paloalto TECHDOCS

Guide de l'utilisateur de l'application GlobalProtect

Version 6.3

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Last Revised

October 24, 2024

Table des matières

Chapitre 1 : Application GlobalProtect pour Windows..... 5

Téléchargement et installation de l'application GlobalProtect pour Windows..... 6
Utilisation de Se connecter avant identification..... 9
Connect Before Logon Using Smart Card Authentication (Se connecter avant identification en utilisant l'authentification Smart card)..... 10
Connect Before Logon Using SAML Authentication (Se connecter avant identification en utilisant l'authentification SAML)..... 15
Connect Before Logon Using Username/Password-Based Authentication (Se connecter avant identification en utilisant l'authentification basée sur un nom d'utilisateur/mot de passe)..... 20
Utilisation de Single Sign-On (ouverture de session unique - SSO) pour l'authentification par carte intelligente..... 26
Utilisation de l'application GlobalProtect pour Windows..... 29
Révéler le mot de passe sur l'écran de connexion Windows pour GlobalProtect..... 41
Signaler un problème depuis l'application GlobalProtect pour Windows..... 43
Déconnexion de l'application GlobalProtect pour Windows..... 46
Désinstallation de l'application GlobalProtect pour Windows..... 49
Résoudre un conflit de programmes d'installation de Microsoft..... 50

Chapitre 2 : Application GlobalProtect pour macOS..... 51

Téléchargement et installation de l'application GlobalProtect pour macOS..... 52
Utilisation de l'application GlobalProtect pour macOS..... 59
Signaler un problème depuis l'application GlobalProtect pour macOS..... 74
Déconnexion de l'application GlobalProtect pour macOS..... 79
Désinstallation de l'application GlobalProtect pour macOS..... 81
Suppression de l'extension du noyau de l'exécutant GlobalProtect..... 86
Activation de l'application GlobalProtect pour macOS afin d'utiliser des certificats clients pour l'authentification..... 87

Chapitre 3 : Application GlobalProtect pour iOS..... 89

Téléchargement et installation de l'application GlobalProtect pour iOS..... 90
Utilisation de l'application GlobalProtect pour iOS..... 91
Signaler un problème depuis l'application GlobalProtect pour iOS..... 96
Installation de l'application GlobalProtect pour iOS..... 99

Chapitre 4 : Application GlobalProtect pour Android..... 101

Téléchargement et installation de l'application GlobalProtect pour Android..... 102
Téléchargement et installation de l'application GlobalProtect pour Android sur Chromebooks..... 103
Utilisation de l'application GlobalProtect pour Android..... 105

Signaler un problème depuis l'application GlobalProtect pour Android 109
Déconnexion de l'application GlobalProtect pour Android 112
Désinstallation de l'application GlobalProtect pour Android 114
Désinstallation de l'application GlobalProtect pour Android depuis des Chromebooks 115

Chapitre 5 : Application GlobalProtect pour Linux 117

Téléchargement et installation de l'application GlobalProtect pour Linux 118
Téléchargement et installation de la version GUI de GlobalProtect pour Linux 118
Téléchargement et installation de la version CLI de GlobalProtect pour Linux 120
Installation de l'application GlobalProtect pour Linux 123
Utilisation de la version GUI de l'application GlobalProtect pour Linux 123
Utilisation de la version CLI de l'application GlobalProtect pour Linux 126
Signaler un problème depuis l'application GlobalProtect pour Linux 130
Déconnexion de l'application GlobalProtect pour Linux 133
Déconnexion de l'application GlobalProtect pour Linux en utilisant la version GUI 133
Déconnexion de l'application GlobalProtect pour Linux en utilisant la version CLI 134
Désinstallation de l'application GlobalProtect pour Linux 136

Chapitre 6 : Exigences de GlobalProtect pour les périphériques IoT 137

Application GlobalProtect pour Windows

GlobalProtect™ est une application qui s'exécute sur votre terminal (ordinateur de bureau, ordinateur portable, tablette ou téléphone intelligent) pour vous protéger en utilisant les mêmes politiques de sécurité qui protègent les ressources sensibles de votre réseau d'entreprise. GlobalProtect™ sécurise votre centre de données, votre cloud privé, votre cloud public et votre trafic Internet et vous permet d'accéder aux ressources de votre entreprise où que vous soyez dans le monde.

Les rubriques suivantes décrivent comment installer et utiliser l'application GlobalProtect pour Windows :

- Téléchargement et installation de l'application GlobalProtect pour Windows
- Utilisation de Se connecter avant identification
- Utilisation de Single Sign-On (ouverture de session unique - SSO) pour l'authentification par carte intelligente
- Utilisation de l'application GlobalProtect pour Windows
- Signaler un problème depuis l'application GlobalProtect pour Windows
- Déconnexion de l'application GlobalProtect pour Windows
- Désinstallation de l'application GlobalProtect pour Windows
- Résoudre un conflit de programmes d'installation de Microsoft

Téléchargement et installation de l'application GlobalProtect pour Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Terminaux Windows uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Avant de vous connecter au réseau GlobalProtect, vous devez télécharger et installer l'application GlobalProtect sur votre terminal Windows. Pour vous assurer d'obtenir la bonne application pour le déploiement GlobalProtect ou Prisma Access de votre organisation, vous devez télécharger l'application directement depuis un portail GlobalProtect au sein de votre organisation. Pour cette raison, il n'y a pas de lien de téléchargement direct de l'application GP disponible sur le site de Palo Alto Networks.

Avant de pouvoir télécharger et installer l'application GP, vous devez obtenir l'adresse IP ou le Fully qualified domain name (nom de domaine complet - FQDN) du portail GlobalProtect auprès de votre administrateur GP. En outre, votre administrateur doit vérifier les informations de nom d'utilisateur et de mot de passe que vous pouvez utiliser pour vous connecter au portail et aux passerelles. Dans la plupart des cas, le nom d'utilisateur et le mot de passe sont les mêmes que ceux que vous utilisez pour vous connecter à votre réseau d'entreprise. Après avoir rassemblé les informations requises, utilisez les étapes suivantes pour télécharger et installer l'application :

Pour exécuter l'application GlobalProtect 5.0 et versions ultérieures, les terminaux Windows nécessitent Visual C++ Redistributables 12.0.3 pour Visual Studio 2013. Si vous n'avez pas déjà installé de packages redistribuables sur votre terminal, l'application GlobalProtect installe automatiquement Visual C++ Redistributables 12.0.3. Si vous avez déjà installé Visual C++ + Redistributables 12.0.2 ou une version antérieure, vous devez désinstaller les packages redistribuables existants de votre terminal ou passer à Visual C++ Redistributables 12.0.3 avant d'installer l'application GlobalProtect.

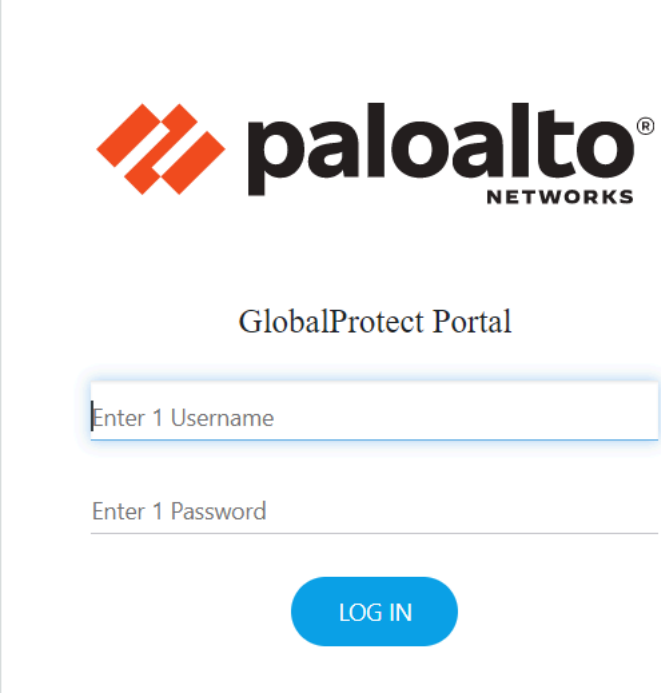
1. Connectez-vous au portail GlobalProtect.
   1. Lancez un navigateur Web et accédez à l'URL suivante :

      `https://<portal IP address or FQDN>`

      Exemple : **`http://gp.acme.com`**

      Si vous utilisez GlobalProtect 6.3 ou une version ultérieure et que vous avez prédéployé la fonctionnalité de portail intelligent, GlobalProtect vous redirige automatiquement vers le portail Prisma Access approprié en fonction de votre emplacement. Les portails définis dans la carte des pays du portail sont disponibles dans le menu déroulant. Pour plus d'informations, consultez la section Configuration du portail intelligent.
   2. Sur la page de connexion au portail, saisissez vos **Name (Nom)** (nom d'utilisateur) et **Password (Mot de passe)**, puis cliquez sur **LOG IN (Connexion)**. Dans la plupart des cas,

vous pouvez utiliser le même nom d'utilisateur et le même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise.



2. 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 êtes connecté au portail. Utilisez cette page pour télécharger le dernier package logiciel de l'application.

Si votre administrateur système a 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'application). Sélectionnez **GlobalProtect Agent (Agent GlobalProtect)** pour ouvrir la page de téléchargement.

3. Téléchargez l'application.

1. Pour commencer le téléchargement, cliquez sur le lien du logiciel qui correspond au système d'exploitation qui s'exécute sur votre ordinateur. Si vous n'êtes pas sûr si le système d'exploitation est 32 ou 64 bits, demandez à votre administrateur système avant de continuer.
2. Ouvrez le fichier d'installation du logiciel.
3. Lorsque vous y êtes invité, **Run (Exécutez)** le logiciel.
4. Lorsque vous y êtes invité à nouveau, **Run (Exécutez)** l'assistant de configuration GlobalProtect.

4. Terminez la configuration de l'application logicielle GlobalProtect.
   1. Dans l’assistant de configuration GlobalProtect, cliquez sur **Next (Suivant)**.
   2. Cliquez sur **Next (Suivant)** pour accepter le dossier d’installation par défaut (C:\Program Files\Palo Alto Networks\GlobalProtect), puis cliquez sur **Next (Suivant)** deux fois.

      *Bien que vous puissiez utiliser **Browse (Parcourir**) pour sélectionner un autre emplacement où installer l’application GlobalProtect, la meilleure pratique consiste à l’installer à l’emplacement par défaut. L’emplacement d’installation par défaut est en lecture seule pour les utilisateurs non privilégiés et par conséquent, l’installation à cet emplacement protège contre les accès malveillants à l’application.*
   3. Une fois l’installation terminée, **Close (Fermez)** l’assistant.

Utilisation de Se connecter avant identification

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Terminaux Windows uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Les méthodes de préouverture de session et préouverture de session puis connexion à la demande ne sont pas possibles de façon simultanée avec Se connecter avant identification.

L'option Se connecter avant identification n'est pas prise en charge pour les configurations de passerelles internes.

Pour simplifier le processus de connexion et améliorer votre expérience, GlobalProtect propose l'option Se connecter avant identification pour vous permettre d'établir la connexion VPN au réseau d'entreprise avant de vous connecter au terminal Windows 10 en utilisant une carte intelligente, un service d'authentification tel que LDAP, RADIUS ou Security Assertion Markup Language (SAML), une authentification basée sur un nom d'utilisateur/mot de passe, ou une authentification par One-Time Password (mot de passe à usage unique - OTP). Les administrateurs peuvent bénéficier de l'activation de Se connecter avant identification lorsqu'ils intègrent de nouveaux utilisateurs GlobalProtect sur le terminal qui n'est pas configuré avec un profil local ou un compte pour l'utilisateur. L'option Se connecter avant identification est désactivée par défaut. Lorsque l'administrateur active Se connecter avant identification, vous pouvez lancer le fournisseur d'identifiants de l'application GlobalProtect et vous connecter au réseau d'entreprise avant de vous connecter au terminal Windows. Une fois que Se connecter avant identification a établi une connexion VPN, vous pouvez utiliser l'écran de connexion Windows pour vous connecter au terminal Windows. GlobalProtect peut agir en tant que fournisseur d'identifiants d'accès préconnexion (PLAP) pour fournir un accès à votre organisation avant de vous connecter à Windows.

Parce que Se connecter avant identification vous demande de vous authentifier deux fois sur le portail et la passerelle lors de la connexion au terminal Windows pour la première fois, le cookie de contournement d'authentification ne fonctionne pas comme prévu.

Pour utiliser Se connecter avant identification, l'administrateur doit déployer les paramètres dans le registre Windows et vous devez choisir la méthode d'authentification :

- Connect Before Logon Using Smart Card Authentication (Se connecter avant identification en utilisant l'authentification Smart card)
- Connect Before Logon Using SAML Authentication (Se connecter avant identification en utilisant l'authentification SAML)
- Connect Before Logon Using Username/Password-Based Authentication (Se connecter avant identification en utilisant l'authentification basée sur un nom d'utilisateur/mot de passe)

Connect Before Logon Using Smart Card Authentication (Se connecter avant identification en utilisant l'authentification Smart card)

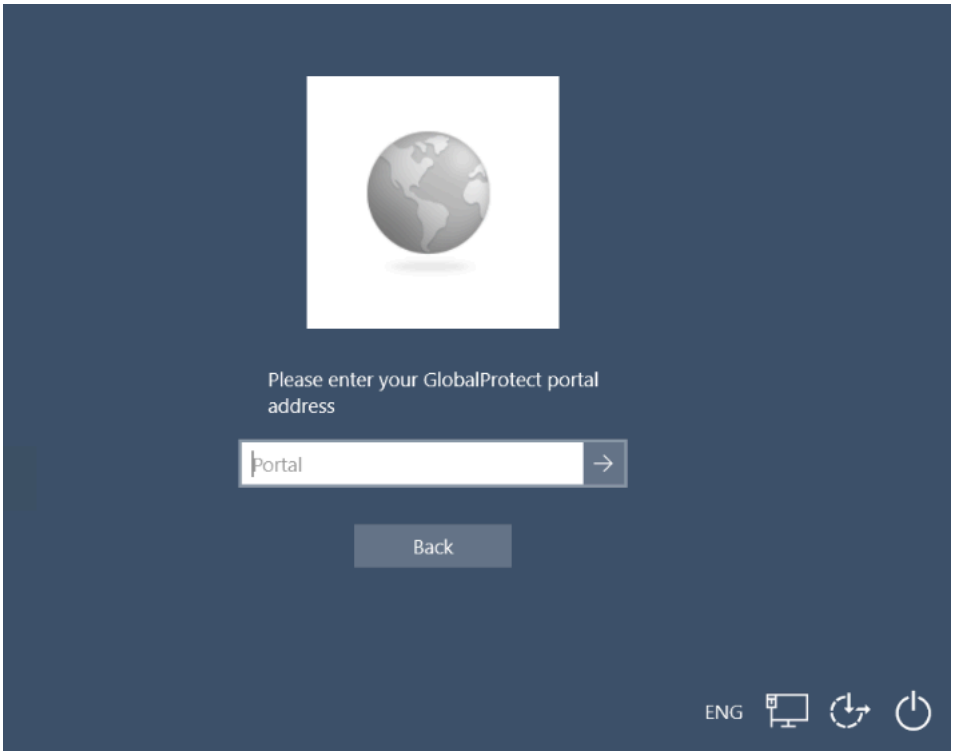
Se connecter avant identification prend en charge l'authentification par carte intelligente. L'administrateur doit importer le certificat CA racine qui a émis les certificats contenus sur la carte intelligente sur le portail et la passerelle. L'administrateur peut appliquer le profil de certificat et cette CA racine à votre configuration de portail ou de passerelle pour permettre l'utilisation de la carte intelligente dans le processus d'authentification. Vous pouvez vous authentifier à GlobalProtect avant de vous connecter au terminal Windows en utilisant une carte intelligente. Lorsque vous y êtes invité, insérez votre carte intelligente pour vérifier que l'authentification par carte intelligente est réussie. Si l'authentification par carte intelligente est réussie, GlobalProtect se connecte au portail ou à la passerelle spécifiée dans la configuration.

1. Avant de pouvoir utiliser Se connecter avant identification, l'administrateur doit avoir complété les tâches suivantes :
   1. Déployez les paramètres de Se connecter avant identification dans le registre de Windows.
   2. Configurez la carte intelligente pour l'authentification à deux facteurs.
   3. Attribuez le profil de certificat au portail GlobalProtect.
   4. Configurez la passerelle pour authentifier les utilisateurs finaux sur la base d'une carte intelligente.
2. Connectez-vous au terminal Windows en utilisant Se connecter avant identification.
   1. Cliquez sur le bouton **Network Sign-In (Connexion au réseau)** () dans le coin inférieur droit de l'écran de connexion Windows.

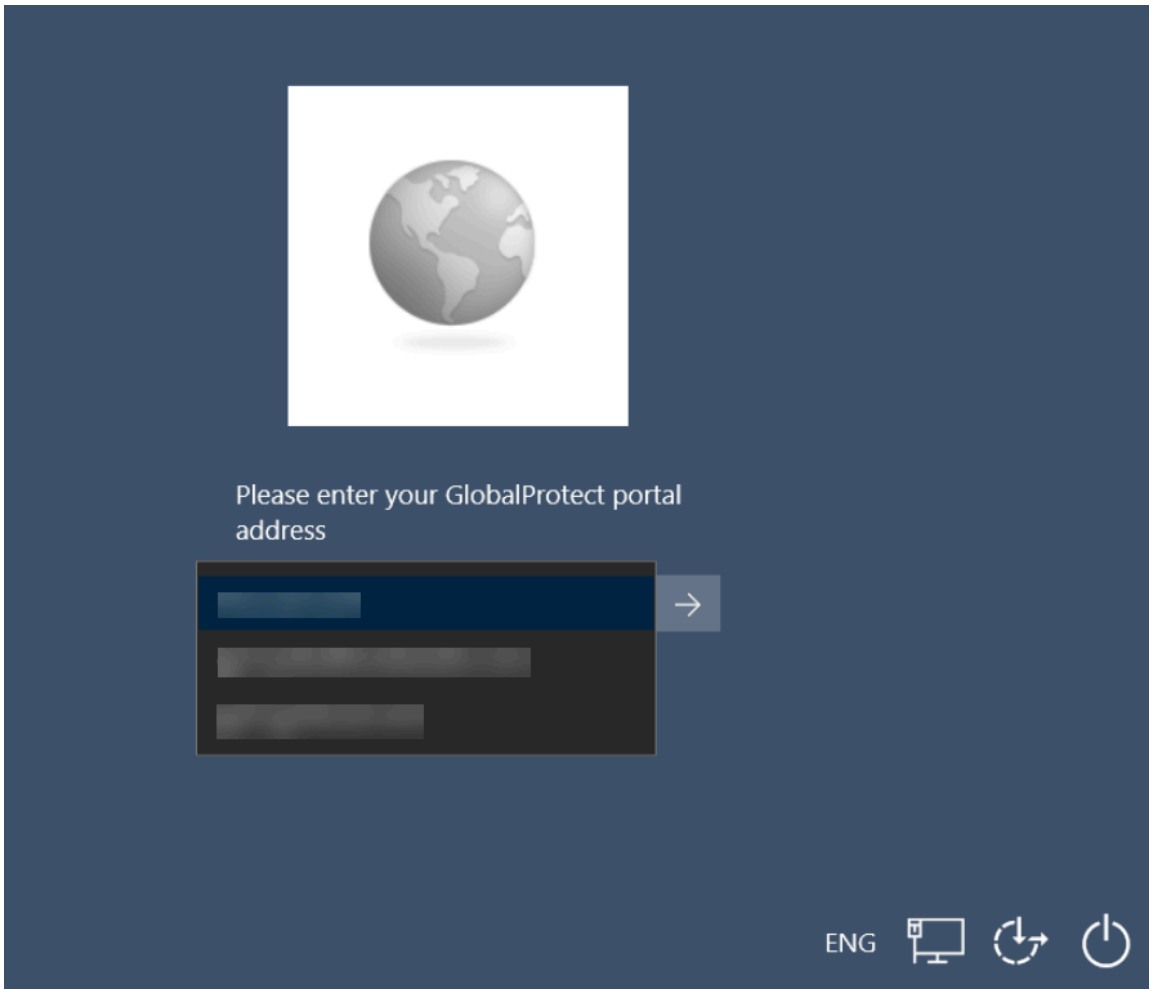
      Si la connexion VPN est réussie, le bouton **Disconnect (Déconnecter)** () apparaît à côté du bouton **Network Sign-In (Connexion au réseau)** de l'écran de connexion

Windows. Vous êtes déconnecté du VPN si vous ne vous êtes pas encore connecté à votre terminal dans le délai configuré. Cela provoque la déconnexion du tunnel VPN.

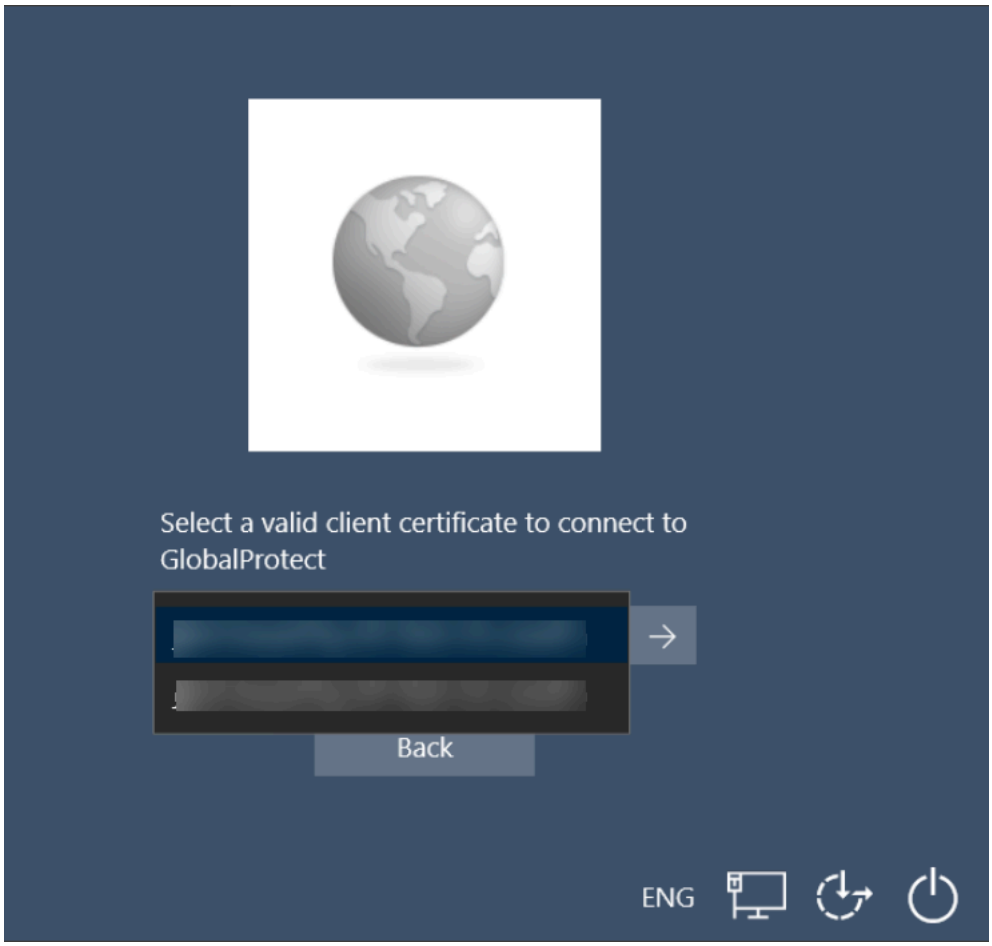
2. (Facultatif) Si vous vous connectez au terminal pour la première fois et que les portails n'ont pas été prédéfinis par l'administrateur, entrez le FQDN ou l'adresse IP du portail GlobalProtect, puis sur **Submit (Soumettre)**.



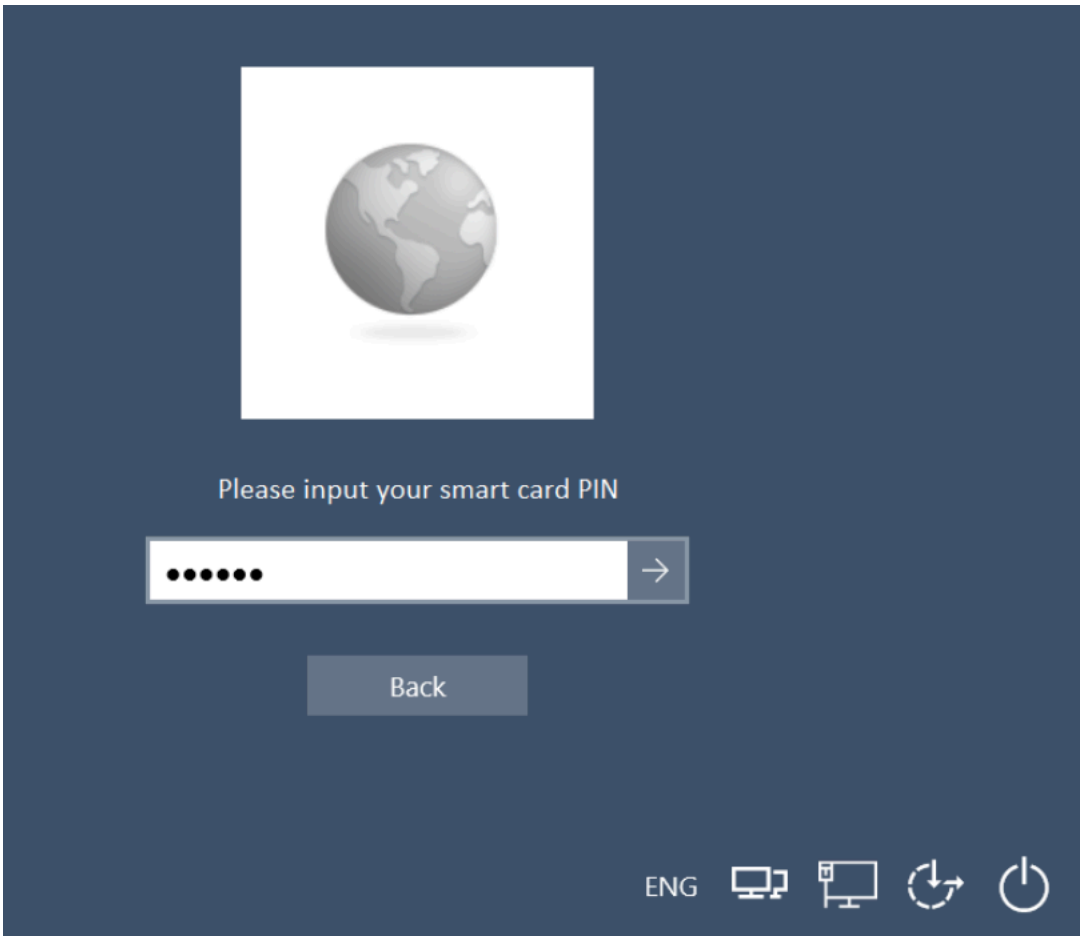
3. (Facultatif) Si vous vous connectez au terminal pour la première fois et que les portails ont été prédéfinis par l'administrateur, sélectionnez un portail dans le menu déroulant **Portal (Portail)**, puis cliquez sur la flèche pour soumettre.



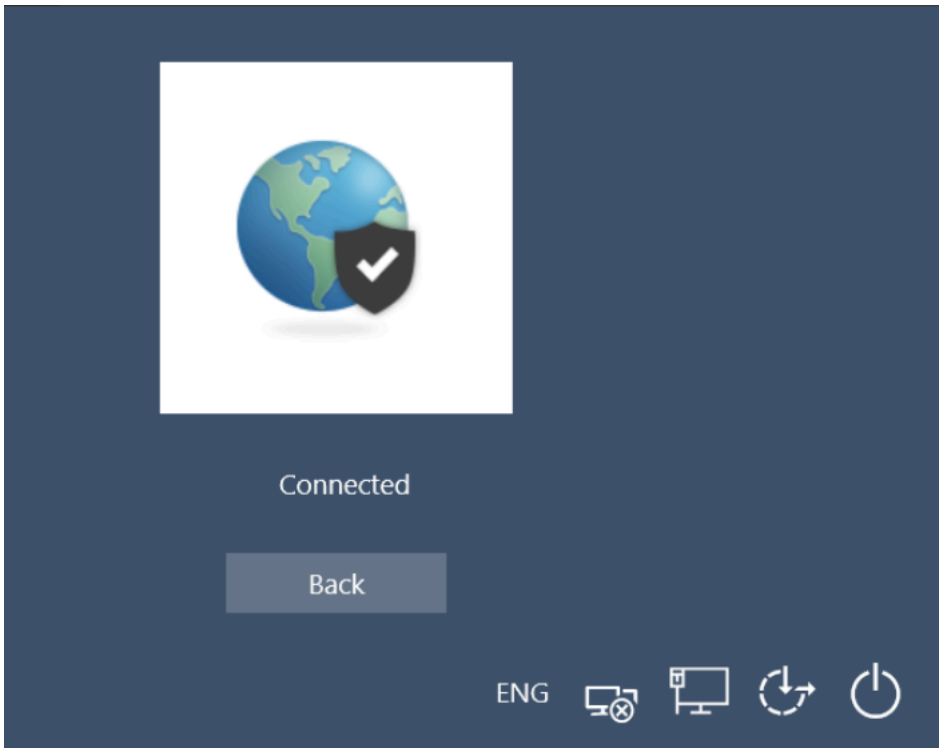
4. Sélectionnez le certificat client dans une liste de certificats valides sur le terminal pour vous authentifier auprès du portail ou de la passerelle, puis cliquez sur la flèche pour soumettre.



5. Entrez le numéro d'identification personnel (PIN) de la carte intelligente, puis cliquez sur la flèche pour soumettre.



6. Si l'authentification est réussie, l'état de la connexion affiche **Connected (Connecté)** après une connexion VPN réussie. Cliquez sur **Back (Retour)** pour afficher l'écran de connexion Windows.



3. Vérifiez que vous êtes connecté à la passerelle GlobalProtect.
   1. Reconnectez-vous au terminal Windows. Cliquez sur le bouton **Network Sign-In (Connexion au réseau)** ( ) dans le coin inférieur droit de l'écran de connexion Windows.
   2. Le panneau d'état s'ouvre. Par défaut, vous êtes automatiquement connecté à la passerelle **Best Available (Meilleure disponible)**.

Connect Before Logon Using SAML Authentication (Se connecter avant identification en utilisant l'authentification SAML)

Se connecter avant identification prend en charge l'authentification SAML pour la connexion des utilisateurs. Vous pouvez vous authentifier à GlobalProtect avant de vous connecter au terminal Windows en utilisant les fournisseurs d'identité SAML configurés (IdP) tels que Onelogin ou Okta. Si l'authentification SAML est réussie, GlobalProtect se connecte au portail ou à la passerelle spécifiée dans la configuration.

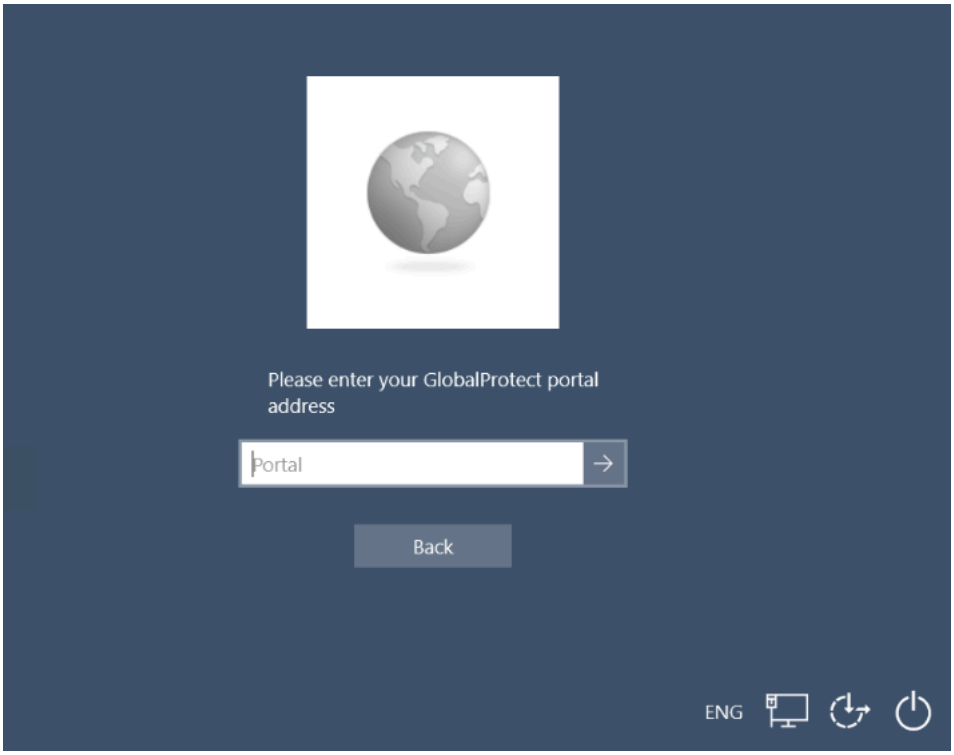
Se connecter avant identification avec la méthode d'authentification SAML est pris en charge sur toutes les versions de GlobalProtect lors de l'utilisation de l'ancienne vue Web intégrée (oew). Cependant, un écran blanc et des erreurs JavaScript peuvent être affichés de manière intermittente lors du chargement de certaines URL IdP externes en mode Se connecter avant identification. Ce problème provient du fait que l'ancienne vue Web intégrée utilise le navigateur IE hérité, qui a été déprécié dans Windows 11. Le navigateur Edge basé sur WebView2 alternatif ne prend pas en charge la méthode Se connecter avant identification. GlobalProtect continue d'utiliser l'ancienne vue Web intégrée basée sur IE (oew) avec la limitation ci-dessus.

1. Avant de pouvoir utiliser Se connecter avant identification, l'administrateur doit avoir complété les tâches suivantes :
   1. Déployez les paramètres de Se connecter avant identification dans le registre de Windows.
   2. Configurez l'authentification SAML pour authentifier les utilisateurs.
      - Créez un profil de serveur avec des paramètres pour le service d'authentification SAML.
      - Créez un profil d'authentification qui se réfère au profil de serveur SAML.
   3. Spécifiez l'authentification SAML pour la passerelle GlobalProtect.
   4. Spécifiez une authentification SAML pour le client (voir la section Définition des configurations d'authentification du client GlobalProtect).
2. Connectez-vous au terminal Windows en utilisant Se connecter avant identification.
   1. Cliquez sur le bouton **Network Sign-In (Connexion au réseau)** () dans le coin inférieur droit de l'écran de connexion Windows.

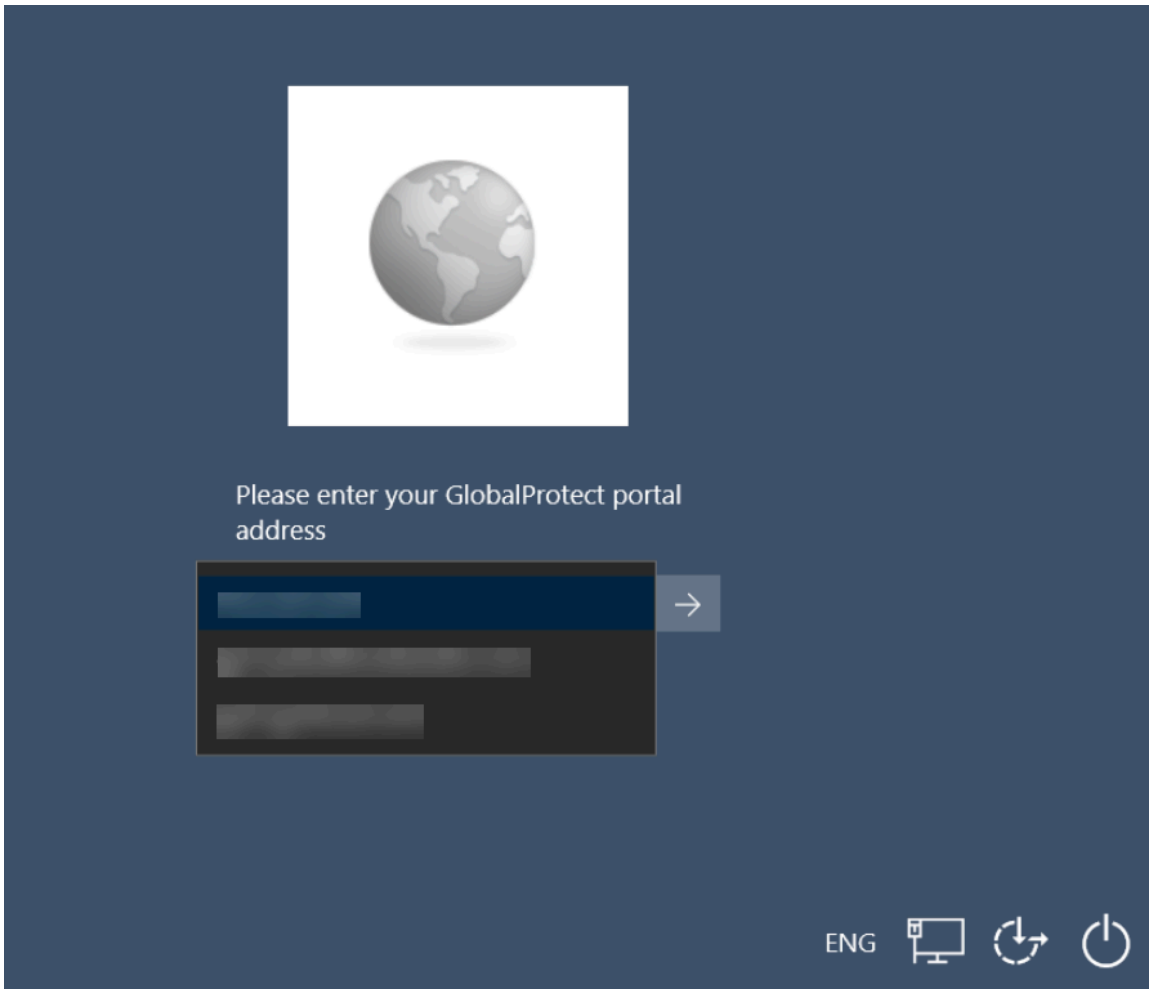
      Si la connexion VPN est réussie, le bouton **Disconnect (Déconnecter)** () apparaît à côté du bouton **Network Sign-In (Connexion au réseau)** de l'écran de connexion

Windows. Vous êtes déconnecté du VPN si vous ne vous êtes pas encore connecté à votre terminal dans le délai configuré. Cela provoque la déconnexion du tunnel VPN.

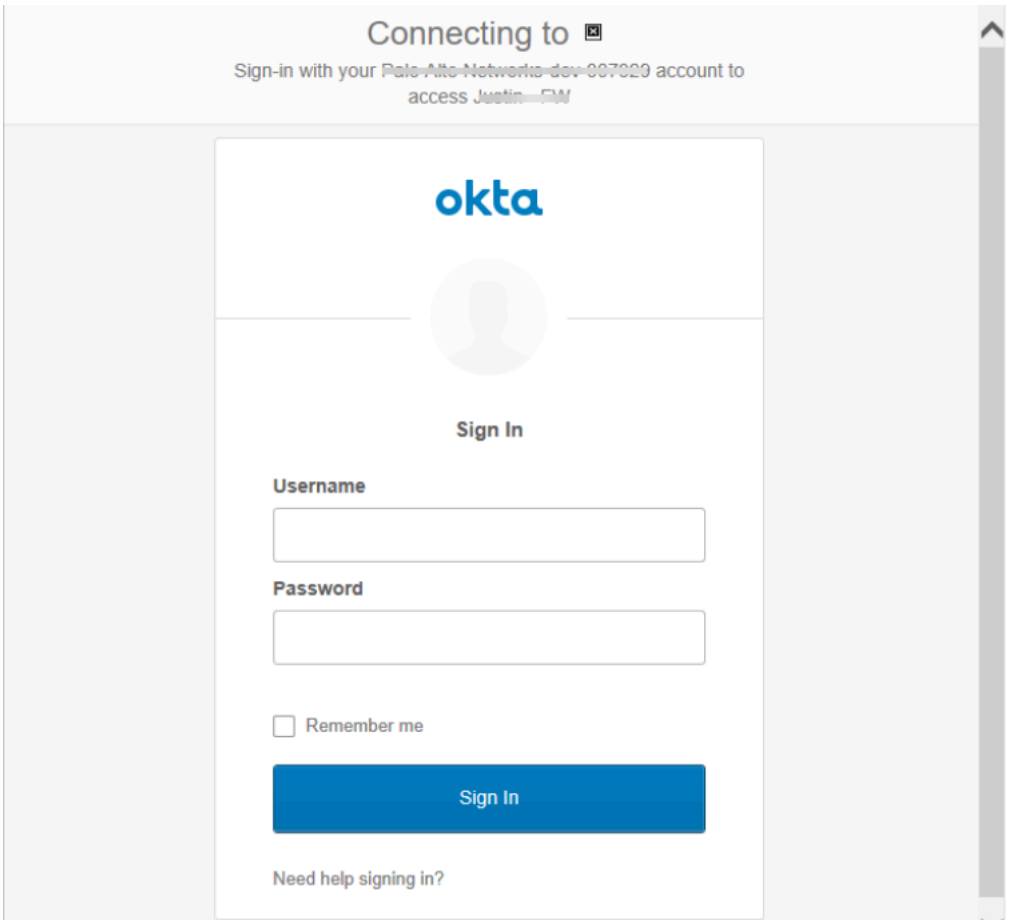
2. (Facultatif) Si vous vous connectez au terminal pour la première fois et que les portails n'ont pas été prédéfinis par l'administrateur, entrez le FQDN ou l'adresse IP du portail GlobalProtect, puis cliquez sur la flèche pour soumettre.



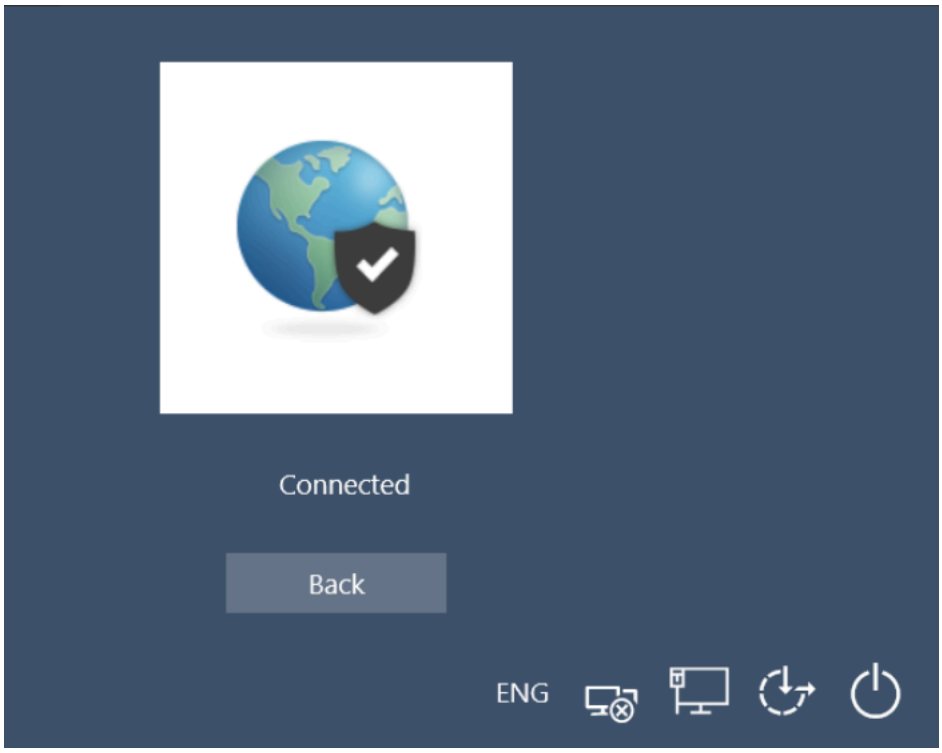
3. (Facultatif) Si vous vous connectez au terminal pour la première fois et que les portails ont été prédéfinis par l'administrateur, sélectionnez un portail dans le menu déroulant **Portal (Portail)**, puis cliquez sur la flèche pour soumettre.



4. Entrez le nom d'utilisateur et le mot de passe pour vous authentifier auprès de l'IdP, puis cliquez sur **Sign In (Se connecter)**.



5. Si l'authentification est réussie, l'état de la connexion affiche **Connected (Connecté)** après une connexion VPN réussie. Cliquez sur **Back (Retour)** pour afficher l'écran de connexion Windows.



3. Vérifiez que vous êtes connecté à la passerelle GlobalProtect.
   1. Reconnectez-vous au terminal Windows. Cliquez sur le bouton **Network Sign-In (Connexion au réseau)** ( ) dans le coin inférieur droit de l'écran de connexion Windows.
   2. Le panneau d'état s'ouvre. Par défaut, vous êtes automatiquement connecté à la passerelle **Best Available (Meilleure disponible)**.

Connect Before Logon Using Username/Password-Based Authentication (Se connecter avant identification en utilisant l'authentification basée sur un nom d'utilisateur/mot de passe)

Se connecter avant identification prend en charge l'authentification basée sur le nom d'utilisateur/mot de passe pour la connexion des utilisateurs en utilisant un service d'authentification tel que LDAP, RADIUS ou OTP. Vous pouvez vous authentifier auprès de GlobalProtect avant de vous connecter au terminal Windows en utilisant le nom d'utilisateur et le mot de passe. Si l'authentification basée sur le nom d'utilisateur/mot de passe est réussie, GlobalProtect se connecte au portail ou à la passerelle spécifiée dans la configuration.

1. Avant de pouvoir utiliser Se connecter avant identification, l'administrateur doit avoir complété les tâches suivantes :
   1. Déployez les paramètres de Se connecter avant identification dans le registre de Windows.
   2. Configurez l'accès au portail GlobalProtect pour authentifier les utilisateurs finaux au portail en utilisant leurs identifiants.
   3. Configurez une passerelle GlobalProtect pour authentifier les utilisateurs finaux à la passerelle en utilisant leurs identifiants.

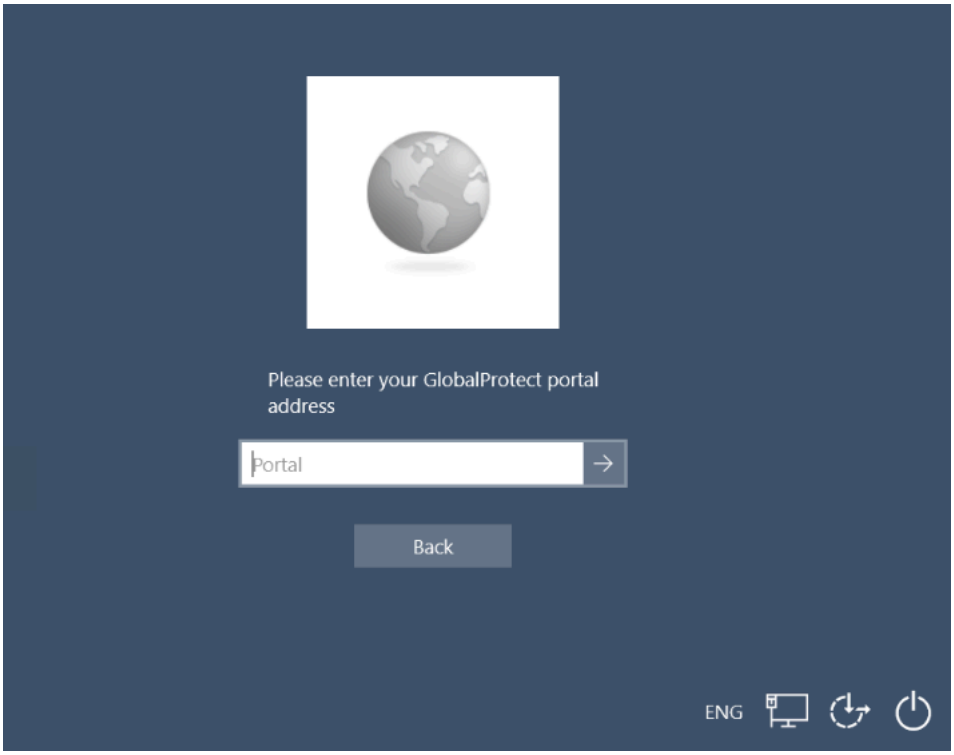
   Se connecter avant identification ne prend pas en charge un message d'authentification personnalisé.

2. Connectez-vous au terminal Windows en utilisant Se connecter avant identification.
   1. Cliquez sur le bouton **Network Sign-In (Connexion au réseau)** () dans le coin inférieur droit de l'écran de connexion Windows.

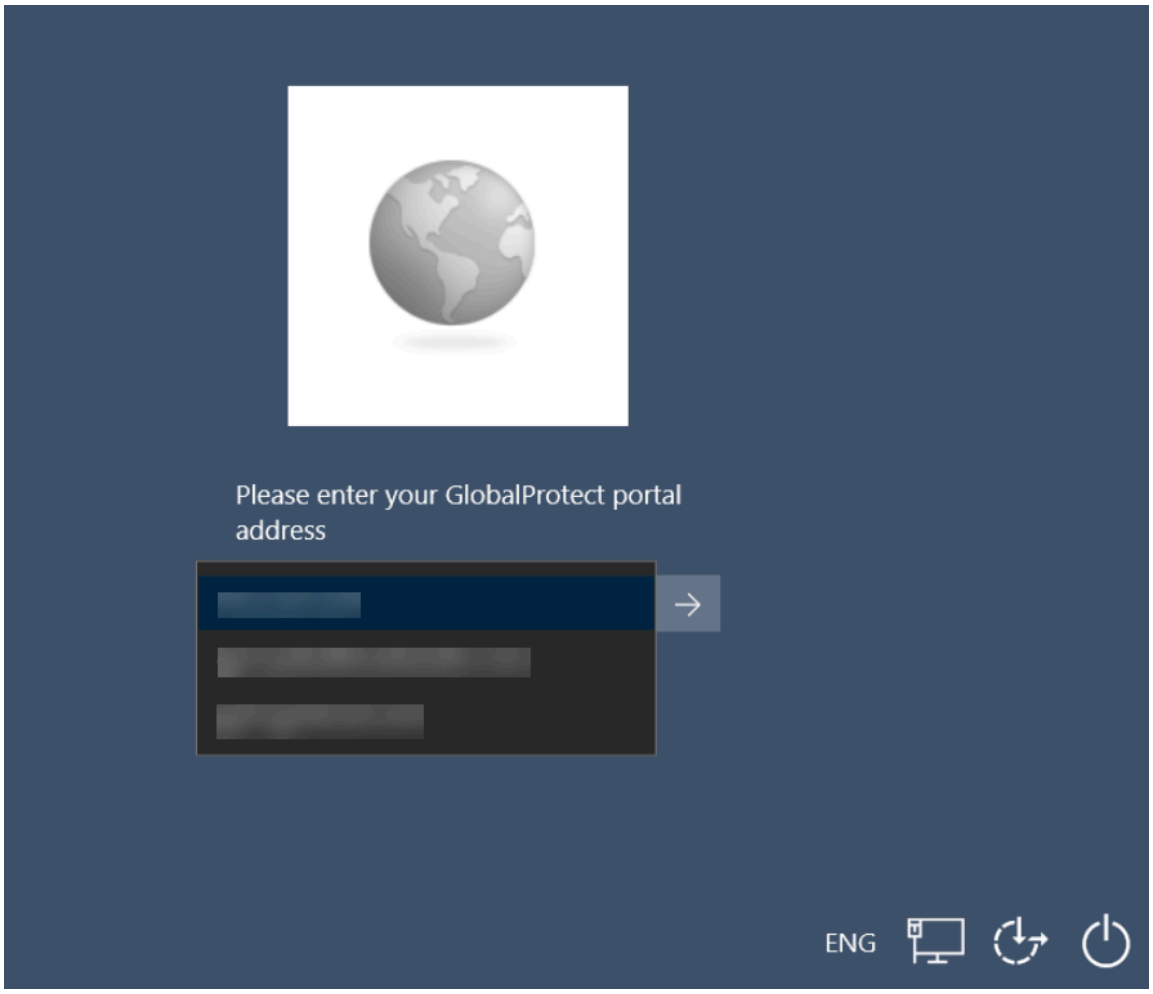
      Si la connexion VPN est réussie, le bouton **Disconnect (Déconnecter)** () apparaît à côté du bouton **Network Sign-In (Connexion au réseau)** de l'écran de connexion

Windows. Vous êtes déconnecté du VPN si vous ne vous êtes pas encore connecté à votre terminal dans le délai configuré. Cela provoque la déconnexion du tunnel VPN.

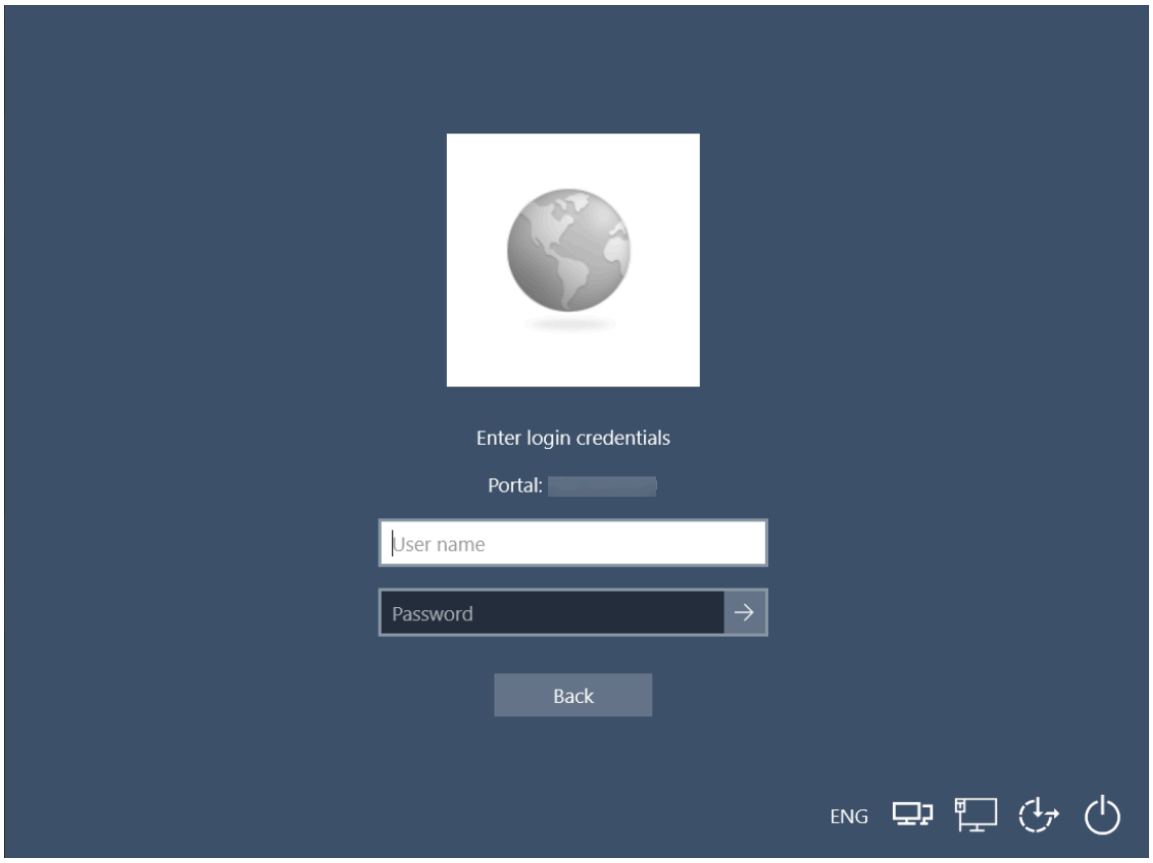
2. (Facultatif) Si vous vous connectez au terminal pour la première fois et que les portails n'ont pas été prédéfinis par l'administrateur, entrez le FQDN ou l'adresse IP du portail GlobalProtect, puis cliquez sur la flèche pour soumettre.



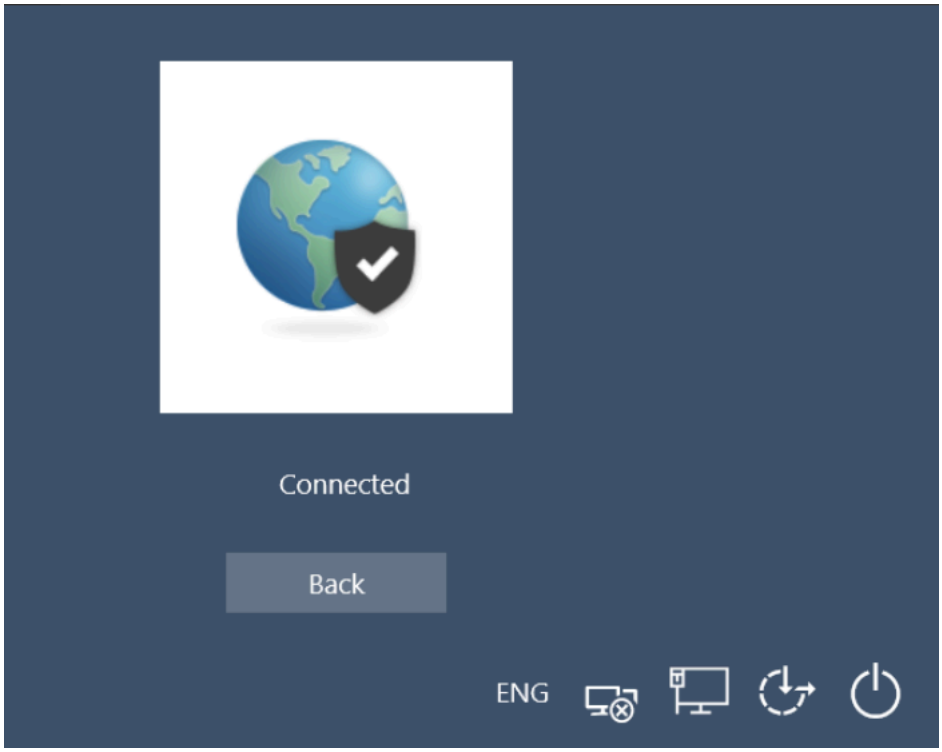
3. (Facultatif) Si vous vous connectez au terminal pour la première fois et que les portails ont été prédéfinis par l'administrateur, sélectionnez un portail dans le menu déroulant **Portal (Portail)**, puis cliquez sur la flèche pour soumettre.



4. Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur la flèche pour soumettre.



5. Si l'authentification est réussie, l'état de la connexion affiche **Connected (Connecté)** après une connexion VPN réussie. Cliquez sur **Back (Retour)** pour afficher l'écran de connexion Windows.



3. Vérifiez que vous êtes connecté à la passerelle GlobalProtect.
   1. Reconnectez-vous au terminal Windows. Cliquez sur le bouton **Network Sign-In (Connexion au réseau)** () dans le coin inférieur droit de l'écran de connexion Windows.
   2. Le panneau d'état s'ouvre. Par défaut, vous êtes automatiquement connecté à la passerelle **Best Available (Meilleure disponible)**.

Utilisation de Single Sign-On (ouverture de session unique - SSO) pour l'authentification par carte intelligente

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Terminaux Windows uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

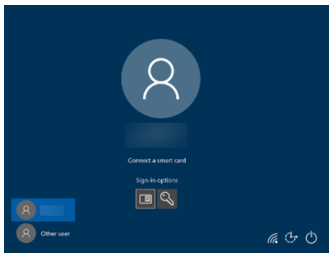
Si votre administrateur a configuré le portail GlobalProtect pour vous permettre de vous authentifier via l'authentification unique (SSO) à l'aide de l'authentification par carte intelligente, vous pouvez vous connecter sans avoir à saisir à nouveau votre numéro d'identification personnel (PIN) de carte intelligente dans l'application GlobalProtect pour une expérience SSO simplifiée. Vous pouvez utiliser le même PIN de carte intelligente pour GlobalProtect avec votre terminal Windows. Vous pouvez bénéficier de l'utilisation de SSO pour l'authentification par carte intelligente en réduisant le nombre de fois où vous devez entrer votre PIN de carte intelligente lorsque vous vous connectez. Une fois connecté avec succès au terminal Windows, l'application GlobalProtect acquiert et mémorise le PIN de votre carte intelligente pour vous authentifier auprès du portail et de la passerelle GlobalProtect.

Votre administrateur peut définir le type de politique de mise en cache du PIN pour Windows qui est associé au PIN du fournisseur de carte intelligente. Le PIN est mis en cache uniquement si cela est autorisé par le fournisseur de carte intelligente. GlobalProtect efface le PIN du cache si vous vous déconnectez manuellement de l'application GlobalProtect, vous vous déconnectez de Windows, ou si le PIN est changé.

1. Avant de pouvoir utiliser SSO pour l'authentification par carte intelligente, l'administrateur doit avoir complété les tâches suivantes :
   1. Définissez le paramètre prédéployé sur les terminaux Windows pour utiliser SSO pour l'authentification par carte intelligente.

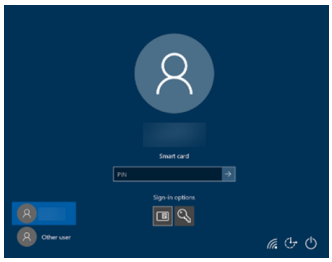
      Votre administrateur doit définir le paramètre prédéployé sur votre terminal Windows avant d'activer SSO pour le PIN de la carte intelligente. GlobalProtect récupère l'entrée du registre une seule fois : lors de l'initialisation de l'application GlobalProtect.
   2. Configurez la carte intelligente pour l'authentification à deux facteurs.
   3. Attribuez le profil de certificat au portail GlobalProtect.
   4. Configurez la passerelle afin que vous puissiez vous authentifier en utilisant une carte intelligente.
   5. Activez l'application GlobalProtect pour utiliser SSO pour le PIN de la carte intelligente sur le portail GlobalProtect afin que vous puissiez utiliser le même PIN de carte intelligente pour GlobalProtect avec votre terminal Windows.

2. Connectez-vous au terminal Windows en utilisant le PIN de la carte intelligente.
   1. Cliquez sur **Sign-in options (Options de connexion)**, puis cliquez sur le bouton **smart card (carte intelligente)** ( ).
   2. Lorsque vous y êtes invité, insérez la carte intelligente pour vérifier que l'authentification par carte intelligente est réussie.



   3. Entrez le PIN de la carte intelligente et cliquez sur la flèche pour soumettre.

      Si l'authentification par carte intelligente est réussie, vous pouvez vous connecter au portail ou à la passerelle spécifiée dans la configuration sans avoir à ressaisir votre PIN de carte intelligente.

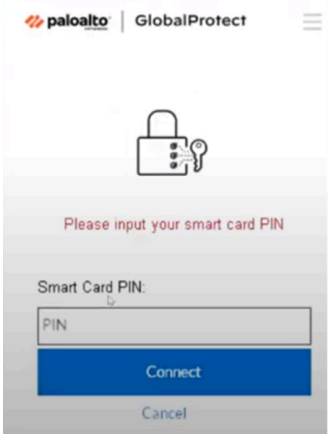


3. (Facultatif) Connectez-vous à GlobalProtect en utilisant le même PIN de carte intelligente.

Vous pouvez utiliser le même PIN de carte intelligente que vous avez utilisé pour vous connecter à votre terminal Windows.

1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
2. Cliquez sur le menu hamburger pour ouvrir le panneau **Settings (Paramètres)**.
3. Dans le panneau **Settings (Paramètres)**, **Sign Out (Déconnectez-vous)** pour effacer vos identifiants utilisateur enregistrés de l'application GlobalProtect.
4. Reconnectez-vous à GlobalProtect avec le même PIN de carte intelligente.

   L'application GlobalProtect affiche une erreur de PIN de carte intelligente si le PIN n'est pas valide.



Utilisation de l'application GlobalProtect pour Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Terminaux Windows uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Ce chapitre s'applique à vous uniquement si votre configuration nécessite que vous saisissiez vos identifiants de connexion GlobalProtect après vous être connecté à votre terminal (l'authentification single sign-on est désactivée).

Nous recommandons généralement aux organisations de permettre à ses utilisateurs GlobalProtect de se connecter de manière transparente après l'installation de l'application. Après vous être connecté à un terminal avec une connexion GlobalProtect transparente, l'application GlobalProtect initie automatiquement et se connecte au réseau d'entreprise sans intervention supplémentaire de l'utilisateur.

Si votre configuration nécessite que vous saisissiez vos identifiants GlobalProtect, suivez les étapes applicables ci-dessous.

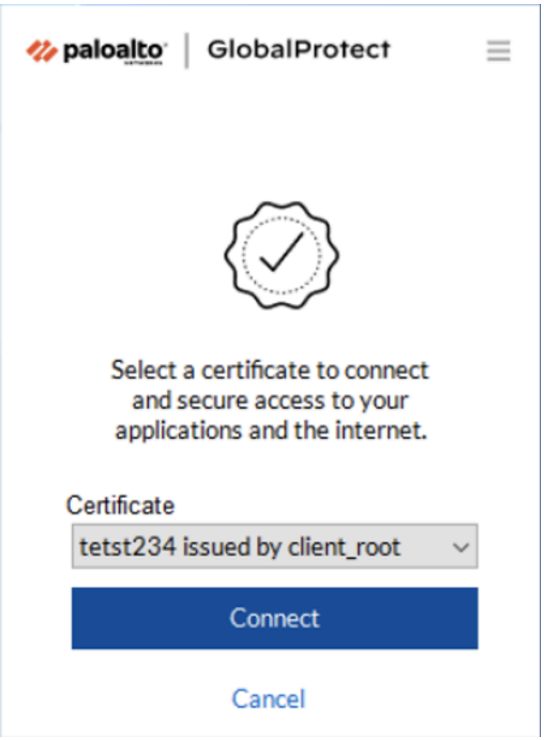
1. Ouvrez une session sur GlobalProtect.

   Si vous vous connectez au terminal pour la première fois, l'application GlobalProtect affiche une page d'accueil conviviale une fois la connexion réussie. Cliquez sur **Get Started (Commencer)**.

   1. (Facultatif) Si votre administrateur configure GlobalProtect avec la méthode de connexion **On-Demand (À la demande)** et que vous vous connectez à GlobalProtect pour la première fois, sélectionnez le certificat client dans une liste de certificats valides dans

le menu déroulant **Certificate (Certificat)** pour vous authentifier auprès du portail ou de la passerelle.

2. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.



3. (Facultatif) Passez en revue les conditions d'utilisation de votre entreprise avant de vous connecter à GlobalProtect si votre administrateur exige que vous consultiez une page pour accéder aux ressources internes.

   Si vous n'acceptez pas les conditions d'utilisation, vous ne pourrez pas vous connecter à GlobalProtect.

   En option, si vous cliquez sur **Cancel (Annuler)**, vous devez saisir l'adresse IP (ou le domaine) du portail GlobalProtect, puis cliquer sur **Connect (Connecter)** pour établir la connexion.

4. Saisissez l'adresse IP ou le domaine du portail fourni par votre administrateur GlobalProtect, puis cliquez sur **Connect (Connecter)**.

5. (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 Change Gateway (Changer la passerelle) (pour les passerelles externes uniquement).

   Cette option n'est disponible que si votre administrateur active la sélection manuelle de la passerelle.

6. (Facultatif) Selon le mode de connexion, cliquez sur **Connect (Connecter)** pour initier la connexion.

7. (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 votre administrateur vous a permis d'utiliser des informations biométriques (empreinte digitale) pour vous connecter, vous devez d'abord vous connecter avec un nom d'utilisateur et un mot de passe deux fois (une fois pour l'enregistrer et à nouveau pour vous authentifier). Vous pouvez ensuite utiliser des informations biométriques pour vous connecter.

   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 votre administrateur configure une page d'accueil pour GlobalProtect, elle s'affiche une fois votre connexion réussie.

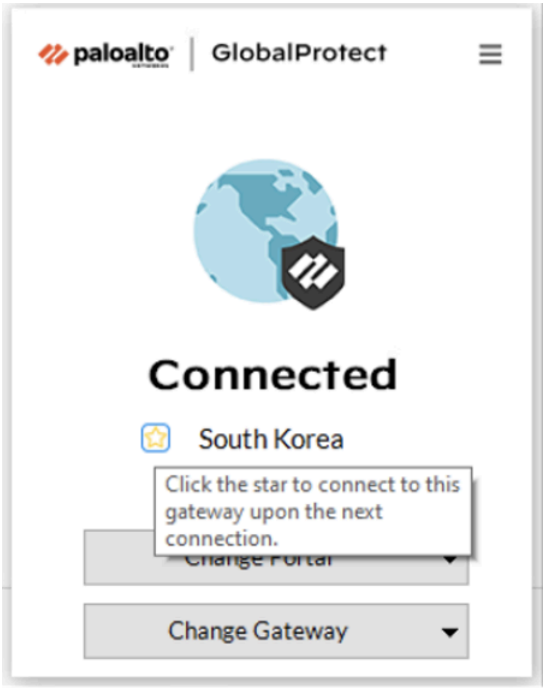
2. Connectez-vous au portail GlobalProtect ou à la passerelle.

Vous pouvez déterminer si vous êtes connecté en vérifiant l'icône de bac de système GlobalProtect. Si vous n'êtes pas connecté, l'icône est grise (), et ***Not Connected (Non connecté)*** *apparaît lorsque vous survolez l'icône.*

1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
2. (Facultatif) Si vous vous connectez à l'application GlobalProtect pour la première fois, entrez l'adresse IP ou le domaine du portail GlobalProtect, puis cliquez sur **Connect (Connecter)**.
3. (Facultatif) Si plusieurs portails sont enregistrés sur votre application, sélectionnez un portail dans la liste déroulante **Change Portal (Modifier le portail)**. Par défaut, le portail le plus récemment connecté est présélectionné dans la liste déroulante **Change Portal (Modifier le portail)**.
4. (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, cliquez sur la liste déroulante **Change Gateway (Modifier la passerelle)**, puis utilisez l'une des options suivantes :
   - Sélectionnez une passerelle manuellement (passerelles externes uniquement). Cette option n'est disponible que si votre administrateur active la sélection manuelle de la passerelle.

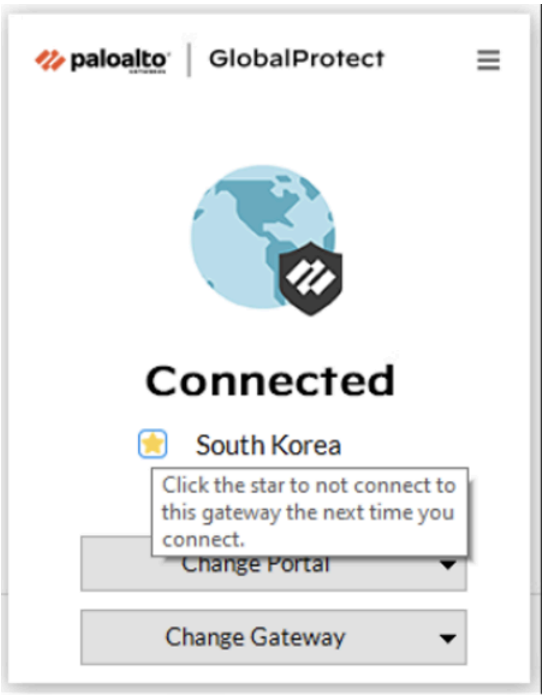
- Attribuez et connectez-vous automatiquement à une passerelle préférée :

  1. Pour désigner une passerelle préférée, cliquez sur l'icône en forme d'étoile ( ). La prochaine fois que vous vous connecterez, vous vous connecterez automatiquement à votre passerelle préférée désignée.



  Si vous décidez plus tard que vous ne souhaitez plus cette passerelle comme passerelle préférée, vous pouvez effacer l'icône en forme d'étoile. La prochaine

fois que vous vous connecterez, vous serez automatiquement connecté à la meilleure passerelle disponible.



2. Par défaut, vous vous connectez automatiquement à la passerelle **Best Available (Meilleure disponible)** qui est identifiée par une coche dans la liste déroulante **Change Gateway (Modifier la passerelle)**. Si vous définissez la passerelle préférée, une étoile s'affiche par la passerelle étoilée dans la liste déroulante **Change Gateway (Modifier la passerelle)**.

   Si votre administrateur a configuré des passerelles externes manuelles dans la configuration de l'agent du portail, vous pouvez choisir une passerelle spécifique en utilisant le champ de recherche de passerelle.

5. (Facultatif) Selon le mode de connexion, cliquez sur **Connect (Connecter)** pour initier la connexion.
6. (Facultatif) Si vous y êtes invité, entrez votre **Username (Nom d'utilisateur)** et votre **Password (Mot de passe)**, et cliquez sur **Connect (Connecter)**.

   Si votre administrateur vous a permis d'utiliser des informations biométriques (empreinte digitale) pour vous connecter, vous devez d'abord vous connecter avec un nom d'utilisateur et un mot de passe deux fois (une fois pour l'enregistrer et à nouveau pour vous authentifier). Vous pouvez ensuite utiliser des informations biométriques pour vous connecter.

Lorsque l'application se connecte en mode externe, l'icône de bac de système GlobalProtect affiche un bouclier (), et **Connected (Connecté)** apparaît lorsque vous survolez l'icône. Lorsque l'application se connecte en mode interne, l'icône de bac de système GlobalProtect affiche une maison (), et **Internal Network (Réseau interne)** apparaît lorsque vous survolez l'icône.

3. Ouvrez l'application GlobalProtect.

Cliquez sur l'icône de bac de système GlobalProtect pour lancer l'interface de l'application.

Une notification s'affiche si votre administrateur a configuré le portail pour installer l'agent de terminal DEM autonome (ADEM) lors de l'installation de l'application GlobalProtect et vous a autorisé à activer les tests ou non. Si votre administrateur a déjà installé l'agent de terminal ADEM et configuré ultérieurement le portail pour désinstaller l'agent de terminal ADEM, une notification apparaît lors de la prochaine connexion.

4. Affichez des informations sur votre connexion réseau.

Après avoir lancé l'application, cliquez sur le menu hamburger dans le panneau d'état pour ouvrir le menu des paramètres. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau **GlobalProtect Settings (Paramètres GlobalProtect)**, puis sélectionnez l'un des paramètres suivants pour afficher et modifier l'application GlobalProtect :

- **Connections (Connexions)** : l'onglet **Connections (Connexions)** affiche le ou les portails associés au compte GlobalProtect. Vous pouvez ajouter, modifier ou supprimer des portails à partir de cet onglet. Cet onglet affiche également la passerelle à laquelle vous êtes connecté. Vous pouvez afficher les statistiques de connexion sur la passerelle (par exemple, l'adresse IP de la passerelle, l'emplacement et la disponibilité de la session VPN) lorsque votre administrateur définit **Enable Advanced View (Activer la vue avancée)** sur **Yes (Oui)** dans la configuration de l'agent du portail GlobalProtect.

  L'onglet **Connections (Connexions)** affiche également le compte à rebours pour la durée de vie de la connexion.

  L'onglet **Connections (Connexions)** affiche les détails du proxy si la fonctionnalité Explicit Proxy Connectivity (Connectivité explicite du proxy) dans GlobalProtect pour la sécurité Internet toujours active est activée pour l'application via Prisma Access.

  Mode proxy :

- **Preferences (Préférences)** : l'onglet **Preferences (Préférences)** n'est désormais disponible que si votre administrateur configure au moins l'une des options suivantes :
  - **Enable Biometric Sign-in (Activer la connexion biométrique)** : vous pouvez choisir d'utiliser les informations biométriques (empreinte digitale) pour vous connecter. Cette option n'est disponible que si votre administrateur configure l'option **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)** sur **Only with User Fingerprint (Uniquement avec l'empreinte digitale de l'utilisateur)** dans la configuration de l'agent GlobalProtect. Vous devez 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.
  - **Do not display a welcome page upon each successful connection (Ne pas afficher de page d'accueil lors de chaque connexion réussie)** : vous pouvez choisir d'afficher une page d'accueil lors de la connexion réussie. Cette option n'est disponible que si votre administrateur définit la **Welcome Page (Page d'accueil)** sur **factory-default** dans la configuration de l'agent du portail GlobalProtect.

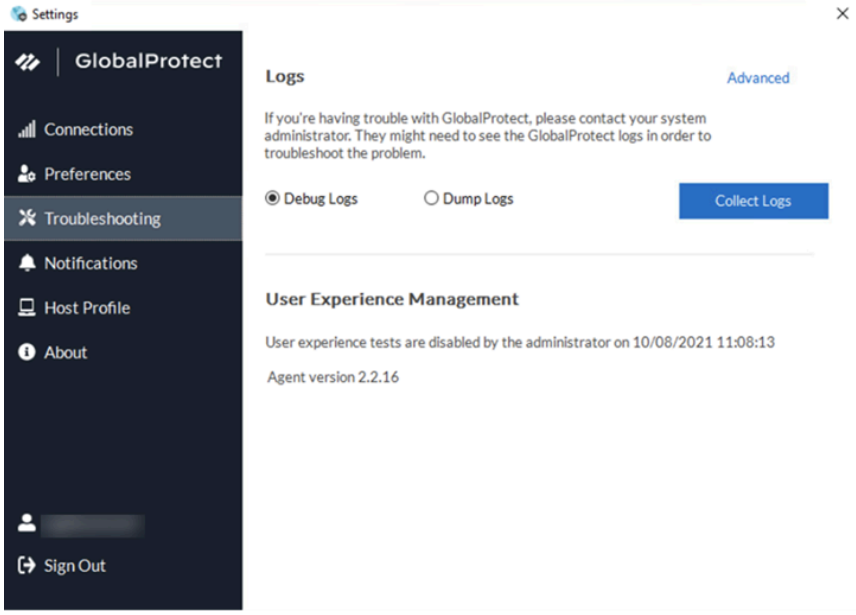
- **Connect with SSL (Se connecter avec SSL)** : vous pouvez choisir d'utiliser SSL ou de rester avec IPSec. Cette option n'est disponible que si votre administrateur définit **Connect with SSL Only (Se connecter avec SSL uniquement)** sur**User can Change (L'utilisateur peut modifier)** dans la configuration de l'agent du portail GlobalProtect.
- **Always run diagnostic tests and include logs (Toujours exécuter des tests de diagnostic et inclure des journaux)** : vous pouvez choisir d'activer l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic. Cette option n'est disponible que si votre administrateur active la collecte de journaux de l'application GlobalProtect pour le dépannage sur le portail GlobalProtect.

- **Troubleshooting (Dépannage)** : l'onglet **Troubleshooting (Dépannage)** vous permet de **Collect Logs (Collecter les journaux)** et de définir le niveau de journalisation sur **Debug Logs (Déboguer les journaux)** ou **Dump Logs (Journaux de vidage)**, et éventuellement **Enable User Experience Tests (Activer les tests d'expérience utilisateur)**.

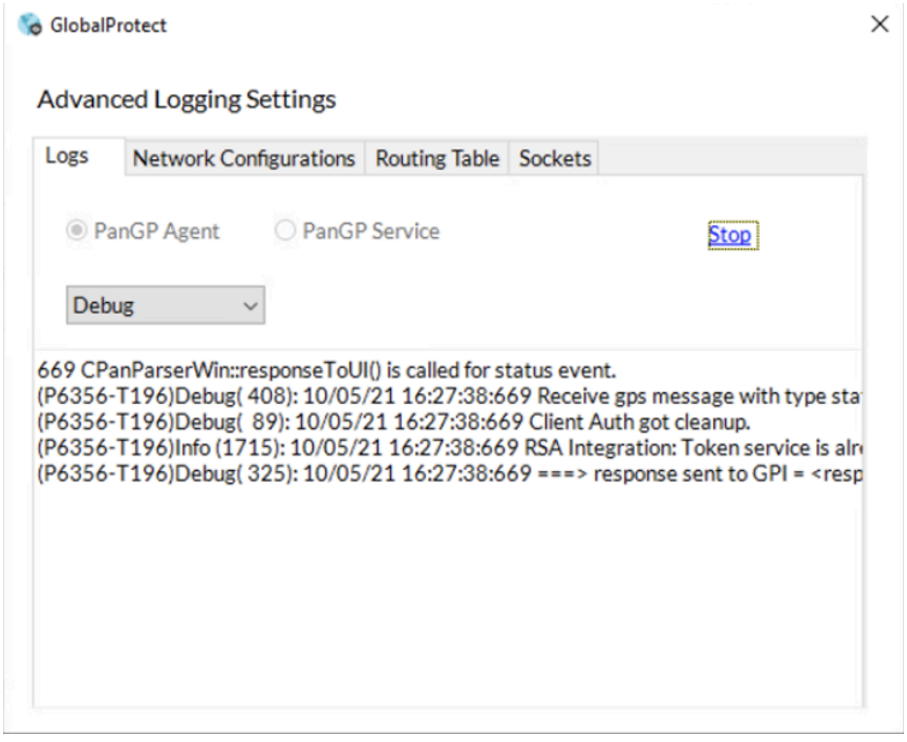
  Pour que l'application GlobalProtect envoie des journaux de dépannage, des journaux de diagnostic ou les deux au service de journalisation Strata pour une analyse plus approfondie, vous devez configurer le portail GlobalProtect pour activer la GlobalProtect app log collection for troubleshooting (Collecte de journaux d'application GlobalProtect pour le dépannage). De plus, vous pouvez configure the HTTPS-based destination URLs (configurer les URL de destination basées sur HTTPS) qui peuvent contenir des adresses IP ou des noms de domaine complets des serveurs/ressources

Web que vous souhaitez sonder, et déterminer des problèmes tels que la latence ou les performances du réseau sur le point de terminaison de l'utilisateur final.

Vous pouvez cliquer sur **Advanced (Avancé)** pour afficher des informations détaillées sur leur terminal.



La fenêtre **Advanced Logging Settings (Paramètres avancés de journalisation)** affiche les informations concernant la configuration du réseau, les paramètres d'itinéraire, les connexions actives et les journaux.



Lorsque GlobalProtect est connecté, vous pouvez vérifier que l'agent du terminal DEM autonome (ADEM) peut effectuer des tests d'expérience utilisateur si la case à cocher

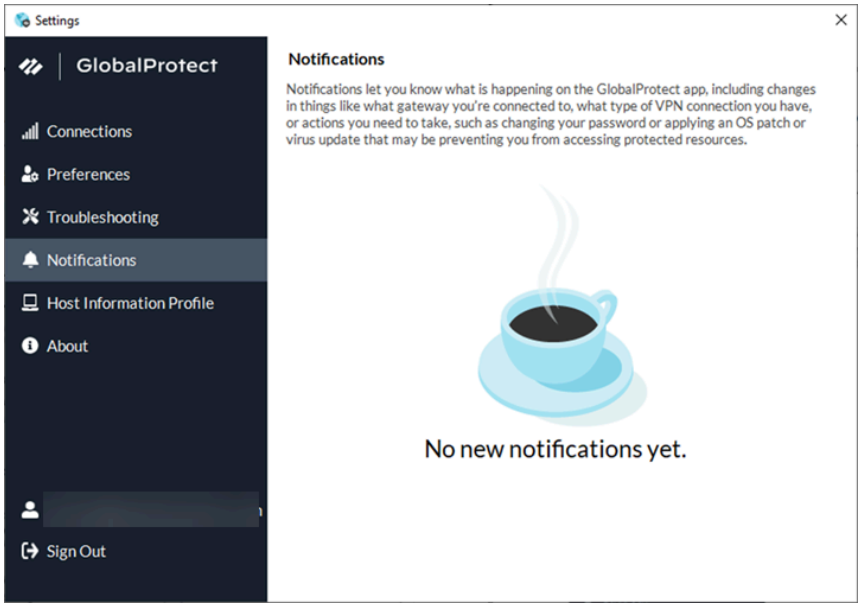
Enable user experience tests (Activer les tests d'expérience utilisateur) est affichée sur l'application GlobalProtect. Ou vous pouvez vérifier qu'un message est affiché si votre administrateur a installé l'agent du terminal ADEM lors de l'installation de l'application GlobalProtect, mais ne vous permet pas d'activer ou de désactiver les tests d'expérience utilisateur depuis l'application GlobalProtect. Par défaut, les alertes de pulsation sont toujours transmises à l'ADEM même lorsque GlobalProtect est désactivé ou déconnecté.

Si votre administrateur a configuré le portail pour installer l'agent de terminal DEM autonome lors de l'installation de l'application GlobalProtect et vous a autorisé à activer les tests, cochez la case **Enable user experience tests (Activer les tests d'expérience utilisateur)** sur l'application GlobalProtect. Cette case à cocher ne s'affiche pas si votre administrateur ne vous permet pas d'activer ou de désactiver les tests d'expérience utilisateur à partir de l'application GlobalProtect. Au lieu de cela, un message s'affiche, confirmant que l'application est activée pour exécuter des tests d'expérience utilisateur.

Si vous ne cochez pas la case **Enable user experience tests (Activer les tests d'expérience utilisateur)**, les alertes de pulsation sont toujours transmises à l'ADEM.

- **Notifications** : l'onglet **Notifications** affiche les informations détaillées sur les notifications spécifiques déclenchées sur l'application GlobalProtect. Vous pouvez configurer les notifications de l'utilisateur final concernant l'expiration des sessions de l'application GlobalProtect sur la passerelle et planifier l'affichage de ces notifications personnalisées sur l'application.

  Vous êtes également informé s'il n'y a pas de nouvelles notifications déclenchées sur l'application GlobalProtect.

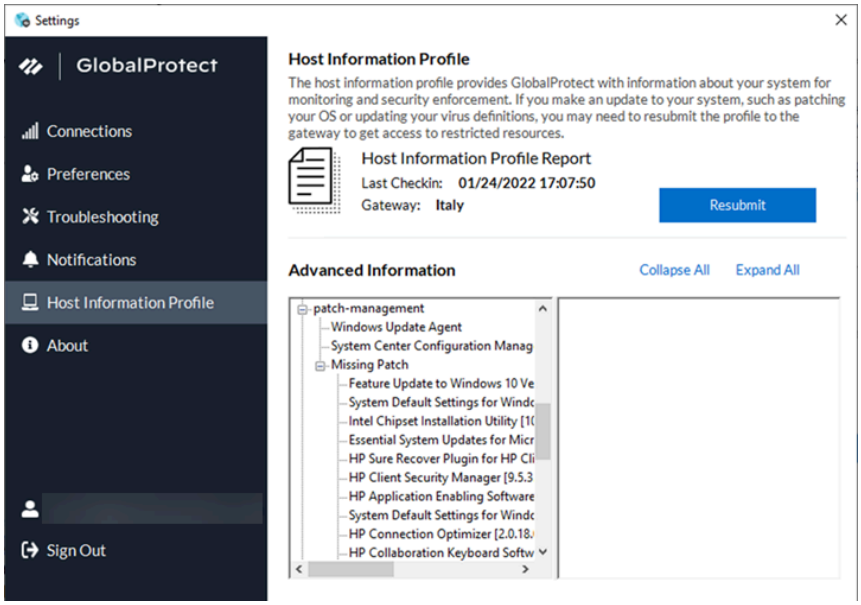


  À partir de la version 6.2.3 de l'application GlobalProtect, les messages de session et de délai d'inactivité sont supprimés pour la méthode de connexion toujours active.

  À partir de la version 6.2 de l'application GlobalProtect, vous pouvez prolonger la durée de vie de la session de connexion de l'application GlobalProtect avant son expiration pour éviter une déconnexion soudaine de la session de l'application. La notification d'expiration de la durée de vie de la connexion vous informe à l'avance lorsque les sessions

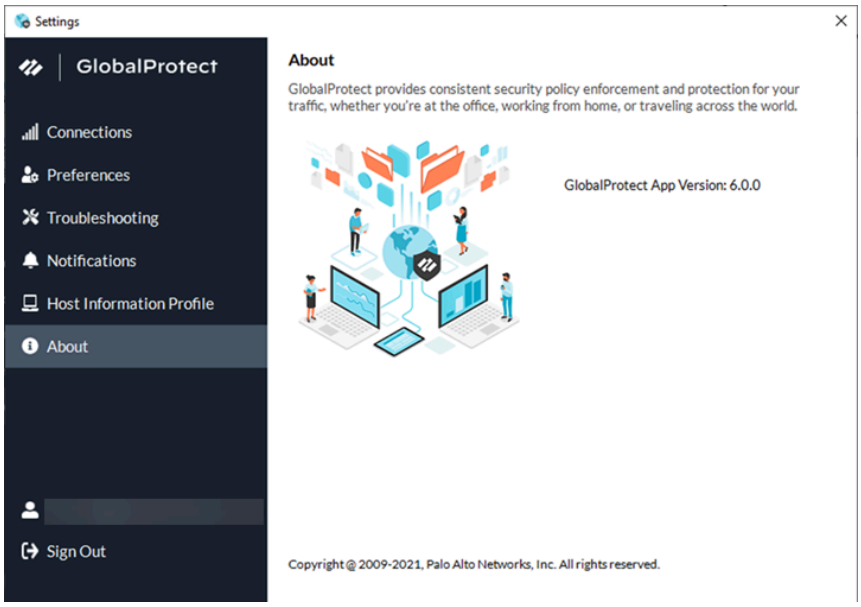
de l'application sont sur le point d'expirer et offre la possibilité de prolonger la durée de la session utilisateur afin que vous ne soyez pas déconnecté brusquement de votre session. L'application affiche la notification d'expiration avec l'option Extend User Session (Étendre la session utilisateur) si votre administrateur a configuré les paramètres de notification pour l'extension de la session.

- **Host Information Profile (Profil d'informations sur l'hôte - HIP)** : l'onglet **Host Information Profile (Profil d'informations sur l'hôte - HIP)** affiche les données sur les terminaux que GlobalProtect utilise pour la surveillance et l'application des politiques de sécurité par l'intermédiaire du Host Information Profile (Profil d'informations sur l'hôte - HIP). Vous pouvez cliquer sur **Resubmit (Renvoyer)** pour renvoyer manuellement les données HIP à la passerelle.



Si votre administrateur a configuré plusieurs passerelles internes en mode sans tunnel et en détection d'hôte interne, vous pouvez cliquer sur **More Details (Plus de détails)** pour surveiller l'envoi du rapport Host Information Profile (Profil d'informations sur l'hôte - HIP) pour chaque passerelle à partir d'un emplacement central afin de vous aider à résoudre rapidement les problèmes liés au HIP.

- **About (À propos)** : l'onglet **About (À propos)** affiche la version de GlobalProtect actuellement installée sur le terminal et vous permet de **Check for Updates (Vérifier les mises à jour)**.



5. (Facultatif) Connectez-vous en utilisant un nouveau mot de passe.

   *Si votre administrateur GlobalProtect configure l'agent du portail GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vos informations d'identification sont automatiquement enregistrées dans l'application GlobalProtect. Si votre mot de passe pour accéder au réseau d'entreprise change, vous devez vous connecter à GlobalProtect en utilisant votre nouveau mot de passe.*

   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
   2. Cliquez sur le menu hamburger pour ouvrir le menu des paramètres.
   3. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau des **GlobalProtect Settings (Paramètres GlobalProtect)**.
   4. Dans le panneau **GlobalProtect Settings (Paramètres GlobalProtect)**, **Sign Out (Déconnectez-vous)** pour effacer vos informations d'identification d'utilisateur enregistrées de l'application GlobalProtect.
   5. Après avoir effacé vos identifiants utilisateur, vous pouvez vous reconnecter à GlobalProtect avec votre nouveau nom d'utilisateur et mot de passe.

6. (Facultatif) Déconnectez-vous de GlobalProtect.

   Si votre administrateur configure GlobalProtect avec la méthode de connexion **On-Demand (À la demande)**, vous pouvez vous déconnecter de GlobalProtect en cliquant sur **Disconnect (Déconnecter)** dans le panneau d'état.

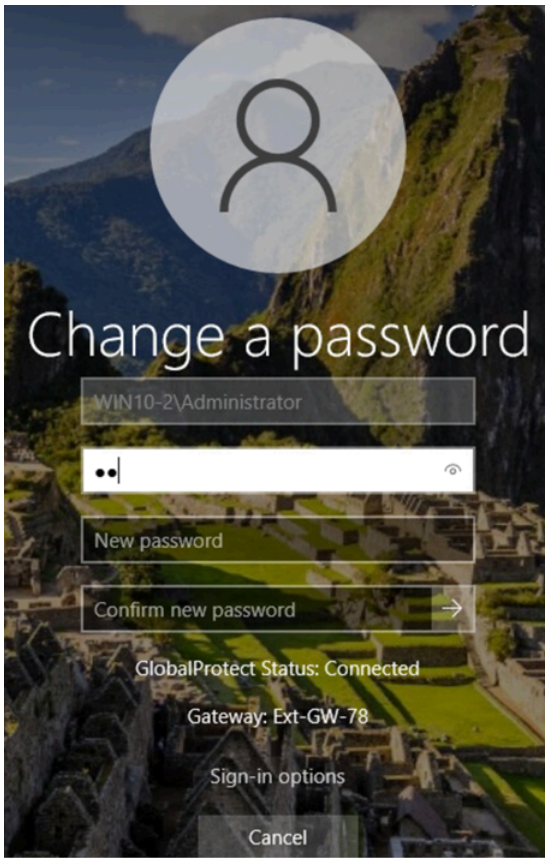
Révéler le mot de passe sur l'écran de connexion Windows pour GlobalProtect

Lorsque vous vous connectez à votre bureau Windows 10 ou Windows 11 ou lorsque vous modifiez votre mot de passe, vous pouvez cliquer sur l'icône **Reveal Password (Révéler le mot de passe)** pour afficher le mot de passe au fur et à mesure de la saisie. Le mot de passe s'affiche en texte brut. Cette fonctionnalité permet d'éviter les erreurs de saisie et de réduire le risque de verrouillage du compte en vous permettant de confirmer votre mot de passe visuellement.

Cette fonctionnalité est disponible dans GlobalProtect™ 6.3.3 et peut être activée via une clé de registre. Pour plus d'informations sur la clé de registre, reportez-vous à la section Options d'affichage de l'application.

L'écran de connexion Windows affiche l'état de la connexion GlobalProtect et la passerelle en plus de l'icône Reveal Password (Révéler le mot de passe) dans le champ du mot de passe.

La boîte de dialogue Change Password (Modifier le mot de passe) affiche votre nom d'utilisateur, votre nom de domaine, l'état de la connexion GlobalProtect et votre passerelle en plus de l'icône Reveal Password (Révéler le mot de passe) dans le champ du mot de passe.



Signaler un problème depuis l'application GlobalProtect pour Windows

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Terminaux Windows uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si vous rencontrez un comportement inhabituel, tel qu'une mauvaise performance du réseau ou une impossibilité d'établir une connexion avec le portail et la passerelle, vous pouvez signaler le problème directement au service de journalisation Strata auquel votre administrateur peut accéder. Vous n'avez plus besoin de collecter manuellement et d'envoyer les journaux de l'application GlobalProtect par e-mail ou de les stocker sur un lecteur cloud.

*Pour afficher l'option **Report an Issue (Signaler un problème)** sur l'application GlobalProtect, votre administrateur doit activer la collecte des journaux de l'application GlobalProtect pour le dépannage sur le portail GlobalProtect.*

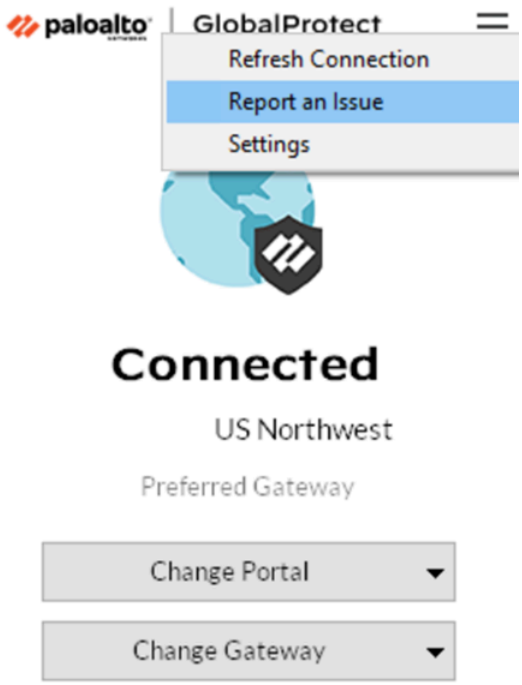
1. Connectez-vous au portail GlobalProtect ou à la passerelle.
   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
   2. (Facultatif) Si vous vous connectez à l'application GlobalProtect pour la première fois, saisissez le FQDN ou l'adresse IP du portail GlobalProtect, puis cliquez sur **Connect (Se connecter)**.
   3. (Facultatif) Si plusieurs portails sont enregistrés sur votre application, sélectionnez un portail dans le menu déroulant **Portal (Portail)**. Par défaut, le portail le plus récemment connecté est présélectionné dans le menu déroulant **Portal (Portail)**.
   4. (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 passerelle différente, cliquez sur le menu déroulant de la passerelle.
2. Ouvrez l'application GlobalProtect.

   Cliquez sur l'icône de bac de système GlobalProtect pour lancer l'interface de l'application.

3. Signalez un problème depuis l'application GlobalProtect à partir de votre terminal.

Après avoir lancé l'application, cliquez sur le menu hamburger du panneau d'état pour signaler un problème à votre administrateur.

1. Sélectionnez **Report an Issue (Signaler un problème)**.



2. Activez l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic. Les journaux de diagnostic et de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact.

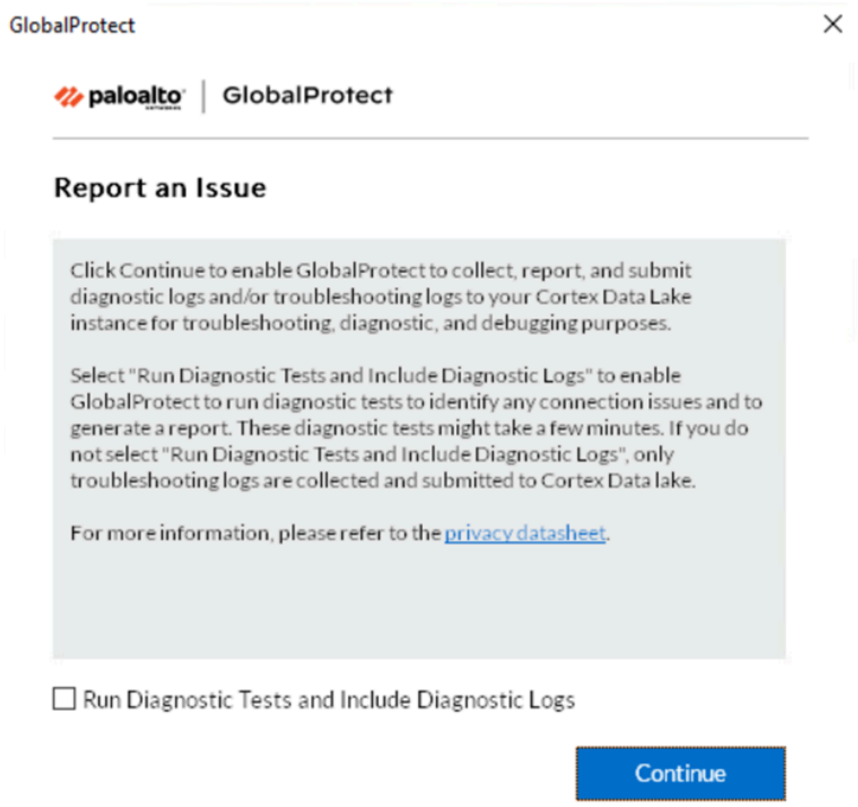
   Une fois les tests de diagnostic terminés avec succès, les fichiers journaux de débogage GlobalProtect sont téléchargés vers le service de journalisation Strata depuis votre terminal.

   Si vous n'activez pas l'application pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, seuls les journaux de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact. L'application GlobalProtect vérifie les fichiers de rapport (pan_gp.trb.log ou pan_gp_trbl.log) qui sont générés automatiquement au format `.json`*. Un message de notification apparaît si aucun problème n'a été trouvé dans les journaux de dépannage. Cliquez sur* ***Retry (Réessayer)*** *pour vérifier si les fichiers pan_gp.trb*.log existent.*

3. Cochez la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure les journaux de diagnostic)**.
4. Cliquez sur **Continue (Continuer)** pour permettre à l'application de créer un journal de dépannage et d'envoyer le rapport à l'instance du service de journalisation Strata de votre administrateur.

   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log.

L'application GlobalProtect peut exécuter des tests de diagnostic avec ou sans tunnel. Par exemple, vous voudrez peut-être entrer vos identifiants de connexion GlobalProtect avant que l'application ne se connecte et n'exécute des tests de diagnostic via le tunnel.



Un message s'affiche, confirmant que l'application exécute des tests de diagnostic uniquement si vous avez coché la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure des journaux de diagnostic)**.

5. Cliquez sur **Close (Fermer)** pour confirmer que l'application a réussi à envoyer le rapport au service de journalisation Strata. Ce message de confirmation affiche la date et l'heure auxquelles le rapport a été traité et envoyé.

Déconnexion de l'application GlobalProtect pour Windows

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Windows uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si votre administrateur configure la méthode de connexion à GlobalProtect sur **Always On (Toujours active)**, vous pouvez déconnecter l'application GlobalProtect si vous avez une bonne raison. Par exemple, vous pourriez vouloir déconnecter l'application si le Virtual Private Network (réseau privé virtuel - VPN) GlobalProtect ne fonctionne pas dans un hôtel, et l'échec du VPN vous empêche de vous connecter à Internet. Après avoir déconnecté l'application GlobalProtect, vous pouvez vous connecter à Internet en utilisant une communication non sécurisée (sans VPN).

La méthode, la durée et le nombre de déconnexions possibles de l'application GlobalProtect dépendent de la configuration du service GlobalProtect (PanGPS) par l'administrateur. Cette configuration peut vous empêcher de déconnecter complètement l'application ou vous permettre de déconnecter l'application uniquement après avoir répondu correctement à un défi.

Si votre configuration inclut un défi, l'application GlobalProtect vous demande l'un des éléments suivants :

- Raison pour laquelle vous souhaitez déconnecter l'application
- Répondez à une ou plusieurs raisons telles que **Internet speed slow (L'Internet est lent)** ou **App not working (L'application ne fonctionne pas)** (si nécessaire).
- Code secret
- Numéro de ticket

Si le défi nécessite un code secret ou un numéro de ticket, nous vous recommandons de contacter un administrateur GlobalProtect ou une personne du service d'assistance par téléphone.

Les administrateurs fournissent généralement des codes secrets à l'avance, soit par e-mail (pour les nouveaux utilisateurs de GlobalProtect), soit publiés sur le site Web de votre organisation. En réponse à une panne ou à un problème système, les administrateurs peuvent également fournir des codes secrets par téléphone.

Avant de pouvoir obtenir un numéro de ticket valide, votre terminal affiche un numéro de requête de ticket que vous devez communiquer à votre administrateur GlobalProtect ou à une personne du service d'assistance. Si votre requête de déconnexion est approuvée, vous recevrez un numéro de ticket valide que vous pouvez utiliser pour déconnecter GlobalProtect.

Les étapes suivantes décrivent comment déconnecter l'application et réussir un défi :

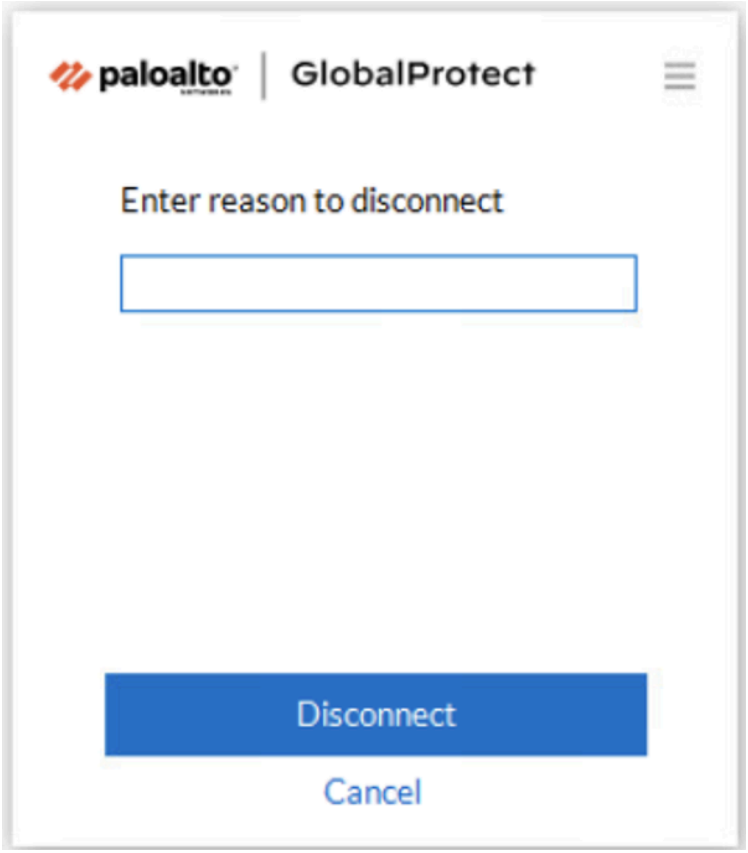
1. Déconnectez l'application GlobalProtect.
   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système GlobalProtect. Le panneau d'état s'ouvre.
   2. Cliquez sur le menu hamburger pour ouvrir le menu des paramètres.
   3. Sélectionnez **Disconnect (Déconnecter)**.

   *L'option **Disconnect (Déconnecter)** n'est visible que si la configuration de votre agent GlobalProtect vous permet de déconnecter l'application. Si la configuration vous permet de déconnecter l'application GlobalProtect sans exiger que vous répondiez à un défi, l'application GlobalProtect se ferme sans nécessiter d'action supplémentaire.*

2. Répondez à un ou plusieurs défis, si nécessaire.

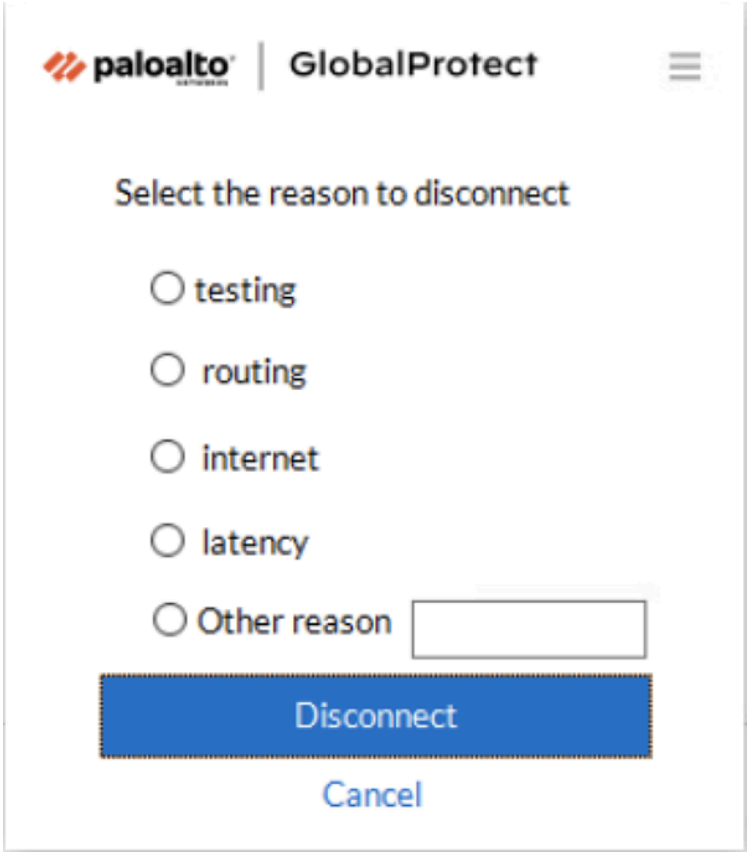
Si vous y êtes invité, fournissez les informations suivantes :

- **Tell us the issue to disconnect (Indiquer le problème lors de la déconnexion)** : la raison pour laquelle vous souhaitez déconnecter l'application GlobalProtect.



- **Select the reason to disconnect (Sélectionner la raison de la déconnexion)** : si votre configuration nécessite que vous répondiez à une ou plusieurs raisons ou que vous

saisissiez une autre raison, l'application GlobalProtect affiche les raisons dès que vous sélectionnez **Disconnect (Déconnecter)**.



- **Passcode (Code secret)** : un code secret fourni à l'avance par votre administrateur, en fonction d'un problème ou d'un événement connu qui vous oblige à désactiver l'application.
- **Ticket** : si votre configuration nécessite que vous fournissiez un numéro de ticket, l'application GlobalProtect affiche un numéro de requête de ticket hexadécimal à huit caractères dès que vous sélectionnez **Disconnect (Déconnecter)**. Pour déconnecter l'application avec un numéro de ticket, contactez votre administrateur ou la personne du service d'assistance (par téléphone) et fournissez le numéro de requête de ticket. Après avoir approuvé votre requête, votre administrateur ou la personne du service d'assistance vous fournit un numéro de ticket hexadécimal à huit caractères. Entrez le numéro de ticket dans le champ **Ticket**, puis cliquez sur **OK**.

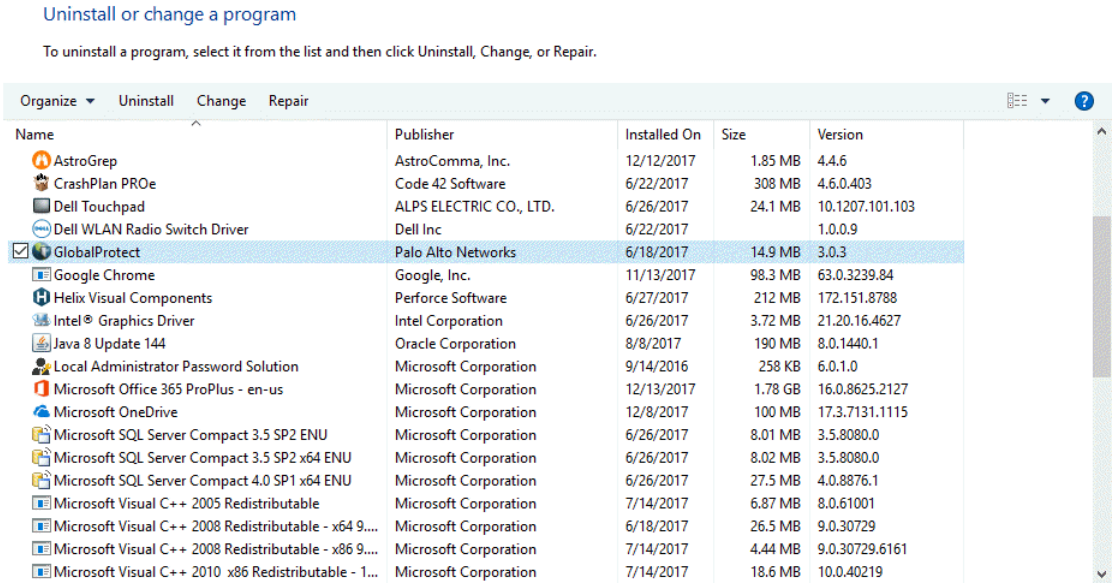
Désinstallation de l'application GlobalProtect pour Windows

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Windows uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Utilisez les étapes suivantes pour désinstaller l'application GlobalProtect de votre terminal Windows . Gardez à l'esprit qu'en désinstallant l'application, vous n'avez plus accès au VPN de votre réseau d'entreprise et que votre terminal ne sera pas protégé par les politiques de sécurité de votre entreprise.

Seuls les utilisateurs disposant de privilèges d'administrateur peuvent désinstaller l'application GlobalProtect des terminaux Windows.

1. Sélectionnez **Start (démarrer)** > **Control Panel (panneau de configuration)** > **Programs (Programmes)** > **Programs and Features (Programmes et fonctionnalités)**.
2. Sélectionnez **GlobalProtect** dans la liste, puis cliquez sur **Uninstall (Désinstaller)**.



3. Lorsque vous êtes invité à poursuivre la désinstallation, cliquez sur **Yes (Oui)**.

Résoudre un conflit de programmes d'installation de Microsoft

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Windows uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si vous cliquez sur **Enforce GlobalProtect for Network Access (Appliquer GlobalProtect pour l'accès réseau)** dans une configuration d'agent de portail GlobalProtect, puis que vous mettez à niveau un terminal Windows vers une version plus récente de l'application GlobalProtect, l'installation peut échouer et la configuration d'application peut bloquer tout le trafic.

Ce problème est causé par une limitation du système d'exploitation qui se produit lorsque plusieurs instances du programme d'installation Microsoft (`msiexec.exe`) s'exécutent simultanément sur un terminal Windows. Vous devez utiliser la procédure suivante pour résoudre le conflit de programmes d'installation de Microsoft :

1. Redémarrez le terminal.
2. Arrêtez tous les programmes d'installation tiers qui s'exécutent en arrière-plan.
   1. Appuyez sur **Ctrl+Alt+Suppr**, puis cliquez sur **Task Manager (Gestionnaire de tâches)**.
   2. Dans le **Task Manager (Gestionnaire de tâches)**, localisez tous les programmes `msiexec` tiers qui s'exécutent actuellement (par exemple, **`ligne de commande msiexec - Recherche Google`**).
   3. Sélectionnez le programme d'installation tiers, puis cliquez sur **End Task (Terminer la tâche)** pour arrêter le programme d'installation.
3. Restaurez la version existante de GlobalProtect, puis mettez à niveau vers la version plus récente de l'application.
   1. (Facultatif) Si nécessaire, réinstallez la version existante (plus ancienne) de GlobalProtect pour la réparer. Cette étape est requise si la mise à niveau continue d'échouer.
   2. Permettez à la mise à niveau de se dérouler comme prévu.

Application GlobalProtect pour macOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux MacOS uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

GlobalProtect™ est une application qui s'exécute sur votre terminal (ordinateur de bureau, ordinateur portable, tablette ou téléphone intelligent) pour vous protéger en utilisant les mêmes politiques de sécurité qui protègent les ressources sensibles de votre réseau d'entreprise. GlobalProtect™ sécurise votre intranet, votre cloud privé, votre cloud public et votre trafic Internet et vous permet d'accéder aux ressources de votre entreprise où que vous soyez dans le monde.

Les rubriques suivantes décrivent comment installer et utiliser l'appli GlobalProtect pour macOS :

- Téléchargement et installation de l'application GlobalProtect pour macOS
- Utilisation de l'application GlobalProtect pour macOS
- Signaler un problème depuis l'application GlobalProtect pour macOS
- Désactivation de l'application GlobalProtect pour macOS
- Désinstallation de l'application GlobalProtect pour macOS
- Suppression de l'extension du noyau de l'exécutant GlobalProtect
- Activation de l'application GlobalProtect pour macOS afin d'utiliser des certificats clients pour l'authentification

Téléchargement et installation de l'application GlobalProtect pour macOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux MacOS uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Avant de vous connecter au réseau GlobalProtect, vous devez télécharger et installer l'application GlobalProtect sur votre terminal macOS. Pour vous assurer d'obtenir la bonne application pour le déploiement GlobalProtect ou Prisma Access de votre organisation, vous devez télécharger l'application directement depuis un portail GlobalProtect au sein de votre organisation. Pour cette raison, il n'y a pas de lien de téléchargement direct de l'application GP disponible sur le site de Palo Alto Networks.

Avant de pouvoir télécharger et installer l'application GlobalProtect, vous devez obtenir l'adresse IP ou le FQDN du portail GlobalProtect auprès de votre administrateur. De plus, votre administrateur doit vérifier quel nom d'utilisateur et quel mot de passe vous pouvez utiliser pour vous connecter au portail et aux passerelles. Il s'agit généralement du même nom d'utilisateur et du même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise.

Lorsque vous installez l'application GlobalProtect pour la première fois sur un périphérique macOS exécutant macOS Catalina 10.15.4, macOS Big Sur 11 ou une version ultérieure ou que vous mettez à niveau vers l'application GlobalProtect 5.1.4, vous devez activer les extensions système utilisées pour des fonctionnalités spécifiques de GlobalProtect. Si votre administrateur a configuré un tunnel fractionné sur la passerelle GlobalProtect en fonction du nom de domaine de destination et du nom du processus d'application ou a imposé des connexions GlobalProtect pour l'accès réseau sur le portail GlobalProtect (voir Personnalisation de l'application GlobalProtect), le message de notification **System Extension Blocked (Extension système bloquée)** s'affiche sur l'application GlobalProtect pendant l'installation. Le message invite les utilisateurs à activer et à autoriser les extensions système dans macOS qui sont bloquées pour le chargement afin d'utiliser les fonctionnalités de tunnel fractionné et d'imposer GlobalProtect pour l'accès réseau.

Suivez ces directives lorsque vous utilisez des extensions système :

- *Seuls les utilisateurs ayant des privilèges d'administrateur peuvent activer les extensions système sur l'application GlobalProtect pour les terminaux macOS.*
- *En raison de l'amélioration de la sécurité sur macOS Catalina 10.15 et macOS Big Sur 11 pour garantir que vos données sont protégées lors de l'utilisation d'applications tierces, GlobalProtect doit demander votre autorisation avant de tenter d'accéder aux fichiers et dossiers stockés dans vos dossiers Documents, Bureau et Téléchargements ainsi que sur les lecteurs réseau. Si votre administrateur a activé les vérifications HIP, de nouvelles fenêtres contextuelles d'autorisation apparaissent sur votre terminal macOS lorsque GlobalProtect demande l'accès à certains fichiers et dossiers stockés dans votre système de fichiers.*
- *L'application GlobalProtect 5.1.4 fonctionnant sur macOS Catalina 10.15.4, macOS Big Sur 11 ou une version ultérieure n'utilise pas d'extensions de noyau et utilise des extensions système.*

- *L'application GlobalProtect 5.1.4 fonctionnant sur macOS Catalina 10.15.4, macOS Big Sur 11 ou une version ultérieure n'utilise pas les extensions de noyau (**com.paloaltonetworks.kext.pangpd**) et utilise plutôt l'une des* interfaces utun *disponibles fournies par macOS comme adaptateur virtuel.*
- *Si vous mettez à niveau d'une version antérieure vers l'application GlobalProtect 5.1.4 fonctionnant sur macOS Catalina 10.15.4, macOS Big Sur 11 ou une version ultérieure, les extensions de noyau ne sont plus nécessaires. Après la mise à niveau, le message de notification **System Extension Blocked (Extension système bloquée)** s'affiche sur l'application GlobalProtect, invitant les utilisateurs à activer et à autoriser les extensions système dans macOS qui ont été bloquées pour le chargement. Par défaut, l'application n'installe pas d'extensions système et les mêmes paramètres par défaut sont appliqués.*

Après avoir rassemblé les informations requises, utilisez les étapes suivantes pour télécharger et installer l'application :

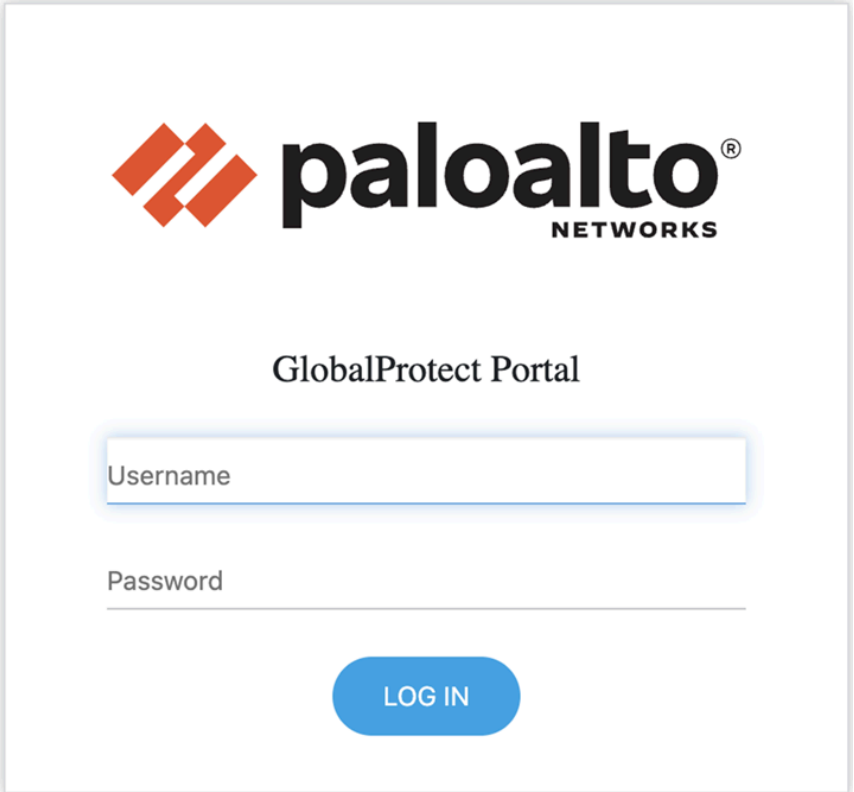
1. Connectez-vous au portail GlobalProtect.
   1. Lancez un navigateur Web et accédez à l'URL suivante :

      `https://<portal IP address or FQDN>`

      Exemple : **`http://gp.acme.com`**

      Si vous utilisez GlobalProtect 6.3 ou une version ultérieure et que vous avez prédéployé la fonctionnalité de portail intelligent, GlobalProtect vous redirige automatiquement vers le portail Prisma Access approprié en fonction de votre emplacement. Les portails définis dans la carte des pays du portail sont disponibles dans le menu déroulant. Pour plus d'informations, consultez la section Configuration du portail intelligent.
   2. Sur la page de connexion au portail, saisissez vos **Name (Nom)** (nom d'utilisateur) et **Password (Mot de passe)**, puis cliquez sur **LOG IN (Connexion)**. Dans la plupart des cas,

vous pouvez utiliser le même nom d'utilisateur et le même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise.



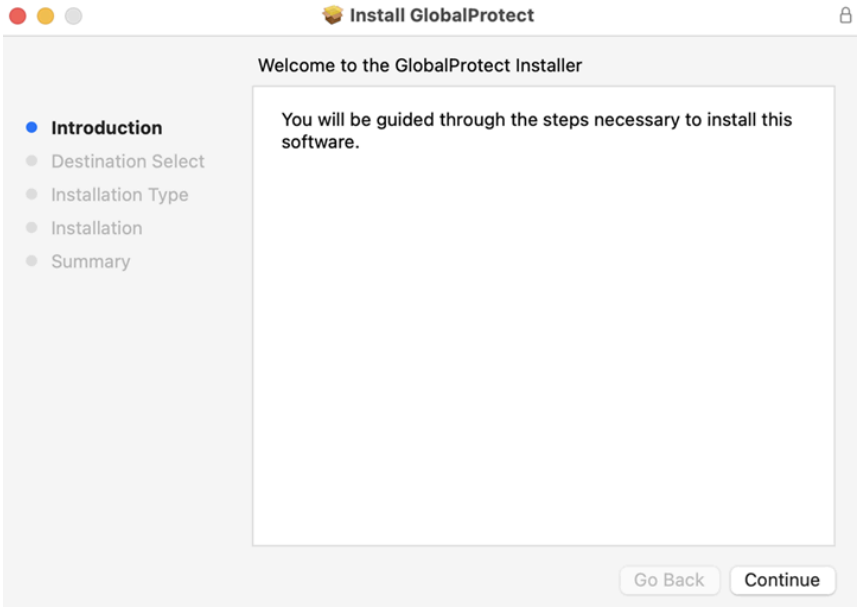
2. Accédez à la page de téléchargement de l'application.

Dans la plupart des cas, les pages de téléchargement de l'application apparaissent immédiatement après que vous vous êtes connecté au portail. Utilisez cette page pour télécharger le dernier package logiciel de l'application.

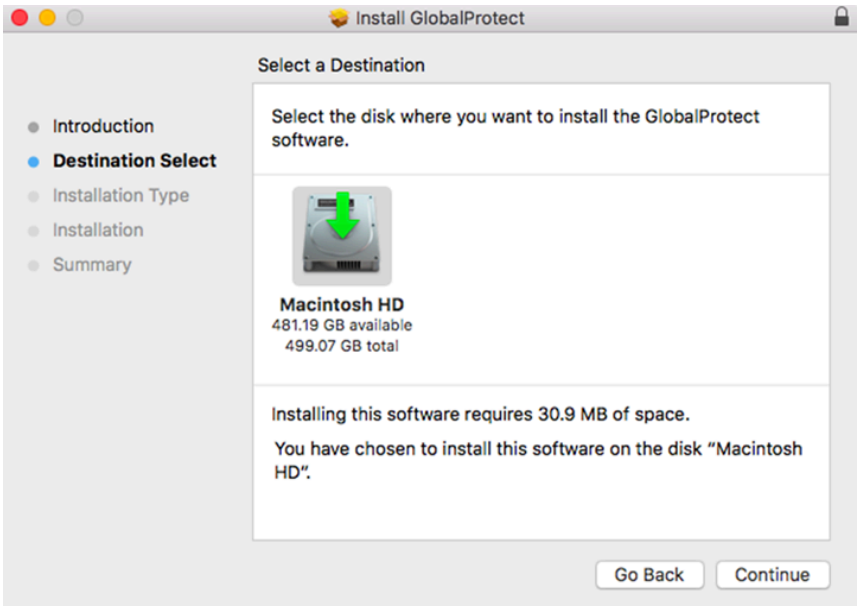
Si votre administrateur système a activé l'accès VPN sans client GlobalProtect, la page d'applications s'ouvre lorsque vous vous connectez au portail (au lieu de la page de téléchargement de l'application). Sélectionnez **GlobalProtect Agent (Agent GlobalProtect)** pour ouvrir la page de téléchargement.

3. Téléchargez l'application.
   1. Cliquez sur **Download Mac 32/64 bit GlobalProtect agent (Télécharger l'agent GlobalProtect pour Mac 32/64 bits)**.
   2. Lorsque vous y êtes invité, **Run (Exécutez)** le logiciel.
   3. Lorsque vous y êtes invité à nouveau, **Run (Exécutez)** le programme d'installation de GlobalProtect.

4. Complétez la configuration de l'application GlobalProtect à l'aide du programme d'installation de GlobalProtect.



1. Depuis le programme d'installation GlobalProtect, cliquez sur **Continue (Continuer)**.
2. Sur l'écran **Destination Select (Sélection de la destination)**, sélectionnez le dossier d'installation de l'application GlobalProtect, puis cliquez sur **Continue (Continuer)**.

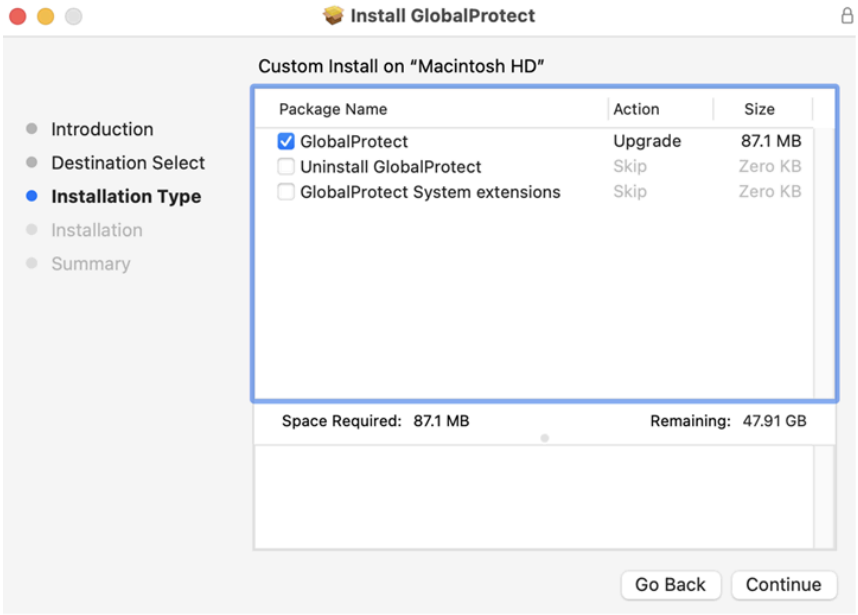


3. Sur l'écran **Installation Type (Type d'installation)**, cochez la case du package d'installation **GlobalProtect**.

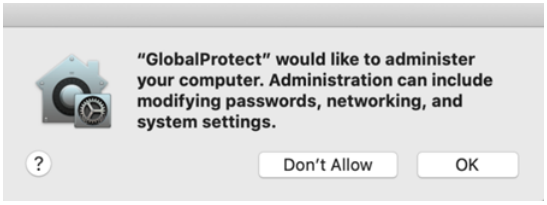
   Si votre administrateur système a configuré le tunnel fractionné sur la passerelle ou imposé des connexions GlobalProtect pour l'accès réseau sur le portail, cochez la case

GlobalProtect System extensions (Extensions système GlobalProtect) (désactivée par défaut).

Cliquez sur **Continue (Continuer)**.

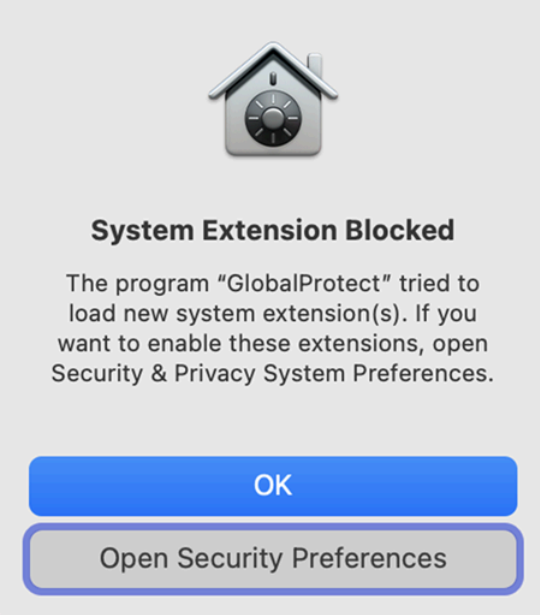


4. Cliquez sur **Install (Installer)** pour confirmer que vous souhaitez installer GlobalProtect.
5. À l'invite, saisissez votre **User Name (Nom d'utilisateur)** et votre **Password (Mot de passe)**, puis cliquez sur **Install Software (Installer le logiciel)** pour commencer l'installation.
6. Une fois l'installation terminée, cliquez sur **Close (Fermer)** pour fermer le programme d'installation.
7. Si votre administrateur a configuré le portail pour installer l'agent de terminal du DEM autonome (ADEM) lors de la première installation de l'application GlobalProtect, sélectionnez **OK** dans la fenêtre contextuelle suivante afin qu'elle n'apparaisse plus :



8. Si vous avez activé l'option **GlobalProtect System Extensions (Extensions système GlobalProtect)**, sélectionnez **Open Security Preferences (Ouvrir les préférences de sécurité)** pour activer les extensions système dans macOS qui ont été bloquées lors du

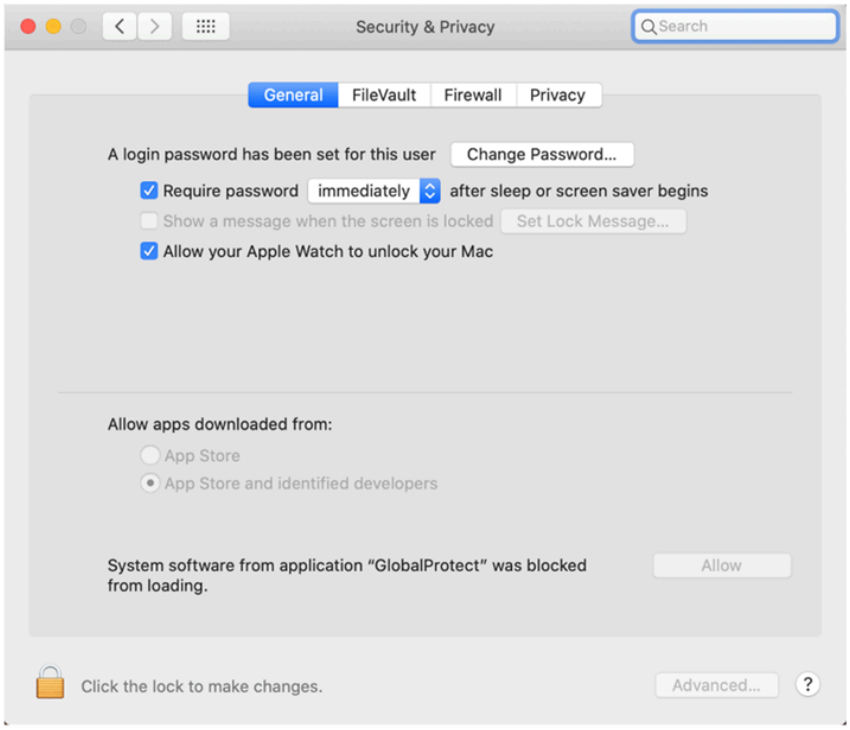
chargement de la notification suivante **System Extension Blocked (Extension système bloquée)** :



Si votre administrateur a supprimé cette notification en utilisant la Mobile Device Management (gestion des appareils mobiles - MDM) prise en charge, Jamf Pro, vous pouvez charger automatiquement les extensions système sans recevoir cette notification.

9. Dans la boîte de dialogue **Security & Privacy (Sécurité et confidentialité)**, cliquez sur l'icône **padlock (cadenas)** pour apporter des modifications, puis sélectionnez **App Store and identified developers (App Store et développeurs identifiés)** dans la zone **Allow**

apps downloaded from (Autoriser les applications téléchargées depuis). Cliquez sur **Allow (Autoriser)**.



Utilisation de l'application GlobalProtect pour macOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux MacOS uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Cette rubrique s'applique uniquement si votre configuration vous oblige à saisir vos informations d'identification de connexion GlobalProtect après vous être connecté à votre terminal (la connexion single sign-on est désactivée).

Nous recommandons généralement aux organisations de permettre à ses utilisateurs GlobalProtect de se connecter de manière transparente après l'installation de l'application. Après vous être connecté à un terminal avec une connexion GlobalProtect transparente, l'application GlobalProtect initie automatiquement et se connecte au réseau d'entreprise sans intervention supplémentaire de l'utilisateur.

Une fois l'installation terminée, le message de notification **System Extension Blocked (Extension système bloquée**) s'affiche, invitant les utilisateurs à activer les extensions système dans macOS dont le chargement a été bloqué. Si l'option **GlobalProtect System Extensions (Extensions système GlobalProtect)** n'est pas sélectionnée lors de l'installation, ce message de notification apparaît une fois que les utilisateurs se connectent à la passerelle. Cette notification apparaît si votre administrateur a configuré soit un tunnel fractionné sur la passerelle GlobalProtect, soit des connexions GlobalProtect appliquées pour l'accès au réseau sur le portail GlobalProtect (consultez la section Personnalisation de l'application GlobalProtect), soit les deux. Les deux fonctionnalités nécessitent que les utilisateurs activent les extensions système.

Si votre configuration nécessite que vous saisissiez vos identifiants GlobalProtect, suivez les étapes applicables ci-dessous.

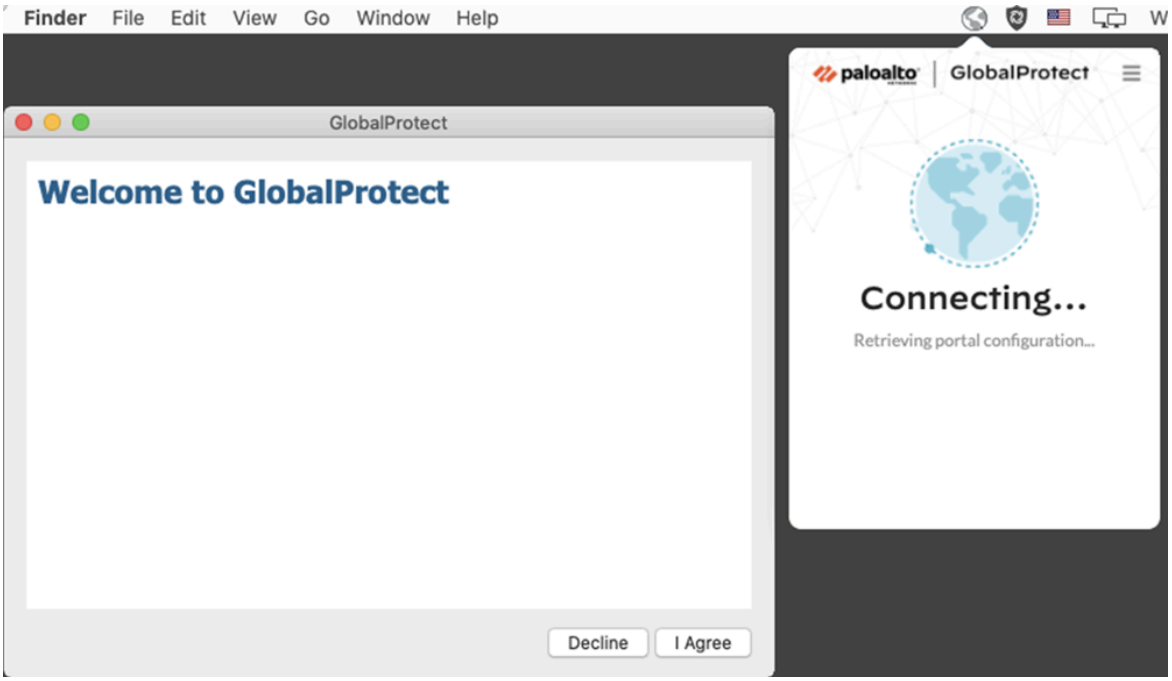
1. Ouvrez une session sur GlobalProtect.

   Si vous vous connectez au terminal pour la première fois, l'application GlobalProtect affiche une page d'accueil conviviale une fois la connexion réussie. Cliquez sur **Get Started (Commencer)**.

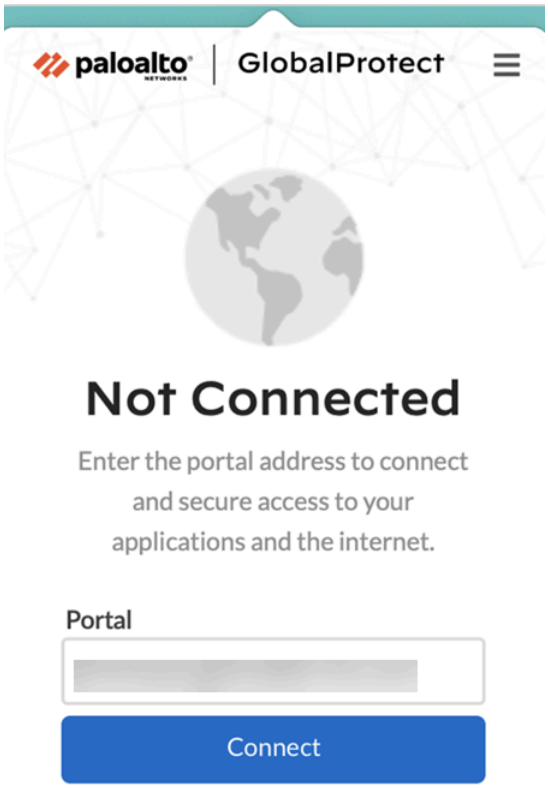
   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
   2. (Facultatif) Passez en revue les conditions d'utilisation de votre entreprise avant de vous connecter à GlobalProtect si votre administrateur exige que vous consultiez une page pour accéder aux ressources internes.

      Si vous n'acceptez pas les conditions d'utilisation, vous ne pourrez pas vous connecter à GlobalProtect.

      En option, si vous cliquez sur **Cancel (Annuler)**, vous devez saisir l'adresse IP (ou le domaine) du portail GlobalProtect, puis cliquer sur **Connect (Connecter)** pour établir la connexion.



3. Saisissez l'adresse IP ou le domaine du portail fourni par votre administrateur GlobalProtect, puis cliquez sur **Connect (Connecter)**.



2. Connectez-vous au portail GlobalProtect ou à la passerelle.

Vous pouvez déterminer si vous êtes connecté en vérifiant l'icône de bac de système GlobalProtect. Si vous n'êtes pas connecté, l'icône est grise () et ***Not Connected (Non connecté)*** *apparaît lorsque vous survolez l'icône.*

1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
2. (Facultatif) Si vous vous connectez à l'application GlobalProtect pour la première fois, saisissez le FQDN ou l'adresse IP du portail GlobalProtect, puis cliquez sur **Connect (Se connecter**).
3. (Facultatif) Si plusieurs portails sont enregistrés sur votre application, sélectionnez un portail dans la liste déroulante **Change Portal (Modifier le portail)**. Par défaut, le portail le plus récemment connecté est présélectionné dans la liste déroulante **Change Portal (Modifier le portail)**.
4. (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, cliquez sur la liste déroulante **Change Gateway (Modifier la passerelle)**, puis utilisez l'une des options suivantes :
   - Sélectionnez une passerelle manuellement (passerelles externes uniquement). Cette option n'est disponible que si votre administrateur active la sélection manuelle de la passerelle.

- Attribuez et connectez-vous automatiquement à une passerelle préférée :

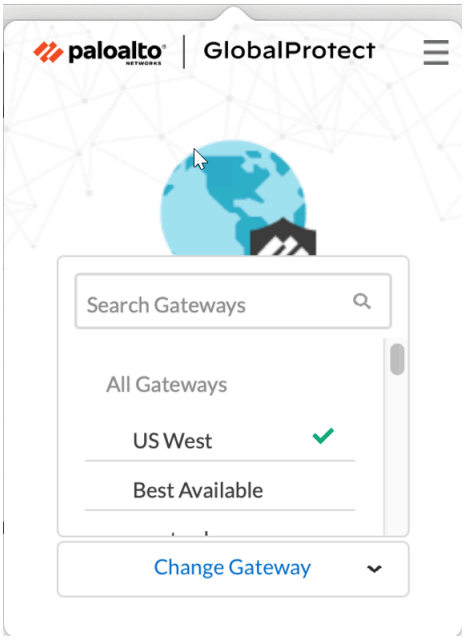
  1. Pour désigner une passerelle comme préférée, cliquez sur l'icône en forme d'étoile ( ). La prochaine fois que vous vous connecterez, vous vous connecterez automatiquement à cette passerelle préférée.

     Si vous décidez ultérieurement de ne plus vouloir de la passerelle comme passerelle préférée, vous pouvez simplement effacer l'icône en forme d'étoile pour supprimer cette passerelle comme connexion préférée.

  2. Par défaut, vous vous connectez automatiquement à la passerelle **Best Available (Meilleure disponible)** qui est identifiée par une coche dans la liste déroulante **Change Gateway (Modifier la passerelle)**. Si vous définissez la passerelle préférée,

une étoile s'affiche par la passerelle étoilée dans la liste déroulante **Change Gateway (Modifier la passerelle)**.

Si votre administrateur a configuré des passerelles externes manuelles dans la configuration de l'agent de portail, vous pouvez choisir une passerelle spécifique à l'aide du champ de recherche de passerelle.



5. (Facultatif) Selon le mode de connexion, cliquez sur **Connect (Connecter)** pour initier la connexion.
6. (Facultatif) Si vous y êtes invité, entrez votre **Username (Nom d'utilisateur)** et votre **Password (Mot de passe)**, et cliquez sur **Sign In (Se connecter)**.

   Si votre administrateur vous a permis d'utiliser des informations biométriques (empreinte digitale) pour vous connecter, vous devez d'abord vous connecter avec un nom d'utilisateur et un mot de passe deux fois (une fois pour l'enregistrer et à nouveau pour vous authentifier). Vous pouvez ensuite utiliser des informations biométriques pour vous connecter.

   Si votre administrateur système a activé les **GlobalProtect System Extensions (Extensions système GlobalProtect)**, vous devez activer les extensions système dans macOS dont le chargement a été bloqué pour utiliser le tunnel fractionné et appliquer GlobalProtect pour les fonctionnalités d'accès au réseau.

   > *Les utilisateurs n'ont pas besoin de privilèges d'administrateur pour autoriser les invites contextuelles* ***Network Extensions Configuration (Configuration des extensions réseau)****. Votre administrateur peut supprimer ces invites de message en utilisant le Mobile Device Management (gestion des appareils mobiles - MDM) tel que Jamf Pro pour charger automatiquement les extensions réseau sans recevoir ces invites. Reportez-vous à l'article de la base de données de connaissances à l'adresse* https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8

*pour des informations sur la façon de*enable system and network extensions using Jamf Pro (activer le système et les extensions de réseau en utilisant Jamf Pro).

1. (macOS Catalina 10.15.4 ou version ultérieure et macOS Big Sur 11 ou version ultérieure uniquement) Si votre administrateur système a configuré un tunnel fractionné en fonction des domaines et des applications sur la passerelle GlobalProtect ou activé la fonctionnalité Enforce GlobalProtect Connections for Network Access (Appliquer les connexions GlobalProtect pour l'accès au réseau), sélectionnez **Allow (Autoriser)** dans l'invite contextuelle suivante :

Si vous sélectionnez **Don't Allow (Ne pas autoriser)**, la fonctionnalité Split Tunnel (Tunnel fractionné) ne peut pas être utilisée sur l'application GlobalProtect, la fonctionnalité Enforce GlobalProtect Connections for Network Access (Appliquer les connexions GlobalProtect pour l'accès au réseau) ne fonctionnera pas et les connexions GlobalProtect pour l'accès au réseau ne peuvent pas être appliquées. Cette invite contextuelle apparaîtra lors de votre prochaine connexion au portail ou à la passerelle ou jusqu'à ce que vous sélectionniez **Allow (Autoriser)**.

Lorsque l'application se connecte en mode externe, l'icône de bac de système GlobalProtect affiche un bouclier (), et **Connected (Connecté)** apparaît lorsque vous survolez l'icône. Lorsque l'application se connecte en mode interne, l'icône de bac de système GlobalProtect affiche une maison (), et **Internal Network (Réseau interne)** apparaît lorsque vous survolez l'icône.

3. Ouvrez l'application GlobalProtect.

Cliquez sur l'icône de bac de système GlobalProtect pour lancer l'interface de l'application.

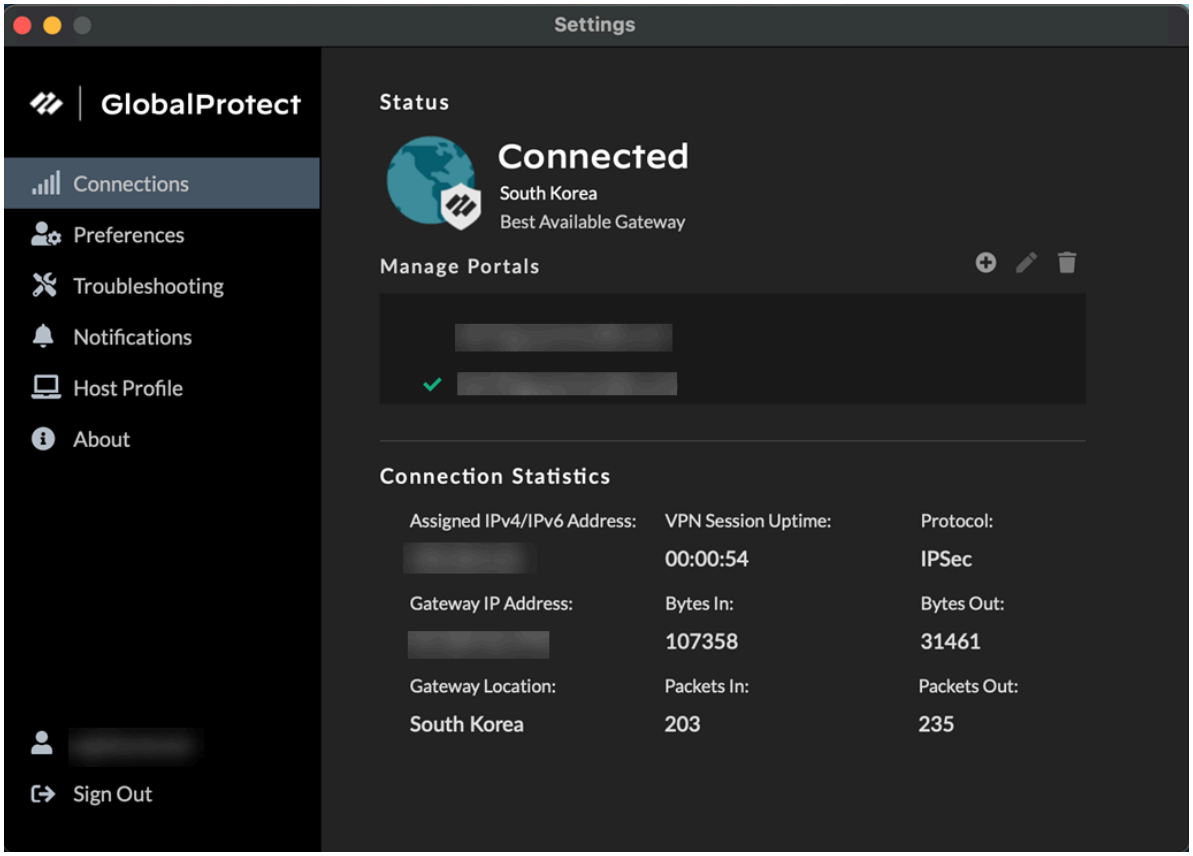
Une notification s'affiche si votre administrateur a configuré le portail pour installer l'agent de terminal DEM autonome (ADEM) lors de l'installation de l'application GlobalProtect et vous a autorisé à activer les tests ou non. Si votre administrateur a déjà installé l'agent de terminal ADEM et configuré ultérieurement le portail pour désinstaller l'agent de terminal ADEM, une notification apparaît lors de la prochaine connexion.

4. Affichez des informations sur votre connexion réseau.

Après avoir lancé l'application, cliquez sur le menu hamburger dans le panneau d'état pour ouvrir le menu des paramètres. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau **GlobalProtect Settings (Paramètres GlobalProtect)**, puis sélectionnez l'un des paramètres suivants pour afficher et modifier l'application GlobalProtect :

- **Connections (Connexions)** : l'onglet **Connections (Connexions)** affiche le ou les portails associés au compte GlobalProtect. Vous pouvez ajouter, modifier ou supprimer des portails

à partir de cet onglet. Cet onglet affiche également la passerelle à laquelle vous êtes connecté. Vous pouvez afficher les statistiques de connexion sur la passerelle (par exemple, l'adresse IP de la passerelle, l'emplacement et la disponibilité de la session VPN) lorsque votre administrateur définit **Enable Advanced View (Activer la vue avancée)** sur **Yes (Oui)** dans la configuration de l'agent du portail GlobalProtect. Sélectionnez l'onglet **Connections (Connexions)** pour voir le compte à rebours de la durée de vie de la connexion.



L'onglet **Connections (Connexions)** affiche les détails du proxy si la fonctionnalité Explicit Proxy Connectivity (Connectivité explicite du proxy) dans GlobalProtect pour la sécurité Internet toujours active est activée pour l'application via Prisma Access.

Mode proxy :

- **Preferences (Préférences)** : l'onglet **Preferences (Préférences)** n'est désormais disponible que si votre administrateur configure au moins l'une des options suivantes :
  - **Enable Biometric Sign-in (Activer la connexion biométrique)** : vous pouvez choisir d'utiliser les informations biométriques (empreinte digitale) pour vous connecter. Cette option n'est disponible que si votre administrateur configure l'option **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)** sur **Only with User Fingerprint (Uniquement avec l'empreinte digitale de l'utilisateur)** dans la configuration de l'agent GlobalProtect. Vous devez 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.

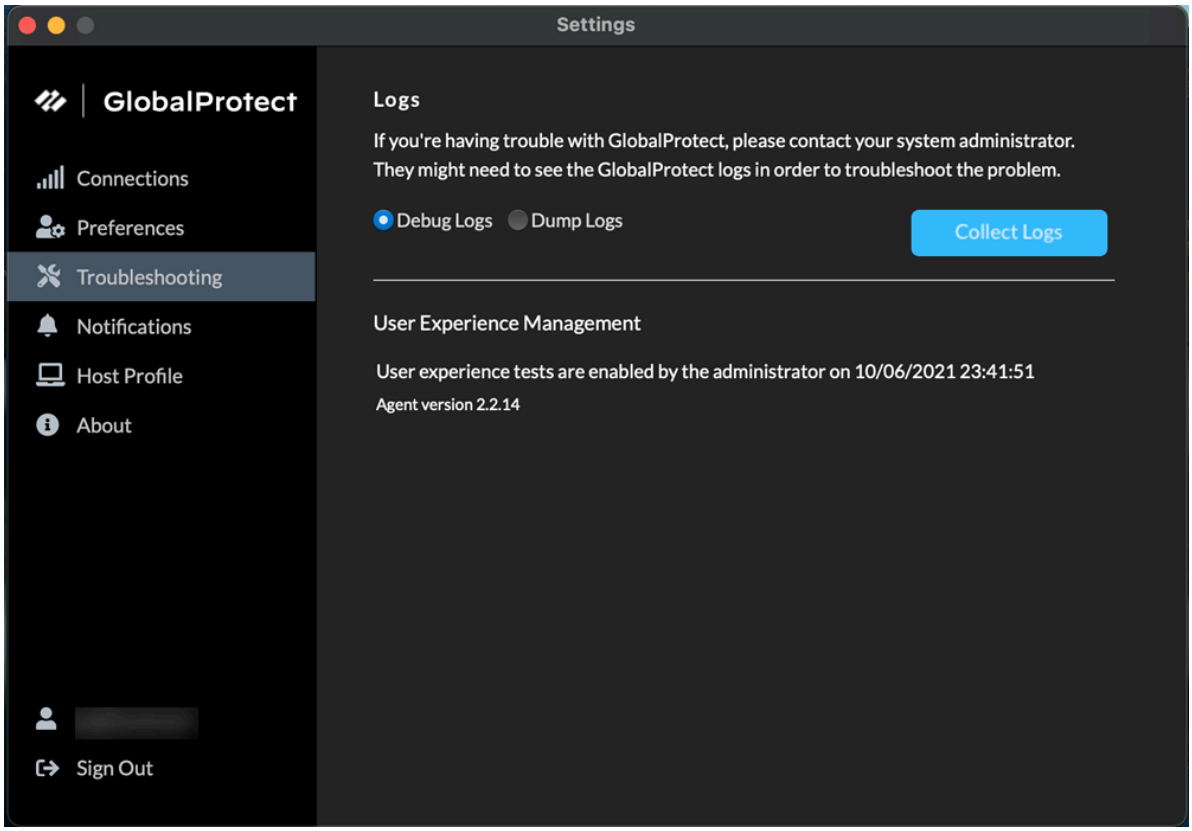
- **Do not display a welcome page upon each successful connection (Ne pas afficher de page d'accueil lors de chaque connexion réussie)** : vous pouvez choisir d'afficher une page d'accueil lors de la connexion réussie. Cette option n'est disponible que si votre administrateur définit la **Welcome Page (Page d'accueil)** sur **factory-default** dans la configuration de l'agent du portail GlobalProtect.
- **Connect with SSL (Se connecter avec SSL)** : vous pouvez choisir d'utiliser SSL ou de rester avec IPSec. Cette option n'est disponible que si votre administrateur définit **Connect with SSL Only (Se connecter avec SSL uniquement)** sur**User can Change (L'utilisateur peut modifier)** dans la configuration de l'agent du portail GlobalProtect.
- **Always run diagnostic tests and include logs (Toujours exécuter des tests de diagnostic et inclure des journaux)** : vous pouvez choisir d'activer l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic. Cette option n'est disponible que si votre administrateur active la collecte de journaux de l'application GlobalProtect pour le dépannage sur le portail GlobalProtect.

- **Troubleshooting (Dépannage)** : l'onglet **Troubleshooting (Dépannage)** vous permet de **Collect Logs (Collecter les journaux)** et de définir le niveau de journalisation sur **Debug Logs (Déboguer les journaux)** ou **Dump Logs (Journaux de vidage)**, et éventuellement **Enable User Experience Tests (Activer les tests d'expérience utilisateur)**.

  Pour que l'application GlobalProtect envoie des journaux de dépannage, des journaux de diagnostic ou les deux au service de journalisation Strata pour une analyse plus approfondie, vous devez configurer le portail GlobalProtect pour activer la GlobalProtect app log collection for troubleshooting (Collecte de journaux d'application GlobalProtect pour le dépannage). De plus, vous pouvez configure the HTTPS-based destination URLs (configurer les URL de destination basées sur HTTPS) qui peuvent contenir des adresses IP ou des noms de domaine complets des serveurs/ressources

Web que vous souhaitez sonder, et déterminer des problèmes tels que la latence ou les performances du réseau sur le point de terminaison de l'utilisateur final.

Vous pouvez cliquer sur **Advanced (Avancé)** pour afficher des informations détaillées sur leur terminal.



La fenêtre **Advanced Logging Settings (Paramètres avancés de journalisation)** affiche les informations concernant la configuration du réseau, les paramètres d'itinéraire, les connexions actives et les journaux.

Lorsque GlobalProtect est connecté, vérifiez que l'agent du terminal ADEM peut effectuer des tests d'expérience utilisateur si la case à cocher **Enable user experience tests (Activer les tests d'expérience utilisateur)** s'affiche sur l'application GlobalProtect. Vous pouvez également vérifier qu'un message s'affiche si votre administrateur a installé l'agent de terminal ADEM lors de l'installation de l'application GlobalProtect, mais ne vous permet pas d'activer ou de désactiver les tests d'expérience utilisateur à partir de l'application GlobalProtect. Par défaut, les alertes de pulsation sont toujours transmises à l'ADEM même lorsque GlobalProtect est désactivé ou déconnecté.

Si votre administrateur a configuré le portail pour installer l'agent de terminal DEM autonome lors de l'installation de l'application GlobalProtect et vous a autorisé à activer les tests, cochez la case **Enable user experience tests (Activer les tests d'expérience utilisateur)** sur l'application GlobalProtect. Cette case à cocher ne s'affiche pas si votre administrateur ne vous permet pas d'activer ou de désactiver les tests d'expérience utilisateur à partir

de l'application GlobalProtect. Au lieu de cela, un message s'affiche, confirmant que l'application est activée pour exécuter des tests d'expérience utilisateur.

Si vous ne cochez pas la case **Enable user experience tests (Activer les tests d'expérience utilisateur)**, les alertes de pulsation sont toujours transmises à l'ADEM.

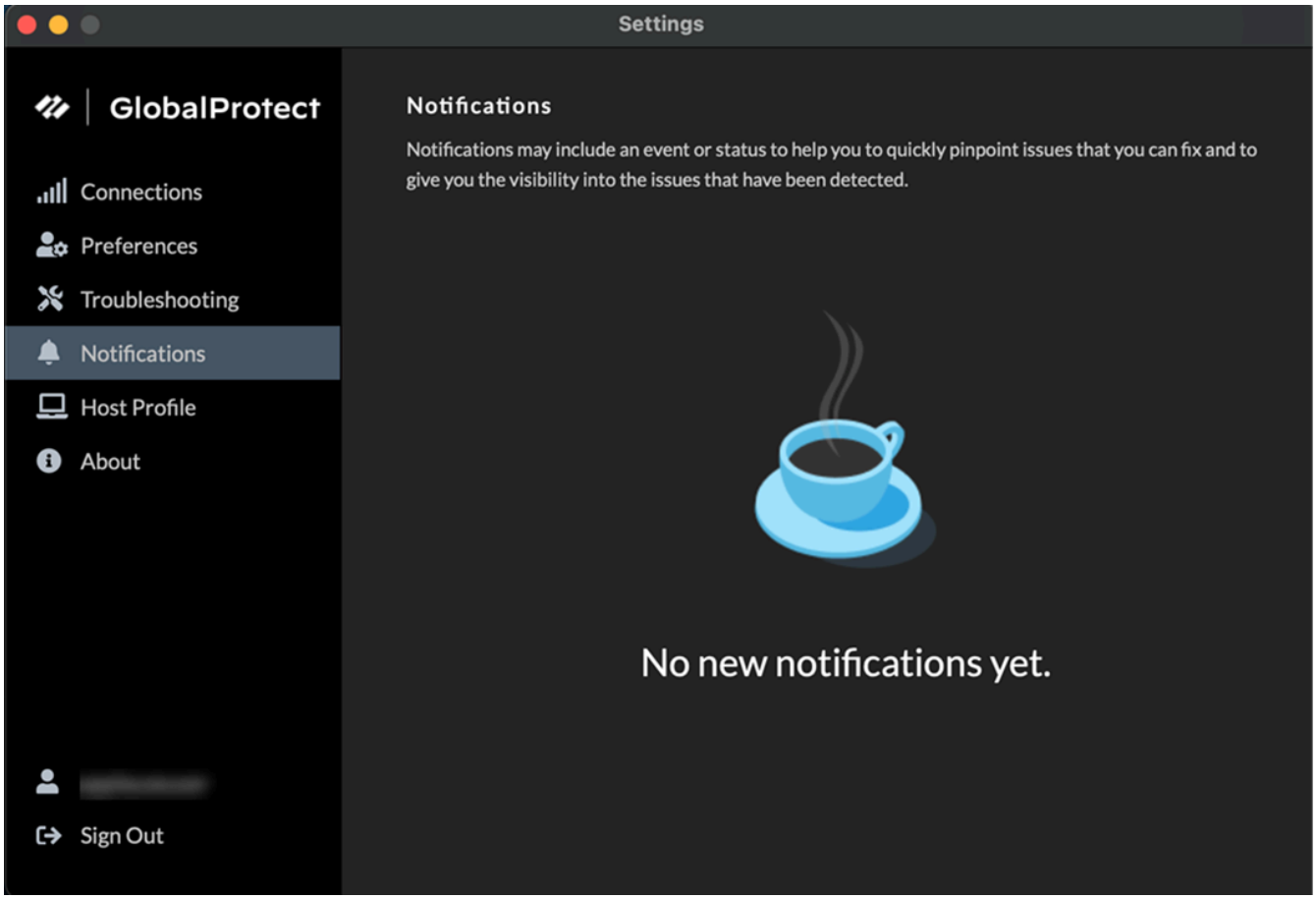
- **Notifications** : l'onglet **Notifications** affiche les informations détaillées sur les notifications spécifiques déclenchées sur l'application GlobalProtect. Vous pouvez configurer les notifications de l'utilisateur final concernant l'expiration des sessions de l'application GlobalProtect sur la passerelle et planifier l'affichage de ces notifications personnalisées sur l'application.

  À partir de la version 6.2.3 de l'application GlobalProtect, les messages de session et de délai d'inactivité sont supprimés pour la méthode de connexion toujours active.

  À partir de la version 6.2 de l'application GlobalProtect, vous pouvez prolonger la durée de vie de la session de connexion de l'application GlobalProtect avant son expiration pour éviter une déconnexion soudaine de la session de l'application. La notification d'expiration de la durée de vie de la connexion vous informe à l'avance lorsque les sessions de l'application sont sur le point d'expirer et offre la possibilité de prolonger la durée de la session utilisateur afin que vous ne soyez pas déconnecté brusquement de votre session. L'application affiche la notification d'expiration avec l'option Extend User Session (Étendre

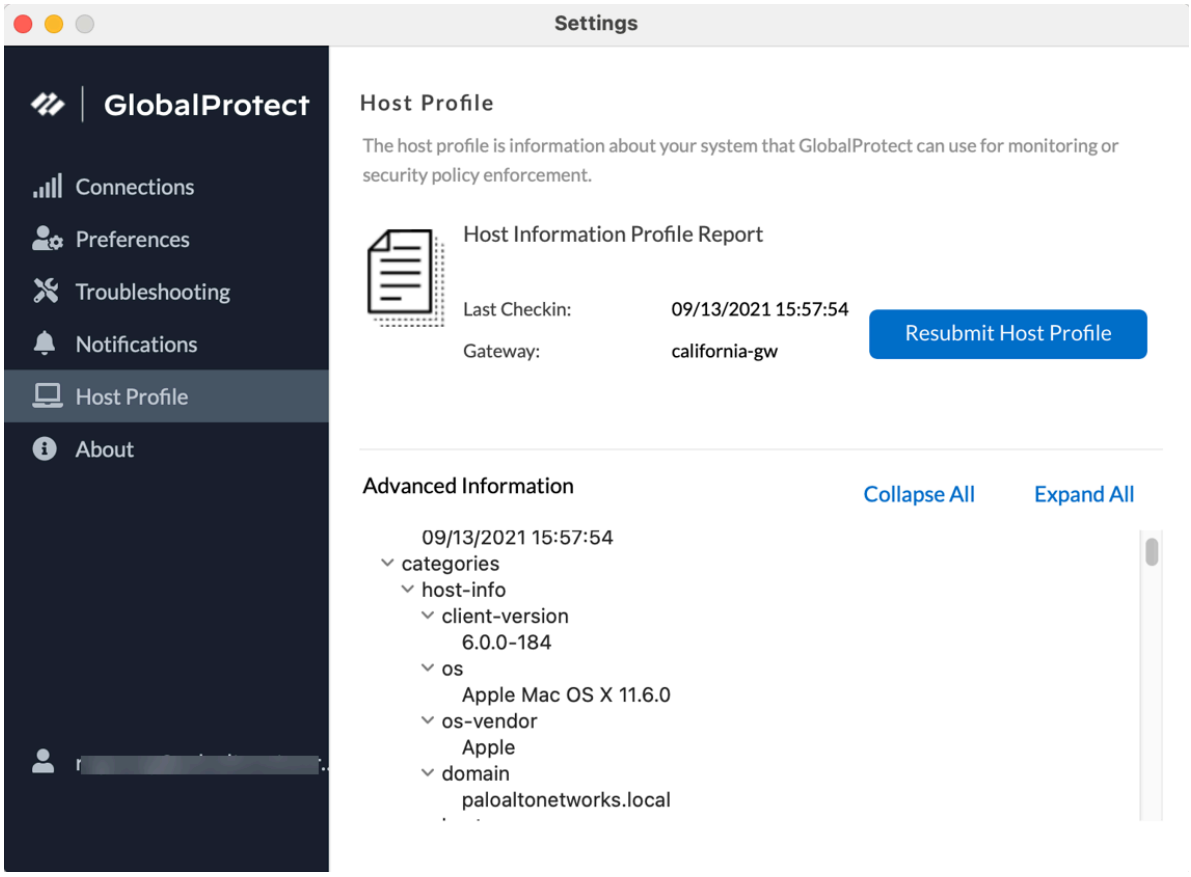
la session utilisateur) si votre administrateur a configuré les paramètres de notification pour l'extension de la session.

Vous êtes également informé s'il n'y a pas de nouvelles notifications déclenchées sur l'application GlobalProtect.



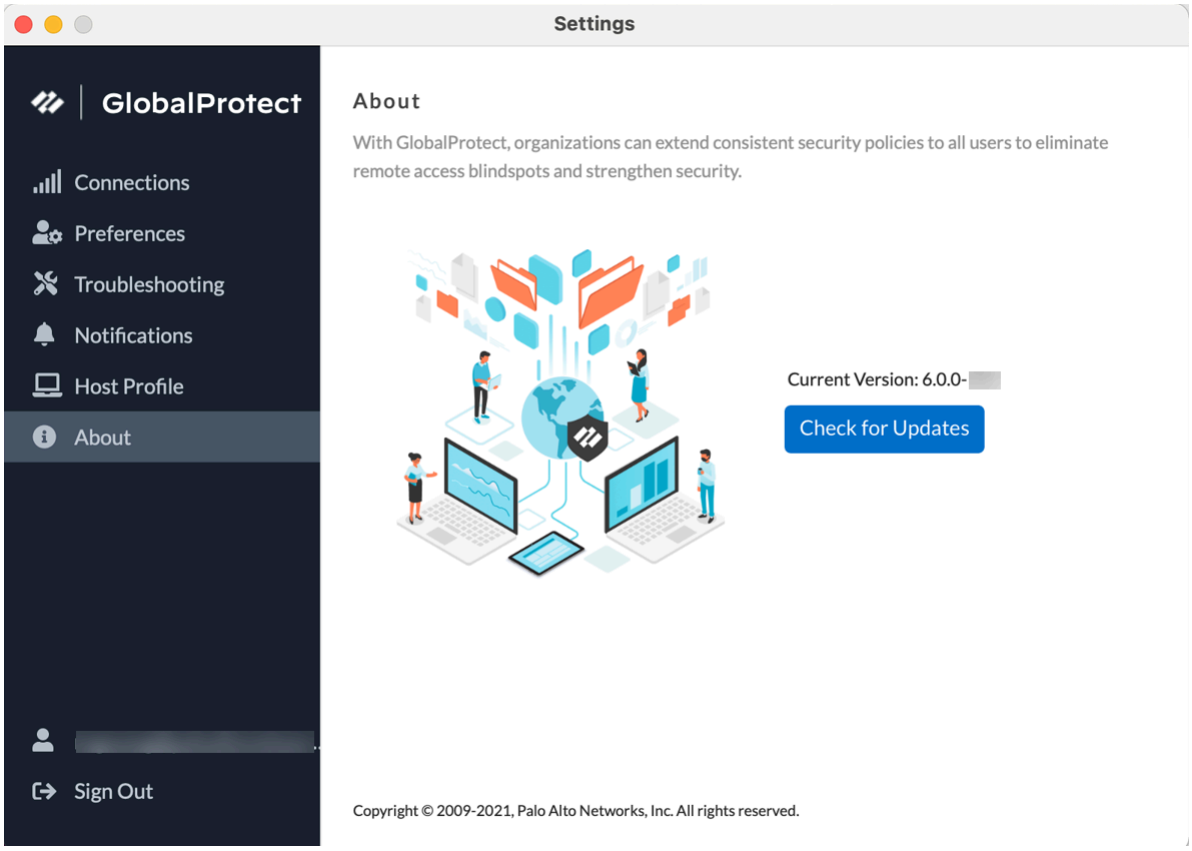
- **Host Profile (Profil d'hôte)** : l'onglet **Host Profile (Profile d'hôte)** affiche les données sur les terminaux que GlobalProtect utilise pour la surveillance et l'application des politiques de sécurité par l'intermédiaire du Host Information Profile (Profil d'informations sur l'hôte

- HIP). Vous pouvez cliquer sur **Resubmit Host Profile (Envoyer de nouveau le profil de l'hôte)** pour procéder au renvoi manuel des données HIP à la passerelle.



Si votre administrateur a configuré plusieurs passerelles internes en mode sans tunnel et en détection d'hôte interne, vous pouvez cliquer sur **More Details (Plus de détails)** pour surveiller l'envoi du rapport Host Information Profile (Profil d'informations sur l'hôte - HIP) pour chaque passerelle à partir d'un emplacement central afin de vous aider à résoudre rapidement les problèmes liés au HIP.

- **About (À propos)** : l'onglet **About (À propos)** affiche la version de GlobalProtect actuellement installée sur le terminal et permet aux utilisateurs finaux de **Check for Updates (Vérifier les mises à jour)**.



5. (Facultatif) Connectez-vous en utilisant un nouveau mot de passe.

   *Si votre administrateur GlobalProtect configure l'agent du portail GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vos informations d'identification sont automatiquement enregistrées dans l'application GlobalProtect. Si votre mot de passe pour accéder au réseau d'entreprise change, vous devez vous connecter à GlobalProtect en utilisant votre nouveau mot de passe.*

   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
   2. Cliquez sur le menu hamburger pour ouvrir le menu des paramètres.
   3. Sélectionnez **Settings (Paramètres)** pour ouvrir le panneau des **GlobalProtect Settings (Paramètres GlobalProtect)**.
   4. Dans le panneau **GlobalProtect Settings (Paramètres GlobalProtect)**, **Sign Out (Déconnectez-vous)** pour effacer vos informations d'identification d'utilisateur enregistrées de l'application GlobalProtect.
   5. Après avoir effacé vos identifiants utilisateur, vous pouvez vous reconnecter à GlobalProtect avec votre nouveau nom d'utilisateur et mot de passe.

6. (Facultatif) Déconnectez-vous de GlobalProtect.

   Si votre administrateur configure GlobalProtect avec la méthode de connexion **On-Demand (À la demande)**, vous pouvez vous déconnecter de GlobalProtect en cliquant sur **Disconnect (Déconnecter)** dans le panneau d'état.

Signaler un problème depuis l'application GlobalProtect pour macOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux MacOS uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si vous rencontrez un comportement inhabituel, tel qu'une mauvaise performance du réseau ou une impossibilité d'établir une connexion avec le portail et la passerelle, vous pouvez signaler le problème directement au service de journalisation Strata auquel votre administrateur peut accéder. Vous n'avez plus besoin de collecter manuellement et d'envoyer les journaux de l'application GlobalProtect par e-mail ou de les stocker sur un lecteur cloud.

*Pour afficher l'option **Report an Issue (Signaler un problème)** sur l'application GlobalProtect, votre administrateur doit activer la collecte des journaux de l'application GlobalProtect pour le dépannage sur le portail GlobalProtect.*

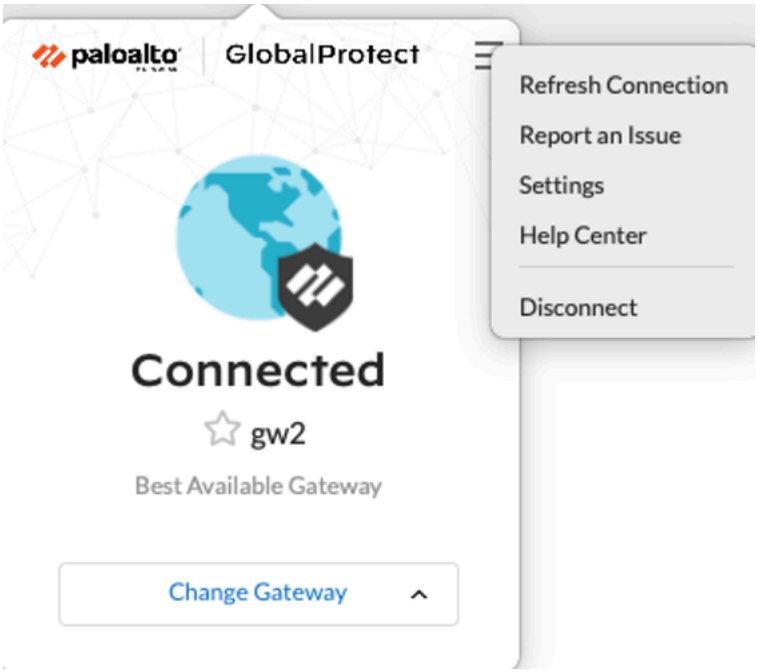
1. Connectez-vous au portail GlobalProtect ou à la passerelle.
   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
   2. (Facultatif) Si vous vous connectez à l'application GlobalProtect pour la première fois, saisissez le FQDN ou l'adresse IP du portail GlobalProtect, puis cliquez sur **Connect (Se connecter)**.
   3. (Facultatif) Si plusieurs portails sont enregistrés sur votre application, sélectionnez un portail dans le menu déroulant **Portal (Portail)**. Par défaut, le portail le plus récemment connecté est présélectionné dans le menu déroulant **Portal (Portail)**.
   4. (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 passerelle différente, cliquez sur le menu déroulant de la passerelle.
2. Ouvrez l'application GlobalProtect.

   Cliquez sur l'icône de bac de système GlobalProtect pour lancer l'interface de l'application.

3. Signalez un problème depuis l'application GlobalProtect à partir de votre terminal.

Après avoir lancé l'application, cliquez sur le menu hamburger du panneau d'état pour signaler un problème à votre administrateur.

1. Sélectionnez **Report an Issue (Signaler un problème)**.



2. Activez l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic. Les journaux de diagnostic et de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact.

   Une fois les tests de diagnostic terminés avec succès, les fichiers journaux de débogage GlobalProtect sont téléchargés vers le service de journalisation Strata depuis votre terminal.

   Si vous n'activez pas l'application pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, seuls les journaux de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact. L'application GlobalProtect vérifie les fichiers de rapport (pan_gp.trb.log ou pan_gp_trbl.log) qui sont générés automatiquement au format `.json`. Un message de

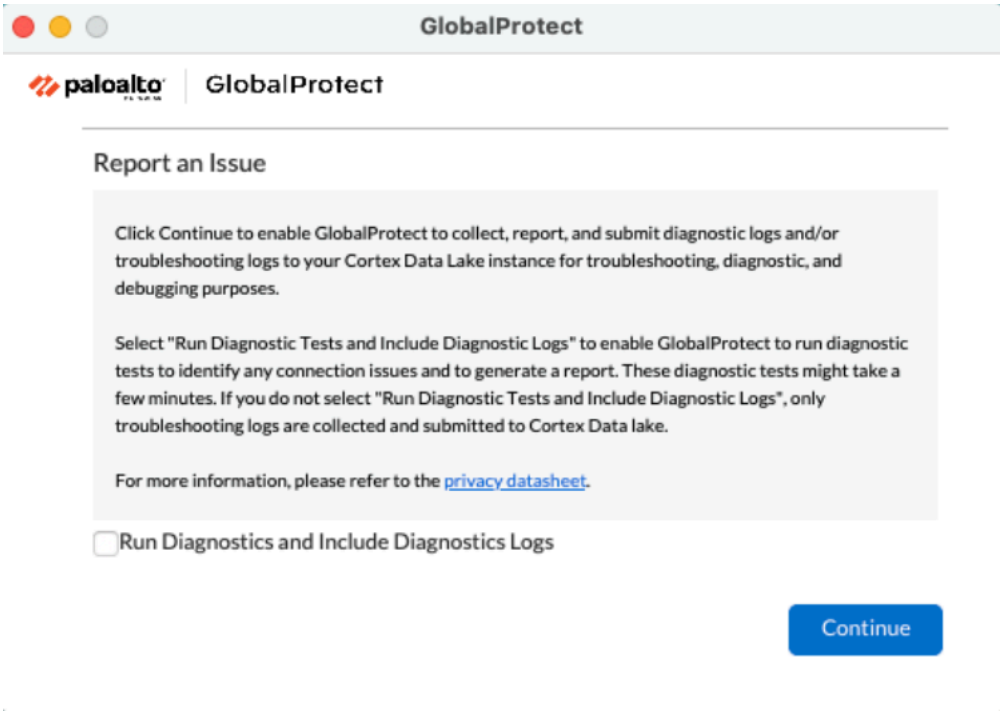
*notification apparaît si aucun problème n'a été trouvé dans les journaux de dépannage. Cliquez sur **Retry (Réessayer)** pour vérifier si les fichiers pan_gp.trb*.log existent.*

3. Cochez la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure les journaux de diagnostic)**.
4. Cliquez sur **Continue (Continuer)** pour permettre à l'application de créer un journal de dépannage et d'envoyer le rapport à l'instance du service de journalisation Strata de votre administrateur.

   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log.

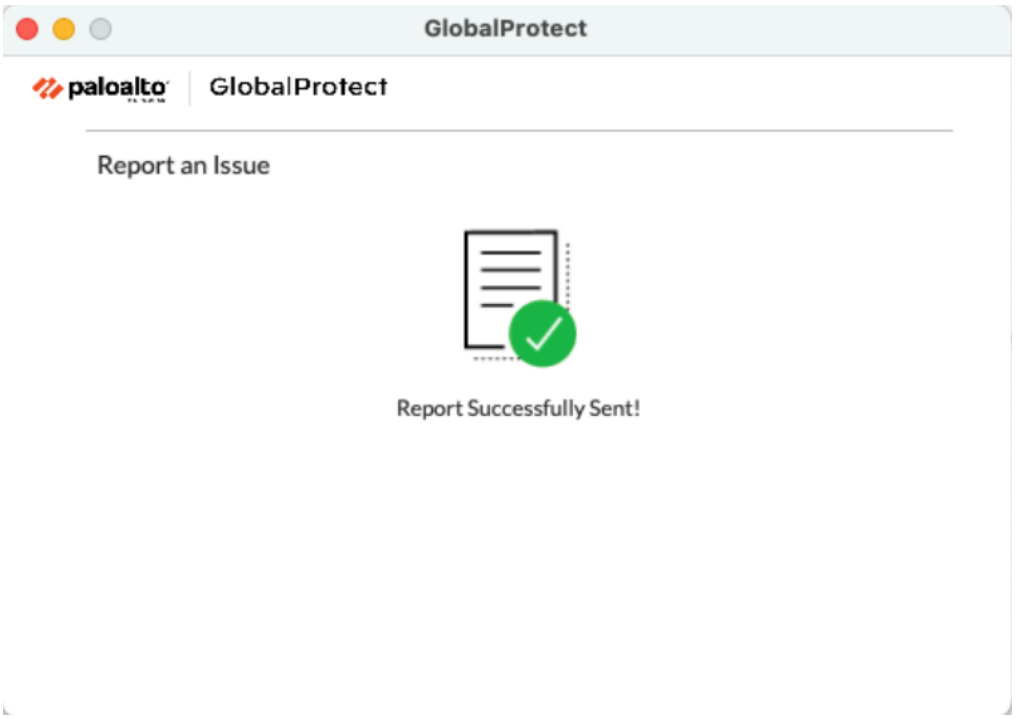
   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log. L'application GlobalProtect peut exécuter des tests de diagnostic avec ou sans tunnel.

Par exemple, vous voudrez peut-être entrer vos identifiants de connexion GlobalProtect avant que l'application ne se connecte et n'exécute des tests de diagnostic via le tunnel.



Un message s'affiche, confirmant que l'application exécute des tests de diagnostic uniquement si vous avez coché la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure des journaux de diagnostic)**.

5. Cliquez sur **Close (Fermer)** pour confirmer que l'application a réussi à envoyer le rapport au service de journalisation Strata. Ce message de confirmation affiche la date et l'heure auxquelles le rapport a été traité et envoyé.



Déconnexion de l'application GlobalProtect pour macOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux MacOS uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si votre administrateur configure la méthode de connexion à GlobalProtect sur **Always On (Toujours active)**, vous pouvez déconnecter l'application GlobalProtect. Par exemple, vous pourriez vouloir déconnecter l'application si le Virtual Private Network (réseau privé virtuel - VPN) GlobalProtect ne fonctionne pas dans un hôtel, et l'échec du VPN vous empêche de vous connecter à Internet. Après avoir déconnecté l'application GlobalProtect, vous pouvez vous connecter à Internet en utilisant une communication non sécurisée (sans VPN).

La méthode, la durée et le nombre de déconnexions possibles de l'application GlobalProtect dépendent de la configuration du service GlobalProtect (PanGPS) par l'administrateur. Cette configuration peut vous empêcher de déconnecter complètement l'application ou vous permettre de déconnecter l'application uniquement après avoir répondu correctement à un défi.

Si votre configuration inclut un défi, l'application GlobalProtect demande l'un des éléments suivants :

- Raison pour laquelle vous souhaitez déconnecter l'application
- Répondez à une ou plusieurs raisons telles que **Internet speed slow (L'Internet est lent)** ou **App not working (L'application ne fonctionne pas)** (si nécessaire).
- Code secret
- Numéro de ticket

Si le défi implique un code secret ou un numéro de ticket, nous vous recommandons de contacter un administrateur GlobalProtect ou une personne du service d'assistance par téléphone.

Les administrateurs fournissent généralement des codes secrets à l'avance, soit par e-mail (pour les nouveaux utilisateurs de GlobalProtect), soit publiés sur le site Web de votre organisation. En réponse à une panne ou à un problème système, les administrateurs peuvent également fournir des codes secrets par téléphone.

Avant de pouvoir obtenir un numéro de ticket valide, votre terminal affiche un numéro de requête de ticket que vous devez communiquer à votre administrateur GlobalProtect ou à une personne du service d'assistance. Si votre requête de déconnexion est approuvée, vous recevrez un numéro de ticket valide que vous pouvez utiliser pour déconnecter GlobalProtect.

Les étapes suivantes décrivent comment déconnecter l'application et réussir un défi :

1. Déconnectez l'application GlobalProtect.
   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système GlobalProtect. Le panneau d'état s'ouvre.
   2. Cliquez sur le menu hamburger pour ouvrir le menu des paramètres.
   3. Sélectionnez **Disconnect (Déconnecter)**.

   *L'option **Disconnect (Déconnecter)** n'est visible que si la configuration de votre agent GlobalProtect vous permet de déconnecter l'application. Si la configuration vous permet de déconnecter l'application GlobalProtect sans exiger que vous répondiez à un défi, l'application GlobalProtect se ferme sans nécessiter d'action supplémentaire.*

2. Répondez à un ou plusieurs défis, si nécessaire.

Si vous y êtes invité, fournissez les informations suivantes :

- **Tell us the issue to disconnect (Indiquer le problème lors de la déconnexion)** : la raison pour laquelle vous souhaitez déconnecter l'application GlobalProtect.

- **Select the reason to disconnect (Sélectionner la raison de la déconnexion)** : si votre configuration nécessite que vous répondiez à une ou plusieurs raisons ou que vous saisissiez une autre raison, l'application GlobalProtect affiche les raisons dès que vous sélectionnez **Disconnect (Déconnecter)**.

- **Passcode (Code secret)** : un code secret fourni à l'avance par votre administrateur, en fonction d'un problème ou d'un événement connu qui vous oblige à déconnecter l'application.
- **Ticket** : si votre configuration nécessite que vous fournissiez un numéro de ticket, l'application GlobalProtect affiche un numéro de requête de ticket hexadécimal à huit caractères dès que vous sélectionnez **Disconnect (Déconnecter)**. Pour déconnecter l'application avec un numéro de ticket, contactez votre administrateur ou la personne du service d'assistance (par téléphone) et fournissez le numéro de requête de ticket. Après avoir approuvé votre requête, votre administrateur ou la personne du service d'assistance vous fournit un numéro de ticket hexadécimal à huit caractères. Entrez le numéro de ticket dans le champ **Ticket**, puis cliquez sur **OK**.

Désinstallation de l'application GlobalProtect pour macOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux MacOS uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Utilisez les étapes suivantes pour désinstaller l'application GlobalProtect de votre terminal macOS . Gardez à l'esprit qu'en désinstallant l'application, vous n'avez plus accès au VPN de votre réseau d'entreprise et votre terminal ne sera pas protégé par les politiques de sécurité de votre entreprise.

Seuls les utilisateurs ayant des privilèges d'administrateur peuvent désinstaller l'application GlobalProtect des terminaux macOS.

Sur les terminaux macOS, vous pouvez utiliser le programme d'installation macOS (dans ce cas, le programme d'installation GlobalProtect) pour désinstaller un programme. Pour désinstaller l'application GlobalProtect de votre terminal, installez le package logiciel GlobalProtect, puis lancez le programme d'installation GlobalProtect. Le programme d'installation GlobalProtect vous invite à sélectionner le package **Uninstall GlobalProtect (Désinstaller GlobalProtect)**. Si votre administrateur a activé les extensions système dans l'application GlobalProtect pour votre terminal macOS lors de l'installation de l'application GlobalProtect, l'application GlobalProtect vous demandera également de supprimer les extensions système lors de la désinstallation de GlobalProtect. Une fois le package **Uninstall GlobalProtect (Désinstaller GlobalProtect)** installé avec succès, l'application GlobalProtect est supprimée du terminal.

Si vous n'avez plus le programme d'installation GlobalProtect sur votre terminal macOS, vous pouvez désinstaller GlobalProtect en exécutant la commande suivante depuis la ligne de commande :

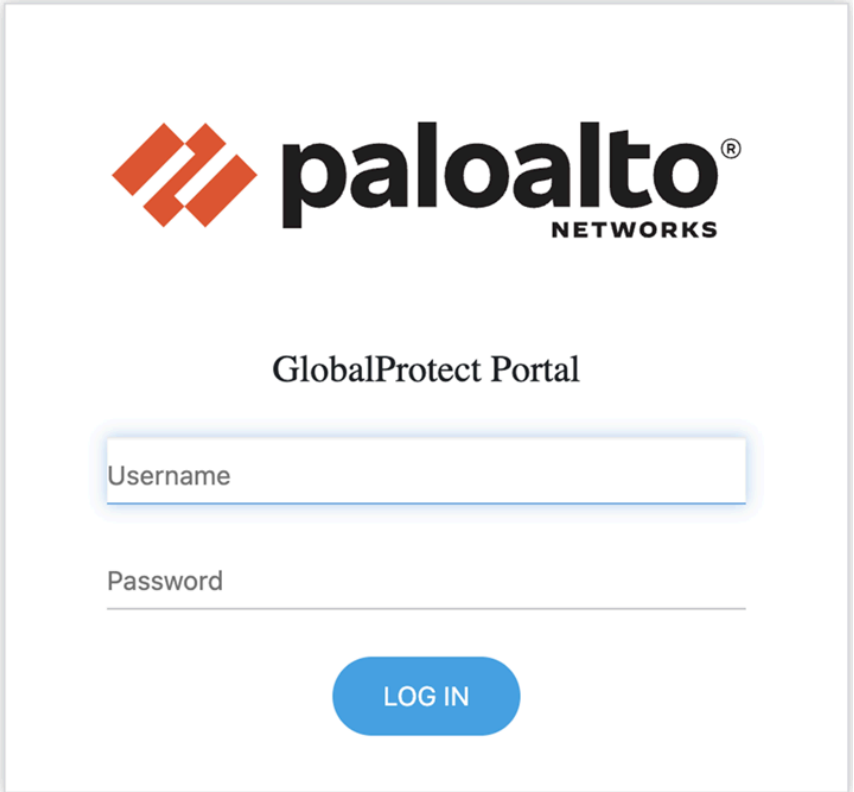
```
sudo /Applications/GlobalProtect.app/Contents/Resources/
uninstall_gp.sh
```

1. Connectez-vous au portail GlobalProtect.
   1. Lancez votre navigateur Web et accédez à l'URL suivante :

      https://<portal address or name>

      Exemple : **http://gp.acme.com**
   2. Sur la page de connexion au portail, saisissez vos **Name (Nom)** (nom d'utilisateur) et **Password (Mot de passe)**, puis cliquez sur **LOG IN (Connexion)**. Dans la plupart des cas,

vous pouvez utiliser le même nom d'utilisateur et le même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise.



2. Accédez à la page de téléchargement de l'application.

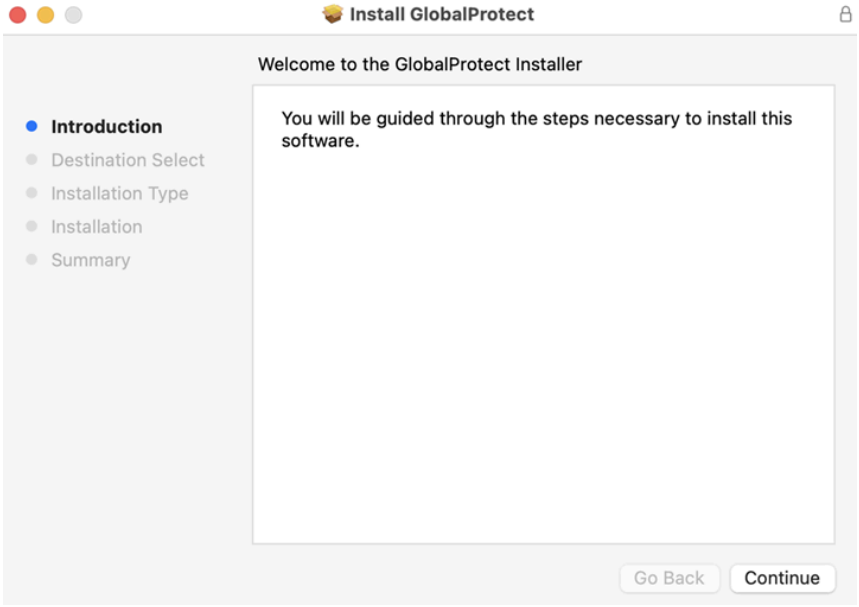
Dans la plupart des cas, la page de téléchargement de l'application apparaît immédiatement après que vous vous êtes connecté au portail.

*Si votre administrateur système a activé l'accès VPN sans client GlobalProtect, la page de l'application s'ouvre après votre connexion au portail (au lieu de la page de téléchargement de l'application). Sélectionnez **GlobalProtect Agent (Agent GlobalProtect)** pour ouvrir la page de téléchargement.*

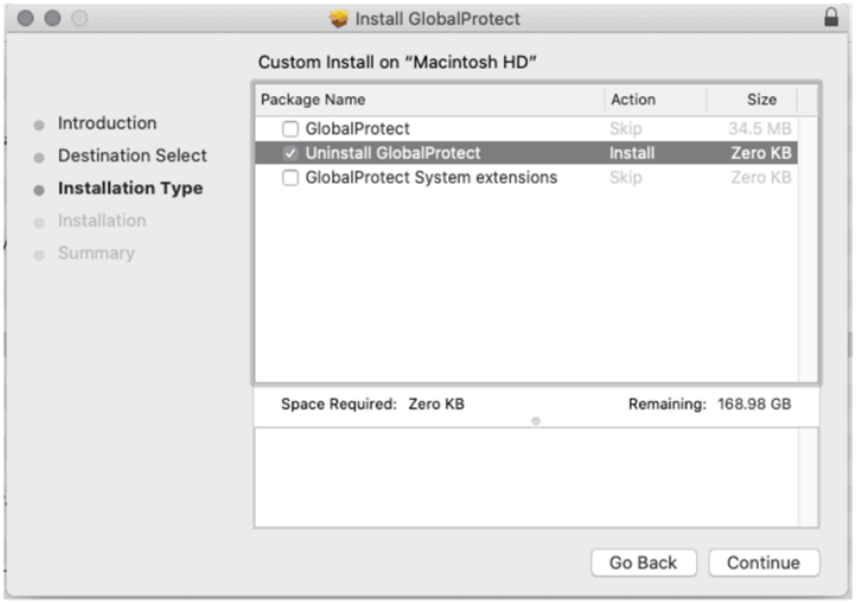
3. Téléchargez l'application.

1. Cliquez sur **Download Mac 32/64 bit GlobalProtect agent (Télécharger l'agent GlobalProtect pour Mac 32/64 bits)**.
2. Lorsque vous y êtes invité, **Run (Exécutez)** le logiciel.
3. Lorsque vous y êtes invité à nouveau, **Run (Exécutez)** le programme d'installation de GlobalProtect.

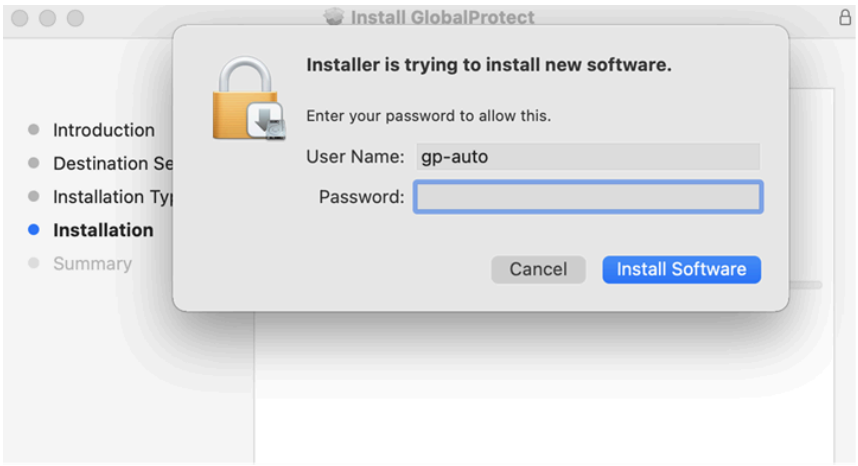
4. Désinstallez GlobalProtect.
   1. Depuis le programme d'installation GlobalProtect, cliquez sur **Continue (Continuer)**.



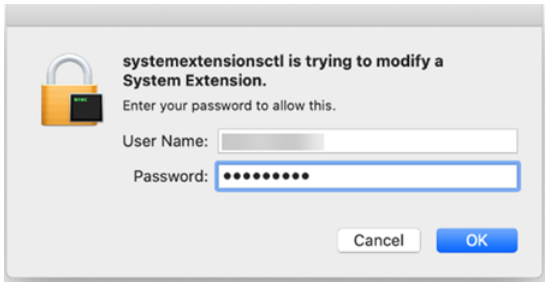
   2. Sur l'écran **Destination Select (Sélection de la destination)**, cliquez sur **Continue (Continuer)**.
   3. Sur l'écran **Installation Type (Type d'installation)**, cochez la case **Uninstall GlobalProtect (Désinstaller GlobalProtect)**, puis cliquez sur **Continue (Continuer)**.



   4. Cliquez sur **Install (Installer)** pour confirmer que vous souhaitez supprimer l'application GlobalProtect.
   5. Lorsque vous y êtes invité, saisissez votre **User Name (Nom d'utilisateur)** et votre **Password (Mot de passe)**, puis cliquez sur **Install Software (Installer le logiciel)** pour désinstaller GlobalProtect.

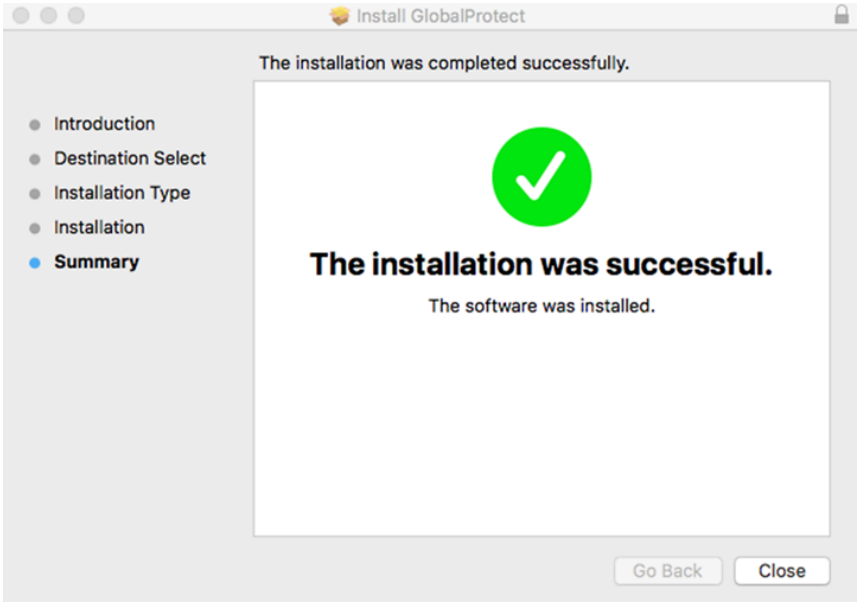


6. Si votre administrateur système a activé les extensions système macOS lors de l'installation de l'application GlobalProtect 5.1.4 sur macOS Catalina 10.15.4 ou version ultérieure, une invite contextuelle apparaît pour vous demander de désinstaller les extensions système. Lorsque vous y êtes invité, saisissez votre **User Name (Nom d'utilisateur)** et **Password (Mot de passe)**, puis cliquez sur **OK** pour supprimer les extensions système.



5. Confirmez que l'application GlobalProtect n'est plus installée.

Un message s'affiche, confirmant que le package **Uninstall GlobalProtect (Désinstaller GlobalProtect)** a été installé avec succès. Cette confirmation indique que l'application GlobalProtect a été supprimée de votre terminal.



Suppression de l'extension du noyau de l'exécutant GlobalProtect

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux MacOS uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Lorsque vous désinstallez l'application GlobalProtect pour macOS, puis installez une nouvelle instance de l'application, vous pouvez rencontrer des problèmes de connexion si l'extension de noyau de l'exécutant GlobalProtect n'est pas mise à jour correctement. Une extension de noyau (`kext`) est un plug-in pour le système d'exploitation macOS qui gère les applications. Si vous ne pouvez pas vous connecter à GlobalProtect après avoir installé une nouvelle instance de l'application, utilisez les procédures suivantes pour localiser et supprimer l'extension de noyau de l'exécutant GlobalProtect.

1. Désinstallez l'application GlobalProtect pour Mac.
2. Déterminez si l'extension de noyau de l'exécutant GlobalProtect existe sur le terminal.

   Sur le terminal macOS, ouvrez l'application **Terminal** dans le dossier **Applications** > **Utilities (Utilitaires)**, puis entrez la commande suivante :

   ```
   kextstat | grep gplock
   ```
3. Si l'extension existe, déchargez l'exécutant.

   Entrez la commande suivante dans l'application **Terminal** pour décharger l'exécutant :

   ```
   sudo kextunload -b com.paloaltonetworks.GlobalProtect.gplock
   ```
4. Empêchez l'exécutant de se recharger après un redémarrage.

   Entrez la commande suivante dans l'application **Terminal** pour supprimer l'exécutant du disque dur macOS :

   ```
   sudo rm -r "/System/Library/Extensions/gplock*.kext"
   ```
5. Téléchargez et installez l'application GlobalProtect pour Mac.

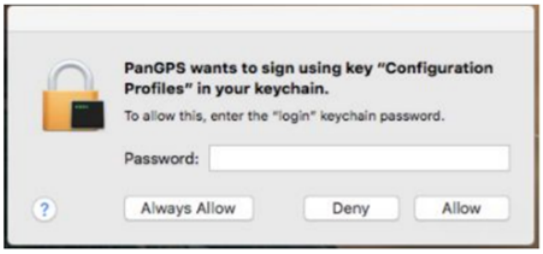
Activation de l'application GlobalProtect pour macOS afin d'utiliser des certificats clients pour l'authentification

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux MacOS uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Lorsque l'application GlobalProtect est installée sur des terminaux macOS pour la première fois et que l'authentification par certificat client est activée sur le portail ou la passerelle, une invite contextuelle de trousseau apparaît, invitant les utilisateurs à saisir leur mot de passe afin que GlobalProtect puisse accéder aux certificats clients du trousseau de connexion et les utiliser. L'invite contextuelle du trousseau peut également apparaître lorsqu'un nouveau certificat est installé, car le certificat précédent a expiré.

Vous devez suivre la procédure suivante pour activer l'application GlobalProtect pour macOS afin d'utiliser des certificats clients pour l'authentification :

1. Entrez votre mot de passe pour permettre l'accès au trousseau de connexion avec le terminal macOS dans l'invite contextuelle du trousseau suivante :



2. Sélectionnez **Always Allow (Autoriser toujours)** pour permettre à GlobalProtect d'établir le tunnel VPN. L'invite contextuelle du trousseau n'apparaît pas tant que le certificat client n'a pas expiré. Cette invite contextuelle peut réapparaître lorsque le certificat client est renouvelé.

   *Si vous sélectionnez **Allow (Autoriser)**, l'invite contextuelle du trousseau apparaît chaque fois que les utilisateurs se connectent à GlobalProtect. Si vous sélectionnez **Deny (Refuser)**, GlobalProtect ne peut pas établir de tunnel VPN et l'invite contextuelle du trousseau apparaît. GlobalProtect ne peut établir un tunnel VPN qu'après avoir autorisé l'accès au trousseau de connexion.*

Application GlobalProtect pour iOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux iOS uniquement	Version 6.1 ou ultérieure de l'application GlobalProtect

GlobalProtect™ est une application qui s'exécute sur votre terminal (ordinateur de bureau, ordinateur portable, tablette ou téléphone intelligent) pour vous protéger en utilisant les mêmes politiques de sécurité qui protègent les ressources sensibles de votre réseau d'entreprise. GlobalProtect™ sécurise votre intranet, votre cloud privé, votre cloud public et votre trafic Internet et vous permet d'accéder aux ressources de votre entreprise où que vous soyez dans le monde.

Téléchargement et installation de l'application GlobalProtect pour iOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux iOS uniquement	Version 6.1 ou ultérieure de l'application GlobalProtect

Avant de pouvoir connecter votre terminal iOS au réseau GlobalProtect, vous devez télécharger et installer l'application. Si votre terminal iOS est géré par un Mobile Device Management (gestion des appareils mobiles - MDM), votre administrateur a peut-être automatiquement installé l'application GlobalProtect vers votre terminal et configuré les paramètres VPN. Si vous n'avez pas déjà l'application GlobalProtect sur votre terminal iOS, vous pouvez la télécharger depuis l'App Store.

Avant de télécharger l'application, vous devez obtenir l'adresse IP ou le FQDN du portail GlobalProtect auprès de votre administrateur. De plus, votre administrateur doit vérifier quel nom d'utilisateur et quel mot de passe vous pouvez utiliser pour vous connecter au portail et aux passerelles. Il s'agit généralement du même nom d'utilisateur et du même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise. Si votre administrateur vous a autorisé à utiliser des informations biométriques (empreinte digitale ou, uniquement pour les périphériques macOS X, reconnaissance faciale) pour vous connecter, vous devez d'abord vous connecter avec un nom d'utilisateur et un mot de passe deux fois (une fois pour l'enregistrer et à nouveau pour vous authentifier). Vous pouvez ensuite utiliser des informations biométriques pour vous connecter.

Après avoir rassemblé les informations requises, vous pouvez télécharger et installer l'application comme suit :

1. Lancez l'App Store.
2. **Search (Recherchez)** **`GlobalProtect`**.
3. Dans les résultats de recherche, sélectionnez **GlobalProtect™**.
4. Depuis la page produit de l'application GlobalProtect, appuyez sur **GET (Obtenir)**.
5. **Install (Installez)** l'application.
6. Lorsque vous y êtes invité, **Sign In (Connectez-vous)** avec votre identifiant Apple-ID.

Utilisation de l'application GlobalProtect pour iOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux iOS uniquement	Version 6.1 ou ultérieure de l'application GlobalProtect

Ce sujet ne s'applique à vous que si votre configuration nécessite que vous saisissiez vos identifiants de connexion GlobalProtect après vous être connecté à votre terminal (l'authentification single sign-on est désactivée).

Nous recommandons généralement aux organisations de permettre à ses utilisateurs GlobalProtect de se connecter de manière transparente après l'installation de l'application. Après vous être connecté à un terminal avec une connexion GlobalProtect transparente, l'application GlobalProtect initie automatiquement et se connecte au réseau d'entreprise sans intervention supplémentaire de l'utilisateur.

Si votre configuration nécessite que vous saisissiez vos identifiants GlobalProtect, suivez les étapes applicables ci-dessous.

1. Connectez-vous au portail GlobalProtect ou à la passerelle.

   Utilisez l'un des flux de travail suivants pour vous connecter au portail GlobalProtect ou à la passerelle :

   - Expérience de première connexion :
     1. Lancez l'application GlobalProtect.
     2. (Facultatif) Si vous n'avez pas activé les notifications GlobalProtect sur votre terminal, une boîte de dialogue d'autorisation de notification apparaît. **Allow (Autorisez)** GlobalProtect à vous envoyer des notifications.

        Si vous **Don't Allow (N'autorisez pas)** GlobalProtect à vous envoyer des notifications, un rappel apparaît la prochaine fois que vous lancez l'application. Appuyez sur le lien **Settings -> GlobalProtect (Paramètres -> GlobalProtect)** pour accéder à l'écran d'autorisation de notification, où vous pouvez activer les notifications. Si vous ne souhaitez toujours pas activer les notifications, **Skip (Ignorez)** cet écran.

     3. Entrez l'adresse du portail GlobalProtect.

     4. (Facultatif) Selon le mode de connexion, appuyez sur **Connect (Connecter)** pour initier la connexion.
     5. Lorsque le message « `GlobalProtect » Would Like to AddVPN Configurations (« GlobalProtect » souhaite ajouter des`

`configurations VPN)` apparaît, utilisez les étapes suivantes pour ajouter des configurations VPN à votre terminal :

1. **Allow (Autorisez)** GlobalProtect à ajouter des configurations VPN à votre terminal. Ce paramètre permet à GlobalProtect de filtrer et de surveiller l'activité réseau sur le terminal lorsque vous utilisez le VPN.

2. Saisissez le code secret de votre iPhone ou iPad pour confirmer que vous souhaitez ajouter des configurations VPN à votre terminal.

6. (Facultatif) Si votre terminal est incapable de vérifier l'identité du portail GlobalProtect à l'aide du certificat du serveur du portail, le message `Cannot Verify Server Identity (Impossible de vérifier l'identité du serveur)` apparaît. Si vous faites confiance au certificat, appuyez sur **Continue (Continuer)** pour poursuivre la connexion.
7. (Facultatif) Si vous y êtes invité, entrez votre **Username (Nom d'utilisateur)** et votre **Password (Mot de passe)**, et cliquez sur **SIGN IN (Se connecter)**.

   Si votre administrateur vous a permis d'utiliser des informations biométriques (empreinte digitale ou, uniquement pour les périphériques iOS X, identification faciale) pour vous connecter, vous devez d'abord vous connecter avec un nom d'utilisateur et un mot de passe deux fois (une fois pour l'enregistrer et à nouveau pour vous authentifier). Vous pouvez ensuite utiliser des informations biométriques pour vous connecter.

8. (Facultatif) Si vous utilisez l'authentification multifacteur, entrez le **Code** de vérification GlobalProtect qui est envoyé à votre terminal après votre connexion, puis appuyez sur **Continue (Continuer)**.
9. (Facultatif) Si votre administrateur configure l'application GlobalProtect pour afficher un message de bienvenue, le message de bienvenue apparaît lors de la connexion réussie. Fermez le message de bienvenue pour accéder à l'écran d'accueil.

10. (Facultatif) S'il y a des notifications sur votre application, la boîte de dialogue Notifications apparaît lors de la connexion réussie. Fermez la boîte de dialogue Notifications pour passer à l'écran d'accueil.

11. Lorsque l'écran d'accueil apparaît, vérifiez que votre connexion a été établie avec succès. Si la connexion est réussie, l'écran d'accueil affiche l'état **CONNECTED (Connecté)**.

12. (Facultatif) Par défaut, le terminal se connecte automatiquement à la passerelle **Best Available (Meilleure disponible)** selon la configuration que l'administrateur définit et les temps de réponse des passerelles disponibles. Pour vous connecter à une autre passerelle, appuyez sur le menu déroulant de la passerelle en bas de l'écran d'accueil, puis utilisez l'une des options suivantes :

    - Sélectionnez une passerelle manuellement (passerelles externes uniquement). Si votre administrateur configure plus de 10 passerelles externes manuelles dans

la configuration de votre agent de portail, vous pouvez également localiser une passerelle spécifique en utilisant l'option de recherche de passerelle.

- Attribuez et connectez-vous automatiquement à une passerelle préférée en appuyant sur l'icône More Options (Plus d'options) ( ) pour la passerelle que vous souhaitez définir comme passerelle préférée, puis en appuyant sur **Set As Preferred (Définir comme préférée)**. Vous pouvez également appuyer longuement (appuyer et maintenir) sur la passerelle, puis sur **Set As Preferred (Définir comme préférée)**.

  Pour supprimer l'attribution de la passerelle préférée, appuyez sur l'icône More Options (Plus d'options) ( ) pour la passerelle préférée, puis sur **Remove Preferred (Supprimer la préférée)**. Vous pouvez également appuyer longuement (appuyer et maintenir) sur la passerelle, puis sur **Remove Preferred (Supprimer la préférée)**.

- Expérience de connexion à la demande (VPN d'accès à distance) :

  Lorsque l'administrateur GlobalProtect configure GlobalProtect avec la méthode de connexion **On-Demand (À la demande)**, vous devez lancer l'application GlobalProtect pour lancer la connexion manuellement. Après le lancement de la connexion, vous pouvez **TAP TO CONNECT (Appuyer pour se connecter)** pour établir la connexion à GlobalProtect. Si votre administrateur active GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, la connexion s'établit sans nécessiter d'interaction supplémentaire de l'utilisateur. Si votre administrateur n'active pas GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vous devez vous connecter pour établir la connexion.

- Expérience de connexion toujours active

  Lorsque votre administrateur GlobalProtect configure GlobalProtect avec la méthode de connexion **Always On (Toujours active)**, la connexion se lance automatiquement. Selon que votre administrateur configure l'application GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vous pouvez établir la connexion GlobalProtect sans lancer l'application. Si votre administrateur active GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, la connexion s'établit automatiquement sans nécessiter d'interaction de l'utilisateur. Si votre administrateur n'active pas GlobalProtect pour **Save User Credentials**

(Enregistrer les informations d'identification de l'utilisateur), vous devez vous connecter via l'application pour établir la connexion.

- (Facultatif) Si votre administrateur a configuré GlobalProtect avec la méthode de connexion **Always On (Toujours active)**, la connexion se lance automatiquement. L'écran d'accueil affiche l'état **CONNECTED (Connecté)**.

  Avec la méthode de connexion **Always On (Toujours active)**, l'écran d'accueil affiche l'état **CONNECTED (Connecté)** avec un message de déconnexion pour vous empêcher de vous déconnecter lorsque vous essayez d'appuyer sur l'icône **Connect (Connecter)**.

2. Affichez les informations sur votre connexion GlobalProtect.

Après avoir établi la connexion à GlobalProtect, lancez l'application GlobalProtect. Appuyez sur l'icône des paramètres pour ouvrir le menu des paramètres. Dans le menu des paramètres, appuyez sur **SETTINGS (Paramètres)** pour voir les informations sur votre connexion, y compris l'adresse du **Portal (Portail)** et le **Status (État)** de la connexion.

- Si vous souhaitez vous connecter à un autre portail GlobalProtect, appuyez sur l'adresse **Portal (Portail)**. Lorsque vous y êtes invité, entrez une nouvelle adresse de portail, puis appuyez sur **CONNECT (Connecter)**.
- Si vous êtes connecté à une passerelle externe, appuyez sur le **Status (État)** de la connexion pour voir des détails supplémentaires sur votre connexion (y compris le SSID du réseau et l'adresse IP/FQDN de la passerelle).

3. (Facultatif) Modifiez votre mot de passe enregistré.

Si votre administrateur GlobalProtect configure l'agent du portail GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vos informations d'identification sont automatiquement enregistrées dans l'application GlobalProtect. Lorsque votre mot de passe expire ou qu'un administrateur RADIUS ou AD exige un changement de mot de passe lors de la prochaine connexion, vous pouvez mettre à jour votre mot de passe dans l'application. Cette fonctionnalité est activée uniquement lorsque vous êtes authentifié avec un serveur RADIUS utilisant le protocole d'authentification extensible protégé Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).

1. Lancez l'application GlobalProtect.
2. Depuis l'écran d'accueil, **TAP TO CONNECT (Appuyez pour vous connecter)**.
3. (Facultatif) Si vous y êtes invité, entrez vos *anciens* **Username (Nom d'utilisateur)** et **Password (Mot de passe)**, et cliquez sur **SIGN IN (Se connecter)**.
4. Lorsque l'application GlobalProtect vous invite à `mettre à jour le mot de passe`, entrez votre **Current Password (Mot de passe actuel)** suivi de votre **New Password (Nouveau mot de passe)**.

5. **Retype Password (Retapez le mot de passe)** pour confirmer votre nouveau mot de passe.
6. **SIGN IN (Connectez-vous)** pour vous reconnecter à GlobalProtect avec votre nouveau mot de passe.

4. (Facultatif) Déconnectez-vous de GlobalProtect.

Si votre administrateur configure GlobalProtect avec la méthode de connexion **On-Demand (À la demande)**, vous pouvez **TAP TO DISCONNECT (Appuyer pour se déconnecter)** depuis l'écran d'accueil.

Signaler un problème depuis l'application GlobalProtect pour iOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux iOS uniquement	Version 6.1 ou ultérieure de l'application GlobalProtect

Si vous rencontrez un comportement inhabituel, tel qu'une mauvaise performance du réseau ou une impossibilité d'établir une connexion avec le portail et la passerelle, vous pouvez signaler le problème directement au service de journalisation Strata auquel votre administrateur peut accéder. Vous n'avez plus besoin de collecter manuellement et d'envoyer les journaux de l'application GlobalProtect par e-mail ou de les stocker sur un lecteur cloud.

*Pour afficher l'option **Report an Issue (Signaler un problème)** sur l'application GlobalProtect, votre administrateur doit activer la collecte des journaux de l'application GlobalProtect pour le dépannage sur le portail GlobalProtect.*

1. Connectez-vous au portail GlobalProtect ou à la passerelle.
   1. Lancez l'application GlobalProtect.
   2. Entrez l'adresse du portail GlobalProtect.
   3. (Facultatif) Selon le mode de connexion, appuyez sur **Connect (Connecter)** pour initier la connexion.
   4. **Allow (Autorisez)** GlobalProtect à ajouter des configurations VPN à votre terminal. Ce paramètre permet à GlobalProtect de filtrer et de surveiller l'activité réseau sur le terminal lorsque vous utilisez le VPN.
   5. Saisissez le code secret de votre iPhone ou iPad pour confirmer que vous souhaitez ajouter des configurations VPN à votre terminal.
   6. (Facultatif) Si vous y êtes invité, entrez votre **Username (Nom d'utilisateur)** et votre **Password (Mot de passe)**, et cliquez sur **SIGN IN (Se connecter)**.
   7. Lorsque l'écran d'accueil apparaît, vérifiez que votre connexion a été établie avec succès. Si la connexion est réussie, l'écran d'accueil affiche l'état **CONNECTED (Connecté)**.
   8. (Facultatif) Par défaut, le terminal se connecte automatiquement à la meilleure passerelle disponible selon la configuration que l'administrateur définit et les temps de réponse des passerelles disponibles. Pour vous connecter à une passerelle différente, appuyez sur le menu déroulant de la passerelle en bas de l'écran d'accueil, puis sélectionnez une passerelle dans la liste (passerelles externes uniquement).
2. Affichez les informations sur votre connexion GlobalProtect.

   Après avoir établi la connexion à GlobalProtect, lancez l'application GlobalProtect. Appuyez sur l'icône des paramètres pour ouvrir le menu des paramètres. Dans le menu des paramètres, appuyez sur **SETTINGS (Paramètres)** pour voir les informations sur votre connexion, y compris l'adresse du **Portal (Portail)** et le **Status (État)** de la connexion.

3. Signalez un problème à partir de l'application GlobalProtect à partir du terminal de l'utilisateur final.

Après avoir lancé l'application, appuyez sur **HELP (Aide)** pour signaler un problème depuis votre terminal.

1. Appuyez sur **Report an Issue (Signaler un problème)**.

2. Activez l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic. Les journaux de diagnostic et de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact.

   Une fois les tests de diagnostic terminés avec succès, les fichiers journaux de débogage GlobalProtect sont téléchargés vers le service de journalisation Strata depuis votre terminal.

   *Si vous n'activez pas l'application pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, seuls les journaux de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact. L'application GlobalProtect vérifie les fichiers de rapport (pan_gp.trb.log ou pan_gp_trbl.log) qui sont générés automatiquement au format `.json`. Un message de notification apparaît si aucun problème n'a été trouvé dans les journaux de dépannage. Cliquez sur **Retry (Réessayer)** pour vérifier si les fichiers pan_gp.trb*.log existent.*
3. Cochez la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure les journaux de diagnostic)**.
4. Appuyez sur **CONTINUE (Continuer)** pour permettre à l'application de créer un journal de dépannage et d'envoyer le rapport à l'instance du service de journalisation Strata de votre administrateur.

   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log.

   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log. L'application GlobalProtect peut exécuter des tests de diagnostic avec ou sans tunnel.

Par exemple, vous voudrez peut-être entrer vos identifiants de connexion GlobalProtect avant que l'application ne se connecte et n'exécute des tests de diagnostic via le tunnel.

Un message s'affiche, confirmant que l'application exécute des tests de diagnostic uniquement si vous avez coché la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure des journaux de diagnostic)**.

Un message s'affiche, confirmant que l'application envoie le rapport au service de journalisation Strata.

5. Appuyez sur **DONE (Terminé)** pour confirmer que l'application a bien envoyé le rapport au service de journalisation Strata.

Installation de l’application GlobalProtect pour iOS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux iOS uniquement	Version 6.1 ou ultérieure de l’application GlobalProtect

Utilisez les étapes suivantes pour désinstaller l’application GlobalProtect de votre terminal iOS . Gardez à l’esprit qu’en désinstallant l’application, vous n’avez plus accès au VPN de votre réseau d’entreprise et que votre terminal ne sera pas protégé par les politiques de sécurité de votre entreprise.

1. Appuyez longuement sur l’icône de l’application GlobalProtect jusqu’à ce que l’icône tremble.
2. Appuyez sur le **X** dans le coin supérieur gauche de l’icône.
3. Lorsque vous y êtes invité, **Delete (Supprimez)** GlobalProtect.
4. Appuyez sur **Done (Terminé)** ou appuyez sur le bouton d’accueil pour revenir à l’écran d’accueil.

Application GlobalProtect pour Android

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Android uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

GlobalProtect™ est une application qui s'exécute sur votre terminal (ordinateur de bureau, ordinateur portable, tablette ou téléphone intelligent) pour vous protéger en utilisant les mêmes politiques de sécurité qui protègent les ressources sensibles de votre réseau d'entreprise. GlobalProtect™ sécurise votre intranet, votre cloud privé, votre cloud public et votre trafic Internet et vous permet d'accéder aux ressources de votre entreprise où que vous soyez dans le monde.

Les rubriques suivantes décrivent comment installer et utiliser l'appli GlobalProtect pour Android :

- Téléchargement et installation de l'application GlobalProtect pour Android
- Téléchargement et installation de l'application GlobalProtect pour Android sur Chromebooks
- Utilisation de l'application GlobalProtect pour Android
- Signaler un problème depuis l'application GlobalProtect pour Android
- Déconnexion de l'application GlobalProtect pour Android
- Désinstallation de l'application GlobalProtect pour Android
- Désinstallation de l'application GlobalProtect pour Android depuis des Chromebooks

Téléchargement et installation de l'application GlobalProtect pour Android

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Android uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Avant de pouvoir connecter votre terminal Android au réseau GlobalProtect, vous devez télécharger et installer l'application. Si votre terminal Android est géré par un Mobile Device Management (gestion des appareils mobiles - MDM), votre administrateur a peut-être automatiquement installé l'application GlobalProtect sur votre terminal et configuré les paramètres VPN. Si vous n'avez pas déjà l'application GlobalProtect sur votre terminal Android, vous pouvez la télécharger depuis Google Play.

Avant de télécharger l'application, vous devez obtenir l'adresse IP ou le FQDN du portail GlobalProtect auprès de votre administrateur. De plus, votre administrateur doit vérifier quel nom d'utilisateur et quel mot de passe vous pouvez utiliser pour vous connecter au portail et aux passerelles. Il s'agit généralement du même nom d'utilisateur et du même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise.

Après avoir rassemblé les informations requises, vous pouvez télécharger et installer l'application comme suit :

1. Lancez Google Play.
2. **Search (Recherchez)** **`GlobalProtect`**.
3. Dans les résultats de recherche, sélectionnez **GlobalProtect**.
4. Depuis la page produit de l'application GlobalProtect, appuyez sur **Install (Installer)**.
5. Lorsque vous y êtes invité, examinez et **Accept (Acceptez)** les informations pour lesquelles GlobalProtect a besoin d'accès.

Téléchargement et installation de l'application GlobalProtect pour Android sur Chromebooks

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Android (Chromebooks) uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Pour utiliser l'application GlobalProtect pour Android sur un Chromebook, vous devez télécharger et installer l'application. Si votre Chromebook est géré par Workspace ONE ou la console d'administration Google, votre administrateur a peut-être automatiquement installé l'application GlobalProtect sur votre terminal et configuré les paramètres VPN. Si vous n'avez pas déjà l'application GlobalProtect pour Android sur votre Chromebook, vous pouvez la télécharger depuis le Google Play Store.

Avant de télécharger l'application, vous devez obtenir l'adresse IP ou le FQDN du portail GlobalProtect auprès de votre administrateur. De plus, votre administrateur doit vérifier quel nom d'utilisateur et quel mot de passe vous pouvez utiliser pour vous connecter au portail et aux passerelles. Il s'agit généralement du même nom d'utilisateur et du même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise.

Après avoir rassemblé les informations requises, vous pouvez télécharger et installer l'application comme suit :

L'application GlobalProtect pour Android n'est prise en charge que sur certains Chromebook. Si vous utilisiez la version 4.1.x de l'application GlobalProtect pour Chrome OS, l'application n'est plus disponible. Envisagez de passer à un système Chrome OS qui prend en charge les applications Android et d'utiliser l'application GlobalProtect pour Android.

1. Activez l'application Google Play Store sur votre Chromebook.
   1. (Facultatif) Si votre Chromebook exécute la version 52 ou antérieure de Chrome OS, mettez à jour le système d'exploitation de votre Chromebook.
   2. Depuis votre Chromebook, cliquez sur votre photo de compte dans le coin inférieur droit de l'écran.
   3. Sélectionnez **Settings (Paramètres)**.
   4. Dans la zone Google Play Store, **Enable Google Play Store on your Chromebook (Activez Google Play Store sur votre Chromebook)**.

      Si cette option n'est pas disponible, votre Chromebook ne prend pas en charge les applications Android.
   5. Lorsque vous y êtes invité, cliquez sur **Get Started (Démarrer)** pour lancer le Google Play Store.
   6. **Agree (Acceptez)** les conditions d'utilisation.
   7. Sur la page d'accueil, **SIGN IN (Connectez-vous)** au Google Play Store.
   8. **Accept (Acceptez)** les conditions d'utilisation de Google Play.

2. Téléchargez et installez l'application GlobalProtect pour les terminaux Android sur votre Chromebook.
   1. Ouvrez l'application Google Play Store.
   2. Recherchez **`GlobalProtect App (Application GlobalProtect)`**.
   3. Cliquez sur l'icône de l'application GlobalProtect.
   4. Cliquez sur **INSTALL (Installer)**, puis suivez les instructions à l'écran pour terminer l'installation de l'application.

Utilisation de l'application GlobalProtect pour Android

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Android uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Ce sujet ne s'applique à vous que si votre configuration nécessite que vous saisissiez vos identifiants de connexion GlobalProtect après vous être connecté à votre terminal (l'authentification single sign-on est désactivée).

Nous recommandons généralement aux organisations de permettre à ses utilisateurs GlobalProtect de se connecter de manière transparente après l'installation de l'application. Après vous être connecté à un terminal avec une connexion GlobalProtect transparente, l'application GlobalProtect initie automatiquement et se connecte au réseau d'entreprise sans intervention supplémentaire de l'utilisateur.

Si votre configuration nécessite que vous saisissiez vos identifiants GlobalProtect, suivez les étapes applicables ci-dessous.

1. Connectez-vous au portail GlobalProtect ou à la passerelle.

   Utilisez l'un des flux de travail suivants pour vous connecter au portail GlobalProtect ou à la passerelle :

   - Expérience de première connexion :
     1. Lancez l'application GlobalProtect.
     2. Entrez l'adresse du portail GlobalProtect.
     3. (Facultatif) Selon le mode de connexion, appuyez sur **Connect (Connecter)** pour initier la connexion.
     4. (Facultatif) Si votre terminal est incapable de vérifier l'identité du portail GlobalProtect à l'aide du certificat du serveur du portail, le message `Cannot Verify Server Identity (Impossible de vérifier l'identité du serveur)` apparaît. Si vous faites confiance au certificat, appuyez sur **Continue (Continuer)** pour poursuivre 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 (Se connecter)**.

        Si votre administrateur vous a permis d'utiliser des informations biométriques (empreinte digitale) pour vous connecter, vous devez d'abord vous connecter avec un

nom d'utilisateur et un mot de passe. Vous pouvez ensuite utiliser des informations biométriques pour vous connecter.

6. Lorsque le message `Connection request (Requête de connexion)` apparaît, appuyez sur **OK** pour permettre à GlobalProtect de configurer une connexion VPN sur votre terminal.

7. (Facultatif) Si vous utilisez l'authentification multifacteur, entrez le **Code** de vérification GlobalProtect qui est envoyé à votre terminal après votre connexion, puis appuyez sur **Continue (Continuer)**.
8. (Facultatif) Si votre administrateur configure l'application GlobalProtect pour afficher un message de bienvenue, le message de bienvenue apparaît lors de la connexion réussie. Appuyez en dehors du message de bienvenue pour passer à l'écran d'accueil.

9. (Facultatif) S'il y a des notifications sur votre application, la boîte de dialogue Notifications apparaît lors de la connexion réussie. Fermez la boîte de dialogue Notifications pour passer à l'écran d'accueil.

10. Lorsque l'écran d'accueil apparaît, vérifiez que votre connexion a été établie avec succès. Si la connexion est réussie, l'écran d'accueil affiche l'état **CONNECTED (Connecté)**.

11. (Facultatif) Si votre administrateur a configuré GlobalProtect avec la méthode de connexion **Always On (Toujours active)**, la connexion se lance automatiquement. L'écran d'accueil affiche l'état **CONNECTED (Connecté)**.

    Avec la méthode de connexion **Always On (Toujours active)**, l'écran d'accueil affiche l'état **CONNECTED (Connecté)** avec un message de déconnexion pour vous empêcher de vous déconnecter lorsque vous essayez d'appuyer sur l'icône **Connect (Connecter)**.

12. (Facultatif) Par défaut, le terminal se connecte automatiquement à la passerelle **Best Available (Meilleure disponible)** selon la configuration que l'administrateur définit et les temps de réponse des passerelles disponibles. Pour vous connecter à une passerelle différente, appuyez sur le menu déroulant de la passerelle en bas de l'écran d'accueil, puis sélectionnez une passerelle dans la liste (passerelles externes uniquement).

- Expérience de connexion à la demande (VPN d'accès à distance) :

  Lorsque votre administrateur GlobalProtect configure GlobalProtect avec la méthode de connexion **On-Demand (À la demande)**, vous devez lancer l'application GlobalProtect pour lancer la connexion manuellement. Après le lancement de la connexion, vous pouvez **TAP TO CONNECT (Appuyer pour se connecter)** pour établir la connexion à GlobalProtect. Si votre administrateur active GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, la connexion s'établit sans nécessiter d'interaction supplémentaire de l'utilisateur. Si votre administrateur n'active pas

GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vous devez vous connecter pour établir la connexion.

- Expérience de connexion toujours active :

  Lorsque votre administrateur GlobalProtect configure GlobalProtect avec la méthode de connexion **Always On (Toujours active)**, la connexion se lance automatiquement. Selon que votre administrateur configure l'application GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vous pouvez établir la connexion GlobalProtect sans lancer l'application. Si votre administrateur active GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, la connexion s'établit automatiquement sans nécessiter d'interaction de l'utilisateur. Si votre administrateur n'active pas GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vous devez vous connecter via l'application pour établir la connexion.

2. Affichez les informations sur votre connexion GlobalProtect.

Après avoir établi la connexion à GlobalProtect, lancez l'application GlobalProtect. Appuyez sur l'icône des paramètres pour ouvrir le menu des paramètres. Dans le menu des paramètres, appuyez sur **SETTINGS (Paramètres)** pour voir les informations sur votre connexion, y compris l'adresse du **Portal (Portail)** et le **Status (État)** de la connexion.

- Si vous souhaitez vous connecter à un autre portail GlobalProtect, appuyez sur l'adresse **Portal (Portail)**. Lorsque vous y êtes invité, entrez une nouvelle adresse de portail, puis appuyez sur **CONNECT (Connecter)**.

- Si vous êtes connecté à une passerelle externe, appuyez sur le **Status (État)** de la connexion pour voir des détails supplémentaires sur votre connexion (y compris le SSID du réseau et l'adresse IP/FQDN de la passerelle).

3. (Facultatif) Modifiez votre mot de passe enregistré.

Si votre administrateur GlobalProtect configure l'agent du portail GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vos informations d'identification sont automatiquement enregistrées dans l'application GlobalProtect. Lorsque votre mot de passe expire ou qu'un administrateur RADIUS ou AD exige un changement de mot de passe lors de la prochaine connexion, vous pouvez mettre à jour votre mot de passe dans l'application. Cette fonctionnalité est activée uniquement lorsque vous êtes authentifié avec un serveur RADIUS utilisant le protocole d'authentification extensible protégé Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MSCHAPv2).

1. Lancez l'application GlobalProtect.
2. Depuis l'écran d'accueil, **TAP TO CONNECT (Appuyez pour vous connecter)**.

3. (Facultatif) Si vous y êtes invité, entrez vos *anciens* **Username (Nom d'utilisateur)** et **Password (Mot de passe)**, et cliquez sur **SIGN IN (Se connecter)**.
4. Lorsque l'application GlobalProtect vous invite à `mettre à jour le mot de passe`, entrez votre **Current Password (Mot de passe actuel)** suivi de votre **New Password (Nouveau mot de passe)**.
5. **Retype Password (Retapez le mot de passe)** pour confirmer votre nouveau mot de passe.
6. **SIGN IN (Connectez-vous)** pour vous reconnecter à GlobalProtect avec votre nouveau mot de passe.

4. (Facultatif) Déconnectez-vous de GlobalProtect.

Si votre administrateur configure GlobalProtect avec la méthode de connexion **On-Demand (À la demande)**, vous pouvez **TAP TO DISCONNECT (Appuyer pour se déconnecter)** depuis l'écran d'accueil.

Signaler un problème depuis l'application GlobalProtect pour Android

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Android uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si vous rencontrez un comportement inhabituel, tel qu'une mauvaise performance du réseau ou une impossibilité d'établir une connexion avec le portail et la passerelle, vous pouvez signaler le problème directement au service de journalisation Strata auquel votre administrateur peut accéder. Vous n'avez plus besoin de collecter manuellement et d'envoyer les journaux de l'application GlobalProtect par e-mail ou de les stocker sur un lecteur cloud.

*Pour afficher l'option **Report an Issue (Signaler un problème)** sur l'application GlobalProtect, votre administrateur doit activer la collecte des journaux de l'application GlobalProtect pour le dépannage sur le portail GlobalProtect.*

1. Connectez-vous au portail GlobalProtect ou à la passerelle.
   1. Lancez l'application GlobalProtect.
   2. Entrez l'adresse du portail GlobalProtect.
   3. (Facultatif) Selon le mode de connexion, appuyez sur **Connect (Connecter)** pour initier la connexion.
   4. (Facultatif) Si vous y êtes invité, entrez votre **Username (Nom d'utilisateur)** et votre **Password (Mot de passe)**, et cliquez sur **SIGN IN (Se connecter)**.
   5. Lorsque le message **Connection request (Requête de connexion)** apparaît, appuyez sur **OK** pour permettre à GlobalProtect de configurer une connexion VPN sur votre terminal.
   6. Lorsque l'écran d'accueil apparaît, vérifiez que votre connexion a été établie avec succès. Si la connexion est réussie, l'écran d'accueil affiche l'état **CONNECTED (Connecté)**.
   7. (Facultatif) Par défaut, le terminal se connecte automatiquement à la meilleure passerelle disponible selon la configuration que l'administrateur définit et les temps de réponse des passerelles disponibles. Pour vous connecter à une passerelle différente, appuyez sur le menu déroulant de la passerelle en bas de l'écran d'accueil, puis sélectionnez une passerelle dans la liste (passerelles externes uniquement).
2. Affichez les informations sur votre connexion GlobalProtect.

   Après avoir établi la connexion à GlobalProtect, lancez l'application GlobalProtect. Appuyez sur l'icône des paramètres pour ouvrir le menu des paramètres. Dans le menu des paramètres, appuyez sur **SETTINGS (Paramètres)** pour voir les informations sur votre connexion, y compris l'adresse du **Portal (Portail)** et le **Connection Status (État de la connexion)**.

3. Signalez un problème à partir de l'application GlobalProtect à partir du terminal de l'utilisateur final.

Après avoir lancé l'application, appuyez sur **HELP (Aide)** pour signaler un problème depuis votre terminal.

1. Appuyez sur **Report an Issue (Signaler un problème)**.

2. Activez l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic. Les journaux de diagnostic et de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact.

   Une fois les tests de diagnostic terminés avec succès, les fichiers journaux de débogage GlobalProtect sont téléchargés vers le service de journalisation Strata depuis votre terminal.

   *Si vous n'activez pas l'application pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, seuls les journaux de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact. L'application GlobalProtect vérifie les fichiers de rapport (pan_gp.trb.log ou pan_gp_trbl.log) qui sont générés automatiquement au format `.json`. Un message de notification apparaît si aucun problème n'a été trouvé dans les journaux de dépannage. Cliquez sur **Retry (Réessayer)** pour vérifier si les fichiers pan_gp.trb*.log existent.*

3. Cochez la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure les journaux de diagnostic)**.
4. Appuyez sur **CONTINUE (Continuer)** pour permettre à l'application de créer un journal de dépannage et d'envoyer le rapport à l'instance du service de journalisation Strata de votre administrateur.

   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log.

   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log. L'application GlobalProtect peut exécuter des tests de diagnostic avec ou sans tunnel.

Par exemple, vous voudrez peut-être entrer vos identifiants de connexion GlobalProtect avant que l'application ne se connecte et n'exécute des tests de diagnostic via le tunnel.

Un message s'affiche, confirmant que l'application exécute des tests de diagnostic uniquement si vous avez coché la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure des journaux de diagnostic)**.

Un message s'affiche, confirmant que l'application envoie le rapport au service de journalisation Strata.

5. Appuyez sur **DONE (Terminé)** pour confirmer que l'application a bien envoyé le rapport au service de journalisation Strata.

Déconnexion de l'application GlobalProtect pour Android

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Android uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si votre administrateur configure la méthode de connexion à GlobalProtect sur **Always On (Toujours active)**, vous pouvez déconnecter l'application GlobalProtect. Par exemple, vous pourriez vouloir déconnecter l'application si le Virtual Private Network (réseau privé virtuel - VPN) GlobalProtect ne fonctionne pas dans un hôtel, et l'échec du VPN vous empêche de vous connecter à Internet. Après avoir déconnecté l'application GlobalProtect, vous pouvez vous connecter à Internet en utilisant une communication non sécurisée (sans VPN).

La méthode, la durée et le nombre de déconnexions possibles de l'application GlobalProtect dépendent de la configuration du service GlobalProtect (PanGPS) par l'administrateur. Cette configuration peut vous empêcher de déconnecter complètement l'application ou vous permettre de déconnecter l'application uniquement après avoir répondu correctement à un défi.

Si votre configuration inclut un défi, l'application GlobalProtect demande l'un des éléments suivants :

- Raison pour laquelle vous souhaitez déconnecter l'application
- Code secret

Si le défi implique un code secret, nous vous recommandons de contacter un administrateur GlobalProtect ou une personne du service d'assistance par téléphone. Les administrateurs fournissent généralement des codes secrets à l'avance, soit par e-mail (pour les nouveaux utilisateurs de GlobalProtect), soit publiés sur le site Web de votre organisation. En réponse à une panne ou à un problème système, les administrateurs peuvent également fournir des codes secrets par téléphone.

Les étapes suivantes décrivent comment déconnecter l'application et réussir un défi :

1. Déconnectez l'application GlobalProtect.
   1. Lancez l'application GlobalProtect.
   2. Appuyez sur l'icône des paramètres pour ouvrir le menu des paramètres.
   3. Dans le menu des paramètres, appuyez sur **DISCONNECT (Déconnecter)**.

   *L'option **Disconnect (Déconnecter)** n'est visible que si la configuration de votre agent GlobalProtect vous permet de déconnecter l'application. Si la configuration vous permet de déconnecter l'application GlobalProtect sans exiger que vous répondiez à un défi, l'application GlobalProtect se ferme sans nécessiter d'action supplémentaire.*

2. Répondez à un ou plusieurs défis, si nécessaire.

Si vous y êtes invité, fournissez les informations suivantes :

- **Reason (Raison)** : votre raison pour déconnecter l'application GlobalProtect.

- **Passcode (Code secret)** : un code secret fourni à l'avance par votre administrateur, en fonction d'un problème ou d'un événement connu qui vous oblige à déconnecter l'application.

Désinstallation de l’application GlobalProtect pour Android

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Android uniquement	Version 6.3 ou ultérieure de l’application GlobalProtect

Utilisez les étapes suivantes pour désinstaller l’application GlobalProtect de votre terminal Android. Gardez à l’esprit qu’en désinstallant l’application, vous n’avez plus accès au VPN de votre réseau d’entreprise et que votre terminal ne sera pas protégé par les politiques de sécurité de votre entreprise.

1. Lancez l’application Settings (Paramètres).
2. Appuyez sur **Apps & notifications (Applications et notifications)**.
3. Appuyez sur **GlobalProtect**.
4. Appuyez sur **Uninstall (Désinstaller)**.

Désinstallation de l'application GlobalProtect pour Android depuis des Chromebooks

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Android (Chromebooks) uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Utilisez les étapes suivantes pour désinstaller l'application GlobalProtect pour Android de votre Chromebook . Gardez à l'esprit qu'en désinstallant l'application, vous n'avez plus accès au VPN de votre réseau d'entreprise et que votre terminal ne sera pas protégé par les politiques de sécurité de votre entreprise.

1. Ouvrez l'application Google Play Store.
2. Cliquez sur le bouton de menu () à côté de la barre de recherche Google Play.
3. Sélectionnez **Apps & games (Applications et jeux)** > **My apps & games (Mes applications et jeux)**.
4. Sélectionnez **INSTALLED (Installé)**.
5. Dans la zone On this device (Sur ce périphérique), sélectionnez **GlobalProtect**.
6. Cliquez sur **UNINSTALL (Désinstaller)**.

Application GlobalProtect pour Linux

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Linux uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

GlobalProtect™ est un programme qui s'exécute sur votre terminal (ordinateur de bureau, ordinateur portable ou serveur) pour vous protéger en utilisant les mêmes politiques de sécurité qui protègent les ressources sensibles de votre réseau d'entreprise. GlobalProtect™ sécurise votre intranet, votre cloud privé, votre cloud public et votre trafic Internet et vous permet d'accéder aux ressources de votre entreprise où que vous soyez dans le monde.

Les sections suivantes fournissent des instructions pour installer et utiliser l'application GlobalProtect pour Linux :

- Téléchargement et installation de l'application GlobalProtect pour Linux
- Installation de l'application GlobalProtect pour Linux
- Signaler un problème depuis l'application GlobalProtect pour Linux
- Désactivation de l'application GlobalProtect pour Linux
- Désinstallation de l'application GlobalProtect pour Linux

Téléchargement et installation de l'application GlobalProtect pour Linux

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Linux uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

GlobalProtect vous propose deux méthodes différentes pour installer l'application GlobalProtect sur votre périphérique Linux : une version d'installation basée sur une interface graphique et une version CLI. Si vous utilisez un système d'exploitation Linux pris en charge qui prend en charge une interface graphique, vous pouvez installer la version GUI de GlobalProtect. Sinon, téléchargez et installez la version CLI de l'application GlobalProtect.

- Téléchargement et installation de la version GUI de GlobalProtect pour Linux
- Téléchargement et installation de la version CLI de GlobalProtect pour Linux

Téléchargement et installation de la version GUI de GlobalProtect pour Linux

Si votre périphérique Linux prend en charge une interface utilisateur graphique, suivez ces étapes pour installer la version GUI de GlobalProtect pour Linux.

1. Téléchargez l'application GlobalProtect pour Linux.
   1. Ouvrez une session dans le portail de support client. Après avoir saisi votre nom d'utilisateur et votre mot de passe, vous êtes authentifié et connecté au site d'assistance.
   2. Sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**.
   3. Filtrez par agent GlobalProtect pour Linux et téléchargez le fichier TGZ associé.
   4. Extrayez les fichiers du package.

```
user@linuxhost:~$ tar -xvf ~/pkgs/PanGPLinux-6.0.0.tgz
 ./ ./GlobalProtect_deb-6.0.0.0-62.deb ./
GlobalProtect_deb_arm-6.0.0.0-62.deb ./
GlobalProtect_rpm-6.0.0.0-62.rpm ./
GlobalProtect_rpm_arm-6.0.0.0-62.rpm ./
GlobalProtect_tar-6.0.0.0-62.tgz ./
GlobalProtect_tar_arm-6.0.0.0-62.tgz ./
GlobalProtect_UI_deb-6.0.0.0-62.deb ./
GlobalProtect_UI_rpm-6.0.0.0-62.rpm /
GlobalProtect_UI_tar-6.0.0.0-62.tgz ./manifest ./relinfo ./
gp_install.sh ./gp_uninstall.sh
```

   Vous verrez plusieurs packages d'installation pour les versions de systèmes d'exploitation prises en charge : DEB pour Debian et Ubuntu et RPM pour CentOS et Red Hat. Le package pour la version GUI est désigné par un préfixe GlobalProtect_UI.

2. (Facultatif) Si votre terminal Linux doit utiliser une configuration de serveur proxy manuelle, configurez les paramètres du proxy.

   L'application GlobalProtect pour Linux ne prend en charge qu'une configuration de serveur proxy de base, mais ne prend pas en charge l'utilisation de fichiers de configuration automatique de proxy (PAC) et l'authentification proxy.

   L'application GlobalProtect pour Linux obtient les paramètres du proxy à partir des variables d'environnement `HTTP_PROXY`, `HTTPS_PROXY` et `NO_PROXY` dans le fichier `/etc/environment`. Si vous modifiez ultérieurement la configuration du proxy système, vérifiez que le terminal à partir duquel GlobalProtect s'exécute utilise les variables d'environnement du proxy. Si vous ne voyez pas les nouveaux paramètres, déconnectez-vous et reconnectez-vous pour que les nouveaux paramètres prennent effet.

   Si vous avez configuré la variable HTTP_PROXY ou la variable HTTPS_PROXY, assurez-vous que le portail GlobalProtect correspond aux paramètres configurés pour la variable NO_PROXY.

   1. Pour définir votre proxy sur votre terminal Linux, modifiez la variable d'environnement `HTTP_PROXY` ou la variable d'environnement `HTTPS_PROXY` (par exemple, `HTTPS_PROXY="https://yourproxy.local:8080"`).
   2. Pour configurer les adresses IP ou les noms de domaine que vous souhaitez exclure du proxy, modifiez la variable d'environnement `NO_PROXY` (par exemple, `NO_PROXY="www.gpqa.com"`).

      Utilisez des virgules pour séparer plusieurs adresses IP ou noms de domaine. À partir de l'application GlobalProtect 5.1.6, vous pouvez utiliser le caractère générique (*) pour les adresses IP ou les noms de domaine (par exemple, `NO_PROXY="*.domain.com"`).

3. Installez la version GUI de l'application GlobalProtect pour Linux.

   Pour installer le package de distribution de l'interface utilisateur de l'application GlobalProtect, utilisez la commande **`$ ./gp_install.sh`** :

   ```
   $ ./gp_install.sh --help Usage: $ sudo ./gp_install [--cli-only |
    --arm | --help] --cli-only: CLI Only --arm: ARM no options: UI
   ```

   Une fois l'installation terminée, l'application GlobalProtect se lance automatiquement.

4. Déconnectez-vous du système d'exploitation Linux ou de la session SSH selon la méthode d'installation que vous avez utilisée, puis reconnectez-vous.

   Cette étape est nécessaire pour s'assurer que toutes les nouvelles mises à jour de package pendant l'installation sont appliquées à l'application GlobalProtect.

5. Spécifiez l'adresse de votre portail et entrez vos identifiants lorsque vous y êtes invité pour commencer le processus de connexion.

6. (Facultatif) Pour importer un certificat, complétez les étapes suivantes.

   Lorsque vous souhaitez prédéployer un certificat client sur un terminal pour une authentification basée sur un certificat, vous pouvez copier le certificat sur le terminal et l'importer pour qu'il soit utilisé par l'application GlobalProtect. Utilisez la commande **`globalprotect import-certificate --location <location>`** pour importer le

certificat sur le terminal. Lorsque vous y êtes invité, vous devez fournir le mot de passe du certificat.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12 Veuillez entrer le code
 secret : L'importation du certificat a réussi.
```

Téléchargement et installation de la version CLI de GlobalProtect pour Linux

Si votre périphérique Linux ne prend pas en charge une interface utilisateur graphique, installez l'application GlobalProtect pour Linux en complétant ces étapes. L'application GlobalProtect pour Linux prend en charge les packages d'installation DEB, RPM et TAR.

1. Téléchargez l'application GlobalProtect pour Linux.
   1. Obtenez le package de l'application auprès de votre administrateur informatique, puis copiez le fichier TGZ sur le terminal Linux.

      Par exemple, si vous avez téléchargé le package sur un terminal macOS, vous pouvez ouvrir un terminal et copier le fichier :

      ```
      macUser@mac:~$ scp ~/Downloads/PanGPLinux-6.0.0.tgz
       linuxUser@linuxHost: <DestinationFolder>
      ```

      où ***<DestinationFolder>*** est un emplacement tel que `~/pkgs/` où vous souhaitez stocker le fichier TGZ.
   2. Depuis le terminal Linux, décompressez le package.

      ```
      user@linuxhost:~$ tar -xvf ~/pkgs/PanGPLinux-6.0.0.tgz
      ```

      Après avoir décompressé le package, vous verrez des packages d'installation (DEB pour Ubuntu et RPM pour CentOS et Red Hat) et les scripts pour installer et désinstaller les packages.
2. (Facultatif) Si votre terminal Linux doit utiliser une configuration de serveur proxy manuelle, configurez les paramètres du proxy.

   L'application GlobalProtect pour Linux ne prend en charge qu'une configuration de serveur proxy de base, mais ne prend pas en charge l'utilisation de fichiers de configuration automatique de proxy (PAC) et l'authentification proxy.

   L'application GlobalProtect pour Linux obtient les paramètres du proxy à partir des variables d'environnement `HTTP_PROXY`, `HTTPS_PROXY` et `NO_PROXY` dans le fichier `/etc/environment`. Si vous modifiez ultérieurement la configuration du proxy système, vérifiez que le terminal à partir duquel GlobalProtect s'exécute utilise les variables d'environnement du

proxy. Si vous ne voyez pas les nouveaux paramètres, déconnectez-vous et reconnectez-vous pour que les nouveaux paramètres prennent effet.

Si vous avez configuré la variable HTTP_PROXY ou la variable HTTPS_PROXY, assurez-vous que le portail GlobalProtect correspond aux paramètres configurés pour la variable NO_PROXY.

1. Pour définir votre proxy sur votre terminal Linux, modifiez la variable d'environnement HTTP_PROXY ou la variable d'environnement HTTPS_PROXY (par exemple, `HTTPS_PROXY="https://yourproxy.local:8080"`).
2. Pour configurer les adresses IP ou les noms de domaine que vous souhaitez exclure du proxy, modifiez la variable d'environnement NO_PROXY (par exemple, `NO_PROXY="www.gpqa.com"`).

   Utilisez des virgules pour séparer plusieurs adresses IP ou noms de domaine. À partir de l'application GlobalProtect 5.1.6, vous pouvez utiliser le caractère générique (*) pour les adresses IP ou les noms de domaine (par exemple, `NO_PROXY="*.domain.com"`).

3. Installez le package de l'application en utilisant la commande **`CLI Only`** :

```
$ ./gp_install.sh --help Usage: $ sudo ./gp_install [--cli-only |
 --arm | --help] --cli-only: CLI Only --arm: ARM no options: UI
```

4. (Facultatif) Changez les modes de CLI.

Vous pouvez exécuter des commandes en mode ligne de commande ou en mode invite. Le mode ligne de commande nécessite que vous spécifiiez la commande complète de GlobalProtect. Le mode invite nécessite que vous spécifiiez uniquement la commande (sans le nom de l'application). Cela affiche une sortie plus détaillée que le mode ligne de commande.

1. Pour passer en mode invite, entrez **`globalprotect`** sans aucun argument.

```
user@linuxhost:~$ globalprotect >>
```

2. Pour quitter le mode invite, entrez **`quit`**.

```
>> quit user@linuxhost:~$
```

5. Affichez l'aide pour l'application GlobalProtect pour Linux.

Mode invite :

```
>> help Utilisation : seules les commandes suivantes sont prises en
 charge : collect-log -- collect log information connect -- connect
 to server disconnect -- disconnect disable -- disable connection
 import-certificate -- import client certificate file quit -- quit
 from prompt mode rediscover-network -- network rediscovery remove-
user -- clear credential resubmit-hip -- resubmit hip information
 set-log -- set debug level show -- show information
```


Mode ligne de commande :

```
user@linuxhost:~$ globalprotect help Utilisation : seules les
 commandes suivantes sont prises en charge : collect-log --
 collect log information connect -- connect to server disconnect
 -- disconnect disable -- disable connection import-certificate
 -- import client certificate file quit -- quit from prompt mode
 rediscover-network -- network rediscovery remove-user -- clear
 credential resubmit-hip -- resubmit hip information set-log -- set
 debug level show -- show information
```

6. Utilisez la version CLI de l'application GlobalProtect pour Linux.

Installation de l'application GlobalProtect pour Linux

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Linux uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

GlobalProtect prend en charge deux versions de l'application GlobalProtect pour Linux : Une version si votre périphérique Linux prend en charge une interface graphique (GUI), et une version CLI si votre périphérique Linux ne prend pas en charge une interface graphique (GUI).

- Utilisation de la version GUI de l'application GlobalProtect pour Linux
- Utilisation de la version CLI de l'application GlobalProtect pour Linux

Utilisation de la version GUI de l'application GlobalProtect pour Linux

Pour utiliser la version GUI de l'application GlobalProtect pour Linux, suivez ces étapes.

1. Dans la fenêtre GlobalProtect, entrez le FQDN ou l'adresse IP du portail GlobalProtect, puis cliquez sur **Connect (Connecter)**.

   Après avoir téléchargé et installé la version GUI de l'application GlobalProtect pour Linux, l'application GlobalProtect se lance automatiquement.

   1. (Facultatif) Si plusieurs portails sont enregistrés sur votre application, sélectionnez un portail dans le menu déroulant **Portal (Portail)**. Par défaut, le portail le plus récemment connecté est présélectionné dans le menu déroulant **Portal (Portail)**.

   2. Saisissez le **Username (Nom d'utilisateur)** et le **Password (Mot de passe)** pour le portail, puis cliquez sur **Sign In (Se connecter)**.

      Dans la plupart des cas, vous pouvez utiliser le même nom d'utilisateur et le même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise. Après vous être connecté, le portail GlobalProtect affiche un état **Connected (Connecté)**.

   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 passerelle

différente, cliquez sur le menu déroulant de la passerelle, puis utilisez l'une des options suivantes :

- Sélectionnez une passerelle manuellement (passerelles externes uniquement).

  Cette option n'est disponible que si votre administrateur active la sélection manuelle de la passerelle.

- Attribuez et connectez-vous automatiquement à une passerelle préférée :

  1. Dans le menu en haut à droite du panneau d'état de l'application, sélectionnez **Preferred Gateway (Passerelle préférée)** pour ouvrir GlobalProtect : Boîte de dialogue Preferred Gateway (Passerelle préférée).
  2. Dans la liste des passerelles disponibles, sélectionnez la passerelle que vous souhaitez définir comme passerelle préférée, puis **Set as Preferred (Définir comme préférée)**.
  3. **Fermez** la boîte de dialogue.

  Si vous ne souhaitez plus vous connecter automatiquement à la passerelle, vous pouvez également supprimer l'attribution de la passerelle préférée :

  1. Dans le menu en haut à droite du panneau d'état de l'application, sélectionnez **Preferred Gateway (Passerelle préférée)** pour ouvrir GlobalProtect : Boîte de dialogue Preferred Gateway (Passerelle préférée).
  2. Dans la liste des passerelles disponibles, sélectionnez la passerelle préférée, puis **Remove Preferred (Supprimer la préférée)**.
  3. **Fermez** la boîte de dialogue.

2. Ouvrez l'application GlobalProtect.

   Cliquez sur l'icône de bac de système GlobalProtect pour lancer l'interface de l'application.

3. Affichez des informations sur votre connexion réseau.

   Après avoir lancé l'application, sélectionnez le menu ( ) en haut à droite du panneau de l'application, sélectionnez **Settings (Paramètres)** pour ouvrir le panneau **GlobalProtect Settings**

(Paramètres GlobalProtect), puis sélectionnez l'un des onglets suivants pour afficher des informations sur votre connexion réseau :

- **Général** : affiche le nom d'utilisateur et le ou les portails associés au compte GlobalProtect. Vous pouvez également ajouter, supprimer ou modifier des portails à partir de cet onglet.

- **Connection (Connexion)** : répertorie les passerelles qui sont configurées pour l'application GlobalProtect et fournit des informations à propos de chaque passerelle :
  - Nom de la passerelle
  - État du tunnel
  - Statut d'authentification
  - Type de connexion
  - Adresse IP ou FQDN de la passerelle (disponible uniquement en mode externe)

  *Pour le mode interne, l'onglet **Connection (Connexion)** présente la liste complète des passerelles disponibles. Pour le mode externe, l'onglet **Connection (Connexion)** affiche uniquement la passerelle à laquelle vous êtes connecté ainsi que des détails supplémentaires sur la passerelle (comme l'adresse IP de la passerelle, l'emplacement et la disponibilité).*

- **Troubleshooting (Dépannage)** : vous permet de **Collect Logs (Collecter les journaux)** et de définir le **Logging Level (Niveau de Journalisation)**.

  Pour que l'application GlobalProtect envoie des journaux de dépannage, des journaux de diagnostic ou les deux au service de journalisation Strata pour une analyse plus approfondie, vous devez configurer le portail GlobalProtect pour activer la GlobalProtect app log collection for troubleshooting (Collecte de journaux d'application GlobalProtect pour le dépannage). De plus, vous pouvez configure the HTTPS-based destination URLs (configurer les URL de destination basées sur HTTPS) qui peuvent contenir des adresses IP ou des noms de domaine complets des serveurs/ressources Web que vous souhaitez sonder, et déterminer des problèmes tels que la latence ou les performances du réseau sur le point de terminaison de l'utilisateur final.

4. (Facultatif) Connectez-vous en utilisant un nouveau mot de passe.

   *Si votre administrateur GlobalProtect configure l'agent du portail GlobalProtect pour **Save User Credentials (Enregistrer les informations d'identification de l'utilisateur)**, vos informations d'identification sont automatiquement enregistrées dans l'application GlobalProtect. Si votre mot de passe pour accéder au réseau d'entreprise change, vous devez vous connecter à GlobalProtect en utilisant votre nouveau mot de passe.*

   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système. Le panneau d'état s'ouvre.
   2. Sélectionnez le menu ( ) en haut à droite du panneau de l'application, puis sélectionnez **Settings (Paramètres)** pour ouvrir le panneau **GlobalProtect Settings (Paramètres GlobalProtect)**.

3. Dans l'onglet **General (Général)** du panneau **GlobalProtect Settings (Paramètres GlobalProtect)**, **Sign Out (Déconnectez-vous)** pour effacer vos identifiants utilisateur enregistrés de l'application GlobalProtect.
4. Après avoir effacé vos identifiants utilisateur, vous pouvez vous reconnecter à GlobalProtect avec votre nouveau nom d'utilisateur et mot de passe.

5. (Facultatif) Déconnectez-vous de GlobalProtect.

Si votre administrateur configure GlobalProtect avec la méthode de connexion **On-Demand (À la demande)**, vous pouvez vous déconnecter de GlobalProtect en cliquant sur **Disconnect (Déconnecter)** dans le panneau d'état.

Utilisation de la version CLI de l'application GlobalProtect pour Linux

En utilisant la Command Line Interface (interface de ligne de commande - CLI) de l'application GlobalProtect™ pour Linux, vous pouvez effectuer des tâches courantes de l'application GlobalProtect. Les exemples suivants affichent la sortie en mode ligne de commande. Pour exécuter la même commande en mode invite, entrez-la sans le préfixe **globalprotect** (pour plus d'informations, consultez la section Téléchargement et installation de l'application GlobalProtect pour Linux).

Connectez-vous à un portail GlobalProtect :

Utilisez la commande **globalprotect connect --portal *<gp-portal>*** où ***<gp-portal>*** est l'adresse IP ou le FQDN de votre portail GlobalProtect.

Par exemple :

```
user@linuxhost:~$ globalprotect connect --portal
 myportal.example.com Récupération de la configuration…
 Disconnected myportal.example.com - portal:local:Enter login
 credentials username:user1 Password: Récupération de la
 configuration… Découverte du réseau… En cours de connexion...
 Connecté
```

Lorsque vous utilisez l'authentification basée sur un certificat, la première fois que vous vous connectez sans un certificat CA racine, l'application GlobalProtect et le portail GlobalProtect échangent des certificats. L'application GlobalProtect affiche une erreur de certificat, que vous devez reconnaître avant de vous authentifier. Lorsque vous vous connecterez à nouveau, vous ne serez pas invité avec le message d'erreur de certificat.

```
user@linuxhost:~$ globalprotect connect --
portal myportal.example.com Récupération de la
 configuration…
 Déconnecté Il y a un problème avec le certificat de sécurité,
 donc l'identité de 10.3.188.61 ne peut pas être vérifiée.
 Veuillez contacter le service d'assistance de votre organisation
 pour faire rectifier le problème. Attention : La communication
 avec 10.3.188.61 a peut-être été compromise. Nous vous
 recommandons de ne pas continuer avec cette connexion. Détails
```



```
de l'erreur : Voulez-vous continuer (o/n) ?o Récupération de
la configuration…
 Disconnected 10.3.188.61 - portal:local:Enter login
credentials username:user1 Password: Récupération de la
configuration…
Découverte du réseau… En cours de connexion... Connecté
```

Vous pouvez également spécifier un nom d'utilisateur dans la commande en utilisant l'option ***--username <username>****. L'application GlobalProtect vous invite à vous authentifier et, si vous avez spécifié l'option de nom d'utilisateur, à confirmer votre nom d'utilisateur.*

Importez un certificat.

Lorsque vous souhaitez prédéployer un certificat client sur un terminal pour une authentification basée sur un certificat, vous pouvez copier le certificat sur le terminal et l'importer pour qu'il soit utilisé par l'application GlobalProtect. Utilisez la commande **globalprotect import-certificate --location *<location>*** pour importer le certificat sur le terminal. Lorsque vous y êtes invité, vous devez fournir le mot de passe du certificat.

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12 Veuillez entrer le code
 secret : L'importation du certificat a réussi.
```

Connectez-vous à une passerelle :

1. (Facultatif) Affichez les passerelles manuelles auxquelles vous pouvez vous connecter en utilisant la commande **globalprotect show --manual-gateway**.
2. Connectez-vous à une passerelle en utilisant la commande **globalprotect connect --gateway *<gp-gateway>*** où ***<gp-gateway>*** est l'adresse IP ou le FQDN de la passerelle GlobalProtect.
3. Affichez les détails de votre connexion en utilisant la commande **globalprotect show --details**.

```
user@linuxhost:~$ globalprotect show --manual-gateway Nom Adresse
 ---------------------------- gw1 192.168.1.180 gw2 192.168.1.181
 user@linuxhost:~$ globalprotect connect --gateway 192.168.1.180
 Récupération de la configuration… Découverte du réseau… En cours
 de connexion... Connecté
```

Vérifiez l'état et consultez les détails de votre connexion GlobalProtect :

Utilisez la commande **globalprotect show --status** pour vérifier l'état de votre connexion.

Utilisez la commande **globalprotect show --details** pour consulter les détails de votre connexion.

```
user@linuxhost:~$ globalprotect show --status État de
 GlobalProtect : Connecté user@linuxhost:~$ globalprotect
```



```
 show --details Adresse IP assignée : Adresse IP de la
 passerelle 192.168.1.132 : Protocole 192.168.1.180 : Temps de
 fonctionnement IPSec (sec) : 231
```

Redécouvrez le réseau :

Utilisez la commande **globalprotect rediscover-network** pour vous déconnecter et vous reconnecter à GlobalProtect.

```
user@linuxhost:~$ globalprotect rediscover-network Déconnexion…
 Récupération de la configuration… Récupération de la
 configuration… Découverte du réseau… En cours de connexion... En
 cours de connexion... État de GlobalProtect connecté : Connecté
```

Effacez les identifiants pour l'utilisateur actuel :

Utilisez la commande **globalprotect remove-user** pour effacer les identifiants utilisés pour s'authentifier auprès du portail et des passerelles. Après avoir confirmé que l'application GlobalProtect doit effacer vos identifiants, l'application GlobalProtect déconnecte le tunnel et vous demande ensuite de saisir vos identifiants la prochaine fois que vous vous connectez.

```
user@linuxhost:~$ globalprotect remove-user Les identifiants seront
 effacés et le tunnel actuel sera terminé. Voulez-vous continuer
 (o/n) ?o L'effacement a été effectué avec succès. user@linuxhost:~
$ globalprotect connect --portal 192.168.1.179 Récupération de
 la configuration… 192.168.1.179 déconnecté - portal:local:Enter
 login credentials username:user1 Mot de passe : Récupération de
 la configuration… Découverte du réseau… En cours de connexion...
 Connecté
```

Renvoyez les informations de l'hôte à la passerelle.

Utilisez la commande **globalprotect show --host-state** pour consulter les informations actuelles sur l'hôte concernant votre terminal. Utilisez la commande **globalprotect resubmit-hip** pour renvoyer des informations sur le terminal à la passerelle. Ceci est utile dans les cas où la politique de sécurité basée sur HIP empêche les utilisateurs d'accéder aux ressources, car elle permet à l'utilisateur de résoudre le problème de conformité sur le terminal et ensuite de renvoyer le HIP.

```
user@linuxhost:~$ globalprotect show --host-state generate-time:
 09/28/2017 11:24:07 categories host-info client-version: 4.1.0
 os: Linux Ubuntu 16.04.3 LTS os-vendor: Linux domain: host-
name: linuxhost host-id: 4C4C4544-0034-4D10-804C-************
 network-interface enp0s31f6 description: enp0s31f6 mac-address:
 D4:81:D7:D4:5A:A5 wlp2s0 description: wlp2s0 mac-address:
 14:AB:C5:DE:D1:0E user@linuxhost:~$ globalprotect resubmit-hip La
 nouvelle soumission est réussie.
```

Affichez toutes les notifications GlobalProtect.

Utilisez la commande **globalprotect show --notification** pour voir les notifications.

Affichez l'icône de bac de système GlobalProtect.

Utilisez la commande **`globalprotect launch-ui`** pour afficher l'icône de bac de système sur votre bureau. Vous pouvez lancer l'application GlobalProtect en cliquant sur l'icône de bac de système.

Affichez la page d'accueil.

Utilisez la commande **`globalprotect show --welcome-page`**. L'application GlobalProtect affiche la page d'accueil dans un navigateur si une page d'accueil existe ou affiche une notification si la page d'accueil n'existe pas.

Affichez les erreurs.

Utilisez la commande **`globalprotect show --error`** pour voir les erreurs signalées par l'application.

```
user@linuxhost:~$ globalprotect show --error Erreur : Impossible de
 se connecter au portail GlobalProtect
```

Collecter les journaux.

L'application stocke les fichiers journaux PanGPA et PanGPI dans le répertoire `/home/<user>/.Globalprotect`. Utilisez la commande **`globalprotect collect-logs`** pour activer l'application GlobalProtect pour Linux afin de regrouper ces journaux et d'autres informations utiles. Vous pouvez ensuite utiliser ces journaux pour résoudre les problèmes ou les transmettre à un ingénieur du support pour une analyse experte.

```
user@linuxhost:~$ globalprotect collect-log Début de la collecte…
 collecte des informations réseau… collecte des informations
 machine… copie des fichiers… génération du fichier de résultat
 final… Le fichier de support est enregistré dans /home/
user/.GlobalProtect/Collect.tgz
```

Affichez la version de l'application GlobalProtect pour Linux.

```
user@linuxhost:~$ globalprotect show --version GlobalProtect :
 6.0.0-23 Copyright(c) 2009-2021 Palo Alto Networks, Inc.
```


Signaler un problème depuis l'application GlobalProtect pour Linux

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Linux uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si vous rencontrez un comportement inhabituel, tel qu'une mauvaise performance du réseau ou une impossibilité d'établir une connexion avec le portail et la passerelle, vous pouvez signaler le problème directement au service de journalisation Strata auquel votre administrateur peut accéder. Vous n'avez plus besoin de collecter manuellement et d'envoyer les journaux de l'application GlobalProtect par e-mail ou de les stocker sur un lecteur cloud.

Vous ne pouvez signaler un problème à votre administrateur qu'en utilisant la version GUI de l'application GlobalProtect pour Linux.

*Pour afficher l'option **Report an Issue (Signaler un problème)** sur l'application GlobalProtect, votre administrateur doit activer la collecte des journaux de l'application GlobalProtect pour le dépannage sur le portail GlobalProtect.*

1. Connectez-vous au portail GlobalProtect ou à la passerelle.
   1. Dans la fenêtre GlobalProtect, entrez le FQDN ou l'adresse IP du portail GlobalProtect, puis cliquez sur **Connect (Connecter)**.

      Après avoir téléchargé et installé la version GUI de l'application GlobalProtect pour Linux, l'application GlobalProtect se lance automatiquement.
   2. (Facultatif) Si plusieurs portails sont enregistrés sur votre application, sélectionnez un portail dans le menu déroulant **Portal (Portail)**. Par défaut, le portail le plus récemment connecté est présélectionné dans le menu déroulant **Portal (Portail)**.
   3. Saisissez le **Username (Nom d'utilisateur)** et le **Password (Mot de passe)** pour le portail, puis cliquez sur **Sign In (Se connecter)**.

      Dans la plupart des cas, vous pouvez utiliser le même nom d'utilisateur et le même mot de passe que vous utilisez pour vous connecter à votre réseau d'entreprise. Après vous être connecté, le portail GlobalProtect affiche un état **Connected (Connecté)**.
   4. (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 passerelle différente, cliquez sur le menu déroulant de la passerelle.
2. Ouvrez l'application GlobalProtect.

   Cliquez sur l'icône de bac de système GlobalProtect pour lancer l'interface de l'application.

3. Signalez un problème depuis l'application GlobalProtect à partir de votre terminal.

Après avoir lancé l'application, sélectionnez le menu ( ) en haut à droite du panneau de l'application pour signaler un problème à votre administrateur.

1. Sélectionnez **Report an Issue (Signaler un problème)**.

2. Activez l'application GlobalProtect pour exécuter des tests de diagnostic et inclure des journaux de diagnostic. Les journaux de diagnostic et de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact.

   Une fois les tests de diagnostic terminés avec succès, les fichiers journaux de débogage GlobalProtect sont téléchargés vers le service de journalisation Strata depuis votre terminal.

   Si vous n'activez pas l'application pour exécuter des tests de diagnostic et inclure des journaux de diagnostic, seuls les journaux de dépannage sont collectés et envoyés au service de journalisation Strata sous forme de rapport de dépannage compact. L'application GlobalProtect vérifie les fichiers de rapport (pan_gp.trb.log ou pan_gp_trbl.log) qui sont générés automatiquement au format `.json`*. Un message de notification apparaît si aucun problème n'a été trouvé dans les journaux de dépannage. Cliquez sur* ***Retry (Réessayer)*** *pour vérifier si les fichiers pan_gp.trb*.log existent.*

3. Cochez la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure les journaux de diagnostic)**.
4. Cliquez sur **Continue (Continuer)** pour permettre à l'application de créer un journal de dépannage et d'envoyer le rapport à l'instance du service de journalisation Strata de votre administrateur.

   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log.

   Les résultats des tests de diagnostic de bout en bout sont stockés dans le fichier pan_gp_diag.log au format `.json` et envoyés à l'instance du service de journalisation Strata de votre administrateur avec les fichiers pan_gp.trb*.log. L'application GlobalProtect peut exécuter des tests de diagnostic avec ou sans tunnel.

Par exemple, vous voudrez peut-être entrer vos identifiants de connexion GlobalProtect avant que l'application ne se connecte et n'exécute des tests de diagnostic via le tunnel.

Un message s'affiche, confirmant que l'application exécute des tests de diagnostic uniquement si vous avez coché la case **Run Diagnostic Tests and Include Diagnostic Logs (Exécuter des tests de diagnostic et inclure des journaux de diagnostic)**.

Un message s'affiche, confirmant que l'application envoie le rapport au service de journalisation Strata.

5. Cliquez sur **Close (Fermer)** pour confirmer que l'application a réussi à envoyer le rapport au service de journalisation Strata. Ce message de confirmation affiche la date et l'heure auxquelles le rapport a été traité et envoyé.

Déconnexion de l'application GlobalProtect pour Linux

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Linux uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Si votre administrateur configure la méthode de connexion à GlobalProtect sur **Always On (Toujours active)**, vous pouvez déconnecter l'application GlobalProtect. Par exemple, vous pourriez vouloir déconnecter l'application si le Virtual Private Network (réseau privé virtuel - VPN) GlobalProtect ne fonctionne pas dans un hôtel, et l'échec du VPN vous empêche de vous connecter à Internet. Après avoir déconnecté l'application GlobalProtect, vous pouvez vous connecter à Internet en utilisant une communication non sécurisée (sans VPN).

La méthode, la durée et le nombre de déconnexions autorisées de l'application GlobalProtect dépendent de la configuration du service GlobalProtect par l'administrateur. Cette configuration peut vous empêcher de déconnecter complètement l'application ou vous permettre de déconnecter l'application uniquement après avoir répondu correctement à un défi.

Si votre configuration inclut un défi, l'application GlobalProtect demande l'un des éléments suivants :

- Raison pour laquelle vous souhaitez déconnecter l'application
- Code secret

Si le défi implique un code secret, nous vous recommandons de contacter un administrateur GlobalProtect ou une personne du service d'assistance par téléphone. Les administrateurs fournissent généralement des codes secrets à l'avance, soit par e-mail (pour les nouveaux utilisateurs de GlobalProtect), soit publiés sur le site Web de votre organisation. En réponse à une panne ou à un problème système, les administrateurs peuvent également fournir des codes secrets par téléphone.

GlobalProtect prend en charge deux versions de l'application GlobalProtect pour Linux : Une version si votre périphérique Linux prend en charge une interface graphique (GUI), et une version CLI si votre périphérique Linux ne prend pas en charge une interface graphique (GUI).

- Déconnexion de l'application GlobalProtect pour Linux en utilisant la version GUI
- Déconnexion de l'application GlobalProtect pour Linux en utilisant la version CLI

Déconnexion de l'application GlobalProtect pour Linux en utilisant la version GUI

(Disponible uniquement en mode toujours actif) Pour déconnecter l'application GlobalProtect pour Linux en utilisant la version GUI, suivez ces étapes.

1. Déconnectez l'application GlobalProtect.
   1. Lancez l'application GlobalProtect en cliquant sur l'icône de bac de système GlobalProtect. Le panneau d'état s'ouvre.
   2. Sélectionnez le menu ( ) en haut à droite du panneau de l'application pour ouvrir le menu des paramètres.
   3. Sélectionnez **Disconnect (Déconnecter)**.

      *L'option **Disconnect (Déconnecter)** n'est visible que si la configuration de votre agent GlobalProtect vous permet de déconnecter l'application. Si la configuration vous permet de déconnecter l'application GlobalProtect sans exiger que vous répondiez à un défi, l'application GlobalProtect se ferme sans nécessiter d'action supplémentaire.*

2. Répondez à un ou plusieurs défis, si nécessaire.

   Si vous y êtes invité, fournissez les informations suivantes :

   - **Reason (Raison)** : votre raison pour déconnecter l'application GlobalProtect.
   - **Passcode (Code secret)** : un code secret fourni à l'avance par votre administrateur, en fonction d'un problème ou d'un événement connu qui vous oblige à déconnecter l'application.

Déconnexion de l'application GlobalProtect pour Linux en utilisant la version CLI

Pour déconnecter l'application GlobalProtect pour Linux en utilisant la version CLI, suivez ces étapes.

(Disponible uniquement en mode à la demande) Déconnectez-vous de GlobalProtect :

Utilisez la commande **`globalprotect disconnect`** pour vous déconnecter de GlobalProtect.

```
user@linuxhost:~$ globalprotect disconnect État de GlobalProtect :
 Déconnecté
```


(Disponible uniquement en mode toujours actif) Déconnectez GlobalProtect :

Utilisez la commande **globalprotect disconnect** pour vous déconnecter et désactiver l'application GlobalProtect. Si votre configuration l'exige, vous devez également spécifier une raison ou un code secret lorsque vous y êtes invité.

```
user@linuxhost:~$ globalprotect disconnect
```

```
user@linuxhost:~$ globalprotect disconnect Veuillez entrer la
 raison de la déconnexion : C'est la raison de ma déconnexion
```

```
user@linuxhost:~$ globalprotect disconnect Veuillez entrer le code
 secret pour la déconnexion : ITp@ssw0rd
```


Désinstallation de l'application GlobalProtect pour Linux

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Terminaux Linux uniquement	Version 6.3 ou ultérieure de l'application GlobalProtect

Vous pouvez désinstaller l'application GlobalProtect pour Linux en utilisant la commande suivante :

```
$ ./gp_uninstall.sh --help Usage: $ sudo ./gp_uninstall [--cli-only |
 --arm | --help] --cli-only: CLI Only --arm: ARM no options: UI
```

Exigences de GlobalProtect pour les périphériques IoT

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Périphériques IoT uniquement	Version 6.1 ou ultérieure de l'application GlobalProtect

GlobalProtect™ est une application qui s'exécute sur votre terminal (ordinateur de bureau, ordinateur portable ou serveur, ou périphérique IoT) pour vous protéger en utilisant les mêmes politiques de sécurité qui protègent les ressources sensibles de votre réseau d'entreprise. Pour les périphériques IoT, GlobalProtect™ sécurise le trafic vers et depuis le périphérique vers toute source ou destination sur Internet ou au sein de votre réseau d'entreprise.

Vous pouvez installer GlobalProtect sur les périphériques IoT qui sont intégrés dans les systèmes d'exploitation suivants :

- IoT sur Android
- IoT sur Raspbian
- IoT sur Ubuntu
- IoT sur Windows

