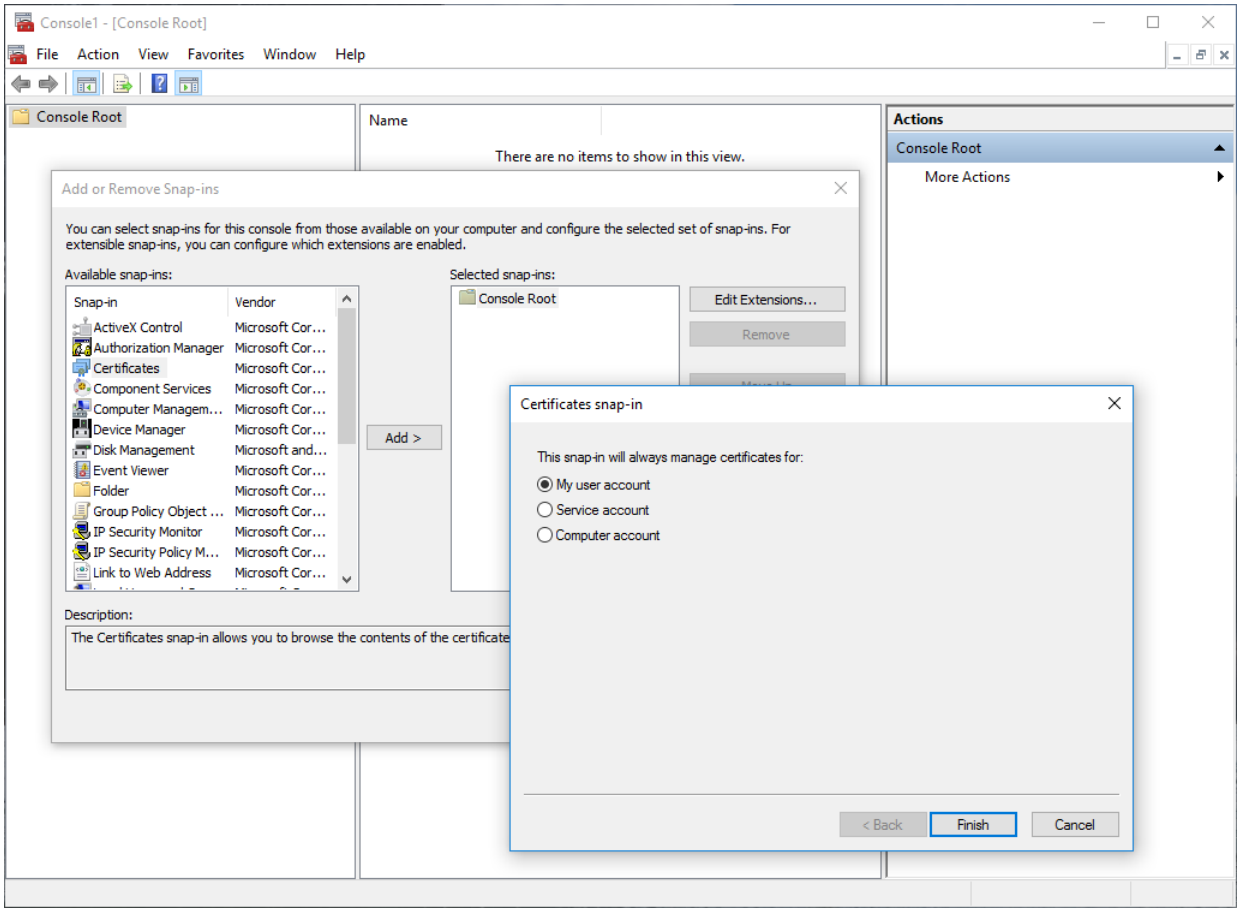
STEP 2 | Installez les certificats dans le magasin de certificats personnel sur les points d'extrémité.

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 point de terminaison avant le premier portail ou la connexion de passerelle. Installez les certificats machines dans le magasin de certificats de l'ordinateur local sur Windows et dans System Keychain sur MacOS. Installez les certificats utilisateurs dans le magasin de certificats de l'utilisateur actuel sur Windows et dans le trousseau sur MacOS.

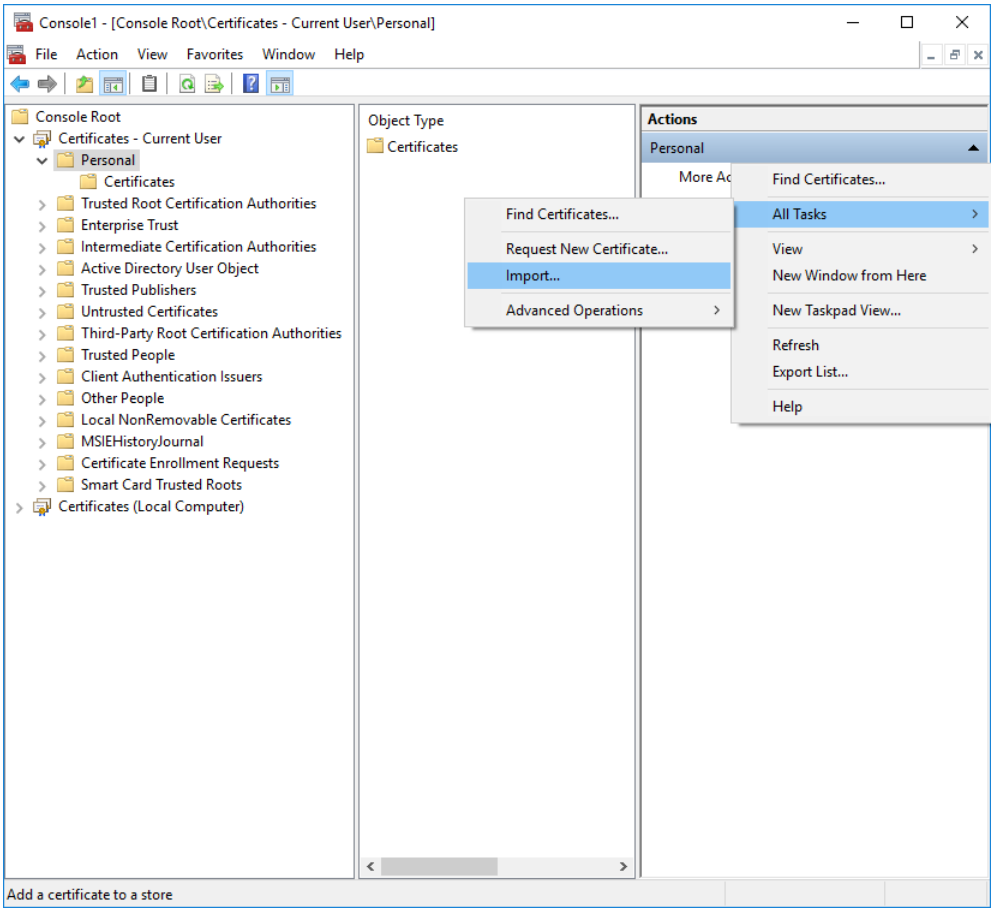
Par exemple, pour installer un certificat sur un système Windows utilisant la Console de gestion Microsoft :

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



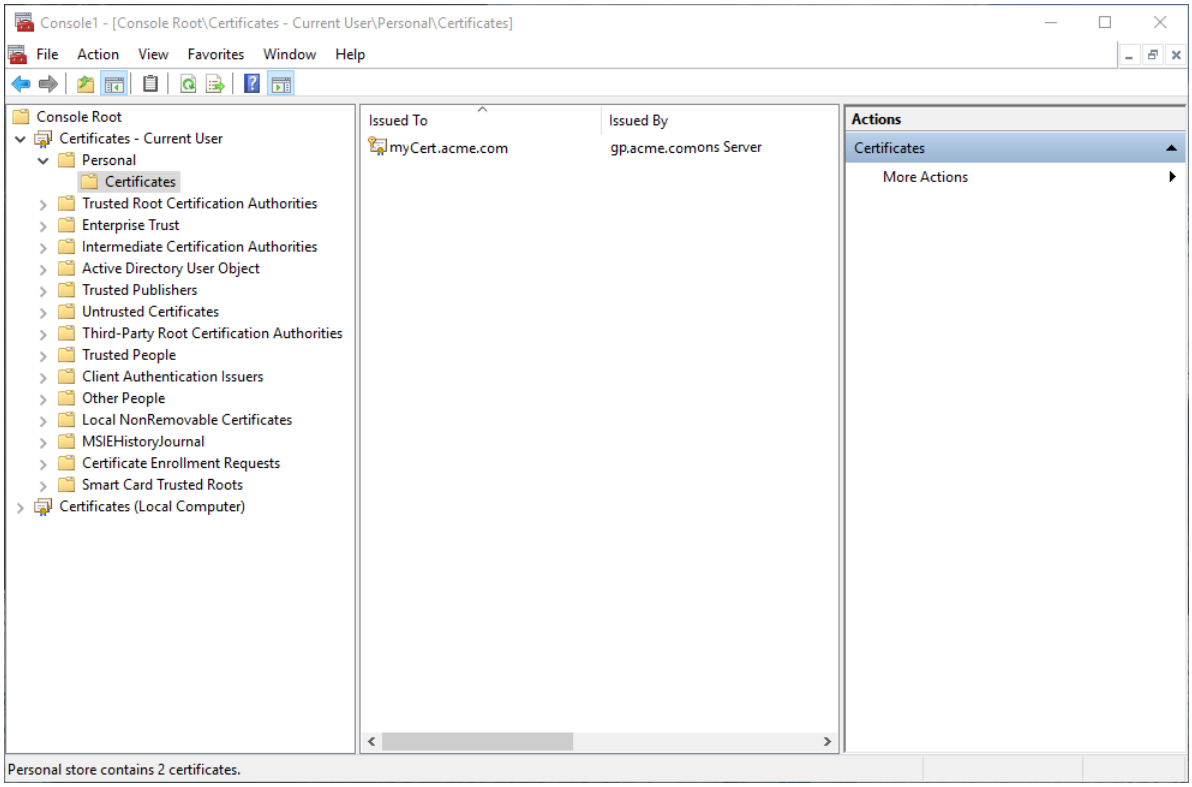
4. À partir de la **Console Root (Racine de la console)**, développez les **Certificates (Certificats)**, puis sélectionnez **Personal (Personnel)**.
5. Dans la colonne **Actions**, sélectionnez **Personal (Personnel)** > **More Actions (Plus d'actions)** > **All Tasks (Toutes les tâches)** > **Import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

STEP 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)** :



STEP 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. 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**.

STEP 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**.

STEP 6 | Enregistrer la configuration.

Commit (Validez) les modifications.

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

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.

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.

STEP 1 | Créez un profil SCEP.

1. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SCEP (SCEP)**, puis **Add (Ajouter)** un nouveau profil SCEP.
2. Saisissez un **Name (Nom)** pour identifier le profil.
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.

STEP 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.

STEP 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), 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.

STEP 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.

STEP 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.

STEP 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: // <nom d'hôte ou 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)**.

STEP 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)**.

STEP 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)**.

STEP 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.

STEP 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.

Configurer l'authentification à deux facteurs

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.

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

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.

STEP 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.

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

1. Sélectionnez **Périphérique** > **Profils du serveur** et un type de profil (**LDAP**, **Kerberos**, **RADIUS** ou **TACACS+**).
2. **Add (Ajoutez)** un nouveau profil de serveur.
3. Saisissez un **Profile Name (Nom de profil)**, par exemple **`gp-user-auth`**.
4. (LDAP uniquement) Sélectionnez le **Type** de serveur LDAP (**active-directory**, **e-directory**, **sun** ou **other (autre)**).
5. Cliquez sur **Add (Ajouter)** dans la zone **Servers (Serveurs)** ou **Servers List (Liste de serveurs)** (selon le type de profil de serveur), puis entrez les informations suivantes pour les connexions au service d'authentification :
   - **Name (Nom)** du serveur
   - Adresse IP ou nom de domaine complet du **Server (Serveur)**.
   - **Port**
6. (RADIUS, TACACS+ et LDAP uniquement) Définissez les paramètres suivants pour permettre au pare-feu de s'authentifier auprès du service d'authentification :
   - RADIUS et TACACS+ : saisissez le **Secret** partagé lors de l'ajout de l'entrée de serveur.
   - LDAP : saisissez le **Bind DN (Nom distinctif Bind)** et le **Password (Mot de passe)**.

7. (LDAP uniquement) 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 que le point de terminaison utilise dépend du **Port** de serveur de la **Server list (liste des serveurs)** :
   - 389 (par défaut) : TLS (en particulier, le point de terminaison utilise l'opération StartTLS pour mettre à niveau la connexion initiale en clair à TLS).
   - 636 : SSL.
   - Tout autre port : le point de terminaison tente tout d'abord d'utiliser TLS. Si le serveur d'annuaire ne prend pas en charge TLS, le point de terminaison utilise SSL.
8. (LDAP uniquement) 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 que la vérification réussisse, l'une des conditions suivantes doit être vraie :
   - Le certificat se trouve dans la liste des certificats de périphériques : **Device (Périphérique)** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique).** Importez le certificat dans le point de terminaison si nécessaire.
   - Le signataire du certificat figure dans la liste des autorités de certification de confiance : **Périphérique** > **Gestion de Certificats** > **Certificats** > **Autorités de certificats de confiance par défaut**.
9. Cliquez sur **OK** pour enregistrer le profil de serveur.

STEP 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.

1. Sélectionnez **Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**, puis **Add (Ajoutez)** un nouveau profil.
2. Saisissez un **Name (Nom)** pour le profil.
3. Sélectionnez le **Type Authentication** (Type d'authentification).
4. Sélectionnez le **Server Profile (Profil de serveur)** que vous avez créé à l'étape 1.
5. (LDAP uniquement) Saisissez **sAMAccountName** dans le champ **Login Attribute (Attribut d'ouverture)**.
6. Cliquez sur **OK** pour enregistrer le profil d'authentification.

STEP 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, 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. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**, puis **Add (Ajouter)** un nouveau profil de 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) 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**.

STEP 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 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.

STEP 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.

STEP 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 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.

STEP 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.

STEP 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.

STEP 4 | Affectez le profil d'authentification à la passerelle 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.

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

STEP 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.

STEP 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.

STEP 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 des informations d'identification régulières ou un MPUU. Pour plus d'informations, voir Authentification par cookie sur le portail ou la passerelle.

Dans le cas où vous devez bloquer immédiatement l'accès à un point de terminaison dont le cookie n'a pas encore expiré (par exemple, si le point de terminaison est perdu ou volé), vous pouvez bloquer l'accès du point de terminaison en ajoutant le périphérique à une liste de blocage.

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> (configuration de l'agent)* > **Authentication (Authentification)**.
   - **Configuration de la passerelle GlobalProtect** : Dans la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Client Settings (Paramètres du client)** > *<client-setting>(paramètre du client)* > **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.
- **Accept cookie for authentication override (Accepter un cookie pour substituer l'authentification)** : indique au portail ou à la passerelle qu'il ou elle doit 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> (configuration du portail) > Agent > <agent-config> (configuration de l'agent). > 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.
- **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.

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

STEP 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 :

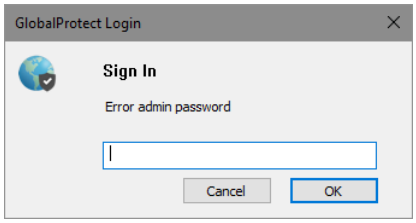


Figure 1: Fenêtre contextuelle relative au mot de passe à usage unique

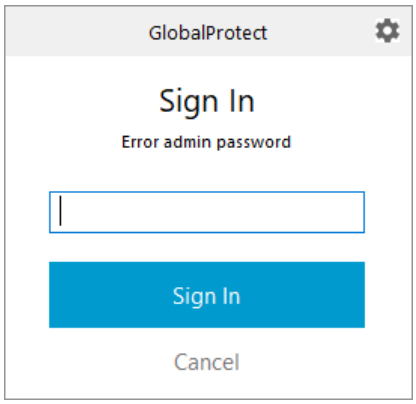


Figure 2: Invite relative au mot de passe à usage unique sur le panneau d'état de GlobalProtect

Activer l'authentification à deux facteurs basée sur les cartes à puce intelligentes

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.

STEP 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.

STEP 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. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importez)** 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.

STEP 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. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificats)**.
2. Sélectionnez un profil de certificat existant ou **Add (Ajoutez)**-en un nouveau.
3. Donnez un **Name (Nom)** au profil de certificat.
4. 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.
5. 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**.
6. Cliquez sur **OK** pour enregistrer le profil de certificat.

STEP 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 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.

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

STEP 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.

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

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 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.

Cette fonctionnalité et prise en charge sur les périphériques Windows à partir de la version 5.1 de l'application GlobalProtect™.

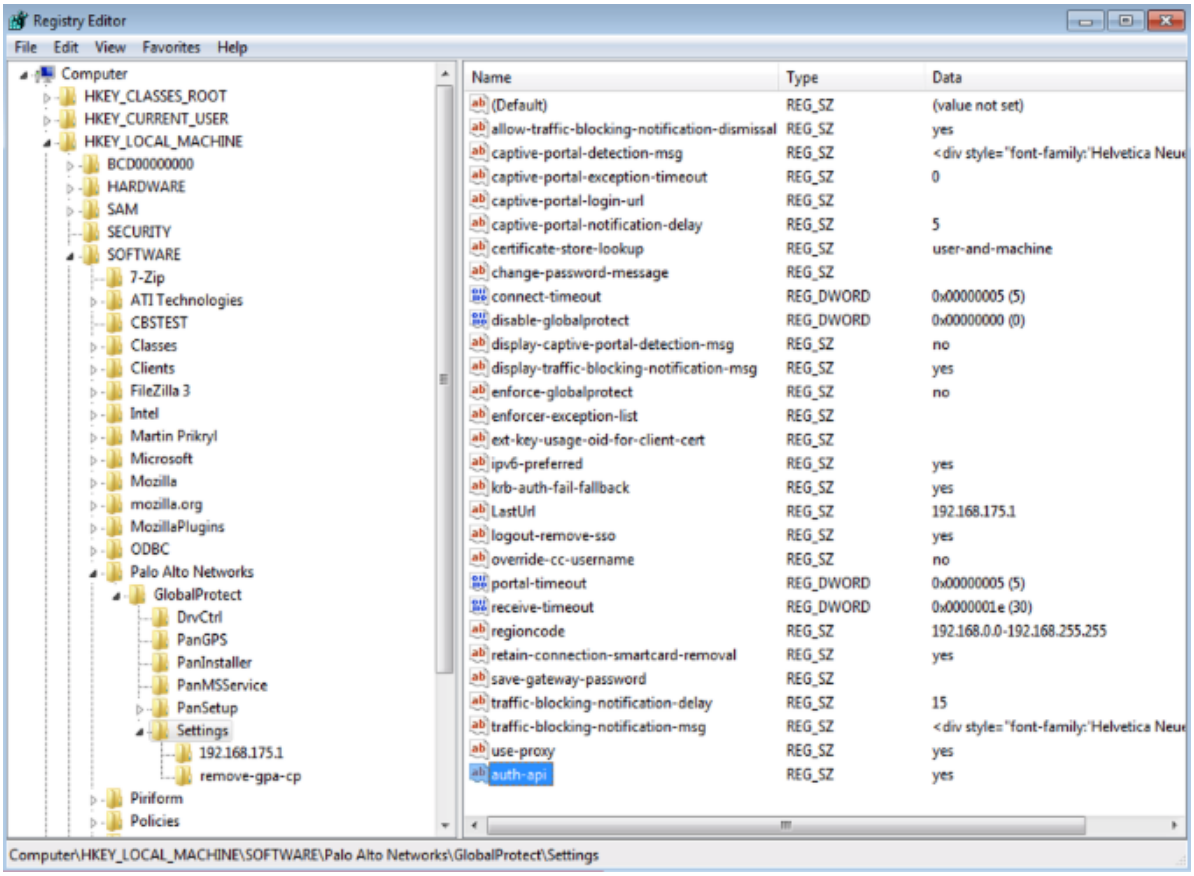
STEP 1 | Modifiez les clés de registre sur les périphériques Windows client pour activer l'authentification par jeton logiciel en toute fluidité.

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

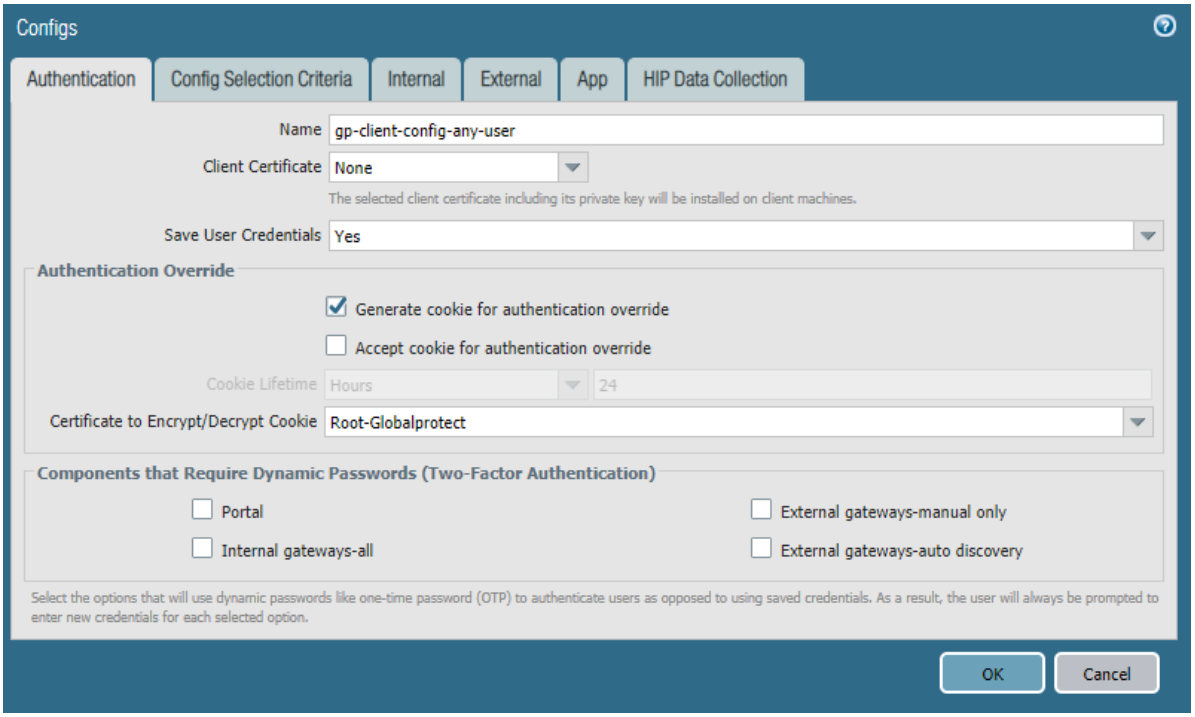


STEP 2 | Configurez le portail et la passerelle à l'aide de l'authentification RSA.

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

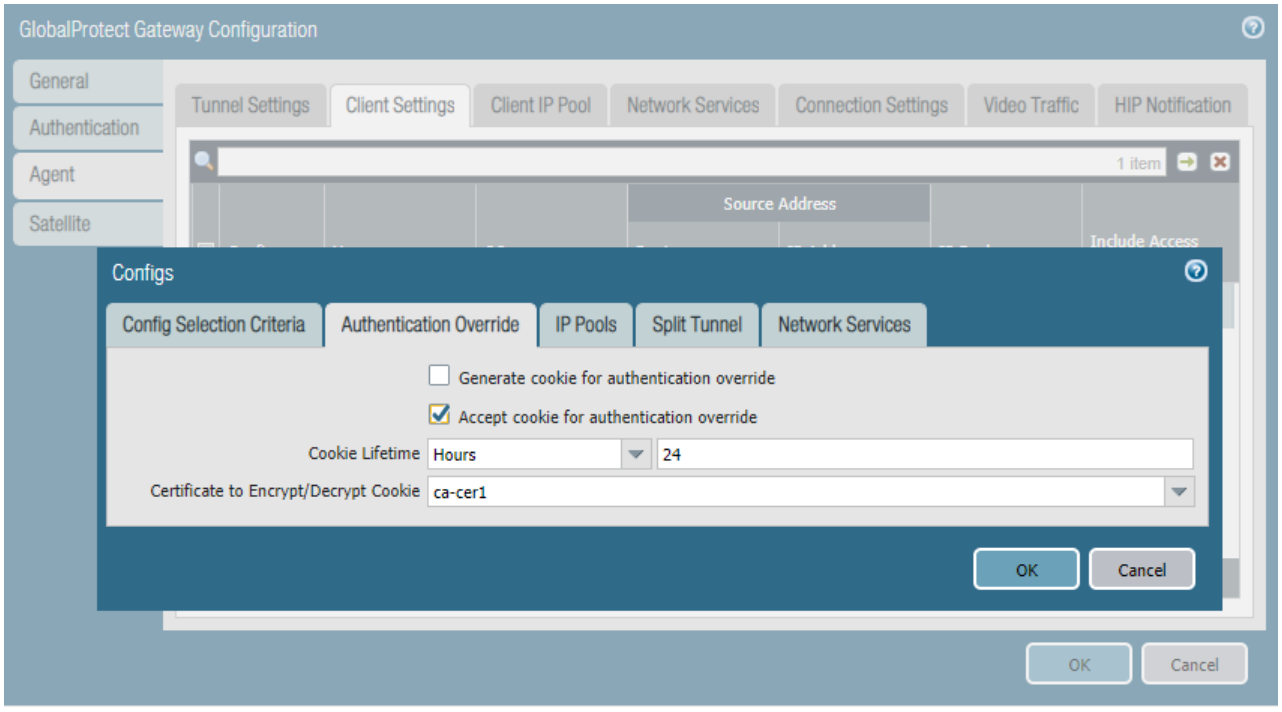
En permettant à GlobalProtect de réécrire une authentification existante, GlobalProtect peut remplacer un code secret existant par un code secret nouvellement créé.

1. Sélectionnez **Réseau** > **GlobalProtect** > **Portails** > *configuration du portail*, puis sélectionnez l'onglet **Agent**.
2. **Ajoutez** une configuration d'agent ou sélectionnez-en une qui existe déjà.
3. Sélectionnez **Générer le cookie pour la réécriture de l'authentification**.



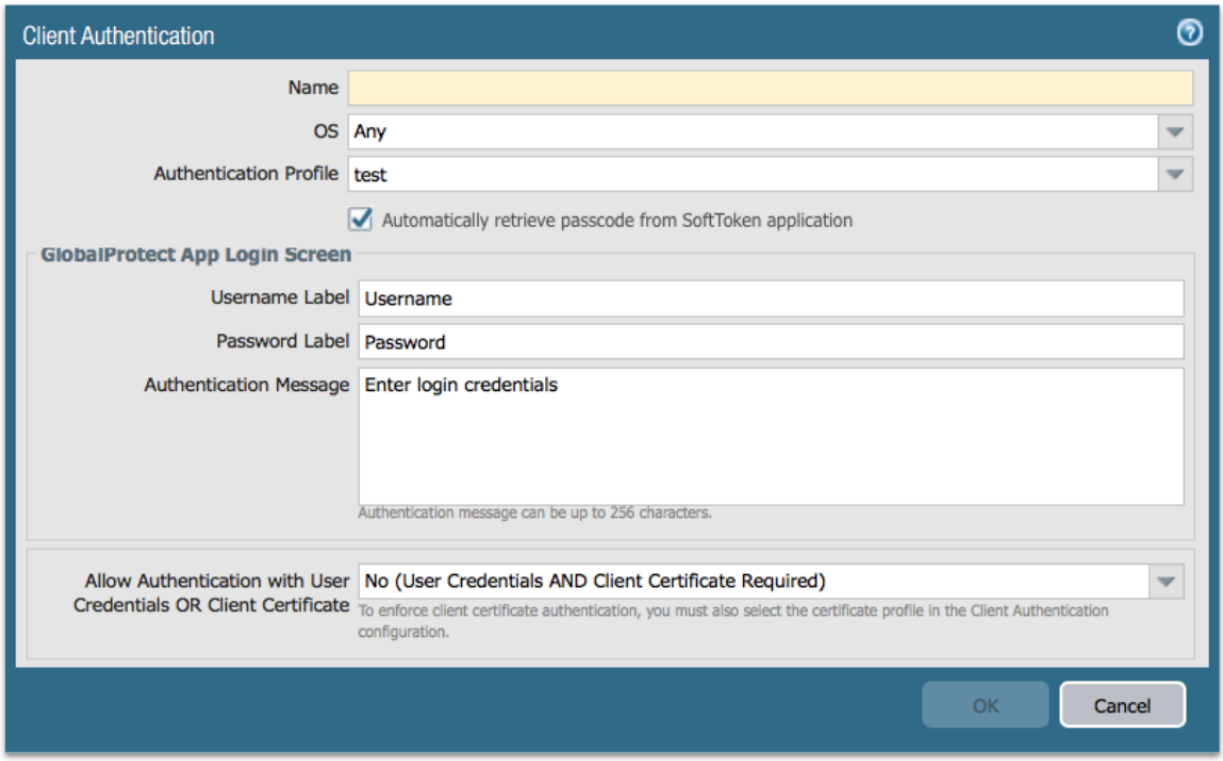
STEP 4 | Activez l'option Accepter le cookie pour la substitution d'authentification sur la passerelle GlobalProtect.

1. Sélectionnez **Réseau** > **GlobalProtect** > **Passerelles** > *passerelle*, puis 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**.



STEP 5 | Sélectionnez **Réseau** > **GlobalProtect** > **Portails** > *configuration du portail*, puis sélectionnez l'onglet **Agent**.

STEP 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**.



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

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

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 à l'aide d'un profil de certificat
- Activer l'authentification à l'aide d'un profil d'authentification
- Activer l'authentification à l'aide de l'authentification à deux facteurs

Activer l'authentification à l'aide d'un profil de certificat

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

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

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)** que vous souhaitez utiliser pour l'authentification.
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 les paramètres.

STEP 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
```

STEP 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>"
```

STEP 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 <nom>` pour nommer la configuration de tunnel.

- Ubuntu :

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

- CentOS :

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

STEP 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)**.

Activer l'authentification à l'aide d'un profil d'authentification

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.

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

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.

STEP 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
```

STEP 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>"
```

STEP 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>
```

STEP 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)**.

Activer l'authentification à l'aide de l'authentification à deux facteurs

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.

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

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.

STEP 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
```

STEP 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>"
```

STEP 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>
```

STEP 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>]
     ```

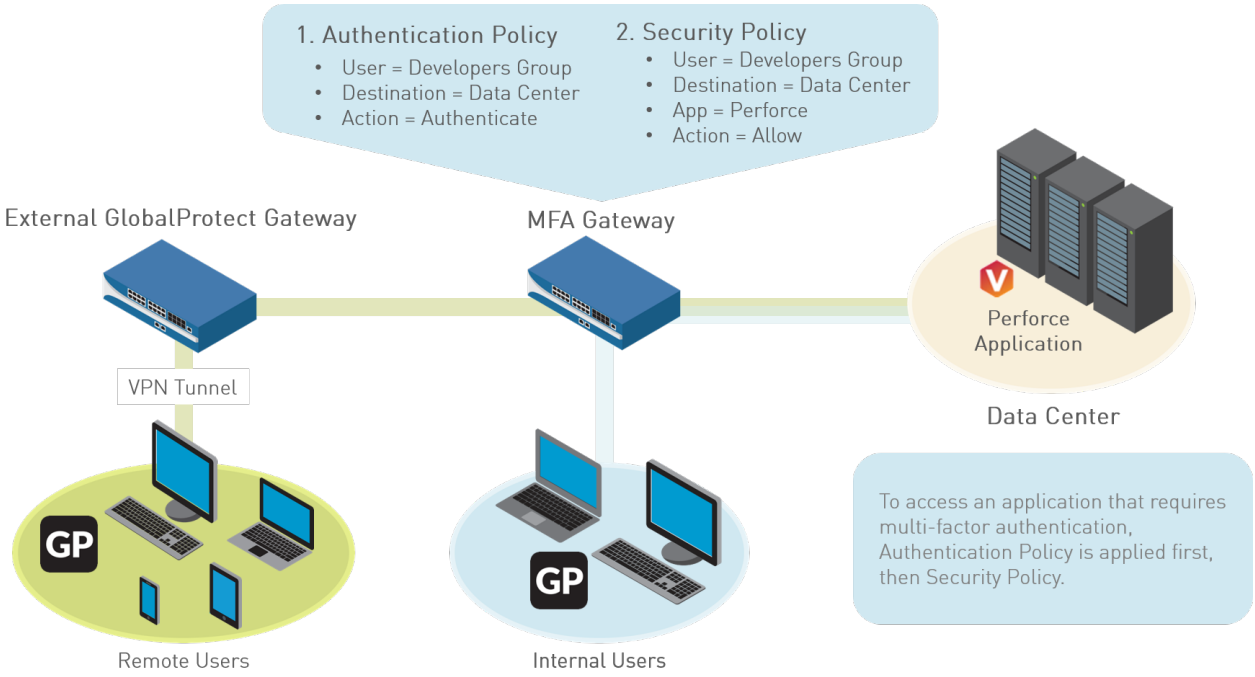
   - CentOS :

     ```
     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)**.

Configurer GlobalProtect pour faciliter les notifications d'authentification multifacteur

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 (MFA). 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.



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. Pour plus d'informations, reportez-vous à la section Configuration de l'authentification multifacteur.

Pour configurer GlobalProtect afin d'afficher les notifications MFA pour les applications non basées sur un navigateur, utilisez le flux de travail suivant :

STEP 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. Pour plus d'informations, reportez-vous à Configurer l'authentification multifacteur.

- 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.

STEP 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)**.

STEP 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**.

STEP 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)**.

STEP 5 | (Passerelles externes uniquement) **Activer l'identification de l'utilisateur** sur la zone associée à l'interface de tunnel (**Réseau** > **Zones** > **<tunnel-zone**).

STEP 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, 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 de la page Authentication Portal (Portail d'authentification) que vous avez spécifiée Configurer 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.

Activer la transmission des ASV vers un serveur RADIUS

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.

STEP 1 | Connectez-vous à l'ILC du pare-feu.

STEP 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****.*

Activer le mappage des groupes

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 :

STEP 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.)
   - 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**.

STEP 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 (Ajoutez)** 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.

STEP 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)**.

STEP 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.

STEP 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.

STEP 6 | Validez vos modifications.

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

Passerelles GlobalProtect

- Concepts des passerelles GlobalProtect
- Tâches préalables à la configuration de la passerelle GlobalProtect
- Configurer une passerelle GlobalProtect
- Séparation du trafic tunnel sur les passerelles GlobalProtect

Aperçu des passerelles GlobalProtect

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. Pour plus d'informations sur l'activation des archivages HIP, reportez-vous à la section Informations de l'hôte.
- 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 point de terminaison et l'interface de tunnel sur le pare-feu qui héberge la passerelle.

Vous pouvez également configurer les passerelles GlobalProtect sur des pare-feu VM-Series déployés dans le cloud AWS. En déployant le pare-feu VM-Series dans le cloud AWS, vous pouvez déployer rapidement et facilement des passerelles GlobalProtect dans n'importe quelle région sans les coûts ou la logistique informatique généralement liés à la configuration de cette infrastructure. Pour plus d'informations, reportez-vous à la section Cas d'utilisation : Pare-feu VM-Series en tant que passerelles GlobalProtect dans AWS*.*

Concepts des passerelles GlobalProtect

Ces sections fournissent des informations sur la priorité de connexion de passerelle dans une configuration de passerelle multiple et la prise en charge MIB pour les passerelles GlobalProtect.

- Type de passerelles
- Priorité de passerelle dans une configuration de passerelle multiple
- GlobalProtect MIB support

Type de passerelles

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

Configurez une passerelle GlobalProtect sur n'importe quel pare-feu de dernière génération Palo Alto Networks. 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.

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.
- **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.

Priorité de passerelle dans une configuration de passerelle multiple

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
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.

GlobalProtect MIB support

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 points de terminaison) définis dans les MIB (pour plus de détails, voir Utilisation d'un gestionnaire SNMP pour explorer les MIB et les objets dans le Guide de l'administrateur PAN-OS 8.1).

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.

Tâches préalables à la configuration de la passerelle GlobalProtect

Avant de configurer la passerelle GlobalProtect, vous devez avoir effectué les tâches suivantes :

- Création 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. 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. Voir Authentification.

Configurer une passerelle GlobalProtect

Après avoir effectué les tâches préalables, configurez la passerelle GlobalProtect :

STEP 1 | Ajoutez une passerelle.

1. **Ajoutez** une nouvelle passerelle (**Réseau** > **GlobalProtect** > **Passerelles**).
2. **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.
3. (Facultatif) Sélectionnez le **Location (Emplacement)** du système virtuel auquel la passerelle appartient.

STEP 2 | 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.

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-feu d'une manière qui empêchera les attaques réussies.*

1. Sélectionnez l'**Interface** que les points de terminaison utiliseront pour la communication avec la passerelle.
2. Spécifiez le **IP Address Type (Type d'adresse IP)** et la **IP Address (Adresse IP)** pour le service Web 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.

STEP 3 | 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 (Authentification)** de la passerelle suivants (**Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** > *<gateway-config> (<configuration de la passerelle>)* > **Authentication (Authentification)**) :

- 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.

  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.
  - 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.
- 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 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.*

STEP 4 | 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.

Pour obtenir de plus amples informations sur les algorithmes cryptographiques, reportez-vous à la section Fonctions cryptographiques de l'application GlobalProtect.

1. Dans la boîte de dialogue GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect), sélectionnez **Agent** > **Tunnel Settings (Paramètres de Tunnel)** .
2. Activez le **Tunnel Mode (Mode tunnel)** pour activer la segmentation des tunnels.
3. Sélectionnez la **Tunnel Interface (Interface de tunnel)** que vous avez définie lors de la création de l'interface réseau de la passerelle.

4. (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.
5. **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 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.
6. (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)**.

   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.

STEP 5 | (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.

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 **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.
   - 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.

STEP 6 | (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.

Dans le cas où vous devez bloquer immédiatement l'accès à un périphérique dont le cookie n'a pas expiré (par exemple, si l'appareil est perdu ou volé), vous pouvez immédiatement bloquer l'accès du point de terminaison *en ajoutant le périphérique à une liste de blocage.*

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 au point de terminaison et d'émettre les cookies d'authentification au point de terminaison.
   - **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> (configuration du portail) > Agent > <agent-config> (configuration de l'agent). > 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.
   - **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).

STEP 7 | (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.

Vous devez configurer les pools d'adresses IP à un seul niveau : soit au niveau client (Network (Réseau) > GlobalProtect > Gateways (Passerelles) > <gateway-config> (configuration de la passerelle) > GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect) > Agent > Client Settings (Paramètres client) > <client-setting> (paramètre client) > Configs (Configurations) > IP Pools (Pools d'adresses IP)) ou au niveau de la passerelle (Network (Réseau) > GlobalProtect > Gateways (Passerelles) > <gateway-config> (configuration de la passerelle) > GlobalProtect Gateway Configuration (Configuration de la passerelle GlobalProtect) > Agent > Client IP Pool (Pools d'adresses IP du client)).

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)**. Une fois le tunnel établi, une interface est créée sur l'ordinateur de l'utilisateur distant avec une adresse du sous-réseau ou de la plage d'adresses IP qui correspond à l'attribut adresse IP tramée 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.

STEP 8 | (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.

STEP 9 | (Mode tunnel uniquement) (Facultatif) Configurez les paramètres de séparation des tunnels selon l'itinéraire d'accès.

STEP 10 | (Mode tunnel uniquement) (Facultatif) Configurez les paramètres de séparation des tunnels selon le domaine de destination.

STEP 11 | (Mode tunnel uniquement) (Facultatif) Configurez les paramètres de séparation des tunnels selon l'application.

STEP 12 | (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> (<configuration de la passerelle>) > Agent > Client Settings (Paramètres du client) > <client-settings-config> (<configuration des paramètres du client>) > Network Services (Services réseaux)), la passerelle envoie la configuration du serveur DNS et du suffixe DNS au point de terminaison. 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 point de terminaison, s'ils sont configurés (Réseaux > GlobalProtect > Passerelles > <gateway-config> > Agent > 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.

STEP 13 | (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)**.
- Pour faire descendre une configuration de passerelle dans la liste de configurations, sélectionnez la configuration, puis cliquez sur **Move Down (Descendre)**.

STEP 14 | (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> (configuration de la passerelle) > Agent > Client IP Pool (Pool d'adresses IP du client)) ou au niveau du client (Network (Réseau) > GlobalProtect > Gateways

(Passerelles) > <gateway-config> (configuration de la passerelle) > Agent > Client Settings (Paramètres du client) > <client-setting> (paramètre du client) > IP Pools (Pools d'adresses IP)).

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 IP Pool (Pools 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.

STEP 15 | (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.

STEP 16 | (Facultatif) Modifiez les paramètres de temporisation par défaut pour les points de terminaison.

Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Connection Settings (Paramètres de connexion)**, puis configurez ce qui suit dans la section Timeout Configuration (Configuration du délai avant expiration) :

- 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.
- Modifiez la période de **Inactivity Logout (Déconnexion en cas d'inactivité)** pour spécifier la durée de temps après laquelle une session inactive est automatiquement déconnectée (la valeur par défaut est de trois heures). Les utilisateurs sont déconnectés de GlobalProtect si la passerelle ne reçoit pas une vérification HIP du point de terminaison au cours de la période de temps configurée.

- Modifiez le paramètre de **Disconnect on Idle (Déconnexion en cas d'inactivité)** pour préciser le nombre de minutes qui peuvent s'écouler avant que les utilisateurs inactifs soient déconnectés de GlobalProtect (la valeur par défaut est de 180 minutes). Les utilisateurs sont déconnectés de GlobalProtect si l'application GlobalProtect n'a pas acheminé de trafic via le tunnel VPN au cours de la période de temps configurée. Ce paramètre s'applique uniquement aux applications GlobalProtect qui utilisent la méthode de connexion à la demande.

STEP 17 | (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. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **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).

STEP 18 | (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. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **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`).

STEP 19 | (Mode tunnel uniquement) Exclure le trafic de diffusion vidéo HTTP/HTTPS du tunnel VPN.

STEP 20 | (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'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. Dans la boîte de dialogue Configuration de la passerelle 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.

STEP 21 | Enregistrez la configuration de la passerelle.

1. Cliquez sur **OK** pour enregistrer les paramètres.
2. **Commit (Validez)** les modifications.

STEP 22 | (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 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> set deviceconfig setting 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>'
```

Séparation du trafic tunnel sur les passerelles GlobalProtect

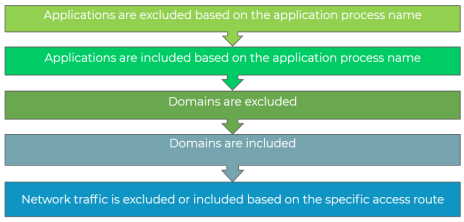
Vous pouvez configurer la séparation du trafic tunnel en fonction de l'itinéraire d'accès, du domaine de destination, de l'application ou de l'application de diffusion vidéo en continu HTTP/HTTPS.

Un abonnement à GlobalProtect vous permet d'appliquer les règles de séparation du trafic tunnel aux terminaux Windows et macOS.

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 applicables au tunnel séparé sont appliquées aux terminaux Windows et macOS dans l'ordre suivant :



Reportez-vous aux sections suivantes qui portent sur la configuration du trafic tunnel séparé sur les passerelles :

- Configuration d'un tunnel séparé en fonction de l'itinéraire d'accès
- Configuration d'un tunnel séparé en fonction du domaine et de l'application
- Exclusion du trafic vidéo à partir du tunnel VPN GlobalProtect

Configuration d'un tunnel séparé en fonction de l'itinéraire d'accès

Si vous n'incluez ou n'excluez pas d'itinéraires, chaque demande est acheminée à travers le tunnel VPN (sans tunnel séparé). Vous pouvez inclure ou exclure certain trafic du sous-réseau IP de destination de l'envoi par le tunnel VPN. Les itinéraires que vous transmettez par le tunnel VPN peuvent être définis comme des itinéraires que vous incluez dans le tunnel ou comme des itinéraires que vous excluez du tunnel, ou une combinaison des 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.

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. En désactivant la segmentation de tunnel, 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. Vous pouvez tenir compte du comportement du trafic IPv4 et IPv6 selon que vous avez activé ou désactivé l'accès direct aux réseaux locaux.

Table 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.	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.
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.	Le trafic est suspendu.	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.

Table 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 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.
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.

STEP 1 | Avant de commencer :

1. Configurez une passerelle GlobalProtect.
2. Sélectionnez **Réseau** > **GlobalProtect** > **Passerelles** > *<gateway-config>* pour modifier une passerelle existante ou en ajouter une nouvelle.

STEP 2 | Activez un tunnel séparé.

1. Dans la boîte de dialogue **Configuration de la passerelle GlobalProtect**, sélectionnez **Agent** > **Paramètres de Tunnel** pour activer le **Mode Tunnel**.
2. Configurez les paramètres de tunnel pour l'application GlobalProtect.

STEP 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.

1. Dans la boîte de dialogue **Configuration de la passerelle GlobalProtect**, sélectionnez **Agent** > **Paramètres du client** > *<client-setting-config>* pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.
2. Sélectionnez **Split Tunnel (Segmentation de tunnel)** > **Access Route (Accéder à l'itinéraire)**, puis activez l'option **No direct access to local network** (Aucun accès direct au réseau local).

   Si vous activez cette option, le tunnel séparé 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.

STEP 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 **Configuration de la passerelle GlobalProtect**, sélectionnez **Agent** > **Paramètres du client** > *<client-setting-config>* pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.
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.

STEP 5 | Enregistrez la configuration de la passerelle.

1. Cliquez sur **OK** pour enregistrer les paramètres.
2. **Commit (Validez)** les modifications.

Configuration d'un tunnel séparé en fonction du domaine et de l'application

Lorsque vous configurez un tunnel séparé pour qu'il inclut tout le trafic (IPv4 et IPv6) en fonction du domaine et du port de destination (facultatif) ou de l'application, tout le trafic qui se rend à ce domaine ou à cette application est acheminé par le tunnel VPN à des fins d'inspection et d'application de la stratégie. 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 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**.

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.

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.

STEP 1 | Avant de commencer :

1. Configurez une passerelle GlobalProtect.
2. Sélectionnez **Réseau** > **GlobalProtect** > **Passerelles** > *<gateway-config>* pour modifier une passerelle existante ou en ajouter une nouvelle.

STEP 2 | Activez un tunnel séparé.

1. Dans la boîte de dialogue **Configuration de la passerelle GlobalProtect**, sélectionnez **Agent** > **Paramètres de Tunnel** pour activer le **Mode Tunnel**.
2. Configurez les paramètres de tunnel pour l'application GlobalProtect.

STEP 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 ne pouvez configurer de tunnel séparé en fonction du domaine de destination, car ce paramètre est incompatible avec Sophos sur les terminaux macOS. Pour éviter ce problème d'incompatibilité,

1. dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Paramètres du client** > *<client-setting-config>* pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.
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.

STEP 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 environnementaux pour configurer un tunnel séparé selon l'application sur les terminaux Windows et macOS.

1. dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Paramètres du client** > <*client-setting-config*> pour sélectionner une configuration de paramètres client existante ou en ajouter une nouvelle.
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.
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.

STEP 5 | Enregistrez la configuration de la passerelle.

1. Cliquez sur **OK** pour enregistrer la configuration de la passerelle.
2. **Commit (Validez)** vos modifications.

Exclusion du trafic vidéo à partir du tunnel VPN GlobalProtect

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.

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.

STEP 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.
   - 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. Sélectionnez **Réseau** > **GlobalProtect** > **Passerelles** > *<gateway-config>* pour modifier une passerelle existante ou en ajouter une nouvelle.

STEP 2 | Activez un tunnel séparé.

1. Dans la boîte de dialogue Configuration de la passerelle GlobalProtect, sélectionnez **Agent** > **Paramètres de Tunnel**.
2. Configurez les paramètres de tunnel pour l'application GlobalProtect.

STEP 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** > **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.
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.

STEP 4 | Enregistrez la configuration de la passerelle.

1. Cliquez sur **OK** pour enregistrer la configuration de la passerelle.

2. **Commit (Validez)** vos modifications.

Portails GlobalProtect

- Aperçu du portail GlobalProtect
- Tâches préalables à la configuration du portail GlobalProtect
- Paramétrer l'accès au portail GlobalProtect
- Définir les configurations de l'agent GlobalProtect
- Personnaliser l'application GlobalProtect
- Personnaliser les pages d'accès, de bienvenue et d'aide du Portail GlobalProtect
- VPN sans client GlobalProtect

Aperçu du portail GlobalProtect

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. Pour plus d'informations sur les versions prises en charge, voir la section Quelles sont les versions de système d'exploitation prises en charge par GlobalProtect ?

En plus de distribuer 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 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. Reportez-vous à VPN sans client GlobalProtect.

Tâches préalables à la configuration du portail GlobalProtect

Avant de configurer le portail GlobalProtect, vous devez avoir effectué les tâches suivantes :

- 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. Voir Authentification.
- Configurer une passerelle GlobalProtect et comprendre Priorité de passerelle dans une configuration de passerelle multiple.

Paramétrer l'accès au portail GlobalProtect

Après avoir exécuté les tâches préalables à la configuration du portail GlobalProtect, configurez le portail GlobalProtect de la manière suivante :

STEP 1 | Ajoutez le portail.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, puis **Add (Ajoutez)** un portail.
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)**.

STEP 2 | 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 les attaques réussies.*

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)**.

STEP 3 | 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.

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.

STEP 4 | Spécifiez comment le portail authentifie les utilisateurs.

1. 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.
  - 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.).

STEP 5 | 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.

STEP 6 | Enregistrez la configuration du portail.

1. Cliquez sur **OK** pour enregistrer les paramètres.
2. **Validez** les modifications.

Définir les configurations d'authentification client GlobalProtect

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.

STEP 1 | Paramétrer l'accès au portail GlobalProtect.

STEP 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 Authentification pour obtenir les instructions.

Dans la boîte de dialogue configuration des portails GlobalProtect (**Réseau** > **GlobalProtect** > **Portails** > *<portal-config>*), sélectionnez **Authentification** pour **Ajouter** une nouvelle configuration de **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)**), le **Authentication Profile (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).
  - 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.

STEP 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> (configuration du portail)** > **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)**.

STEP 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 GlobalProtect Portal Configuration (Configuration des portails GlobalProtect) (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)*), sélectionnez **Authentication (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.

STEP 5 | Enregistrez la configuration du portail.

1. Cliquez sur **OK** pour enregistrer votre configuration.
2. **Commit (Validez)** les modifications.

Définir les configurations de l'agent GlobalProtect

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.

STEP 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. Sélectionnez **Network (Réseau)** > **GlobalProtect (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 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.

STEP 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.

1. À partir de la configuration du portail (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (<configuration du portail>)*), **Add (Ajoutez)** 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.

STEP 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.
- 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.

  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.

STEP 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. Sélectionnez **Internal (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.

STEP 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).

STEP 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 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, sélectionnez **User/User Group (Utilisateur/Groupe d'utilisateurs)**, puis configurez l'une des options suivantes :
  - 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.
  - 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.
- Pour transmettre cette configuration aux applications en fonction des informations sur l'hôte personnalisées, sélectionnez **Custom Checks (Vérifications personnalisées)**. 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, 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)**

STEP 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. Sélectionnez **External (Externe)**.
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.

STEP 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. Sélectionnez **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) 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.

   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.

STEP 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.

STEP 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 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.

STEP 11 | Enregistrez la configuration d'agent.

Cliquez sur **OK** pour enregistrer la configuration client.

STEP 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)**.

STEP 13 | Enregistrez la configuration du portail.

1. Cliquez sur **OK** pour enregistrer la configuration de client.
2. **Commit (Validez)** les modifications.

Personnaliser l'application GlobalProtect

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.

Les paramètres supplémentaires qui ne sont disponibles que par l'intermédiaire du registre Windows ou Windows Installer (Msiexec) vous permettent de :

- 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.
- 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.

Pour plus d'informations, consultez la section Paramètres d'application personnalisables.

STEP 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. Sélectionnez **Network (Réseau)** > **GlobalProtect (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.

STEP 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 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.

STEP 3 | Spécifiez s'il faut appliquer les connexions GlobalProtect pour l'accès au réseau.

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 réseau est activée et que la connexion à GlobalProtect n'est pas établie**. Spécifiez un maximum de dix 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.

  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.
- 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)**.

  Pour lancer automatiquement votre navigateur web par défaut lors de la détection du portail captif afin de permettre aux utilisateurs de se connecter facilement au portail captif, dans le champ **Lancer automatiquement la page Web dans le navigateur par défaut lors de la détection du portail captif**, saisissez le FQDN (nom de domaine complet) ou l'adresse IP du site Web que vous souhaitez utiliser pour la tentative de connexion initiale qui initie le trafic Web lors du lancement du navigateur Web par défaut (longueur maximale de 256 caractères). Le portail captif intercepte alors cette tentative de connexion et redirige le navigateur Web par défaut à la page de connexion au portail captif. Si le champ est vide (par défaut), GlobalProtect ne lance pas automatiquement le navigateur Web par défaut lors de la détection du portail captif.

  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.

STEP 4 | 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 »).
- Précisez la période de temps (en heures) pendant laquelle vous voulez que l'application GlobalProtect **Utilise automatiquement SSL lorsque IPSec est indisponible** (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 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.
- 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 **Paramètres** > **Général** pour activer **Se connecter au moyen de SSL uniquement** et **Paramètres** > **Connexion** pour vérifier que le **Protocole** est défini sur **SSL**.

- 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 **Yes (Oui)** pour autoriser GlobalProtect à tenter de rétablir la connexion après la déconnexion du tunnel. Définissez cette option sur **No (Non)** pour empêcher GlobalProtect de tenter de rétablir la connexion après la déconnexion du tunnel. 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).

  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 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.

STEP 5 | 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 consulter les informations des onglets suivants :
  - **Général** : affiche le nom d'utilisateur et le ou les portails associés au compte GlobalProtect.
  - **Notification** : affiche les notifications GlobalProtect.

La valeur par défaut est Oui. Lorsque vous activez cette option, les utilisateurs peuvent voir les onglets supplémentaires suivants :

- **Connexion** : présente les passerelles qui sont configurées pour l'application GlobalProtect et des informations à propos de chaque passerelle.
- **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.

- 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 **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.
- 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 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.

STEP 6 | 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 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.

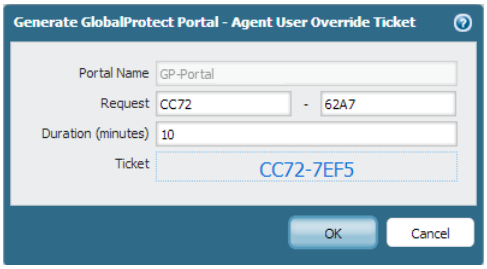
STEP 7 | Spécifiez si les utilisateurs peuvent désactiver l'application GlobalProtect.

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.

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 5.

- 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 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 **Générer un ticket** sur la page **Réseau** > **GlobalProtect** > **Portails** et entre le numéro de demande de l'utilisateur pour générer le ticket. L'administrateur fournit le ticket 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 le **Nombre max. de fois qu'un utilisateur peut désactiver** dans la configuration de l'agent du portail GlobalProtect (**Réseau** > **GlobalProtect** > **Portails** > *<portal-config>* > **Agent** > *<agent-config>* > **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 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).

STEP 8 | Spécifiez si les utilisateurs peuvent désinstaller l'application GlobalProtect.

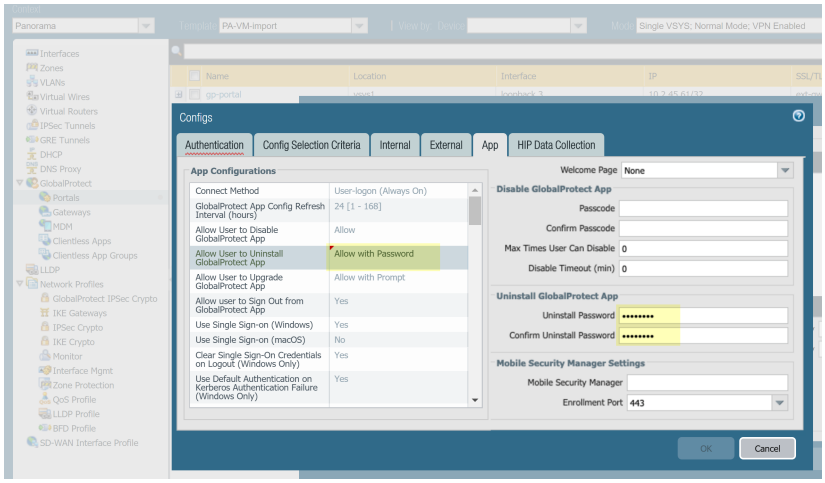
Utilisez l'option **Autoriser l'utilisateur à désinstaller l'application GlobalProtect** pour autoriser les utilisateurs à désinstaller l'application GlobalProtect, pour leur interdire de désinstaller l'application GlobalProtect ou pour les autoriser à la désinstaller spécifiquement au travers d'un mot 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**.
- 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\\ 'Uninstall = 1'`.
- Pour permettre aux utilisateurs de désinstaller l'application GlobalProtect à l'aide d'un mot de passe, sélectionnez **Autoriser avec un mot de passe** ; puis, à la section Désinstaller l'application GlobalProtect, saisissez un **Mot de passe de désinstallation** et **Confirmez le mot de passe de désinstallation**.



STEP 9 | 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 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.

STEP 10 | 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 Guide des nouvelles fonctionnalités de PAN-OS 7.1.
- 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 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).

STEP 11 | 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.

STEP 12 | (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 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.

  Cette fonctionnalité nécessite la version de contenu 731 ou toute version ultérieure et la version de l'application GlobalProtect 4.0.3 ou toute version ultérieure.
- **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.

STEP 13 | (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)**.

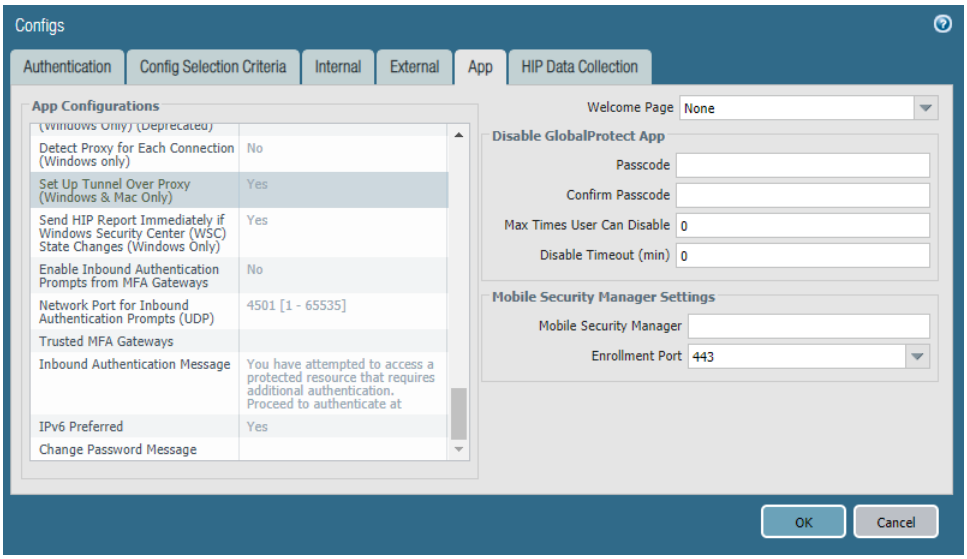
Pour obtenir plus d'informations sur le comportement du trafic réseau en fonction de l'utilisation d'un proxy, reportez-vous à la rubrique Connexions de tunnels via des proxys.

- 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.

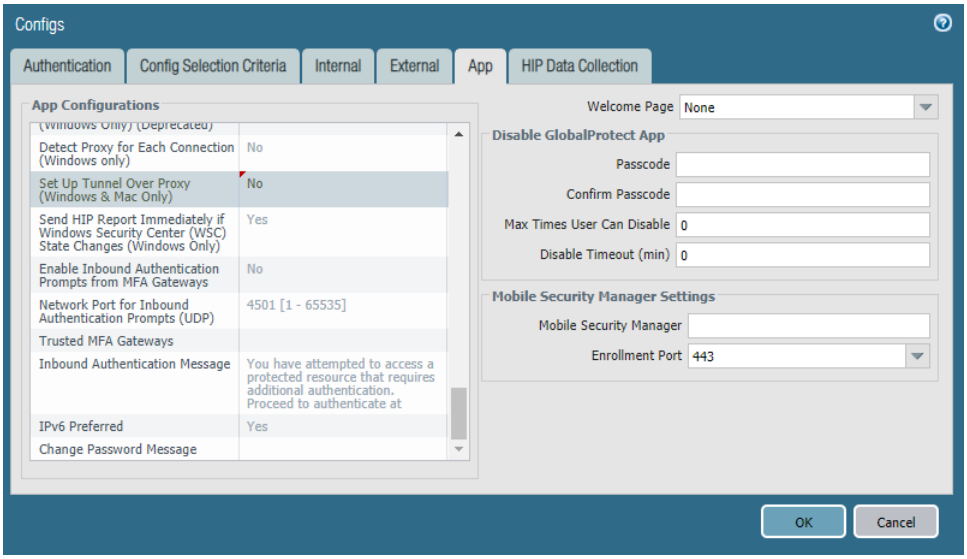
STEP 14 | (Windows et macOS uniquement) Spécifiez si GlobalProtect doit utiliser les proxys ou les contourner.

Ce paramètre vous permet de configurer le comportement du trafic réseau en fonction de l'utilisation des proxys GlobalProtect. Consultez Connexions de tunnels via des proxys pour plus de détails.

- 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)**.



STEP 15 | 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.
- **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).

STEP 16 | 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'attente compris entre 1 et 600 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.

STEP 17 | 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 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.

STEP 18 | 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 5 pour obtenir plus de détails sur les paramètres **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 3.1.3 connecté à un portail GlobalProtect 3.1.1 n'est pas mis à niveau.

STEP 19 | 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).

STEP 20 | 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.

STEP 21 | (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.

STEP 22 | 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. **Commit (Validez)** les modifications.

Personnaliser les pages d'accès, de bienvenue et d'aide du Portail GlobalProtect

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.

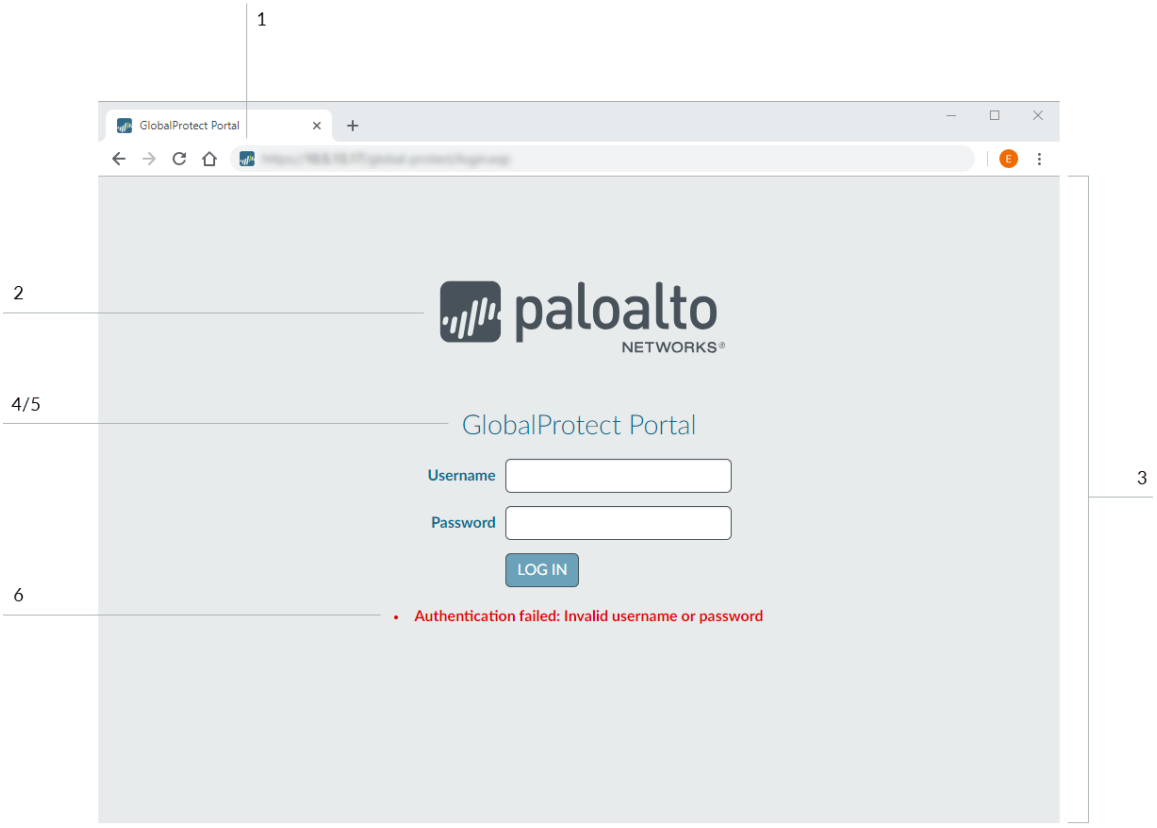
Vous pouvez également désactiver l'accès du navigateur à la page de connexion du portail pour évite les tentatives non autorisées d'authentification au portail Global Protect (configurez l'option Portal Login Page (Page de connexion au portail) > Disable (Désactiver) depuis Network (Réseau) > GlobalProtect > Portals (Portails) > <portal_config > General (Général)). 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.

STEP 1 | Exportez le portail par défaut, la page d'accueil, la page de bienvenue ou la page d'aide.

1. Sélectionnez **Device (Périphérique)** > **Response Pages (Pages de réponse)**.
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)**.

STEP 2 | Modifiez la page exportée.

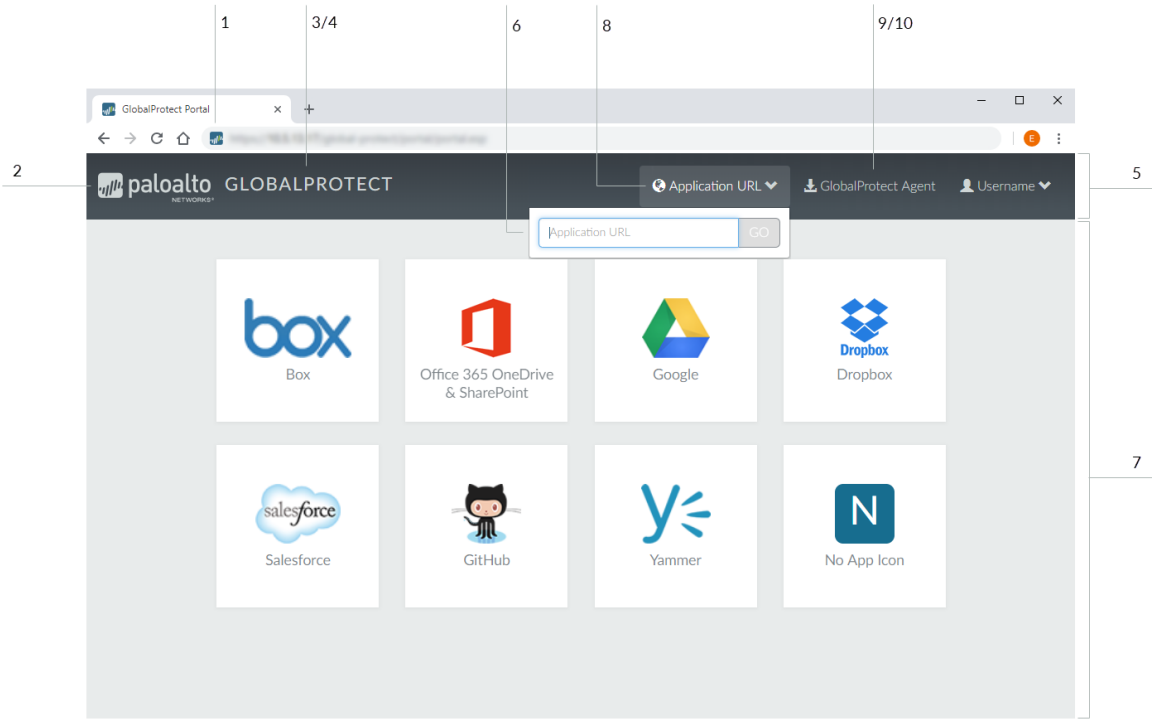
1. À l'aide d'un éditeur de texte HTML de votre choix pour ouvrir et modifier la page.
2. Pour modifier la page d'accueil ou de connexion, configurez l'une des variables suivantes :
   - **GlobalProtect Portal Login Page (Page de connexion du portail GlobalProtect)** :

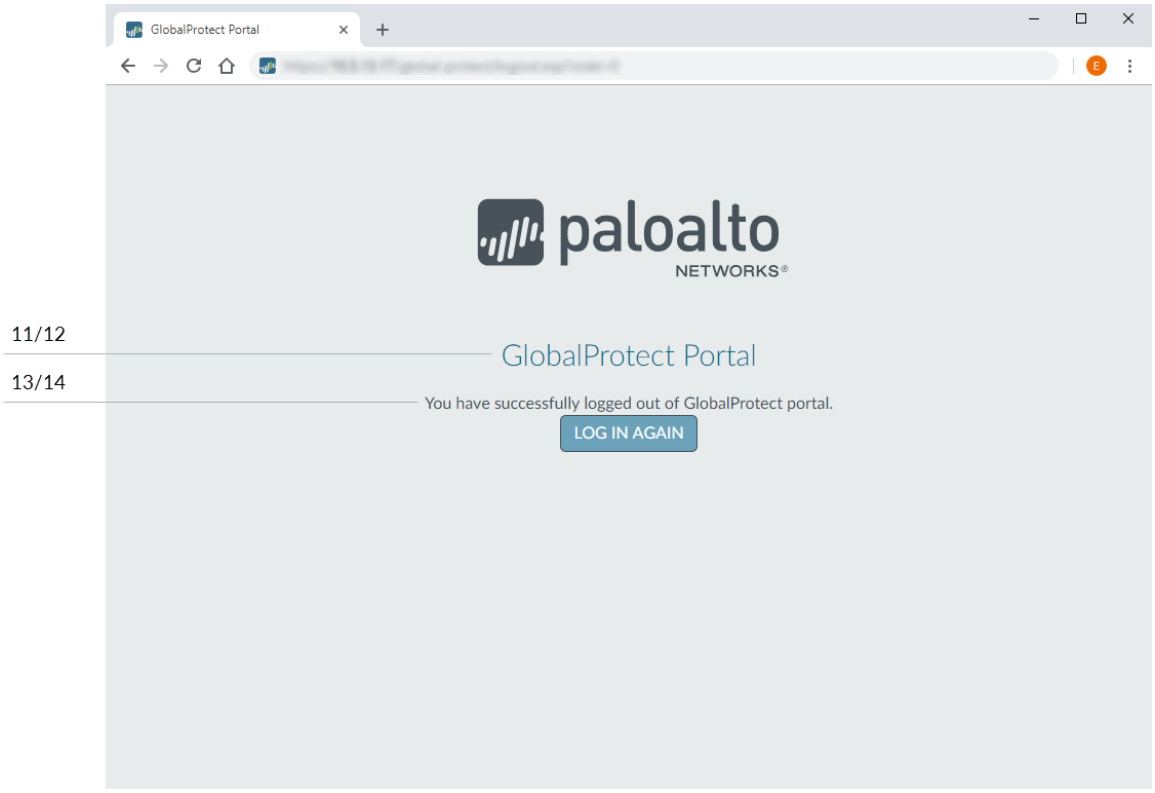


Numéro de l'étiquett	Variable	Description	Exemple
1	`favicon`	URL de l'icône qui s'affiche dans la barre d'adresse du navigateur Web.	`var favicon = 'http://cdn.slidesharecdn.com/logo-24x24.jpg?3975762018';`
2	`logo`	URL du logo de l'entreprise.	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
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';`

Numéro de l'étiquett	Variable	Description	Exemple
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';`

- **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 = 'http://cdn.slidesharecdn.com/logo-24x24.jpg?3975762018';`
2	`logo`	URL du logo de l'entreprise.	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
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';`

Numéro de l'étiquett	Variable	Description	Exemple
5	navbar_bg_color	Couleur d'arrière-plan de la barre de navigation.	var navbar_bg_color = '#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 = 'Application 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_globalprotect_agent = 1;
10	label_globalprotect_agent	Étiquette du bouton de téléchargement de l'application GlobalProtect.	var label_globalprotect_agent = '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	var logout_text_array = ["You have successfully logged out of

Numéro de l'étiquett	Variable	Description	Exemple
		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.*	`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.", "Can not 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';`

3. Enregistrez la page modifiée avec un nouveau nom de fichier. Veillez à ce que la page conserve son codage UTF-8.

STEP 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.

STEP 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 Appearance (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.

STEP 5 | Enregistrez la configuration du portail.

Cliquez sur **OK (OK)** pour enregistrer la configuration du portail, puis sur **Commit (Valider)** pour valider vos modifications.

STEP 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.

Applications GlobalProtect

- Téléchargement de l'application GlobalProtect
- Déployer le logiciel de l’application GlobalProtect
- Définir les configurations de l'agent GlobalProtect
- Personnaliser l'application GlobalProtect
- Déployer les paramètres d'agent de façon transparente

Déployer l'application GlobalProtect aux utilisateurs finaux

Pour se connecter à GlobalProtect™, un poste de travail doit utiliser l'application GlobalProtect. La méthode de déploiement du logiciel dépend des types de points de terminaison 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 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

Platform (Plateforme)	Options de déploiement
	vos points de terminaison mobiles, vous pouvez utiliser le système pour déployer et configurer l'application GlobalProtect. Voir la gestion des points de terminaison mobile.
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. Voir la gestion des points de terminaison mobile. • **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. Voir la gestion des points de terminaison mobile. • **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 les Chromebooks gérés à l'aide de la console Google Admin, reportez-vous à 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, qui n'est pas prise en charge à partir de la version 5.0 de l'application GlobalProtect.* • **À partir de AirWatch** : Vous pouvez déployer l'application GlobalProtect pour Android sur les Chromebook gérés qui sont inscrits auprès de AirWatch. 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 les Chromebook gérés à l'aide d'AirWatch, reportez-vous à Déployez l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide d'AirWatch.
Linux	Après avoir téléchargé l'application GlobalProtect pour Linux sur le Site de support, vous pouvez la distribuer et l'installer :

Platform (Plateforme)	Options de déploiement
	• **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 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.

Téléchargement de l'application GlobalProtect

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 (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 aux utilisateurs finaux). 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 :

STEP 1 | Connectez-vous au portail de support client de Palo Alto Networks (https://support.paloaltonetworks.com/).

Vous devez posséder un compte de réseaux Palo Alto valide pour vous connecter et télécharger des logiciels à partir de la page mises à jour logicielles. Si vous ne pouvez pas vous connecter et ayez besoin d'aide, allez à https://www.paloaltonetworks.com/support/Tabs/Overview.html.

STEP 2 | Sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.

STEP 3 | Sélectionnez la version de l'application GlobalProtect par système d'exploitation.

STEP 4 | Passez en revue les Notes de version de la version de l'application, puis sélectionnez le lien de téléchargement pour procéder au téléchargement.

STEP 5 | Déployer l'application GlobalProtect aux utilisateurs finaux.

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.

Héberger les mises à jour de l'application sur le portail

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 Téléchargement de l'application GlobalProtect 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.

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.

STEP 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.

STEP 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, Téléchargement de l'application GlobalProtect. Après avoir téléchargé l'image du logiciel, revenez à la page **Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)** du pare-feu pour la **Upload (Charger)**.

STEP 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 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

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.

STEP 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.

STEP 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, Téléchargement de l'application GlobalProtect.

STEP 3 | Publiez l'image du logiciel sur votre serveur Web.

STEP 4 | Redirigez les utilisateurs finaux vers le serveur Web.

Sur le pare-feu hébergeant le portail, saisissez les commandes CLI suivantes en mode opérationnel :

```
> set global-protect redirect on
> set global-protect redirect location <path>
```

où *path*> est le chemin de l'URL jusqu'au dossier hébergeant l'image (par exemple **`https://acme/GP`**).

STEP 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.

Tester l'installation de l'application

Utilisez la procédure suivante pour tester l'installation de l'application GlobalProtect.

STEP 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. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**.
2. Sélectionnez une configuration de portail existante que vous souhaitez modifier ou **Add (Ajoutez)**-en une nouvelle.
3. À l'onglet **Agent**, sélectionnez une configuration existante ou **Add (Ajoutez)**-en une nouvelle à déployer sur les utilisateurs / le groupe de test.
4. À l'onglet **User/User Group (Utilisateur/Groupe d'utilisateurs)**, **Add (Ajoutez)** le **User/User Group (Utilisateur/Groupe d'utilisateurs)** qui testera l'application.
5. 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.
6. (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.
7. **Commit (Validez)** les modifications.

STEP 2 | Connectez-vous au portail GlobalProtect.

1. Lancez votre navigateur Web et accédez à l'URL suivante :

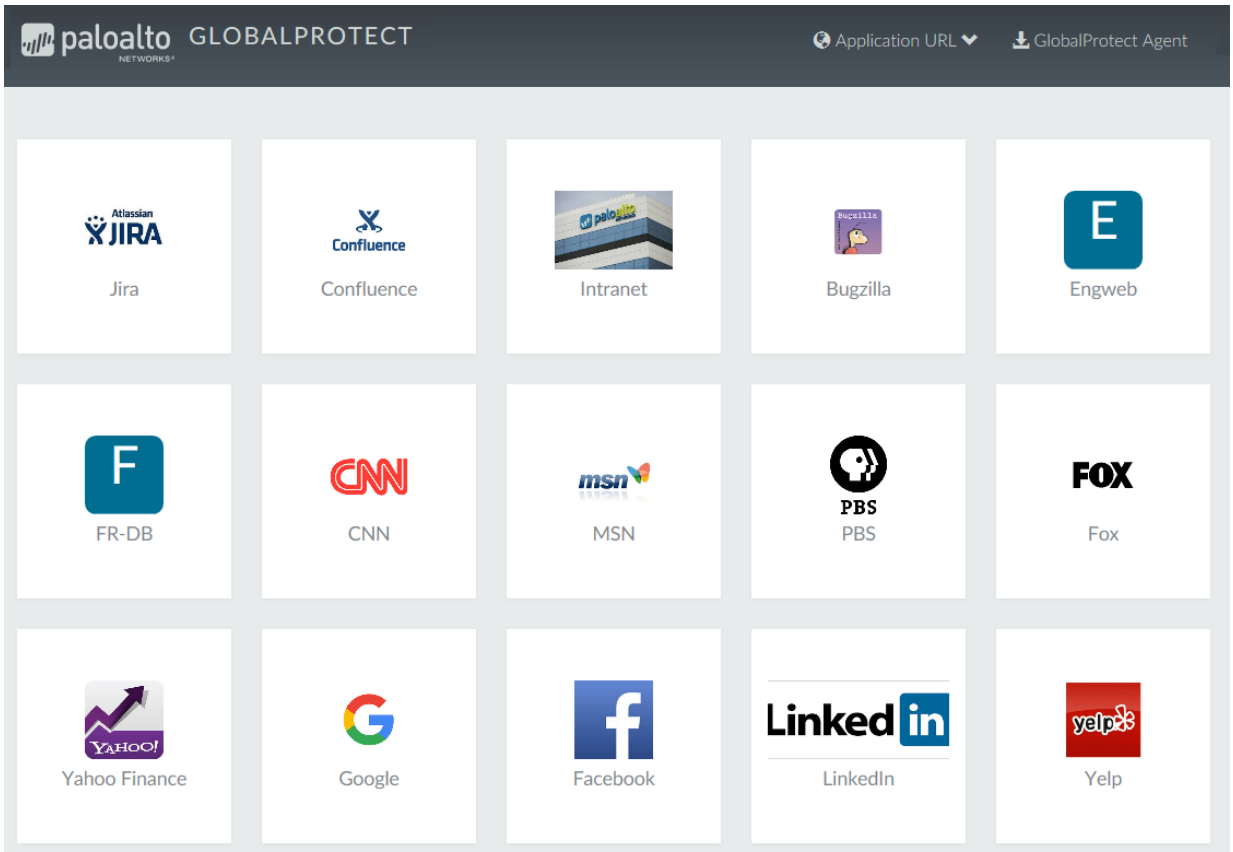
   ```
   https://<portal address or name>
   ```

   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)**.

STEP 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.



STEP 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.

STEP 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`), ou cliquez sur **Browse (Parcourir)** pour choisir un nouvel emplacement, puis cliquez sur **Next (Suivant)** deux fois.
3. Une fois l'installation terminée, **Close (Fermer)** l'assistant.

STEP 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

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
- 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 obtenir des instructions sur le déploiement de l'application GlobalProtect depuis AirWatch, consultez Déployer l'application mobile GlobalProtect à l'aide d'AirWatch..

STEP 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.

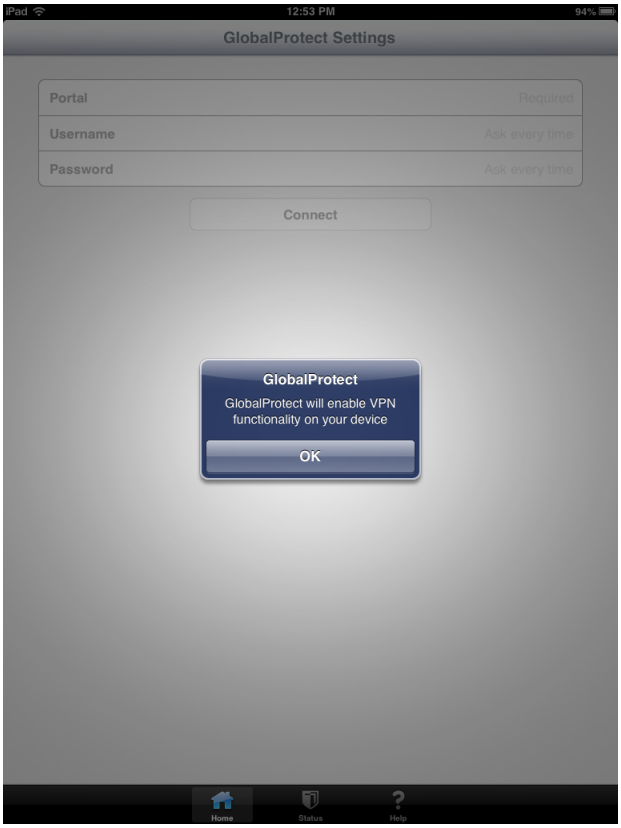
1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**.
2. Sélectionnez une configuration de portail existante à modifier ou **Add (Ajoutez)**-en une nouvelle.
3. À l'onglet **Agent**, sélectionnez une configuration existante ou **Add (Ajoutez)**-en une nouvelle à déployer sur les utilisateurs /le groupe de test.
4. À l'onglet **User/User Group (Utilisateur/Groupe d'utilisateurs)**, **Add (Ajoutez)** le **User/User Group (Utilisateur/Groupe d'utilisateurs)** qui testera l'application.
5. Sélectionnez le **OS (Système d'exploitation)** pour l'application que vous testez (**iOS**, **Android** ou **WindowsUWP**).
6. (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.
7. **Commit (Validez)** les modifications.

STEP 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.

STEP 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**.



STEP 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.

Déployer les paramètres d'application de façon transparente

En tant que solution de rechange au déploiement des paramètres d'application à partir de la configuration du portail, vous pouvez les définir directement à partir du registre Windows ou de la plist MacOS ou - sur les points de terminaison Windows uniquement - en utilisant le programme d'installation de Windows (Msiexec). L'avantage de cette procédure est qu'elle active le déploiement des paramètres de l'application GlobalProtect sur les points de terminaison avant leur première connexion au portail GlobalProtect.

Les paramètres définis dans la configuration du portail annulent toujours les paramètres définis dans le registre Windows ou la Plist MacOS. Si vous définissez les paramètres dans le registre ou la Plist, 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 et MacOS :

- 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

En plus d'utiliser le registre Windows et la plist MacOS 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 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

En plus du pré-déploiement de l'adresse du portail, vous pouvez également définir les paramètres de l'application. Pour Déployer les paramètres d'application sur des points de terminaison Windows, vous devez définir des clés dans le registre Windows (`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`). Pour Déployer les paramètres d'application sur des points de terminaison MacOS, vous devez définir des entrées dans le dictionnaire `PanSetup` de la plist macOS (`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`). 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. Ces paramètres incluent les suivants `:can-prompt-user-credential`, `wrap-cp-guid` *et* `filter-non-gpcp`.

Options d'affichage de l'application

Le tableau suivant répertorie les options que vous pouvez configurer dans le Registre Windows et MacOS plist pour personnaliser l'affichage de l'application GlobalProtect.

Table 3: Tableau : Paramètres d'application personnalisables

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (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`	`RESUBMITHOSTINFO="yes | no"`	`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.

Table 4: Tableau : Options de comportement utilisateur personnalisables

Configuration de l'agent du portail	Registre Windows/Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
Permettre à l'Utilisateur de modifier l'Adresse du portail	`Peut-il changer le portail oui | non`	`CANCHANGEPORTAL="yes | no"`	`yes`

Configuration de l'agent du portail	Registre Windows/Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
Permettre à l'utilisateur de désactiver la page de bienvenue	`Ouvrir-cacher-la page de bienvenue oui | non`	`ENABLEHIDEWELCOMEPAGE= ”yes | no”`	`yes`
Permettre à l'utilisateur de continuer avec un certificat de serveur de portail invalide	`can-continue-if-portal-cert-invalid yes | no`	`CANCONTINUEIFPORTALCERT INVALID= ”yes | no”`	`yes`
Autoriser l'utilisateur à désactiver GlobalProtect App	`Autorisé à désactiver oui | non`	`DISABLEALLOWED="yes | no"`	`no`
Enregistrer les informations 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.	`Sauvegarder les informations d'identification 0 | 1 | 2`	`SAVEUSERCREDENTIALS 0 | 1 | 2`	S. O.
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	`Peut-il sauvegarder un mot de passe oui | non`	`CANSAVEPASSWORD=”yes | no”`	`yes`

Configuration de l'agent du portail	Registre Windows/Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
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.			
Windows uniquement/pas sur le portail 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.	`ShowPrelogonButton yes | no`	S. O.	`no`

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.

Table 5: Tableau : Options de comportement de l'application personnalisables

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
Méthode de connexion	`connect-method on-demand | pre-logon | user-logon`	`CONNECTMETHOD="on-demand | pre-logon | user-logon"`	`user-logon`
Intervalle de rafraîchissement de configuration de l'application GlobalProtect (en heures)	`refresh-config-interval <hours>`	`REFRESHCONFIGINTERVAL= "<hours>"`	`24`
Mettre à jour les paramètres de DNS à la connexion (Windows uniquement)	`flushdns yes | no`	`FLUSHDNS="yes | no"`	`no`
Envoyer immédiatement un rapport HIP si l'état du centre de sécurité de Windows (WSC) change (Windows uniquement)	`wscautodetect yes | no`	`WSCAUTODETECT="yes | no"`	`no`
Détecter le proxy pour chaque connexion (Windows uniquement)	`ProxyMultipleAuto Detection yes | no`	`ProxyMultipleAuto Detection="yes | no"`	`no`
Effacer les identifiants d'ouverture de session unique à la fermeture de session (Windows uniquement)	`LogoutRemoveSSO Oui | Non`	`LogoutRemoveSSO="yes | no"`	`yes`
Utiliser l'authentification par défaut en cas d'échec d'authentification Kerberos	`Solution de repli si échec d'authentification Kerberos oui | non`	`KRBAUTHFAILFALLBACK= "yes | no"`	`no`

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
(Windows uniquement)			
Message personnalisé d'expiration de mot de passe (authentification LDAP uniquement)	`PasswordExpiryMessage <message>`	`PasswordExpiryMessage "<message>"`	
Délai d'expiration de connexion au portail (sec.)	`PortalTimeout <portaltimeout>`	`PORTALTIMEOUT= "<portaltimeout>"`	`5`
Délai d'expiration de connexion TCP (sec.)	`ConnectTimeout <connecttimeout>`	`CONNECTTIMEOUT= "<connecttimeout>"`	`5`
Délai d'expiration de réception TCP (sec)	`ReceiveTimeout <receivetimeout>`	`RECEIVETIMEOUT= "<receivetimeout>"`	`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.
Délai d'expiration pour renommer le tunnel de bascule d'utilisateur (sec)	`user-switch-tunnel-rename-timeout <renameTimeout>`	S. O.	`0`

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
Utiliser l'ouverture de session unique **(Windows uniquement)**	`use-sso yes | no`	`USESSO="yes | no"`	`yes`
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`
Windows uniquement/pas sur le portail Ce paramètre est utilisé en association avec 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.	`can-prompt-user-credential yes | no`	`CANPROMPTUSERCREDENTIAL= "yes | no"`	`yes`
Windows uniquement/pas sur le portail Ce paramètre filtre la fenêtre	`wrap-cp-guid {guide du fournisseur d'informations d'identification indépendantes}`	`WRAPCPGUID="{guid_value]" FILTERNONGPCP="yes | no"`	`no`

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
d'informations d'identification indépendantes du fournisseur dans la page de connexion Windows de sorte que seule la fenêtre Windows native s'affiche.*			
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 de connexion Windows native.*	`filter-non-gpcp no`	S. O.	S. O.
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.

*Pour connaître les étapes détaillées à suivre pour activer ces paramètres à l'aide du registre Windows ou de Windows Installer (Msiexec), consultez l'*emballage SSO pour les fournisseurs d'informations d'identification tierces dans les points de terminaison 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.

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 complet dans les commandes.*	**command <parameter1> <parameter2> [...]** Exemple Windows : **command %userprofile %\vpn_script.bat c: test_user** Exemple MacOS : **command $HOME/ vpn_script.sh / Users/test_user test_user**	**PREVPNCONNECTCOMMAND= "<parameter1> <parameter2> [...]"** **POSTVPNCONNECTCOMMAND= "<parameter1> <parameter2> [...]"** **PREVPNDISCONNECTCOMMAND= "<parameter1> <parameter2> [...]"**	**S. O.**
(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,	**timeout <valeur>** Exemple : **timeout 60**	**PREVPNCONNECTTIMEOUT= "<valeur>"** **POSTVPNCONNECTTIMEOUT= "<valeur>"** **PREVPNDISCONNECTTIMEOUT= "<valeur>"**	0

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
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.*			
(Facultatif) Précisez le chemin d'accès complet d'un fichier utilisé dans une commande. L'application GlobalProtect vérifie l'integrité du fichier en le contrôlant avec la valeur indiquée dans la clé checksum. *Les variables d'environnement sont prises en charge.*	**file <chemin_fichier>**	**PREVPNCONNECTFILE= "<chemin_fichier>"** **POSTVPNCONNECTFILE= "<chemin_fichier>"** **PREVPNDISCONNECTFILE= "<chemin_fichier>"**	**S. O.**
(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	**error-msg <message>** Exemple :	**PREVPNCONNECTERRORMSG= "<message>"**	**S. O.**

Configuration de l'agent du portail	Registre Windows/ Plist MacOS	Paramètre MSIEXEC	Default (Par défaut)
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 Échec de l'exécution de l'action pre-vpn-connect!**	**POSTVPNCONNECTERRORMSG= "<message>"** **PREVPNDISCONNECTERRORMSG ="<message>"**	

Déployer les paramètres d'application sur des points de terminaison Windows

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
- 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
- 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

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*.*

STEP 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 :

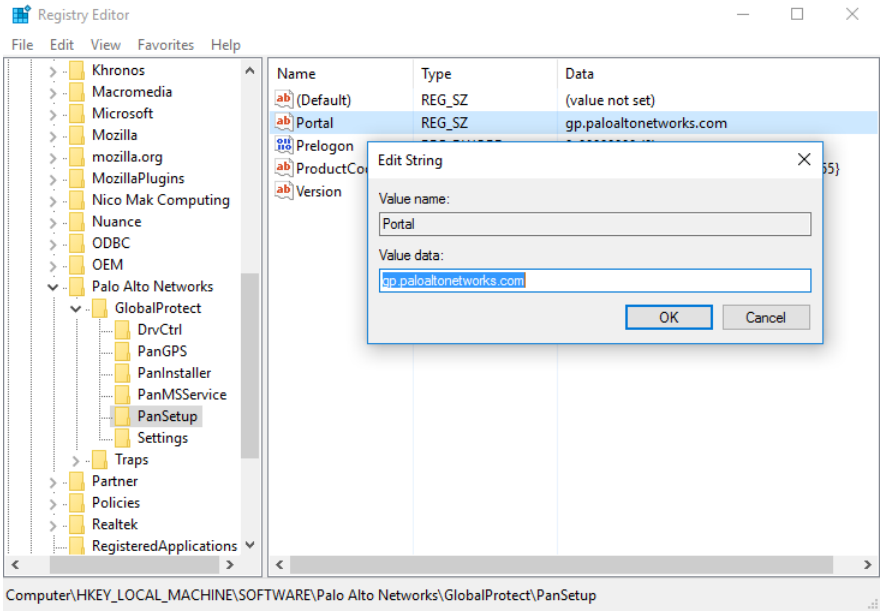
```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings\
```

STEP 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.

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**.



STEP 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.

Affichez les paramètres d'application personnalisables pour obtenir une liste complète des commandes et des valeurs que vous pouvez configurer à l'aide du Registre Windows.

STEP 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

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

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.

STEP 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`

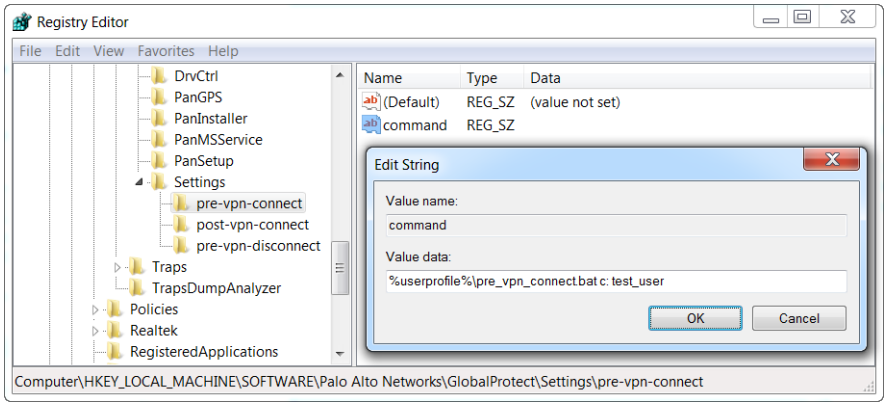
Si la clé n'existe pas dans la touche Settings (Paramètres), créez-la en cliquant avec le bouton droit de la souris sur Settings (Paramètres) et en sélectionnant New (Nouvelle) > Key (Clé)).

STEP 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
```



STEP 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 la section Paramètres d'application personnalisables.

Déployer des scripts à l'aide de Msiexec

Sur les points de terminaison 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 (voir 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 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, reportez-vous à la section 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, reportez-vous à la section Paramètres d'application personnalisables.

Englobement de l'ouverture de session unique pour les fournisseurs d'informations d'identification indépendantes sur les clients Windows

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.

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.

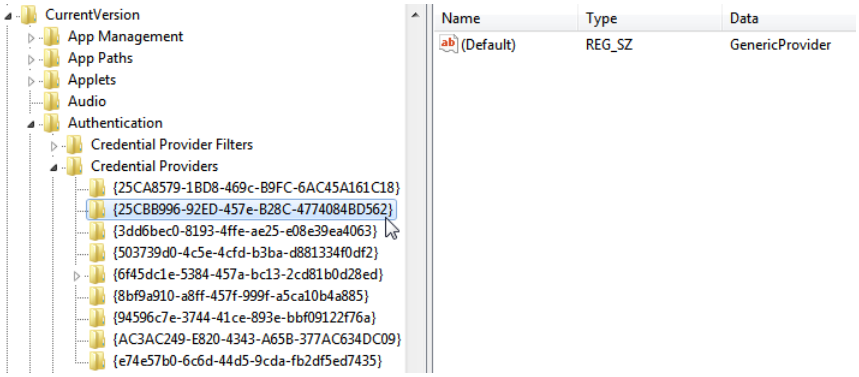
Activer l'englobement d'ouverture de session unique pour les informations d'identification indépendantes avec le registre Windows

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.

STEP 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 :

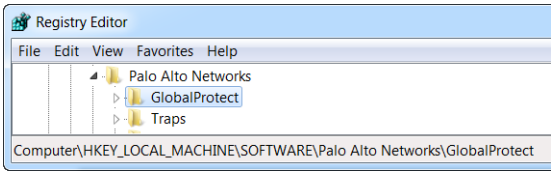
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion \Authentication\Credential Providers.`
3. Copiez la clé GUID pour le fournisseur d'accréditation que vous désirez envelopper (y compris les accolades - `{` et `}` - à la fin du GUID) :



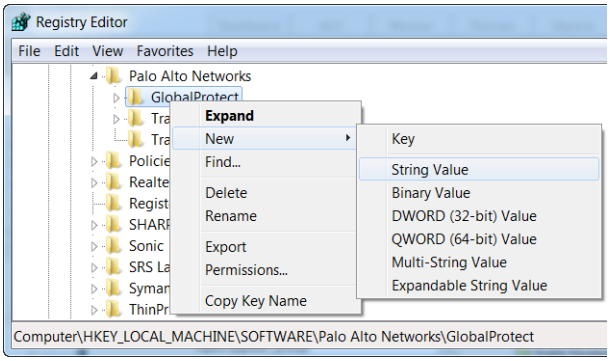
STEP 2 | Activez l'englobement d'ouverture de session unique pour les fournisseurs d'informations d'identification tiers en ajoutant le paramètre **`wrap-cp-guid`** au registre GlobalProtect.

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 :



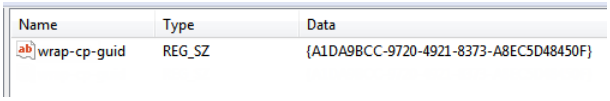
3. Configurez les champs de la **String Value (Chaîne de valeur)** suivants :
   - **Name (Nom)** : **`wrap-cp-guid`**
   - **Value Data (Données de valeur)** :{<**`GUID de fournisseur d'informations d'identification indépendantes`**>}

     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}
```

   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)**.

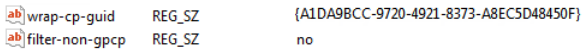


STEP 3 | Étapes suivantes :

- 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.

STEP 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.

STEP 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.

STEP 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.

STEP 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

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

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.

- Déployer les paramètres d'application dans la Plist MacOS
- Déployer des scripts à l'aide de la Plist MacOS

Déployer les paramètres d'application dans la Plist MacOS

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.

STEP 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.

STEP 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`.

STEP 3 | Déployez divers paramètres au point de terminaison macOS, y compris la méthode de connexion utilisée pour l'application GlobalProtect.

Affichez les paramètres d'application personnalisables pour obtenor une liste complète des clés et des valeurs que vous pouvez configurer à l'aide de la plist MacOS.

Déployer des scripts à l'aide de la Plist MacOS

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.

STEP 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.

STEP 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.

STEP 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.

STEP 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 la section Paramètres d'application personnalisables.

STEP 5 | Enregistrez les modifications apportées au fichier de plist.

Enregistrez la plist.

VPN sans client GlobalProtect

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. Les rubriques suivantes fournissent des informations sur la configuration et le dépannage du VPN sans client.

Aperçu du VPN sans client

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.

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.

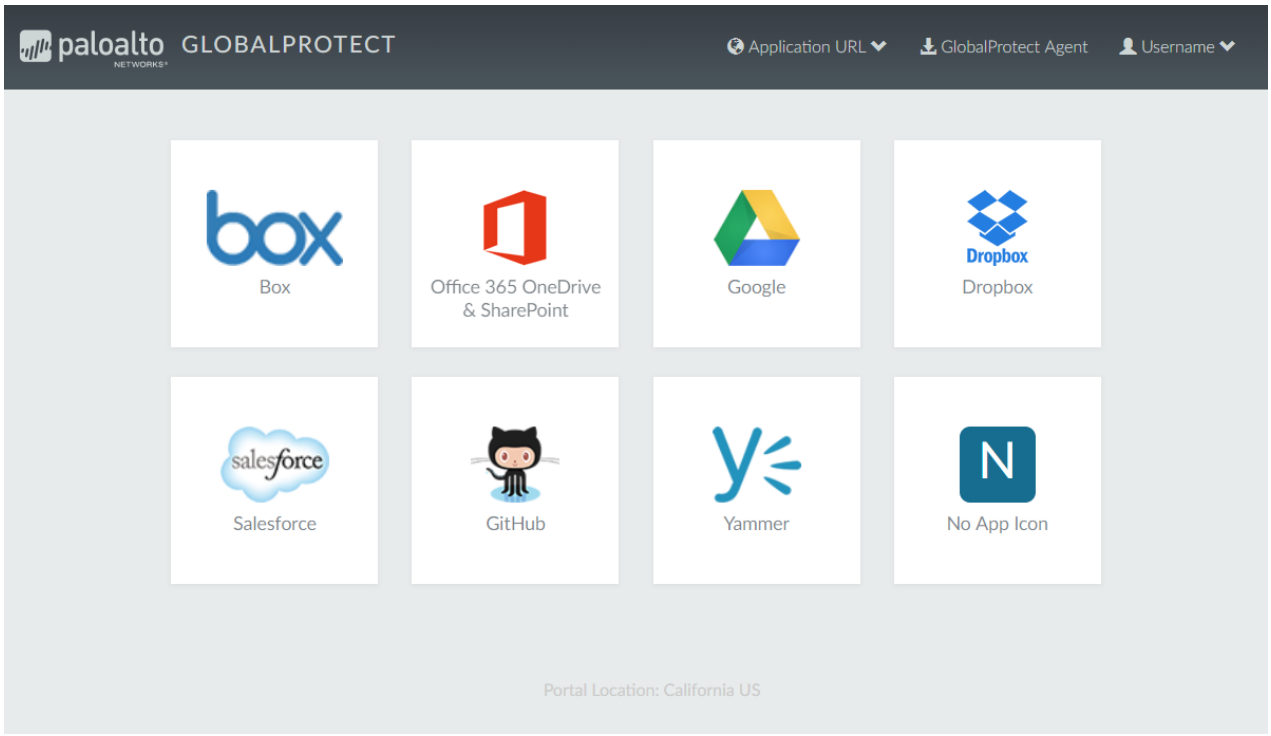


Figure 3: Page d'accueil des applications pour VPN sans client

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 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.

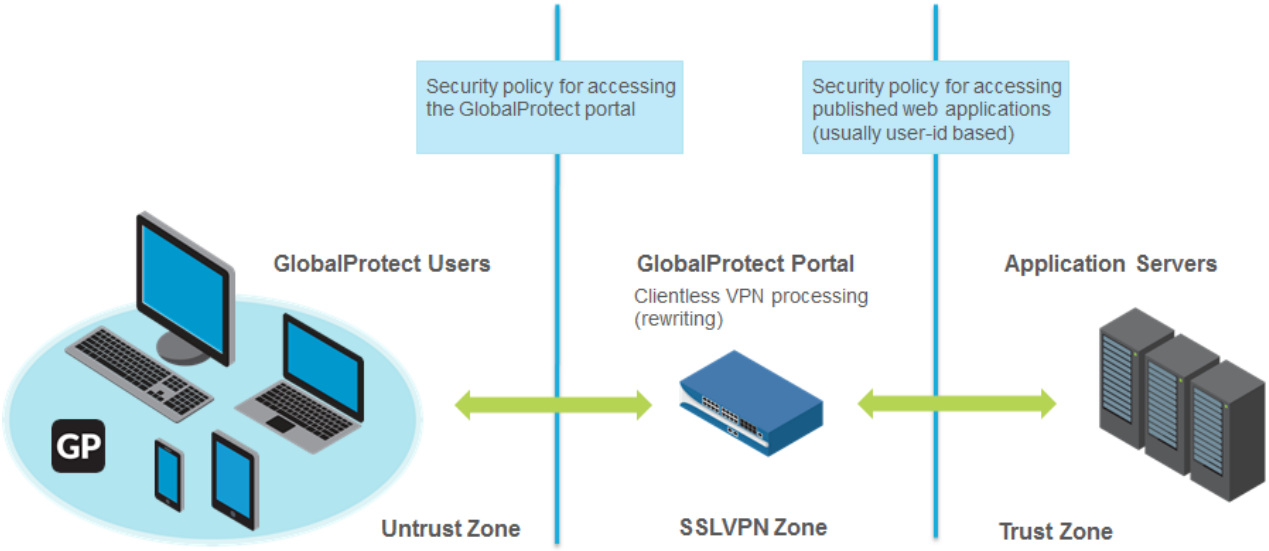


Figure 4: Zones et politique de sécurité pour VPN sans client

Technologies prises en charge

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.

TECHNOLOGIES	Version prise en charge

Technologies d'application Web	• HTML
	• HTML5
	• HTML5-Web-Sockets
	• Javascript
	• Remote Desktop Protocol (protocole de prise de contrôle à distance des postes - 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 ou VMWare Horizon et Vcenter, soutiennent l'accès nativement via HTML5. Vous pouvez utilisez RDP, VNC ouSSH sur ces 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 HOBLink ou 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.
	Les autres technologies (telles que Microsoft Sliverlight ou XML/XSLT) ne sont pas prises en charge.

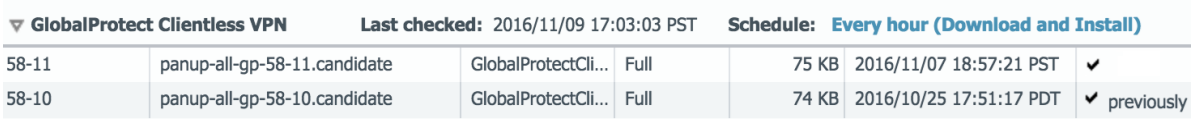
Systèmes d'exploitation	• Windows • macOS • iOS • Android • Chrome • Linux
Navigateurs pris en charge	• Chrome • Microsoft Edge • Internet Explorer • Safari • Firefox

Configurer le VPN sans client

Pour configurer VPN sans client GlobalProtect :

STEP 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.



GlobalProtect Clientless VPN	Last checked: 2016/11/09 17:03:03 PST		Schedule: Every hour (Download and Install)			
58-11	panup-all-gp-58-11.candidate	GlobalProtectCli...	Full	75 KB	2016/11/07 18:57:21 PST	✔
58-10	panup-all-gp-58-10.candidate	GlobalProtectCli...	Full	74 KB	2016/10/25 17:51:17 PDT	✔ previously

- 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.

STEP 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 (Ajoutez)** 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**.

STEP 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**.

STEP 4 | Configurez le portail GlobalProtect pour fournir le service VPN sans client.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portal (Portail)**, puis sélectionnez une configuration de portail existante ou **Add (Ajoutez)**-en 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).

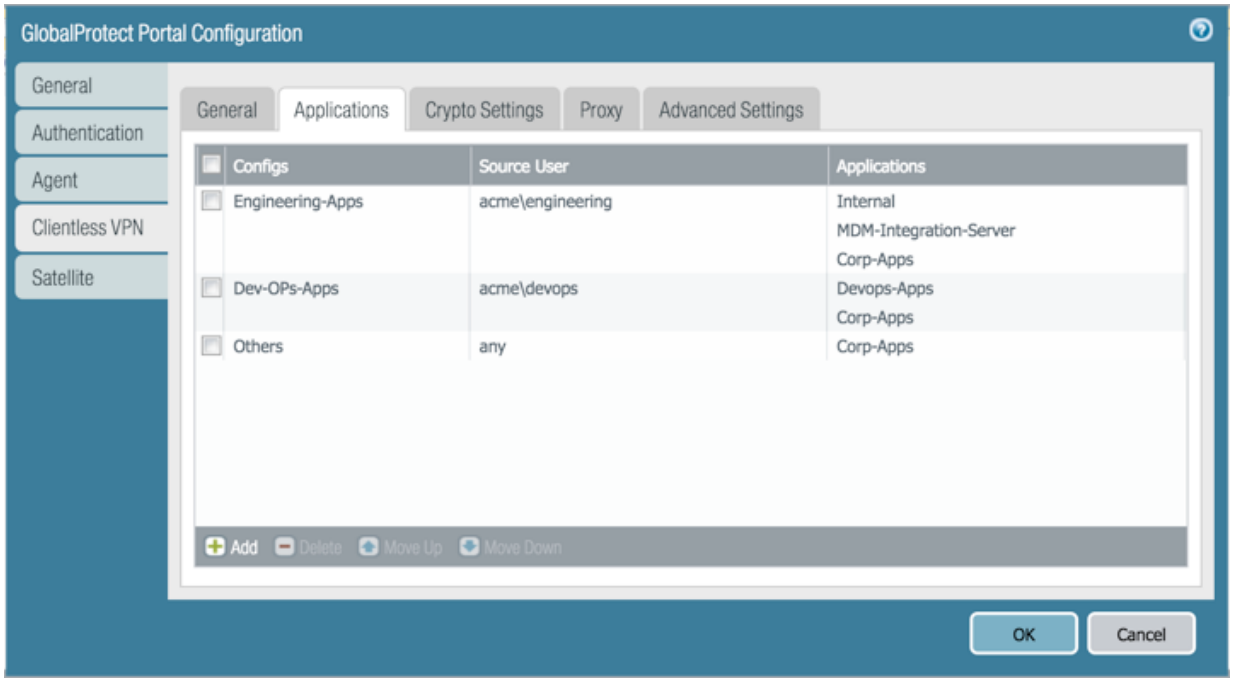
     Si vous utilisez la Traduction des adresses réseau (NAT) pour fournir un accès au portail GlobalProtect, l'adresse IP ou FQDN que vous saisissez doit correspondre à (ou se résoudre en) l'adresse IP NAT du portail GlobalProtect (l'adresse IP publique). Étant donné que les utilisateurs ne peuvent pas accéder 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.

STEP 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 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 d'association des groupes)) 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)**.
2. Spécifiez les **Source Users (Utilisateurs source)**. Vous pouvez **Add (Ajoutez)** des utilisateurs individuels ou des groupes d'utilisateurs auxquels appliquer la configuration 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.

STEP 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**.
   - **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.

STEP 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.

STEP 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).

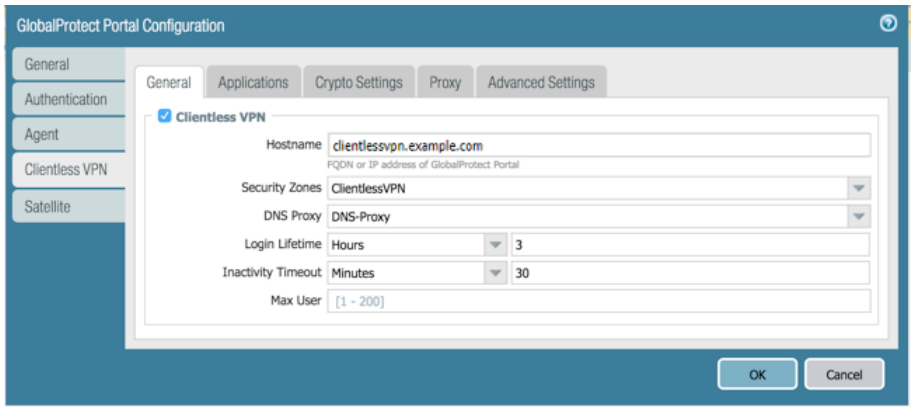
STEP 9 | Enregistrez la configuration du portail.

1. Cliquez deux fois sur **OK**.
2. **Commit (Validez)** vos modifications.

STEP 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 :

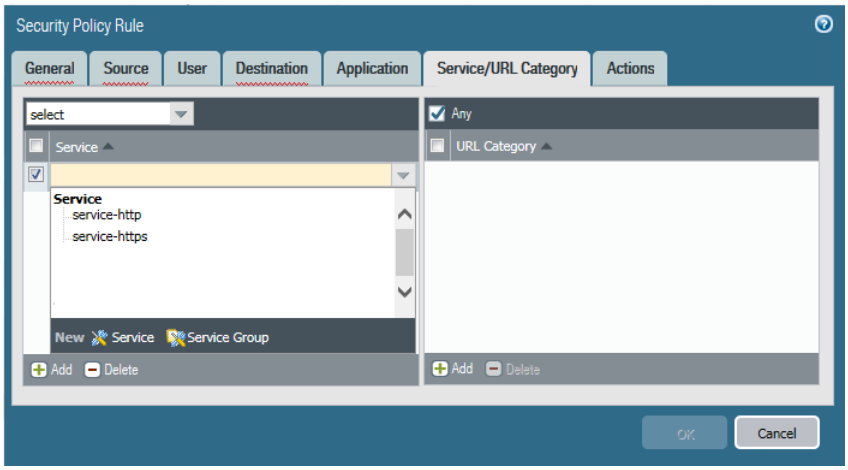
- Rendre le portail GlobalProtect qui héberge le VPN sans client accessible depuis Internet. Il s'agit du trafic depuis une zone non approuvée ou une zone Internet vers la zone où vous hébergez le portail VPN sans client.
- Autoriser les utilisateurs VPN sans client à accéder à Internet. Il s'agit du trafic depuis la zone VPN sans client vers la zone non approuvée ou la zone Internet.



- 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**.



- 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.

STEP 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> set deviceconfig setting 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.

Résoudre les problèmes du VPN sans client

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 :

Table 6: 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** proxy uses shared allocator SSL certificate cache: Current Entries: 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** GlobalProtect Portal : 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 before login lifetime : 10748 Total number of user 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	**show system setting ssl-decrypt dns-cache** Total DNS cache entries: 89 Site IP Expire(secs) Interface bugzilla.panw.local 10.0.2.15 querying 0

Action (Action)	Commande
problème de DNS, vous remarquerez la requête sur un FQDN qui n'était pas résolvable dans la sortie CLI.	`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`** `User: johndoe, Session-id: 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0, 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 au Tableau : Statistiques du moteur de réécriture pour des informations sur les statistiques de réécriture et leur signification ou objectif.
	`show system setting ssl-decrypt rewrite-stats`
	
	`Rewrite Statistics`
	`initiate_connection : 11938`
	`setup_connection : 11909`
	`session_notify_mismatch : 1`
	`reuse_connection : 37`
	`file_end : 4719`
	`packet : 174257`
	`packet_mismatch_session : 1`
	`peer_queue_update_rcvd : 167305`
	`peer_queue_update_sent : 167305`
	`peer_queue_update_rcvd_failure: 66`
	`setup_connection_r : 11910`
	`packet_mismatch_session_r : 22`
	`pkt_no_dest : 23`
	`cookie_suspend : 2826`
	`cookie_resume : 2826`
	`decompress : 26`
	`decompress_freed : 26`
	`dns_resolve_timeout : 27`
	`stop_openend_response : 43`
	`received_fin_for_pending_req : 26`
	`Destination Statistics`
	`To mp : 4015`
	`To site : 12018`
	`To dp : 17276`
	`Return Codes Statistics`
	`ABORT : 18`
	`RESET : 30`
	`PROTOCOL_UNSUPPORTED : 7`
	`DEST_UNKNOWN : 10`
	`CODE_DONE : 52656`
	`DATA_GONE : 120359`
	`SWITCH_PARSER : 48`
	`INSERT_PARSER : 591`
	`SUSPEND : 2826`
	`Total Rewrite Bytes : 611111955`
	`Total Rewrite Useconds : 6902825`
	`Total Rewrite Calls : 176545`

Action (Action)	Commande
Commandes de débogage	
Activer les journaux de débogage sur le pare-feu exécutant le portail de VPN sans client	**debug dataplane packet-diag set log feature ssl all** **debug dataplane packet-diag set log feature misc all** **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

Action (Action)	Commande
	Log-throttle: no Sync-log-by-ticks: yes Features: Counters: ---------- Packet capture Enabled: yes Snaplen: 0 Username: test1 Stage clientless-vpn-client: file client.pcap Captured: packets - 3558 bytes - 11366322 Maximum: packets - 0 bytes - 0 Stage clientless-vpn-server: file server.pcap Captured: packets - 1779 bytes - 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 number on remote host + source-ip Set source address to specified interface address * from from * to Destination (username@host:path) **scp export filter-pcap from *<source-file>*** to <serveur-scpr> Destination (username@host:path)

Table 7: 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

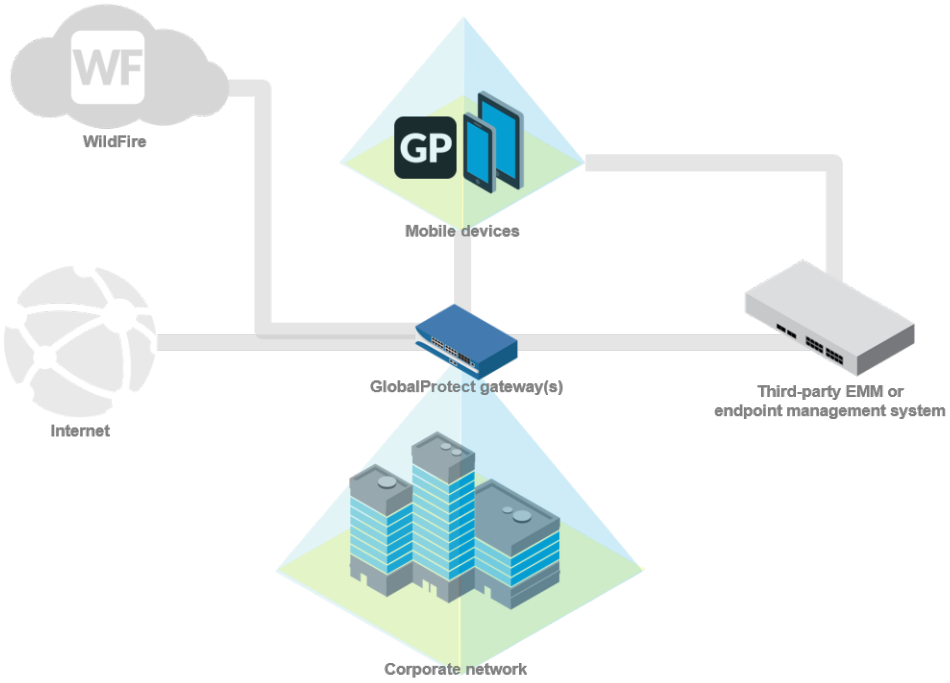
Statistiques	Description
setup_connection_r	Installation de la session homologue sur le serveur d'applications. Cette valeur doit correspondre aux valeurs de **`initiate_connection`** et **`setup_connection`**.
setup_connection_duplicate_r	Sessions en double déjà dans le proxy
setup_connection_failure_r	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.

Gestion des périphériques mobiles

- Aperçu de la gestion des périphériques mobiles
- Paramétrer l'intégration MDM avec GlobalProtect

Aperçu de la gestion des périphériques mobiles

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.



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

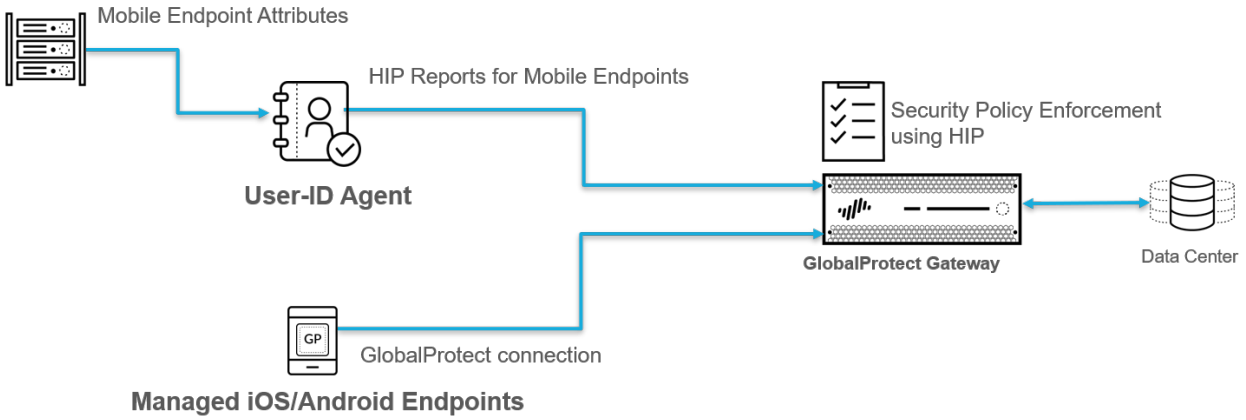
Vous pouvez intégrer votre déploiement MDM avec un système MDM ou EMM à l'aide de l'une des méthodes suivantes :

Intégration du pare-feu avec un système MDM ou EMM (AirWatch uniquement)

Vous pouvez configurer l'agent Windows User-ID pour qu'il communique avec le serveur MDM d'AirWatch pour collecter des informations sur l'hôte auprès des points de terminaison 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.

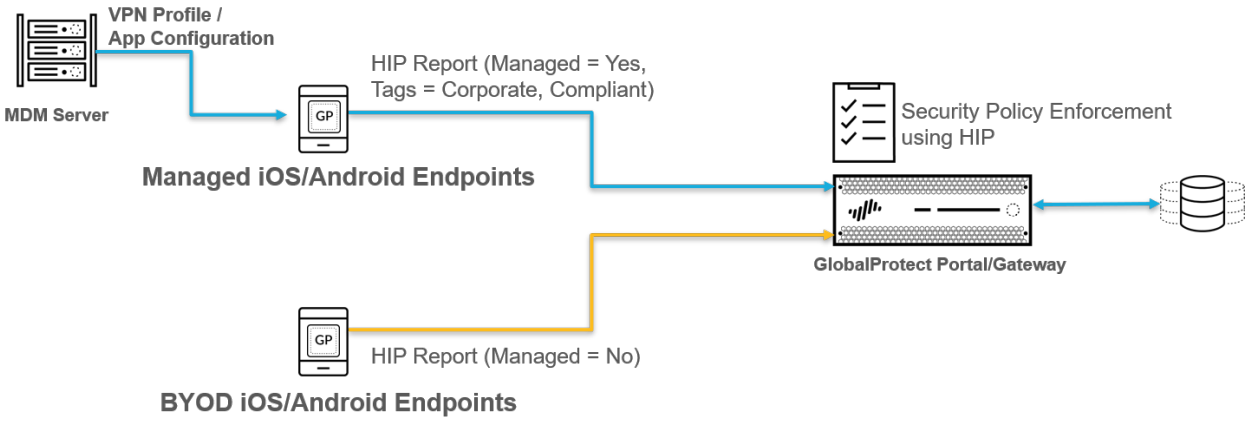
L'intégration du pare-feu est prise en charge par la version 8.0 de PAN-OS ou toute version ultérieure.

L'intégration du pare-feu est prise en charge uniquement avec VMware AirWatch.



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.



L'intégration de l'application GlobalProtect est possible avec VMware AirWatch, 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.
`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

Pour configurer l'intégration MDM avec GlobalProtect, utilisez le workflow suivant :

STEP 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 À propos de l'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.

STEP 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).

STEP 3 | Obtenez l'application GlobalProtect pour les points de terminaison mobiles.

- App Store - Télécharger et installer l'application mobile GlobalProtect
- Support des systèmes de gestion des périphériques mobiles - Déployez l'application mobile GlobalProtect
- 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.

STEP 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 :
  - Gestion de l'application GlobalProtect avec un MDM indépendant tiers qualifié
  - Gérer l'application GlobalProtect à l'aide d'autres MDM tiers

STEP 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 points de terminaison gérés.

Gestion de l'application GlobalProtect avec un MDM indépendant tiers qualifié

Reportez-vous aux sections suivantes pour obtenir des renseignements sur le déploiement, la configuration et la gestion de l'application GlobalProtect pour des points de terminaison mobiles au moyen d'un système MDM de tiers qualifiés :

- Fournisseurs MDM qualifiés
- Déployez l'application mobile GlobalProtect
- Configurations de VPN toujours actives
- Configurations de VPN d'accès à distance initié par l'utilisateur
- Configurations de VPN par application
- Activer l'intégration de l'analyse d'application avec WildFire
- Supprimer les notifications sur l'application GlobalProtect pour les terminaux macOS

Si vous n'utilisez pas de système MDM de tiers qualifié, vous pouvez Gérer l'application GlobalProtect à l'aide d'autres MDM tiers.

Fournisseurs MDM qualifiés

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'a 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
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	✓	✓	–	–	–	–	–

Fournisseur MDM pris en charge	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
	(Configuration de VPN toujours active)						
Console Google Admin	✓ (Pour la prise en charge de l'application Android sur les Chromebook ; déploiement d'application uniquement)	–	✓ (déploiement 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.						

Déployez l'application mobile 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 connectera 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 périphérique mobile est automatiquement soumis à la mise en œuvre de la même politique de sécurité que les autres points de terminaison sur votre réseau d'entreprise. L'application GlobalProtect 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 : Installez l'application directement à partir de l'App Store sur votre point de terminaison (voir Télécharger et installer l'Application Mobile GlobalProtect) ; ou déployez l'application à partir d'un système de gestion de périphériques mobiles (tel que AirWatch) et transmettez de manière transparente l'application à vos points de terminaison gérés.

- Déployez l'application mobile GlobalProtect à l'aide d'AirWatch
- Déployez l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide d'AirWatch
- 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

Déployez l'application mobile GlobalProtect à l'aide d'AirWatch

Vous pouvez déployer l'app GlobalProtect vers des points de terminaison gérés qui sont inscrits à AIRWATCH. Les points de terminaison exécutant iOS ou Android doivent télécharger l'agent AirWatch pour s'enregistrer au MDM AirWatch. Les points de terminaison Windows 10 ne nécessitent pas l'agent AIRWATCH, mais vous obligent à configurer l'inscription sur le point de terminaison. 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 Chromebook gérés, vous pouvez Déployez l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide d'AirWatch.

STEP 1 | Avant de commencer, assurez-vous que les points de terminaison auxquels vous souhaitez déployer l'app GlobalProtect sont inscrits à AIRWATCH :

- **Android et iOS** — téléchargez l'agent AirWatch et suivez les invites pour vous inscrire.
- **Windows Phone et Windows 10 UWP** — configurez le point de terminaison UWP de Windows 10 pour s'inscrire à AIRWATCH (à partir du point de terminaison, sélectionnez **Settings (Paramètres)** > **Accounts (Comptes)** > **Work access (Accès au travail)** > **Connect (Connexion)**).

STEP 2 | Depuis AirWatch, sélectionnez **APPS & BOOKS (Applications & Livres)** > **Public (Public)** > **Add Application (Ajouter une application)**.

STEP 3 | Sélectionnez le groupe de l'entreprise qui gérera cette application.

STEP 4 | Sélectionnez la **Platform (Plateforme)** (**Apple iOS**, **Android** ou **Windows Phone**).

STEP 5 | 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://itunes.apple.com/us/app/globalprotect/id592489989?mt=8&uo=4
- **Android** — https://play.google.com/store/apps/details?id=com.paloaltonetworks.globalprotect
- **Windows Phone**—https://www.microsoft.com/en-us/p/globalprotect/9nblggh6bzl3

STEP 6 | Cliquez sur **Next (Suivant)**. Si vous avez cherché l'application dans l'App Store du point de terminaison, vous devez également **Select (Sélectionner)** l'application à partir d'une liste de résultats de recherche.

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.

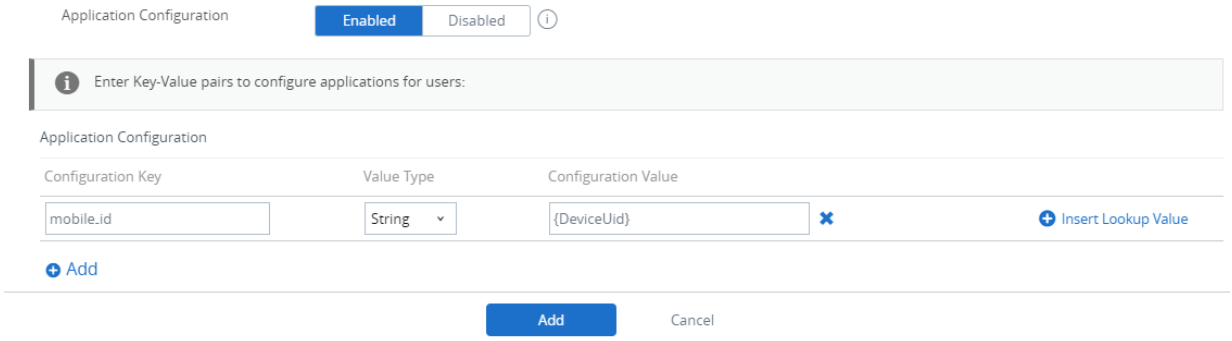
STEP 7 | À l'onglet **Assignment (Affectation)**, sélectionnez les **Assigned Smart Groups (Groupes intelligents affectés)** qui auront accès à cette application.

STEP 8 | 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)**.

STEP 9 | (Application GlobalProtect pour Android uniquement) **Enable (Activez)** la configuration de l'application pour qu'elle utilise l'UDID pour identifier le point de terminaison.

Ajoutez la paire clé-valeur suivante :

- Clé de configuration : **`mobile_id`**
- Type de valeur : **`String`**
- Valeur de configuration : **`{DeviceUid}`**



STEP 10 | Sélectionnez **Save & Publish (Enregistrer et publier)** pour insérer le Catalogue App dans les périphériques des groupes intelligents que vous avez affectés à la section **Assignment (Affectation)**.

Déployez l'application mobile GlobalProtect pour Android sur les Chromebooks gérés à l'aide d'AirWatch

À partir de la version 5.0 de l'application GlobalProtect, vous pouvez déployer l'application GlobalProtect pour Android sur les Chromebook gérés qui sont inscrits auprès de AirWatch. 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 Chromebook gérés à l'aide d'AirWatch :

STEP 1 | Configurez la console Google Admin.

La console Google Admin vous permet de gérer les services Google des utilisateurs de votre organisation. AirWatch utilise la console Google Admin pour l'intégration avec les Chromebook.

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 AirWatch.
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.

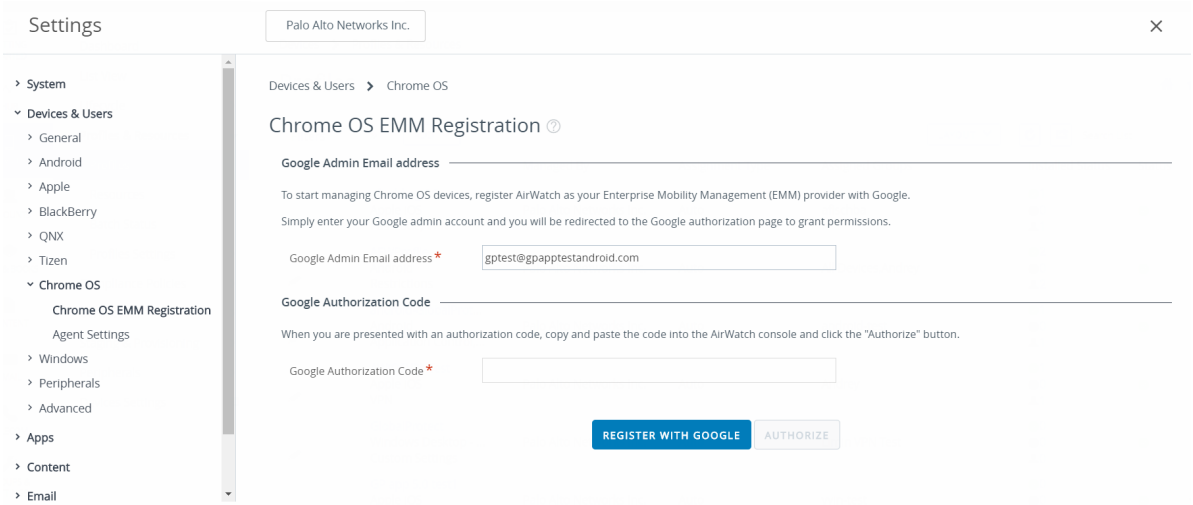
- https://www.googleapis.com/auth/chromedevicemanagementapi
- https://www.googleapis.com/auth/admin.directory.user
- https://www.googleapis.com/auth/admin.directory.device.chromeos

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 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)**).

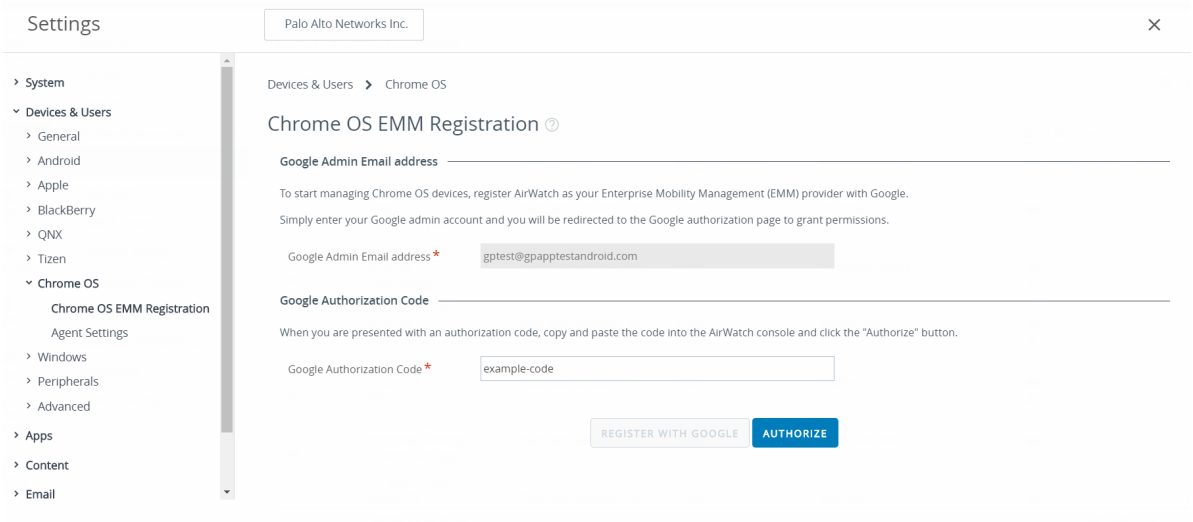
STEP 2 | Enregistrez AirWatch en tant que fournisseur Enterprise Mobility Management (Gestion de la mobilité d'entreprise ; EMM) pour Google.

Pour gérer les Chromebook à l'aide d'AirWatch, vous devez enregistrer AirWatch avec la console Google Admin.

1. Connectez-vous à votre console AirWatch.
2. Sélectionnez **Devices (Périphériques)** > **Devices Settings (Paramètres des périphériques)** > **Devices & Users (Périphériques et utilisateurs)** > **Chrome OS (Système d'exploitation 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.



STEP 3 | Inscrivez les Chromebooks auprès d'AirWatch.

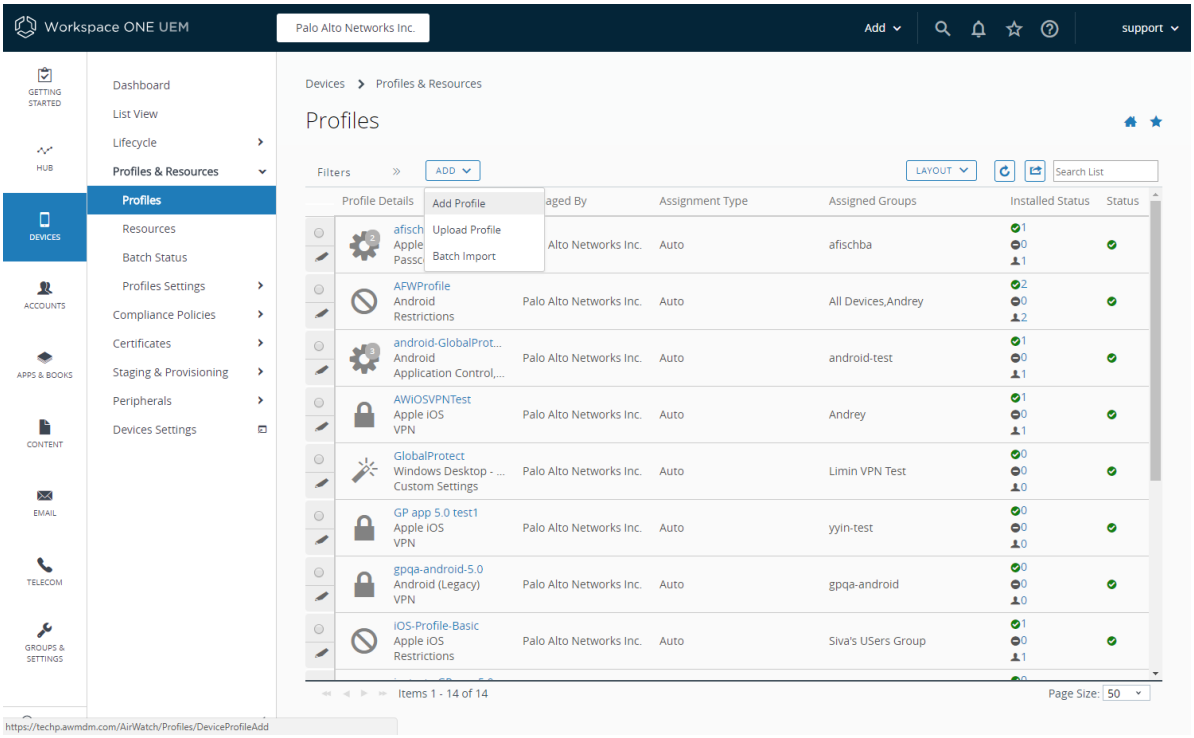
Avant de commencer à gérer vos Chromebook à l'aide d'AirWatch, vous devez inscrire vos Chromebook à AirWatch et les synchronisés.

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 AirWatch.
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 AirWatch.

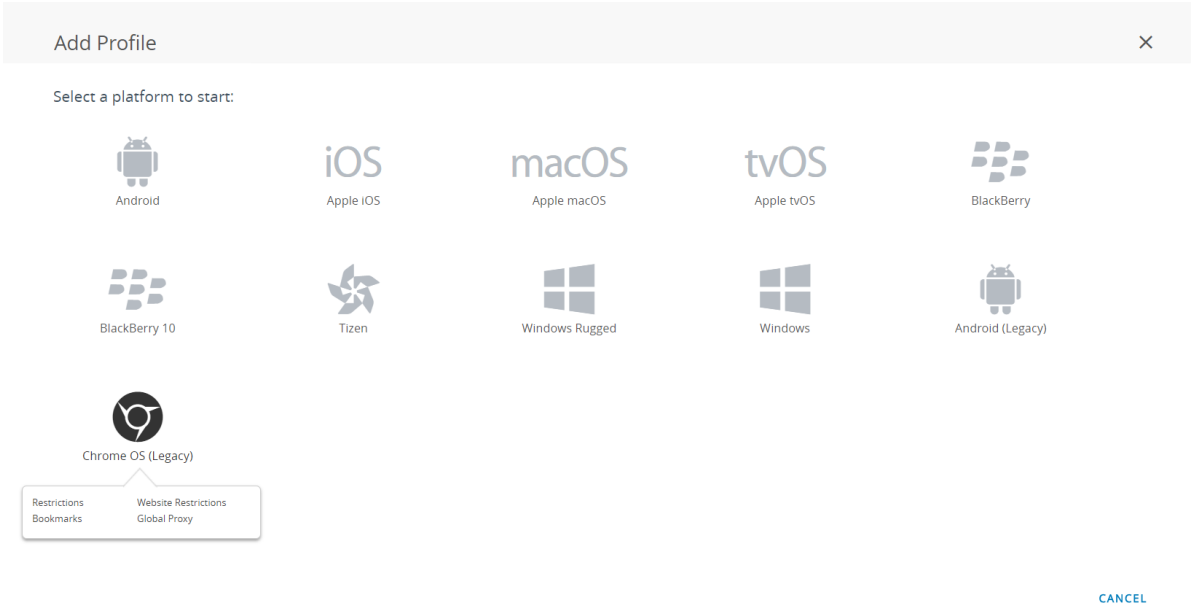
STEP 4 | Ajoutez l'application GlobalProtect pour Android à un profil Chrome OS sur AirWatch.

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.

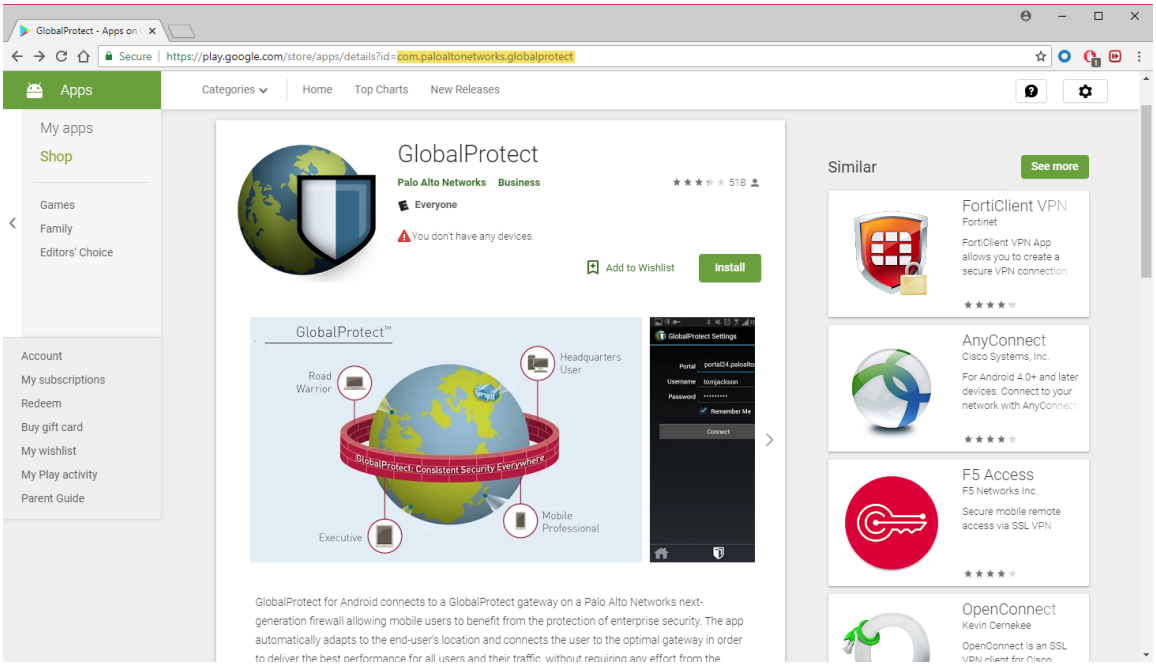
1. Connectez-vous à votre console AirWatch.
2. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)** pour**ADD (Ajouter)** un nouveau profil Chrome OS.



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)**.
    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.

Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune

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.

STEP 1 | Inscrire les points de terminaison 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.

STEP 2 | Ajouter 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.

STEP 3 | Définir 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.

STEP 4 | Affecter l'application GlobalProtect à des utilisateurs ou à des points de terminaison 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.

Déployez l'application mobile GlobalProtect à l'aide de MobileIron

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.

STEP 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.

STEP 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.

STEP 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.

STEP 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.

Déployer l'application GlobalProtect pour Android sur les Chromebooks gérés à l'aide 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. 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 :

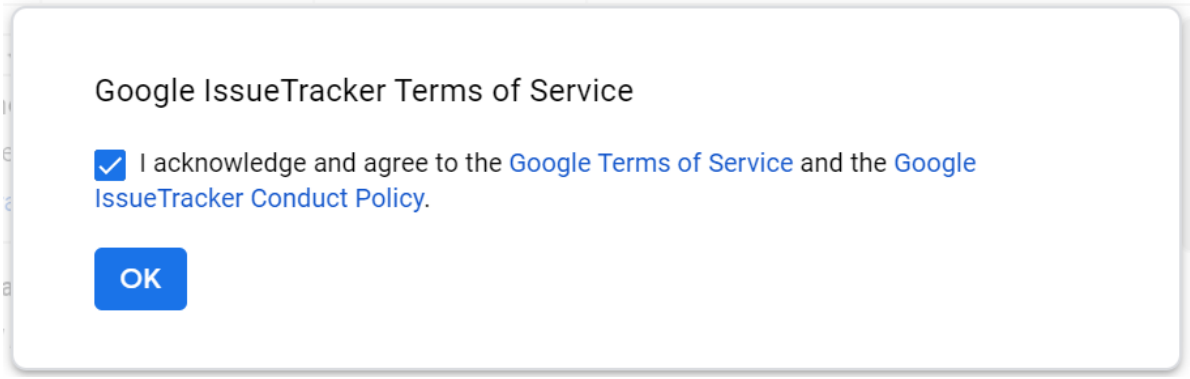
- *Vous ne pouvez transmettre aux appareils qui utilisent la console Google Admin un certificat unique à des fins d'authentification.*
- *À partir de votre Chromebook, appuyez sur CTRL+ALT+T pour ouvrir la ligne de commande du terminal. Utilisez la commande `route` pour afficher les itinéraires qui sont 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 :

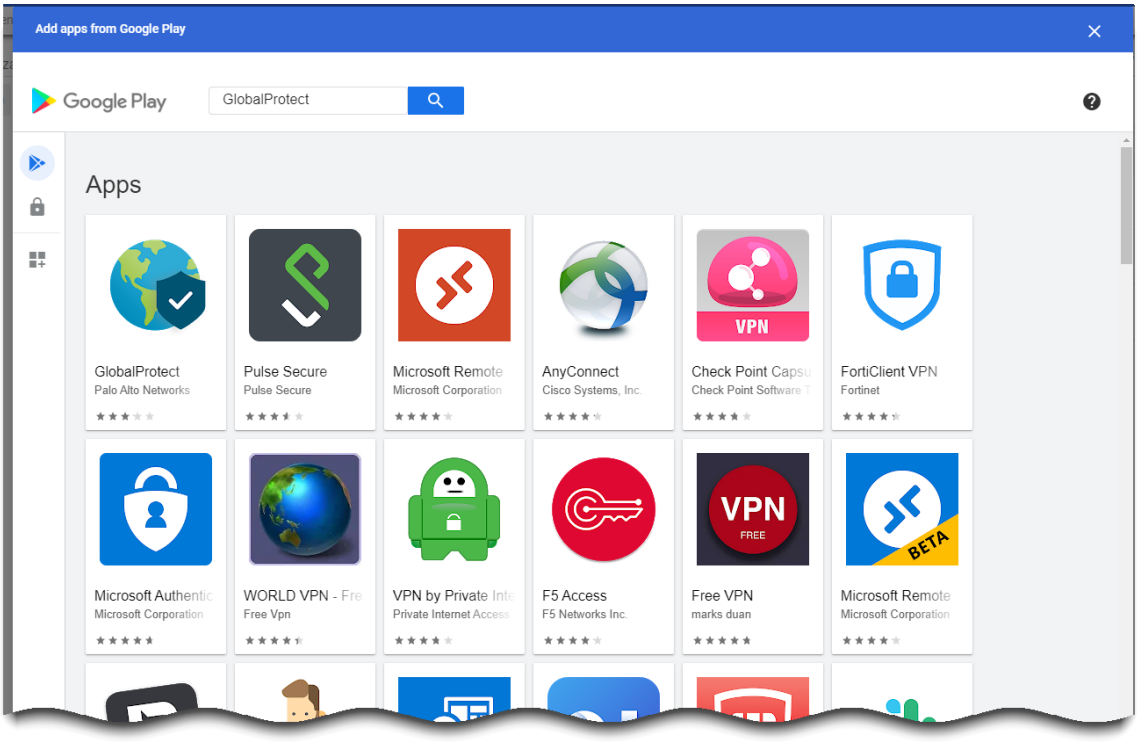
STEP 1 | Avant de commencer :

- 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 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 active. 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 :



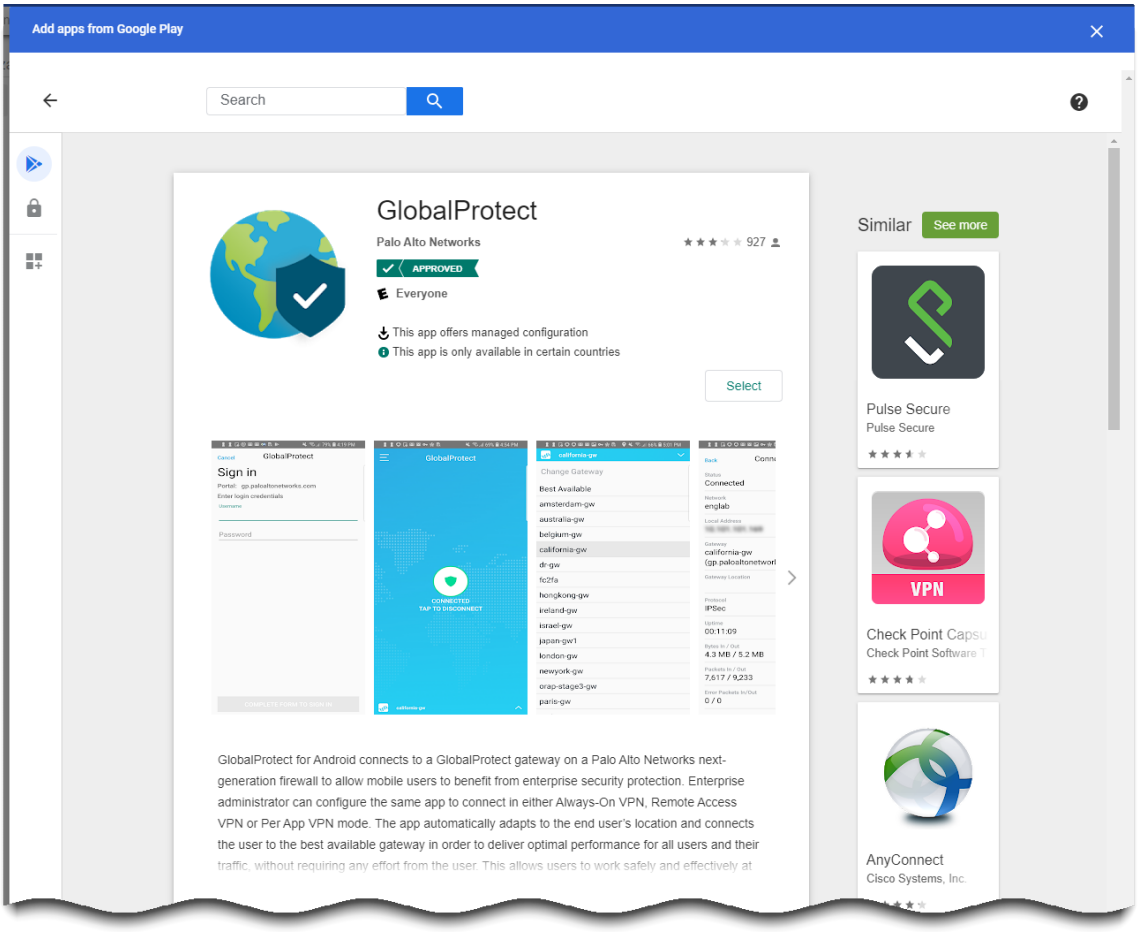
STEP 2 | Approuvez l'application GlobalProtect pour les utilisateurs Chromebook.

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.

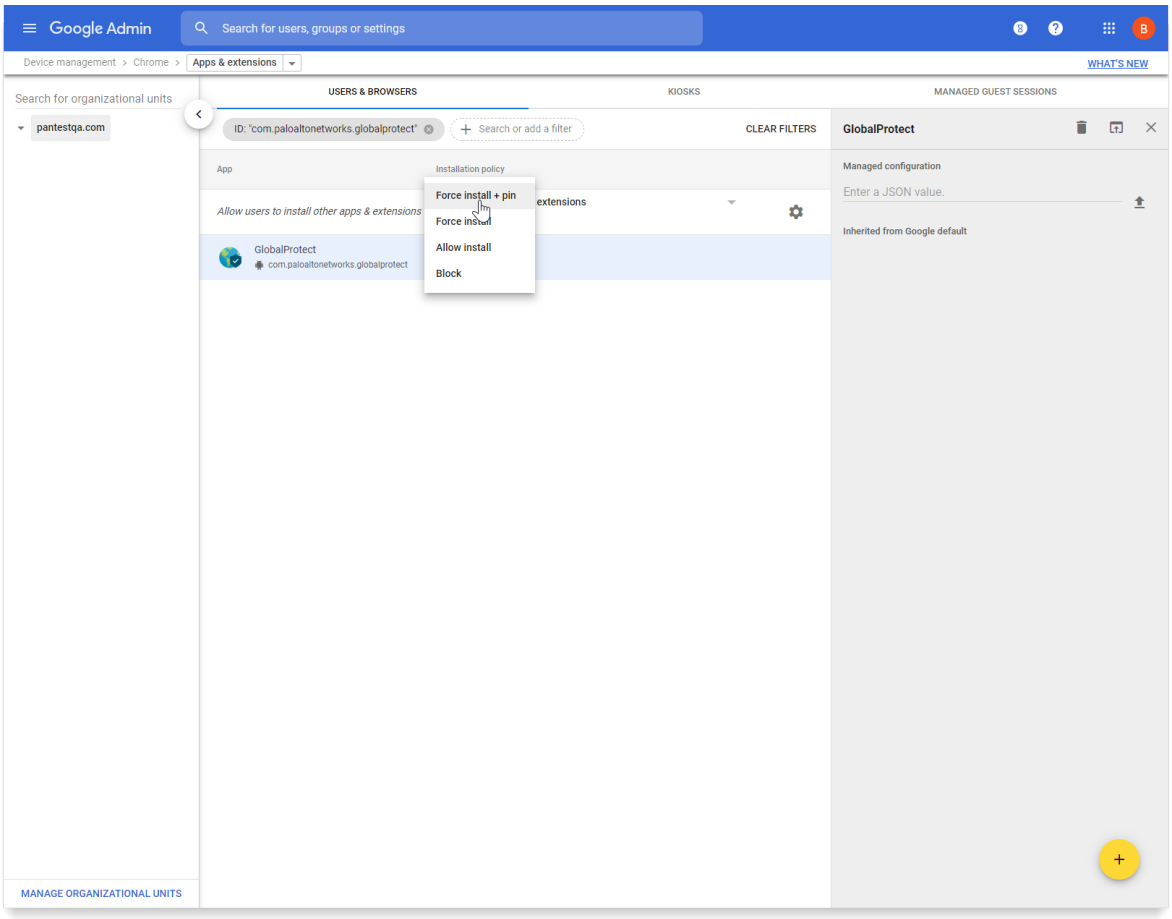


STEP 3 | Déterminez la façon dont l'application GlobalProtect est installée sur les Chromebook.

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 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.

STEP 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 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	Liste de blocage ou liste d'autorisation qui vous permet de contrôler le trafic d'application qui peut traverser le tunnel VPN dans une configuration de VPN par application.	Chaîne	`allow list| block list: com.google.calendar; com.android.email; com.android.chrome`
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`

Paramètre	Description	Type de valeur	Exemple
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`
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.

STEP 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.

Configurations de VPN toujours actives

Dans une configuration de VPN toujours active, la connexion GlobalProtect sécurisée est toujours active. L'application GlobalProtect 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 récupérer la configuration de l'agent. Après que l'application reçoit la configuration de l'agent du portail, elle se connecte automatiquement et établit un tunnel VPN à la passerelle GlobalProtect qui a été spécifiée dans la configuration de l'agent.

Reportez-vous aux sections suivantes pour obtenir des renseignements sur la manière de configurer une configuration de VPN toujours active à l'aide des systèmes de gestion des périphériques mobiles pris en charge :

- Configurer une configuration de VPN toujours active à l'aide d'AirWatch
- Configurer une configuration de VPN toujours active à l'aide de Microsoft Intune

- Configurer une configuration de VPN toujours active à l'aide de MobileIron
- Configuration d'une configuration de VPN toujours active à l'aide de la console Google Admin

Configurer une configuration de VPN toujours active à l'aide d'AirWatch

AirWatch 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 AirWatch 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 renseignements sur la manière de configurer une configuration de VPN toujours active à l'aide d'AirWatch :

- Configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide d'AirWatch
- Configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide d'AirWatch

Configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide d'AirWatch

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 d'AirWatch :

STEP 1 | Téléchargement de l'application GlobalProtect pour Android

- Déployez l'application mobile GlobalProtect à l'aide de AirWatch.
- Téléchargez l'app GlobalProtect directement à partir de l'App Store.

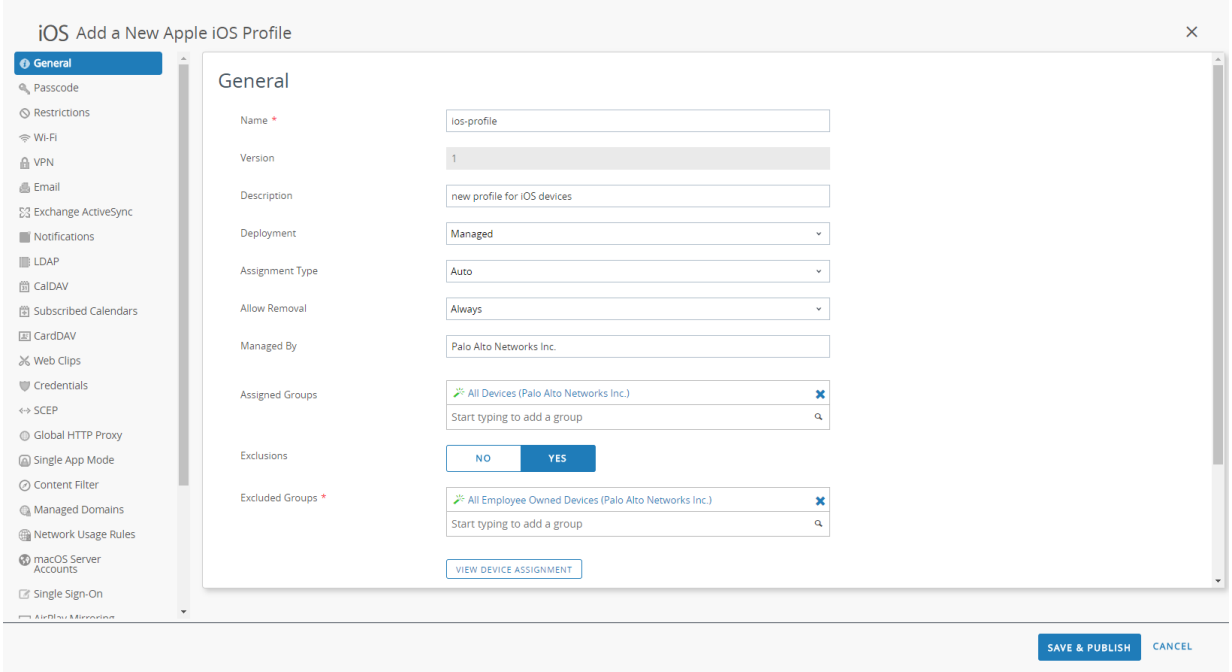
STEP 2 | Depuis la console AirWatch, modifiez un profil Apple iOS existant ou ajoutez-en un nouveau.

1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajoutez)** un nouveau profil.
2. Sélectionnez **iOS** à partir de la liste de la plateforme.

STEP 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, 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.

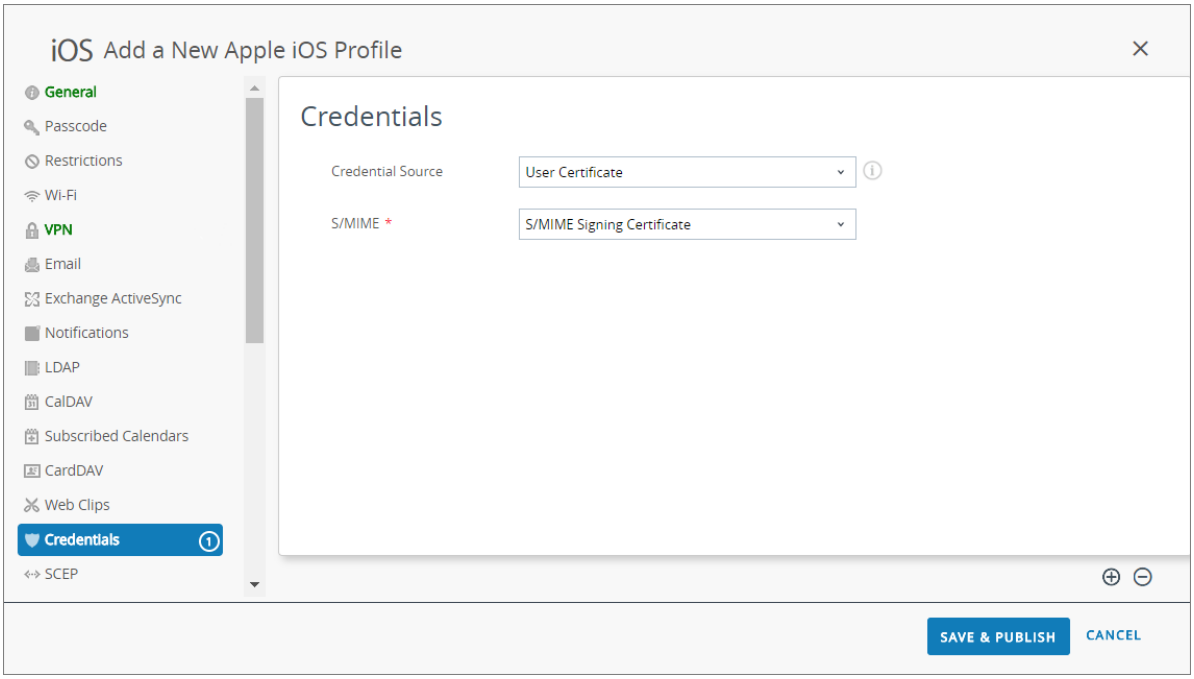


STEP 4 | (Facultatif) Si votre déploiement GlobalProtect exige une authentification du certificat du client, configurez les paramètres des **Credentials (Informations d'identification)** :

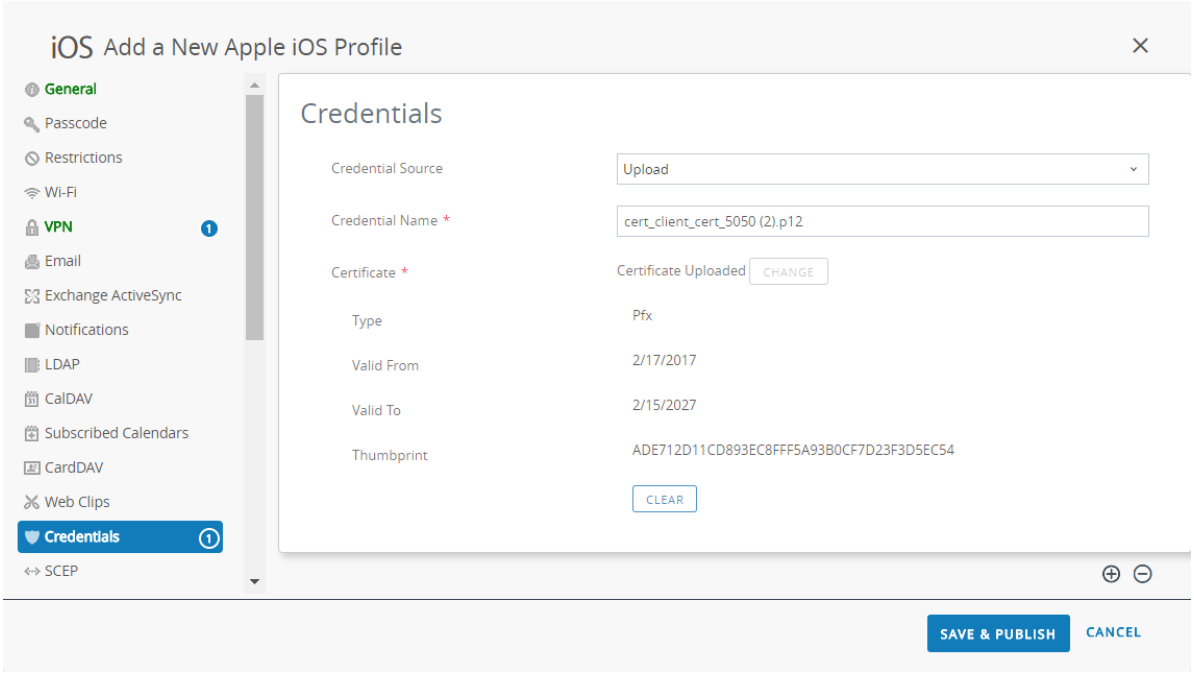
À partir de la version 12 d'iOS, si vous souhaitez utiliser les certificats de client pour procéder à l'authentification du client GlobalProtect, vous devez déployer les certificats de client dans le cadre du profil VPN qui est transmis du serveur MDM. Si vous déployez

des certificats de client à partir du serveur MDM au moyen d'une tout autre méthode, les certificats ne peuvent être utilisés par l'application GlobalProtect.

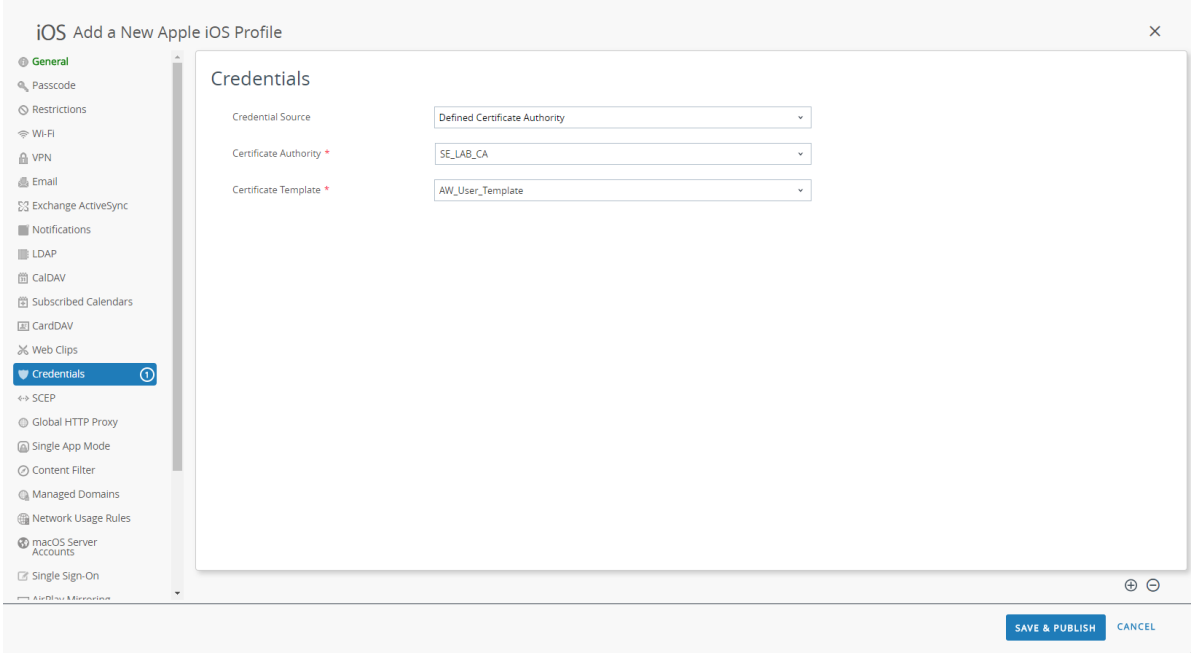
- Pour extraire les certificats de client des utilisateurs d'AirWatch :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).



- 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)**.



- 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.

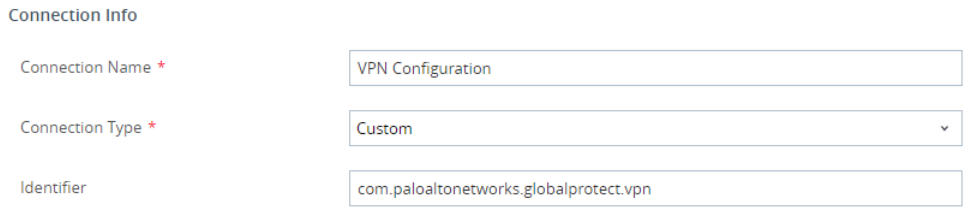


STEP 5 | Configurez les paramètres **VPN** :

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 suivant dans le champ **Identifiant** pour identifier l'application GlobalProtect : **`com.paloaltonetworks.globalprotect.vpn`**.

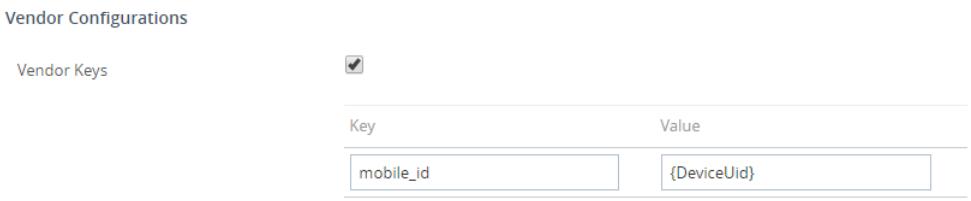


4. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
5. (Facultatif) Saisisissez le nom d'utilisateur du **Account (Compte)** VPN ou cliquez sur le bouton d'ajout (**+**) pour afficher les valeurs de recherche 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.

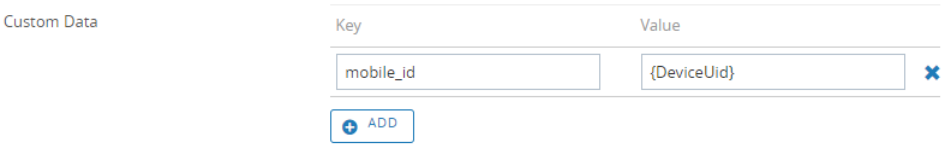
STEP 6 | (Facultatif) (à compter de la version 5.0 de l'application GlobalProtect) Si votre déploiement GlobalProtect exige une intégration HIP avec MDM, précisez l'attribut de Unique device identifier (UDID ; Identificateur de périphérique unique).

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}`**.



STEP 7 | **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

Configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide d'AirWatch

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 AIRWATCH ne répertorie pas encore GlobalProtect comme fournisseur de connexion officiel pour les points de terminaison 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.

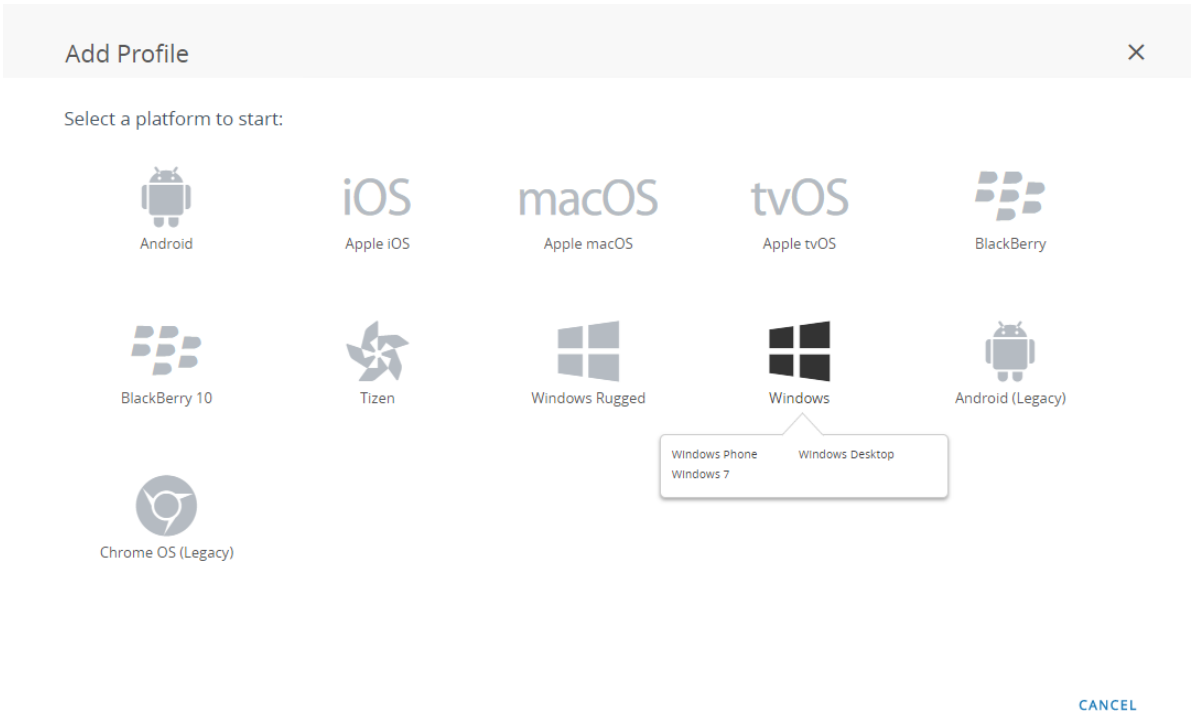
Utilisez les étapes suivantes pour configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide d'AirWatch :

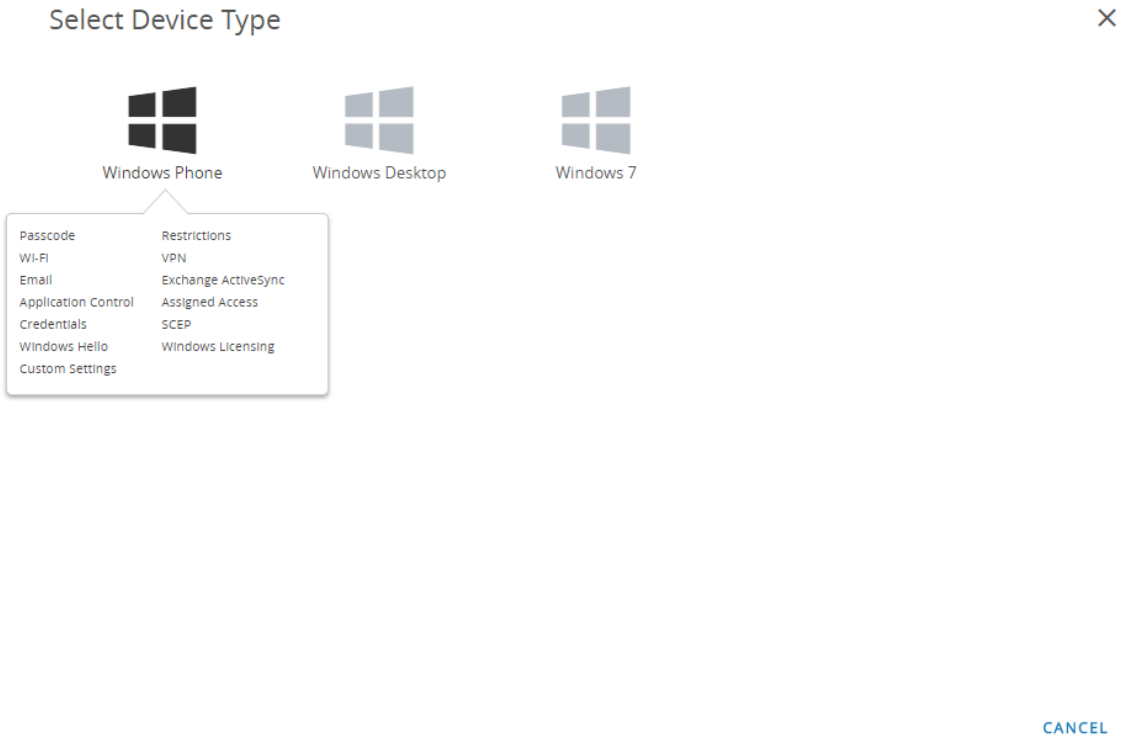
STEP 1 | Téléchargez l'app GlobalProtect pour Windows 10 UWP :

- Déployez l'application mobile GlobalProtect à l'aide de AirWatch.
- Téléchargez l'application GlobalProtect directement à partir du Microsoft Store.

STEP 2 | Depuis la console AirWatch, 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 (Ajoutez)** un nouveau profil.
2. Sélectionnez **Windows** comme plateforme et **Windows Phone** comme type de configuration.

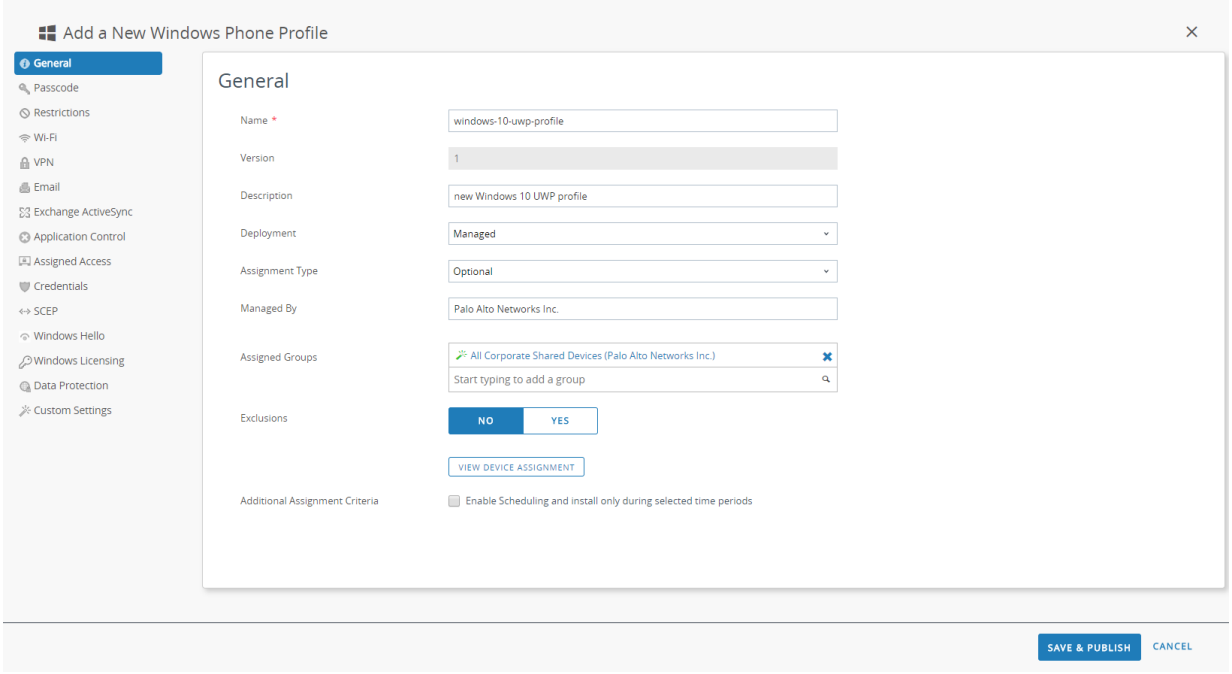




STEP 3 | Configurez les paramètres **General (généraux)**.

1. Saisissez un **Name (Nom)** pour le profil.
2. (Facultatif) Saisissez une brève **description** du profil qui indique son but.

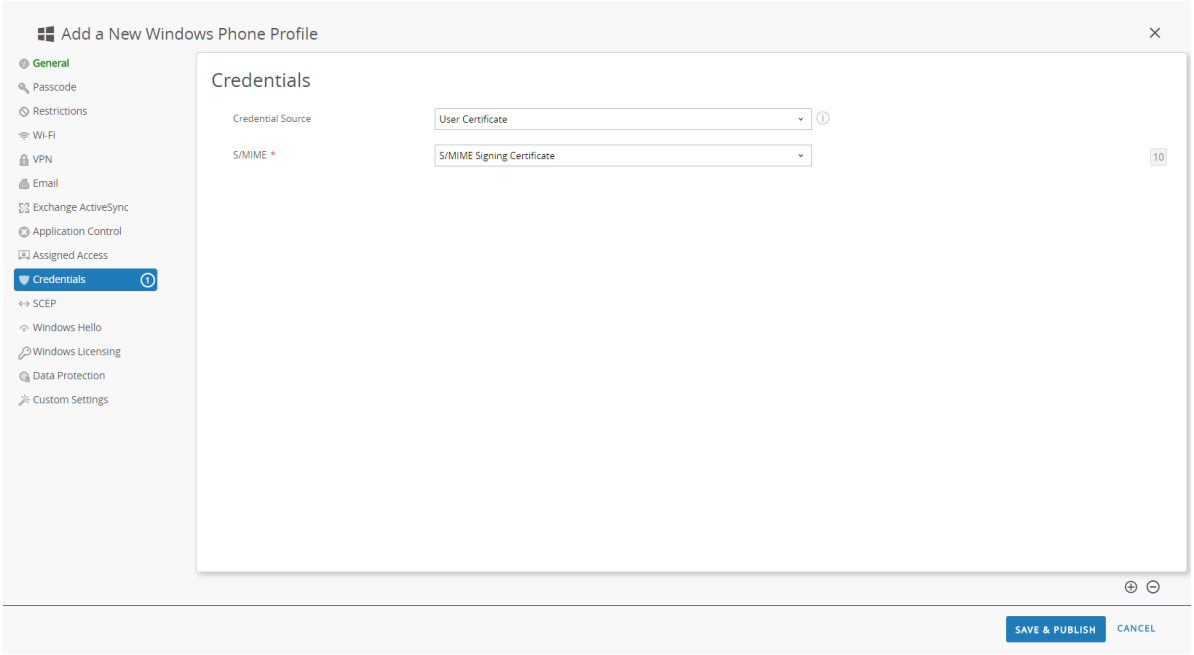
3. (Facultatif) Définissez le mode de **Deployment (Déploiement)** sur **Managed (Géré)** pour permettre la suppression automatique du profil lors de la désinscription.
4. (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les 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 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)**.



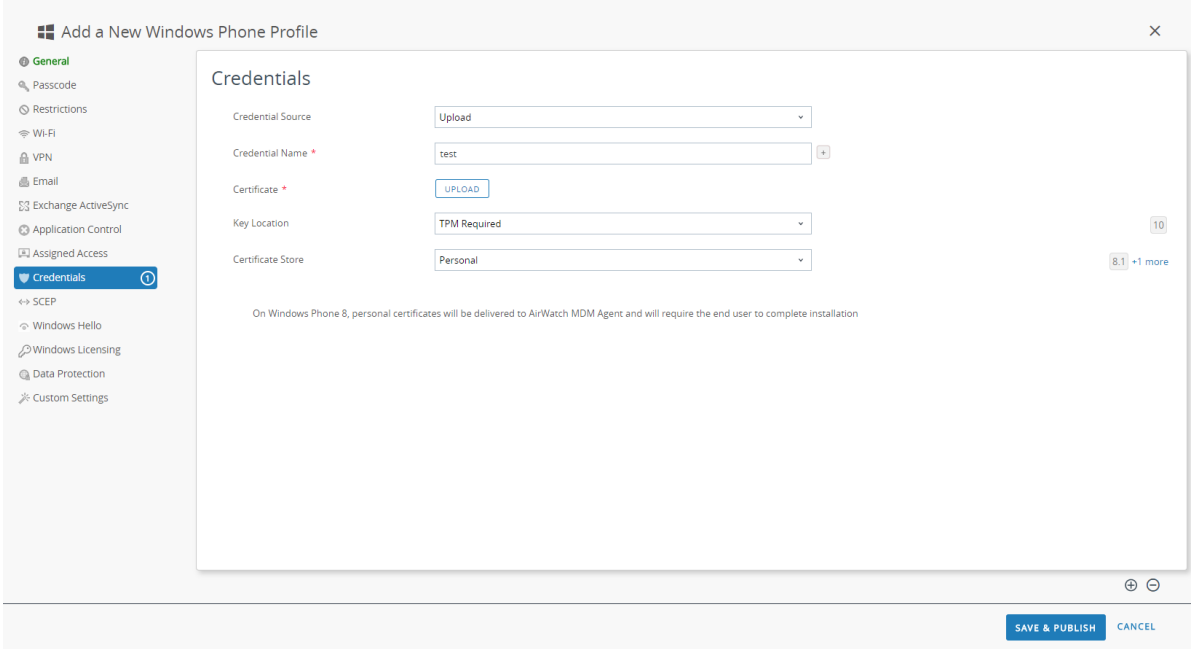
STEP 4 | (Facultatif) Si votre déploiement GlobalProtect exige une authentification du certificat du client, configurez les paramètres des **Credentials (Informations d'identification)** :

- Pour extraire les certificats de client des utilisateurs d'AirWatch :

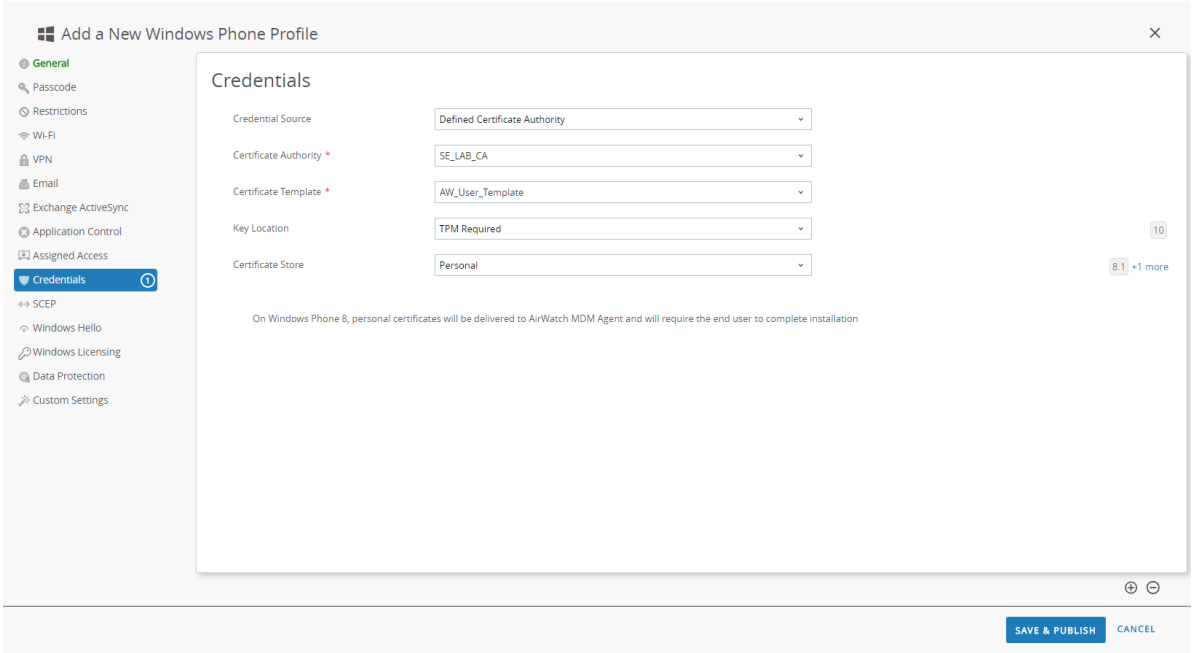
1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).



- 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 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, l'agent AirWatch Protection doit être installé sur le point de terminaison.
  6. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.



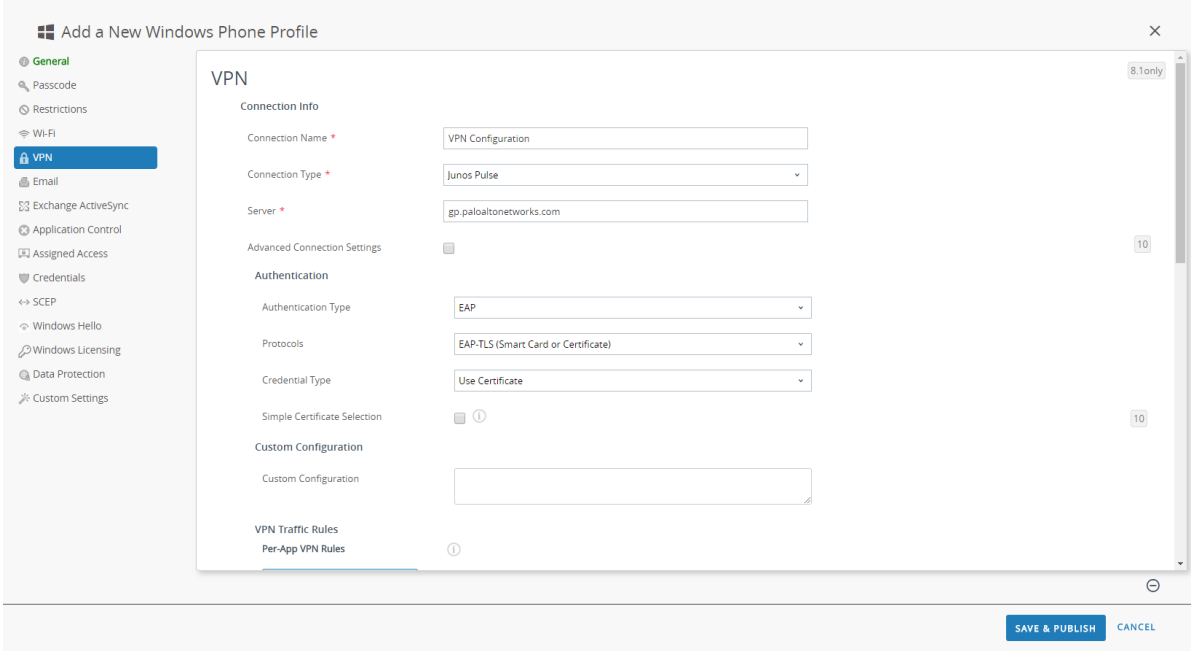
- Pour utiliser une autorité de certification et un modèle prédéfinis :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
  2. Sélectionnez la **Certificate Authority (Autorité de certification)** 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 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, l'agent AirWatch Protection doit être installé sur le point de terminaison.
  5. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.



STEP 5 | Configurez les paramètres **VPN** :

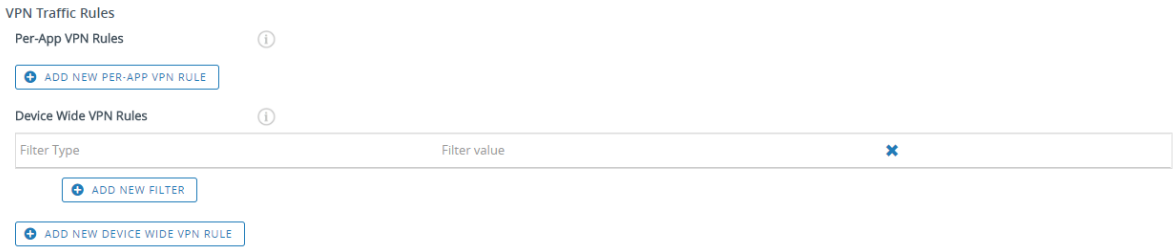
1. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
2. Sélectionnez un autre fournisseur de **Connection Type (Type de connexion)** (ne sélectionnez pas **IKEv2**, **L2TP**, **PPTP** ou **Automatic (Automatique)**, car ceux-ci n'ont pas les paramètres de fournisseur associés requis pour le profil VPN GlobalProtect).

   Vous devez sélectionner un fournisseur de rechange, car AirWatch ne répertorie pas encore GlobalProtect en tant que fournisseur de connexions officiel pour les points de terminaison 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.

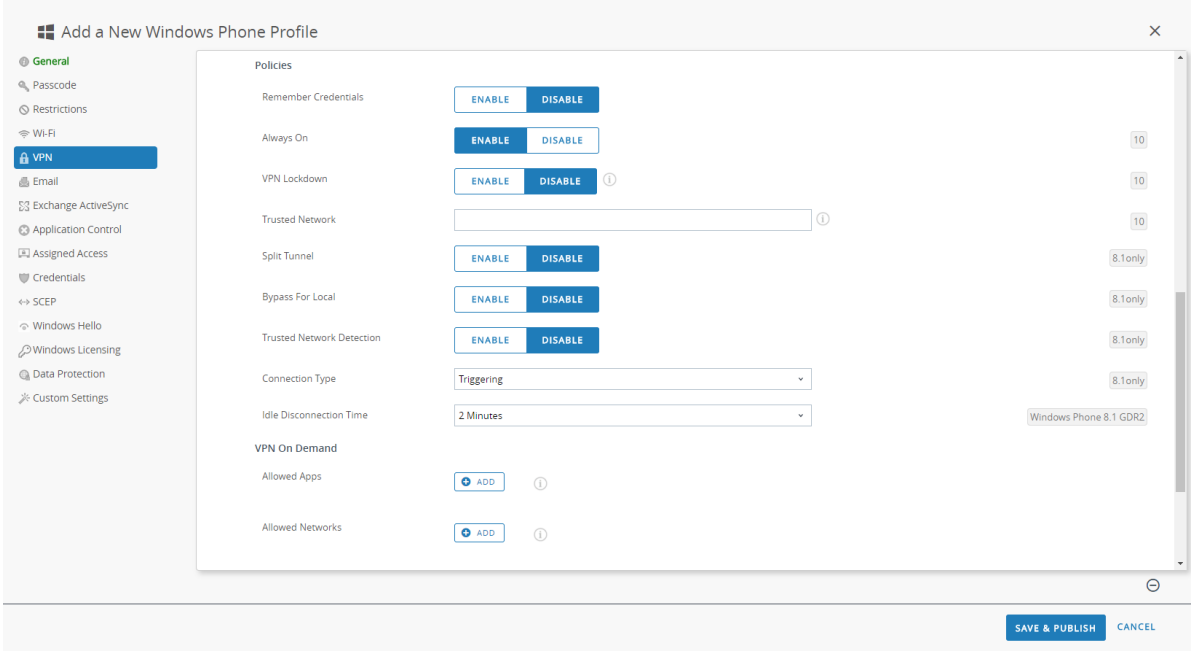


5. (Facultatif) Pour permettre à GlobalProtect d'enregistrer les informations d'identification de l'utilisateur, **ENABLE (ACTIVEZ)** l'option permettant de **Remember Credentials (Mémoriser les informations)** d'identification dans la zone de stratégies.
6. (Facultatif) Dans la section VPN Traffic Rules (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 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 AIRWATCH 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.

STEP 6 | **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

STEP 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. AIRWATCH 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. Retour à AirWatch et, dans la **Devices(Périphériques)** > **Profiles (Profils)** > **List View (Vue de la 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.

STEP 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)**. AIRWATCH déplace le profil sur la liste inactive.

STEP 9 | Testez la configuration.

Configurer une configuration de VPN toujours active à l'aide de Microsoft Intune

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 offre une connexion sécurisée entre le pare-feu et les points de terminaison mobiles gérés par Microsoft Intune 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 renseignements sur la manière de configurer une configuration de VPN toujours active à l'aide de Microsoft Intune :

- Configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide de Microsoft Intune
- Configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide de Microsoft Intune

Configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide de Microsoft Intune

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 Microsoft Intune :

STEP 1 | Téléchargement de l'application GlobalProtect pour Android

- Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune.
- Téléchargez l'app GlobalProtect directement à partir de l'App Store.

STEP 2 | (Facultatif) Si votre déploiement exige une authentification basée sur les certificats, configurez un profil de certificat.

STEP 3 | Créez un nouveau profil VPN iOS.

- Définissez la **Platform (Plateforme)** sur **iOS**.

STEP 4 | Configurez les paramètres de la configuration VPN toujours active pour les points de terminaison iOS.

- Définissez le **Connection type (Type de connexion)** sur **Palo Alto Networks GlobalProtect**.

Configurer une configuration de VPN toujours active sur les terminaux UWP Windows 10 à l'aide de Microsoft Intune

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 :

STEP 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.

STEP 2 | (Facultatif) Si votre déploiement exige une authentification basée sur les certificats, configurez un profil de certificat.

STEP 3 | Créez un nouveau profil VPN Windows 10 UWP .

- Définissez la **Platform (Plateforme)** sur **Windows 10 and later (Windows 10 et versions ultérieures)**.

STEP 4 | Configurez les paramètres de la configuration VPN toujours active pour les points de terminaison 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 toujours active à l'aide de MobileIron

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.

Reportez-vous aux sections suivantes pour obtenir des renseignements sur la manière de configurer une configuration de VPN toujours active à l'aide de MobileIron :

- Configurer une configuration de VPN toujours active sur les terminaux iOS à l'aide de MobileIron
- 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 iOS à l'aide de MobileIron

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 :

STEP 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.

STEP 2 | (Facultatif) Si votre déploiement nécessite une authentification basée sur les certificats, ajoutez une configuration de certificat, puis configurez les paramètres du certificat.

STEP 3 | Ajoutez une configuration de VPN toujours active.

- Définissez le type de configuration sur **Always On VPN (Configuration VPN toujours active)**.

STEP 4 | Configurez les paramètres de la configuration VPN toujours active pour iOS.

Configurer une configuration de VPN toujours active sur les terminaux Android à l'aide de MobileIron

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 :

STEP 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.

STEP 2 | (Facultatif) Si votre déploiement nécessite une authentification basée sur les certificats, ajoutez une configuration de certificat, puis configurez les paramètres du certificat.

STEP 3 | Ajoutez une configuration de VPN toujours active.

- Définissez le type de configuration sur **Always On VPN (Configuration VPN toujours active)**.

STEP 4 | Configurez les paramètres de la configuration VPN toujours active pour Android.

Configuration d'une configuration de VPN toujours active à l'aide de la console Google Admin

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.

Configuration d'une configuration de VPN toujours active pour les Chromebook à l'aide de la console Google Admin

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.

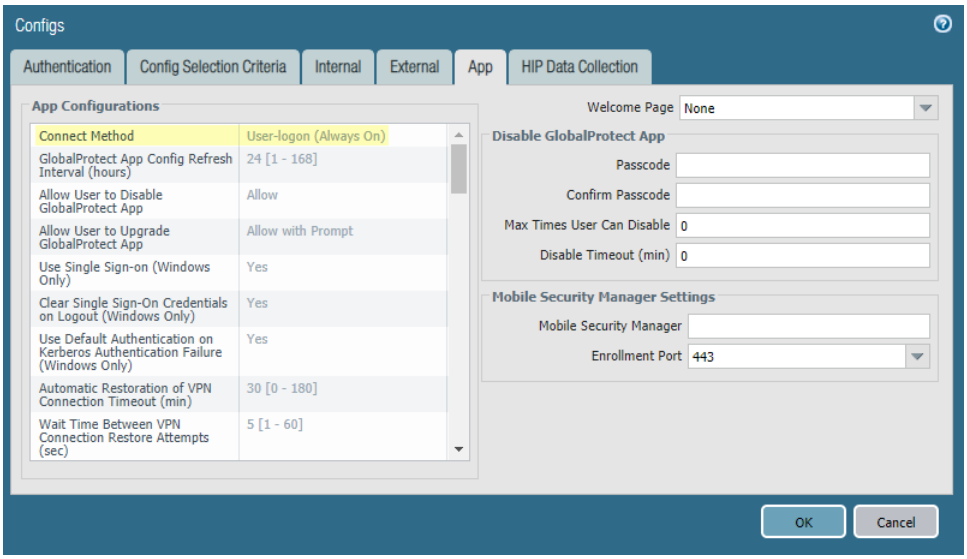
Suivez les étapes suivantes pour déployer l'application GlobalProtect pour Android sur les Chromebook gérés à l'aide de la console Google Admin. À l'heure actuelle, AirWatch ne prend pas en charge les configurations VPN toujours actif pour l'application GlobalProtect pour Android sur des Chromebook gérés.

STEP 1 | À partir de votre pare-feu Palo Alto Networks, Paramétrer l'accès au portail GlobalProtect.

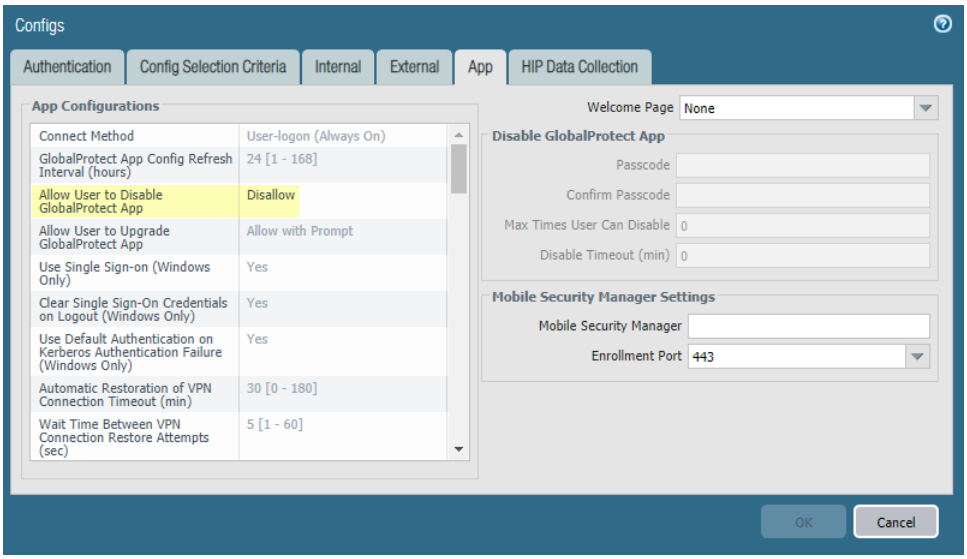
STEP 2 | Définir les configurations de l'agent GlobalProtect.

STEP 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)**.

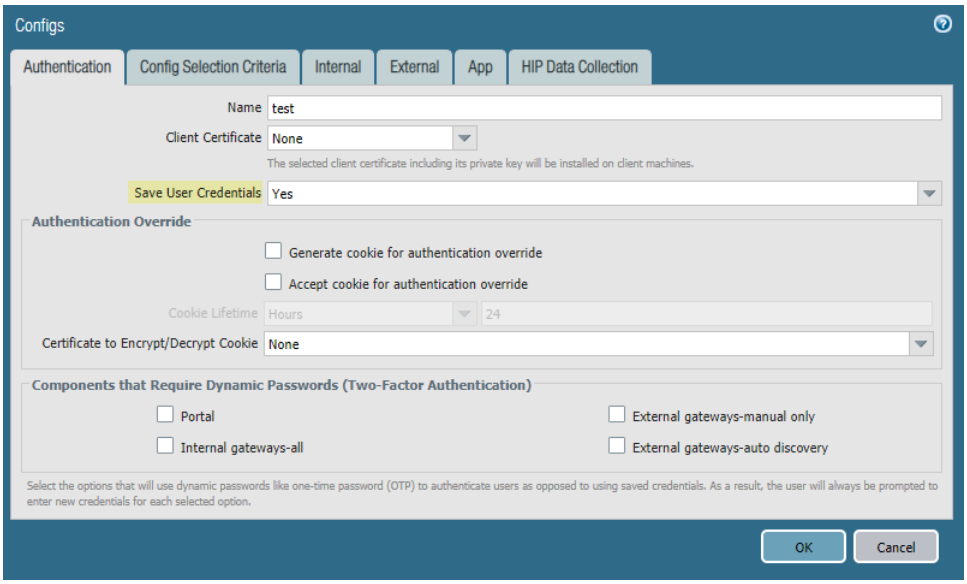


STEP 4 | Activez l'authentification transparente pour GlobalProtect.

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> (<configuration du portail>)* > **Agent** > *<agent-config> (<configuration de l'agent>)*), sélectionnez **Authentication (Authentification)**.
2. Définissez l'option **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)** sur **Yes (Oui)**.

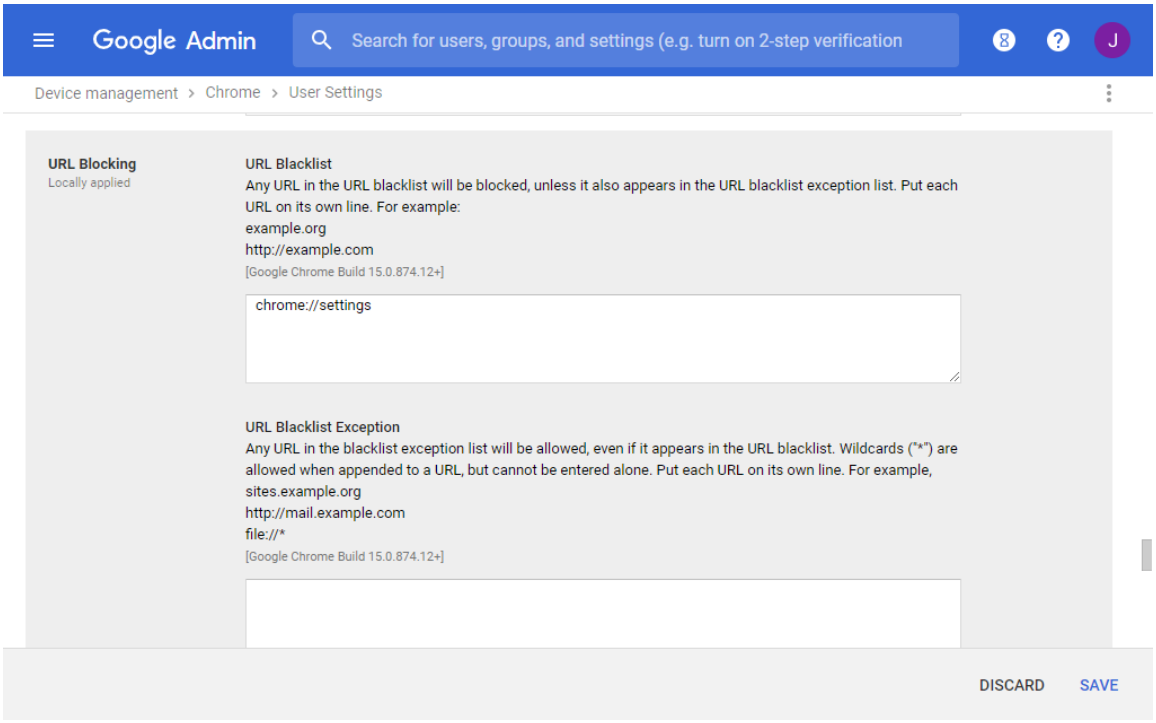


3. Cliquez deux fois sur **OK** pour enregistrer la configuration de l'agent du portail.

STEP 5 | Cliquez sur **Commit (Valider)** pour valider les modifications que vous avez apportées au pare-feu.

STEP 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 noire (**`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 Blacklist (Liste noire des URL)**.



4. **SAVE (Sauvegardez)** vos modifications.

Configurations de VPN d'accès à distance initié par l'utilisateur

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. L'application GlobalProtect 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 récupérer la configuration de l'agent. Après que l'application reçoit la configuration de l'agent du portail, elle se connecte et établit un tunnel VPN à la passerelle GlobalProtect qui a été spécifiée dans la configuration de l'agent.

Reportez-vous aux sections suivantes pour obtenir des renseignements sur la manière de configurer une configuration de VPN d'accès à distance initié par l'utilisateur à l'aide des systèmes de gestion des périphériques mobiles pris en charge :

- Configurer une configuration de VPN d'accès à distance initié par l'utilisateur à l'aide d'AirWatch
- Configurer une configuration de VPN d'accès à distance initié par l'utilisateur à l'aide de Microsoft Intune
- Configurer une configuration de VPN d'accès à distance initié par l'utilisateur à l'aide de MobileIron

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur à l'aide d'AirWatch

AirWatch 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 les points de terminaison mobiles gérés par AirWatch et le pare-feu 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 renseignements sur la manière de configurer une configuration de VPN à accès à distance initié par l'utilisateur à l'aide d'AirWatch :

- Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison iOS à l'aide d'AirWatch

- Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison Windows 10 UWP à l'aide d'AirWatch

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison iOS à l'aide d'AirWatch

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 d'AirWatch :

STEP 1 | Téléchargement de l'application GlobalProtect pour Android

- Déployez l'application mobile GlobalProtect à l'aide de AirWatch.
- Téléchargez l'app GlobalProtect directement à partir de l'App Store.

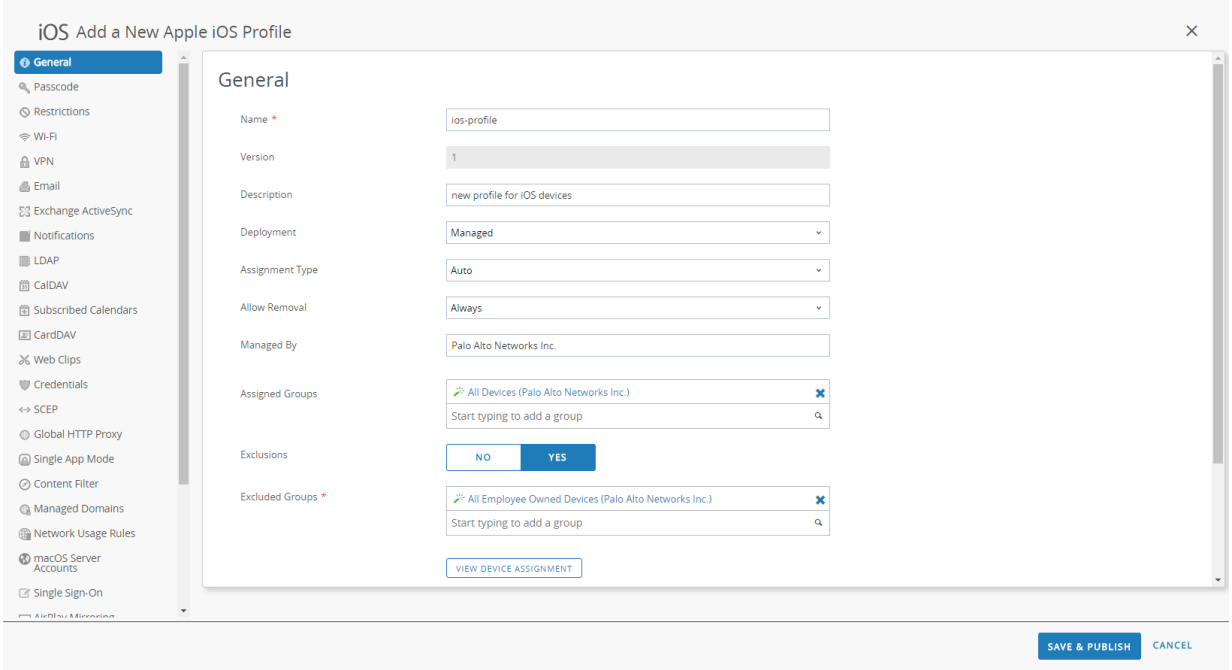
STEP 2 | Depuis la console AirWatch, modifiez un profil Apple iOS existant ou ajoutez-en un nouveau.

1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajoutez)** un nouveau profil.
2. Sélectionnez **iOS** à partir de la liste de la plateforme.

STEP 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, 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.

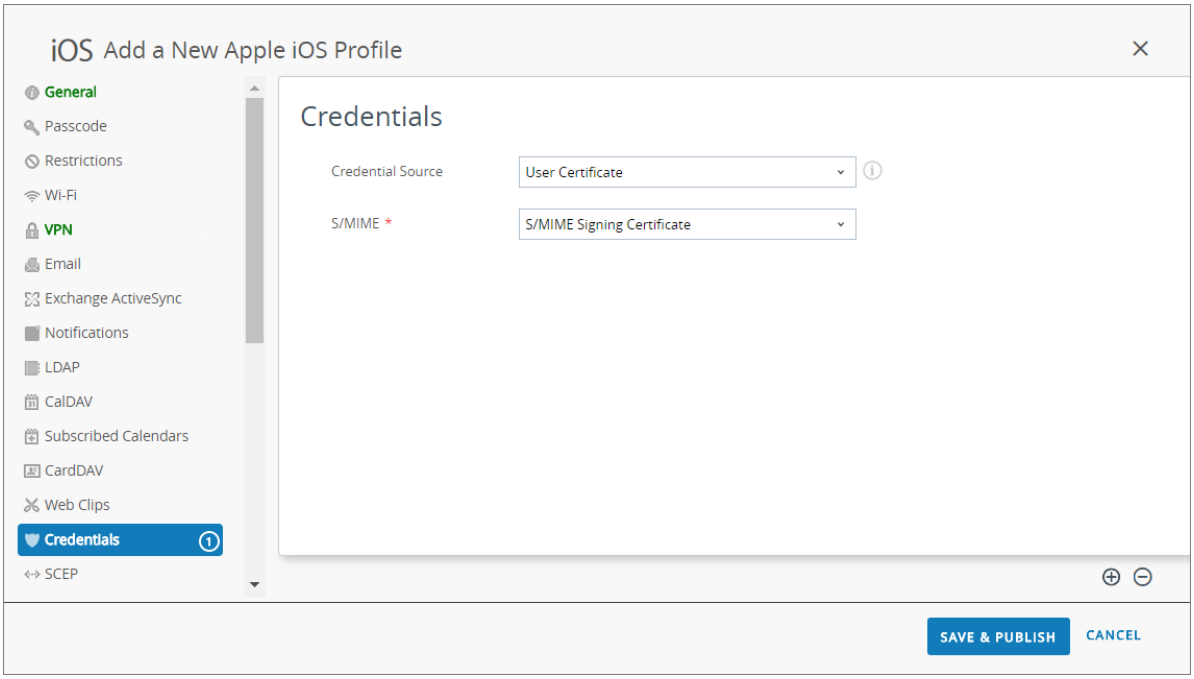


STEP 4 | Configurez les paramètres de **Credentials (Informations d'identification)** :

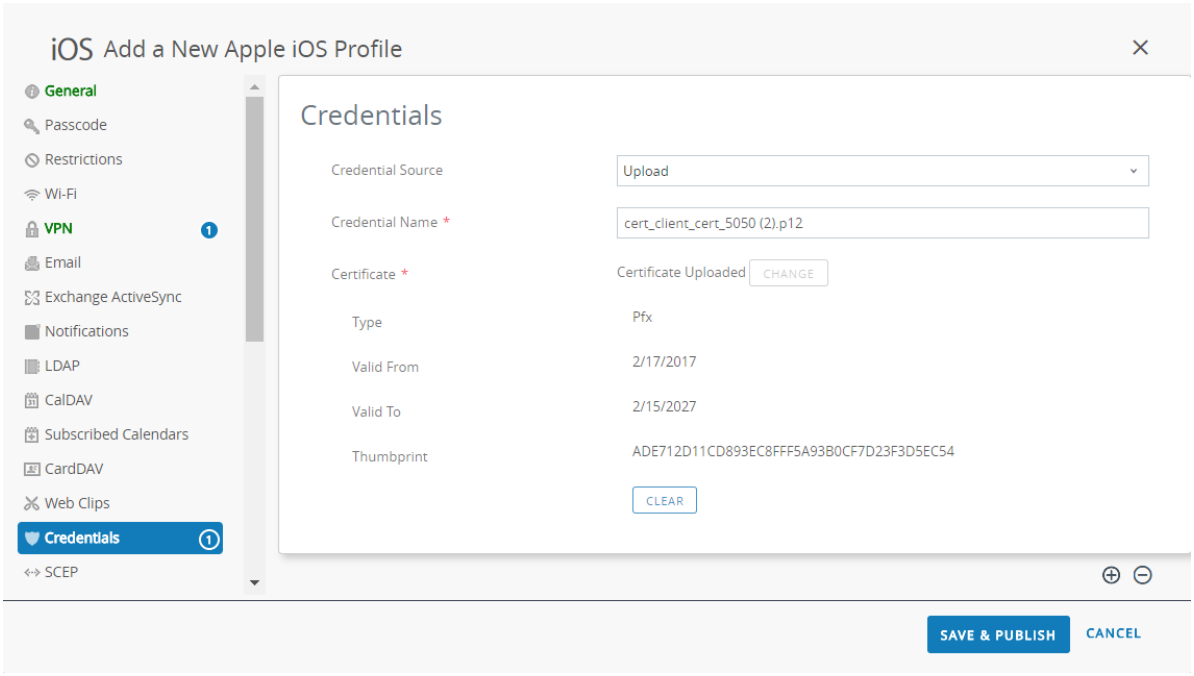
Toutes les configurations de VPN d'accès à distance pour les terminaux iOS exigent une authentification basée sur le certificat.

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 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 d'AirWatch :
  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).

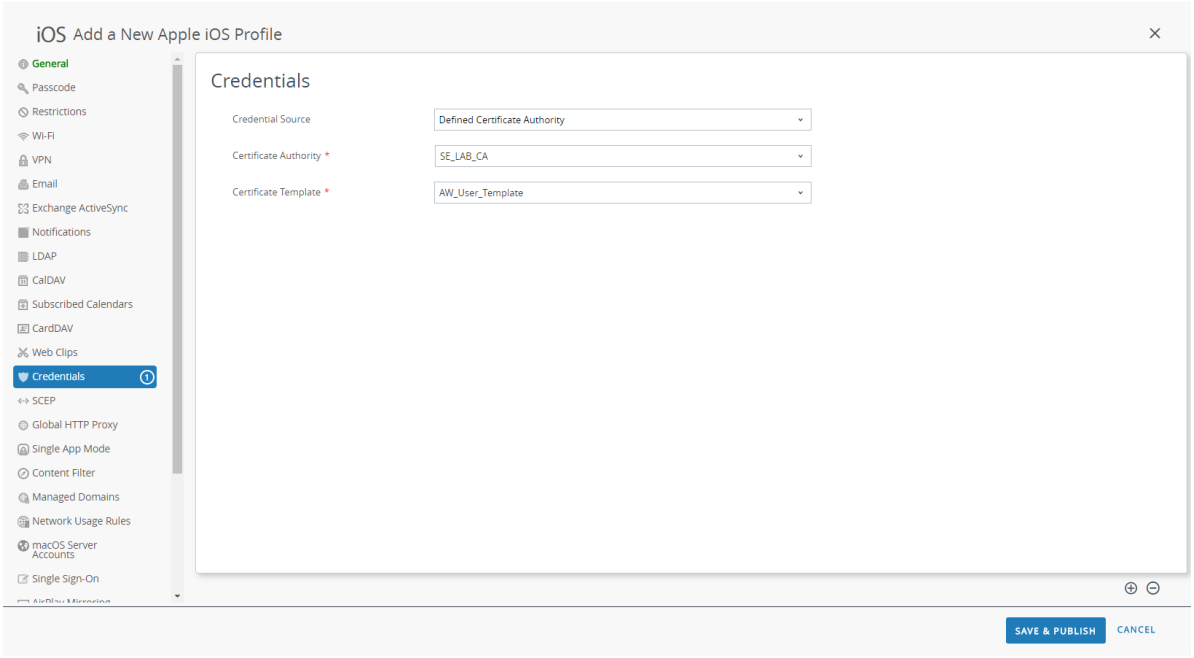


- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.



- 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.

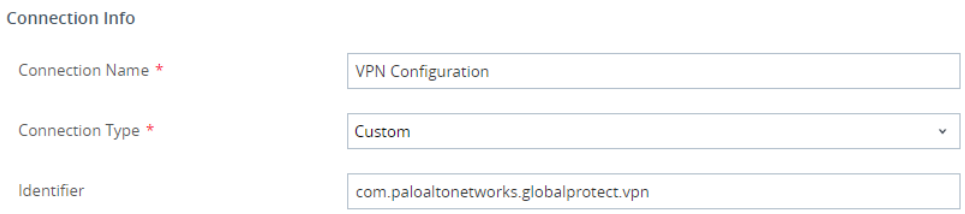
3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.



STEP 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 **Connection Type (Type de connexion)** sur **Custom (Personnalisé)**, saisissez l'ID de groupe suivant dans le champ **Identifier (Identifiant)** pour identifier l'application GlobalProtect :

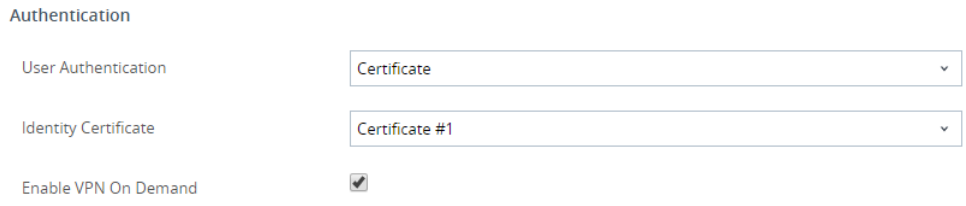
   com.paloaltonetworks.globalprotect.vpn



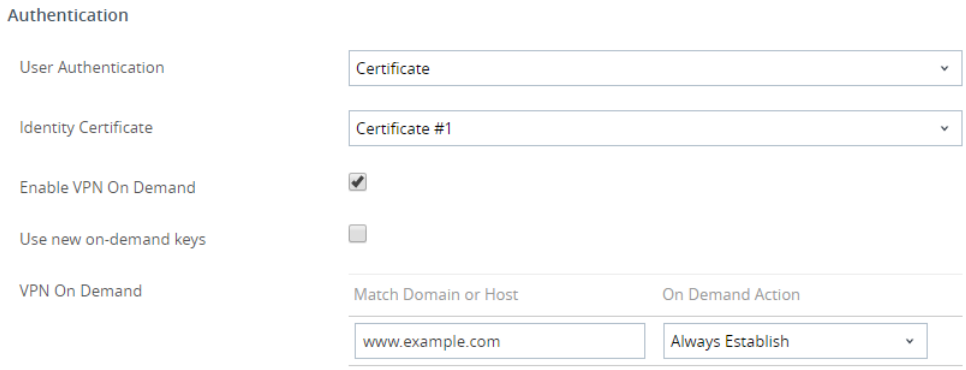
4. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel les utilisateurs doivent se connecter.
5. (Facultatif) Saisisissez le nom d'utilisateur du **Account (Compte)** VPN ou cliquez sur le bouton d'ajout (**+**) pour afficher les valeurs de recherche 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.

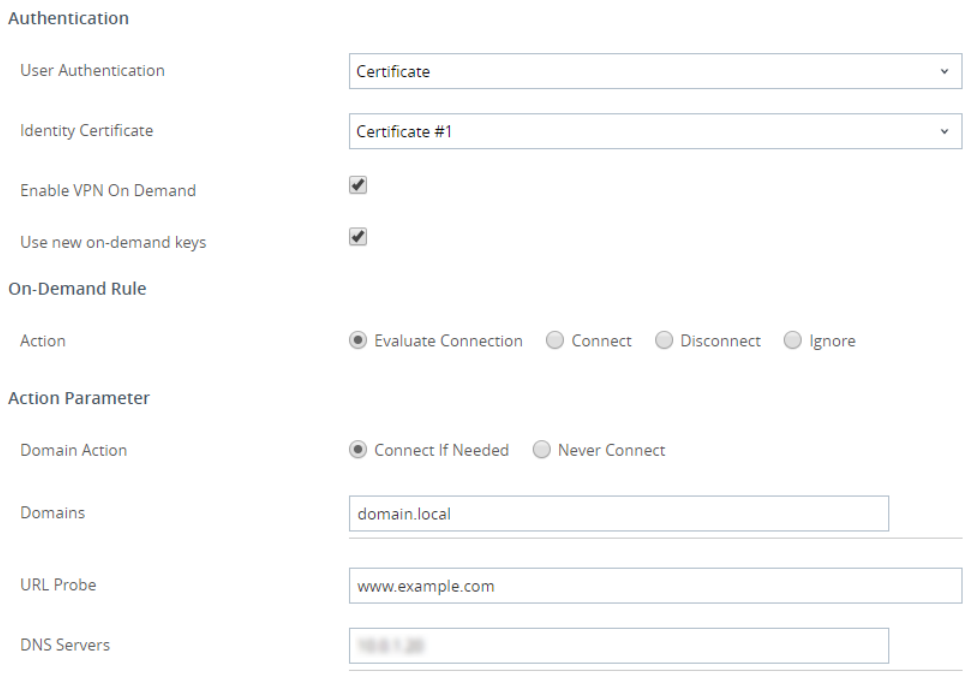
8. Lorsque vous êtes invité à le faire, sélectionnez le **Identity Certificate (Certificat d'identité)** que GlobalProtect utilisera pour authentifier les utilisateurs. Le **Identity Certificate (Certificat d'identité)** est le même certificat que vous avez configuré dans les paramètres de **Credentials (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).



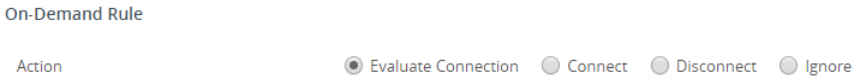
10. (Facultatif) Configurez les anciennes règles de connexion **VPN On-Demand (VPN à la demande)** :
    - **Match Domain or Host (Faire correspondre le domaine ou l'hôte)** : saisissez le domaine ou le nom d'hôte qui entraîne l'établissement de la connexion GlobalProtect lorsque les utilisateurs y accèdent.
    - **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 demande)**. Vous pouvez ajouter plusieurs règles en cliquant sur **ADD RULE (Ajouter une règle)**.

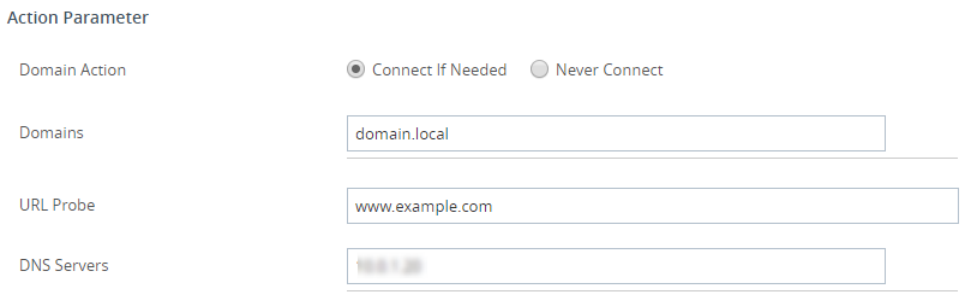


- Dans la section On-Demand Rule (Règle à la demande), sélectionnez une **Action** à appliquer à la connexion GlobalProtect selon les critères que vous définissez :
  - **Evaluate Connection (Évaluer la connexion)** : établit automatiquement la connexion GlobalProtect selon les paramètres de connexion 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.

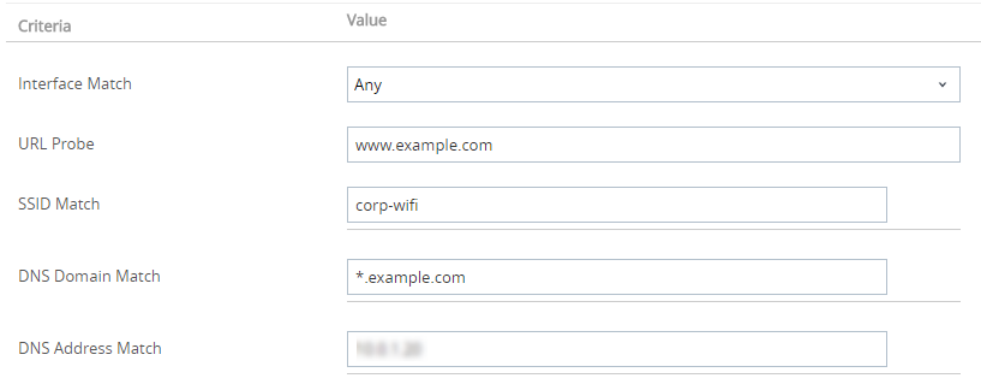


- (Facultatif) Si vous définissez l'**Action** de votre règle de connexion à la demande sur **Evaluate Connection (Évaluer la connexion)**, vous devez également configurer un paramètre d'action pour préciser si GlobalProtect peut tenter de se reconnecter, ou non, si la résolution du nom de domaine échoue 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.
  - 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 correspondance réussie, toutes les adresses IP de serveur DNS énumérées sur le point de terminaison doivent correspondre aux adresses IP de serveur DNS indiquées.

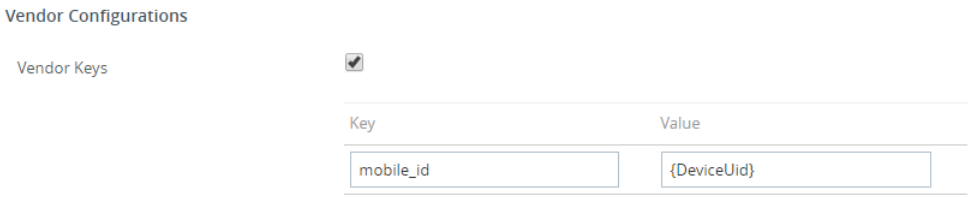


12.(Facultatif) Sélectionnez le type de **Proxy** et configurez les paramètres pertinents.

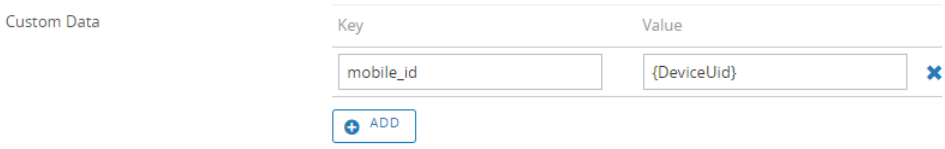
STEP 6 | (Facultatif) (à compter de la version 5.0 de l'application GlobalProtect) Si votre déploiement GlobalProtect exige une intégration HIP avec MDM, précisez l'attribut de Unique device identifier (UDID ; Identificateur de périphérique unique).

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}`**.



STEP 7 | **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison Windows 10 UWP à l'aide d'AirWatch

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 AIRWATCH ne répertorie pas encore GlobalProtect comme fournisseur de connexion officiel pour les points de terminaison 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 d'AirWatch :

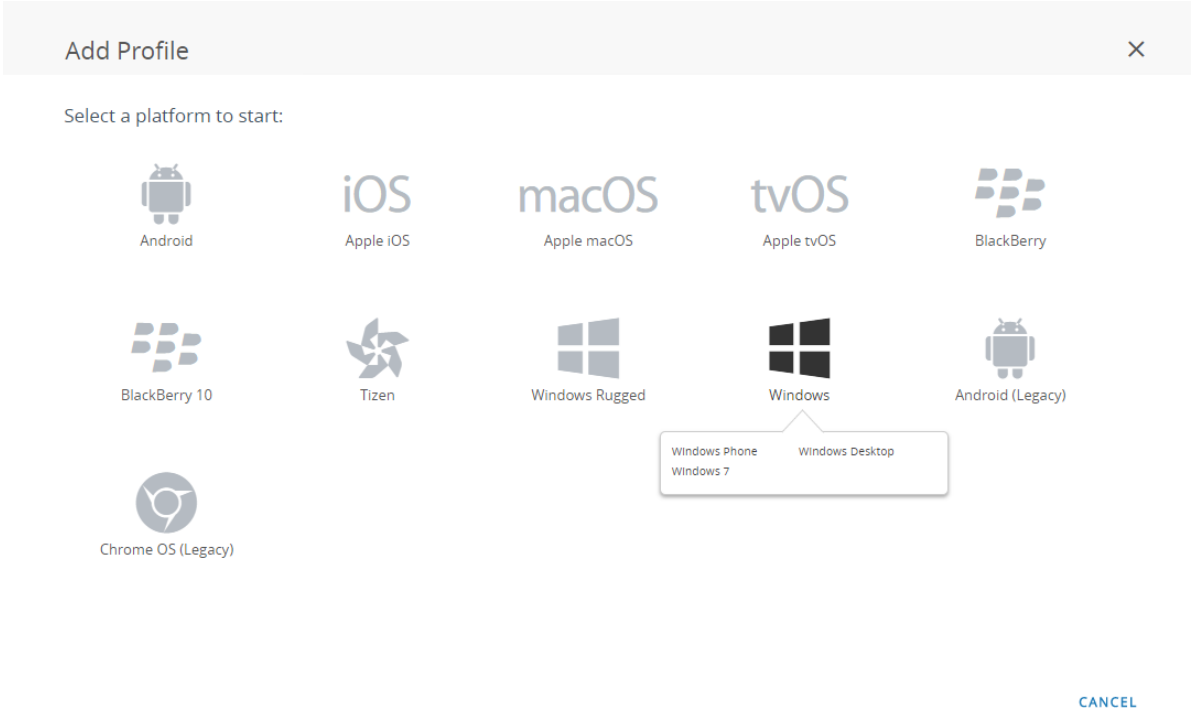
STEP 1 | Téléchargez l'app GlobalProtect pour Windows 10 UWP :

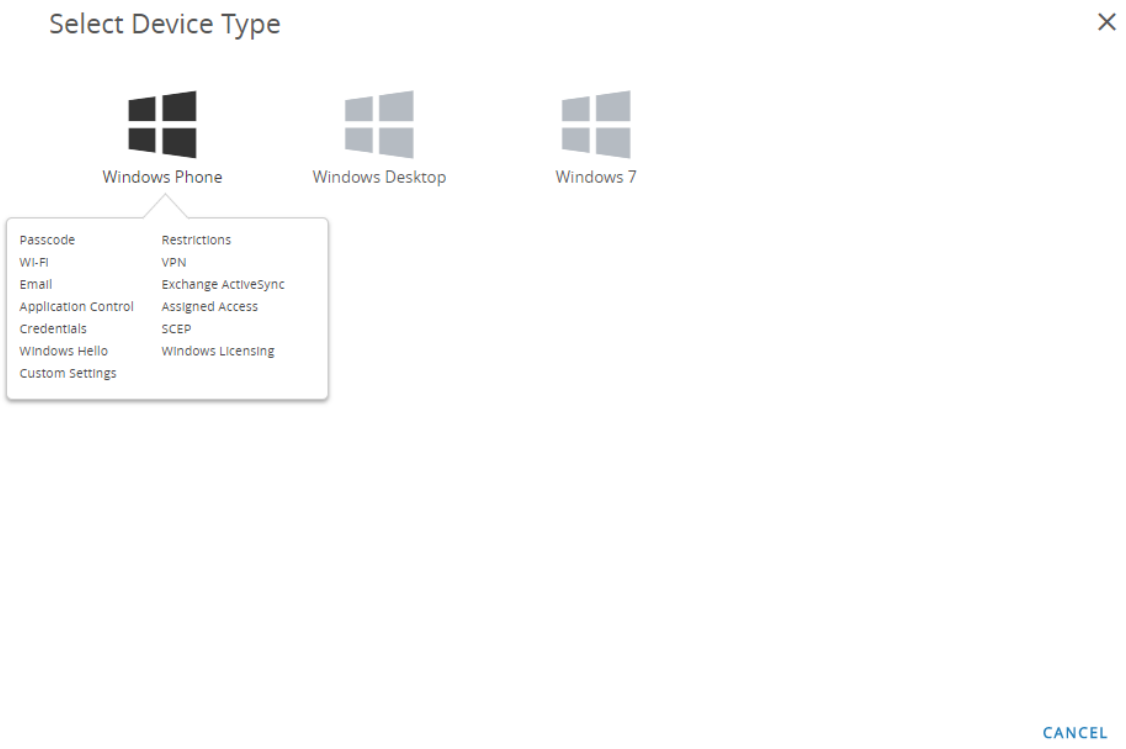
- Déployez l'application mobile GlobalProtect à l'aide de AirWatch.

- Téléchargez l'application GlobalProtect directement à partir du Microsoft Store.

STEP 2 | Depuis la console AirWatch, 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 (Ajoutez)** un nouveau profil.
2. Sélectionnez **Windows** comme plateforme et **Windows Phone** comme type de configuration.

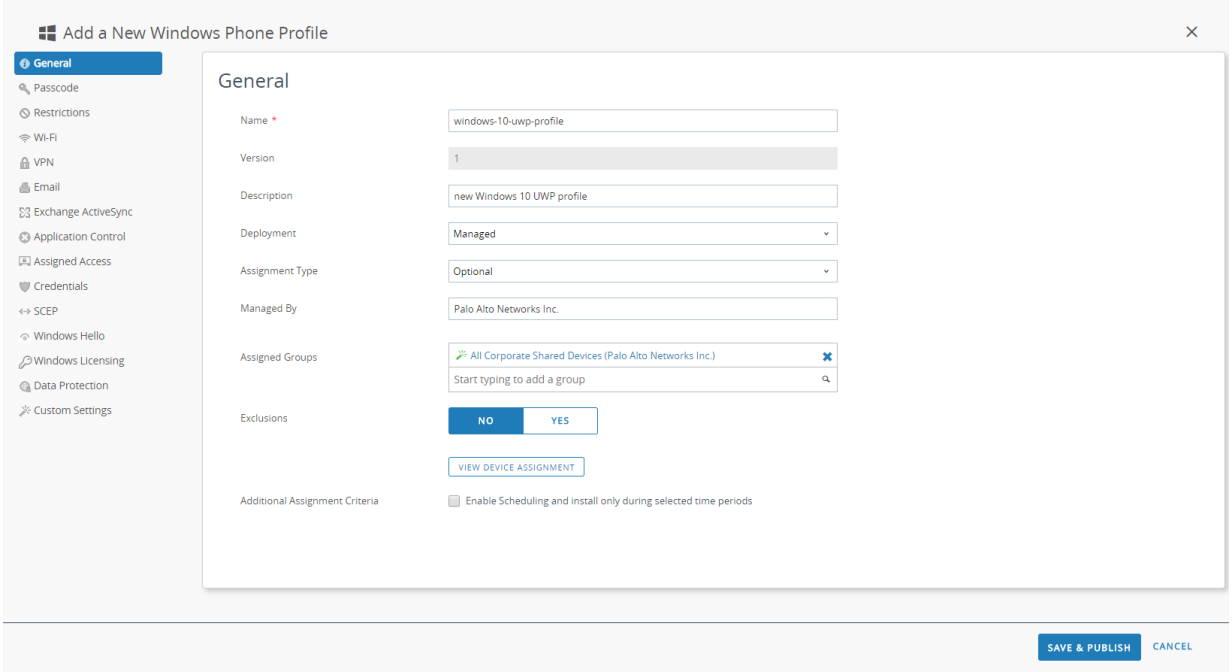




STEP 3 | Configurez les paramètres **General (généraux)**.

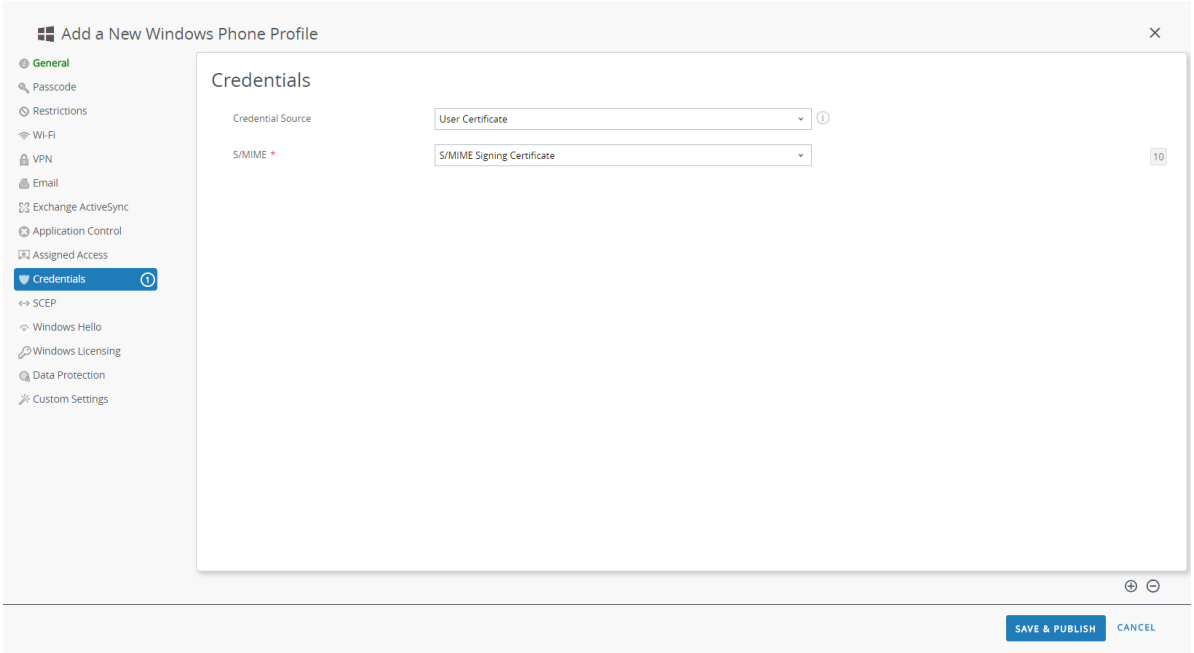
1. Saisissez un **Name (Nom)** pour le profil.
2. (Facultatif) Saisissez une brève **description** du profil qui indique son but.
3. (Facultatif) Définissez le mode de **Deployment (Déploiement)** sur **Managed (Géré)** pour permettre la suppression automatique du profil lors de la désinscription.
4. (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 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)**.

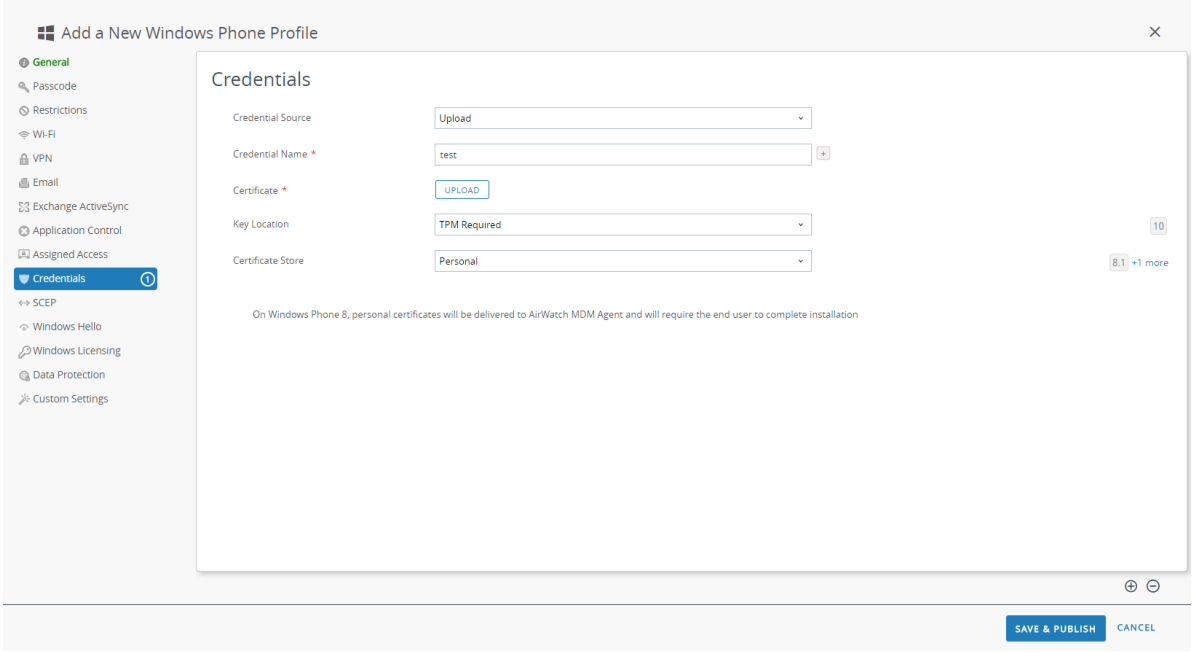


STEP 4 | (Facultatif) Si votre déploiement GlobalProtect exige une authentification du certificat du client, configurez les paramètres des **Credentials (Informations d'identification)** :

- Pour extraire les certificats de client des utilisateurs d'AirWatch :
  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 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, l'agent AirWatch Protection doit être installé sur le point de terminaison.
  6. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.

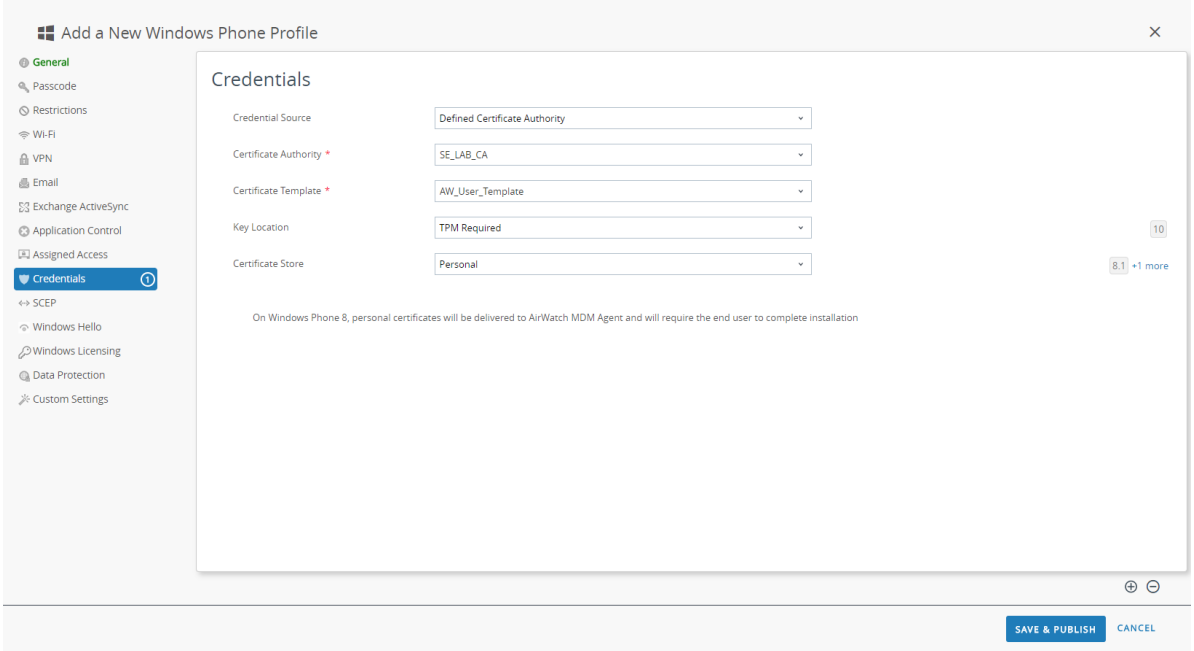


- Pour utiliser une autorité de certification et un modèle prédéfinis :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
  2. Sélectionnez la **Certificate Authority (Autorité de certification)** 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 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, l'agent AirWatch Protection doit être installé sur le point de terminaison.

5. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.

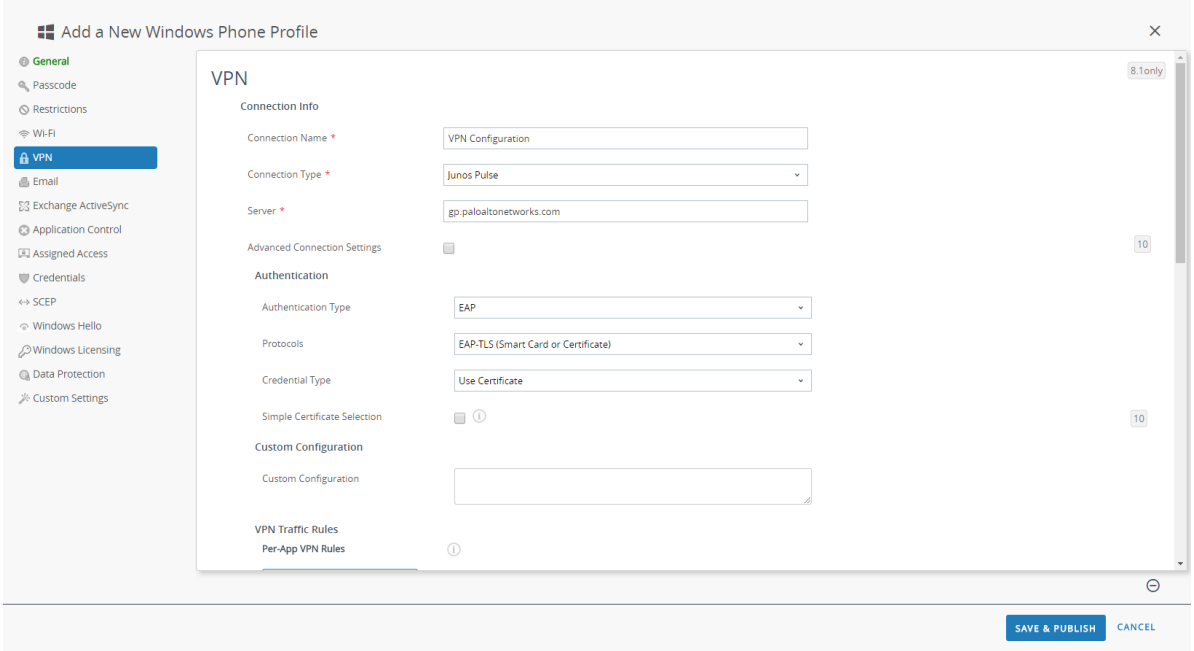


STEP 5 | Configurez les paramètres **VPN** :

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).

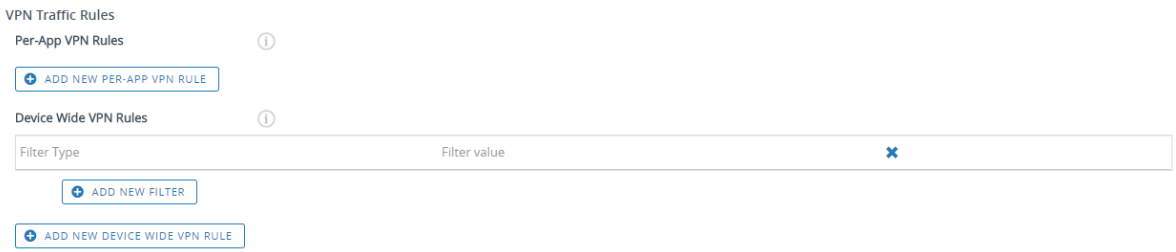
   Vous devez sélectionner un fournisseur de rechange, car AirWatch ne répertorie pas encore GlobalProtect en tant que fournisseur de connexions officiel pour les points de terminaison Windows.

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.

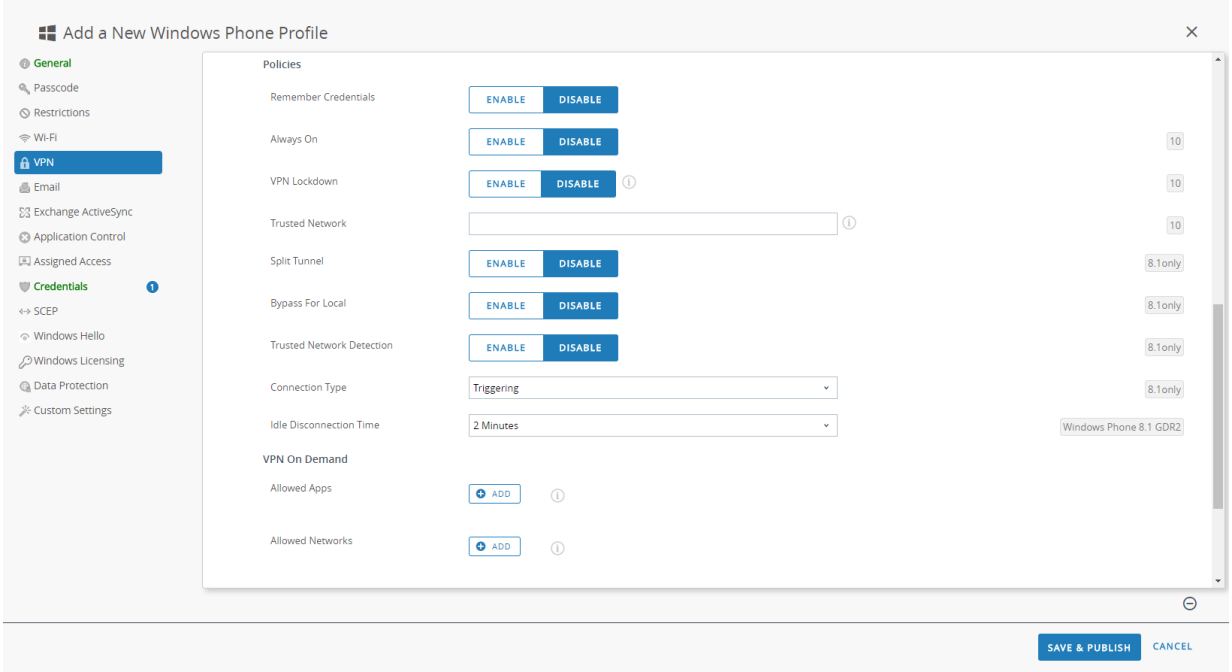


5. (Facultatif) Pour permettre à GlobalProtect d'enregistrer les informations d'identification de l'utilisateur, **ENABLE (ACTIVEZ)** l'option permettant de **Remember Credentials (Mémoriser les informations)** d'identification dans la zone de stratégies.
6. (Facultatif) Dans la section VPN Traffic Rules (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 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 AIRWATCH 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.



STEP 6 | **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

STEP 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. AIRWATCH 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. Retour à AirWatch et, dans la **Devices(Périphériques)** > **Profiles (Profils)** > **List View (Vue de la 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.

STEP 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)**. AIRWATCH déplace le profil sur la liste inactive.

STEP 9 | Testez la configuration.

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur à l'aide de Microsoft Intune

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 offre une connexion sécurisée entre le pare-feu et les points de terminaison mobiles gérés par Microsoft Intune 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 à la section suivante pour obtenir des renseignements sur la manière de configurer une configuration de VPN à accès à distance initié par l'utilisateur à l'aide de Microsoft Intune :

- Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison iOS à l'aide de Microsoft Intune

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison iOS à l'aide de Microsoft Intune

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 Microsoft Intune :

STEP 1 | Téléchargement de l'application GlobalProtect pour Android

- Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune.
- Téléchargez l'app GlobalProtect directement à partir de l'App Store.

STEP 2 | (Facultatif) Si votre déploiement exige une authentification basée sur les certificats, configurez un profil de certificat.

STEP 3 | Créez un nouveau profil VPN iOS.

- Définissez la **Platform (Plateforme)** sur **iOS**.

STEP 4 | Configurez les paramètres VPN à la demande (accès à distance) pour les points de terminaison iOS.

- Définissez le **Connection type (Type de connexion)** sur **Palo Alto Networks GlobalProtect**.
- Dans la section Automatic VPN settings (Paramètres VPN automatiques), activez **On-demand VPN (VPN à la demande)** pour configurer des règles conditionnelles qui contrôlent le moment où la connexion VPN est initiée.

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur à l'aide de MobileIron

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.

Reportez-vous à la section suivante pour obtenir des renseignements sur la manière de configurer une configuration de VPN à accès à distance initié par l'utilisateur à l'aide de MobileIron :

- Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison iOS à l'aide de MobileIron

Configurer une configuration de VPN d'accès à distance initié par l'utilisateur sur les points de terminaison iOS à l'aide de MobileIron

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 :

STEP 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.

STEP 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.

STEP 3 | Ajoutez une configuration VPN à la demande (accès à distance.

- Définissez le type de configuration sur **VPN On-Demand (VPN à la demande)**.

STEP 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.

Configurations de VPN par application

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.

Reportez-vous aux sections suivantes pour obtenir des renseignements sur la manière de configurer une configuration de VPN par application à l'aide des systèmes de gestion des périphériques mobiles pris en charge :

- Configurer une configuration de VPN par application à l'aide d'AirWatch
- Configurer une configuration de VPN par application à l'aide de Microsoft Intune
- Configurer une configuration de VPN par application à l'aide de MobileIron

Configurer une configuration de VPN par application à l'aide d'AirWatch

AirWatch 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 les points de terminaison mobiles gérés par AirWatch et le pare-feu 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 renseignements sur la manière de configurer une configuration de VPN par application à l'aide d'AirWatch :

- Configurer une configuration de VPN par application sur les points de terminaison iOS à l'aide d'AirWatch
- Configurer une configuration de VPN par application sur les points de terminaison Android à l'aide d'AirWatch
- Configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide d'AirWatch

Configurer une configuration de VPN par application sur les points de terminaison iOS à l'aide d'AirWatch

Vous pouvez autoriser l'accès aux ressources internes à partir de vos périphériques mobiles gérés en configurant l'accès VPN GlobalProtect à l'aide d'AirWatch. 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 d'AirWatch :

STEP 1 | Téléchargement de l'application GlobalProtect pour iOS :

- Déployez l'application mobile GlobalProtect à l'aide de AirWatch.
- Téléchargez l'app GlobalProtect directement à partir de l'App Store.

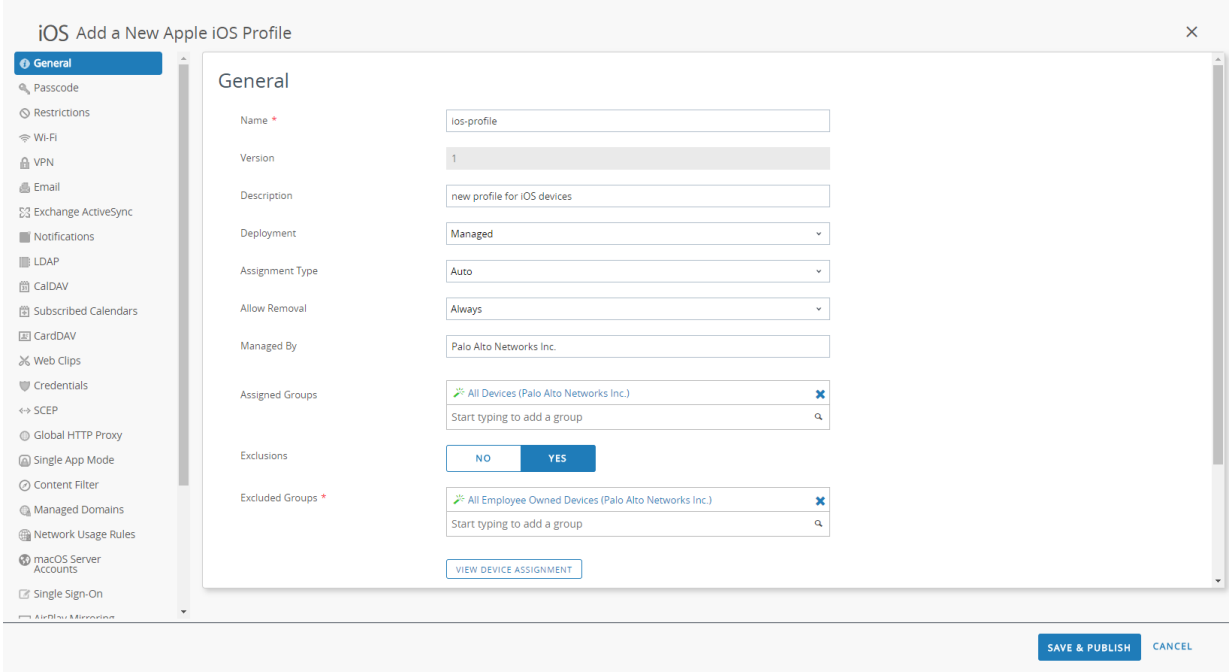
STEP 2 | Depuis la console AirWatch, modifiez un profil Apple iOS existant ou ajoutez-en un nouveau.

1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajoutez)** un nouveau profil.
2. Sélectionnez **iOS** à partir de la liste de la plateforme.

STEP 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, vous permettant de sélectionner les groupes intelligents que vous souhaitez exclure de l'affectation de ce profil de périphérique.

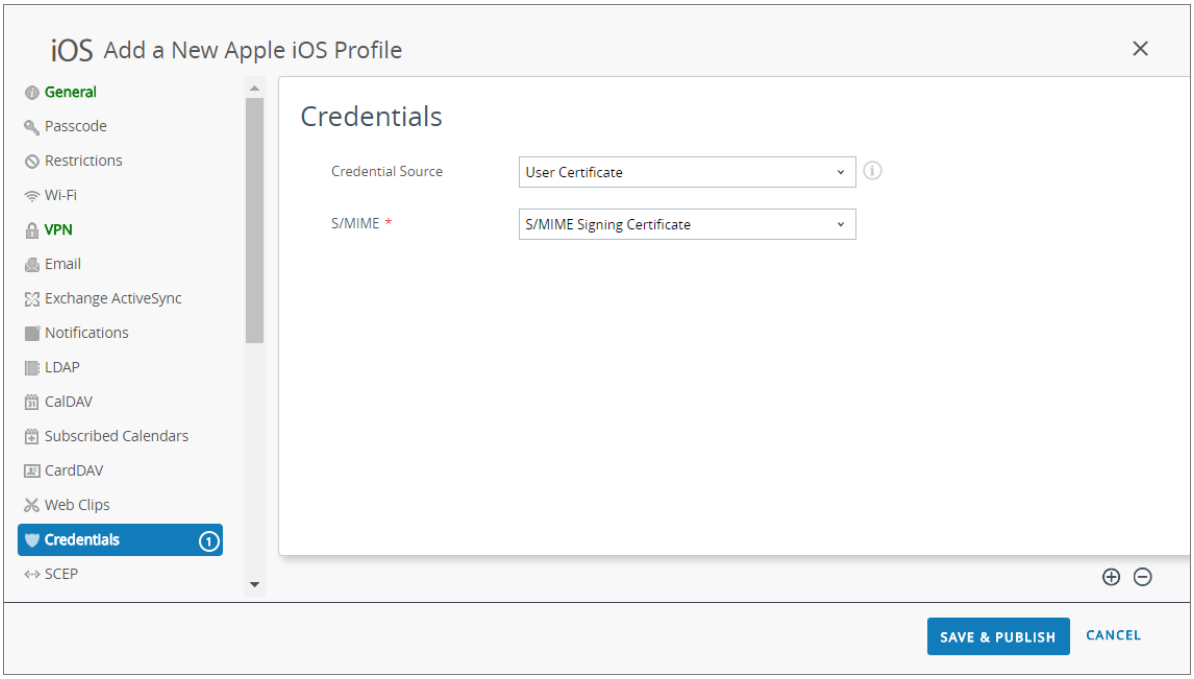


STEP 4 | Configurez les paramètres de **Credentials (Informations d'identification)** :

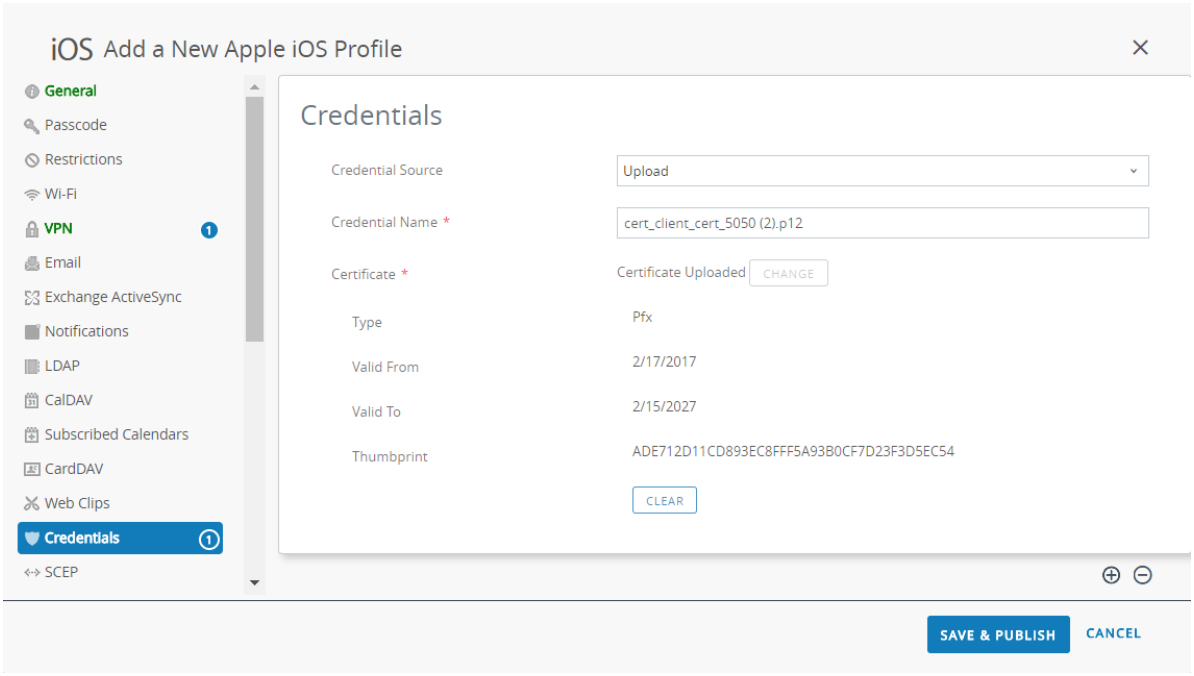
Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

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 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 d'AirWatch :
  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).

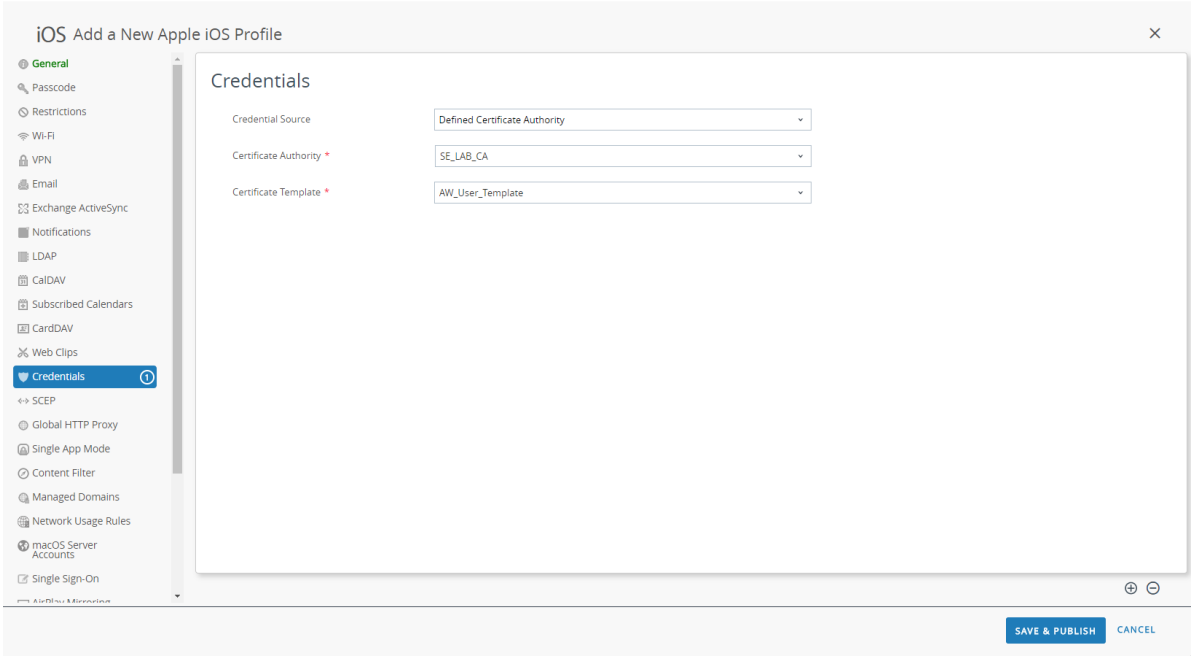


- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.



- 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.

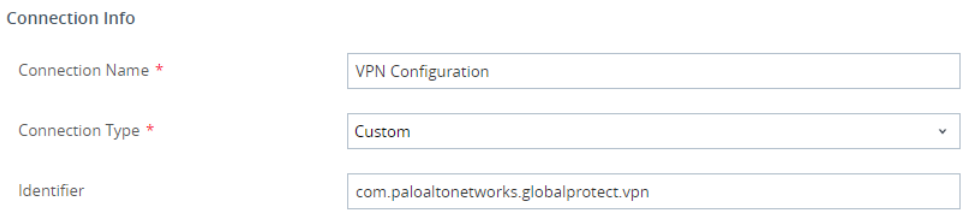
3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.



STEP 5 | Configurez les paramètres **VPN** :

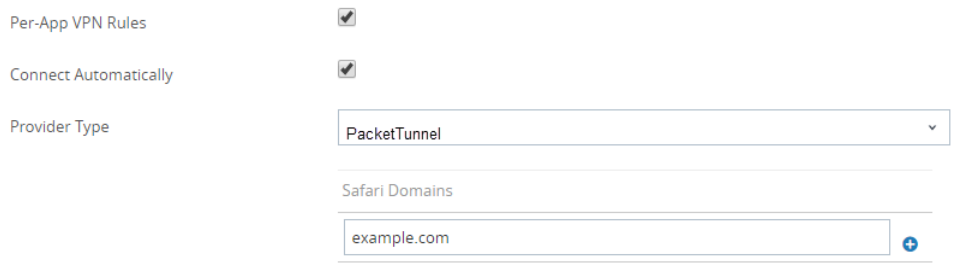
1. Saisissez le **Connection Name (Nom de la connexion)** que le point de terminaison affiche.
2. Sélectionnez le **Connection Type (Type de connexion)** du réseau :
   - Pour l'application 4.1.x de GlobalProtect et les versions antérieures, sélectionnez **Palo Alto Networks GlobalProtect**.
   - Pour l'application 5.0 de GlobalProtect et les versions ultérieures, sélectionnez **Custom (Personnalisé)**.
3. (Facultatif) Si vous définissez le **Connection Type (Type de connexion)** sur **Custom (Personnalisé)**, saisissez l'ID de groupe suivant dans le champ **Identifier (Identifiant)** pour identifier l'application GlobalProtect :

   com.paloaltonetworks.globalprotect.vpn



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) Saisisissez 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. 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 un **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.



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.

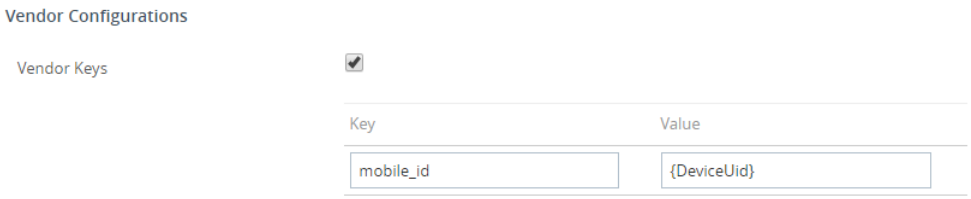
9. Lorsque vous êtes invité à le faire, sélectionnez le **Identity Certificate (Certificat d'identité)** que GlobalProtect utilisera pour authentifier les utilisateurs. Le **Identity Certificate (Certificat d'identité)** est le même certificat que vous avez configuré dans les paramètres de **Credentials (Informations d'identification)**.

10. (Facultatif) Sélectionnez le type de **Proxy** et configurez les paramètres pertinents.

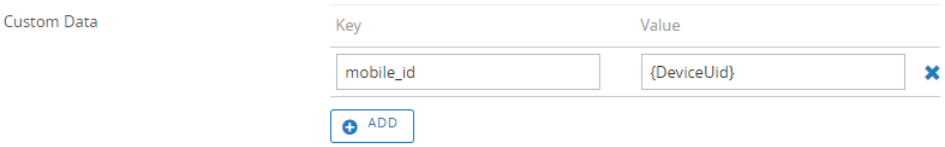
STEP 6 | (Facultatif) (à compter de la version 5.0 de l'application GlobalProtect) Si votre déploiement GlobalProtect exige une intégration HIP avec MDM, précisez l'attribut de Unique device identifier (UDID ; Identificateur de périphérique unique).

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}`**.

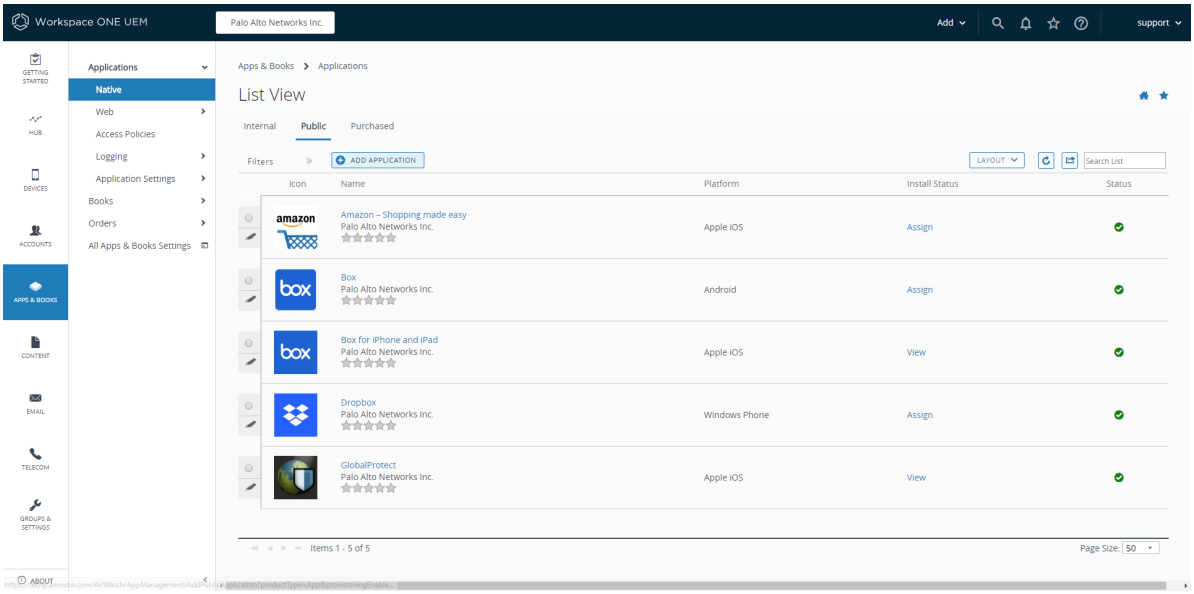


STEP 7 | **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

STEP 8 | Configurez les paramètres VPN par application pour une nouvelle application gérée, ou modifiez les paramètres d'une application gérée existante.

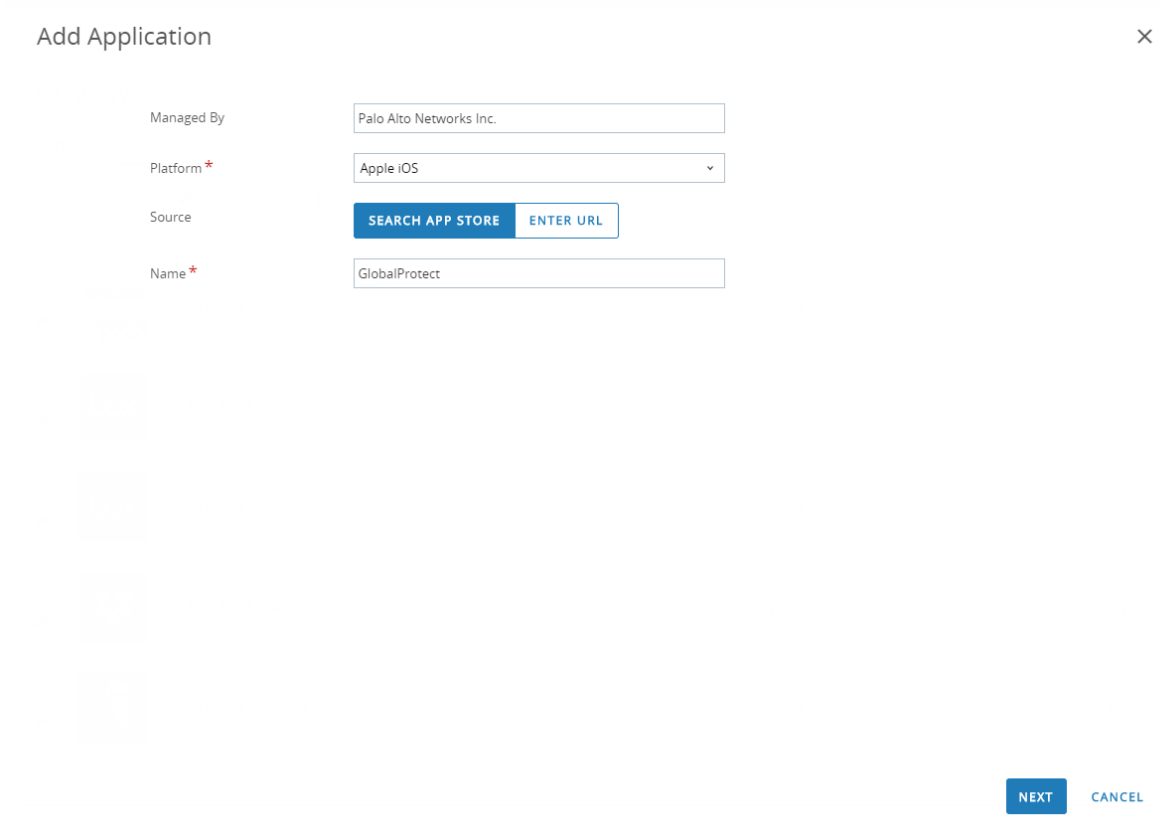
Après avoir configuré les paramètres de l'application et activé le VPN par application, vous pouvez publier l'application à un groupe d'utilisateurs et autoriser l'application à acheminer le trafic via le tunnel VPN GlobalProtect.

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 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.



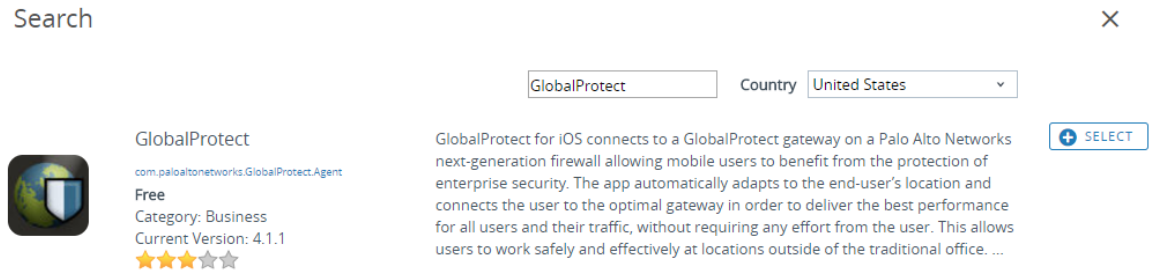
3. Dans le champ **Managed By (Géré par)**, sélectionnez le groupe de l'entreprise qui gérera cette application.
4. Définissez la **Platform (Plateforme)** sur **Apple iOS**.

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).

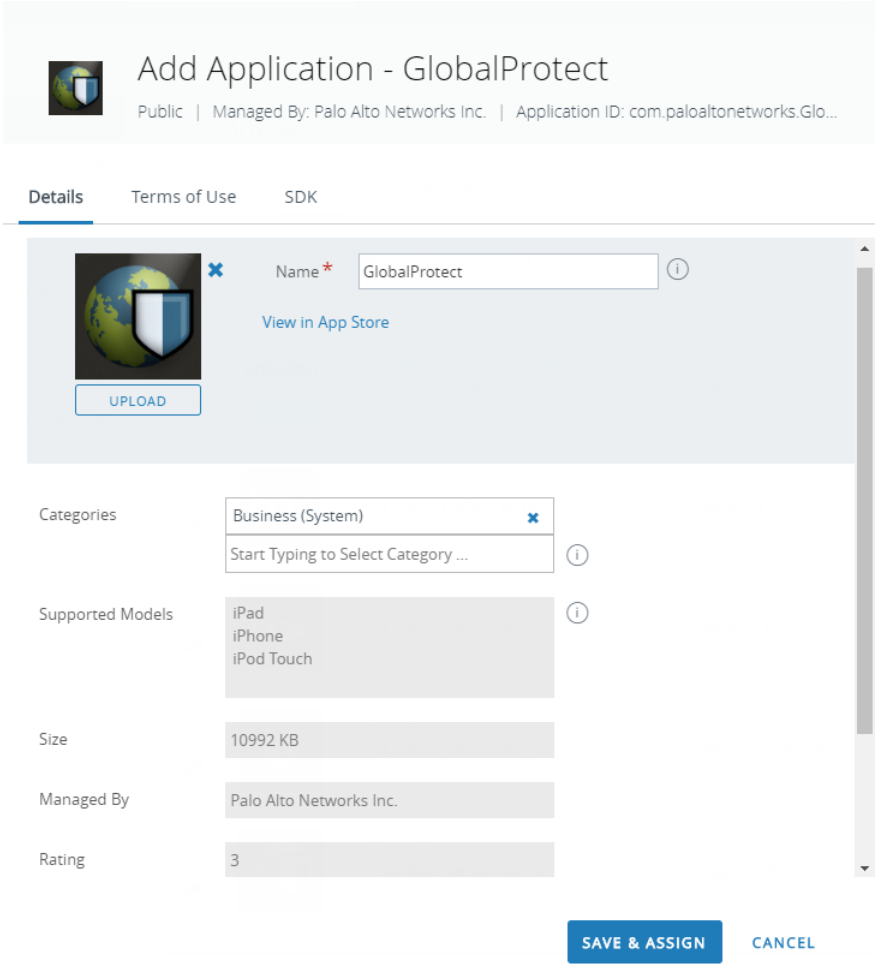


6. Cliquez sur **NEXT (Suivant)**.

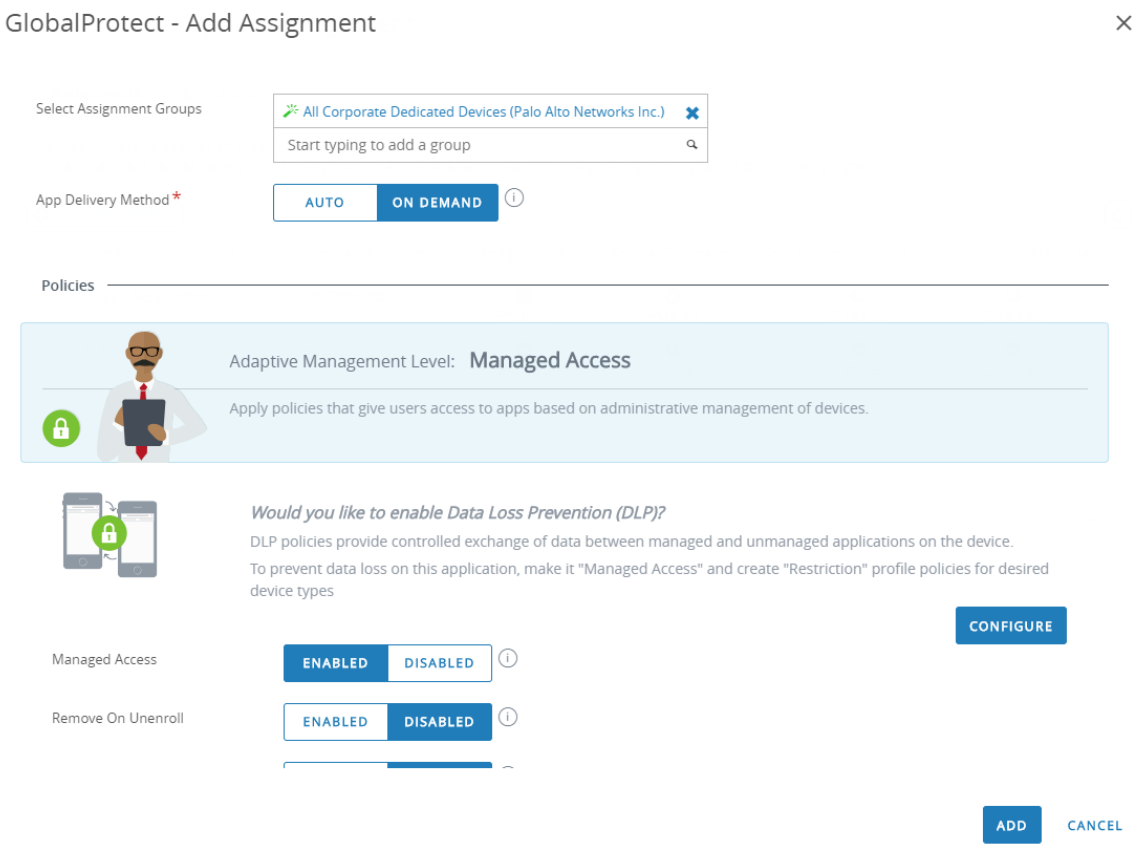
   Si vous choisissez de rechercher l'application dans l'App Store, vous devez également **SELECT (Sélectionner)** l'application à partir d'une liste de résultats de recherche.



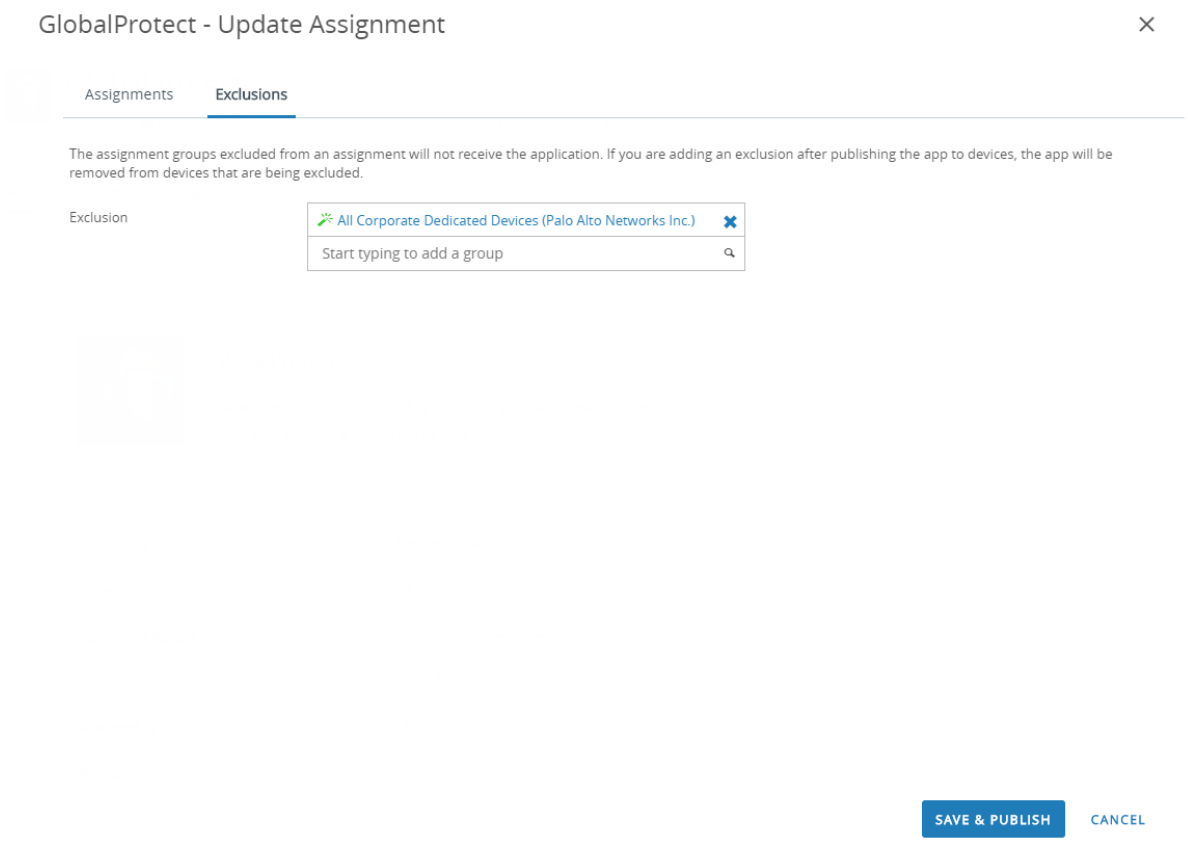
7. Sur le dialogue Add Application (Ajouter une application), assurez-vous que le **Name (Nom)** de l'application est bon. C'est le nom qui figurera dans le catalogue d'applications d'AirWatch.
8. (Facultatif) Affectez l'application à des **Categories (Catégories)** prédéfinies ou personnalisées pour faciliter l'accès dans le catalogue d'applications d'AirWatch.



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.
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 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**.



14. **SAVE & PUBLISH (Enregistrez et publiez)** la configuration dans les groupes intelligents affectés.

Configurer une configuration de VPN par application sur les points de terminaison Android à l'aide d'AirWatch

Vous pouvez autoriser l'accès aux ressources internes à partir de vos périphériques mobiles gérés en configurant l'accès VPN GlobalProtect à l'aide d'AirWatch. 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 d'AirWatch :

STEP 1 | Téléchargement de l'application GlobalProtect pour Android :

- Déployez l'application mobile GlobalProtect à l'aide de AirWatch.
- Téléchargez l'app GlobalProtect directement à partir de Google Play.

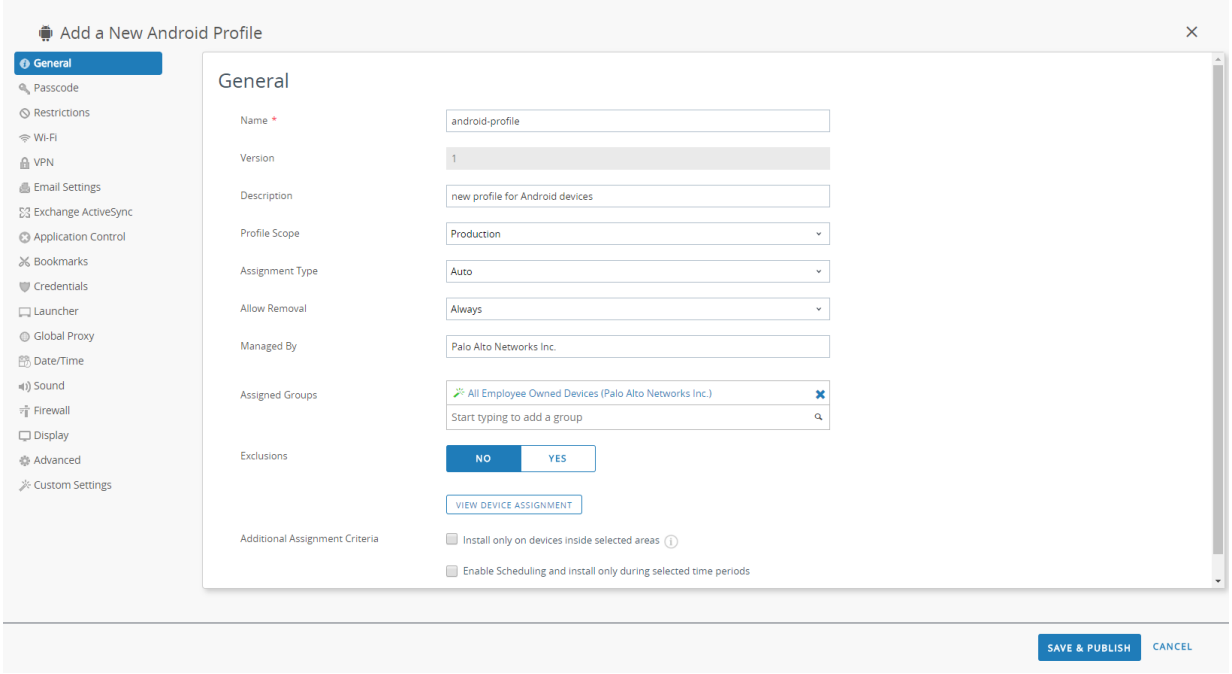
STEP 2 | Depuis la console AirWatch, modifiez un profil Android existant ou ajoutez-en un nouveau.

1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajoutez)** un nouveau profil.
2. Sélectionnez **Android (Legacy) (Android (hérité)** de la liste de la plateforme.

STEP 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.

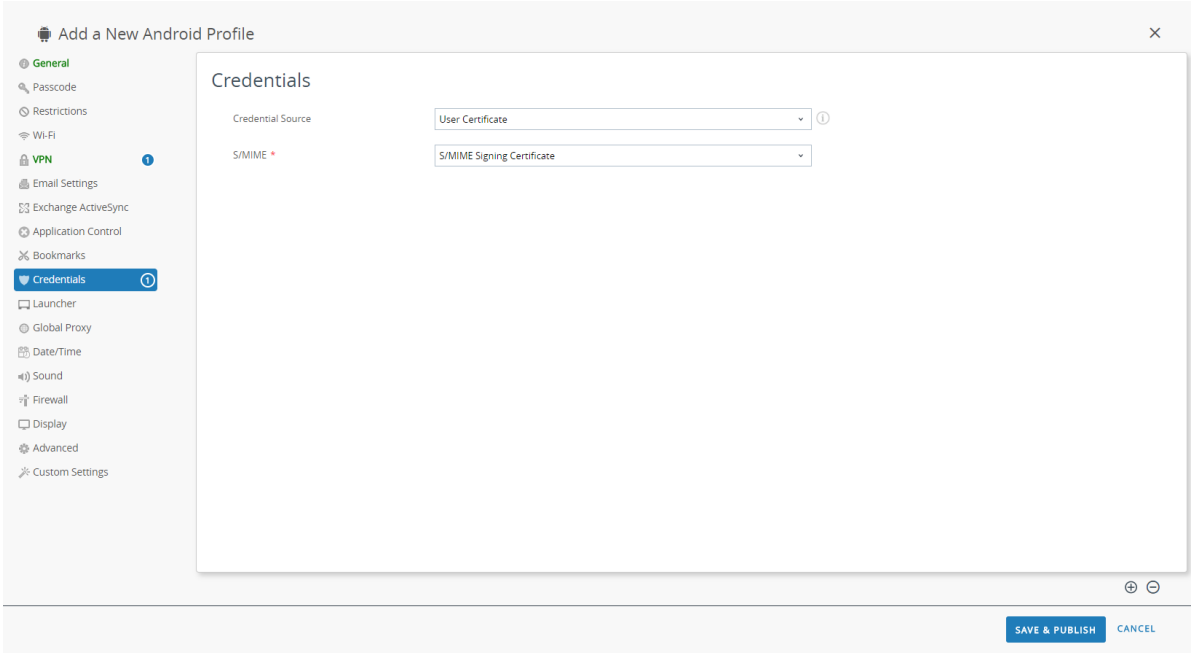
3. (Facultatif) Sélectionnez la **Profile Scope (Portée du profil)**, soit **Production, Staging (Pré-production)** ou **Both (les deux)**.
4. (Facultatif) Sélectionnez un **Assignment Type (Type d'affectation)** pour déterminer la façon dont le profil sera déployé sur les points de terminaison. Sélectionnez **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 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.



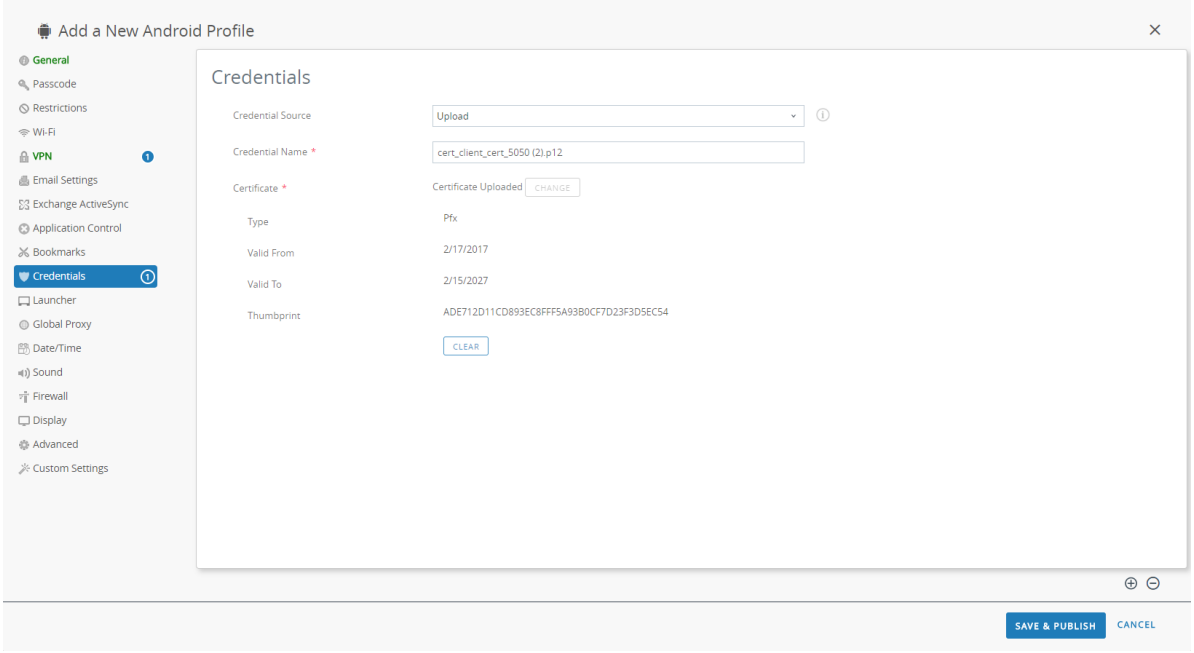
STEP 4 | Configurez les paramètres de **Credentials (Informations d'identification)** :

Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

- Pour extraire les certificats de client des utilisateurs d'AirWatch :
  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).

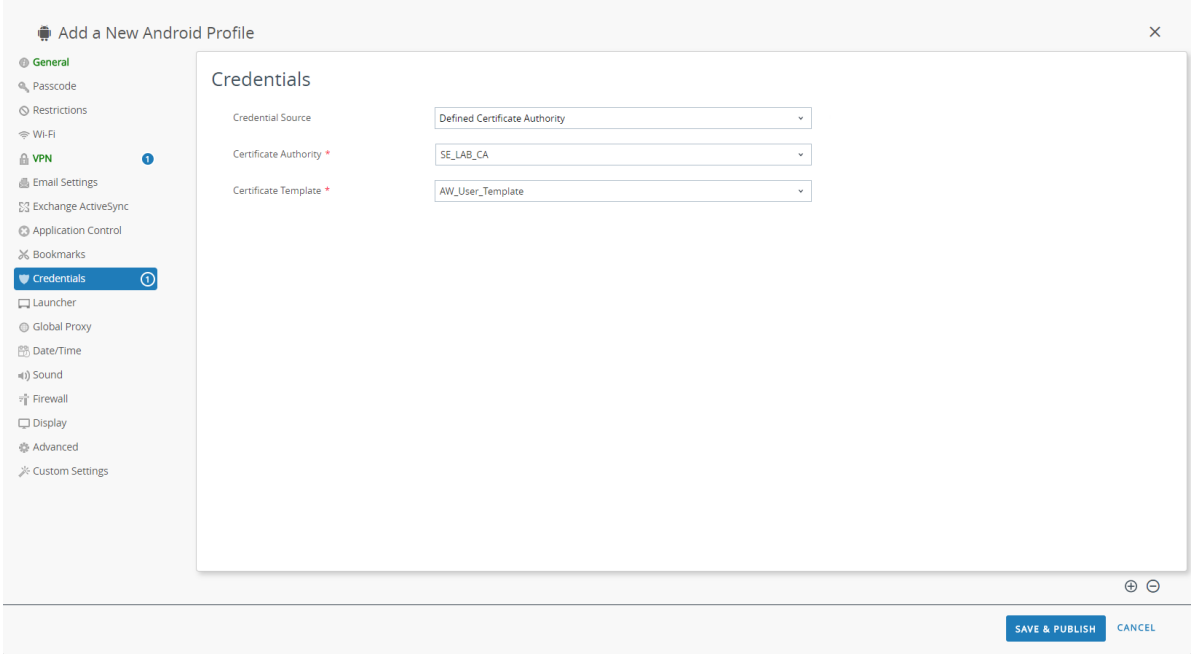


- Pour charger un certificat de client manuellement :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **Upload (Charger)**.
  2. Saisissez un **Credential Name (Nom d'informations d'identification)**.
  3. Cliquez sur **UPLOAD** pour localiser et sélectionner le certificat que vous voulez charger.
  4. Après avoir sélectionné un certificat, cliquez sur **SAVE (ENREGISTRER)**.



- Pour utiliser une autorité de certification et un modèle prédéfinis :

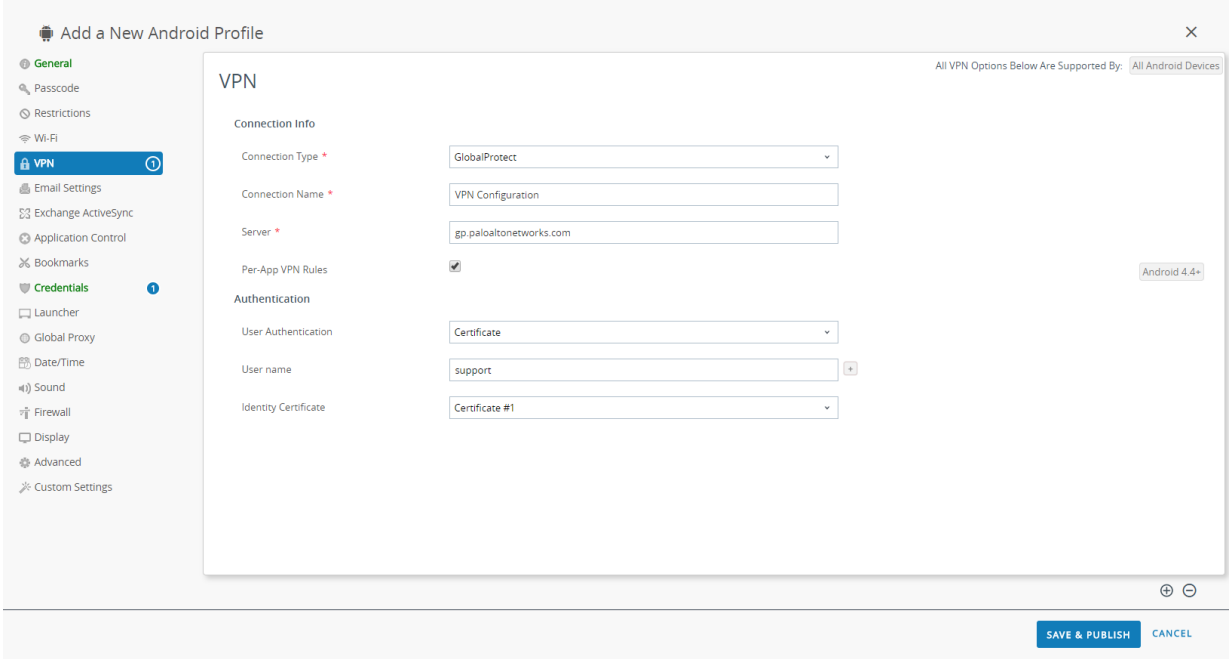
1. Définissez la **Credential Source (Source des informations d'identification)** sur **Defined Certificate Authority (Autorité de certification définie)**.
2. Sélectionnez la **Certificate Authority (Autorité de certification)** de laquelle vous souhaitez obtenir les certificats.
3. Sélectionnez le **Certificate Template (Modèle de certificat)** de l'autorité de certification.



STEP 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)**.

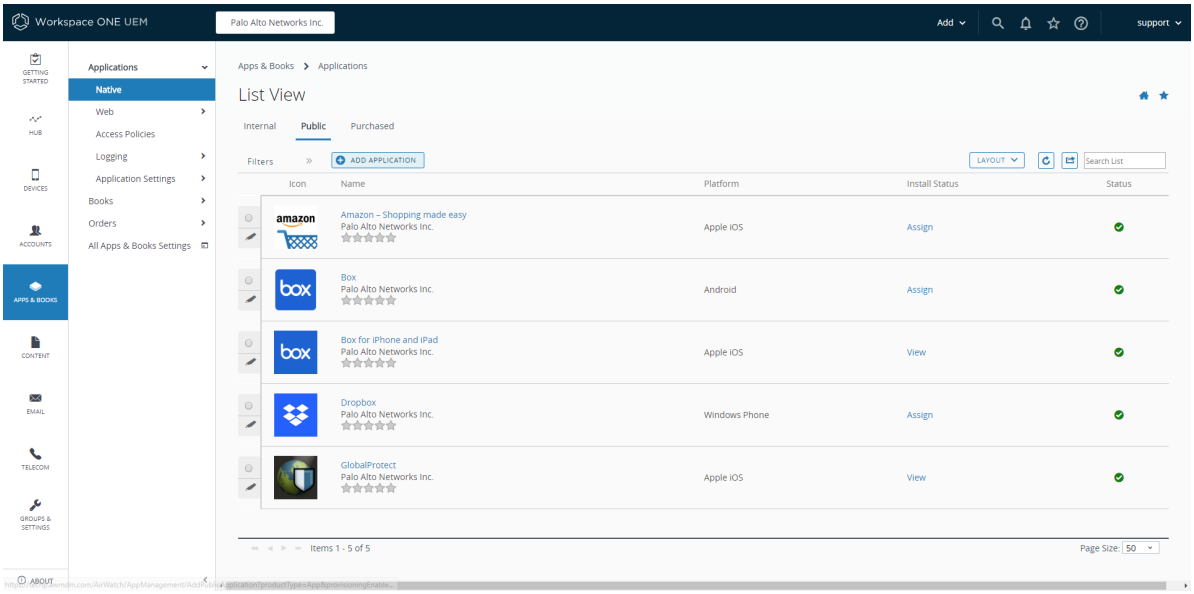


STEP 6 | **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

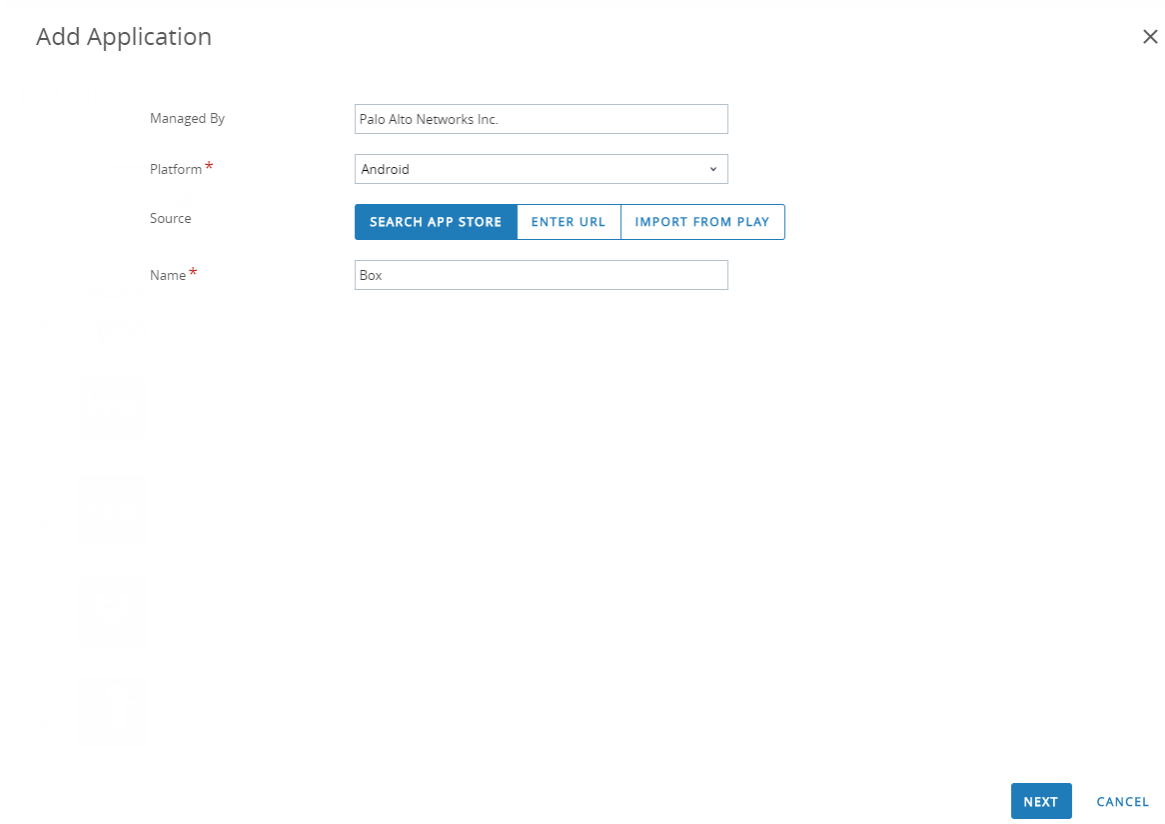
STEP 7 | Configurez les paramètres VPN par application pour une nouvelle application gérée, ou modifiez les paramètres d'une application gérée existante.

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 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.

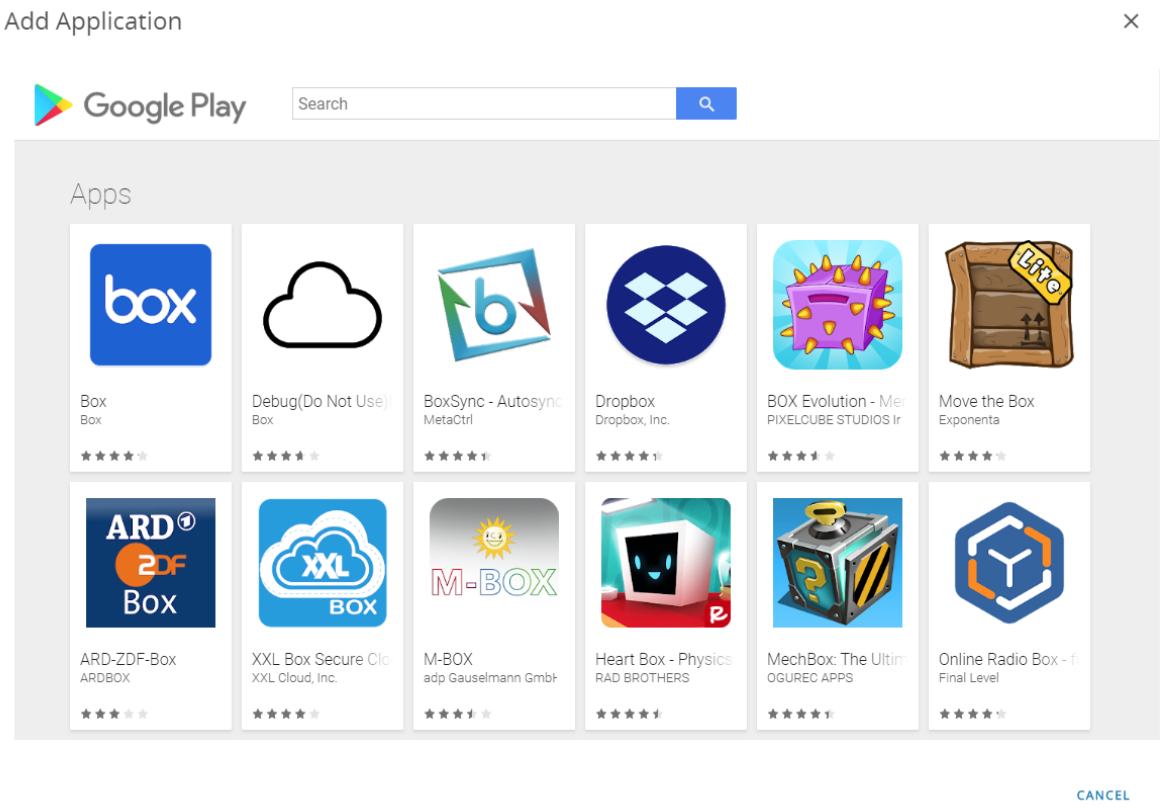


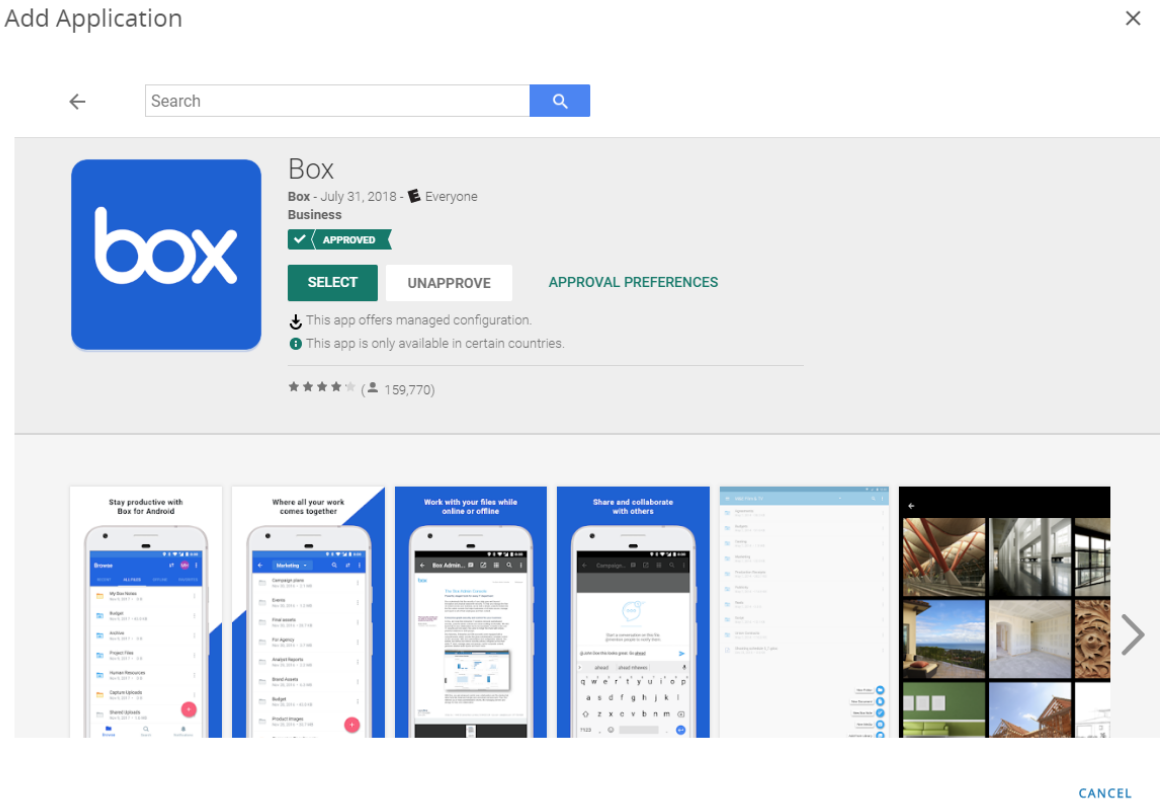
3. Dans le champ **Managed By (Géré par)**, sélectionnez le groupe de l'entreprise qui gérera cette application.
4. Définissez la **Platform (Plateforme)** sur **Android**.
5. Sélectionnez votre **Source** privilégiée pour trouver l'application :
   - **SEARCH APP STORE (Chercher dans l'App Store)** : 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.



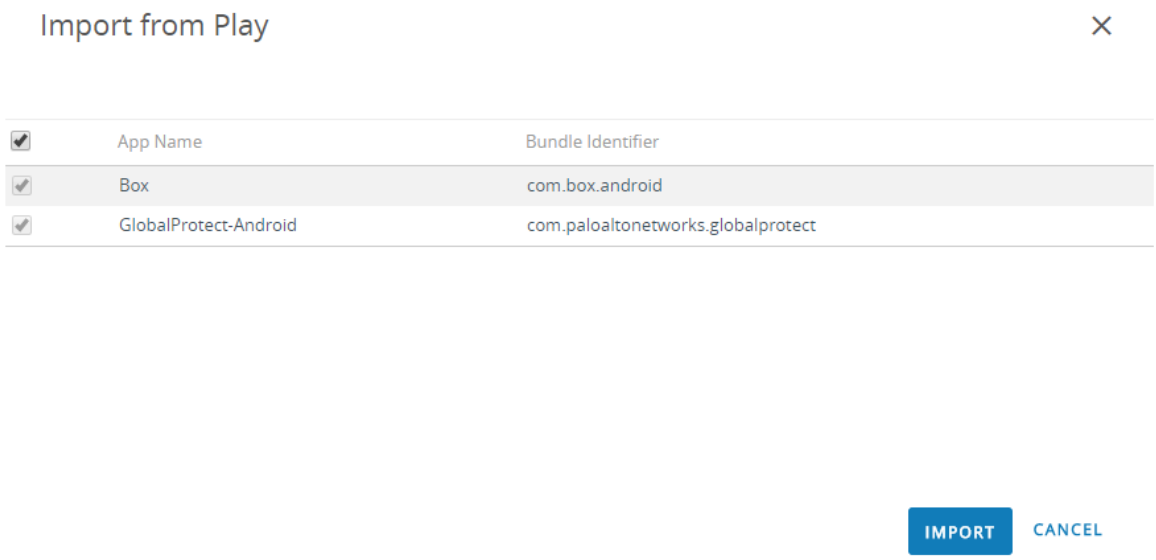
6. Cliquez sur **NEXT (Suivant)**.

   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 approuvée pour votre entreprise, vous devez **APPROVE (Approuver)** l'application. Une fois l'application approuvée, **SELECT (Sélectionnez)**-la.

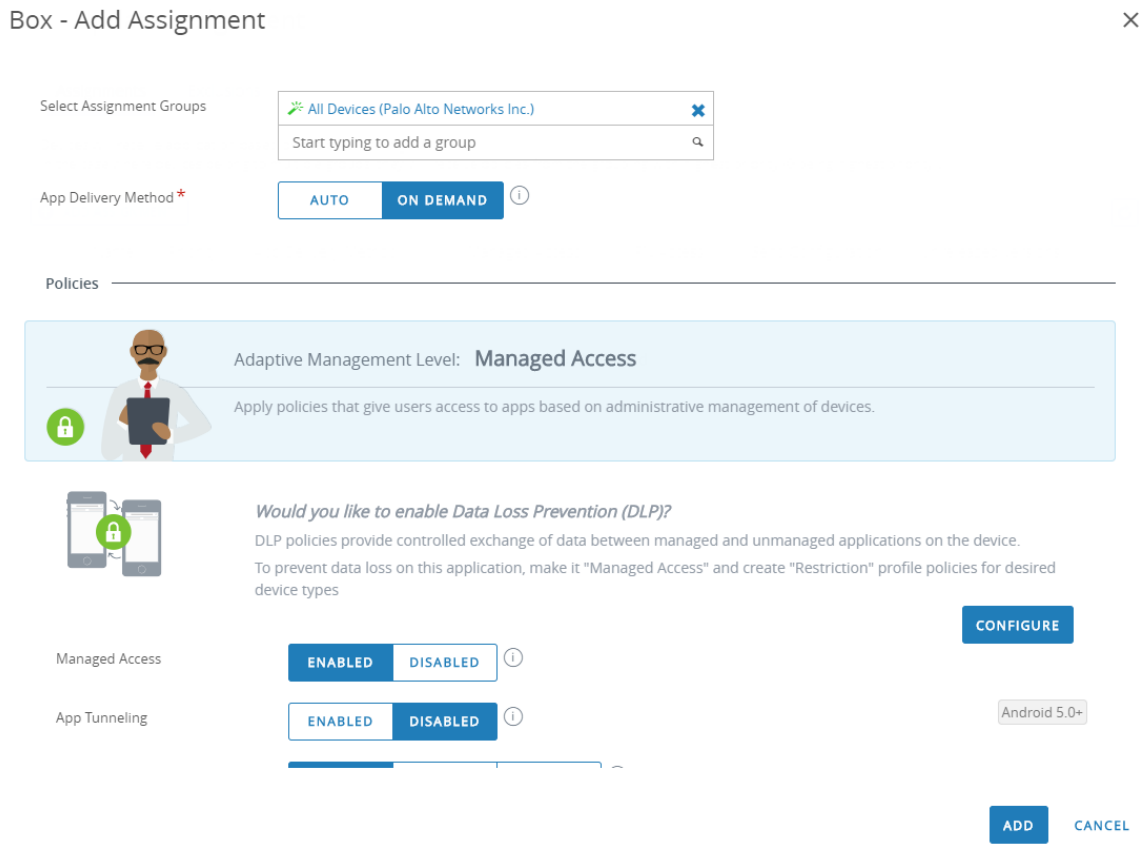




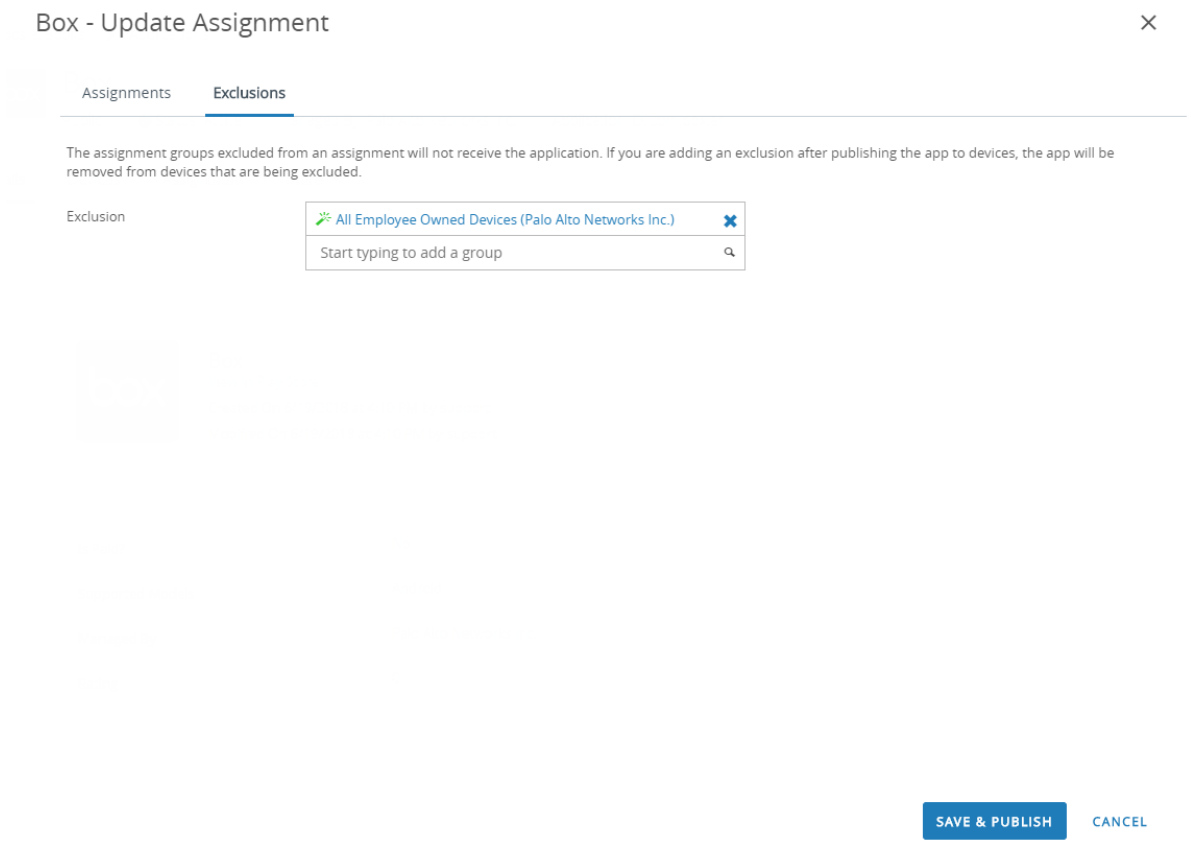
Si vous décidez d'importer l'application à partir de Google Play, sélectionnez l'application dans la liste des applications approuvées de l'entreprise, puis cliquez sur **IMPORT (Importer)**. Si vous ne voyez pas l'application dans la liste, communiquez avec votre administrateur Android for Work pour 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 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**.



11. **SAVE & PUBLISH (Enregistrez et publiez)** la configuration dans les groupes intelligents affectés.

Configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide d'AirWatch

Vous pouvez autoriser l'accès aux ressources internes à partir de vos périphériques mobiles gérés en configurant l'accès VPN GlobalProtect à l'aide d'AirWatch. 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 AIRWATCH ne répertorie pas encore GlobalProtect comme fournisseur de connexion officiel pour les points de terminaison 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.

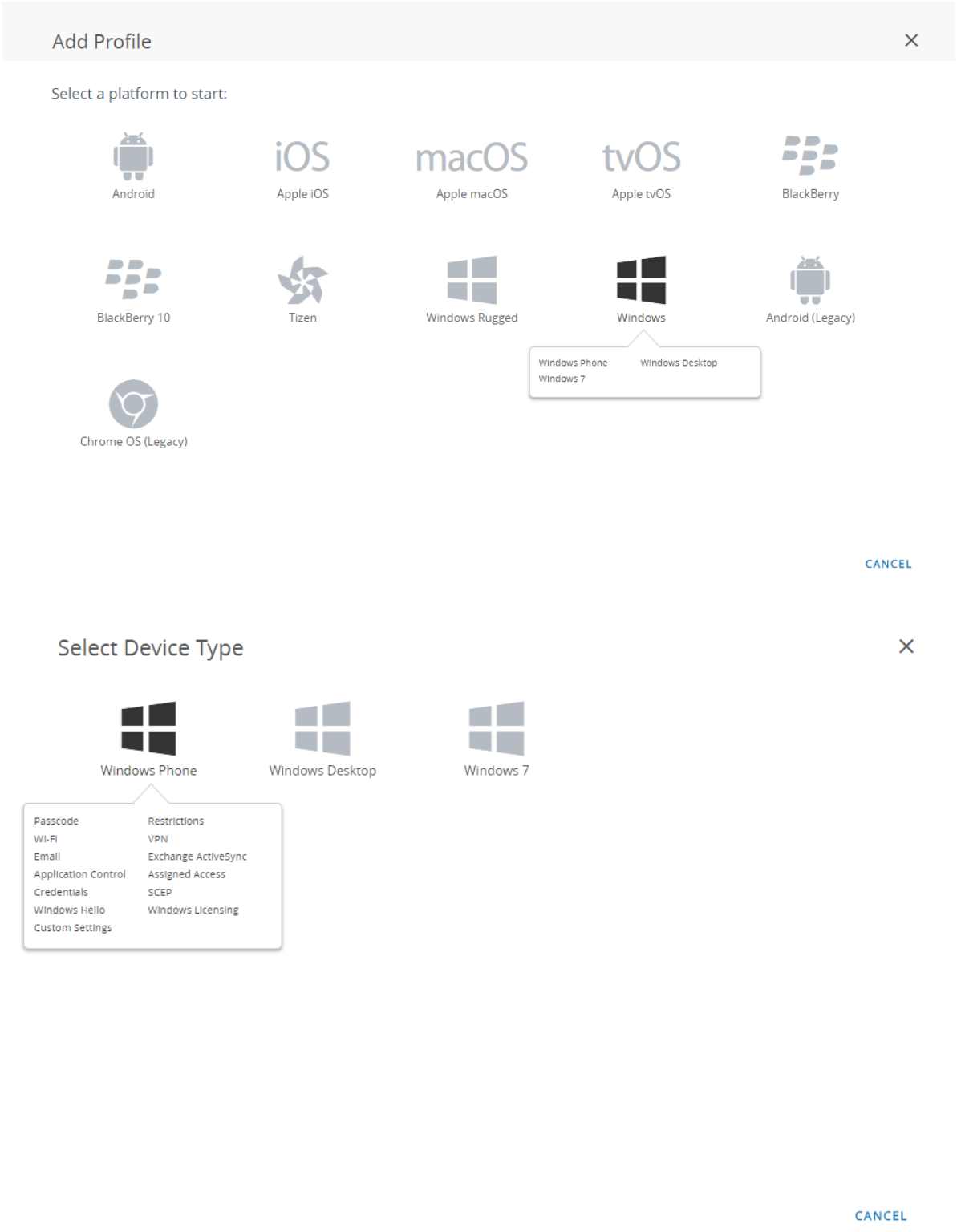
Utilisez les étapes suivantes pour configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide d'AirWatch :

STEP 1 | Téléchargez l'app GlobalProtect pour Windows 10 UWP :

- Déployez l'application mobile GlobalProtect à l'aide de AirWatch.
- Téléchargez l'application GlobalProtect directement à partir du Microsoft Store.

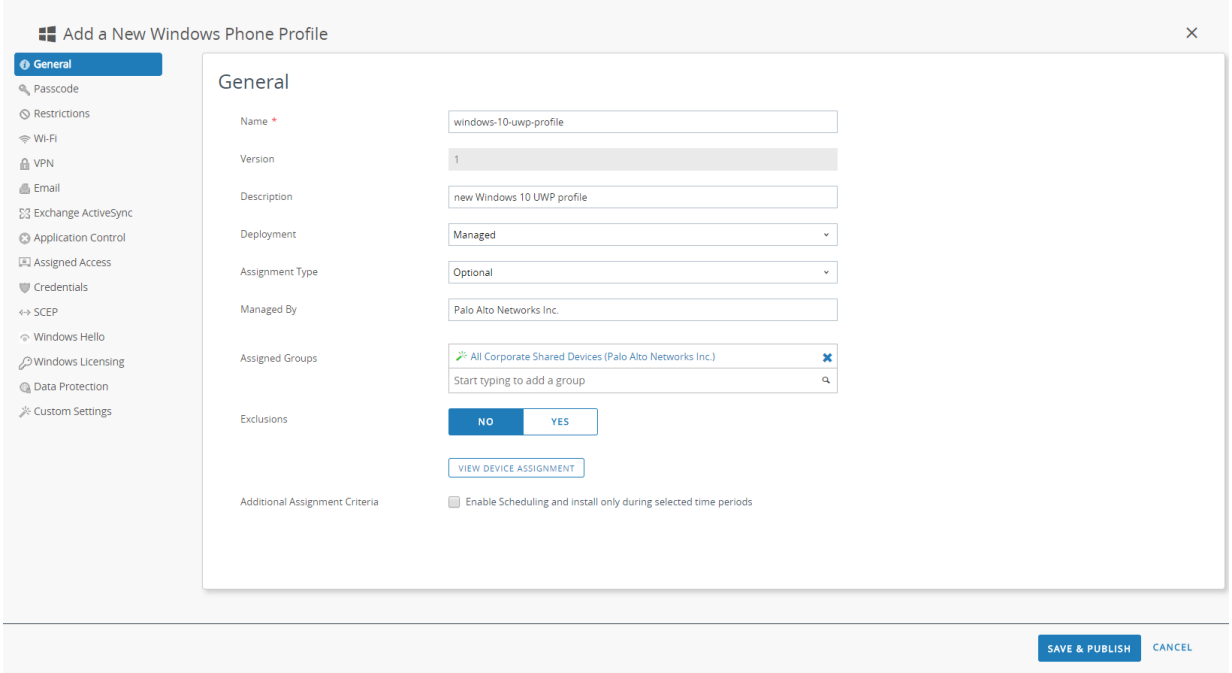
STEP 2 | Depuis la console AirWatch, modifiez un profil UWP Windows 10 existant ou ajoutez-en un nouveau.

1. Sélectionnez **Devices (Périphériques)** > **Profiles & Resources (Profils et ressources)** > **Profiles (Profils)**, puis **ADD (Ajoutez)** un nouveau profil.
2. Sélectionnez **Windows** comme plateforme et **Windows Phone** comme type de configuration.



STEP 3 | Configurez les paramètres **General (généraux)**.

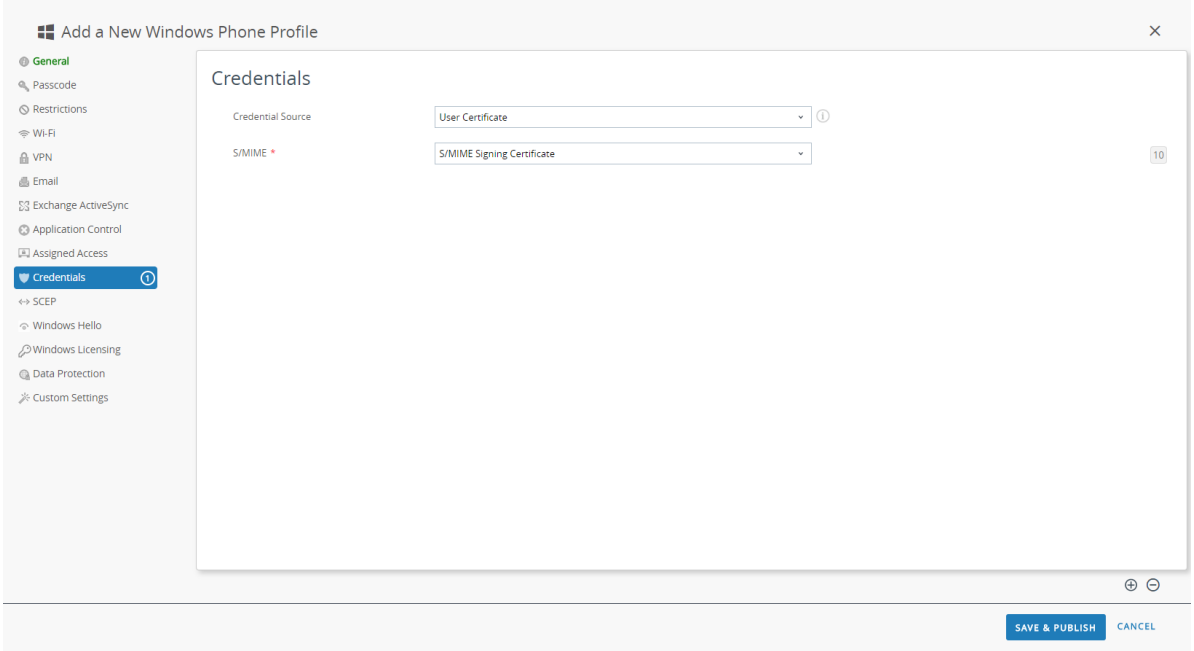
- Saisissez un **Name (Nom)** pour le profil.
- (Facultatif) Saisissez une brève **description** du profil qui indique son but.
- (Facultatif) Définissez le mode de **Deployment (Déploiement)** sur **Managed (Géré)** pour permettre la suppression automatique du profil lors de la désinscription.
- (Facultatif) 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.



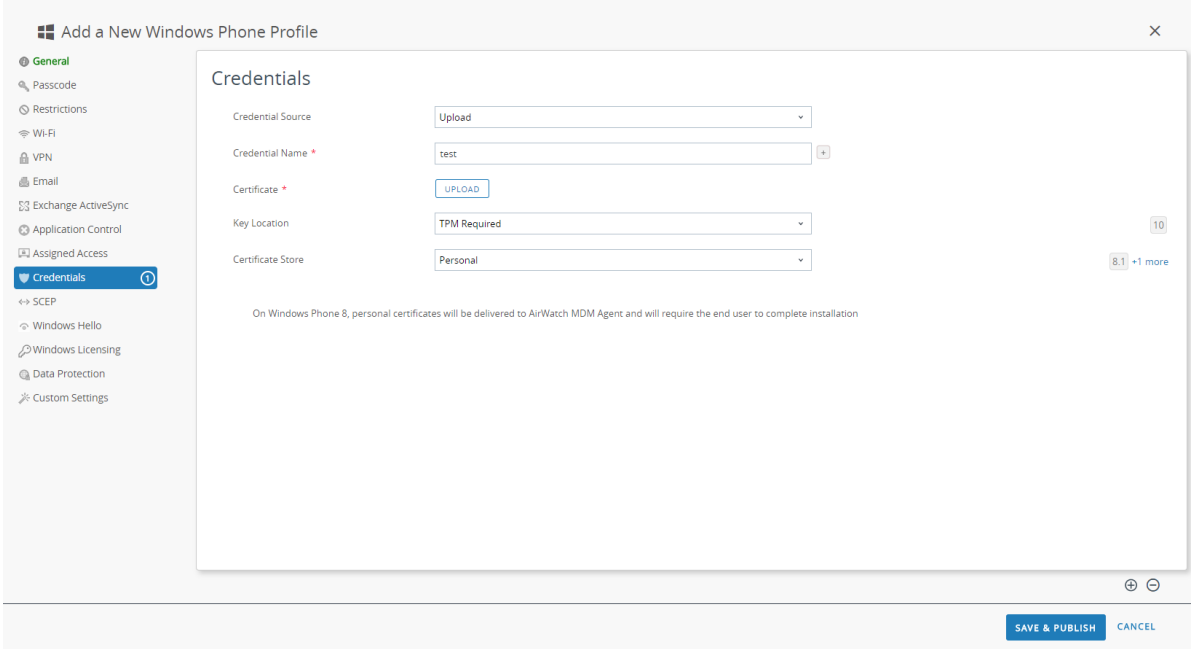
STEP 4 | Configurez les paramètres de **Credentials (Informations d'identification)** :

Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

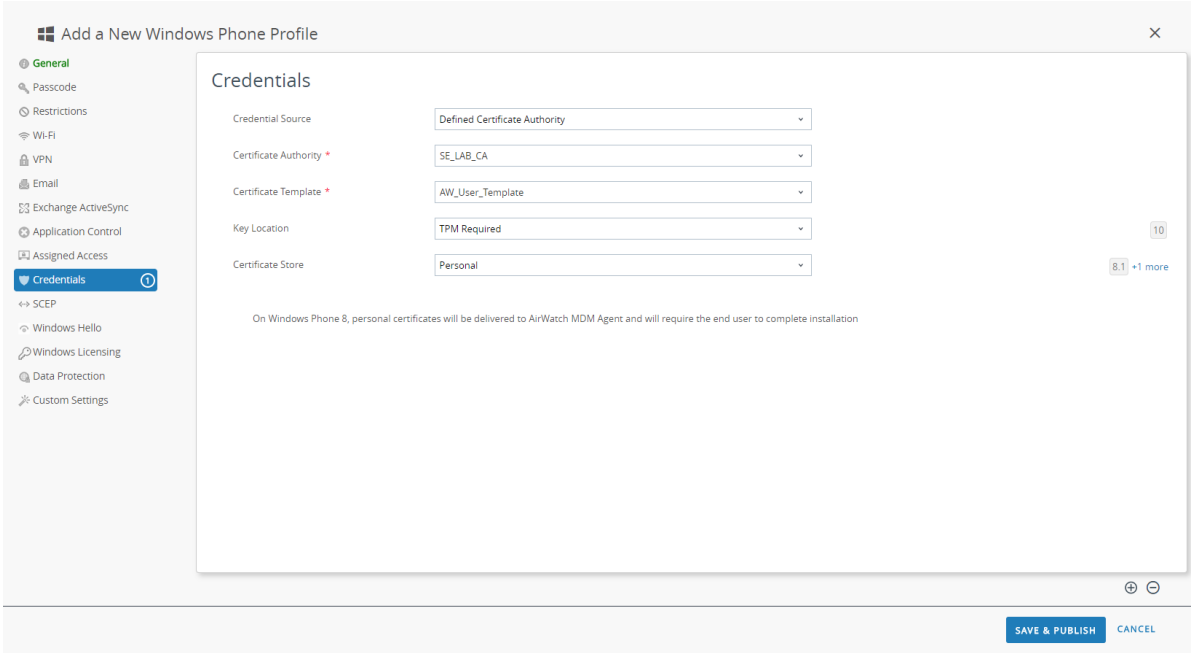
- Pour extraire les certificats de client des utilisateurs d'AirWatch :
  1. Définissez la **Credential Source (Source des informations d'identification)** sur **User Certificate (Certificat d'utilisateur)**.
  2. Sélectionnez le **S/MIME Signing Certificate (Certificat de signature S/MIME)** (par défaut).



- 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 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, l'agent AirWatch Protection doit être installé sur le point de terminaison.
  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 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, l'agent AirWatch Protection doit être installé sur le point de terminaison.
  5. Définissez la **Certificate store (Boutique des certificats)** sur **Personal (Personnel)**.

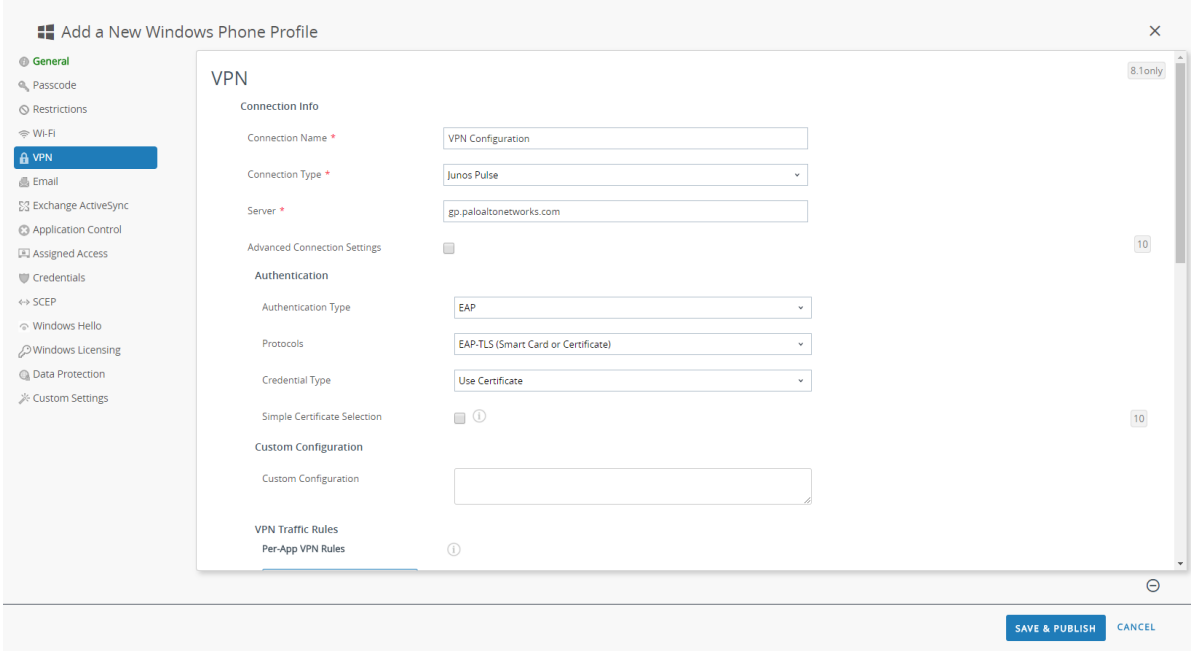


STEP 5 | Configurez les paramètres **VPN** :

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).

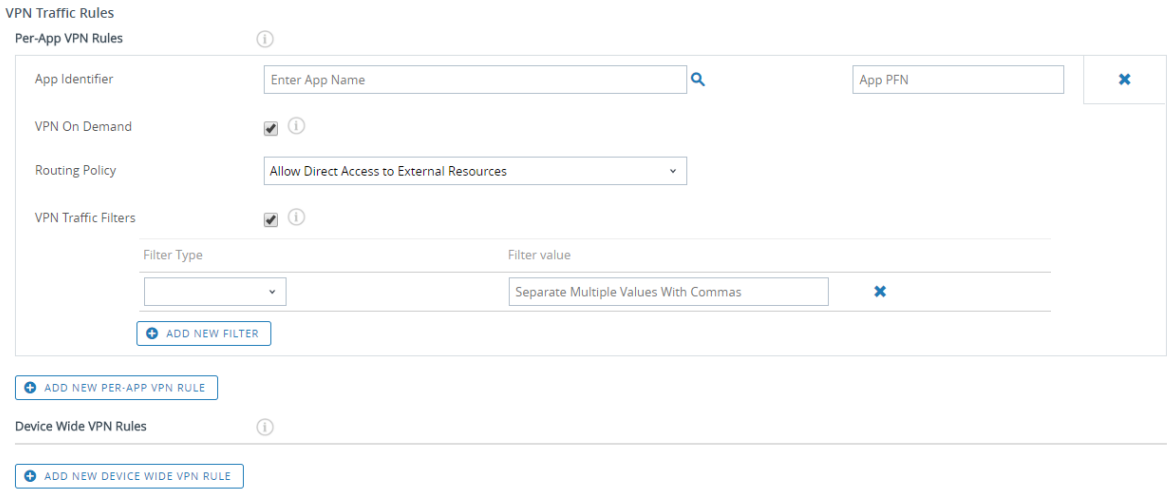
   Vous devez sélectionner un fournisseur de rechange, car AirWatch ne répertorie pas encore GlobalProtect en tant que fournisseur de connexions officiel pour les points de terminaison Windows.
3. Dans le champ **Server (Serveur)**, saisissez le nom d'hôte ou l'adresse IP du portail GlobalProtect auquel 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.
   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.

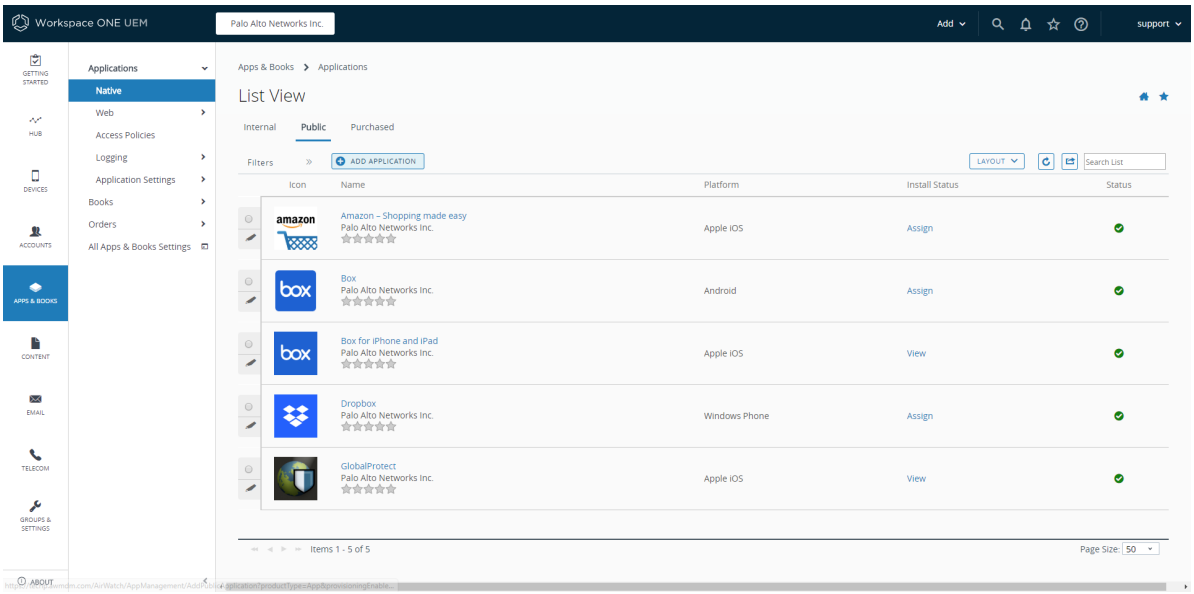


STEP 6 | **SAVE & PUBLISH (Enregistrez et publiez)** vos modifications.

STEP 7 | Configurez les paramètres VPN par application pour une nouvelle application gérée, ou modifiez les paramètres d'une application gérée existante.

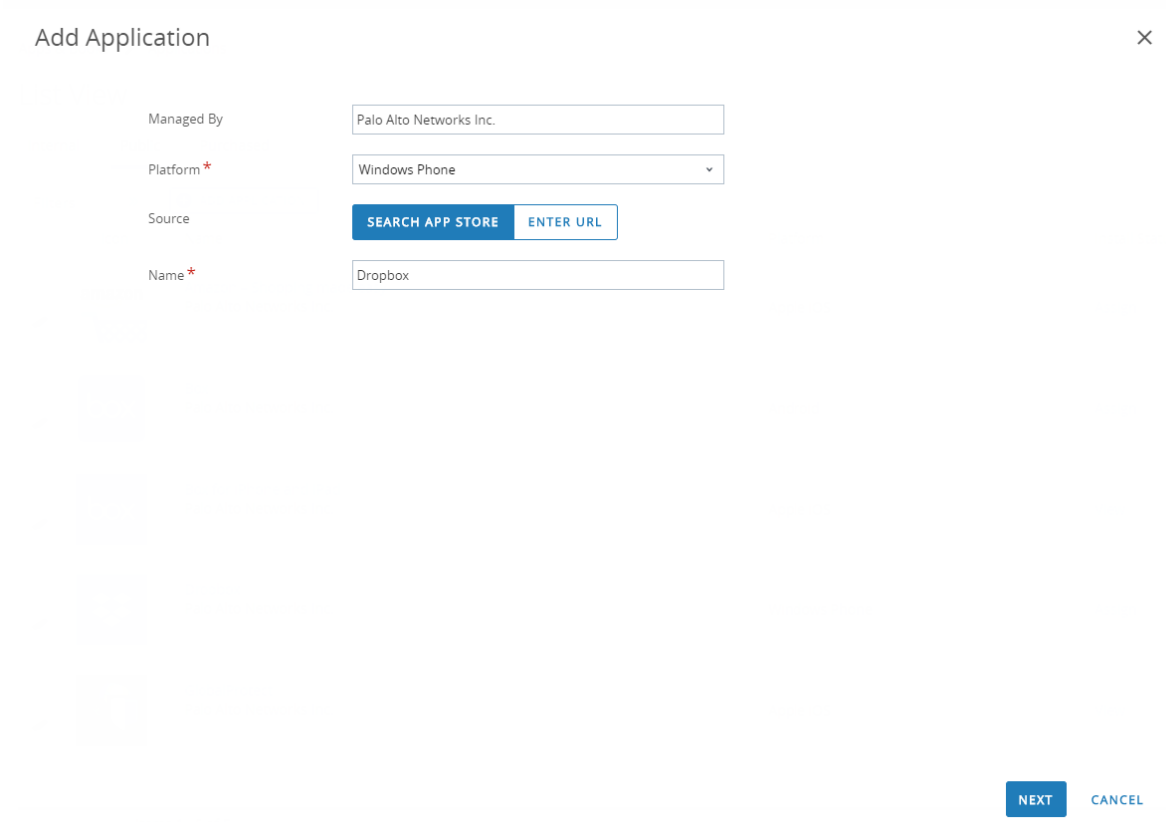
Après avoir configuré les paramètres de l'application et activé le VPN par application, vous pouvez publier l'application à un groupe d'utilisateurs et autoriser l'application à acheminer le trafic via le tunnel VPN GlobalProtect.

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 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.



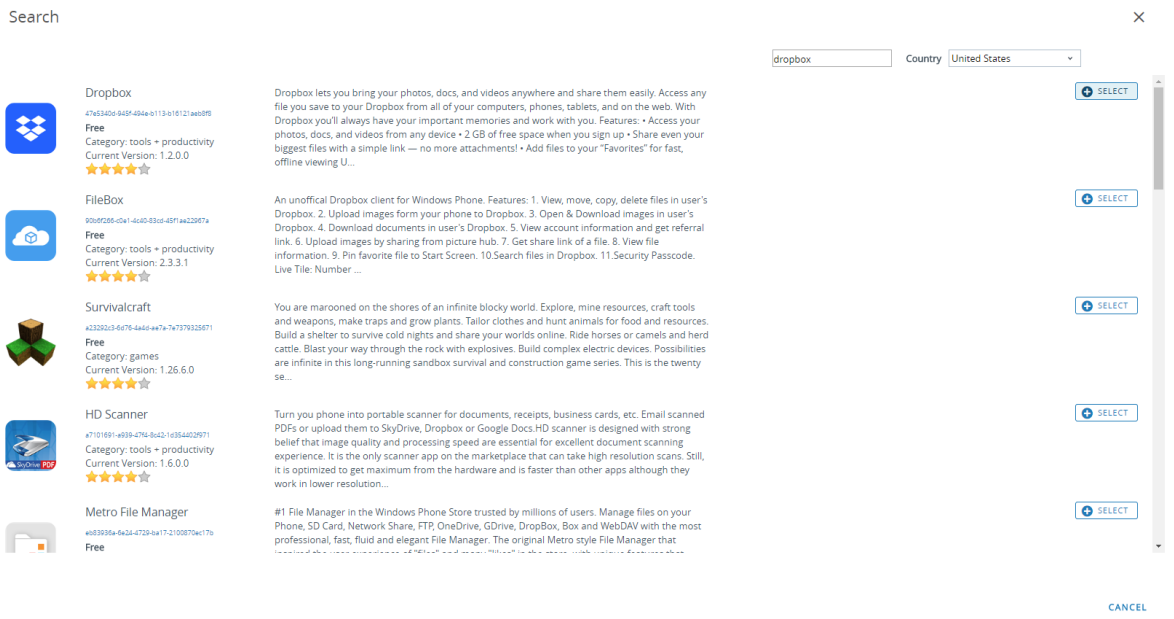
3. Dans le champ **Managed By (Géré par)**, sélectionnez le groupe de l'entreprise qui gérera cette application.
4. Définissez la **Platform (Plateforme)** sur **Windows Phone**.
5. Sélectionnez votre **Source** privilégiée pour trouver l'application :

- **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)

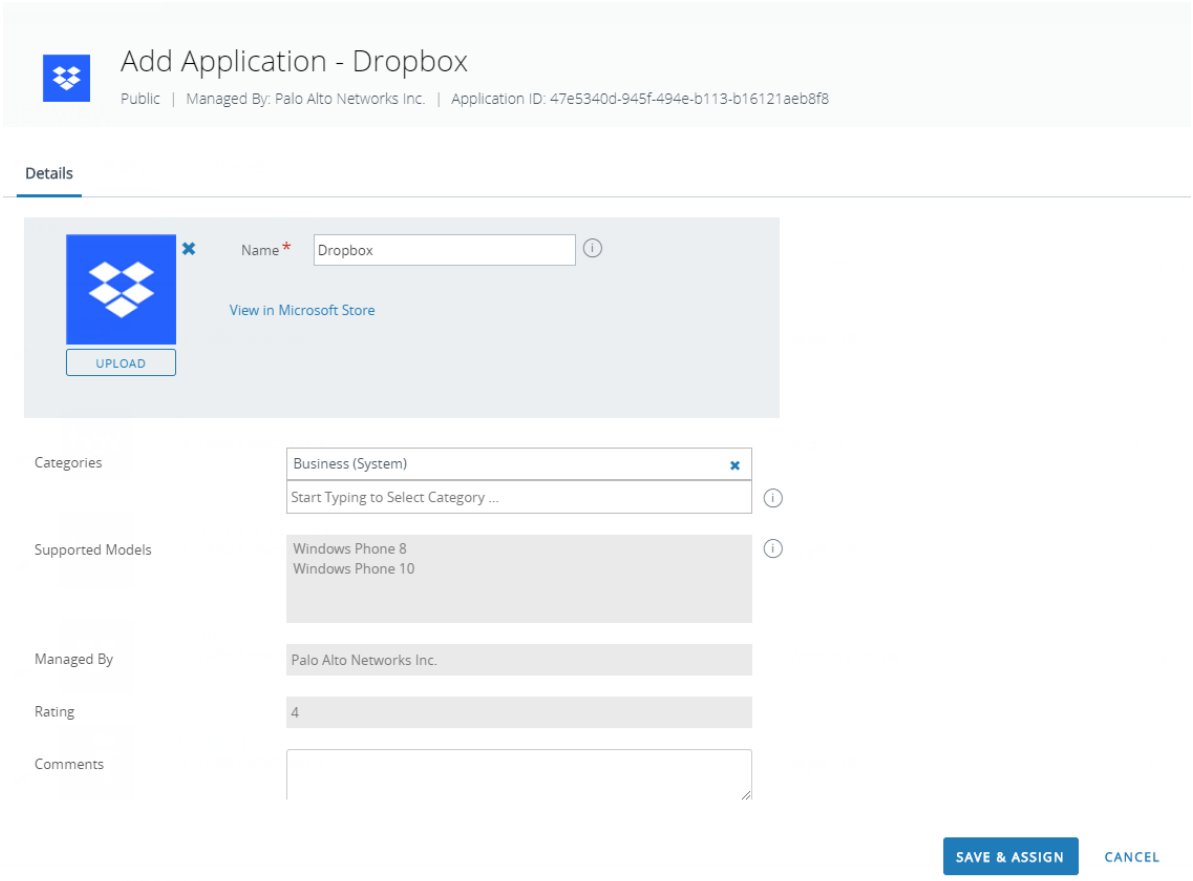


6. Cliquez sur **NEXT (Suivant)**.

   Si vous choisissez de rechercher l'application dans le Microsoft Store, **SELECT (Sélectionnez)** l'application à partir d'une liste de résultats de recherche.

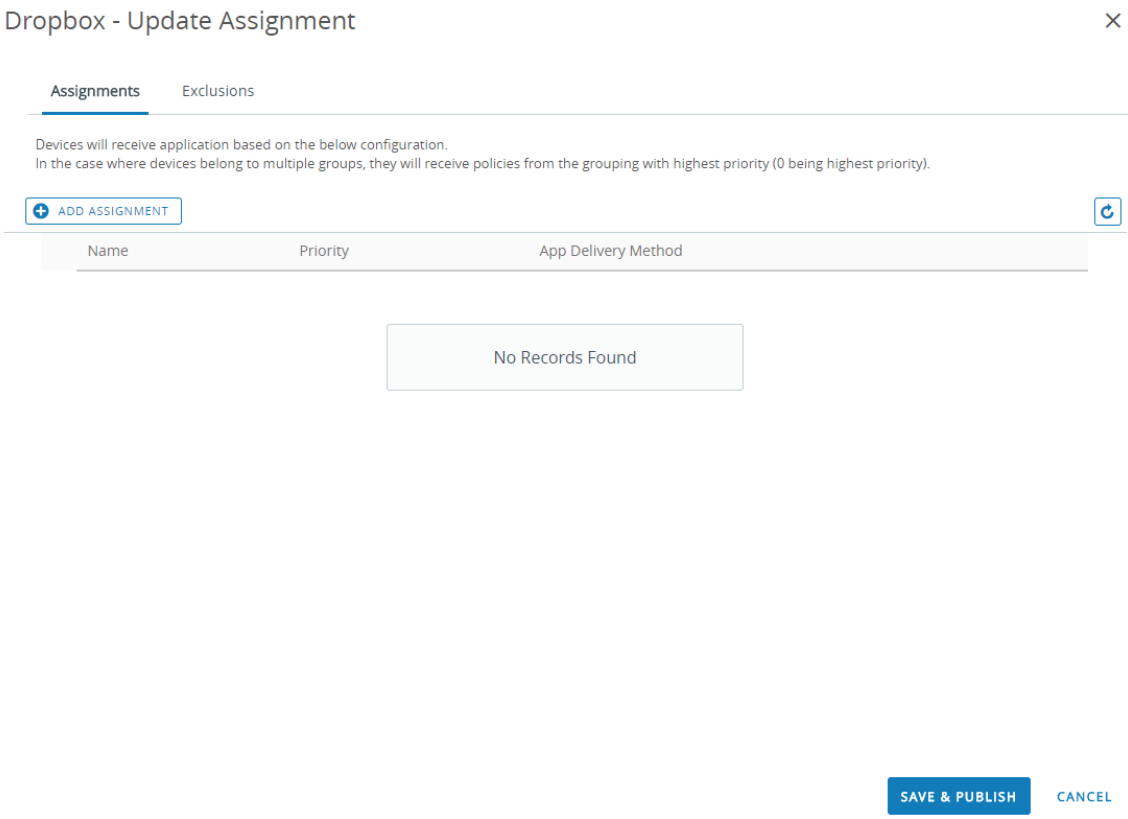


7. Sur le dialogue Add Application (Ajouter une application), assurez-vous que le **Name (Nom)** de l'application est bon. C'est le nom qui figurera dans le catalogue d'applications d'AirWatch.
8. (Facultatif) Affectez l'application à des **Categories (Catégories)** prédéfinies ou personnalisées pour faciliter l'accès dans le catalogue d'applications d'AirWatch.

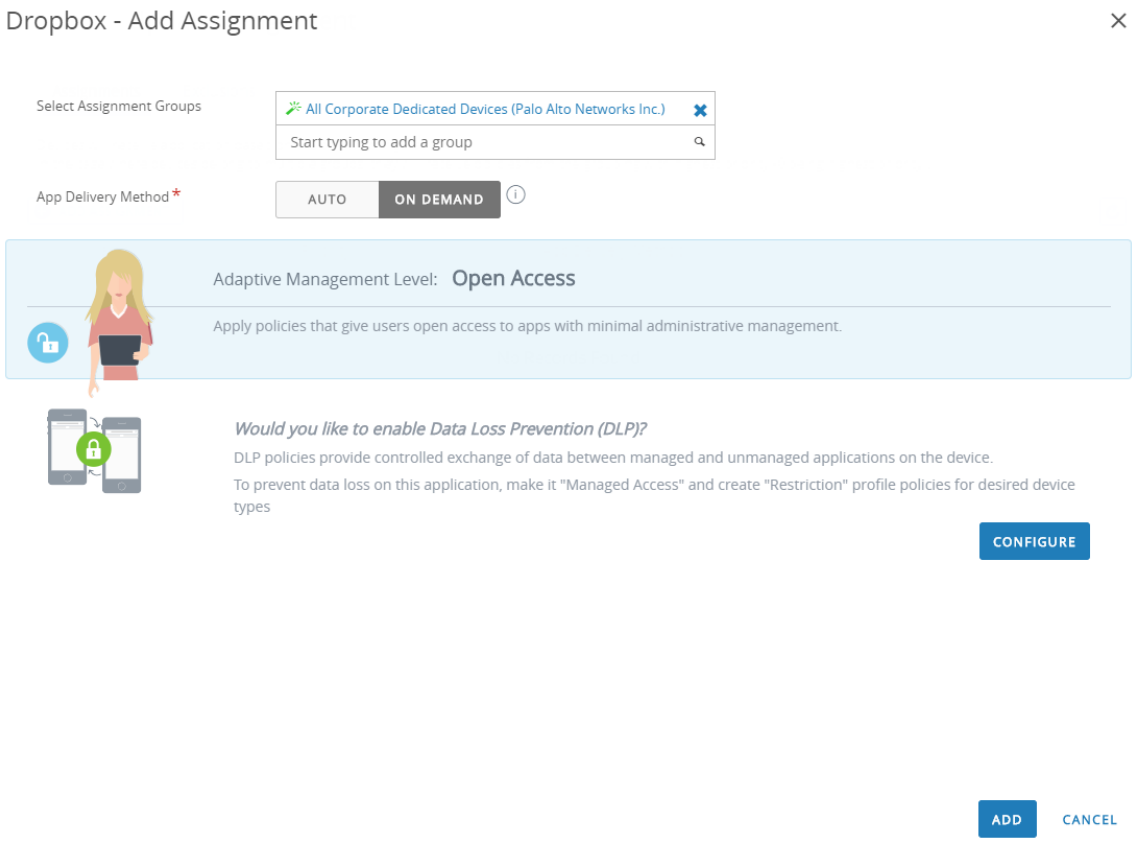


9. **SAVE & ASSIGN (Enregistrez et affectez)** la nouvelle application.

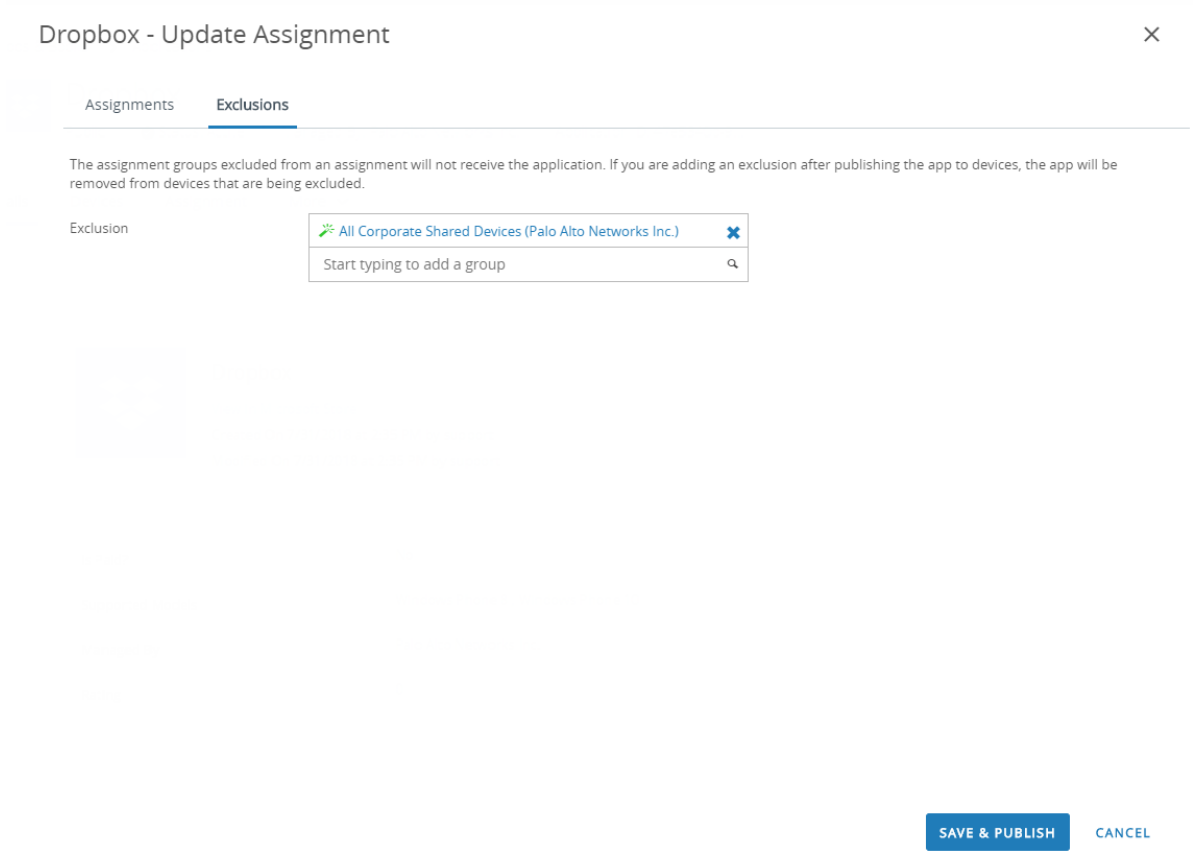
10. Dans la boîte de dialogue Update Assignment (Mise à jour de l'affectation), sélectionnez **Assignments (Affectations)**, puis cliquez sur **ADD ASSIGNMENT (Ajouter l'affectation)** pour ajouter les groupes intelligents qui auront accès à cette application.



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 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**.



12. **SAVE & PUBLISH (Enregistrez et publiez)** la configuration dans les groupes intelligents affectés.

STEP 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. AIRWATCH 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. Retour à AirWatch et, dans la **Devices(Périphériques)** > **Profiles (Profils)** > **List View (Vue de la 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.

STEP 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)**. AIRWATCH déplace le profil sur la liste inactive.

STEP 10 | Testez la configuration.

Configurer une configuration de VPN par application à l'aide de Microsoft Intune

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 offre une connexion sécurisée entre le pare-feu et les points de terminaison mobiles gérés par Microsoft Intune 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 renseignements sur la manière de configurer une configuration de VPN par application à l'aide de Microsoft Intune :

- Configurer une configuration de VPN par application sur les points de terminaison iOS à l'aide de Microsoft Intune
- Configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide de Microsoft Intune

Configurer une configuration de VPN par application sur les points de terminaison iOS à l'aide de Microsoft Intune

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 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 Microsoft Intune :

STEP 1 | Téléchargement de l'application GlobalProtect pour Android

- Déployez l'application mobile GlobalProtect à l'aide de Microsoft Intune.
- Téléchargez l'app GlobalProtect directement à partir de l'App Store.

STEP 2 | Ajoutez des applications à Microsoft Intune.

Avant de pouvoir affecter, surveiller, configurer ou protéger des applications, vous devez les ajouter à Microsoft Intune.

- Définissez le **App type** (Type d'application) sur **iOS**.
- Ajoutez des applications du magasin iOS à Microsoft Intune.

STEP 3 | Définissez des configurations VPN par application pour iOS.

- Lorsque vous créez un profil VPN par application, définissez la **Platform (Plateforme)** sur **iOS** et le **Connection type (Type de connexion)** sur **Palo Alto Networks GlobalProtect**.

- Lorsque vous associez une application au profil VPN, sélectionnez votre profil VPN par application dans le menu déroulant **VPNS**.

Configurer une configuration de VPN par application sur les terminaux UWP Windows 10 à l'aide de Microsoft Intune

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 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 :

STEP 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.

STEP 2 | Configurez un profil de certificat.

Toutes les configurations VPN par application doivent reposer sur l'authentification basée sur les certificats.

STEP 3 | Créez un nouveau profil VPN Windows 10 UWP .

- Définissez la **Platform (Plateforme)** sur **Windows 10 and later (Windows 10 et versions ultérieures)**.

STEP 4 | Configurez les paramètres de la configuration VPN par application pour les points de terminaison 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 **Associez WIP ou des applications à ce VPN** sur **Associate apps with this connection (Associez 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.

Configurer une configuration de VPN par application à l'aide de MobileIron

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.

Reportez-vous à la section suivante pour obtenir des renseignements sur la manière de configurer une configuration de VPN par application à l'aide de MobileIron :

- Configurer une configuration de VPN par application sur les points de terminaison iOS à l'aide de MobileIron

Configurer une configuration de VPN par application sur les points de terminaison iOS à l'aide de MobileIron

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 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 :

STEP 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.

STEP 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.

STEP 3 | Ajoutez une configuration de VPN par application.

- Définissez le type de configuration sur **Per-app VPN (Configuration VPN par application)**.

STEP 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.

Activer l'intégration de l'analyse d'application avec WildFire

En activant App Scan dans AirWatch, vous pouvez tirer parti de l'intelligence de menaces WildFire® sur les applications pour détecter les logiciels malveillants sur les points d'extrémité Android. Lorsqu'il est activé, l'agent AirWatch envoie la liste des applications qui sont installées sur le point d'extrémité Android vers AirWatch. Cela se produit lors de l'inscription et par la suite sur tout enregistrement de point de terminaison. AirWatch interroge périodiquement WildFire pour les verdicts et peut prendre des mesures de conformité sur le point de terminaison en fonction du verdict.

STEP 1 | Avant de commencer, procurez-vous une clé API Wildfire. Si vous n'avez pas déjà une clé API, contactez le support.

STEP 2 | AirWatch, sélectionnez **Groups & Settings (Groupes et paramètres)** > **All Settings (tous les paramètres)** > **Apps (Applications)** > **App Scan (Scan d'applications)** > **Third Party Integration (intégration de tierce partie)**.

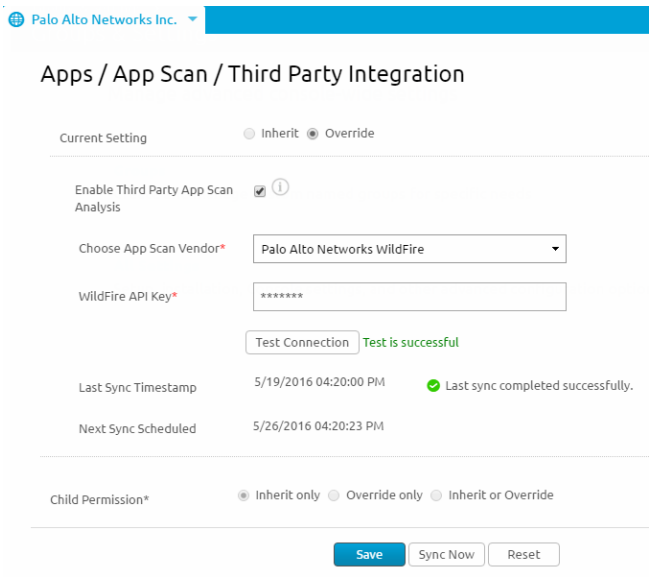
STEP 3 | Sélectionnez le **Current Setting (réglage actuel)** : Override (Substituer).

STEP 4 | Sélectionnez **Enable Third Party App Scan Analysis (Activer l'Analyse de scan d'une application tierce)** pour permettre la communication entre AirWatch et WildFire.

STEP 5 | Choisissez **Palo Alto Networks WildFire** à partir du menu déroulant **Choose App Scan Vendor (Choisir la recherche d'analyse d'application)**.

STEP 6 | Saisissez votre clé API Wildfire.

STEP 7 | Cliquez sur **Test Connection (Tester la connexion)** pour vous assurer qu'AirWatch peut communiquer avec WildFire. Si le test n'est pas réussi, vérifiez la connectivité à Internet, saisissez de nouveau la clé API, puis réessayez.



STEP 8 | Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications. AirWatch 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.

Supprimer les notifications sur l'application GlobalProtect pour les terminaux macOS

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 de charger automatiquement l'extension de noyau ou l'extension système sans recevoir de notification, vous pouvez utiliser le Mobile Device Management (gestion des appareils mobiles - MDM) du périphérique mobile, comme Airwatch, afin de créer une politique applicable à cette extension.

Reportez-vous aux sections suivantes pour obtenir des renseignements sur la suppression des notifications sur l'application GlobalProtect pour les terminaux macOS :

- Activer les extensions de noyau dans l'application GlobalProtect pour les terminaux macOS
- Activer les extensions de système dans l'application GlobalProtect pour les terminaux macOS

Activer les extensions de noyau dans l'application GlobalProtect pour les terminaux macOS

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.

Le flux de production suivant a été testé à l'aide d'Airwatch.

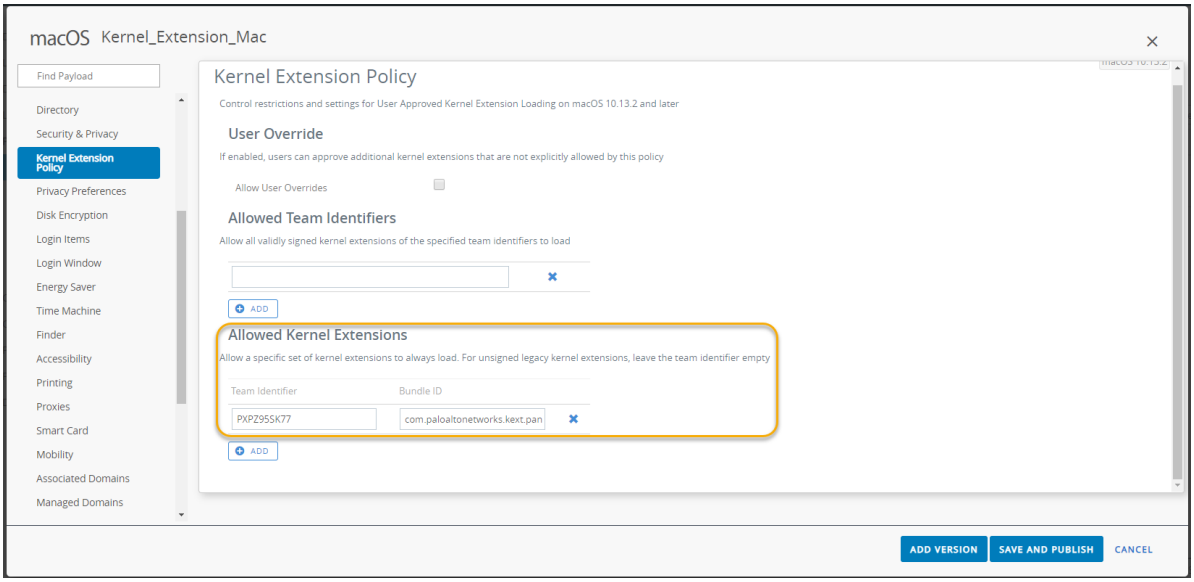
STEP 1 | Créer une politique d'extension de noyau.

1. Connectez-vous à AirWatch en tant qu'administrateur.
2. Sélectionner **Devices Appareils** > **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.

STEP 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

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.

Suivez les étapes suivantes pour configurer un profil qui permet l'approbation automatique de l'extension système au moyen d'AirWatch. Cette configuration a été testée avec AirWatch. Vous pouvez toutefois utiliser n'importe quel fournisseur MDM qualifié pour créer et mettre en œuvre ce profil.

STEP 1 | Créez un profil d'extension système.

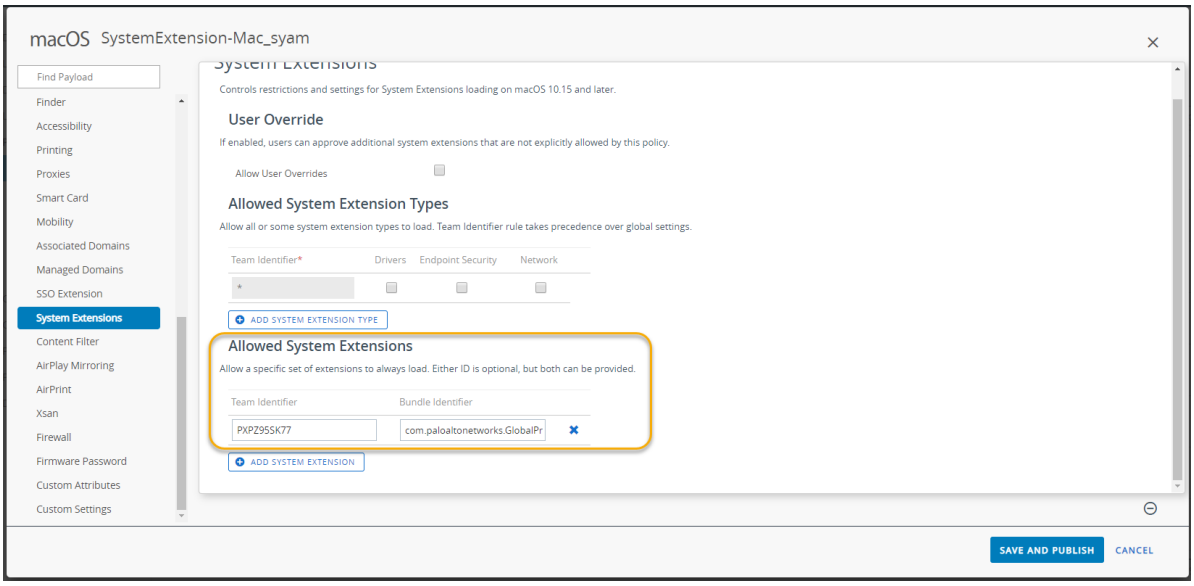
1. Connectez-vous à AirWatch en tant qu'administrateur.
2. Sélectionner **Devices Appareils** > **Profils et ressources** > **Profils**, puis sélectionnez **Ajouter** > **Ajouter le profil** à partir de la liste déroulante.
3. Dans la zone **Ajouter le profil**, cliquez sur **Apple macOS**, puis cliquez 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.

STEP 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

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

Configuration de l'application GlobalProtect pour iOS

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 :

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.vpn**
Serveur	Nom d'hôte ou adresse IP du portail GlobalProtect.	**<nom d'hôte ou adresse IP>** 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 : • Toujours établir une connexion • Ne jamais établir de connexion • Établir une connexion au besoin	**<domaine et nom d'hôte et action à la demande>** Par exemple : `gp.acme.com; Never establish`

Exemple : Configuration de VPN au niveau périphérique de l'application iOS GlobalProtect

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.

```
<?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>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample Device Level VPN)</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</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

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.

```
<?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>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample App Level VPN)</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>
</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

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.

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 la liste d'autorisation ou la liste de blocage, puis poursuivez avec une panoplie de noms d'applications séparés par un point-virgule. La liste d'autorisation indique les applications qui utiliseront le tunnel VPN pour la communication réseau. Le trafic	`allow list | block list: com.google.calendar; com.android.email; com.android.chrome`

Clé	Type de valeur	Description	Exemple
		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	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**

Exemple : Paramétrer la configuration VPN

```
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(this),
"com.paloaltonetworks.globalprotect", config);
```

Exemple : Supprimer la configuration VPN

```
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);
```

GlobalProtect pour les périphériques IoT

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.

- GlobalProtect pour les besoins IoT
- Configuration des portails et des passerelles GlobalProtect pour les périphériques 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

GlobalProtect pour les besoins IoT

GlobalProtect pour les périphériques IoT a les exigences suivantes :

- Accès Prisma ou abonnement à GlobalProtect
- Le pare-feu est doté de PAN-OS 9.1 (mettre à jour dès maintenant)
- L'un des systèmes d'exploitation suivants :
  - Android
  - Raspbian
  - Ubuntu
  - Windows 10 IoT Entreprise
- Mémoire de 128 Mo
- 4 Go de stockage
- Processeur x86 et ARMv7 ou ARMv5
- Installation à l'aide des packages snap à partir de la CLI ou de WebDM

Configuration des portails et des passerelles GlobalProtect pour les périphériques IoT

STEP 1 | Passez en revue les GlobalProtect pour les besoins IoT

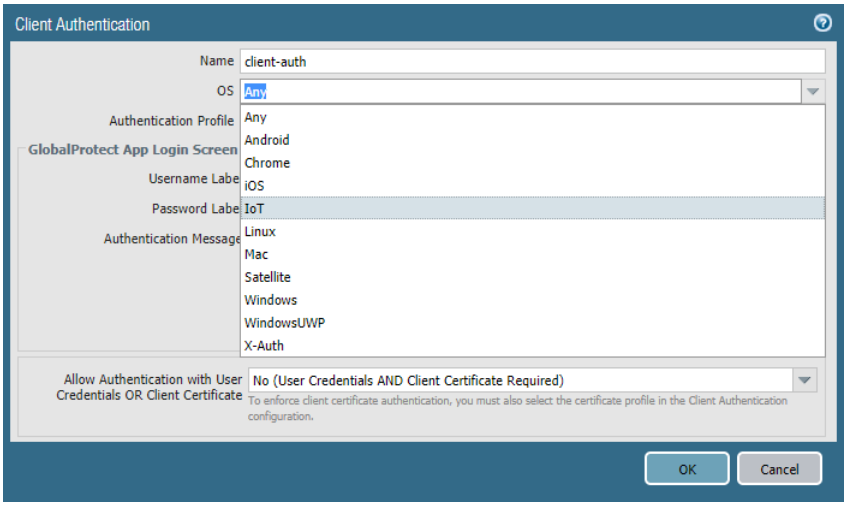
STEP 2 | Configurez vos passerelles GlobalProtect pour qu'elles prennent en charge l'application GlobalProtect pour IoT.

1. Effectuez les tâches préalables à la configuration de la passerelle 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 pouvez configurer l'utilisation à deux facteurs sur les terminaux Windows et macOS et l'authentification basée sur des certificats pour les périphériques IoT.

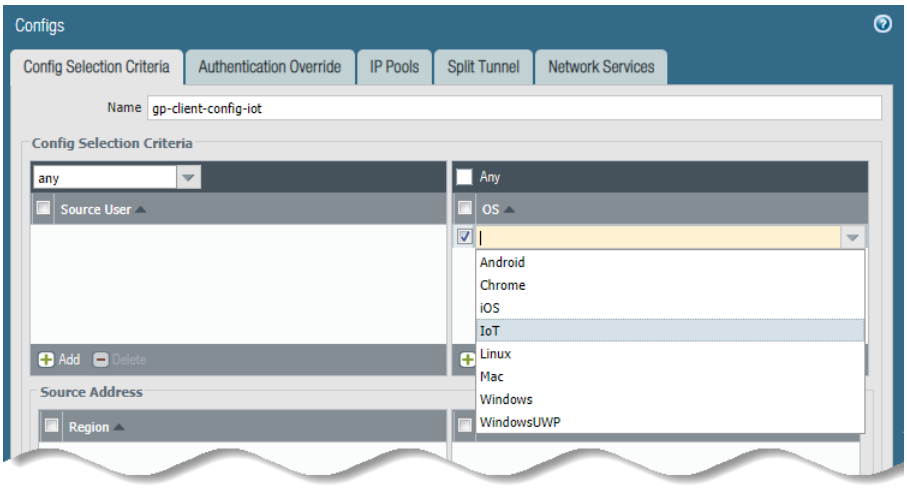
   Vous pouvez également configurer les paramètres réseau et client pris en charge (comme les pools d'adresses IP, les itinéraires d'accès et la séparation des tunnels) pour les périphériques IoT.

   1. Sélectionnez **Réseau** > **GlobalProtect** > **Passerelles**, puis sélectionnez ou **Ajoutez** 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 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**.



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

STEP 3 | 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.
2. Définissez les paramètres du client pour que les périphériques IoT s'authentifient auprès du portail.
    1. Sélectionnez **Réseau** > **GlobalProtect** > **Portails**, puis sélectionnez une configuration du 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 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.

STEP 4 | 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

Installation GlobalProtect pour IoT sur Android

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.

STEP 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.

STEP 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;
    }
}
```

STEP 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();
}
```

STEP 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/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`.

STEP 5 | Créez un fichier APK GlobalProtect.

STEP 6 | Signez le fichier APK GlobalProtect.

STEP 7 | Transmettez le nouveau système d'exploitation aux périphériques Android dans l'image système, puis transmettez le nouveau système d'exploitation aux périphériques Android.

Installation GlobalProtect pour IoT sur Raspbian

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.

STEP 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.

STEP 2 | Installez l'application GlobalProtect pour IoT.

À partir du périphérique IoT, 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`**.*

STEP 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 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>       //pre-deployed portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
         <portal-timeout>5</portal-timeout>
         <connect-timeout>5</connect-timeout>
         <receive-timeout>30</receive-timeout>
```

```
        <os-type>IoT</os-type>              //pre-deployed OS type for IoT.
 If this tag does not present, GP will automatic detect the OS type.
        <head-less>yes</head-less>       //pre-deployed head-less mode
        <username>abc</username>    //optional pre-deployed username
        <password>xyz</password>       //optional pre-deployed password
        <client-cert-path>cli_cert_path</client-cert-path>       //optional
 pre-deployed client certificate file(p12) path
        <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase>       //optional pre-deployed client certificate passphrase file
 path
        <log-path-service>/tmp/gps</log-path-service>  //optional pre-
deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional pre-
deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | Recommencez le processus GlobalProtect pour que la configuration de prédéploiement prenne effet.

STEP 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
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 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.

Installation GlobalProtect pour IoT sur Ubuntu

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.

STEP 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.

STEP 2 | Installez l'application GlobalProtect pour IoT.

À partir du périphérique IoT, utilisez la commande **`sudo dpkg -i GlobalProtect_deb-<version>.deb`** pour installer le logiciel.

```
user@linuxhost:~$ sudo dpkg -i GlobalProtect_deb-4.1.0.0-19.deb
```

*Pour désinstaller le logiciel, utilisez la commande **`sudo dpkg -P globalprotect`**.*

STEP 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 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>       //pre-deployed portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
         <portal-timeout>5</portal-timeout>
         <connect-timeout>5</connect-timeout>
         <receive-timeout>30</receive-timeout>
         <os-type>IoT</os-type>              //pre-deployed OS type for IoT.
 If this tag does not present, GP will automatic detect the OS type.
         <head-less>yes</head-less>       //pre-deployed head-less mode
```

```
        <username>abc</username>    //optional pre-deployed username
        <password>xyz</password>       //optional pre-deployed password
        <client-cert-path>cli_cert_path</client-cert-path>       //optional
 pre-deployed client certificate file(p12) path
        <client-cert-passphrase>cli_cert_passphrase_path< /client-cert-
passphrase>       //optional pre-deployed client certificate passphrase file
 path
        <log-path-service>/tmp/gps</log-path-service>  //optional pre-
deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional pre-
deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | Recommencez le processus GlobalProtect pour que la configuration de prédéploiement prenne effet.

STEP 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
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 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.

Installation GlobalProtect pour IoT sur Windows

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.

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.

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

Informations sur l'hôte

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. La fonction 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.

Les sections suivantes fournissent des informations sur l'utilisation des informations sur l'hôte pour la mise en œuvre d'une politique :

- À propos des informations sur l'hôte
- Configurer la mise en œuvre des politiques basées sur HIP
- Collecter des données d'application et de processus sur des points de terminaison
- Redistribution des rapports HIP
- Bloquer l'accès aux périphériques
- Configurer l'agent User-ID Windows pour collecter des informations d'hôte

À propos des informations sur l'hôte

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.

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 ?
- Comment la passerelle utilise-t-elle les informations sur l'hôte pour la mise en œuvre des politiques ?
- De quelle manière les utilisateurs savent-ils si leurs systèmes sont conformes ?
- Comment obtenir une visibilité de l'état des points de terminaison ?

Quelles sont les données que l'application GlobalProtect collecte ?

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.

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.

L'application collecte par défaut des données sur les catégories d'informations suivantes pour permettre d'identifier l'état de sécurité de l'hôte :

Table 8: 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*

Catégorie	Données collectées
	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 AirWatch.* Pour les périphériques gérés par AirWatch, les informations sur l'hôte collectées par l'application GlobalProtect peuvent être complétées par des informations supplémentaires collectées auprès du service AirWatch. Reportez-vous à la section Configure Windows User-ID Agent to Collect Host Information (Configurer l'agent User-ID Windows pour collecter des informations d'hôte) pour connaître une liste d'attributs qui peuvent être récupérés à partir d'AirWatch.
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 (Objects (Objets) > GlobalProtect > HIP Objects (Objets HIP) > <hip-object> (objet HIP) > Patch Management (Gestion des correctifs) > Criteria (Critère)), utilisez les mappages suivants entre les valeurs de gravité GlobalProtect et les cotes de gravité pour comprendre la signification de chacune des cotes :* • ***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.

Catégorie	Données collectées
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 peut détecter les informations sur le **Anti-Malware (Antivirus)** suivantes pour la fonctionnalité de sécurité Gatekeeper sur les points de terminaison MacOS :* • *Version du moteur* • *Version de la définition* • *Date* • *Dernier balayage*
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.
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) 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 (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > *<portal-config> (configuration du portail)* > **Agent** > *<agent-config> (configuration de l'agent)* > **Data Collection (Collecte de données)**). 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 points de terminaison, 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 la liste des applications installées sur les points de terminaison qui ne sont pas gérés par un gestionnaire tiers des périphériques mobiles.

Comment la passerelle utilise-t-elle les informations sur l'hôte pour la mise en œuvre des politiques ?

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.

De quelle manière les utilisateurs savent-ils si leurs systèmes sont conformes ?

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 ?

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 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.

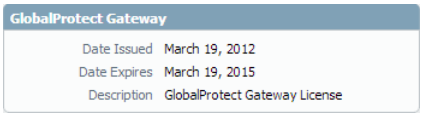
Étant donné qu'un log de correspondances HIP n'est généré que lorsque l'état de l'hôte correspond à un objet HIP que vous avez créé, pour obtenir une visibilité complète de l'état du point de terminaison, vous devrez peut-être créer plusieurs objets HIP afin de journaliser les correspondances HIP de 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

Pour autoriser l'utilisation des informations sur l'hôte pour la mise en œuvre d'une politique, vous devez exécuter les étapes suivantes. Pour plus d'informations sur la fonction HIP, reportez-vous à la section informations sur l'hôte.

STEP 1 | Vérifiez que les licences sont appropriées pour les vérifications HIP.

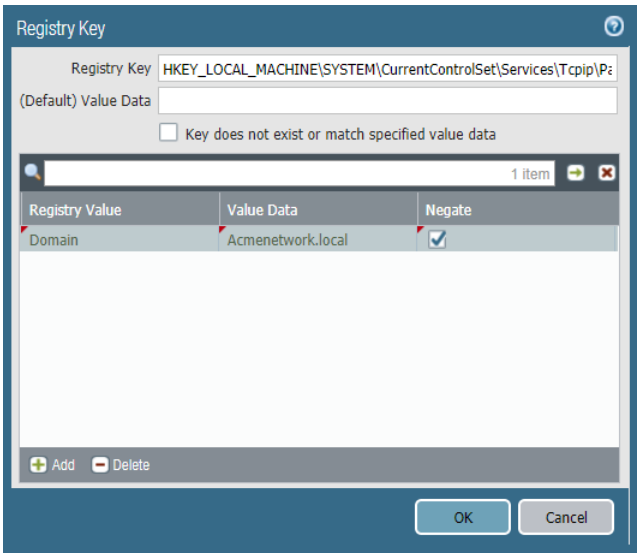


Pour utiliser la fonction HIP, vous devez acheter et installer une licence d'abonnement à GlobalProtect sur chaque passerelle qui effectuera des vérifications HIP. Pour vérifier le statut de vos licences sur chaque portail et passerelle, sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.

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 GlobalProtect licences.

STEP 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 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.*



1. Sur le pare-feu qui héberge votre portail GlobalProtect, 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 **Data Collection (Collecte de données)**, 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** ou **Mac**), puis **Add (Ajoutez)** un processus à la **Process List (Liste des processus)**. Saisissez le nom du processus sur lequel vous souhaitez que l'application collecte des informations.
   - **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. **Commit (Validez)** les modifications.

STEP 3 | (Facultatif) Excluez des catégories de la collecte.

1. Sur le pare-feu qui héberge votre portail GlobalProtect, sélectionnez **Network (Réseau)** > **GlobalProtect (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.
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. **Commit (Validez)** les modifications.

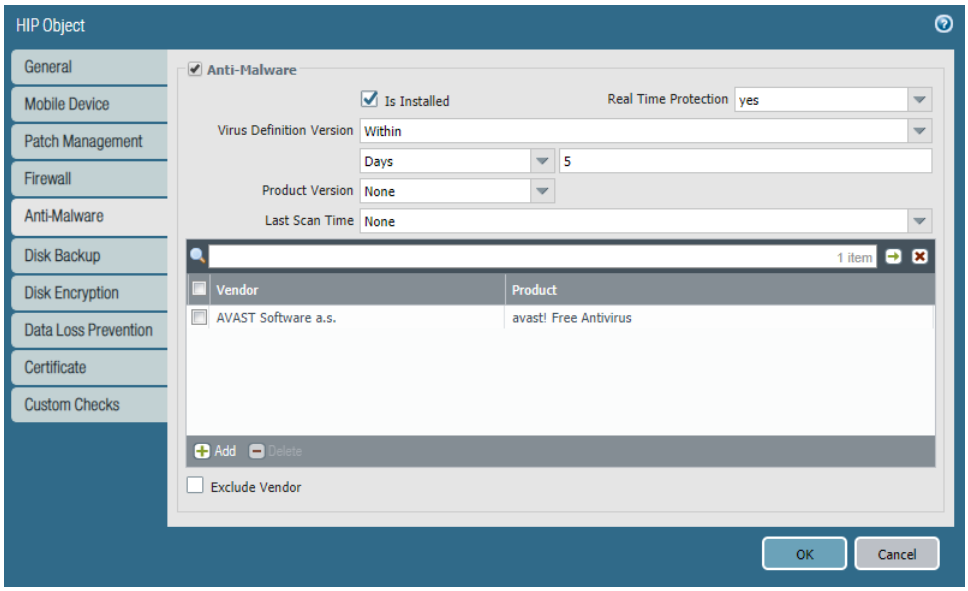
STEP 4 | Créez les objets HIP pour filtrer les données brutes d'hôte collectées par l'application.

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 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. 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 **Objets** > **GlobalProtect** > **Objets HIP**, puis **Ajoutez** un nouvel 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 **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 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.

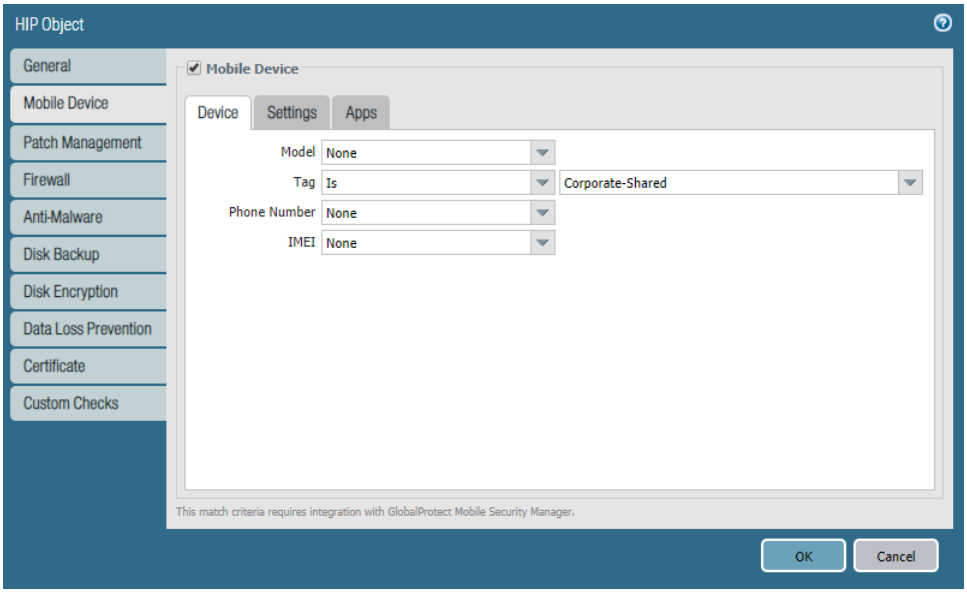
1. Cochez la case **Mobile Device (Périphérique mobile)** pour activer la configuration des paramètres du **Mobile Device (Périphérique mobile)**.
2. À l'onglet **Device (Périphérique)**, sélectionnez un opérateur de correspondance (comme **Contains (Contient)** ou **Is Not (N'est pas)**) dans la liste 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)`**



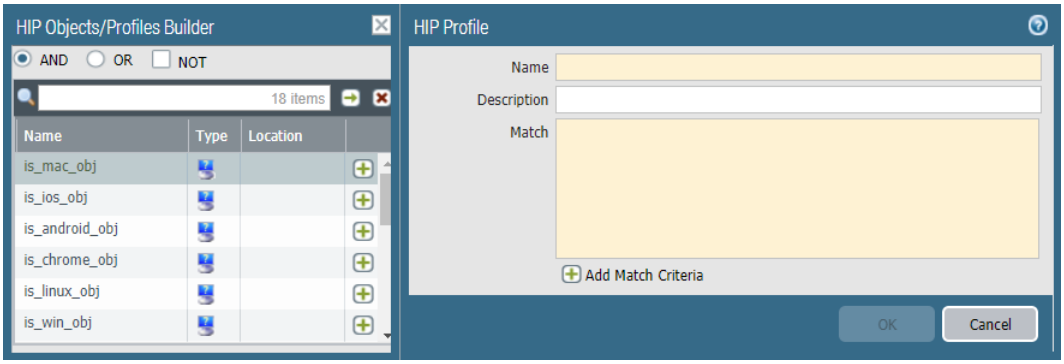
5. Cliquez sur **OK** pour enregistrer l'objet HIP.
6. Répétez ces étapes pour créer chaque objet HIP supplémentaire dont vous avez besoin.
7. **Commit (Validez)** les modifications.

STEP 5 | Créez les profils HIP que vous envisagez d'utiliser dans vos stratégies.

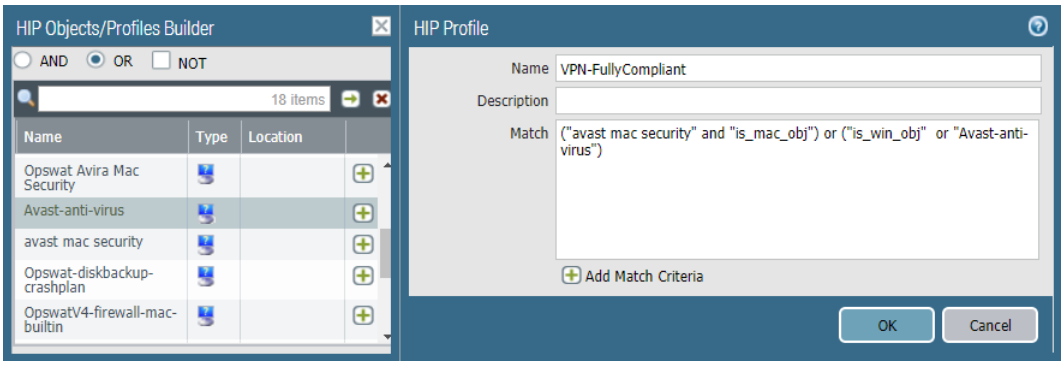
Lors de la création de profils HIP, vous pouvez combiner des objets HIP précédemment créés (ainsi que d'autres profils HIP) à l'aide d'une logique booléenne, notamment lorsqu'un flux de trafic est évalué en fonction d'un profil HIP auquel il correspond ou non. En cas de correspondance, la règle de politique

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. 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.
2. Saisissez un **Name (Nom)** et une **Description** pour identifier le profil.
3. Cliquez sur **Add Match Criteria (Ajouter un critère de correspondance)** pour ouvrir le générateur de profils/d'objets HIP.
4. 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 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.



5. 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).
6. 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 :

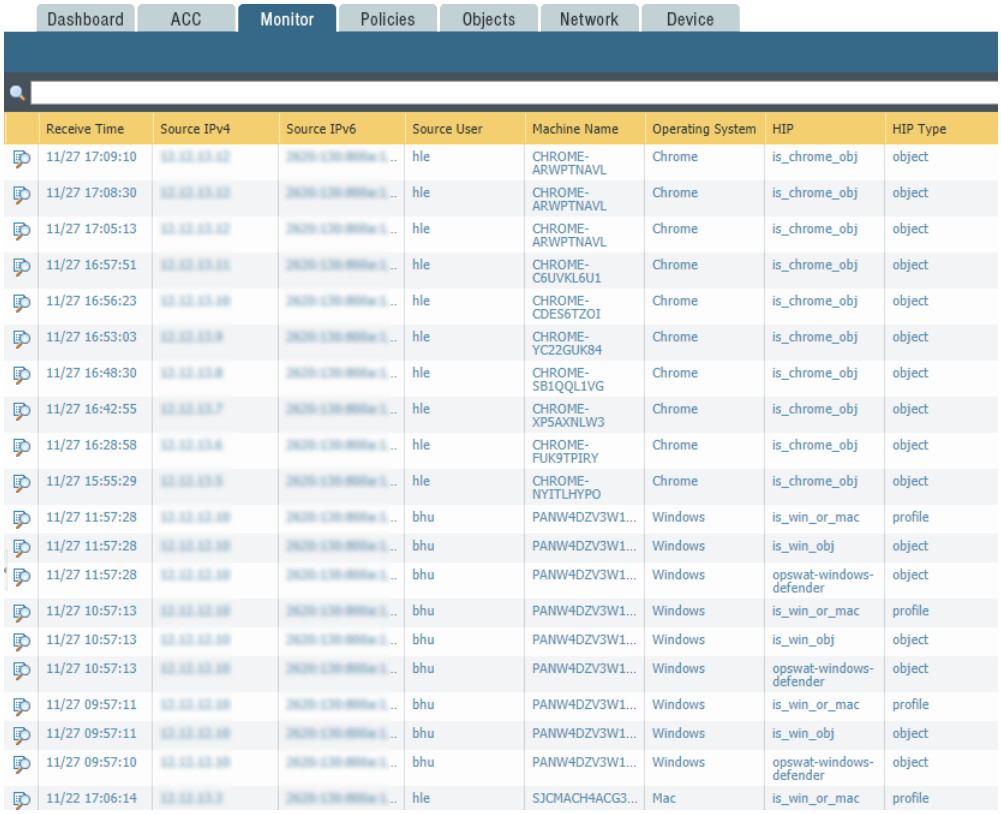


7. Lorsque vous avez ajouté tous vos critères de correspondance, cliquez sur **OK** pour enregistrer le profil.
8. Répétez ces étapes pour créer chaque profil HIP supplémentaire dont vous avez besoin.
9. **Commit (Validez)** les modifications.

STEP 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 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
11/27 17:09:10	[redacted]	[redacted]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 17:08:30	[redacted]	[redacted]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 17:05:13	[redacted]	[redacted]	hle	CHROME-ARWPTNAVL	Chrome	is_chrome_obj	object
11/27 16:57:51	[redacted]	[redacted]	hle	CHROME-C6UVKL6U1	Chrome	is_chrome_obj	object
11/27 16:56:23	[redacted]	[redacted]	hle	CHROME-CDES6TZOI	Chrome	is_chrome_obj	object
11/27 16:53:03	[redacted]	[redacted]	hle	CHROME-YC22GUK84	Chrome	is_chrome_obj	object
11/27 16:48:30	[redacted]	[redacted]	hle	CHROME-SB1QQL1VG	Chrome	is_chrome_obj	object
11/27 16:42:55	[redacted]	[redacted]	hle	CHROME-XP5AXNLW3	Chrome	is_chrome_obj	object
11/27 16:28:58	[redacted]	[redacted]	hle	CHROME-FUK9TPIRY	Chrome	is_chrome_obj	object
11/27 15:55:29	[redacted]	[redacted]	hle	CHROME-NYITLHYPO	Chrome	is_chrome_obj	object
11/27 11:57:28	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 11:57:28	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 11:57:28	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/27 10:57:13	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 10:57:13	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 10:57:13	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/27 09:57:11	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_or_mac	profile
11/27 09:57:11	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	is_win_obj	object
11/27 09:57:10	[redacted]	[redacted]	bhu	PANW4DZV3W1...	Windows	opswat-windows-defender	object
11/22 17:06:14	[redacted]	[redacted]	hle	SJCMACH4ACG3...	Mac	is_win_or_mac	profile

STEP 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	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	User ID: Enabled
corp-vpn	layer3	ethernet1/2			☑
		tunnel.1			

STEP 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 plus à même de déterminer l'inclusion appropriée des règles activées par HIP au sein de la stratégie.

1. Sélectionnez **Policies (Stratégies)** > **Security (Sécurité)** et sélectionnez la règle à laquelle vous souhaitez ajouter un profil HIP.
2. Dans l'onglet **Source**, vérifiez que la **Source Zone (Zone Source)** est une zone pour laquelle vous avez activé l'User-ID.
3. À l'onglet **User (Utilisateur)**, **Add (Ajoutez)** les **HIP Profiles (Profils HIP)** utilisés pour identifier les utilisateurs (vous pouvez ajouter un maximum de 63 profils HIP à une règle).
4. Cliquez sur **OK** pour enregistrer la règle.
5. **Commit (Validez)** les modifications.

		Source				Destination	
Name	Tags	Zone	Address	User	HIP Profile	Zone	Address
iOSApps	none	corp-vpn	any	known-user	is iOS	trust	any

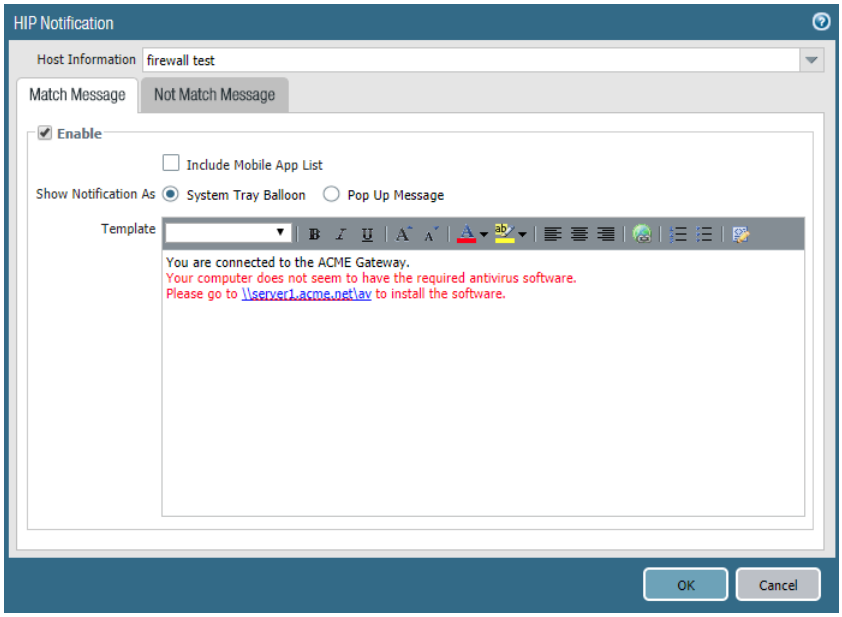
STEP 9 | Ce sous-onglet vous permet de définir les messages de notification à afficher aux utilisateurs finaux lorsqu'une règle de sécurité dotée d'un profil HIP est mise en œuvre.

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 mêmes applications sont installées, vous pouvez créer le message pour les utilisateurs qui ne correspondent pas au profil.

1. Sur le pare-feu qui héberge votre passerelle GlobalProtect, sélectionnez **Réseau** > **GlobalProtect** > **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 exemple un lien pour les utilisateurs directement vers l'URL de téléchargement pour un programme requis.

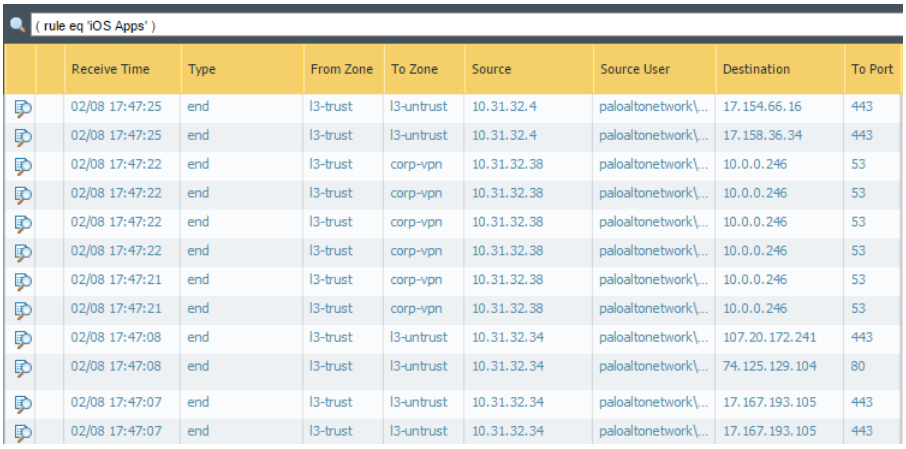


8. Répétez cette procédure pour chaque message que vous souhaitez définir.
9. **Commit (Validez)** les modifications.

STEP 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 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 :



	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port
	02/08 17:47:25	end	l3-trust	l3-untrust	10.31.32.4	paloaltonetwork\...	17.154.66.16	443
	02/08 17:47:25	end	l3-trust	l3-untrust	10.31.32.4	paloaltonetwork\...	17.158.36.34	443
	02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
	02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
	02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
	02/08 17:47:22	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
	02/08 17:47:21	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
	02/08 17:47:21	end	l3-trust	corp-vpn	10.31.32.38	paloaltonetwork\...	10.0.0.246	53
	02/08 17:47:08	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	107.20.172.241	443
	02/08 17:47:08	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	74.125.129.104	80
	02/08 17:47:07	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	17.167.193.105	443
	02/08 17:47:07	end	l3-trust	l3-untrust	10.31.32.34	paloaltonetwork\...	17.167.193.105	443

Collecter des données d'application et de processus sur des points de terminaison

Le registre Windows et le Plist MacOS 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 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). 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 se connecte.

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 et MacOS. 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.

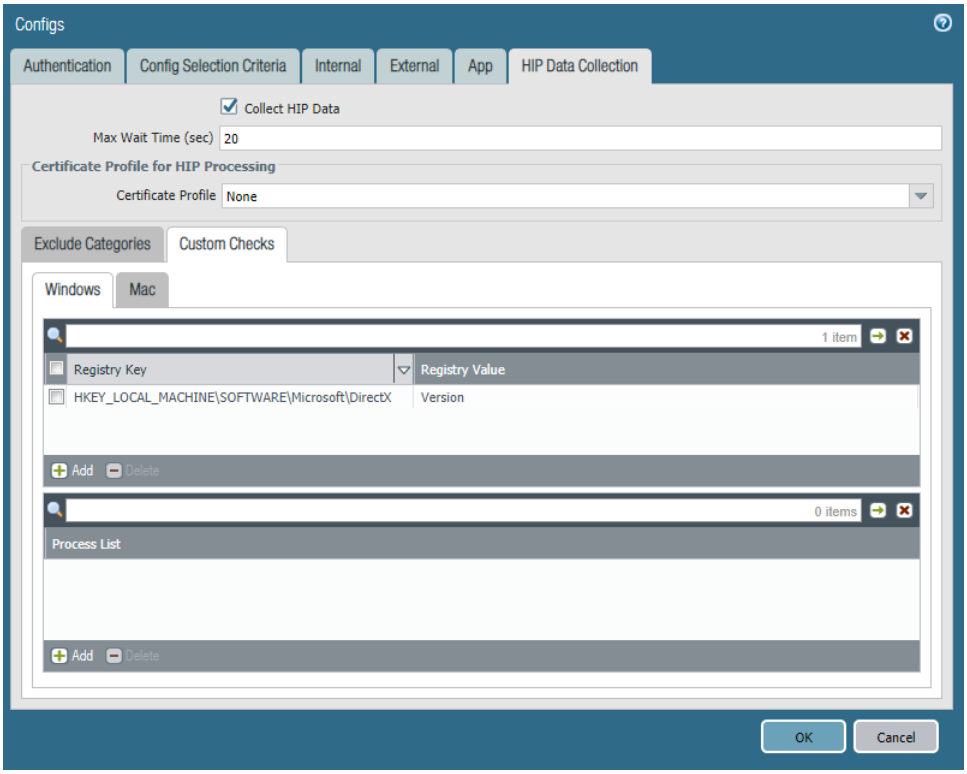
Pour plus d'informations sur la définition des paramètres d'application directement dans le registre Windows ou le plist MacOS global, reportez-vous à la section Déployer les paramètres de l'application de manière transparente*.*

STEP 1 | Activez l'application GlobalProtect pour qu'il collecte des informations de registre Windows sur des points de terminaison Windows ou des informations Plist sur des clients MacOS. 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.

Collectez des données sur un point de terminaison Windows :

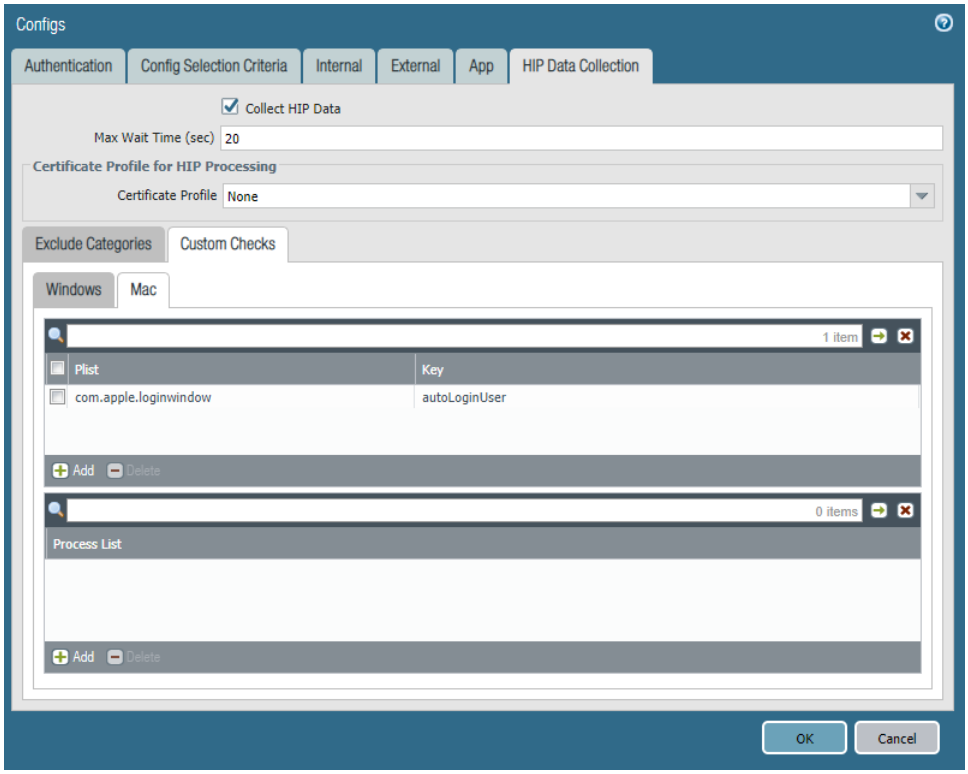
1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**.
2. Sélectionnez une configuration de portail existante ou **Add (Ajoutez)**-en une nouvelle.
3. À l'onglet **Agent (Agent)**, sélectionnez la configuration de l'agent que vous souhaitez modifier (ou **Add (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 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.

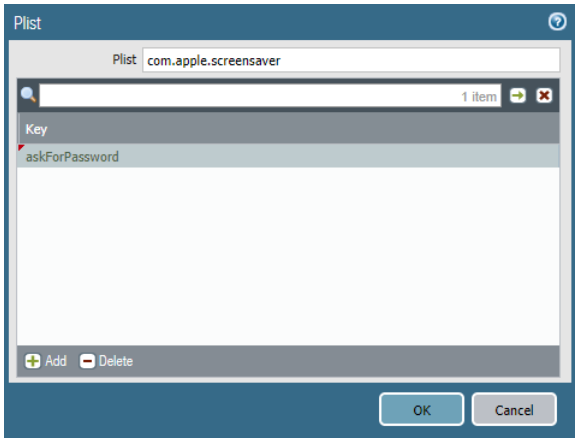


Collectez des données sur un point de terminaison MacOS :

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (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)** > **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.



STEP 2 | (Facultatif) Vérifiez si un processus spécifique est exécuté sur le point de terminaison.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (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** ou **Mac**.
7. **Add (Ajoutez)** le nom du processus sur lequel vous souhaitez collecter des informations dans la **Process List (Liste des processus)**.

STEP 3 | Enregistrez la vérification personnalisée.

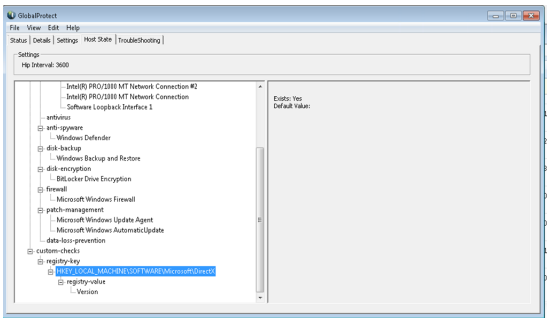
Cliquez sur **OK** et sur **Commit (Valider)** pour enregistrer les modifications.

STEP 4 | Vérifiez que l'application GlobalProtect collecte les données définies dans la vérification personnalisée depuis le point de terminaison.

Pour les points de terminaison Windows :

1. Lancez l'application GlobalProtect pour les points de terminaison Windows en cliquant sur l'icône de bac de système. Le panneau d'état de GlobalProtect s'ouvre.
2. Cliquez sur l'icône des paramètres (

) pour ouvrir le menu des paramètres.
3. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau des **GlobalProtect Settings (Paramètres GlobalProtect)**.
4. Sélectionnez l'onglet **Host Profile (Profil de l'hôte)** pour afficher les informations que l'application GlobalProtect collecte du point de terminaison. Vérifiez que le menu déroulant **custom-checks (vérifications personnalisées)** affiche les données à collecter que vous avez définies.



Pour les points de terminaison MacOS :

1. Lancez l'application GlobalProtect pour les points de terminaison MacOS en cliquant sur l'icône de bac de système. Le panneau d'état de GlobalProtect s'ouvre.
2. Cliquez sur l'icône des paramètres (

) pour ouvrir le menu des paramètres.
3. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau des **GlobalProtect Settings (Paramètres GlobalProtect)**.
4. Sélectionnez l'onglet **Host Profile (Profil de l'hôte)** pour afficher les informations que l'application GlobalProtect collecte du point de terminaison. Vérifiez que le menu déroulant **custom-checks (vérifications personnalisées)** affiche les données à collecter que vous avez définies.

STEP 5 | (Facultatif) Créez un objet HIP à faire correspondre à une clé de registre (Windows) ou à une plist (MacOS). Cela vous permet de filtrer 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 and MacOS :

1. Sélectionnez **Objects (Objets)** > **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)**.

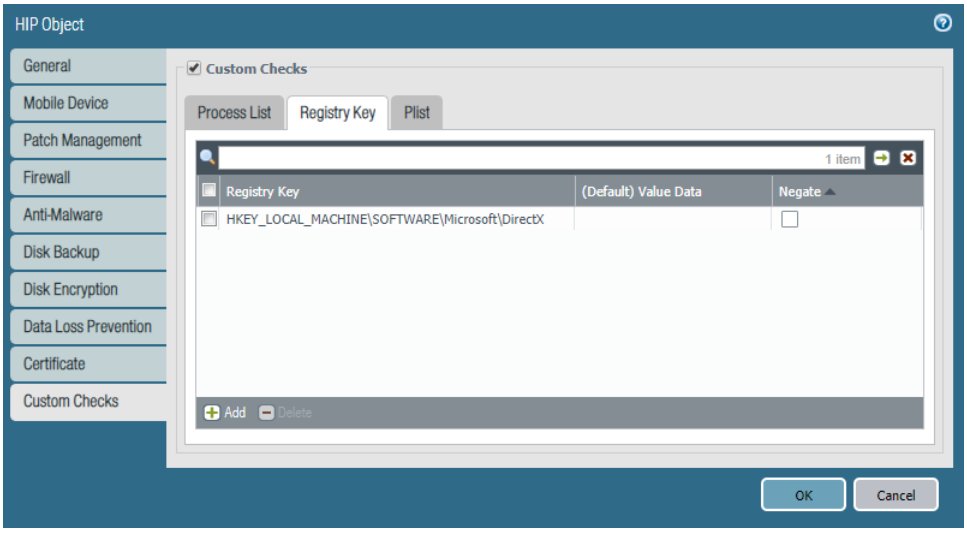
Pour les points de terminaison Windows uniquement :

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)**.
   - 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).

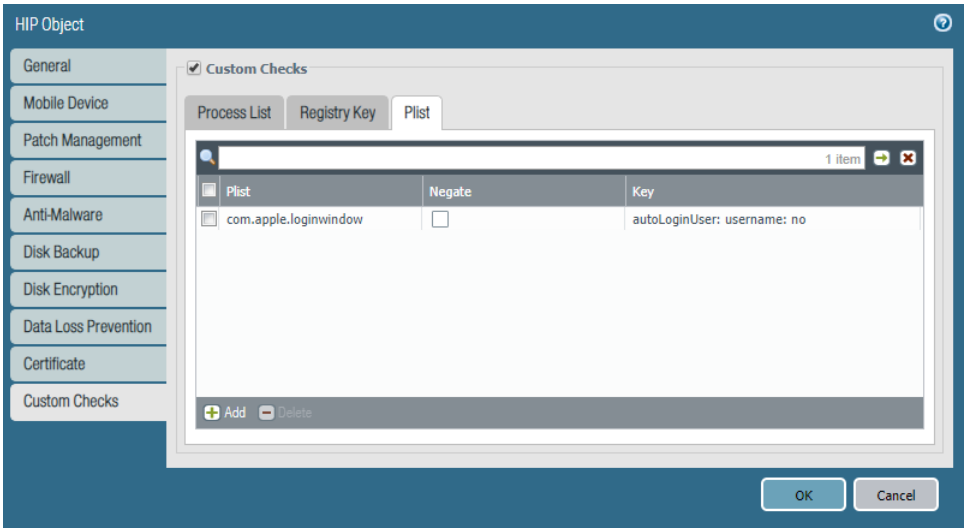
   Si vous ajoutez plus d'une valeur de registre à votre clé de registre, la passerelle GlobalProtect vérifie les points de terminaison pour toutes la valeurs de registre spécifiées.



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)** 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.

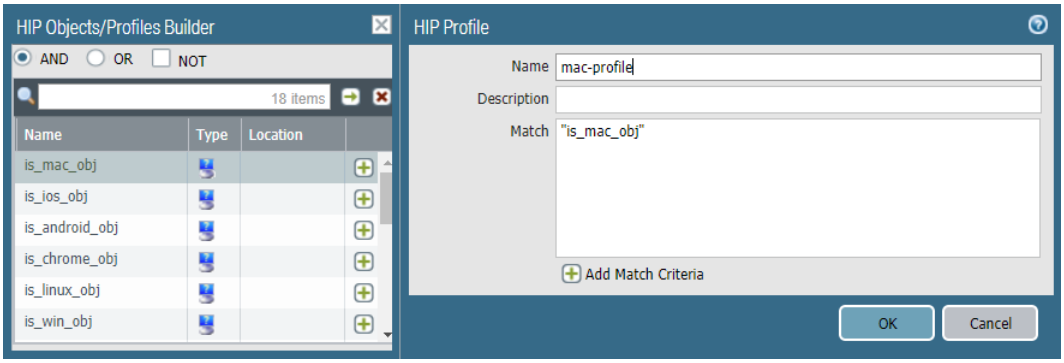
STEP 6 | (Facultatif) Créez un profil HIP pour que l'objet HIP soit évalué par rapport au trafic.

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. Sélectionnez **Objects (Objects)** > **GlobalProtect (GlobalProtect)** > **HIP Profiles (Profils 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.
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.



STEP 7 | 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.

Redistribution des rapports HIP

Pour veiller à l'uniformité de l'application des politiques de Host Information Profile (profil d'informations sur l'hôte - HIP) et pour simplifier la gestion des politiques, vous pouvez distribuer les rapports HIP reçus de l'application GlobalProtect (et envoyés à une passerelle GlobalProtect interne ou externe) aux autres passerelles, pare-feu, collecteurs de journaux dédiés et appareils Panorama au sein de 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.

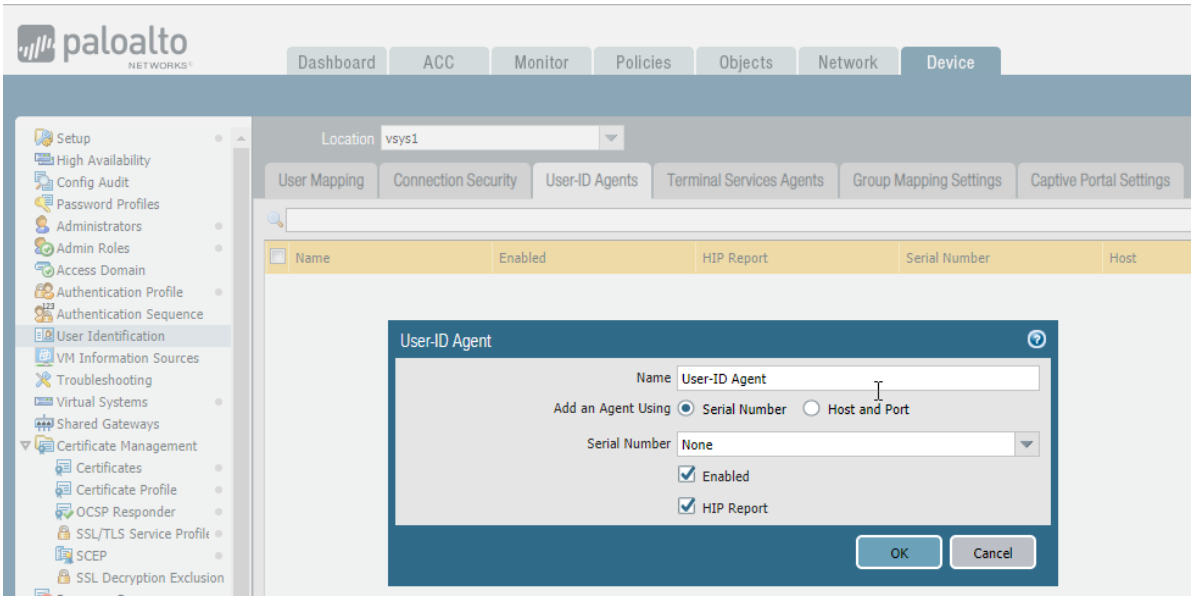
Utilisez les étapes suivantes pour configurer la redistribution des rapports HIP.

STEP 1 | Configurer la mise en œuvre des politiques basées sur HIP pour vos passerelles et pare-feu.

STEP 2 | Configurez la redistribution des rapports HIP.

1. Sélectionnez **Device (Périphérique)** > **User Identification (Identification utilisateur)** > **User-ID Agents (Agents User-ID)**.
2. Sélectionnez un agent User-ID existant ou **Add (Ajoutez)**-en un nouveau.

   Il doit s'agir d'un pare-feu nouvelle génération Palo Alto Networks, d'une passerelle GlobalProtect, d'un contrôleur de journaux dédié ou d'un appareil Panorama.
3. Sélectionnez **HIP Report (Rapport HIP)**.



4. Cliquez sur **OK**.

STEP 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 ou un contrôleur de journaux dédié 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 rapports HIP pour la mise en correspondance avec les groupes d'utilisateurs sur les pare-feu ou passerelles User-ID.

STEP 4 | Redistribuez les rapports HIP à vos appareils Panorama gérés, vos passerelles, vos pare-feu et vos systèmes virtuels qui utilisent le même flux de travail que vous utilisez pour redistribuer les informations User-ID aux pare-feu gérés.

Bloquer l'accès aux points de terminaison

Dans le cas où un utilisateur perd un point de terminaison qui fournit l'accès GlobalProtect à votre réseau, ou que ce point de terminaison est volé, ou qu'un utilisateur quitte votre organisation, vous pouvez empêcher le point de terminaison d'accéder au réseau en le plaçant sur une liste d'interdictions.

Une liste d'interdictions est locale à un emplacement réseau logique (Vsys, 1 par exemple) et peut contenir un maximum de 1 000 points de terminaison par emplacement. Par conséquent, vous pouvez créer des listes d'interdictions distinctes pour chaque emplacement hébergeant un déploiement GlobalProtect.

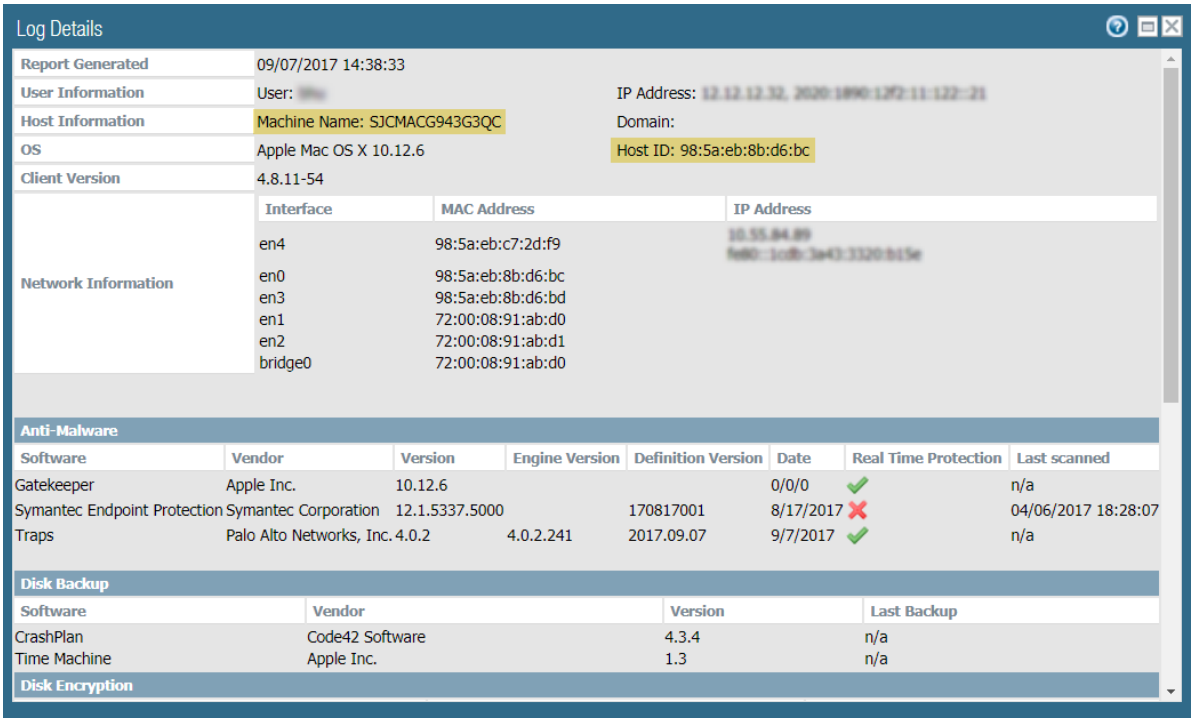
STEP 1 | Identifiez l'ID d'hôte pour les points de terminaison que vous souhaitez bloquer.

L'ID hôte est un ID unique que GlobalProtect affecte afin d'identifier l'hôte. 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 :

1. Sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **HIP Match (Correspondance HIP)**.
2. Filtrez les journaux de correspondance HIP pour l'utilisateur source associé au point de terminaison.
3. 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)**.

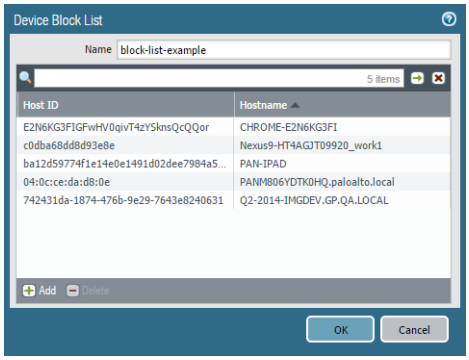


STEP 2 | Créer une liste d'interdictions de périphériques

Vous ne pouvez pas utiliser les modèles Panorama pour transmettre une liste d'interdictions de périphériques à des pare-feu.

1. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Device Block List (Liste d'interdictions de périphériques)** et **Add (ajoutez)** une liste d'interdictions de périphériques.
2. Donnez un **Name (Nom)** descriptif pour la liste.
3. Dans le cas d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez la **Location (Emplacement)** (vsys ou **Shared (Partagé)**) dans laquelle le profil est disponible.

STEP 3 | Ajoutez un périphérique à une liste d'interdictions.



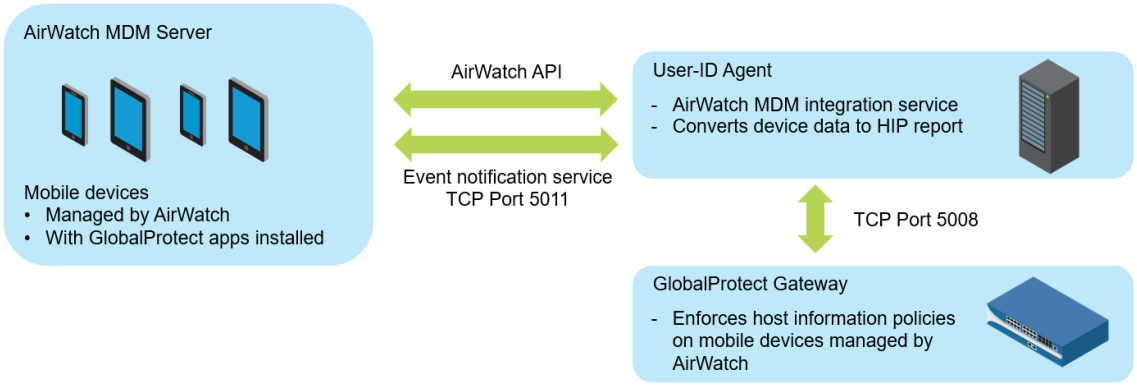
1. **Add (Ajoutez)** les points de terminaisons. Saisissez l'ID d'hôte (requis) et le nom d'hôte (facultatif) du point de terminaison que vous devez bloquer.
2. **Add (Ajoutez)** d'autres points de terminaison si nécessaire.
3. Cliquez sur **OK** pour enregistrer et activer la liste d'interdictions.

La liste d'interdictions des périphériques ne requiert pas de validation et est immédiatement active.

Configurer l'agent User-ID Windows pour collecter des informations d'hôte

L'agent User-ID Windows a été étendu pour prendre en charge un nouveau service d'intégration MDM AirWatch. Ce service permet à GlobalProtect d'utiliser les informations d'hôte collectées par le service pour appliquer les politiques basées sur HIP sur les périphériques gérés par AirWatch. Exécuté en tant qu'agent User-ID Windows, le service d'intégration MDM AirWatch utilise l'API AirWatch pour collecter des informations à partir de points de terminaison mobiles gérés par VMware AirWatch et traduire ces données en informations d'hôte.

Pour les points de terminaison Android gérés par AirWatch, cette fonctionnalité prend en charge les points de terminaison Android for Work, mais pas les autres types de points de terminaison Android.



Aperçu de l'intégration MDM

Le service d'intégration MDM inclus avec l'agent User-ID Windows effectue une requête HIP complète sur le serveur MDM AirWatch 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 AirWatch à intervalles réguliers et pour transmettre ces informations aux passerelles GlobalProtect. En outre, le service peut surveiller les notifications d'événements AirWatch et récupérer les informations de périphérique mises à jour lorsque des événements AirWatch (comme des modifications de conformité) se produisent.

Informations collectées

Le tableau suivant montre comment les informations collectées à partir des points de terminaison qui sont gérés par AirWatch sont traduites en attributs de rapport HIP. Le mappage se fait automatiquement.

Attributs AirWatch	Attributs de rapport HIP
Informations sur le périphérique	
SerialNumber (Numéro de série)	serial-number
MacAddress (Adresse Mac)	wifimac
Imei	IMEI
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

Attributs AirWatch	Attributs de rapport HIP
IsPasscodeCompliant (Mot de passe conforme)	passcode-compliant
Informations sur le réseau	
DataRoamingEnabled (Itinérance de données activée)	data-roaming
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

Le service d'intégration MDM AirWatch 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 AirWatch	8.4.7.0
Windows Server	2008 et 2012 2016 avec agent User-ID 8.0.4 et PAN-OS 8.0.4

Configurer GlobalProtect pour récupérer des informations d'hôte

Utilisez les instructions suivantes pour configurer GlobalProtect afin de récupérer les informations d'hôte à partir des périphériques gérés par AirWatch.

STEP 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 AirWatch.

Le service d'intégration MDM AirWatch est fourni avec l'agent User-ID basé sur Windows PAN-OS.

STEP 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 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)**.

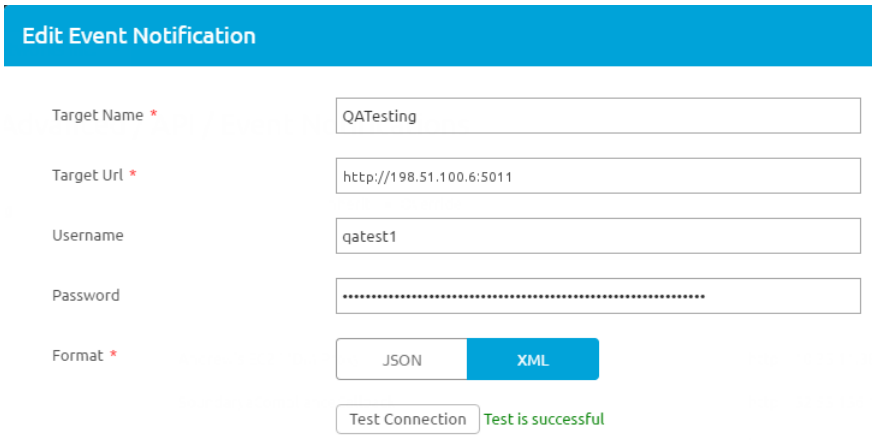
1. Redémarrez l'agent User-ID basé sur Windows.

STEP 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 **AirWatch** pour le **MDM Vendor (Fournisseur MDM)**.

STEP 4 | Spécifiez les paramètres de la **MDM Event Notification (Notification d'événement MDM)** pour surveiller et collecter les événements AirWatch (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 AirWatch et transmet ces informations à toutes les passerelles GlobalProtect configurées.

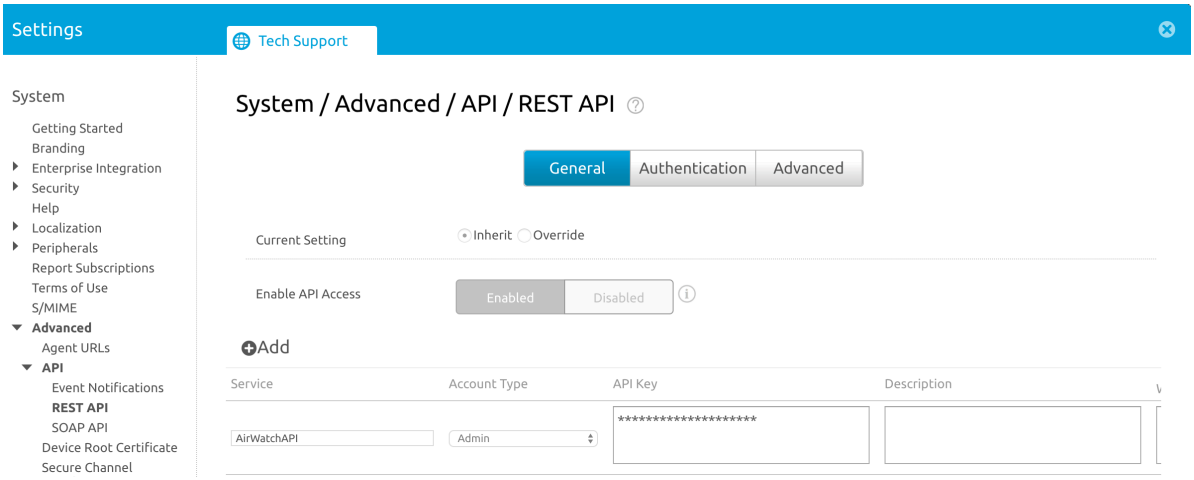
Pour MDM Event Notification (Notification d'événement MDM), assurez-vous que les valeurs que vous entrez ici sont également configurées dans la console AirWatch sous Groups & Settings (Groupes et paramètres) > All Settings (Tous les paramètres) > System (Système) > Advanced (Avancé) > API > Event Notifications (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 AirWatch. Contactez votre équipe d'assistance AirWatch pour obtenir des instructions sur les adresses IP à spécifier.

STEP 5 | Ajoutez les paramètres **MDM API Authentication (Authentification API MDM)** pour vous connecter à l'API AirWatch.

- Saisissez la **Server Address (Adresse du serveur)** du serveur MDM AirWatch 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 AirWatch.
- Saisissez le **Tenant Code (Code du locataire)**. Il s'agit d'un numéro de code hexadécimal unique requis pour accéder à l'API MDM AirWatch. Sur la console AirWatch, vous pouvez trouver le code du locataire dans **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 AirWatch. L'intervalle par défaut est de 30 minutes. Pour changer d'intervalle, indiquez un chiffre entre 1 et 600.

STEP 6 | **Commit (Validez)** vos modifications.

STEP 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 AirWatch.

STEP 8 | Configurez la passerelle GlobalProtect pour communiquer avec le service d'intégration MDM afin de récupérer les rapports HIP pour les périphériques gérés par AirWatch.

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 AirWatch 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.

STEP 9 | Vérifiez votre connexion pour vous assurer que les données du périphérique AirWatch 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 AirWatch.
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.

Résoudre les problèmes du service d'intégration MDM

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 AirWatch.

- Les notifications d'événements provenant du serveur MDM AirWatch 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 :

     ```
     The address x.x.x.x
     is not in the permitted ip list for event notifications.
     ```

  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 de l'API REST Airwatch échoue.

  Assurez-vous que :

  - Les informations d'identification utilisées pour le service d'intégration MDM pour s'authentifier auprès du service MDM AirWatch sont valides.
  - Le compte utilisateur utilisé pour accéder à l'API REST Airwatch 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 AirWatch.
  - Le **Tenant Code (Code du locataire)** (clé API) est correctement associé au compte utilisateur. Retirez toutes les clés API inutilisées.

Certifications

L'application GlobalProtect™ pour les terminaux Windows et macOS respecte les exigences de la Federal Information Processing Standard (FIPS 140-2) et des Critères communs (CC) lorsque vous activez le mode FIPS-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 obtenir de l'information sur la configuration de l'application GlobalProtect et la résolution des problèmes pour les points de terminaison Windows et MacOS en mode FIPS-CC :

- Activation et vérification du mode FIPS-CC
- Fonctions de sécurité FIPS-CC
- Dépannage du mode FIPS-CC

Activation et vérification du mode FIPS-CC

Vous pouvez activer et vérifier le mode FIPS-CC pour l'application FIPS-CC à l'aide des méthodes suivantes :

- Activation et vérification du mode FIPS-CC à l'aide du registre Windows
- Activation et vérification du mode FIPS-CC à l'aide de la liste des propriétés MacOs

Pour modifier le registre Windows ou la plist MacOs, vous devez avoir un compte administrateur dans Windows ou MacOS.

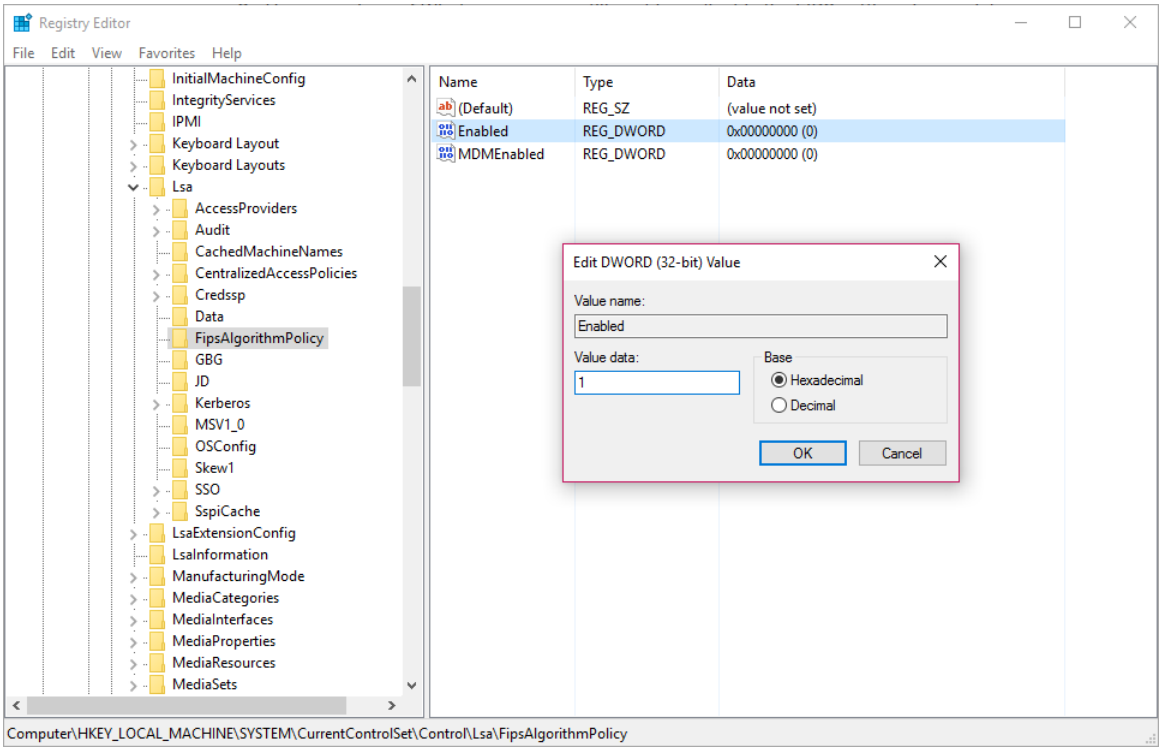
Activation et vérification du mode FIPS-CC à l'aide du registre Windows

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 :

STEP 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 pour le système d'exploitation Windows pour vous assurer que le point de terminaison Windows respecte la norme FIPS 140-2.

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.

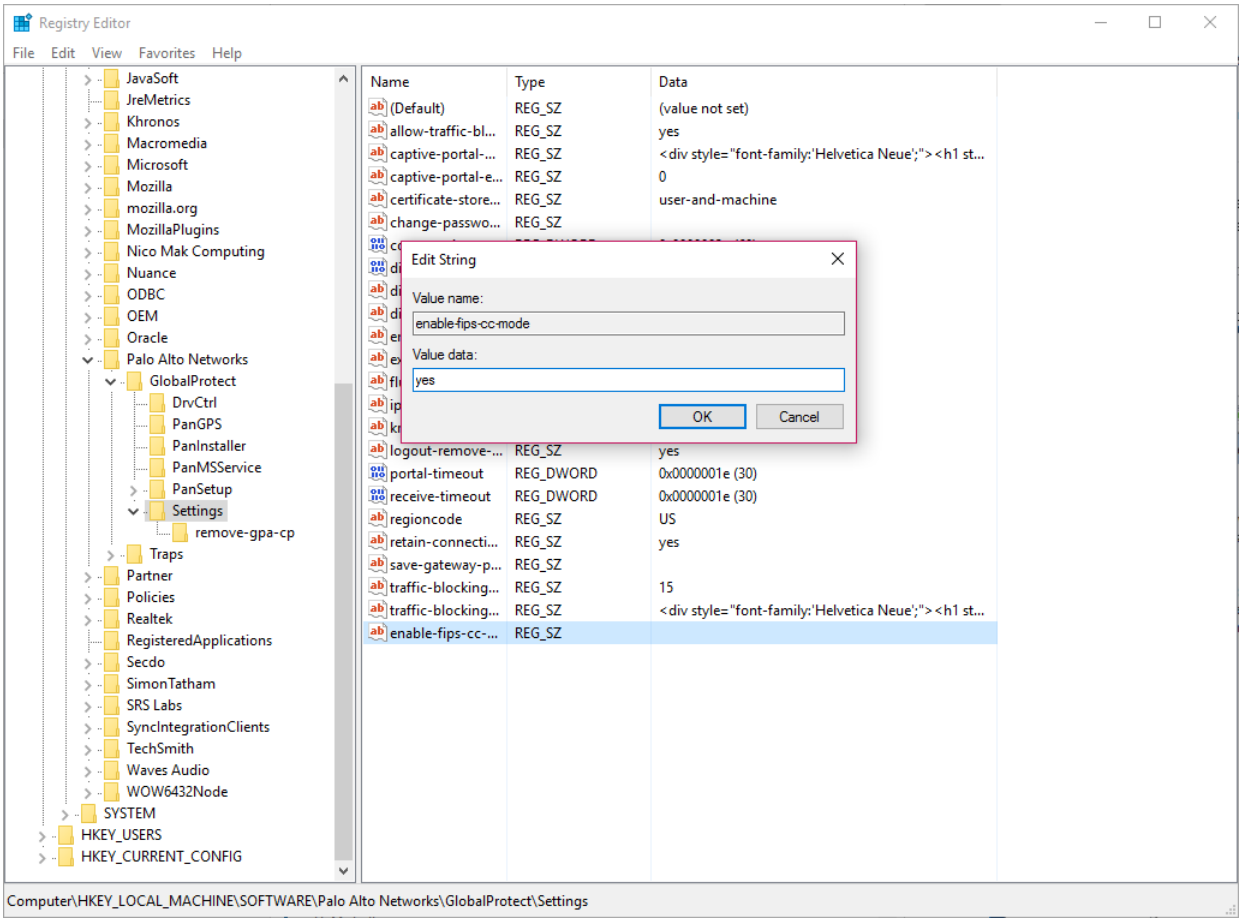


6. Cliquez sur **OK**.
7. Redémarrez votre point de terminaison.

STEP 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 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**.

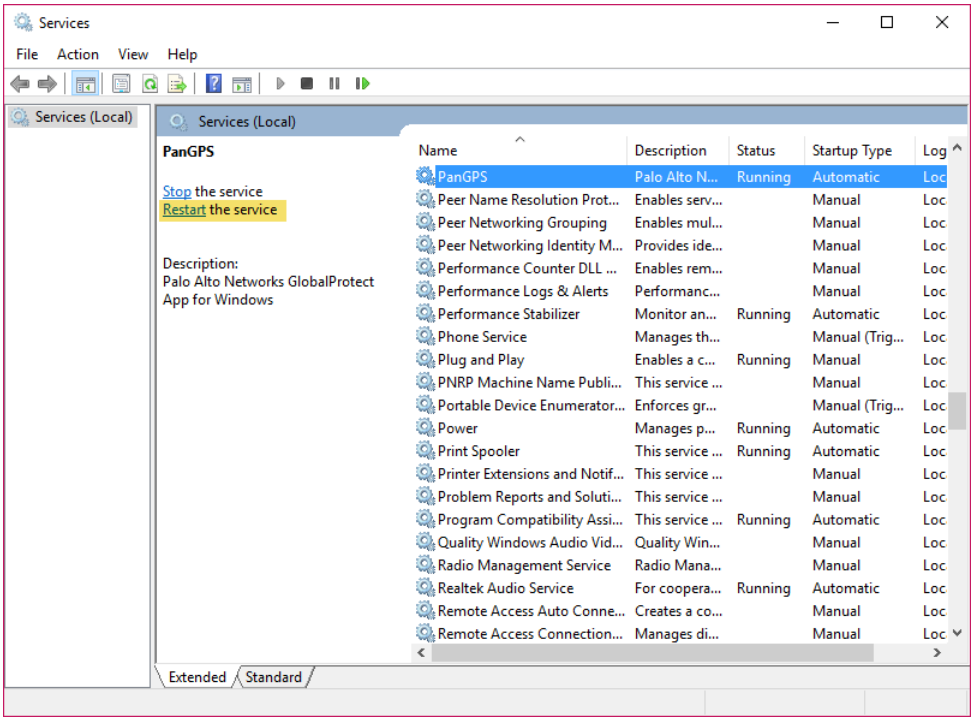


STEP 3 | Redémarrez GlobalProtect.

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 :

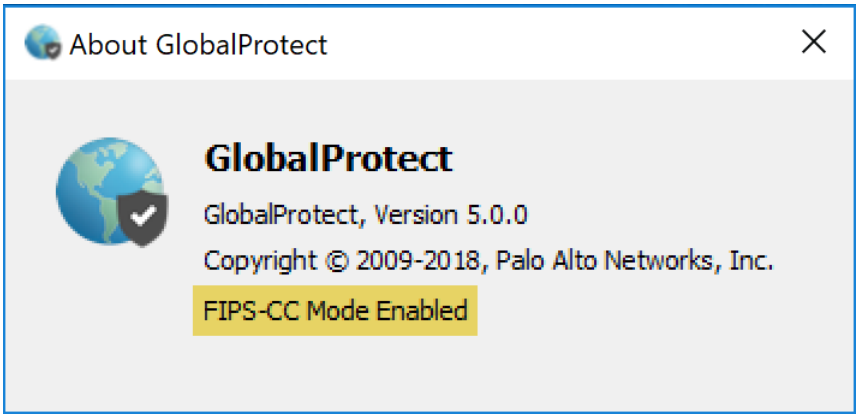
- Redémarrez votre point de terminaison.
- Relancez l'application GlobalProtect et le service GlobalProtect (PanGPS) :

  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.



STEP 4 | Vérifiez que le mode FIPS-CC est activé sur votre 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`.



Activation et vérification du mode FIPS-CC à l'aide de la liste des propriétés 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, votre point de terminaison MacOS doit respecter la norme FIPS 140-2. 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.

STEP 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.

STEP 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 :

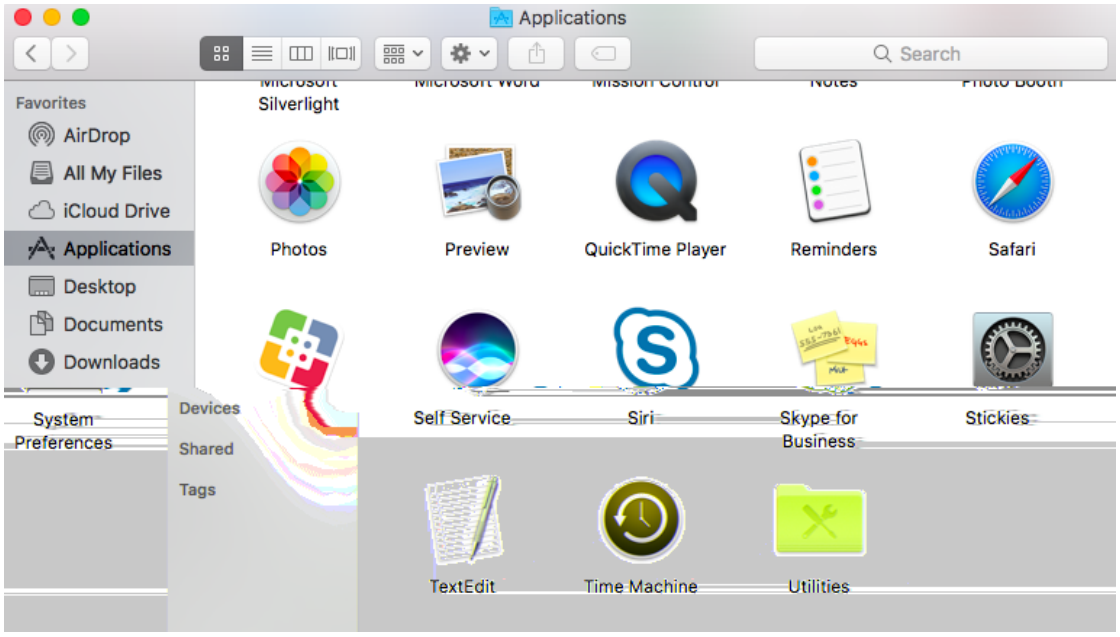
```
<clé>enable-fips-cc-mode</clé>
<chaîne>yes</chaîne>
```

STEP 3 | Redémarrez GlobalProtect.

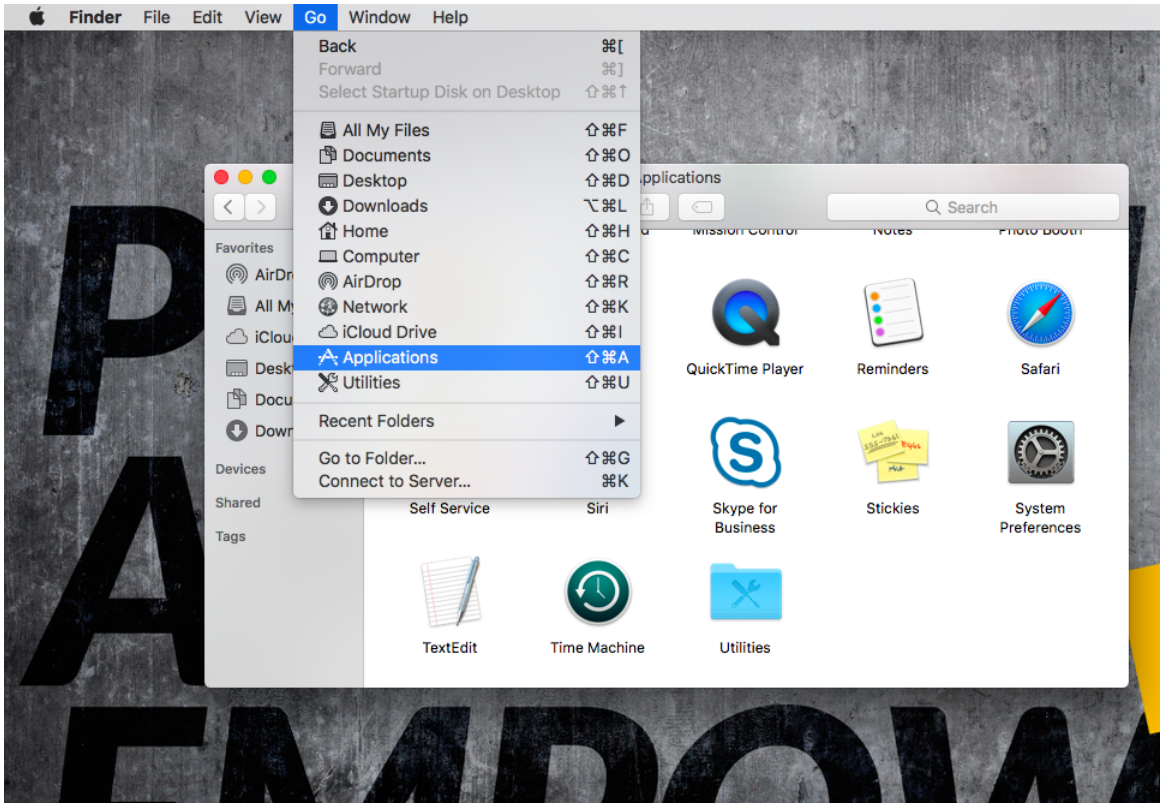
Pour permettre à l'application GlobalProtect d'être lancée en mode FIPS-CC, vous devez redémarrer GlobalProtect à l'aide de l'une des méthodes suivantes :

- 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.



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.

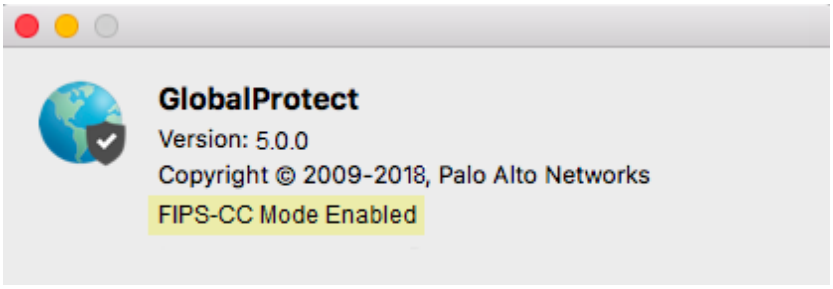
3. Ouvrer le dossier des utilitaires.

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.pangpa.plist
username>$ launchctl load -S Aqua /Library/LaunchAgents/
com.paloaltonetworks.gp.pangps.plist
```

STEP 4 | Vérifiez que le mode FIPS-CC est activé sur votre 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`.



Fonctions de sécurité FIPS-CC

Lorsque vous activez le mode FIPS-CC pour GlobalProtect, les fonctions de sécurité suivantes sont appliquées pour toutes les applications GlobalProtect sur les points de terminaison Windows et MacOS :

- Vous devez 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, vous devez sélectionner une option Suite de cryptage présentée lors de la configuration IPSec.
- Lorsque vous configurez un tunnel VPN IPSec, vous pouvez spécifier l'un des algorithmes de chiffrement suivants :
  - AES-CBC-128 (avec l'algorithme d'authentification SHA1)
  - 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 SHA256, SHA384 ou SHA512.

Dépannage du mode FIPS-CC

Si vous éprouvez des problèmes après avoir activé le mode FIPS-CC, reportez-vous aux sections suivantes pour régler ces problèmes :

- Affichage et collecte des journaux GlobalProtect
- Résolution des problèmes du mode FIPS-CC

Affichage et collecte des journaux GlobalProtect

Vous pouvez voir plus de détails sur les problèmes FIPS-CC dans les journaux GlobalProtect™.

Utilisez les étapes suivantes pour afficher ou collecter les journaux GlobalProtect :

STEP 1 | Lancez l'application GlobalProtect.

STEP 2 | À partir du panneau d'état, ouvrez le dialogue des paramètres ( ).

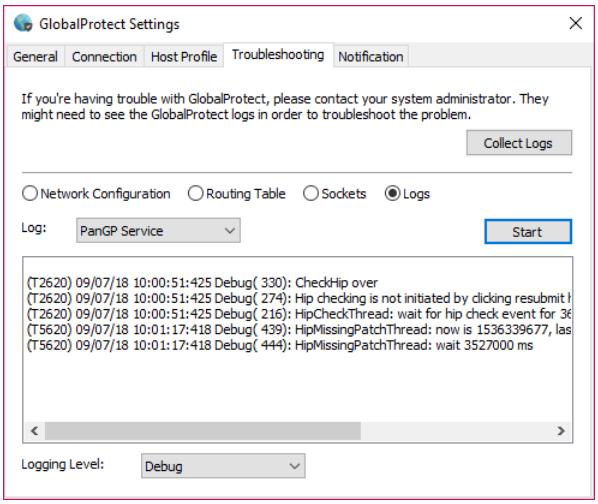
STEP 3 | Sélectionnez **Settings (Paramètres)**.

STEP 4 | À partir du panneau des paramètres GlobalProtect, sélectionnez **Troubleshooting (Résolution de problèmes)**.

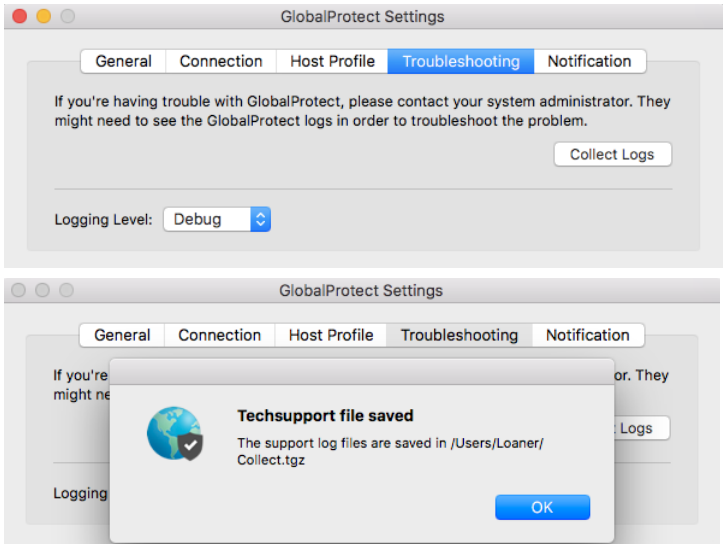
STEP 5 | Sélectionnez un **Logging Level (Niveau de journalisation)**.

STEP 6 | (Facultatif—Windows uniquement) Affichez vos journaux GlobalProtect :

1. Sélectionnez **Logs (Journaux)**.
2. Choisissez un type de **Log (Journal)**.
3. **Start (Commencez)** la collecte des journaux.

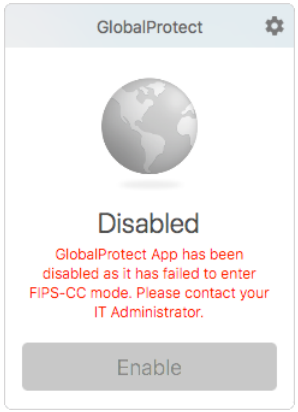


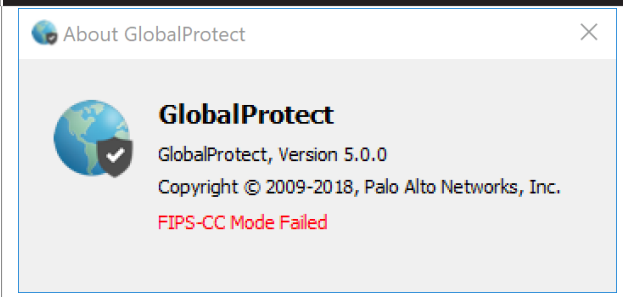
STEP 7 | (Facultatif) **Collect Logs (Collectez les journaux)** à envoyer à votre adminstrateur GlobalProtect à des fins de résolution de problèmes.



Résolution des problèmes du mode FIPS-CC

Le tableau suivant 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.

Problème	Description	Solution
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 FIPS.	Après avoir activé le mode FIPS-CC, l'application GlobalProtect effectue les tests automatiques à la mise sous tension FIPS et les tests d'intégrité lors de l'initialisation des applications et des redémarrages des systèmes ou des applications. En cas 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`: 	Redémarrez l'application pour supprimer la condition d'erreur. Si le problème persiste, désinstallez l'application, puis réinstallez-la.

Problème	Description	Solution
		
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.	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.	Pour établir une connexion à GlobalProtect, vous devez vous réauthentifier auprès du portail GlobalProtect.

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.

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
- Base de connaissances Live : modifications du mot de passe Active Directory

VPN d'accès à distance (Profil d'authentification)

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.

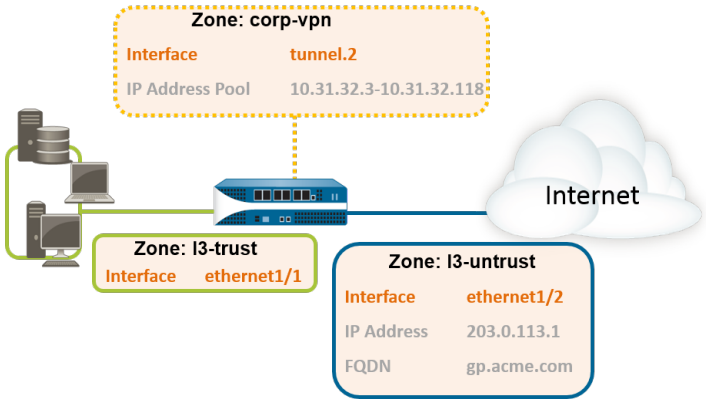


Figure 5: VPN GlobalProtect pour l'accès à distance

STEP 1 | Créer 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 (Ajoutez)** 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**.

STEP 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. Sélectionnez **Policies (Politiques)** > **Security (Securité)**, puis **Add (Ajoutez)** 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

STEP 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.

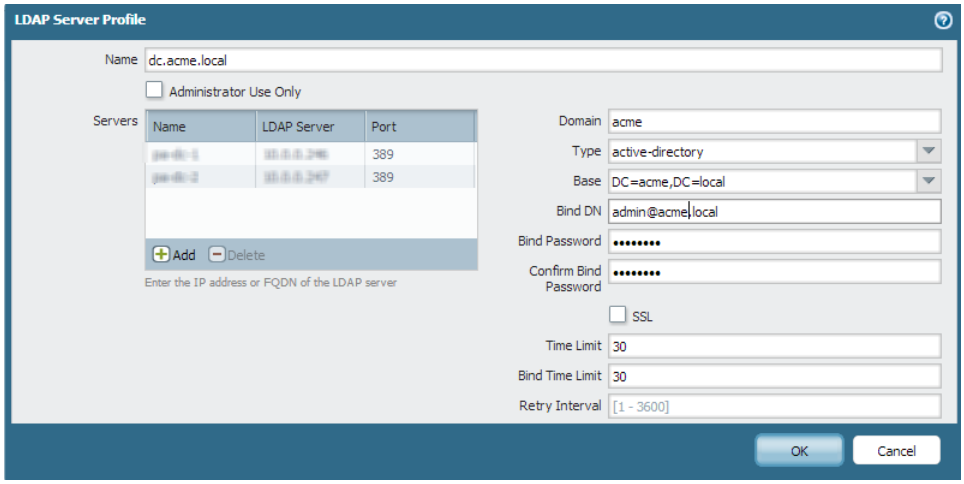
Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion de Certificat)** > **Certificates (Certificats)** pour gérer les certificats comme suit :

- 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.

STEP 4 | Créez un profil de serveur.

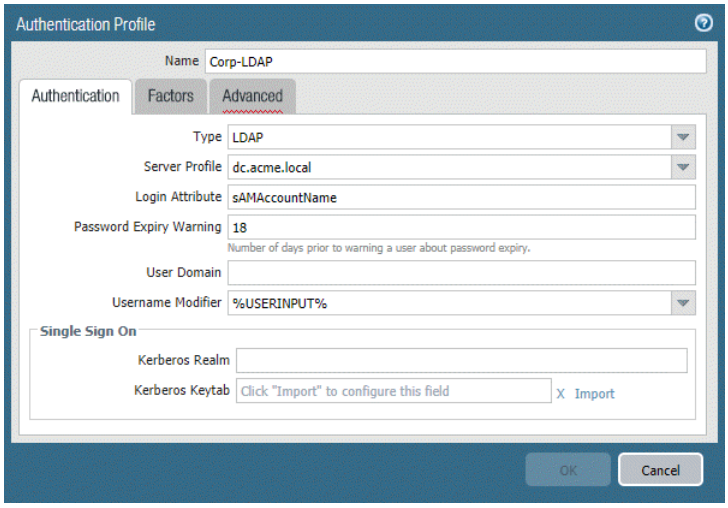
Le profil de serveur indique au pare-feu comment se connecter au service d'authentification. Les méthodes d'authentification locale, RADIUS, Kerberos, SAML et LDAP sont prises en charge. Cet exemple décrit un profil d'authentification LDAP pour authentifier les utilisateurs par rapport à Active Directory.

Créez le profil serveur pour la connexion au serveur LDAP (**Device (Périphérique)** > **Server Profiles (Profils Serveur)** > **LDAP**).



STEP 5 | (Facultatif) Créez un profil d'authentification.

Attachez le profil du serveur à un profil d'authentification (**Device (Périphérique)** > **Authentication Profile (Profil d'authentification)**).



STEP 6 | Configurer une passerelle GlobalProtect.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**, puis **Add (Ajoutez)** 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`

STEP 7 | Configurez les portails GlobalProtect.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, puis **Add (Ajoutez)** 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`

STEP 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.

STEP 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.

STEP 10 | Enregistrez la configuration GlobalProtect.

Cliquez sur **Commit (Valider)**.

VPN d'accès à distance (profil de certificat)

Avec l'authentification de certificat, l'utilisateur doit présenter un certificat client valide qui l'identifie auprès du portail GlobalProtect ou de la passerelle. 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.

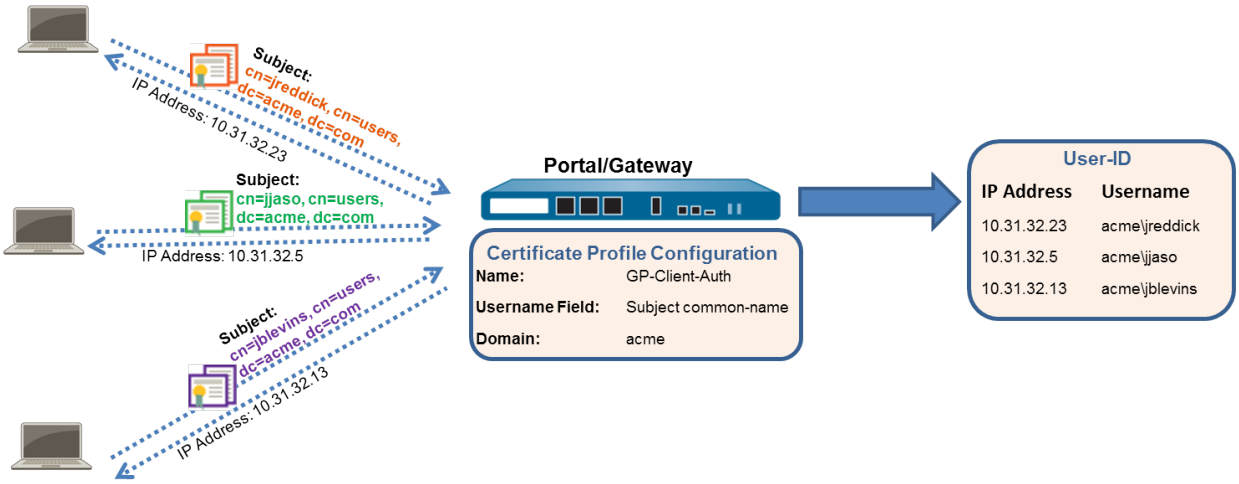


Figure 6: Configuration de l'authentification du certificat client GlobalProtect

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.

STEP 1 | Créer 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 (Ajoutez)** 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**.

STEP 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. Sélectionnez **Policies (Politiques)** > **Security (Securité)**, puis **Add (Ajoutez)** 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**

			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

STEP 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.

Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion de Certificat)** > **Certificates (Certificats)** pour gérer 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.

STEP 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.

STEP 5 | Créer un profil de certificat client.

1. 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**.
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**.

STEP 6 | Configurer une passerelle GlobalProtect.

Consultez le diagramme de la topologie illustré dans VPN GlobalProtect pour l'accès à distance.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**, puis **Add (Ajoutez)** 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`

STEP 7 | Configurez les portails GlobalProtect.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, puis **Add (Ajoutez)** 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`
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`

STEP 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.

STEP 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.

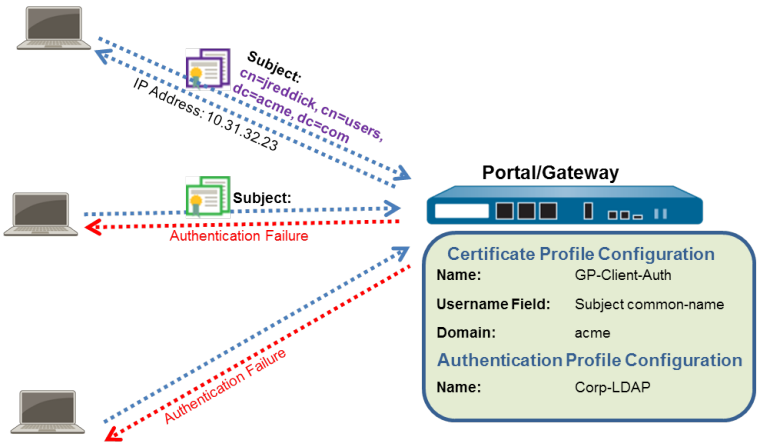
STEP 10 | Enregistrez la configuration GlobalProtect.

Cliquez sur **Commit (Valider)**.

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

Utilisez la procédure suivante pour configurer l'accès distant VPN au moyen de l'authentification à deux facteurs.

STEP 1 | Créer 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 (Ajoutez)** 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`.

STEP 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. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)**, puis cliquez sur **Add (Ajouter)** pour créer 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`

			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

STEP 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.

Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion de Certificat)** > **Certificates (Certificats)** pour gérer 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.

STEP 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.

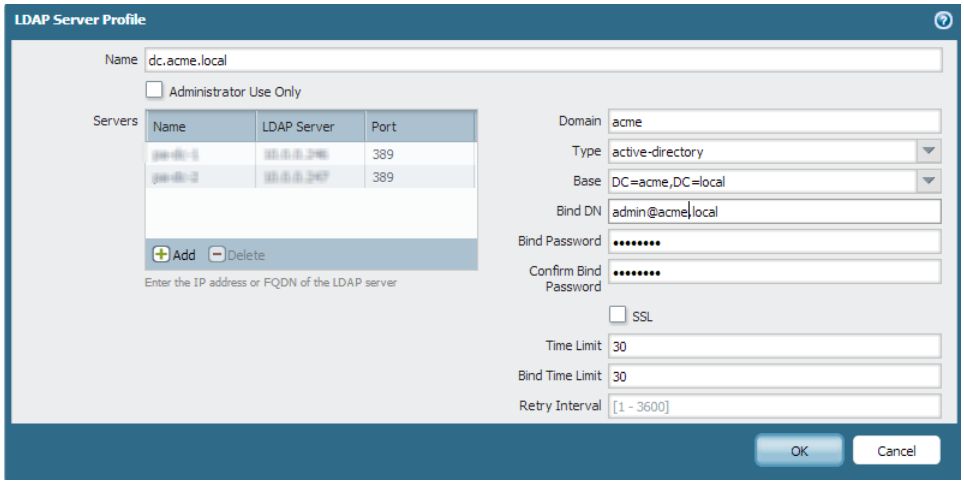
STEP 5 | Créer un profil de certificat client.

1. 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`**.
2. 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 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.
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**.

STEP 6 | Créez un profil de serveur.

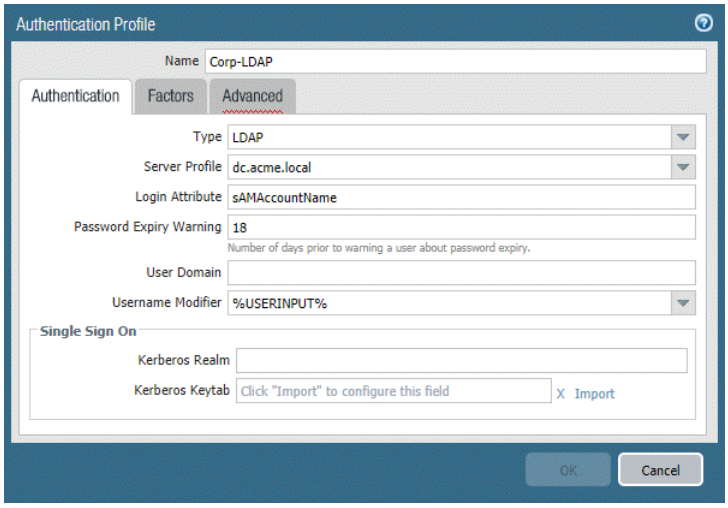
Le profil de serveur indique au pare-feu comment se connecter au service d'authentification. Les méthodes d'authentification locale, RADIUS, Kerberos, SAML et LDAP sont prises en charge. Cet exemple décrit un profil d'authentification LDAP pour authentifier les utilisateurs par rapport à Active Directory.

Créez le profil serveur pour la connexion au serveur LDAP (**Device (Périphérique)** > **Server Profiles (Profils Serveur)** > **LDAP**).



STEP 7 | (Facultatif) Créez un profil d'authentification.

Attachez le profil du serveur à un profil d'authentification (**Device (Périphérique)> Authentication Profile (Profil d'authentification)**).



STEP 8 | Configurer une passerelle GlobalProtect.

Consultez le diagramme de la topologie illustré dans VPN GlobalProtect pour l'accès à distance.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**, puis **Add (Ajoutez)** 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`

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`

STEP 9 | Configurez les portails GlobalProtect.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, puis **Add (Ajoutez)** 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`

STEP 10 | 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.

STEP 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. Pour plus d'informations, consultez la section Paramètres d'application personnalisables.

STEP 12 | (Facultatif) Activez l'utilisation de l'application mobile GlobalProtect.

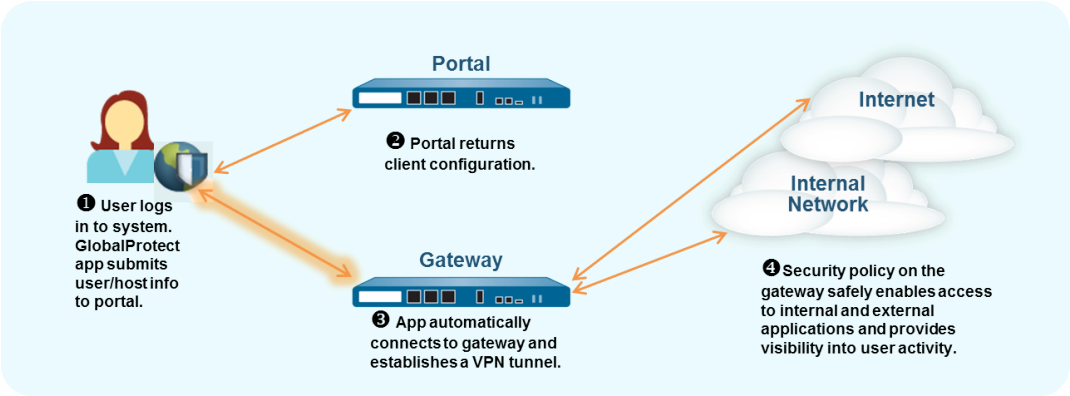
Achetez et installez un abonnement à GlobalProtect (**Device (Périphérique)** > **Licenses (Licences)**) pour activer l'utilisation de l'application.

STEP 13 | Enregistrez la configuration GlobalProtect.

Cliquez sur **Commit (Valider)**.

Configuration de VPN toujours active

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.

STEP 1 | Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, puis sélectionnez une configuration du portail.

STEP 2 | À l'onglet **Agent (Agent)**, sélectionnez la configuration de l'agent que vous souhaitez modifier.

STEP 3 | Sélectionnez **App (Application)**, puis définissez la **Connect Method (Méthode de connexion)** sur **User-logon (Always On) (Connexion-Utilisateur (Toujours Activée))**.

STEP 4 | Cliquez sur **OK** pour enregistrer la configuration client.

STEP 5 | Répétez les étapes 2 à 4 pour chaque configuration de l'agent que vous souhaitez modifier.

STEP 6 | Cliquez sur **OK (OK)** pour enregistrer la configuration du portail, puis sur **Commit (Valider)** pour valider vos modifications.

VPN d'accès à distance avec pré-ouverture de session

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 politiques doivent autoriser l'accès uniquement aux services de base qui sont indispensables pour démarrer le système, tels que DHCP, DNS, Active Directory (pour modifier un mot de passe expiré par exemple), antivirus et/ou aux 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).

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.

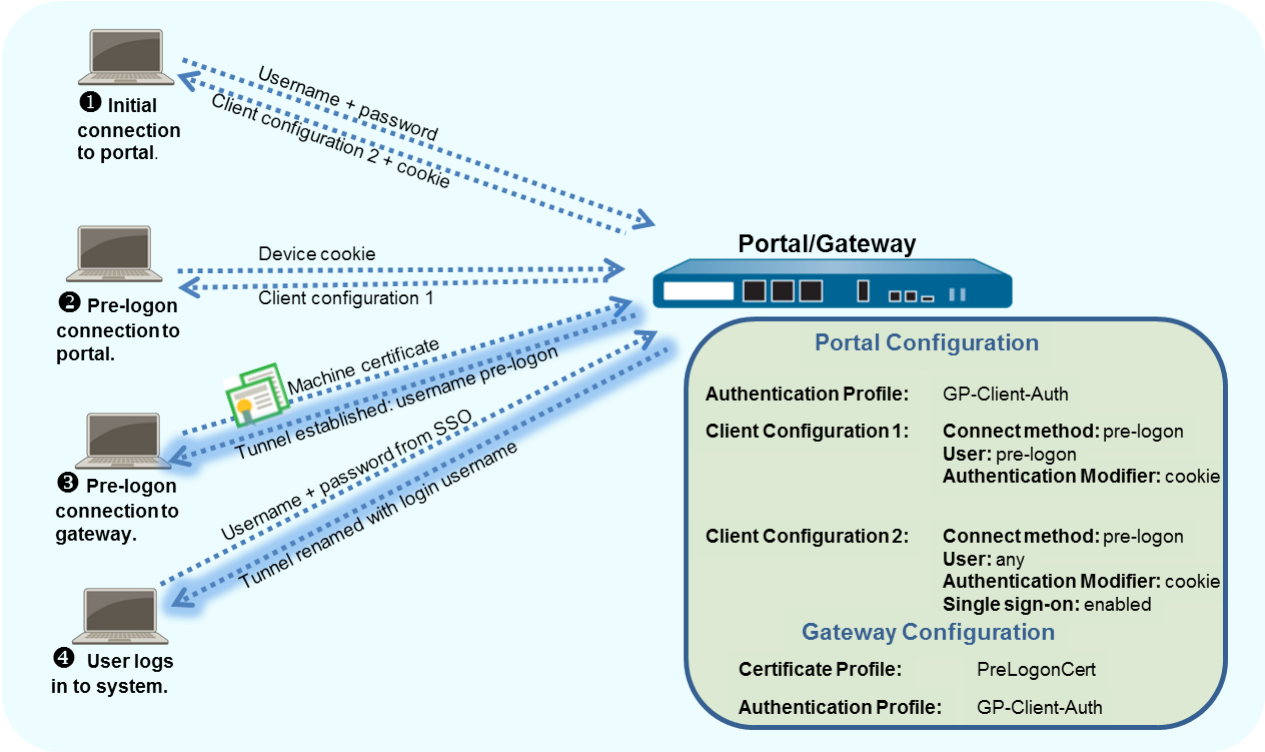
Les points de terminaison Windows se comportent différemment des points de terminaison macOS en ce qui a trait à la pré-ouverture de session. Avec les points de terminaison MacOS, le tunnel créé pour la pré-connexion est déchiré et un nouveau tunnel est créé lorsque l'utilisateur se connecte.

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.



Cet exemple utilise la topologie GlobalProtect illustrée dans VPN GlobalProtect pour l'accès à distance.

STEP 1 | Créer 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 (ethernet1/2)**.
  2. Sélectionnez **Layer3 (Couche 3)** dans la liste déroulante **Interface Type (Type d'interface)**.

3. À l'onglet **Config (Configuration)**, **Assign interface to (Affecter l'interface au) 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 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 (Ajoutez)** 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`.

STEP 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.
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.

STEP 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.

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.

STEP 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)

STEP 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. Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**, puis **Import (Importez)** 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**.

STEP 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 clients est référencé dans le profil de certificat en plus du certificat AC qui a généré les certificats machines s'ils sont différents.

1. Sélectionnez **Device (Périphérique)** > **Certificates (Certificats)** > **Certificate Management (Gestion de Certificats)** > **Certificate Profile (Profil de certificat)**, 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.

STEP 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 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. Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**, puis **Add (Ajoutez)** 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`

2. **Commit (Validez)** la configuration de passerelle.

STEP 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).

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, puis **Add (Ajoutez)** 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`

STEP 9 | Définissez les configurations de l'agent GlobalProtect pour les utilisateurs pré-logon et pour les utilisateurs enregistrés.

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 de terminaison. Si SSO n'est pas activé, le nom d'utilisateur enregistré dans le panneau paramètres de l'agent est utilisé.

Sélectionnez l'onglet **Agent** de la fenêtre **GlobalProtect Portal Configuration (Configuration du portail GlobalProtect)** (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **portal-config> (configuration du portail)**), puis **Add (Ajoutez)** 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)**.

STEP 10 | Enregistrez la configuration GlobalProtect.

Cliquez sur **Commit (Valider)**.

STEP 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 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.

Configuration de plusieurs passerelles GlobalProtect

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.

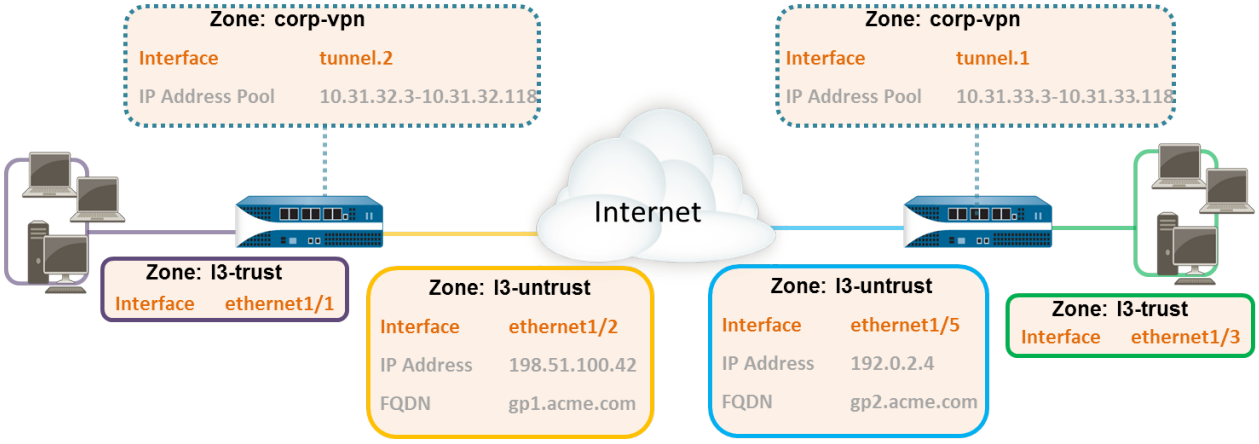


Figure 7: Topologie de multiples passerelles GlobalProtect

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.

STEP 1 | Créer 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 (Ajoutez)** 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**.

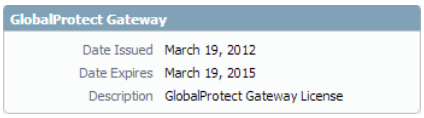
Sur le pare-feu hébergeant la seconde passerelle (gw2) :

- 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 (Ajoutez)** 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**.

STEP 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 de la manière suivante :

1. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
2. Sélectionnez **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**.
3. Lorsque vous y êtes invité, saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK**.
4. Vérifiez que la licence a été activée avec succès :



STEP 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)**).

STEP 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`.

STEP 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.

STEP 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`**

STEP 7 | Configurez les portails GlobalProtect.

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**. 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.

STEP 8 | Déployer l'agent logiciel GlobalProtect.

Sélectionnez **Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)** .

Dans cet exemple, suivez la procédure visant à héberger les mises à jour de l'application sur le portail.

STEP 9 | Enregistrez la configuration GlobalProtect.

Commit (Validez) la configuration sur le pare-feu hébergeant le portail et la ou les passerelle(s).

GlobalProtect pour l'archivage HIP interne et l'accès basé sur l'utilisateur

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.

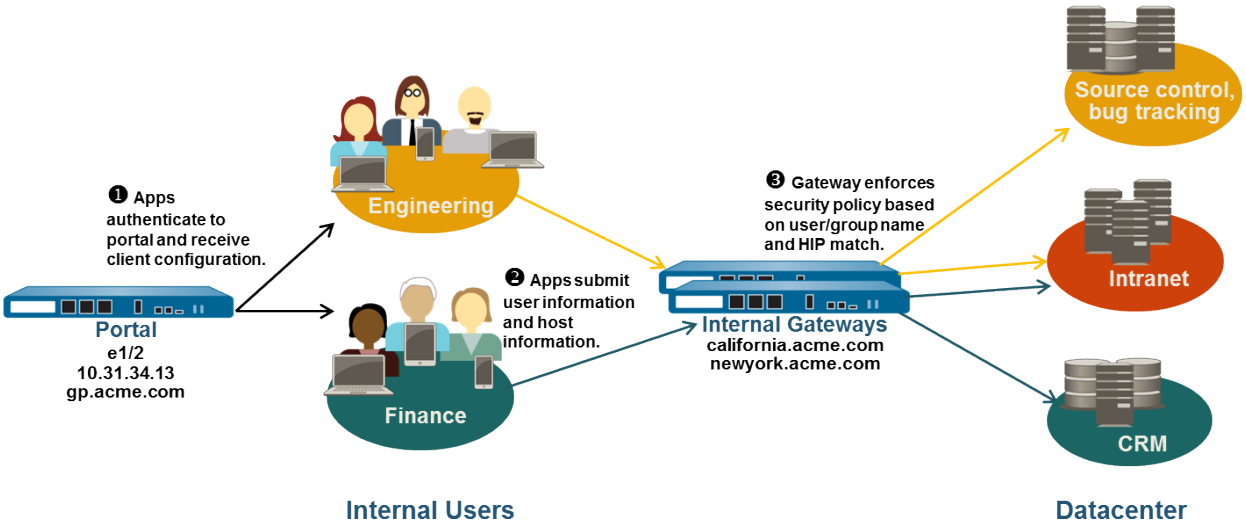


Figure 8: Configuration de passerelles internes GlobalProtect

Utilisez les étapes suivantes pour configurer une passerelle interne GlobalProtect.

STEP 1 | Créer des interfaces et des zones pour GlobalProtect

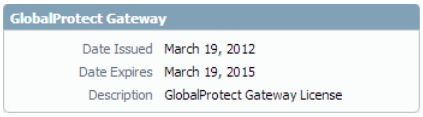
Dans cette configuration, vous devez configurer des interfaces sur chaque pare-feu hébergeant un portail et/ou une passerelle. Comme cette configuration utilise des passerelles internes uniquement, vous devez configurer le portail et les passerelles sur des interfaces sur le réseau interne.

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 la **Security Zone (Zone de sécurité)** `l3-trust` (**Network (Réseau)** > **Interfaces** > **Ethernet**).
2. **Activer l'identification de l'utilisateur** sur la zone `l3-de confiance`.

STEP 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 de la manière suivante :

1. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
2. Sélectionnez **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**.
3. Lorsque vous y êtes invité, saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK**.
4. Vérifiez que la licence a été activée avec succès.

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 GlobalProtect licences.

STEP 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.

STEP 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)

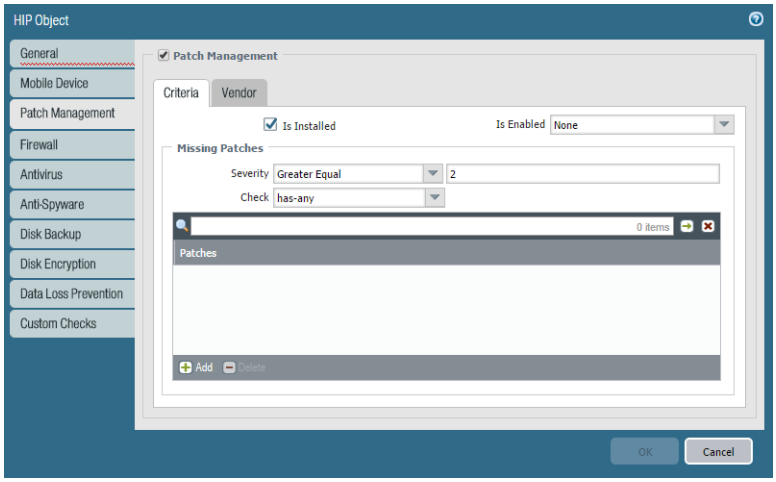
- Configurer l'authentification à deux facteurs (Jeton ou basé sur un MPUU)

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.

STEP 5 | Créez les profils HIP dont vous avez besoin pour mettre en œuvre les politiques de sécurité sur l'accès passerelle.

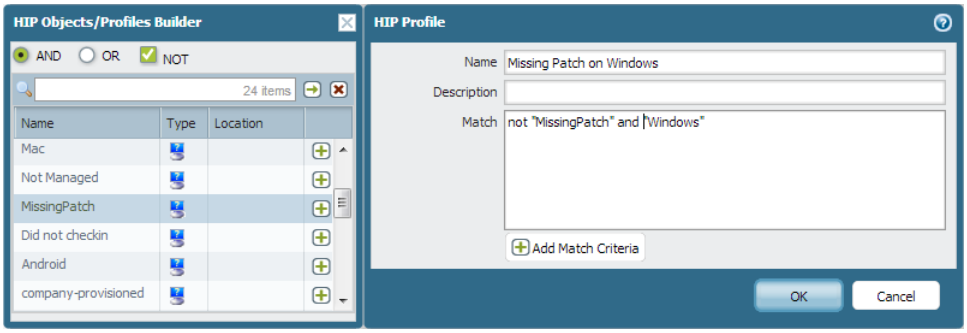
Reportez-vous à la section Informations de l'hôte pour plus d'informations sur les correspondances HIP.

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 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 :



STEP 6 | Configurez les passerelles internes.

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Gateways (Passerelles)**, puis sélectionnez une passerelle interne existante ou **Add (Ajoutez)**-en une nouvelle. Configurez les paramètres de passerelle 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.

STEP 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)).

Sélectionnez **Network (Réseau)** > **GlobalProtect (GlobalProtect)** > **Portals (Portails)**, puis sélectionnez un portail existant ou **Add (Ajoutez)**-en un nouveau. 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.

STEP 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.

STEP 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. Sélectionnez **Policies (Politiques)** > **Security (Sécurité)** et cliquez sur **Add (Ajouter)**.
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.

	Name	Tags	Source				Destination		Application	Service	Action
			Zone	Address	User	HIP Profile	Zone	Address			
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	

Configuration mixte de passerelles internes et externes

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.

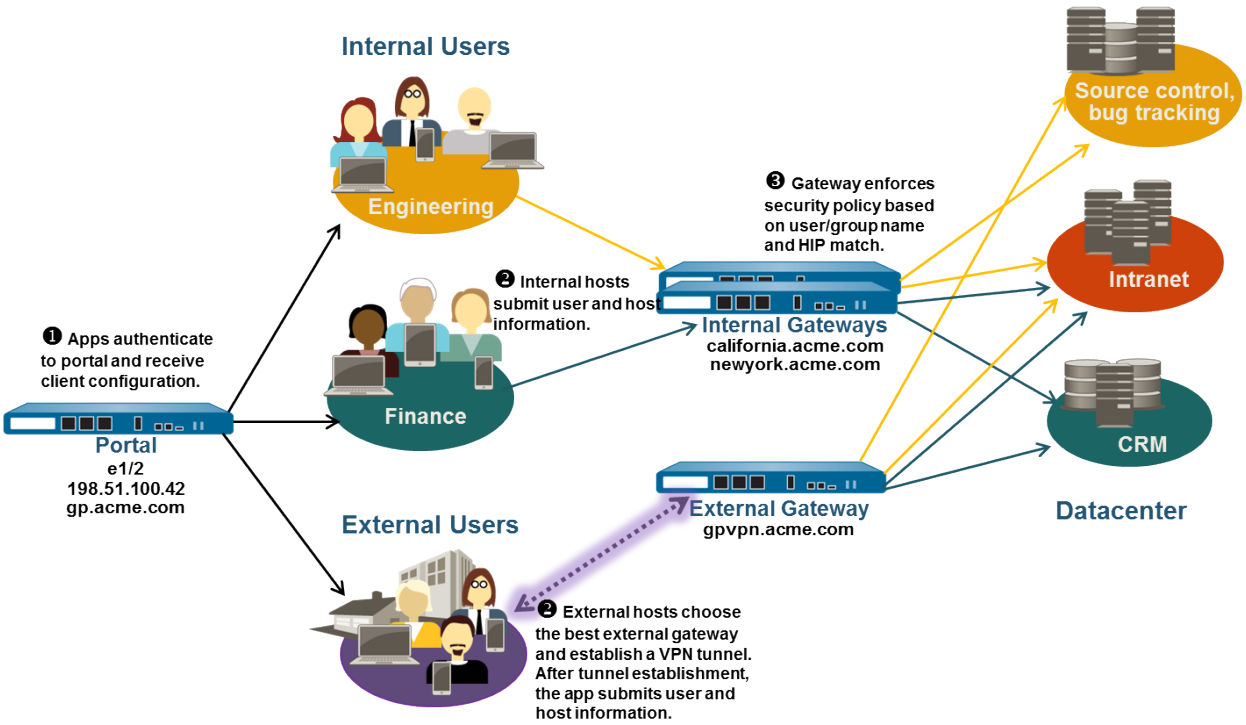


Figure 9: Déploiement de GlobalProtect avec des passerelles internes et externes

Utilisez les étapes suivantes pour configurer un mélange de passerelles GlobalProtect internes et externes.

STEP 1 | Créer 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 les attaques réussies.

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 (Ajoutez)** 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.

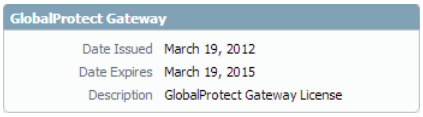
Sur le pare-feu hébergeant la passerelle externe (gpvpn.acme.com) :

- 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 **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 (Ajoutez)** 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.

STEP 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 :

1. Sélectionnez **Device (Périphérique)** > **Licenses (Licences)**.
2. Sélectionnez **Activate feature using authorization code (Activer la fonction à l'aide du code d'autorisation)**.
3. Lorsque vous y êtes invité, saisissez le **Authorization Code (Code d'autorisation)**, puis cliquez sur **OK (OK)**.
4. Vérifiez que la licence et les abonnements ont été activés avec succès.

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 GlobalProtect licences.

STEP 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.

STEP 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 :

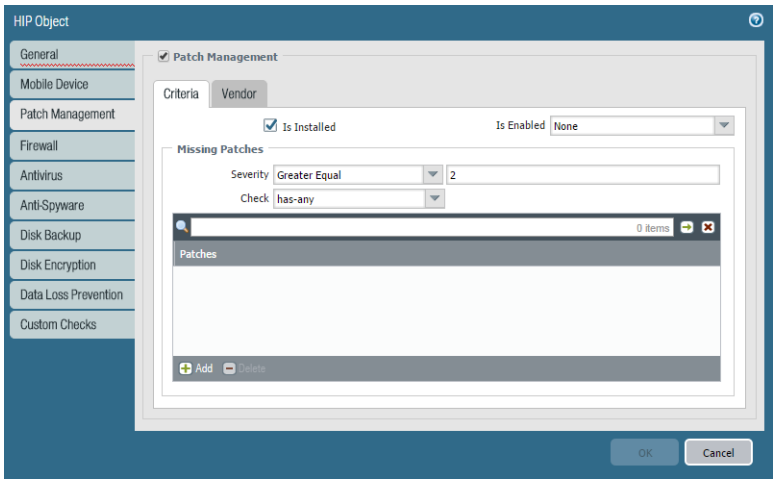
- Configurer l'authentification externe (profil d'authentification)
- Configurer l'authentification du certificat client (profil de certificat)
- Configurer l'authentification à deux facteurs (Jeton ou basé sur un MPUU)

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.

STEP 5 | Créez les profils HIP dont vous aurez besoin pour mettre en œuvre une politique de sécurité sur l'accès passerelle.

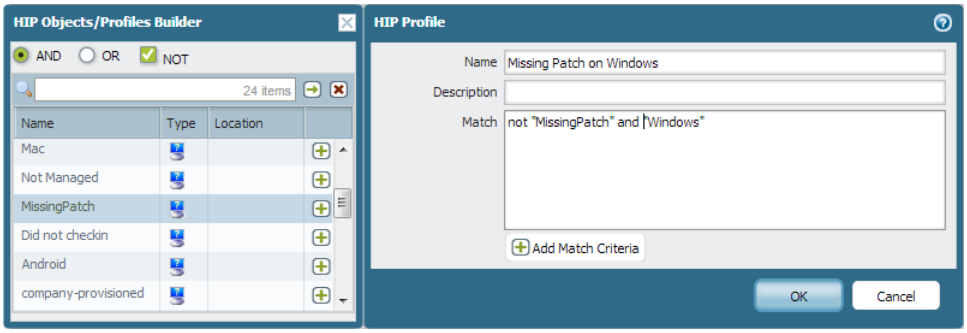
Reportez-vous à la section Informations de l'hôte pour plus d'informations sur les correspondances HIP.

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 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 :



STEP 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 de configuration de 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.

STEP 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/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`

   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:

   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.

STEP 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.

STEP 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		

STEP 10 | Enregistrez la configuration GlobalProtect.

Commit (Validez) vos configurations de portail et de passerelle.

Portail captif et application de GlobalProtect pour l’accès au réseau

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 que votre réseau soit exposé aux menaces de sécurité, vous pouvez également appliquer 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 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.

portail captif	Application de GlobalProtect pour l'accès au réseau	Flux de production
		• 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 : 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.

portail captif	Application de GlobalProtect pour l'accès au réseau	Flux de production
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.

STEP 1 | Paramétrer l'accès au portail GlobalProtect.

STEP 2 | Définir les configurations de l'agent GlobalProtect.

STEP 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 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.

STEP 4 | **Commit (Validez)** les modifications.

Architecture de GlobalProtect

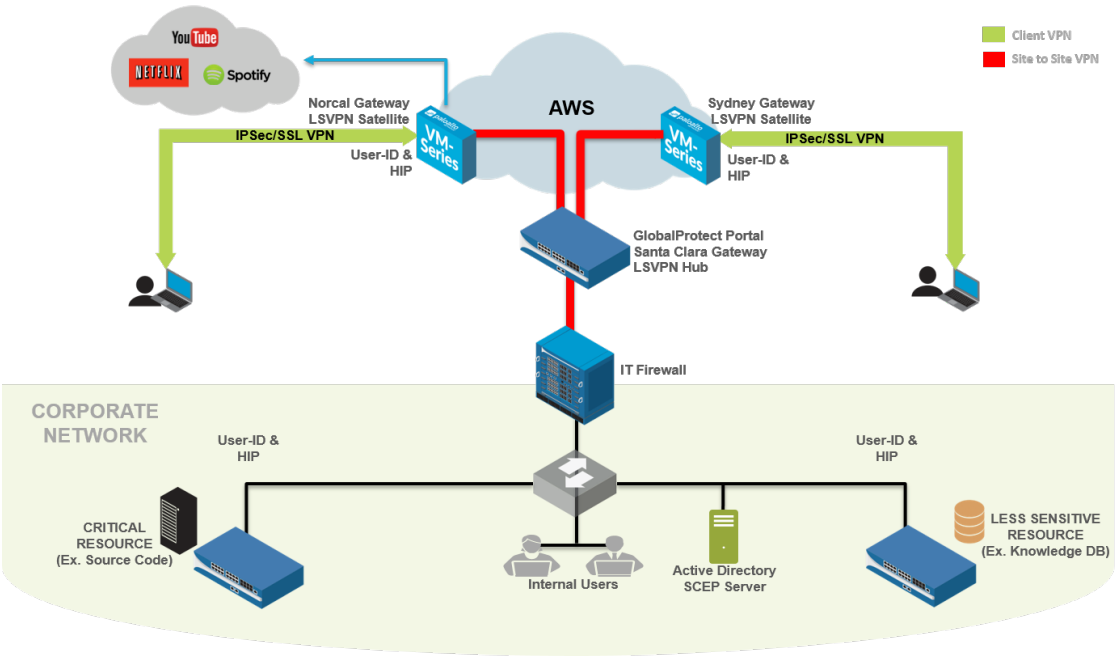
Cette section décrit un exemple d'architecture de référence pour le déploiement de GlobalProtect™ qui sécurise le trafic Internet et fournit un accès sécurisé aux ressources de l'entreprise.

L'architecture de référence et les lignes directrices décrites dans cette section fournissent un scénario de déploiement commun. Avant d'adopter cette architecture, identifiez votre sécurité corporative, la gestion des infrastructures et les exigences d'expérience des utilisateur finaux, puis déployez GlobalProtect en fonction de ces exigences.

Bien que les exigences puissent différer d'une entreprise à l'autre, vous pouvez exploiter les principes communs et les considérations de conception décrites dans ce document ainsi que les lignes directrices en matière de meilleures pratiques de configuration pour répondre à vos besoins de sécurité d'entreprise.

- Topologie de l'architecture de référence GlobalProtect
- Caractéristiques de l'architecture de référence GlobalProtect
- Configurations d'architecture de référence GlobalProtect

Topologie de l'architecture de référence GlobalProtect



- Portail GlobalProtect
- Passerelles GlobalProtect

Portail GlobalProtect

Dans cette topologie, un PA-020 dans l'espace de co-implantation fonctionne comme un portail GlobalProtect.

Les employés et les entrepreneurs peuvent s'authentifier sur le portail à l'aide d'une authentification à deux facteurs (2FA) composée d'informations d'identification Active Directory (AD) et d'un mot de passe ponctuel (MPUU). Le portail déploie des configurations clientes GlobalProtect basées sur l'appartenance à l'utilisateur, au groupe et au système d'exploitation.

En configurant une configuration de client portail distincte qui s'applique à un petit groupe ou à un ensemble d'utilisateurs pilotes, vous pouvez tester les fonctionnalités avant de les déployer sur une base d'utilisateurs plus large. Toute configuration client contenant de nouvelles fonctionnalités, telles que les fonctionnalités de GlobalProtect ou de protocole d'inscription simple (SCEP) qui ont été rendues disponibles avec Pan-OS 7.1 et les mises à jour de contenu qui suivent, est activée dans la configuration pilote d'abord et validée par ces utilisateurs pilotes, avant qu'il soient mis à la disposition des autres utilisateurs.

Le portail GlobalProtect insère également les configurations aux satellites GlobalProtect. Cette configuration comprend les passerelles GlobalProtect auxquelles les satellites peuvent se connecter et établir un tunnel de site à site.

Passerelles GlobalProtect

Le PA-3020 dans l'espace de co-implantation (mentionné précédemment) double également en tant que passerelle GlobalProtect (la passerelle de Santa Clara). 10 passerelles supplémentaires sont déployées dans

Amazon Web Services (AWS) et Microsoft Azure public Cloud. Les régions ou les emplacements POP où ces passerelles AWS et Azure sont déployées reposent sur la répartition des salariés à travers le globe.

- **Passerelle Santa Clara** : les employés et les entrepreneurs peuvent s'authentifier auprès de la passerelle de Santa Clara (PA-3020 dans l'espace de co-implantation) à l'aide de 2FA. Cette passerelle requiert que les utilisateurs fournissent leurs informations d'identification Active Directory et leur MPUU. Parce que cette passerelle protège les ressources sensibles, elle est configurée comme une passerelle manuelle. Par conséquent, les utilisateurs ne se connectent pas automatiquement à cette passerelle et doivent choisir manuellement de se connecter à cette passerelle. Par exemple, lorsque les utilisateurs se connectent à AWS-NorCal, qui n'est pas une passerelle manuelle uniquement, certaines ressources internes sensibles ne sont pas accessibles. L'utilisateur doit ensuite basculer manuellement vers et s'authentifier auprès de la passerelle de Santa Clara pour accéder à ces ressources.

  De plus, la passerelle de Santa Clara est configurée comme un point de terminaison de tunnel VPN (LSVPN) à grande échelle pour toutes les connexions satellites à partir des passerelles d'AWS et d'Azure. La passerelle Santa Clara est également configurée pour configurer un tunnel IPSec (Internet Protocol Security) au pare-feu informatique du siège social. C'est le tunnel qui donne accès aux ressources du siège social.
- **Passerelles dans Amazon Web services et Microsoft Azure** : cette passerelle requiert 2FA: un certificat client et des informations d'identification Active Directory. Le portail GlobalProtect distribue le certificat client qui est requis pour s'authentifier auprès de ces passerelles à l'aide de la fonctionnalité SCEP GlobalProtect.

  Ces passerelles dans le nuage public agissent également en tant que satellites GlobalProtect. Ils communiquent avec le portail GlobalProtect, téléchargent la configuration satellite et établissent un tunnel de site à site avec la passerelle de Santa Clara. Les satellites GlobalProtect s'authentifient initialement en utilisant les numéros de série et s'authentifient ensuite à l'aide de certificats.
- **Passerelles à l'intérieur du siège social** : dans le siège social, trois pare-feu fonctionnent comme passerelles GlobalProtect. Ce sont des passerelles internes qui ne nécessitent pas de points de terminaison pour installer un tunnel. Les utilisateurs s'authentifient à ces passerelles à l'aide de leurs informations d'identification Active Directory. Ces passerelles internes utilisent GlobalProtect pour identifier l'ID utilisateur et pour recueillir le profil d'information de l'hôte (HIP) à partir des points de terminaison.

  Pour rendre l'expérience utilisateur finale aussi homogène que possible, vous pouvez configurer ces passerelles internes pour authentifier les utilisateurs à l'aide de certificats configurés par SCEP ou en utilisant des tickets de service Kerberos.

Caractéristiques de l'architecture de référence GlobalProtect

Expérience de l'utilisateur final

Les utilisateurs finaux qui sont distants (à l'extérieur du réseau d'entreprise) se connectent à l'une des passerelles dans AWS ou Azure. Lorsque vous configurez la configuration client Portail GlobalProtect, affectez une priorité égale aux passerelles. Avec cette configuration, la passerelle vers laquelle les utilisateurs se connectent dépend du temps de réponse SSL de chaque passerelle mesurée sur le point de terminaison pendant la mise en place du tunnel.

Par exemple, un utilisateur en Australie se connectera typiquement à la passerelle AWS-Sydney. Après que l'utilisateur est connecté à AWS-Sydney, l'application GlobalProtect accorde des tunnels à tout le trafic depuis le point de terminaison vers le pare-feu AWS-Sydney pour inspection. GlobalProtect envoie le trafic vers les sites Internet publics directement via la passerelle AWS-Sydney et augmente le trafic des tunnels vers les ressources de l'entreprise grâce à un tunnel de site à site entre la passerelle AWS-Sydney et la passerelle Santa Clara, puis via un tunnel site-à-site IPsec au siège de l'entreprise. Cette architecture est conçue pour réduire toute latence que l'utilisateur peut éprouver lors de l'accès à l'Internet. Si la passerelle AWS-Sydney (ou toute passerelle plus proche de Sydney) était inaccessible, l'application GlobalProtect retourne le trafic Internet vers le pare-feu au siège social et provoque des problèmes de latence.

Les serveurs Active Directory résident dans le réseau d'entreprise. Lorsque les utilisateurs distants s'authentifient, l'application GlobalProtect envoie des demandes d'authentification via le tunnel site-à-site d'AWS/Azure à la passerelle de Santa Clara. La passerelle transmet ensuite la demande via un tunnel de site-à-site IPsec au serveur Active Directory du siège social.

Pour réduire le temps qu'il faut pour l'authentification des utilisateurs distants et configurer le tunnel, envisagez de reproduire le serveur Active Directory et de le rendre disponible dans AWS.

Les utilisateurs finaux à l'intérieur du réseau d'entreprise s'authentifient auprès des trois passerelles internes immédiatement après leur connexion. L'application GlobalProtect envoie le rapport HIP à ces passerelles internes. Les utilisateurs qui sont à l'intérieur du bureau sur le réseau d'entreprise doivent répondre aux exigences de l'ID utilisateur et de HIP pour accéder à toute ressource au travail.

Gestion et journalisation

Dans ce déploiement, vous pouvez gérer et configurer tous les pare-feux de Panorama, qui est déployé dans l'espace de co-implantation.

Pour assurer une sécurité cohérente, tous les pare-feu dans AWS et Azure utilisent les mêmes stratégies et configurations de sécurité. Pour simplifier la configuration des passerelles, panorama utilise également un groupe de périphériques et un modèle. Dans ce déploiement, toutes les passerelles transfèrent tous les journaux vers Panorama. Cela vous permet de surveiller le trafic réseau ou de dépanner les problèmes d'un emplacement central au lieu de vous obliger à vous connecter à chaque pare-feu.

Lorsque des mises à jour logicielles sont requises, vous pouvez utiliser Panorama pour déployer les mises à jour logicielles de tous les pare-feux. Panorama met d'abord à jour un ou deux pare-feux et vérifie si la mise à niveau a réussi avant de mettre à jour les pare-feu restants.

Surveillance et haute disponibilité

Pour surveiller les pare-feu dans ce déploiement, vous pouvez utiliser Nagios, un serveur open-source, un réseau et un logiciel de surveillance des journaux. Configurez Nagios pour vérifier périodiquement la réponse à partir du portail et de la page de connexion préalable de passerelles et envoyez une alerte si la réponse ne correspond pas aux attentes. Vous pouvez également configurer les objets de base de l'information de gestion (MIB) de GlobalProtect Simple Network Management Protocol (SNMP) pour surveiller l'utilisation de la passerelle.

Dans ce déploiement, il n'y a qu'une seule instance du portail GlobalProtect. Si le portail n'est pas disponible, les nouveaux utilisateurs (qui n'ont jamais été connectés au portail avant) ne pourront pas se connecter à GlobalProtect. Toutefois, les utilisateurs existants peuvent utiliser la configuration du client Portail mise en cache pour se connecter à l'une des passerelles.

Plusieurs pare-feu de machine virtuelle (VM) dans AWS configurés comme passerelles GlobalProtect fournissent une redondance de passerelle. Par conséquent, la configuration des passerelles en tant que paire haute disponibilité (HD) n'est pas nécessaire.

Configurations d'architecture de référence GlobalProtect

Pour aligner votre déploiement avec l'architecture de référence, examinez les listes de vérifications de configuration suivantes.

- Configuration de passerelle
- Portail
- Configurations de stratégie

Configuration de passerelle

- Désactivez la segmentation de tunnel. Pour ce faire, assurez-vous qu'il n'y a pas d'itinéraires d'accès spécifiés dans les paramètres **Agent** > **Clients Settings (Paramètres client)** > **Split Tunnel (Segmentation de tunnel)**. Reportez-vous à la section Configurer une passerelle GlobalProtect.
- Activez **No direct access to local network (Aucun accès direct au réseau local)** dans **Agent** > **Client Settings (Paramètres client)** > **Split Tunnel (Segmentation de tunnel)**. Reportez-vous à la section Configurer une passerelle GlobalProtect.
- Activez la passerelle pour **Accept cookie for authentication override (Accepter le cookie pour la substitution d'authentification)**. Reportez-vous à la section Configurer une passerelle GlobalProtect.

Portail

- Configurez la **Connect Method (méthode de connexion)** comme **Always-on (User logon) (Toujours activée (ouverture de session utilisateur))**. Voir la section Personnaliser l'application GlobalProtect.
- Réglez l'**Use Single Sign-On (Windows only) (Utilisation de l'authentification unique (Windows uniquement))** sur **Yes (Oui)**. Voir la section Personnaliser l'application GlobalProtect.
- Configurez le portail pour **Save User Credentials (enregistrer les informations d'identification de l'utilisateur)** (définissez la valeur sur **Yes (Oui)**). Voir Définir les configurations de l'agent GlobalProtect.
- Activez la passerelle pour **Accept cookie for authentication override (accepter le cookie pour la substitution d'authentification)**. Voir Définir les configurations de l'agent GlobalProtect.
- Configurez la **Cookie Lifetime (durée de vie des cookies)** sur 20 heures. Voir Définir les configurations de l'agent GlobalProtect.
- **Enforce GlobalProtect (Appliquer GlobalProtect)** pour l'accès au réseau. Voir la section Personnaliser l'application GlobalProtect.
- Quand **Enforce GlobalProtect for Network Access (Appliquer GlobalProtect pour l'accès au réseau)** est activé, cela permet aux utilisateurs de désactiver l'application GlobalProtect avec un mot de passe. Voir la section Personnaliser l'application GlobalProtect.
- Configurez la **Internal Host Detection (détection interne de l'hôte)**. Voir Définir les configurations de l'agent GlobalProtect.
- Activez l'option **Collect HIP Data (collecter les données HIP)** dans la collecte de données. Voir Définir les configurations de l'agent GlobalProtect.
- Distribuer et installer le certificat SSL avant le Proxy CA utilisé pour le déchiffrement SSL. Voir Définir les configurations de l'agent GlobalProtect.

Configurations de stratégie

- Configurez tous les pare-feux pour utiliser les stratégies de sécurité et les profils basés sur la stratégie idéale de sécurité de la passerelle Internet. Dans ce déploiement de référence, il y a la passerelle Santa Clara dans l'espace de co-implantation et les passerelles dans le cloud public AWS / Azure.

- Activer le décryptage SSL sur toutes les passerelles d'AWS et d'Azur.
- Configurez les règles de transfert basées sur la stratégie pour toutes les passerelles d'AWS pour transférer du trafic vers certains sites Web via la passerelle Santa Clara. Cela garantit que les sites comme www.StubHub.com et www.Lowes.com qui bloquent le trafic des gammes d'adresses IP AWS sont toujours accessibles lorsque les utilisateurs se connectent aux passerelles d'AWS.

Cryptographie de GlobalProtect

À propos de la sélection de chiffrement GlobalProtect

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

La figure suivante montre l'échange de chiffrement entre les passerelles GlobalProtect et les applications GlobalProtect lors de la création du tunnel VPN.

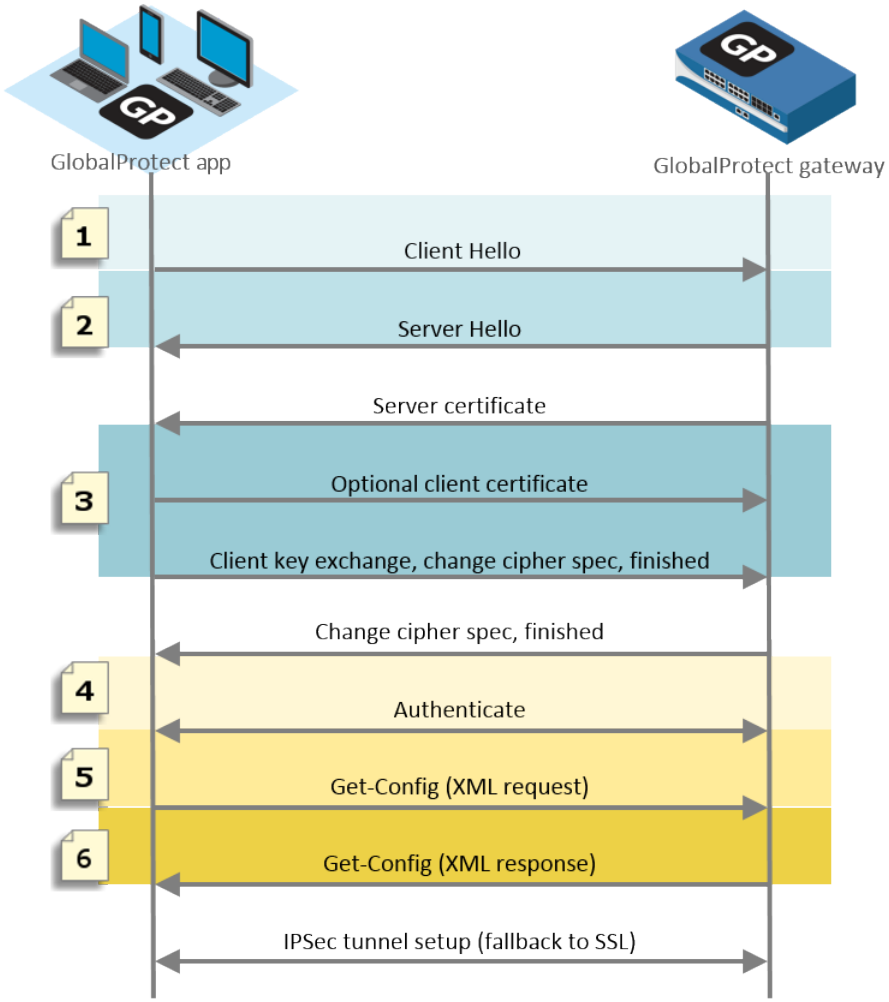


Figure 10: Échange de chiffrement entre l'application et la passerelle

Le tableau suivant décrit ces étapes plus en détail.

Table 9: 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

Étape de communication	Description
	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.

Table 10: 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 (Référence : Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison MacOS)
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.
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.

Références de la cryptographie de GlobalProtect

Référence : Fonctions cryptographiques de l'application GlobalProtect

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 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,

Fonction crypto	Clé	Usage
		même s'il est nécessaire pendant la configuration.

Suites de chiffrement TLS prises en charge par les applications GlobalProtect

Les sections suivantes fournissent des exemples de chiffrements TLS pris en charge sur les applications GlobalProtect installées sur divers systèmes d'exploitation de point de terminaison. Les listes ne sont pas exhaustives pour tous les systèmes d'exploitation pris en charge.

- Référence : Chiffrements TLS pris en charge par les agents GlobalProtect sur les postes de travail de type macOS
- Référence : Chiffrements TLS pris en charge par les agents GlobalProtect sur les points de terminaison Windows 7
- Référence : Chiffrements TLS pris en charge par les agents GlobalProtect sur les points de terminaison Android 6.0.1
- Référence : Chiffrements TLS pris en charge par les agents GlobalProtect sur les points de terminaison iOS 10.2.1
- Référence : Chiffrements TLS pris en charge par les agents GlobalProtect sur les Chromebooks

Référence : 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)

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison MacOS	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
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)

Référence : Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Windows 7

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Windows 7	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384 (0xc02c)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384 (0xc024)	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_SHA (0xc00a)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Windows 7	
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Référence : Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison Android 6.0.1

L'application GlobalProtect pour Android 6.0.1 prend en charge 20 suites de chiffrement.

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)
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)

Référence : Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison iOS 10.2.1

L'application GlobalProtect pour iOS 10.2.1 prend en charge 19 suites de chiffrement.

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)

Chiffrements TLS pris en charge par les applications GlobalProtect sur les points de terminaison iOS 10.2.1	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_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)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Référence : Chiffrements TLS pris en charge par les applications GlobalProtect sur les Chromebooks

L'application GlobalProtect pour Chrome OS 55.0.2883 prend en charge 91 suites de chiffrement.

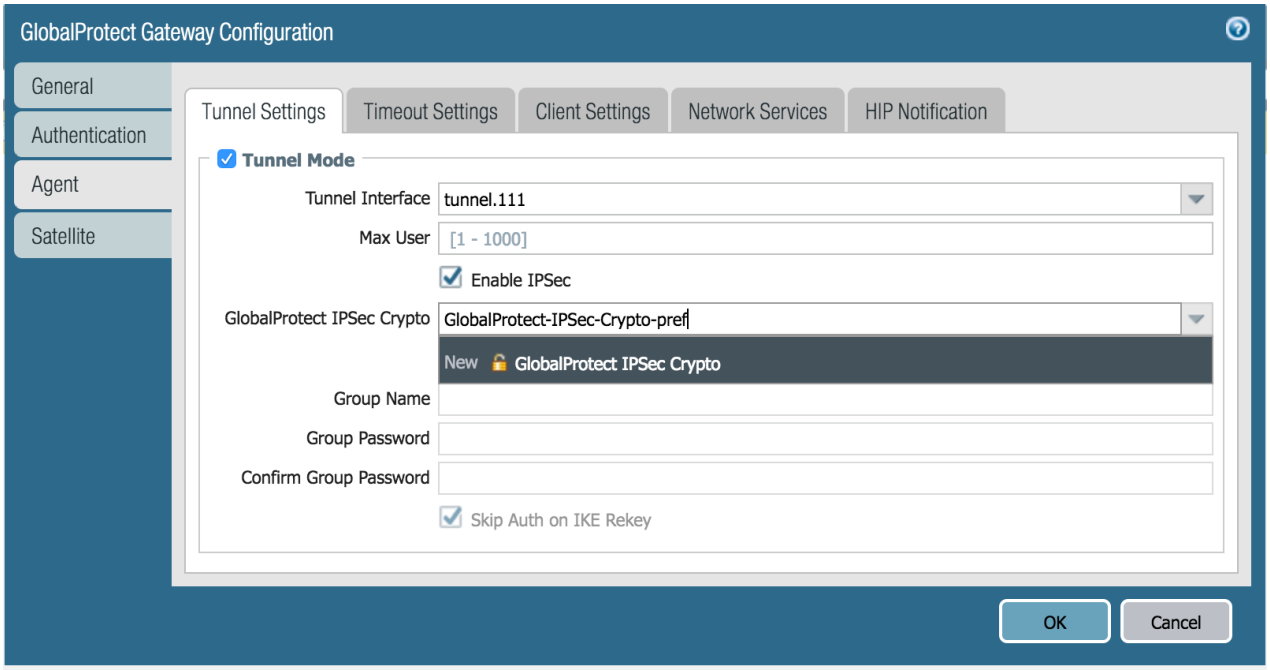
Chiffrements TLS pris en charge par les applications GlobalProtect sur les Chromebooks (Chrome OS 55.0.2883)	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0085)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (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_RSA_WITH_AES_256_CBC_SHA (0x0035)

Chiffrements TLS pris en charge par les applications GlobalProtect sur les Chromebooks (Chrome OS 55.0.2883)	
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x0068)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256 (0xc023)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037)	TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4)
TLS_DH_DSS_WITH_AES_256_CBC_SHA (0x0036)	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0)
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0086)	
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_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_RSA_WITH_RC4_128_MD5 (0x0004)
	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)

Chiffrements TLS pris en charge par les applications GlobalProtect sur les Chromebooks (Chrome OS 55.0.2883)	
TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
TLS_DH_RSA_WITH_SEED_CBC_SHA (0x0098)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_DH_DSS_WITH_SEED_CBC_SHA (0x0097)	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA (0x0010)
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA (0x000d)
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0043)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0042)	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)	TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)	TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_DH_RSA_WITH_DES_CBC_SHA (0x000f)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)	TLS_DH_DSS_WITH_DES_CBC_SHA (0x000c)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_RSA_WITH_DES_CBC_SHA (0x0009)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

Chiffrements utilisés pour configurer les tunnels IPsec

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> (configuration de la passerelle)** > **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.

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.

API SSL

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.