paloalto TECHDOCS

GlobalProtectアプリケーション ユーザー ガイド

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

Last Revised

October 24, 2024

Table of Contents

Windows用GlobalProtect アプリ 5
Windows用 GlobalProtectアプリケーションのダウンロードおよびインストール 6
ログオン前に接続を使用する 9
スマートカード認証を使用した Connect Before Logon (ログイン前接続) 9
SAML 認証を使用した Connect Before Logon (ログイン前接続) 15
ユーザー名/パスワードベースの認証を使用した Connect Before Logon (ログイン前接続) 20
Smart Card認証にシングルサインオンを使用 26
GlobalProtect App for Windowsの使用 29
Windowsログオン画面でのGlobalProtectのパスワード表示 41
Windows用GlobalProtectアプリからの問題を報告する 43
Windows 10 UWP 用 の GlobalProtect アプリケーションをダウンロードします。 46
Windows用のGlobalProtect Appをアンインストールする 50
Microsoft Installerの競合を修正する 51
macOS用GlobalProtect アプリ 53
macOS用GlobalProtectアプリケーションのダウンロードおよびインストール 54
GlobalProtect App for macOSの使用 61
macOS用のGlobalProtectアプリから問題を報告する 76
GlobalProtectアプリをmacOSから接続解除する 81
macOS用のGlobalProtect Appをアンインストールする 83
GlobalProtect Enforcer カーネル拡張機能の削除 87
GlobalProtect App for macOSでクライアント証明書を認証に使用できるようにする 88
iOS 用 GlobalProtect アプリ 89
iOS用GlobalProtectアプリケーションのダウンロードおよびインストール 90
iOS用のGlobalProtectアプリの使用 91
iOS用のGlobalProtectアプリから問題を報告する 95
iOS用 GlobalProtectアプリケーションのアンインストール 97
Android 用 GlobalProtect アプリ 99
Android用GlobalProtectアプリケーションのダウンロードおよびインストール 100
ChromebooksのAndroid用GlobalProtectアプリケーションのダウンロードおよびインストール 101

Android用 GlobalProtectアプリケーションを使用する 103
Android用GlobalProtectアプリからの問題を報告する 107
Android用GlobalProtectアプリケーションの接続を解除する 109
Android用GlobalProtectアプリケーションのアンインストール 111
ChromebookからAndroid用GlobalProtectアプリをアンインストールします。 112
Linux用GlobalProtectアプリ 113
Linux用GlobalProtectアプリケーションのダウンロードおよびインストール 114
GlobalProtect for LinuxのGUIバージョンをダウンロードしてインストールする 114
GlobalProtect for LinuxのCLIバージョンのダウンロードとインストール 116
GlobalProtect App for Linuxの使用 119
Linux用のGlobalProtectアプリのGUIバージョンを使用する 119
Linux用のGlobalProtectアプリのCLIバージョンを使用します。 122
Linux用GlobalProtectアプリケーションからの問題の報告 126
Linux用のグローバル保護アプリの接続を解除 129
GUIバージョンを使用してLinux用のGlobalProtectアプリの接続を解除する 129
CLIバージョンを使用してLinux用GlobalProtectアプリを接続解除する 130
Linux用のGlobalProtect Appをアンインストールする 132
IoTデバイス向けGlobalProtect 133

Windows用GlobalProtect アプリ

GlobalProtect™は、エンドポイント(デスクトップ コンピュータ、ラップトップ、タブレット、またはスマートフォン)上で実行されるアプリケーションであり、企業ネットワーク内の機密リソースを保護するのと同じセキュリティ ポリシーを使用してユーザーを保護します。GlobalProtect™は、データセンター、プライベート クラウド、パブリック クラウド、およびインターネット トラフィックを保護し、世界中のどこからでも会社のリソースにアクセスできるようにします。

次のトピックでは、GlobalProtect app for Windowsをインストールして使用する方法を説明します。

- Windows用 GlobalProtectアプリケーションのダウンロードおよびインストール
- ログオン前に接続を使用する
- Smart Card認証にシングルサインオンを使用
- GlobalProtect App for Windowsの使用
- Windows用GlobalProtectアプリからの問題を報告する
- Windows 10 UWP 用 の GlobalProtect アプリケーションをダウンロードします。
- Windows用のGlobalProtect Appをアンインストールする
- Microsoft Installerの競合を修正する

Windows用 GlobalProtectアプリケーションのダウンロードおよびインストール

どこで使用できますか?	何が必要ですか?
• Windows エンドポイントのみの場合:	❑ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtectネットワークに接続する前に、WindowsエンドポイントにGlobalProtectアプリをダウンロードしてインストールする必要があります。組織の GlobalProtect または Prisma Access のデプロイメントに適したアプリケーションを入手するには、組織内の GlobalProtect ポータルから直接アプリケーションをダウンロードする必要があります。そのため、Palo Alto Networks のサイトでは直接GPアプリをダウンロードできるリンクはありません。

GPアプリをダウンロードしてインストールする前に、GP管理者からGlobalProtectポータルのIPアドレスまたは完全修飾ドメイン名 (FQDN) を取得する必要があります。さらに、管理者は、ポータルおよびゲートウェイへの接続に使用できるユーザ名とパスワードの情報を確認する必要があります。ほとんどの場合、ユーザ名とパスワードは企業ネットワークに接続するときに使用するものと同じユーザ名とパスワードです。必要な情報を収集したら、以下の手順に従ってアプリをダウンロードおよびインストールします。

*GlobalProtectアプリ5.0以降を実行するには、Windowsエンドポイントで*Visual Studio 2013*用の*Visual C++*再頒布可能パッケージ12.0.3*が必要です。再頒布可能パッケージをエンドポイントにまだインストールしていない場合、*GlobalProtect* アプリは *Visual C++* 再頒布可能パッケージ *12.0.3* を自動的にインストールします。*Visual C++*再頒布可能パッケージ*12.0.2*以前のリリースをすでにインストールしている場合は、*GlobalProtect*アプリをインストールする前に、エンドポイントから既存の再頒布可能パッケージをアンインストールするか、*Visual C++*再頒布可能パッケージ*12.0.3*にアップグレードする必要があります。

STEP 1 | GlobalProtect ポータルにログインします。

1. Webブラウザを起動し、以下のURL に移動します:

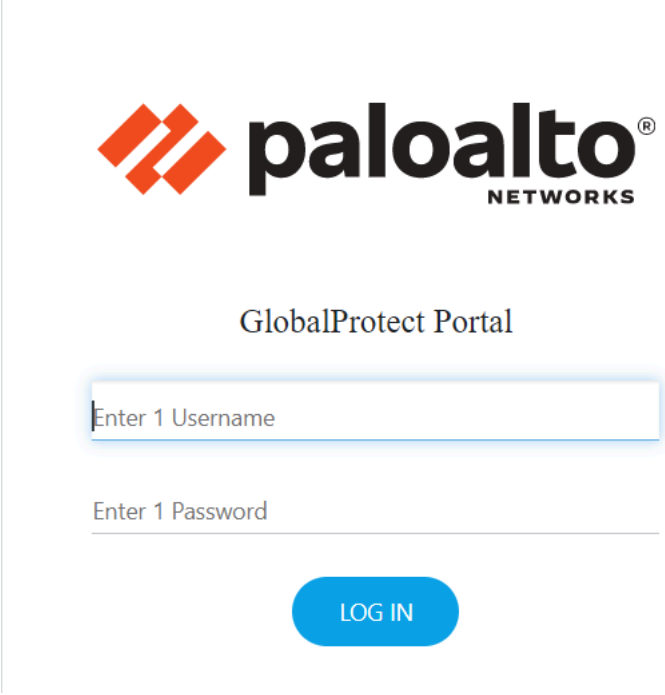
   `https://<portal IP address or FQDN>`

   例: **`http://gp.acme.com`**

   GlobalProtect 6.3以降を実行しており、インテリジェントポータル機能が事前にデプロイされている場合、GlobalProtectはお客様の国の場所に基づいて適切なPrisma Accessポータルに自動的にリダイレクトします。ポータル国マップで定義されている

ポータルは、ドロップダウンで使用できます。詳細については、インテリジェントポータルの設定を参照してください。

2. ポータル ログイン ページで、**[Name (名前)]**と **[Password (パスワード)]**に入力し、**LOG IN (ログイン)]**をクリックします。ほとんどの場合、企業ネットワークに接続するときに使用するのと同じユーザー名とパスワードを使用できます。



STEP 2 | アプリのダウンロード ページに移動します。

ほとんどの場合、ポータルへのログイン後にアプリのダウンロード ページがすぐに表示されます。このページから、最新のアプリ ソフトウェア パッケージをダウンロードします。

システム管理者がGlobalProtectクライアントレスVPNアクセスを有効にしている場合、ポータルにログインした後に(エージェントのダウンロードページの代わりに)アプリケーションページが表示されます。**GlobalProtect Agent**（**GlobalProtect** エージェント）を選択してダウンロード ページを選択します。

STEP 3 | アプリをダウンロードします。

1. ダウンロードを開始するには、お使いのコンピュータで実行されているオペレーティングシステムに対応するリンクをクリックします。オペレーティングシステムが32ビッ

トか64ビットかわからない場合は、システム管理者に問い合わせてから作業を進めてください。

2. ソフトウェア インストール ファイルを開きます。
3. プロンプトが表示されたら、ソフトウェアを実行します。
4. 再度プロンプトが表示されたら、GlobalProtectセットアップウィザードを実行します。

STEP 4 | GlobalProtect アプリ セットアップを完了します。

1. GlobalProtect セットアップ ウィザードで、**[Next (次へ)]** をクリックします。
2. **[Next(次へ)]**をクリックして既定のインストールフォルダー(C:\Program Files\Palo Alto Networks\GlobalProtect)を承認し、その後**[Next(次へ)]**を2回クリックします。

   *GlobalProtect*アプリをインストールする別の場所を参照して選択することもできますが、ベストプラクティスはデフォルトの場所にインストールすることです。デフォルトのインストール場所は、非特権ユーザーの読み取り専用です。したがって、この場所にインストールすると、アプリへの悪意のあるアクセスから保護されます。
3. インストール完了後、ウィザードを 閉じます。

ログオン前に接続を使用する

どこで使用できますか?	何が必要ですか?
• Windows エンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

Connect Before Logon (ログイン前接続)と同時に、プレログオン およびプレログオン後のオンデマンド接続方法は、サポートされません。

ログオン前に接続は、内部ゲートウェイ構成ではサポートされていません。

ログインプロセスを簡素化し、体験を向上させるために、GlobalProtectはログオン前に接続を提供し、スマートカード、LDAP、RADIUS、またはSAMLなどの認証サービス、ユーザー名/パスワードベースの認証、またはワンタイムパスワード(OTP)認証を使用してWindows 10エンドポイントにログインする前に企業ネットワークへのVPN接続を確立できるようにします。管理者は、ローカルプロファイルやユーザーアカウントが設定されていないエンドポイントで新しいGlobalProtectユーザーをオンボードする際に、ログオン前に接続を有効にすることで利益を得ることができます。ログオン前に接続はデフォルトで無効になっています。管理者がログオン前に接続を有効にすると、GlobalProtectアプリの資格情報プロバイダーを起動し、Windowsエンドポイントにログインする前に企業ネットワークに接続できます。ログオン前に接続がVPN接続を確立した後、Windowsログオン画面を使用してWindowsエンドポイントにログインできます。GlobalProtectは、Windowsにログインする前に組織へのアクセスを提供するPre-Login Access Provider (PLAP)資格情報プロバイダーとして機能できます。

ログオン前に接続は、*Windows*エンドポイントに初めてログインする際にポータルとゲートウェイで2回認証を求めるため、*Authentication Override*クッキーは期待通りに機能していません。

ログオン前に接続を使用するには、管理者がWindowsレジストリに設定を展開する必要があり、認証方法を選択します：

- スマートカード認証を使用した Connect Before Logon (ログイン前接続)
- SAML 認証を使用した Connect Before Logon (ログイン前接続)
- ユーザー名/パスワードベースの認証を使用した Connect Before Logon (ログイン前接続)

スマートカード認証を使用した Connect Before Logon (ログイン前接続)

Connect Before Logon (ログイン前接続)は、スマートカード認証をサポートしています。管理者は、スマートカードに含まれる証明書を発行したルートCA証明書をポータルとゲートウェイにインポートする必要があります。管理者は、認証プロセスでスマートカードを使用できるようにするために、証明書プロファイルとそのルートCAをポータルまたはゲートウェイ構成に適用できます。スマートカードを使用してWindowsエンドポイントにログインする前に、GlobalProtectに認証できます。プロンプトが表示されたら、スマートカードを挿

入してスマートカード認証が成功したことを確認します。スマートカード認証が成功した場合、GlobalProtectは構成で指定されたポータルまたはゲートウェイに接続します。

STEP 1 | ログオン前に接続を使用する前に、管理者は次のタスクを完了している必要があります:

1. Windowsレジストリへログオン前の接続設定のデプロイ
2. スマートカードを二要素認証用にセットアップします。
3. 証明書プロファイルをGlobalProtectポータルに割り当てます。
4. ゲートウェイを構成することで、スマートカードに基づいてエンドユーザーを認証します。

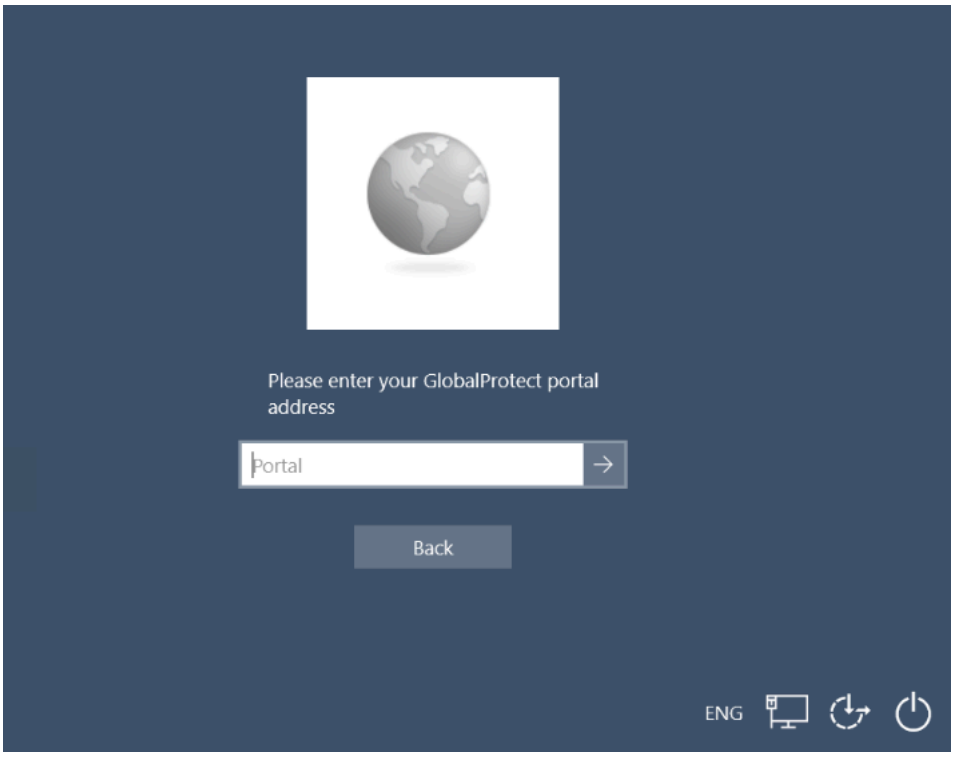
STEP 2 | Windowsエンドポイントにログインするには、ログオン前に接続します。

1. Windowsログオン画面の右下隅にあるネットワークサインイン()ボタンをクリックします。

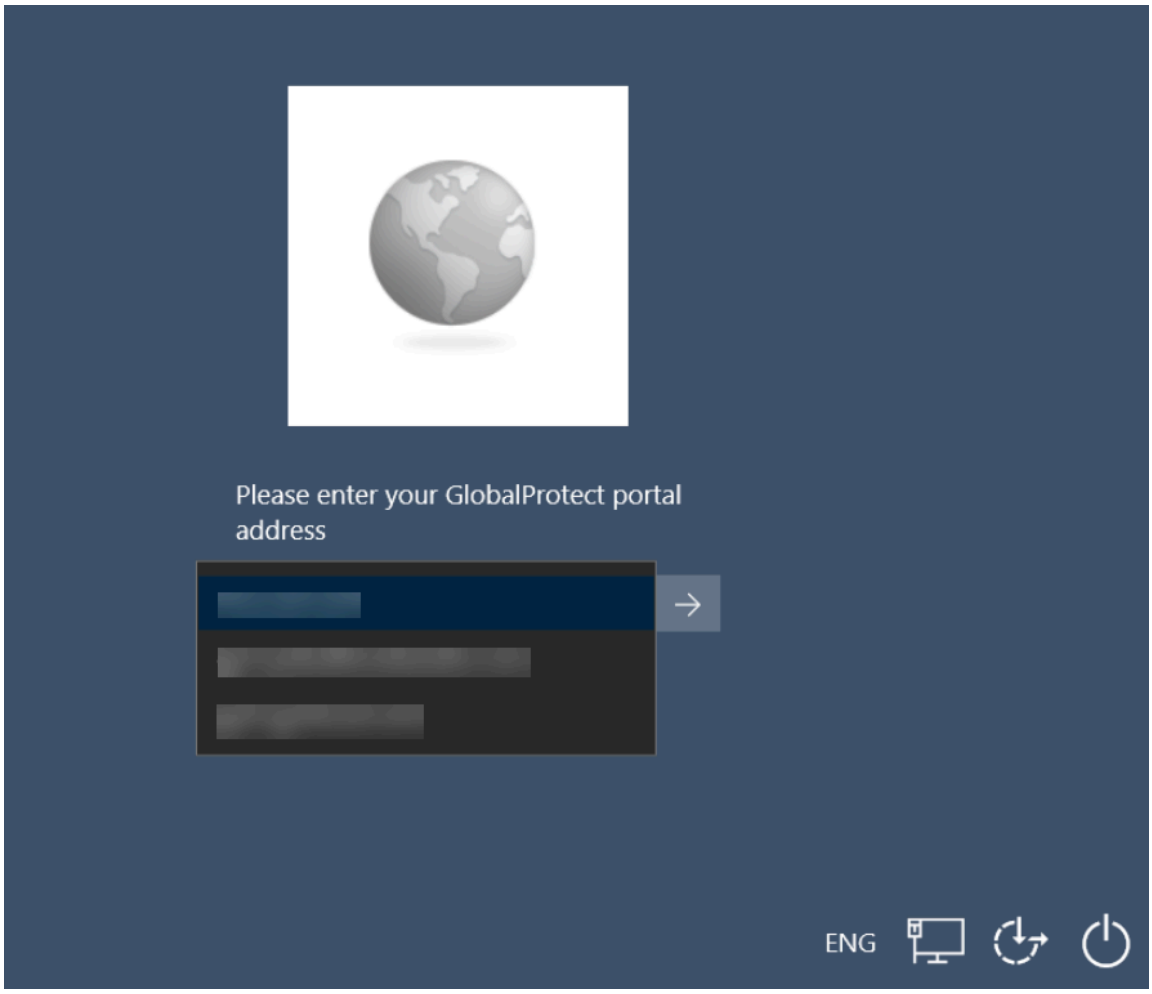
   VPN接続が成功すると、Windowsログオン画面のネットワークサインインボタンの隣に切断()ボタンが表示されます。設定された時間内にエンドポイントにログインして

いない場合、VPNからログアウトされます。これにより、VPNトンネルが切断されます。

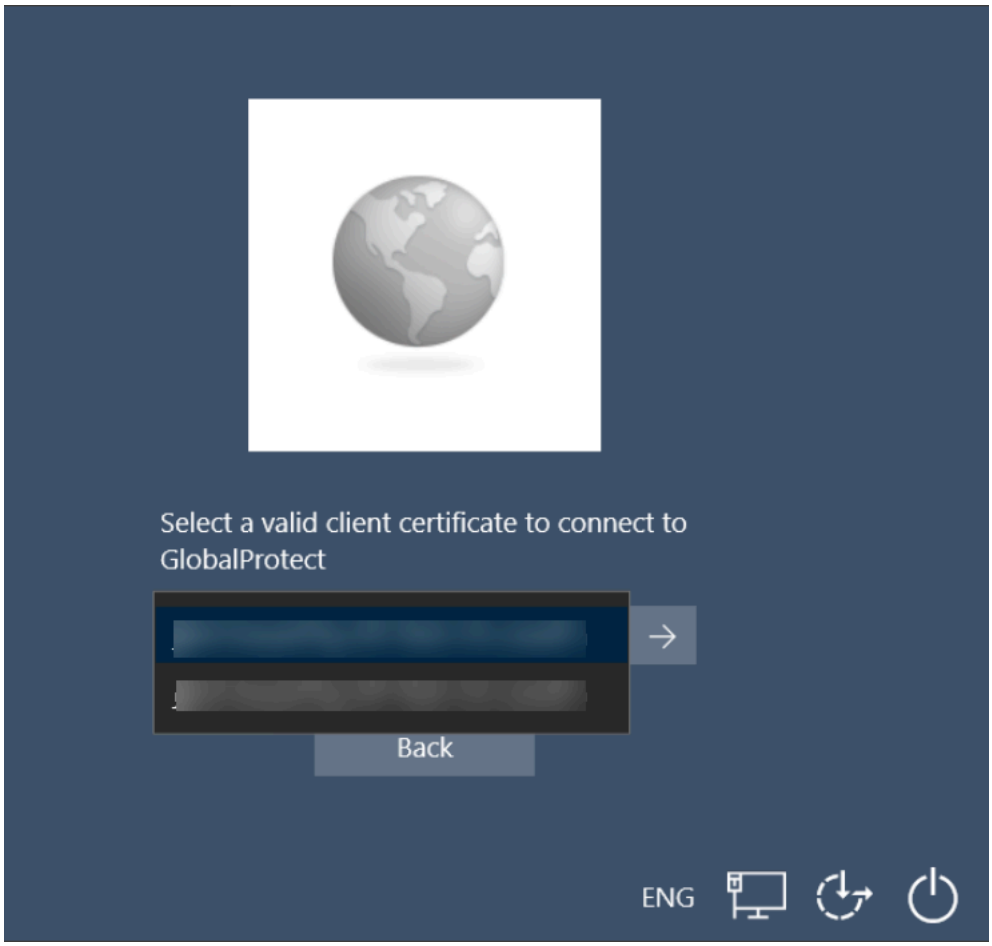
2. (オプション)エンドポイントに初めてログインする場合で、ポータルが管理者によって事前に定義されていない場合は、GlobalProtectポータルのFQDNまたはIPアドレスを入力し、送信します。



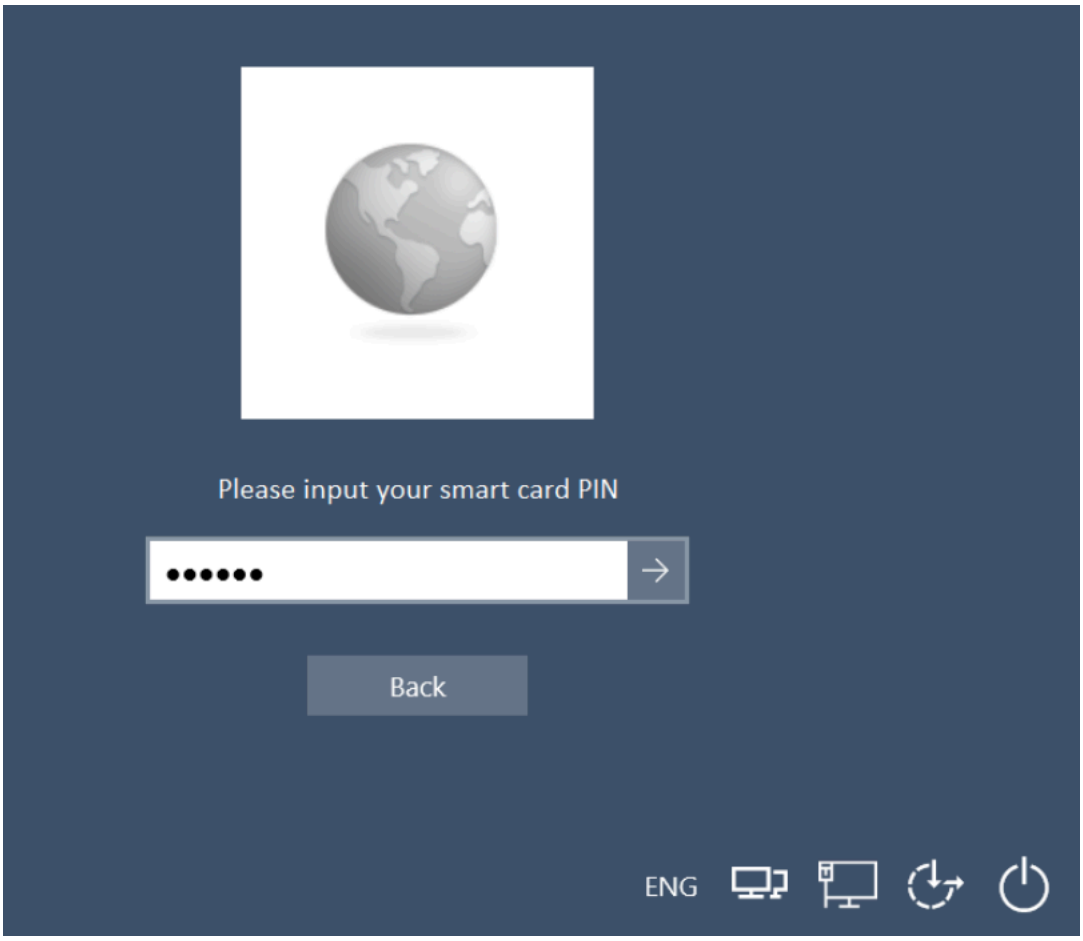
3. (オプション)エンドポイントに初めてログインする場合で、ポータルが管理者によって事前に定義されている場合は、ポータルドロップダウンからポータルを選択し、矢印をクリックして送信します。



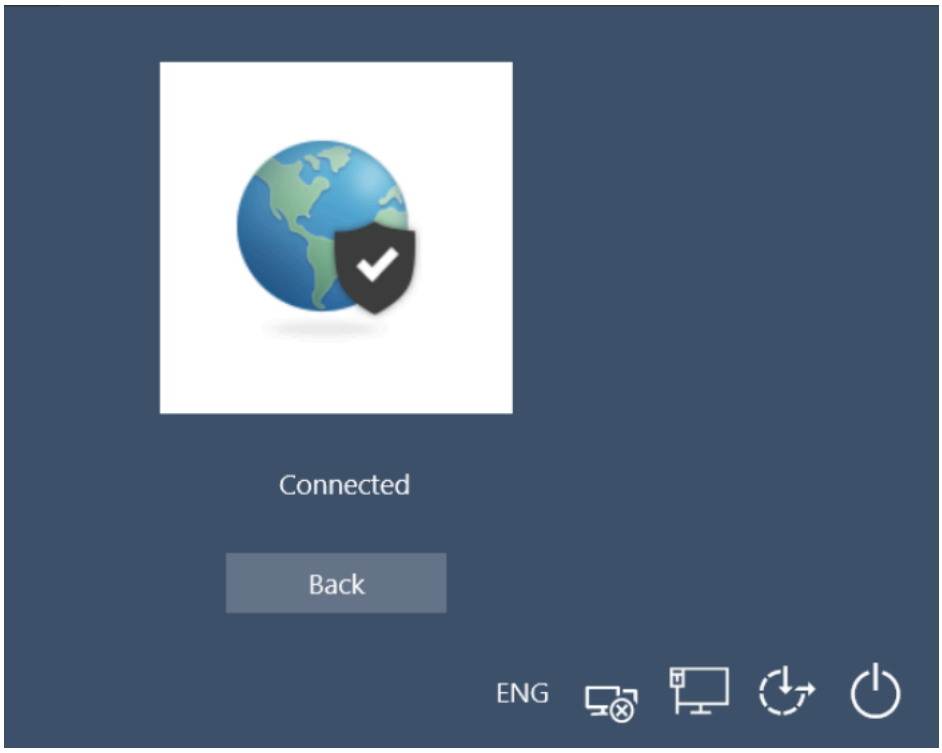
4. ポータルまたはゲートウェイに認証するために、エンドポイント上の有効な証明書のリストからクライアント証明書を選択し、矢印をクリックして送信します。



5. スマートカードの個人識別番号(PIN)を入力し、矢印をクリックして送信します。



6. 認証が成功すると、接続ステータスは成功したVPN接続時に接続済みと表示されます。戻るをクリックしてWindowsログオン画面を表示します。



STEP 3 | GlobalProtectゲートウェイに接続されていることを確認します。

1. 再度Windowsエンドポイントにログインします。Windowsログオン画面の右下隅にあるネットワークサインイン( )ボタンをクリックします。
2. ステータス パネルが開きます。デフォルトでは、最適な利用可能ゲートウェイに自動的に接続されます。

SAML 認証を使用した Connect Before Logon (ログイン前接続)

ログオン前の接続は、ユーザーログインのためのSAML認証をサポートしています。OneloginやOktaなどの設定されたSAMLアイデンティティプロバイダー(IdP)を使用して、Windowsエンドポイントにログインする前にGlobalProtectに認証できます。SAML認証が成功すると、GlobalProtectは設定で指定されたポータルまたはゲートウェイに接続します。

*SAML*認証方式によるログオン前の接続は、古い埋め込み*Web*ビュー*(oew)*を使用するすべての*GlobalProtect*バージョンでサポートされています。ただし、ログオン前の接続モードで特定の外部*IdP URL*を読み込む際に、空白の画面や*JavaScript*エラーが断続的に表示されることがあります。この問題は、古い埋め込み*Web*ビューが*Windows 11*で非推奨となったレガシー*IE*ブラウザを使用しているために発生します。代替の*Edge*ブラウザベースの*WebView2*は、ログオン前接続メソッドをサポートしていません。*GlobalProtect*は、上記の制限付きで従来の*IE*ベースの古い埋め込み*WebView (oew)*を引き続き使用します。

STEP 1 | ログオン前に接続を使用する前に、管理者は次のタスクを完了している必要があります:

1. Windowsレジストリへログオン前の接続設定をデプロイします。
2. エンドユーザーを認証するためのSAML認証のセットアップします。
   - SAML認証サービスの設定を持つサーバープロファイルを作成します。
   - SAMLサーバープロファイルを参照する認証プロファイルを作成します。
3. GlobalProtectゲートウェイのためにSAML認証を指定します。
4. クライアントのためにSAML認証を指定します(GlobalProtectクライアント認証設定の定義を参照)。

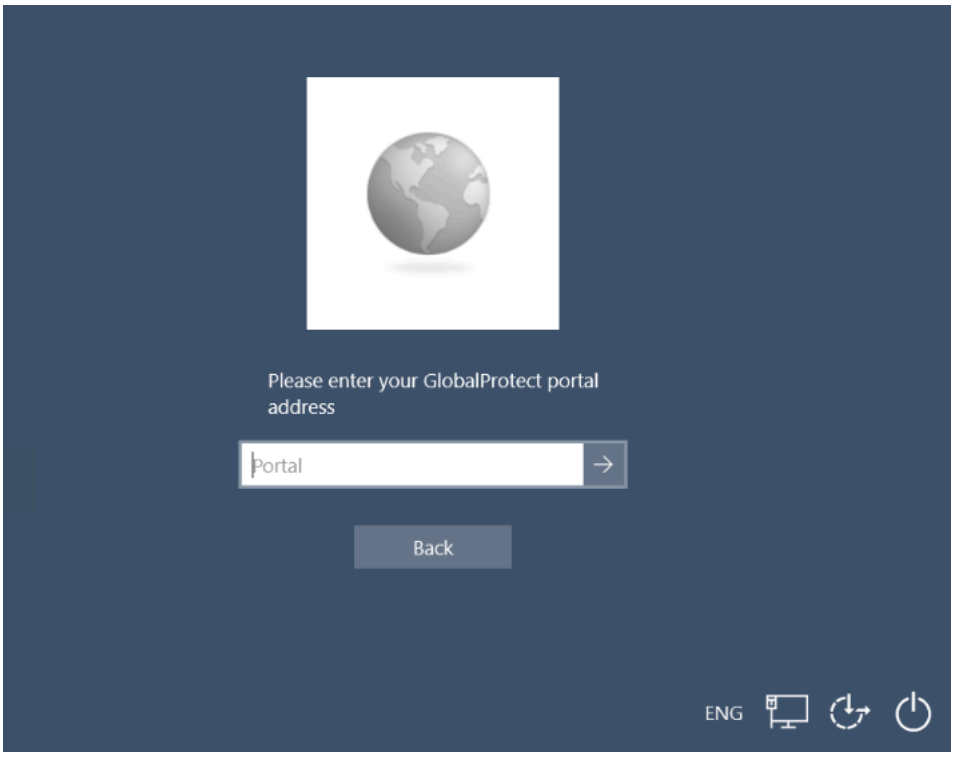
STEP 2 | Windowsエンドポイントにログインするには、ログオン前に接続します。

1. Windowsログオン画面の右下隅にあるネットワークサインイン()ボタンをクリックします。

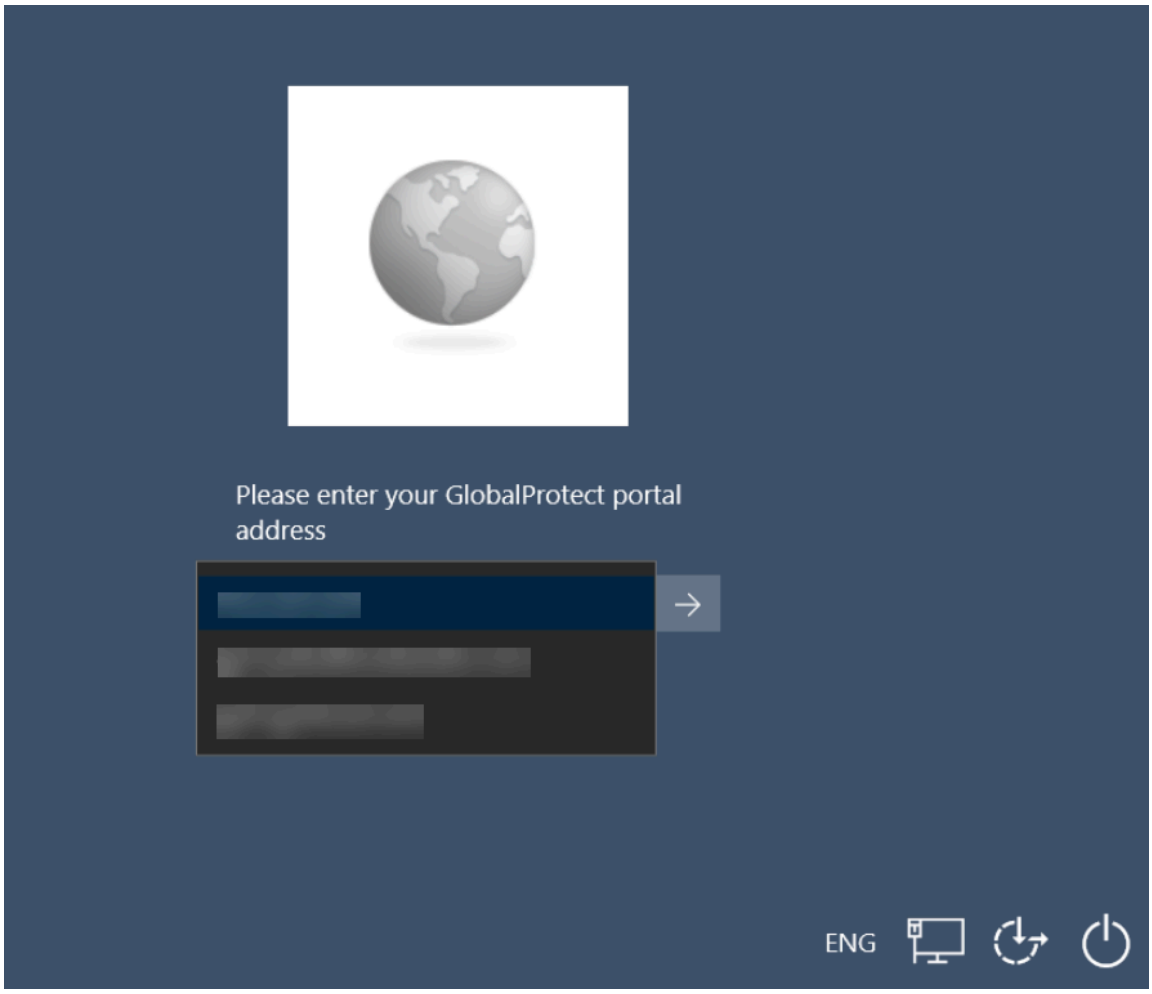
   VPN接続が成功すると、Windowsログオン画面のネットワークサインインボタンの隣に切断()ボタンが表示されます。設定された時間内にエンドポイントにログインして

いない場合、VPNからログアウトされます。これにより、VPNトンネルが切断されます。

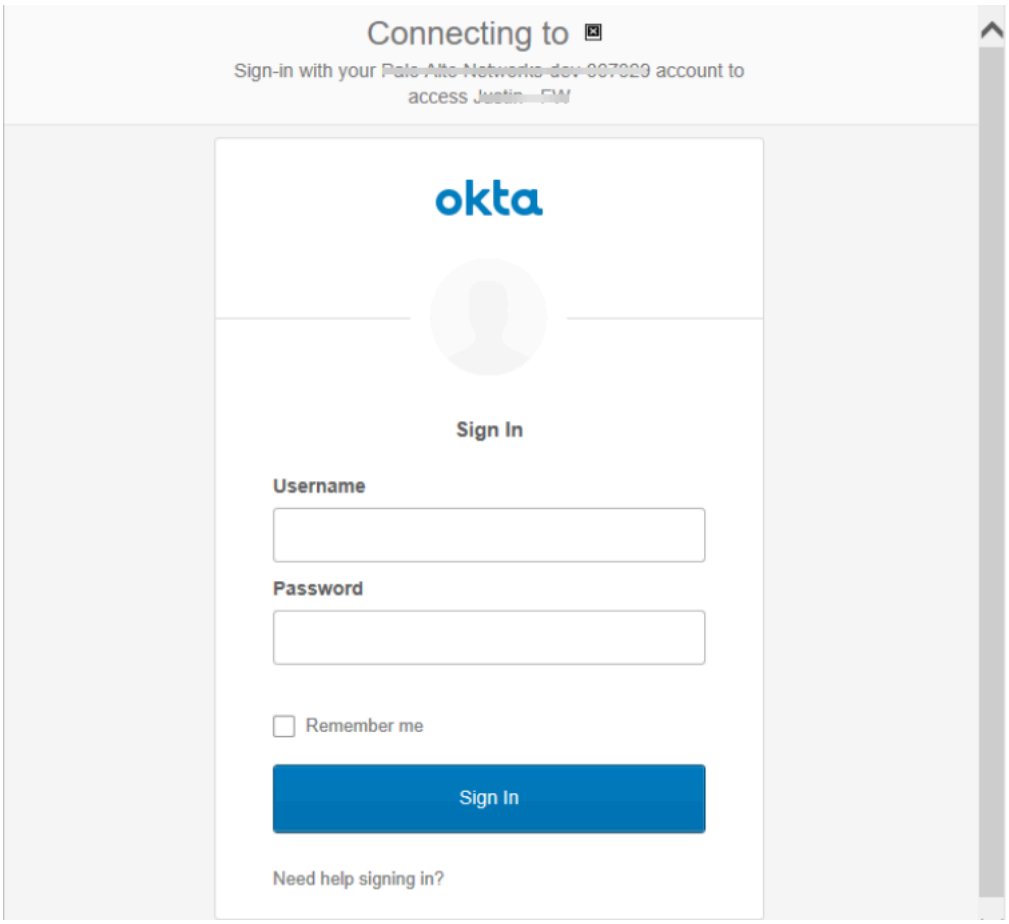
2. (オプション)エンドポイントに初めてログインする場合で、ポータルが管理者によって事前に定義されていない場合は、GlobalProtectポータルのFQDNまたはIPアドレスを入力し、矢印をクリックして送信します。



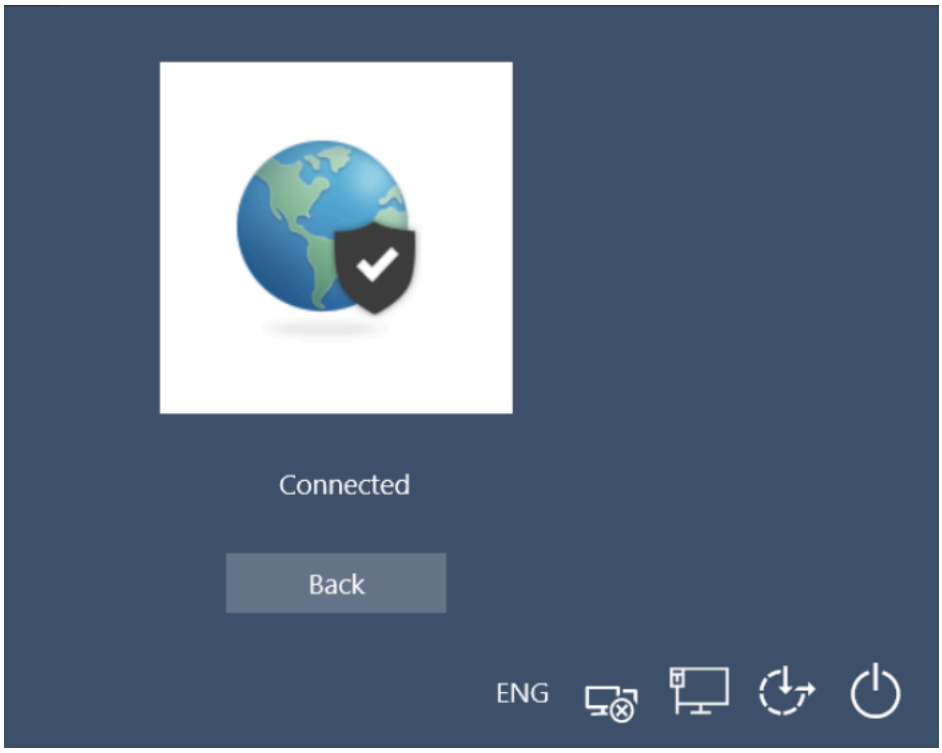
3. (オプション)エンドポイントに初めてログインする場合で、ポータルが管理者によって事前に定義されている場合は、ポータルドロップダウンからポータルを選択し、矢印をクリックして送信します。



4. IdPに認証するためにユーザー名とパスワードを入力し、次にサインインをクリックします。



5. 認証が成功すると、接続ステータスは成功したVPN接続時に接続済みと表示されます。戻るをクリックしてWindowsログオン画面を表示します。



STEP 3 | GlobalProtectゲートウェイに接続されていることを確認します。

1. 再度Windowsエンドポイントにログインします。Windowsログオン画面の右下隅にあるネットワークサインイン( )ボタンをクリックします。
2. ステータス パネルが開きます。デフォルトでは、最適な利用可能ゲートウェイに自動的に接続されます。

ユーザー名/パスワードベースの認証を使用した Connect Before Logon (ログイン前接続)

ログオン前接続は、LDAP、RADIUS、またはOTPなどの認証サービスを使用してユーザーがログインするためのユーザー名/パスワードベースの認証をサポートします。ユーザー名とパスワードの資格情報を使用して、Windowsエンドポイントにログインする前にGlobalProtectに認証できます。ユーザー名/パスワードベースの認証が成功した場合、GlobalProtectは構成で指定されたポータルまたはゲートウェイに接続します。

STEP 1 | ログオン前に接続を使用する前に、管理者は次のタスクを完了している必要があります:

1. Windowsレジストリへログオン前の接続設定をデプロイします。
2. GlobalProtectポータルへのアクセスを設定して、エンドユーザーが資格情報を使用してポータルに認証できるようにします。
3. GlobalProtectゲートウェイを構成して、エンドユーザーが資格情報を使用してゲートウェイに認証できるようにします。

ログオン前接続は、カスタム認証メッセージをサポートしていません。

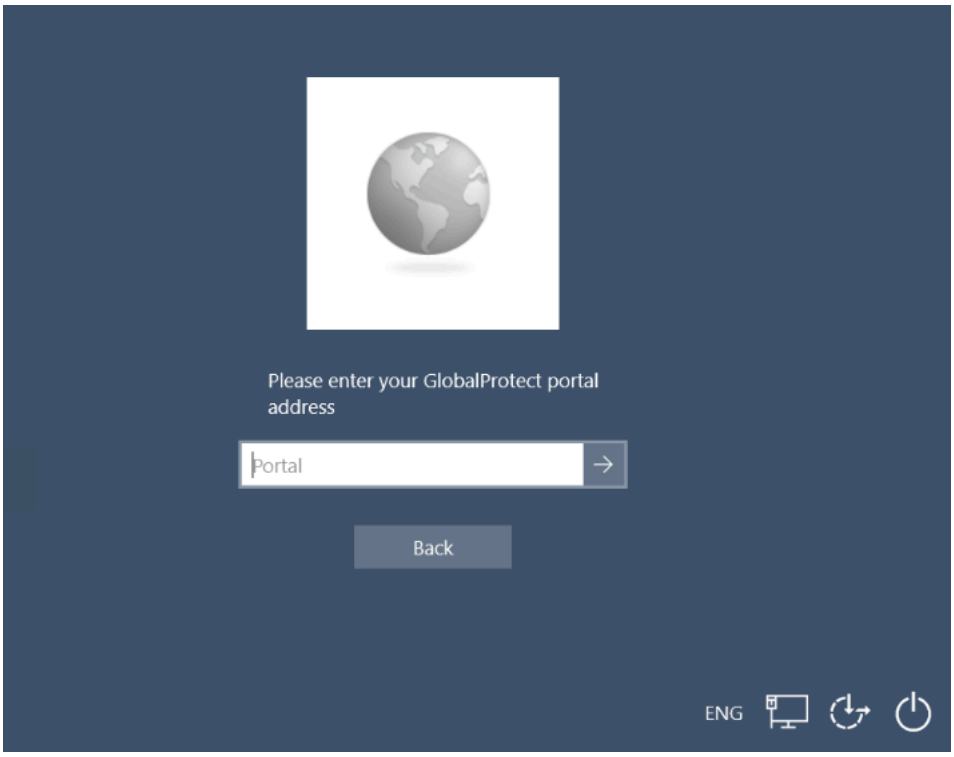
STEP 2 | Windowsエンドポイントにログインするには、ログオン前に接続します。

1. Windowsログオン画面の右下隅にあるネットワークサインイン()ボタンをクリックします。

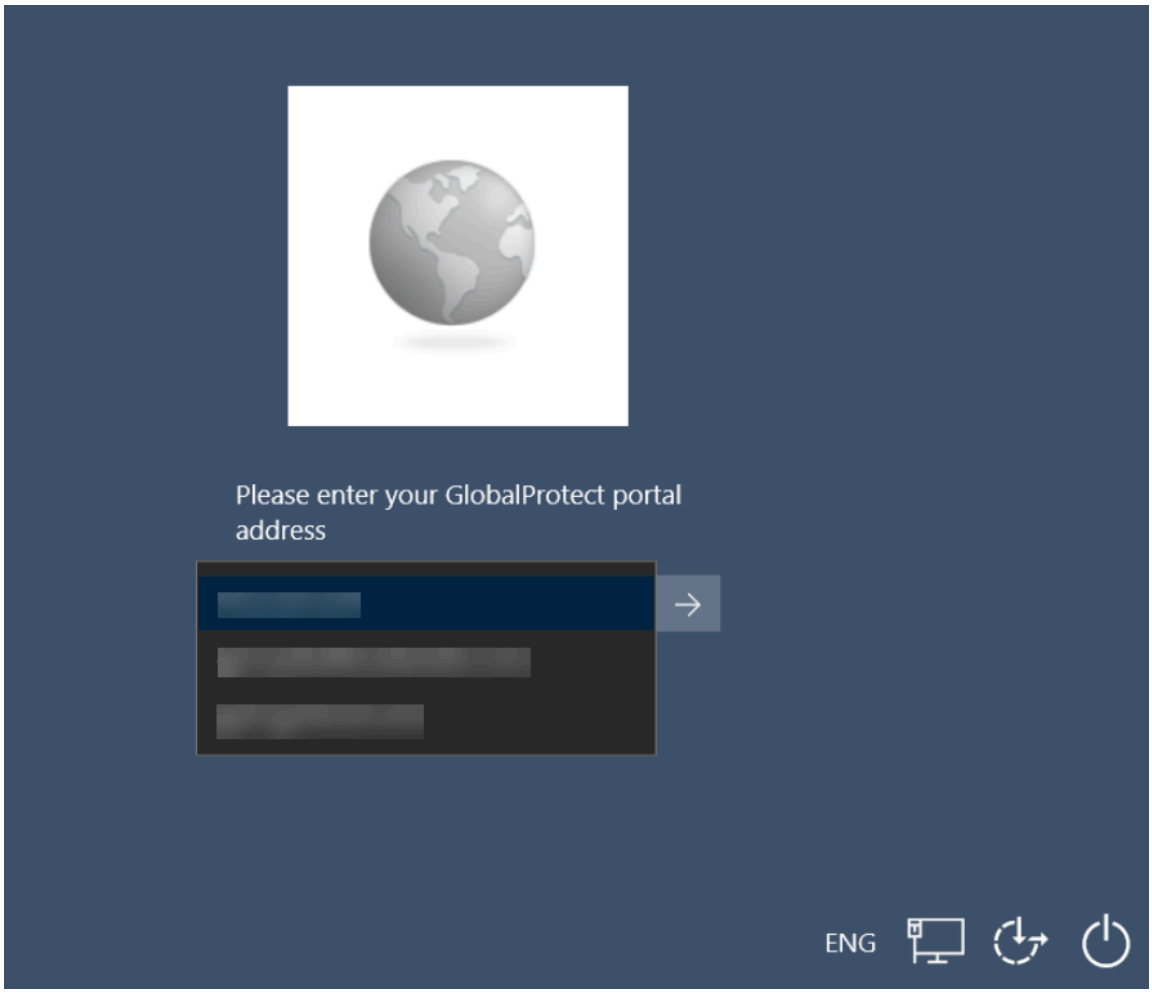
   VPN接続が成功すると、Windowsログオン画面のネットワークサインインボタンの隣に切断()ボタンが表示されます。設定された時間内にエンドポイントにログインして

いない場合、VPNからログアウトされます。これにより、VPNトンネルが切断されます。

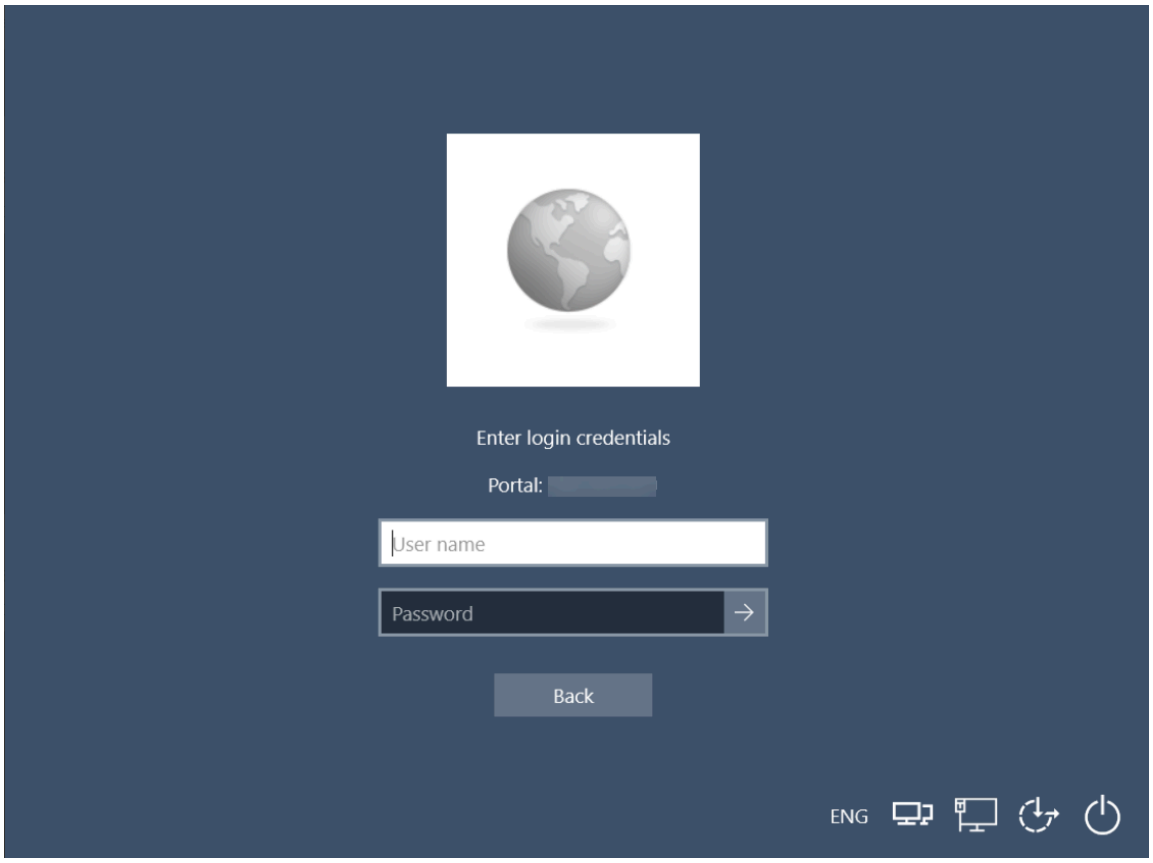
2. (オプション)エンドポイントに初めてログインする場合で、ポータルが管理者によって事前に定義されていない場合は、GlobalProtectポータルのFQDNまたはIPアドレスを入力し、矢印をクリックして送信します。



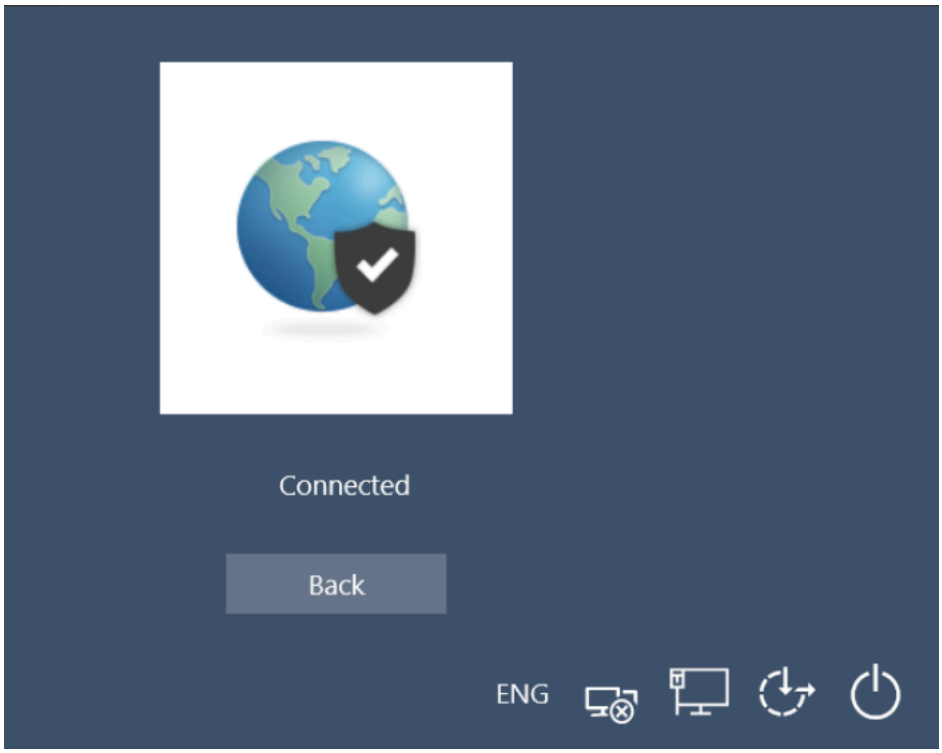
3. (オプション)エンドポイントに初めてログインする場合で、ポータルが管理者によって事前に定義されている場合は、ポータルドロップダウンからポータルを選択し、矢印をクリックして送信します。



4. ユーザー名とパスワードを入力し、矢印をクリックして送信します。



5. 認証が成功すると、接続ステータスは成功したVPN接続時に接続済みと表示されます。戻るをクリックしてWindowsログオン画面を表示します。



STEP 3 | GlobalProtectゲートウェイに接続されていることを確認します。

1. 再度Windowsエンドポイントにログインします。Windowsログオン画面の右下隅にあるネットワークサインイン( )ボタンをクリックします。
2. ステータス パネルが開きます。デフォルトでは、最適な利用可能ゲートウェイに自動的に接続されます。

Smart Card認証にシングルサインオンを使用

どこで使用できますか?	何が必要ですか?
• Windows エンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

管理者がスマート カード認証を使用してシングルサインオン(SSO)を使用してユーザーを認証するようにGlobalProtectポータルを構成した場合、シームレスなSSOエクスペリエンスを実現するために、GlobalProtectアプリでスマート カードの個人識別番号(PIN)を再入力しなくても接続できます。Windowsエンドポイントで同じスマート カードPINをGlobalProtectに利用できます。SSOを使用してスマートカード認証を行うと、ログイン時にスマートカードの暗証番号を入力する回数を減らすことができます。エンドユーザーがWindowsエンドポイントに正常にログインすると、GlobalProtectアプリは、スマート カードPINを取得して記憶し、GlobalProtectポータルとゲートウェイで認証します。

管理者は、スマートカードプロバイダの*PIN*に関連付けられる*Windows*のPINキャッシュポリシーのタイプを定義できます。暗証番号は、スマートカードプロバイダーから許可された場合にのみキャッシュされます。*GlobalProtect*は、*GlobalProtect*アプリから手動でサインアウトした場合、*Windows*からサインアウトした場合、または*PIN*が変更された場合に、キャッシュから*PIN*をクリアします。

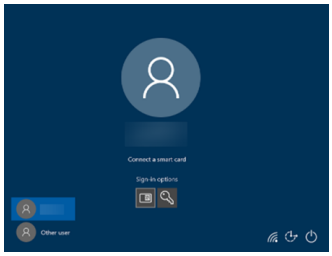
STEP 1 | SSOを使用してスマートカード認証を行うには、管理者が次の作業を完了している必要があります。

1. スマートカード認証にSSOを使用するように、Windowsエンドポイントに事前導入された設定を行います。

   管理者は、スマートカードPINのSSOを有効にする前に、Windowsエンドポイントに導入前設定を行う必要があります。GlobalProtect は、GlobalProtect アプリが初期化されるときに、このエントリを 1 回だけ取得します。
2. スマートカードを二要素認証用にセットアップします。
3. 証明書プロファイルをGlobalProtectポータルに割り当てます。
4. スマートカードを使用して認証できるようにゲートウェイを設定します。
5. GlobalProtectポータルでGlobalProtectアプリがSSOを使用できるようにして、WindowsエンドポイントでGlobalProtectに同じスマートカードPINを活用できるようにします。

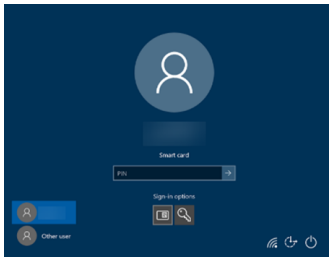
STEP 2 | スマートカードの暗証番号を使用してWindowsエンドポイントにログインします。

1. サインインオプションをクリックし、スマートカード ( )ボタンをクリックします。
2. プロンプトが表示されたら、スマートカードを挿入して、スマートカード認証が成功したことを確認します。



3. スマートカードの暗証番号を入力し、矢印をクリックして送信します。

   スマートカード認証が成功すると、スマートカードの暗証番号を再入力しなくても、設定で指定したポータルまたはゲートウェイに接続できます。

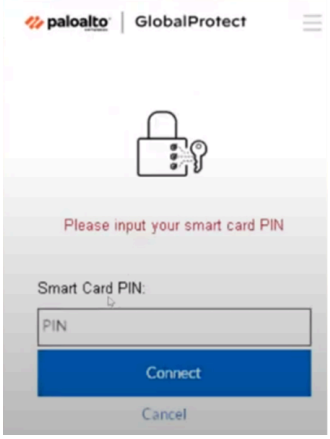


STEP 3 | (オプション)同じスマートカードの暗証番号を使用してGlobalProtectにログインします。

Windowsエンドポイントへのログインに使用したのと同じスマートカードのPINを活用できます。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. ハンバーガーメニューをクリックして設定パネルを開きます。
3. 設定パネルでサインアウトし、GlobalProtectアプリから保存したユーザー資格情報を消去します。
4. 同じスマートカードのPINでGlobalProtectに再接続します。

   GlobalProtectアプリは、PINが有効でない場合、スマートカードのPINエラーを表示します。



GlobalProtect App for Windowsの使用

どこで使用できますか?	何が必要ですか?
• Windows エンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

この章は、エンドポイントにログインした後にGlobalProtectのログイン資格情報を入力する必要がある場合にのみ適用されます(シングルサインオンは無効です)。

通常、組織にはGlobalProtectユーザーがアプリのインストール後に透過的にログインできるようにすることを推奨します。透過的なGlobalProtectログインでエンドポイントにログインすると、GlobalProtectアプリは自動的に起動し、さらなるユーザーの介入なしに企業ネットワークに接続します。

設定でGlobalProtectの資格情報を入力する必要がある場合は、以下の適用可能な手順に従ってください。

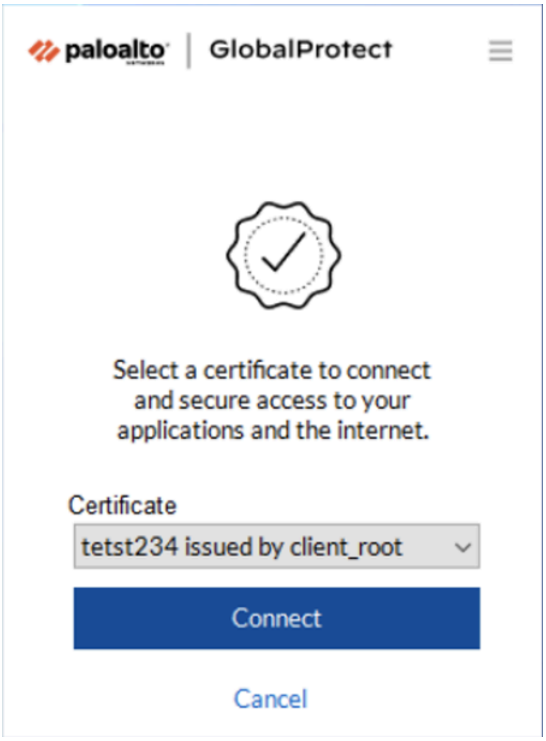
STEP 1 | GlobalProtect にログインします。

エンドポイントに初めてログインする場合、GlobalProtectアプリはログインに成功するとフレンドリーなウェルカムページを表示します。**[Get Started (開始する)]**をクリックしてください。

1. (オプション)管理者がオンデマンド接続方法でGlobalProtectを構成し、初めてGlobalProtectにログインする場合は、ポータルまたはゲートウェイに認証するため

に、証明書のドロップダウンから有効な証明書のリストからクライアント証明書を選択してください。

2. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。



3. (オプション)管理者から内部リソースにアクセスするページを表示するよう要求された場合は、GlobalProtectに接続する前に会社の利用規約を確認してください。

   利用規約に同意しない場合、GlobalProtectに接続できません。

   オプションで、キャンセルをクリックした場合は、GlobalProtectポータルのIPアドレス(またはドメイン)を入力し、接続をクリックして接続を開始する必要があります。

4. GlobalProtect管理者が指定したポータルのIPアドレスまたはドメインを入力し、接続をクリックします。

5. (オプション)デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available** (利用可能な最適な接続)ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、Change Gateway (ゲートウェイの変更)ドロップダウンからゲートウェイを選択します(外部ゲートウェイ専用)。

   このオプションは、管理者が手動ゲートウェイ選択を有効にした場合にのみ利用可能です。

6. (オプション)接続モードに応じて、**Connect** (接続)をクリックして接続を開始します。
7. (オプション)プロンプトが表示されたら、**Username** (ユーザー名)と**Password** (パスワード)を入力して**Sign In** (サインイン)をクリックします。

   管理者が生体認証(指紋)情報を使用してサインインすることを許可している場合は、最初にユーザ名とパスワードを使用して2回(1回は保存して再度認証)サインインする必要があります。その後、生体認証情報を使用してサインインできます。

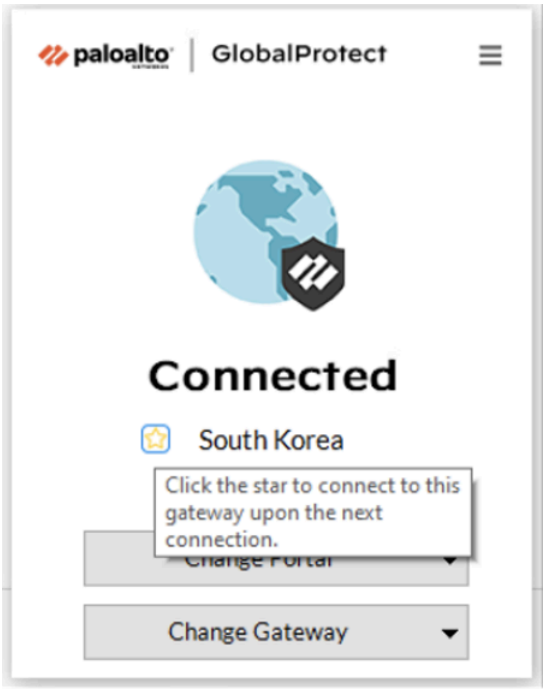
   認証に成功したら、企業のネットワークに接続され、ステータス パネルに **Connected**（接続済み）または **Connected - Internal**（接続済み - 内部）ステータスが表示されます。管理者がGlobalProtectウェルカムページを設定している場合、ログインに成功したことが表示されます。

STEP 2 | GlobalProtectポータルまたはゲートウェイに接続します。

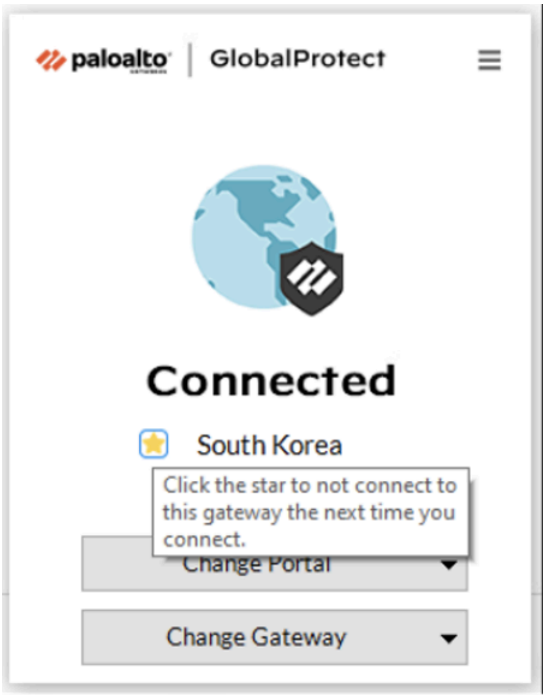
*GlobalProtect*システムトレイアイコンを確認することで、接続されているかどうかを判断できます。接続されていない場合、アイコンは灰色()で、アイコンにカーソルを合わせると接続されていませんと表示されます。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. (オプション)初めてGlobalProtectアプリにログインする場合は、GlobalProtectポータルのIPアドレスまたはドメインを入力し、次に接続をクリックしてください。
3. (オプション)アプリに複数のポータルが保存されている場合は、ポータルの変更ドロップダウンからポータルを選択します。デフォルトでは、最後に接続したポータルがポータルの変更ドロップダウンから事前に選択されています。
4. （オプション）デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available**（利用可能な最適な接続）ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、ゲートウェイの変更ドロップダウンをクリックし、次のいずれかのオプションを使用します。
   - ゲートウェイを手動で選択します(外部ゲートウェイのみ)。このオプションは、管理者が手動ゲートウェイ選択を有効にした場合にのみ利用可能です。

- 優先ゲートウェイに割り当てて自動的に接続します:
  1. 優先ゲートウェイを指定するには、星のアイコンをクリックします(　)。次回接続すると、指定した優先ゲートウェイに自動的に接続されます。



後でこのゲートウェイを優先ゲートウェイとして使用しないことに決めた場合は、星のアイコンをクリアできます。次回接続すると、最適な利用可能なゲートウェイに自動的に接続されます。



2. デフォルトでは、ゲートウェイ変更ドロップダウンからチェックマークで識別される利用可能な最適な接続ゲートウェイに自動的に接続します。優先ゲートウェイを設定すると、ゲートウェイの変更ドロップダウンから星付きゲートウェイの横に星が表示されます。

   管理者がポータルエージェント設定で手動の外部ゲートウェイを構成した場合、ゲートウェイ検索フィールドを使用して特定のゲートウェイを選択できます。

5. （オプション）接続モードに応じて、**Connect**（接続）をクリックして接続を開始します。
6. (オプション)プロンプトが表示されたら、**Username (**ユーザー名)と**Password (**パスワード)を入力して**Connect (**接続)をクリックします。

   管理者が生体認証(指紋)情報を使用してサインインすることを許可している場合は、最初にユーザ名とパスワードを使用して2回(1回は保存して再度認証)サインインする必要があります。その後、生体認証情報を使用してサインインできます。

アプリが外部モードで接続すると、GlobalProtectシステムトレイアイコンにシールド()が表示され、アイコンにカーソルを合わせると接続済みが表示されます。アプリが内部モードで接続すると、GlobalProtectシステムトレイのアイコンに家()が表示され、アイコンにカーソルを合わせると内部ネットワークが表示されます。

STEP 3 | GlobalProtectアプリケーションを開きます。

GlobalProtectシステム トレイ アイコンをクリックして、アプリ インターフェースを起動します。

GlobalProtect アプリのインストール中に、管理者がAutonomous DEM (ADEM)エンドポイントエージェントをインストールするようにポータルを設定し、テストを有効にすることを許可しているか、または許可していない場合、通知が表示されます。管理者がADEMエンドポイント エージェントをすでにインストールしていて、後でADEMエンドポイント エージェントをアンインストールするようにポータルを設定している場合は、次回のログイン時に通知が表示されます。

STEP 4 | ネットワーク接続に関する情報を表示します。

アプリを起動したら、ステータスパネルのハンバーガーメニューをクリックして設定メニューを開きます。設定を選択して**GlobalProtect**設定パネルを開き、次のいずれかの設定を選択してGlobalProtectアプリを表示および変更します。

- 接続–接続タブには、GlobalProtectアカウントに関連付けられたポータルが表示されます。このタブからポータルを追加、編集、または削除できます。このタブには、接続しているゲートウェイも表示されます。管理者が GlobalProtect ポータルエージェントの設定

で高度なビューを許可するをはいに設定すると、ゲートウェイに関する接続統計(ゲートウェイのIPアドレス、場所、VPNセッションの稼働時間など)を表示できます。

接続タブには、ログインの有効期限のカウントダウンタイマーも表示されます。

GlobalProtect for Always-On Internet Security 機能の[Explicit Proxy Connectivity]がPrisma Accessを通じてアプリで有効になっている場合、接続タブにプロキシの詳細が表示されます。

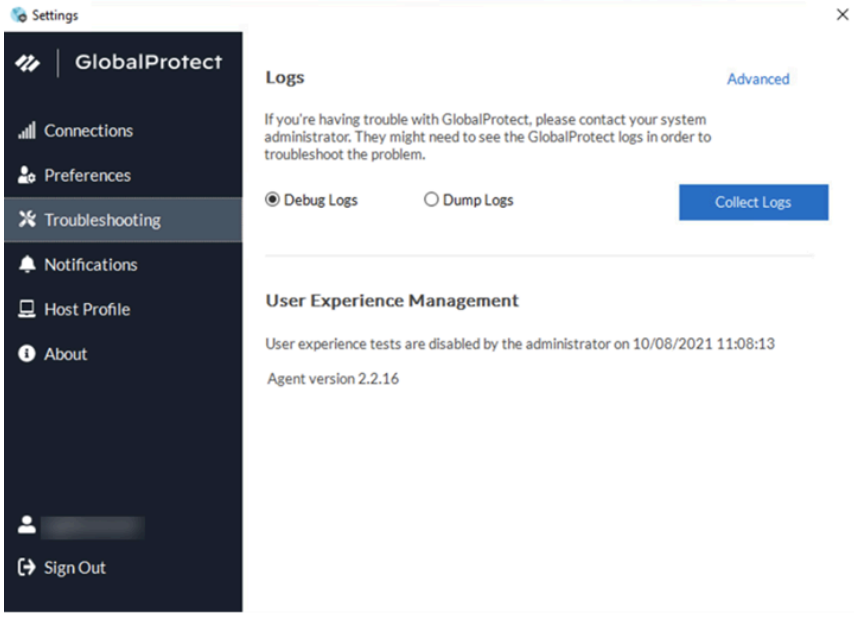
プロキシモード:

- プリファレンス–管理者が次のオプションの少なくとも1つを設定した場合にのみ、プリファレンスタブを使用できるようになりました。
  - 生体認証サインインを有効にする–生体認証(指紋)情報を使用してサインインすることを選択できます。このオプションは、管理者がGlobalProtectエージェント構成でユーザー資格情報を保存をユーザーフィンガープリントでのみに構成している場合にのみ使用できます。GlobalProtectポータルとゲートウェイへの認証の際に、保存されたパスワードを認証に使用するために、エンドポイントの信頼できる指紋テンプレートと一致する指紋を提供する必要があります。
  - 接続が成功するたびにウェルカムページを表示しない:ログインが成功したときにウェルカムページを表示するように選択できます。このオプションは、管理者がGlobalProtect ポータルエージェント設定でようこそページを工場出荷時に設定している場合にのみ使用できます。
  - **SSL**で接続–SSLを使用するか、IPSecのままにするかを選択できます。このオプションは、管理者がGlobalProtectポータルエージェントの設定で**SSL**のみ接続をユーザーが変更できるに設定している場合にのみ使用できます。
  - 常に診断テストを実行し、ログを含める–GlobalProtectアプリが診断テストを実行できるようにするか、診断ログを含めるかを選択できます。このオプションは、管理者がGlobalProtectポータルでトラブルシューティングのためのGlobalProtectアプリログ収集を有効にしている場合にのみ使用できます。

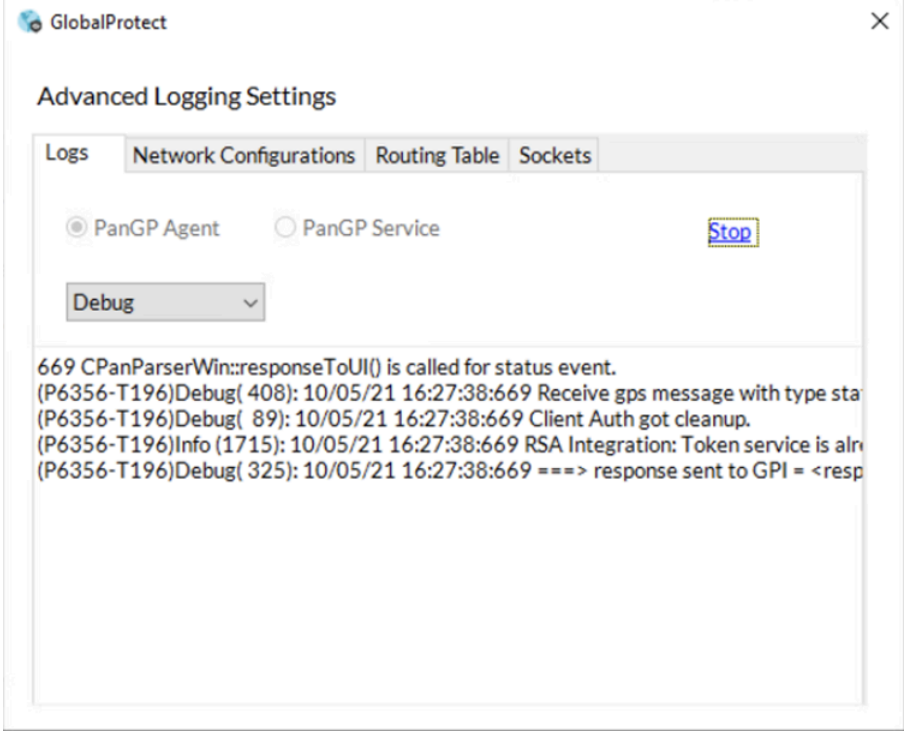
- トラブルシューティングートラブルシューティングタブでは、ログの収集、ログレベルの設定(デバッグ ログまたはダンプ ログ)、およびオプションでユーザ エクスペリエンス テストの有効化を行うことができます。

  詳細な分析のために、*GlobalProtect*アプリがトラブルシューティング ログ、診断ログ、またはその両方をStrata Logging Serviceに送信するには、トラブルシューティング用の GlobalProtect アプリログコレクションを有効にするようにGlobalProtectポータルを構成する必要があります。また、 HTTPS ベースの送信先 URL を構成 には、プローブする *Web* サーバー/リソースの *IP* アドレスまたは完全修飾ドメイン名を含めることができ、エンド ユーザーのエンドポイントでの待機時間やネットワーク パフォーマンスなどの問題を特定できます。

  詳細設定をクリックすると、エンドポイントに関する詳細情報を表示できます。



  ログの詳細設定ウィンドウには、ネットワーク設定、ルート設定、アクティブな接続、およびログに関する情報が表示されます。



GlobalProtectが接続されているとき、GlobalProtectアプリにユーザーエクスペリエンステストを有効にするチェックボックスが表示されている場合、Autonomous DEM (ADEM)エンドポイントエージェントがユーザーエクスペリエンステストを実行できることを確認できます。または、管理者がGlobalProtectアプリのインストール中にADEMエンドポイントエージェントをインストールしたが、GlobalProtectアプリからユーザーエクスペリエンステストを有効または無効にすることができない場合、メッセージが表示されることを確認できます。デフォルトでは、GlobalProtectが無効または切断された場合でも、ハートビートアラートはADEMに転送されます。

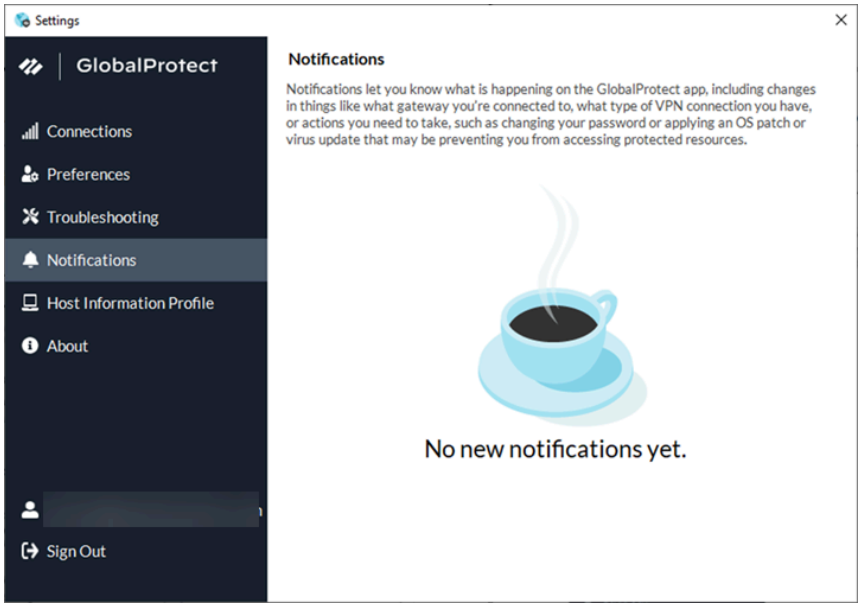
管理者がGlobalProtectアプリのインストール中に自律型 DEM エンドポイントエージェントをインストールするようにポータルを構成し、テストを有効にすることを許可している場合は 、GlobalProtectアプリでユーザーエクスペリエンステストを有効にするチェックボックスをオンにします。このチェックボックスは、管理者がGlobalProtectアプリからユーザーエクスペリエンステストの有効化または無効化を許可していない場合には表示されません。代わりにメッセージが表示され、アプリがユーザーエクスペリエンステストを実行できるように設定されていることを確認します。

ユーザーエクスペリエンステストを有効にするチェックボックスをオンにしない場合でも、ハートビートアラートはADEMに転送されます。

- 通知—通知タブには、GlobalProtectアプリでトリガーされた特定の通知に関する詳細情報が表示されます。ゲートウェイでGlobalProtectアプリセッションの有効期限に関するエン

ドユーザー通知を構成し、アプリ上でこれらのカスタム通知の表示をスケジュールできます。

GlobalProtectアプリでトリガーされた新しい通知がない場合も通知されます。

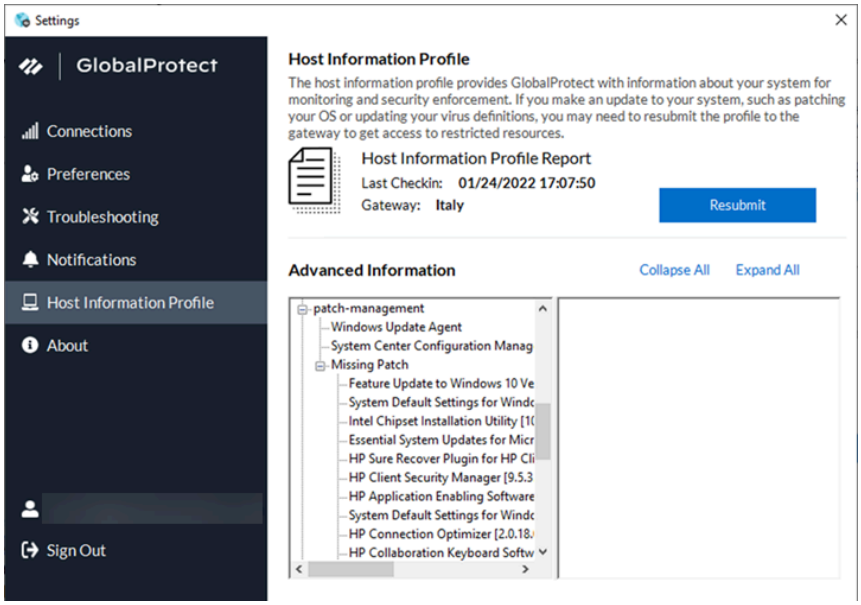


GlobalProtectアプリバージョン6.2.3から、常時接続方式ではセッションタイムアウトメッセージとアイドルタイムアウトメッセージは抑制されます。

GlobalProtectアプリのバージョン6.2から、GlobalProtectアプリのログイン有効期間セッションを期限切れ前に延長して、アプリセッションの突然のログアウトを回避できるようになりました。ログイン有効期間満了通知は、アプリセッションの有効期限が近づくと事前に通知し、セッションから突然ログアウトされないようにユーザーセッションの期間を延長するオプションを提供します。管理者がセッション延長の通知設定を行っている場合、アプリはユーザーセッション延長オプション付きの期限切れ通知を表示します。

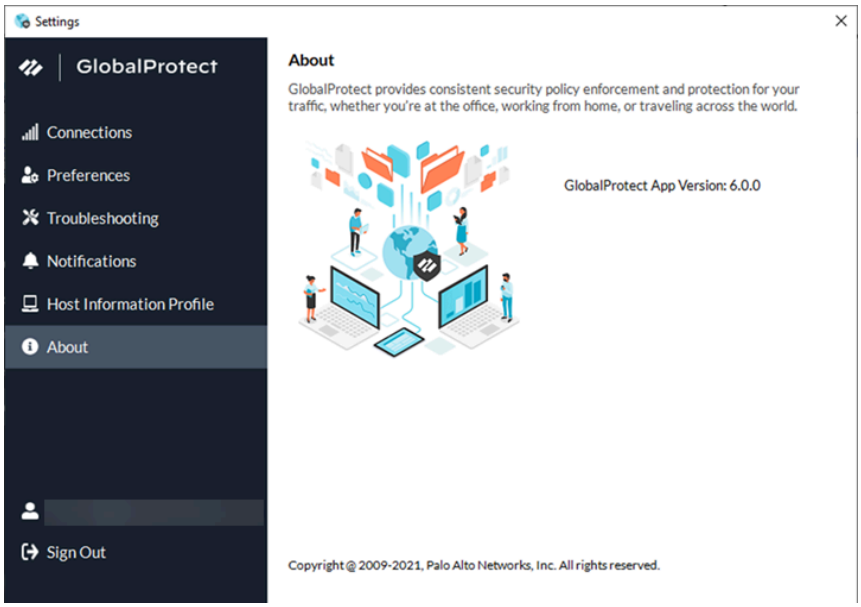
- ホスト情報プロファイル—ホスト情報プロファイルタブは、GlobalProtectがホスト情報プロファイルを使用してセキュリティポリシーを監視および実施するために使用するエンド

ポイント データを表示します。ゲートウェイにHIPデータを手動で再送信するには、再送信をクリックします。



管理者が複数の内部ゲートウェイを非トンネルモードで設定し、内部ホスト検出を行っている場合は、詳細をクリックして、各ゲートウェイのHost Information Profile (HIP)レポート提出を中央から監視し、HIP関連の問題の迅速なトラブルシューティングに役立てることができます。

- 概要–概要タブは、エンドポイントに現在インストールされているGlobalProtectのバージョンを表示し、更新を確認することができます。



STEP 5 | (オプション)新しいパスワードを使用してログインします。

*GlobalProtect*管理者が*GlobalProtect*ポータルエージェントをユーザー資格情報を保存に設定すると、資格情報は自動的に*GlobalProtect*アプリに保存されます。企業ネットワークにアクセスするためのパスワードが変更された場合、新しいパスワードを使用して*GlobalProtect*にログインする必要があります。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. ハンバーガーメニューをクリックして設定メニューを開きます。
3. **Settings**（設定）を選択して、**GlobalProtect Settings**（**GlobalProtect** 設定）パネルを開きます。
4. **GlobalProtect**設定パネルで、サインアウトして、保存したユーザー資格情報をGlobalProtectアプリからクリアします。
5. ユーザー資格情報をクリアした後、新しいユーザー名とパスワードでGlobalProtectに再接続できます。

STEP 6 | (オプション) GlobalProtectから切断します。

管理者がオンデマンド接続方法でGlobalProtectを設定した場合、ステータスパネルの切断をクリックすることでGlobalProtectから切断できます。

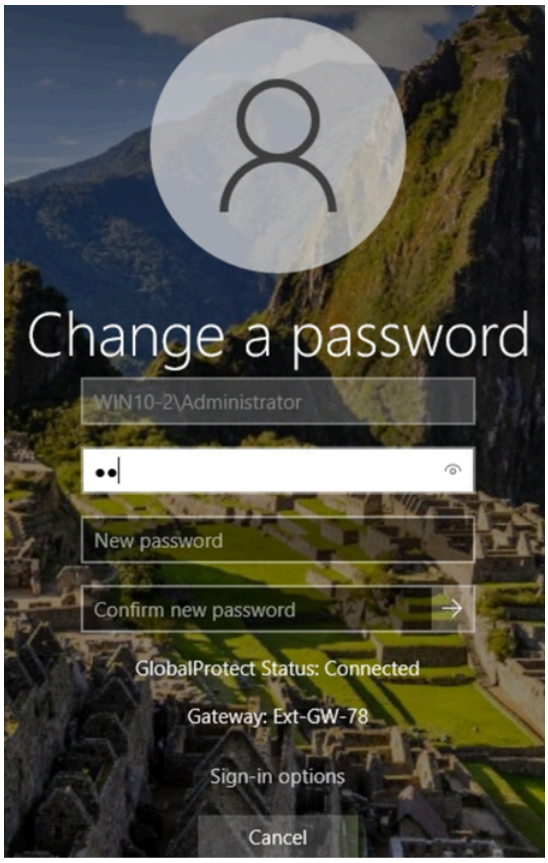
Windowsログオン画面でのGlobalProtectのパスワード表示

Windows 10またはWindows 11デスクトップにログインする際、またはパスワードを変更する際に、パスワードを表示アイコンをクリックして、入力中のパスワードを表示できます。パスワードはプレーンテキストで表示されます。この機能は入力ミスを防ぎ、パスワードを視覚的に確認できることでアカウントのロックアウトのリスクを減らします。

この機能はGlobalProtect™ 6.3.3以降で利用可能で、レジストリキーを介して有効にできます。レジストリキーの詳細については、アプリ表示オプションを参照してください。

Windowsログイン画面には、パスワードフィールド内のパスワード表示アイコンに加えて、GlobalProtectの接続状況とゲートウェイが表示されます。

パスワード変更ダイアログボックスには、ユーザー名、ドメイン名、GlobalProtectの接続状況、ゲートウェイに加えて、パスワードフィールド内のパスワード表示アイコンが表示されます。



Windows用GlobalProtectアプリからの問題を報告する

どこで使用できますか?	何が必要ですか?
• Windows エンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

ネットワーク パフォーマンスが低下したり、ポータルやゲートウェイとの接続が確立されなかったりするなどの異常な動作が発生した場合は、管理者がアクセスできるStrata Logging Serviceに直接問題を報告できます。GlobalProtectアプリのログを手動で収集してメールで送信したり、クラウドドライブに保存したりする必要はなくなりました。

*GlobalProtect*アプリに問題を報告するオプションを表示するには、管理者が*GlobalProtect*ポータルでトラブルシューティングのためのGlobalProtectアプリログ収集を有効にする必要があります。

STEP 1 | GlobalProtectポータルまたはゲートウェイに接続します。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. (オプション)GlobalProtectアプリに初めてログインする場合は、GlobalProtectポータルのFQDNまたはIPアドレスを入力し、**[Connect (接続)]**をクリックします。
3. (任意)複数のポータルがアプリに保存されている場合は、[ポータル]ドロップダウンからポータルを選択します。デフォルトでは、最後に接続されたポータルが[ポータル]ドロップダウンから事前に選択されています。
4. （オプション）デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available**（利用可能な最適な接続）ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、ゲートウェイのドロップダウンをクリックします。

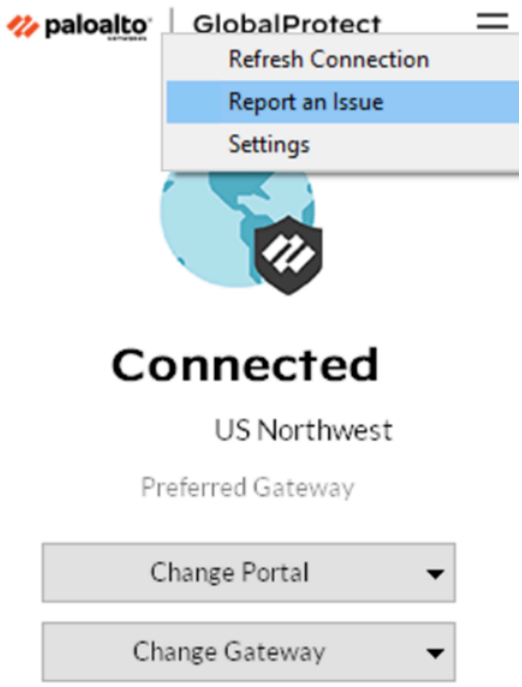
STEP 2 | GlobalProtectアプリケーションを開きます。

GlobalProtectシステム トレイ アイコンをクリックして、アプリ インターフェースを起動します。

STEP 3 | エンドポイントからGlobalProtectアプリケーションから問題を報告します。

アプリを起動したら、ステータスパネルのハンバーガーメニューをクリックして管理者に問題を報告してください。

1. **Report an Issue (**問題の報告**)**を選択します。



2. GlobalProtectアプリが診断テストを実行し、診断ログを含めることを有効にします。診断ログとトラブルシューティングログの両方が収集され、コンパクトなトラブルシューティングレポートとしてStrata Logging Serviceに送信されます。

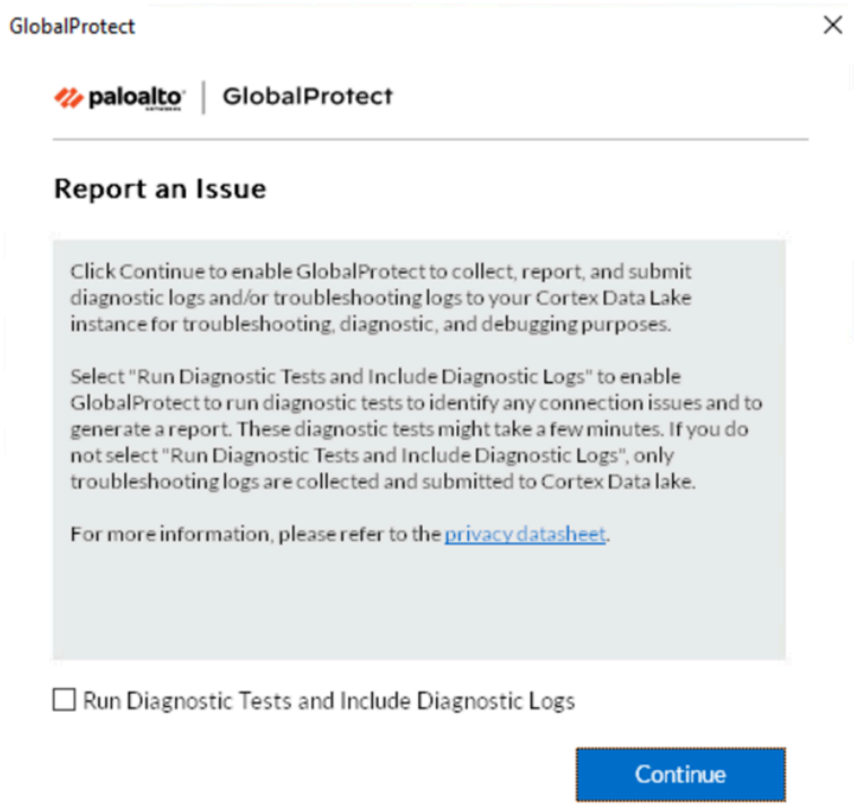
   診断テストが正常に完了した後、GlobalProtectデバッグログファイルがエンドポイントからStrata Logging Serviceにアップロードされます。

   アプリが診断テストを実行し、診断ログを含めることを有効にしない場合、トラブルシューティングログのみが収集され、コンパクトなトラブルシューティングレポートとして*Strata Logging Service*に送信されます。*GlobalProtect*アプリは、`.json`形式で自動的に生成されたレポートファイル*(pan_gp.trb.log*または*pan_gp_trbl.log)*をチェックします。トラブルシューティングログに問題が見つからなかった場合、通知メッセージが表示されます。再試行をクリックして、*pan_gp.trb*.log*ファイルが存在するか確認します。

3. **Run Diagnostic Tests and Include Diagnostic Logs(**診断テストを実行して診断ログを含める**)**チェックボックスを選択します。
4. 続行をクリックして、アプリがトラブルシューティング ログを作成し、管理者のStrata Logging Serviceインスタンスにレポートを送信できるようにします。

   エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。GlobalProtectアプリは、トンネルありまたはトンネルなしで診断テスト

を実行できます。例えば、アプリが接続してトンネルを通じて診断テストを実行する前に、GlobalProtectのログイン資格情報を入力したいかもしれません。



アプリが診断テストを実行していることを確認するメッセージがポップアップしますが、これは**Run Diagnostic Tests and Include Diagnostic Logs (**診断テストを実行して診断ログを含める**)**チェックボックスを選択した場合のみです。

5. 閉じる]をクリックして、アプリがレポートをStrata Logging Serviceに正常に送信したことを確認します。この確認メッセージには、レポートが処理および送信された日時が表示されます。

Windows 10 UWP 用 の GlobalProtect アプリケーションをダウンロードします。

どこで使用できますか?	何が必要ですか?
• Windows エンドポイントのみの場合:	❑ GlobalProtect アプリのバージョン 6.3 以降

管理者が GlobalProtect の接続方法を **Always On** (常時オン)に設定している場合、正当な理由があれば GlobalProtect アプリを切断できます。たとえば、ホテルでGlobalProtect仮想プライベートネットワーク（VPN）が機能しておらず、VPN障害によってインターネットに接続できない場合、アプリを切断したい場合があります。GlobalProtectアプリを切断した後は、セキュアでない通信（VPNなし）を使用してインターネットに接続できます。

GlobalProtect アプリを切断する方法、時間、および回数は、管理者が GlobalProtect サービス(PanGPS)をどのように設定するかによって異なります。この構成では、アプリを完全に切断できないようにしたり、チャレンジに正しく応答した後にのみアプリを切断したりすることができます。

設定にチャレンジが含まれている場合、GlobalProtectアプリは次のいずれかを求めるプロンプトを表示します。

- アプリを切断したい理由
- インターネット速度が遅いやアプリが動作しないなどの理由に応答します(必要な場合)
- パスコード
- チケット番号

チャレンジでパスコードまたはチケット番号が必要な場合は、GlobalProtect 管理者またはヘルプデスク担当者に電話で問い合わせることをお勧めします。

通常、管理者は事前にパスコードを電子メール(GlobalProtectの新規ユーザー用)または組織のウェブサイトに掲載して提供します。また、システム停止やシステム障害が発生した場合には、管理者が電話でパスコードを提供することもあります。

有効なチケット番号を取得する前に、エンドポイントにチケット要求番号が表示されます。この番号は、GlobalProtect管理者またはヘルプデスク担当者に通知しなければなりません。切断リクエストが承認されると、GlobalProtectを切断するために使用できる有効なチケット番号が届きます。

次の手順では、アプリを切断してチャレンジを渡す方法について説明します。

STEP 1 | GlobalProtectアプリの接続を解除します。

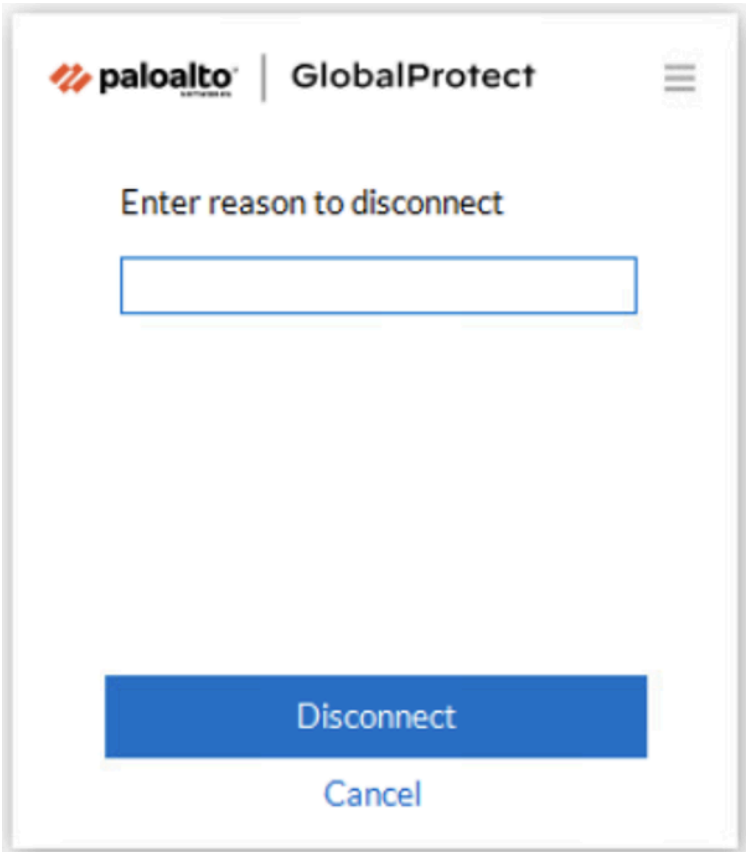
1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. ハンバーガーメニューをクリックして設定メニューを開きます。
3. **[Disconnect (接続解除)]**を選択します。

[Disconnect (接続解除)]オプションは、*GlobalProtect*エージェント構成でアプリケーションの切断が許可されている場合にのみ表示されます。構成で、チャレンジに応答することなく *GlobalProtect* アプリを切断できる場合、*GlobalProtect* アプリは追加のアクションを必要とせずに終了します。

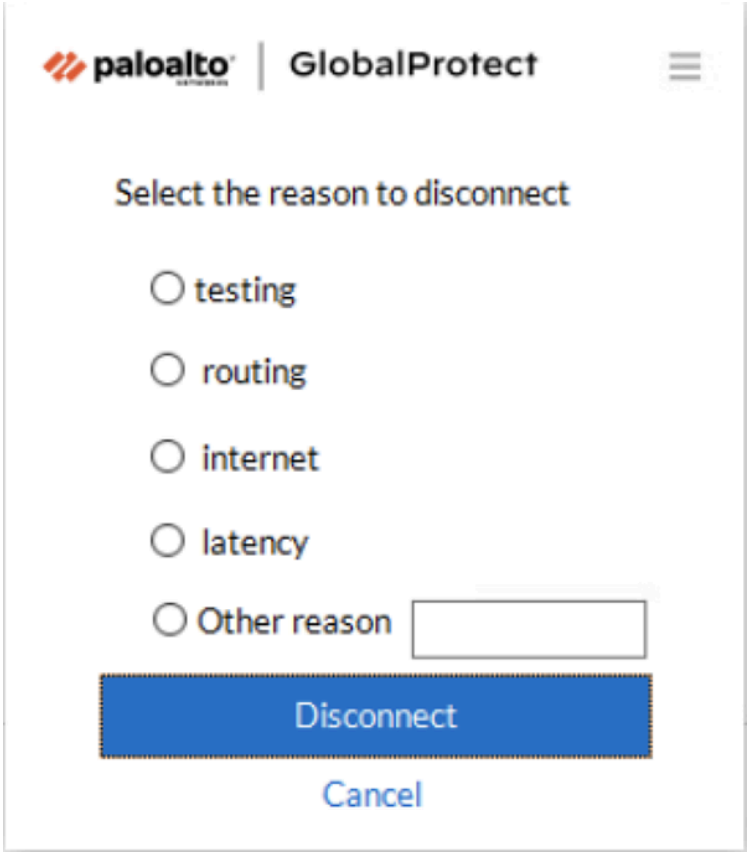
STEP 2 | 必要に応じて、1つ以上の課題に対応します。

プロンプトが表示されたら、次の情報を入力します。

- **Tell us the issue to disconnect (**問題を教えてください**)**—GlobalProtectアプリを切断する理由。



- **Select the reason to disconnect (**切断する理由を選択してください**)**—構成により、1つ以上の理由に応答する必要がある場合や別の理由を入力する必要がある場合、GlobalProtectアプリは接続解除を選択するとすぐに理由を表示します。



- **Passcode (**パスコード**)** – 通常、アプリケーションを無効にする必要のある既知の問題またはイベントに基づいて、管理者が事前に提供するパスコード。
- **Ticket (**チケット**)**–構成によりチケット番号を提供する必要がある場合、GlobalProtectアプリは接続解除を選択するとすぐに8文字の16進数のチケットリクエスト番号を表示します。チケット番号でアプリを接続解除するには、管理者またはヘルプデスクの担当者(電話)に連絡し、チケットリクエスト番号を提供してください。リクエストが承認された後、管理者またはヘルプデスクの担当者が8文字の16進数のチケット番号を提供します。チケット番号をチケットフィールドに入力し、次に**OK**をクリックします。

Windows用のGlobalProtect Appをアンインストールする

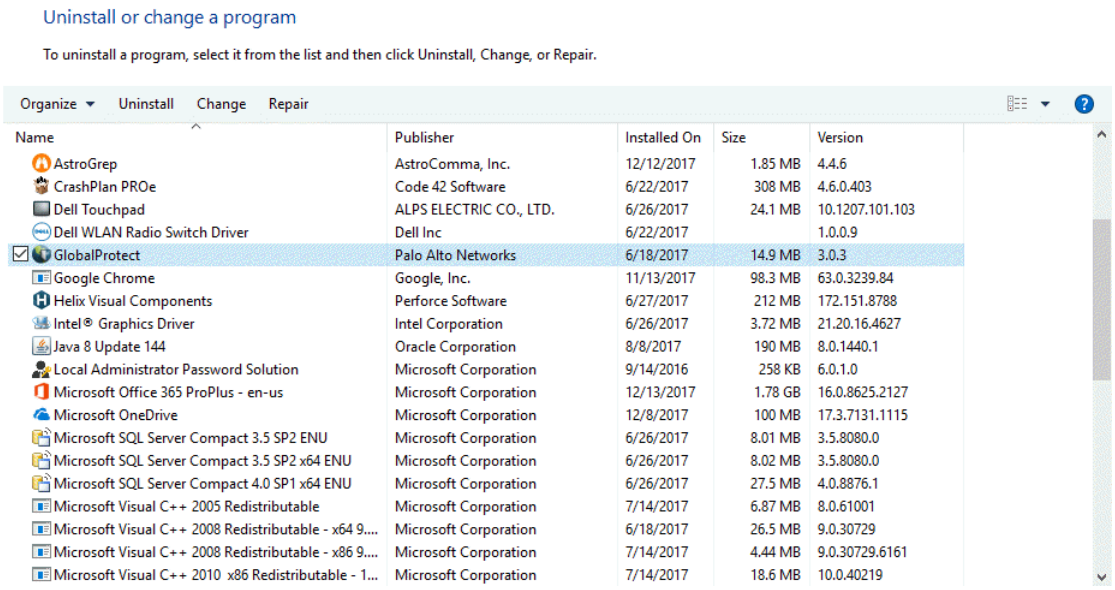
どこで使用できますか?	何が必要ですか?
• Windows エンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

場合、Windows エンドポイントからGlobalProtectアプリケーションをアンインストールするには、以下の手順を実行します。アプリをアンインストールすると、企業ネットワークへのVPNアクセスがなくなり、エンドポイントは会社のセキュリティポリシーによって保護されなくなることに注意してください。

管理者権限を持つユーザーのみが*Windows*エンドポイントから*GlobalProtect*アプリケーションをアンインストールできます。

STEP 1 | **[Start (スタート) > [Control Panel (コントロールパネル) > [Programs (プログラム) > [Programs and Features (プログラムと機能)**の順に選択します。

STEP 2 | リストから **GlobalProtect**を選択し、**[Uninstall (アンインストール)]**をクリックします。



STEP 3 | アンインストールを続行するかどうかの確認メッセージが表示されたら、はいをクリックします。

Microsoft Installerの競合を修正する

どこで使用できますか?	何が必要ですか?
• Windows エンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtectポータルエージェントの設定で**GlobalProtect**をネットワークアクセスに強制するを有効にし、その後Windowsエンドポイントを新しいバージョンのGlobalProtectアプリにアップグレードすると、インストールが失敗し、強制設定がすべてのトラフィックをブロックする可能性があります。

この問題は、複数のMicrosoftインストーラー（`msiexec.exe`）インスタンスがWindowsエンドポイントで同時に実行されるときに発生するOSの制限によって引き起こされます。Microsoftインストーラーの競合を解決するには、次の手順を使用する必要があります:

STEP 1 | エンドポイントを再起動します。

STEP 2 | バックグラウンドで実行中のすべてのサードパーティインストーラーを停止します。

1. **Ctrl+Alt+Delete**を押し、次にタスクマネージャーをクリックします。
2. タスクマネージャーで、現在実行中のすべてのサードパーティの`msiexec`プログラムを見つけます(例：**`msiexec`**コマンドライン **`- Google`**検索)。
3. サードパーティのインストーラーを選択し、次にタスクの終了をクリックしてインストーラーを停止します。

STEP 3 | 既存のGlobalProtectのバージョンを復元し、次にアプリの新しいバージョンにアップグレードします。

1. (オプション)必要に応じて、既存の(古い)バージョンのGlobalProtectを再インストールして修復します。アップグレードが引き続き失敗する場合は、このステップが必要です。
2. アップグレードが期待通りに進行することを許可します。

macOS用GlobalProtect アプリ

どこで使用できますか?	何が必要ですか?
• macOS エンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtect™は、デスクトップコンピュータ、ラップトップ、タブレット、またはスマートフォンなどのエンドポイントで実行され、企業ネットワーク内の機密リソースを保護するのと同じセキュリティポリシーを使用してあなたを保護するアプリケーションです。GlobalProtect™は、イントラネット、プライベートクラウド、パブリッククラウド、インターネットトラフィックを保護し、世界中のどこからでも会社のリソースにアクセスできるようにします。

次のトピックでは、GlobalProtect app for macOSをインストールして使用する方法を説明します。

- macOS用GlobalProtectアプリケーションのダウンロードおよびインストール
- GlobalProtect App for macOSの使用
- macOS用のGlobalProtectアプリから問題を報告する
- GlobalProtect App for macOSを無効にする
- macOS用のGlobalProtect Appをアンインストールする
- GlobalProtect Enforcer カーネル拡張機能の削除
- GlobalProtect App for macOSでクライアント証明書を認証に使用できるようにする

macOS用GlobalProtectアプリケーションのダウンロードおよびインストール

どこで使用できますか?	何が必要ですか?
• macOS エンドポイントのみの場合:	❑ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtect ネットワークに接続する前に、macOS エンドポイントに GlobalProtect アプリケーションをダウンロードしてインストールする必要があります。組織の GlobalProtect または Prisma Access のデプロイメントに適したアプリケーションを入手するには、組織内の GlobalProtect ポータルから直接アプリケーションをダウンロードする必要があります。そのため、Palo Alto Networks のサイトでは直接GPアプリをダウンロードできるリンクはありません。

GlobalProtectアプリケーションをダウンロードしてインストールする前に、管理者からGlobalProtectポータルの IP アドレスまたはFQDNを入手する必要があります。さらに、管理者は、ポータルおよびゲートウェイへの接続に使用できるユーザ名とパスワードを確認する必要があります。これは通常、企業ネットワークに接続するときに使用するユーザ名とパスワードと同じです。

macOS Catalina 10.15.4、macOS Big Sur 11 以降を実行している macOS デバイスに GlobalProtect アプリケーションを初めてインストールする場合、または GlobalProtect アプリケーション 5.1.4 にアップグレードする場合は、特定の GlobalProtect 機能に使用するシステム拡張機能を有効にする必要があります。管理者が宛先ドメイン名とアプリケーション プロセス名に基づいて GlobalProtect ゲートウェイにスプリット トンネルを設定した場合、または GlobalProtect ポータルでネットワーク アクセスに GlobalProtect 接続を適用した場合(「GlobalProtect アプリのカスタマイズ」を参照)、インストール中に GlobalProtect アプリに **System Extension Blocked**(システム拡張機能ブロック)通知メッセージが表示されます。このメッセージは、ロードがブロックされている macOS のシステム拡張機能を有効にして許可し、スプリット トンネルおよびEnforce GlobalProtect for Network Access機能を使用するようにユーザーに求めます。

システム拡張機能を使用する場合は、次のガイドラインに従ってください。

- 管理者権限を持つユーザーのみが、*macOS*エンドポイント用の*GlobalProtect*アプリケーションでシステム拡張機能を有効にできます。
- *macOS Catalina 10.15*および*macOS Big Sur 11*のセキュリティ強化により、サードパーティ アプリケーションの使用中にデータが確実に保護されるため、*GlobalProtect*は、*Documents*、*Desktop*、および*Downloads*フォルダとネットワーク ドライブに保存されているファイルとフォルダにアクセスする前に、許可を要求する必要があります。管理者が*HIP*チェックを有効にしている場合、*GlobalProtect*がファイルシステムに保存されている特定のファイルとフォルダへのアクセスを要求すると、*macOS*エンドポイントに新しいアクセス許可ポップアップが表示されます。
- *macOS Catalina 10.15.4*、*macOS Big Sur 11*以降で動作する*GlobalProtect*アプリ*5.1.4*は、カーネル拡張機能を使用せず、システム拡張機能を使用します。
- *macOS Catalina 10.15.4*または*macOS Big Sur 11*以降で実行される*GlobalProtect*アプリ*5.1.4* は、カーネル拡張機能 (***com.paloaltonetworks.kext.pangpd***) を使用せず、代わりに *macOS* が提供する使用可能な utunインターフェースを仮想アダプタとして使用します。
- 以前のリリースから、*macOS Catalina 10.15.4*、*macOS Big Sur 11*以降で実行されている*GlobalProtect*アプリ*5.1.4*にアップグレードする場合、カーネル拡張機能は不要になります。アップグレード後、*GlobalProtect*アプリに ***System Extension Blocked***(システム拡張機能ブロック)通知メッセージが表示され、ロードがブロックされた *macOS* のシステム拡張機能を有効化および許可するようにユーザーに促します。デフォルトでは、アプリはシステム拡張機能をインストールせず、同じデフォルト設定が適用されます。

必要な情報を収集したら、以下の手順に従ってアプリをダウンロードおよびインストールします。

STEP 1 | GlobalProtect ポータルにログインします。

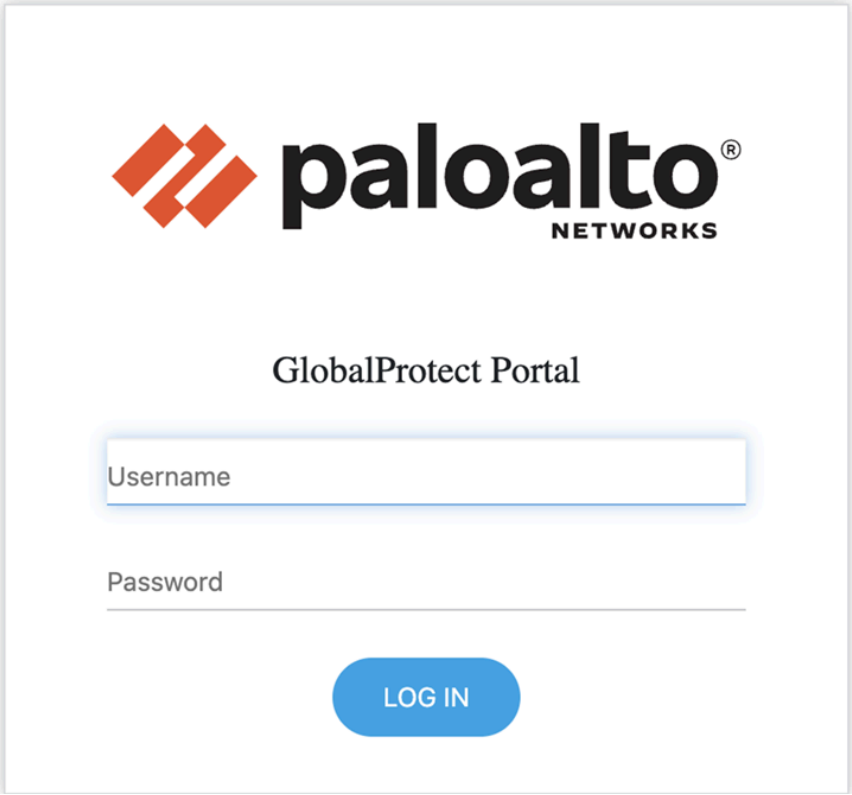
1. Webブラウザを起動し、以下のURL に移動します:

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

   例: **`http://gp.acme.com`**

   GlobalProtect 6.3以降を実行しており、インテリジェントポータル機能が事前にデプロイされている場合、GlobalProtectはお客様の国の場所に基づいて適切なPrisma Accessポータルに自動的にリダイレクトします。ポータル国マップで定義されているポータルは、ドロップダウンで使用できます。詳細については、インテリジェントポータルの設定を参照してください。

2. ポータル ログイン ページで、**Name (名前)**と **Password (パスワード)**に入力し、**LOG IN (ログイン)**をクリックします。ほとんどの場合、企業ネットワークに接続するときに使用するのと同じユーザー名とパスワードを使用できます。



STEP 2 | アプリのダウンロード ページに移動します。

ほとんどのインスタンスでは、ポータルへのログイン後にアプリのダウンロード ページがすぐに表示されます。このページから、最新のアプリ ソフトウェア パッケージをダウンロードします。

システム管理者がGlobalProtectクライアントレスVPNアクセスを有効にしている場合、ポータルにログインした後に(エージェントのダウンロードページの代わりに)アプリケーション

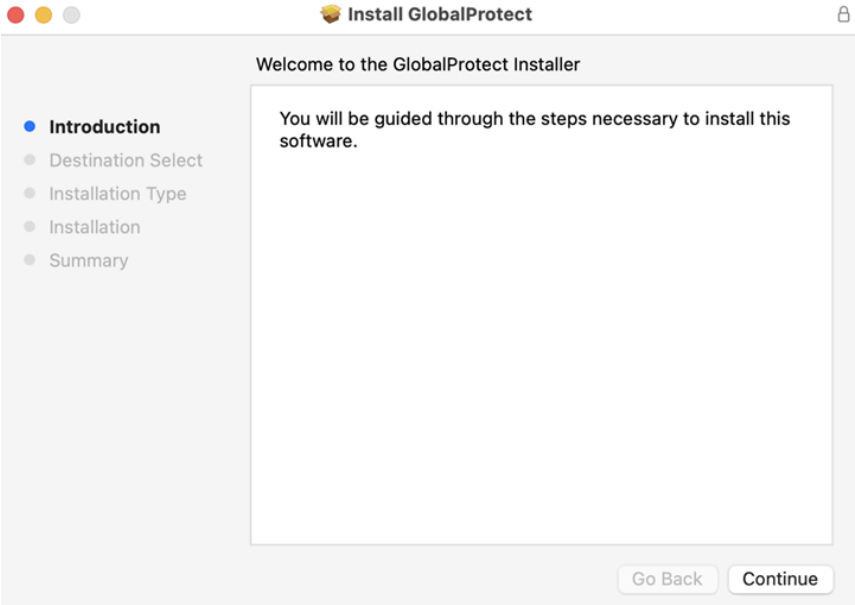
ページが表示されます。**GlobalProtect Agent**（**GlobalProtect** エージェント）を選択してダウンロード ページを選択します。

STEP 3 | アプリをダウンロードします。

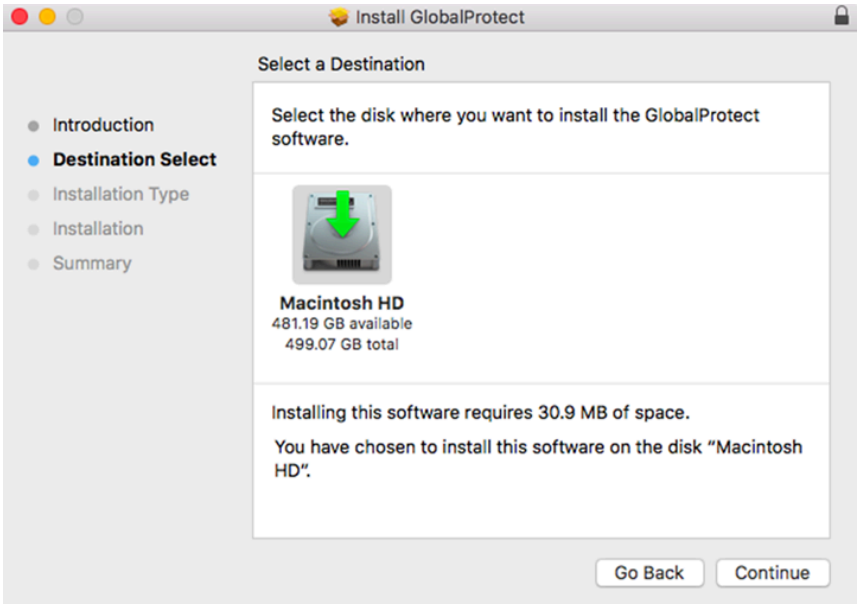
1. **[Download Mac 32/64 bit GlobalProtect agent (Mac 32/64 bit GlobalProtect**エージェントのダウンロード**)]**をクリックします。

2. プロンプトが表示されたら、ソフトウェアを実行します。
3. 再度プロンプトが表示されたら、GlobalProtect Installerを実行します。

STEP 4 | GlobalProtect インストーラを使用してGlobalProtectアプリのセットアップを完了します。



1. GlobalProtect Installerで、**Continue** (続行)をクリックします。
2. **[Destination Select** (宛先選択)]画面で、GlobalProtectアプリケーションのインストールフォルダを選択し、**[Continue** (続行)]をクリックします。

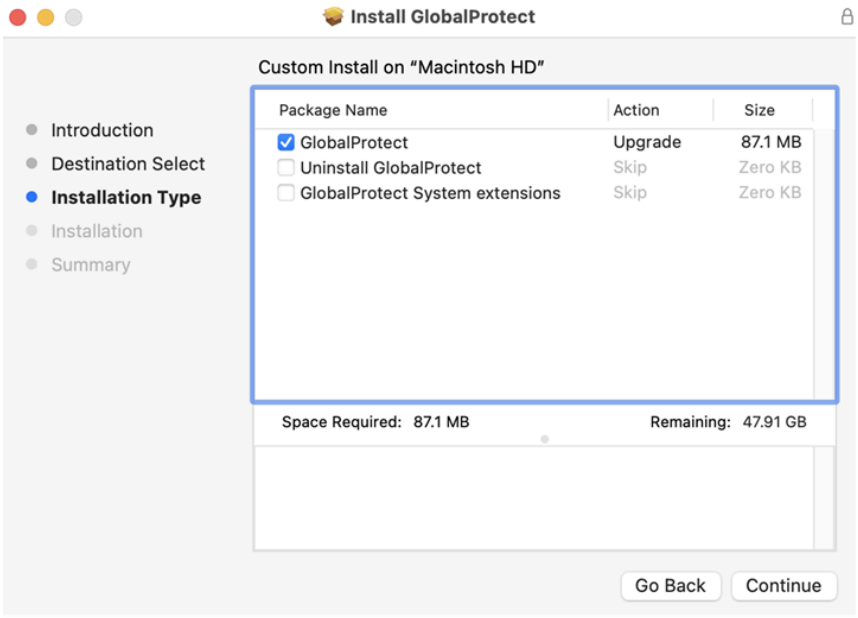


3. **[Installation Type** (インストールタイプ)] 画面で、**[GlobalProtect** installation package]チェックボックスをオンにします。

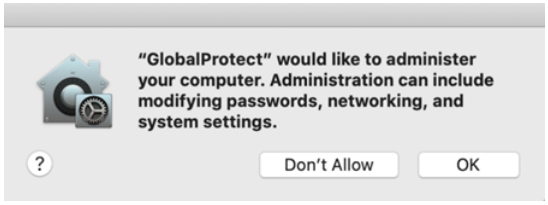
   システム管理者がゲートウェイでスプリット トンネルを設定した場合、またはポータルでネットワークアクセス用に GlobalProtect 接続を適用している場合

は、**[GlobalProtect**システム拡張]チェックボックスをオンにします(デフォルトでは無効)。

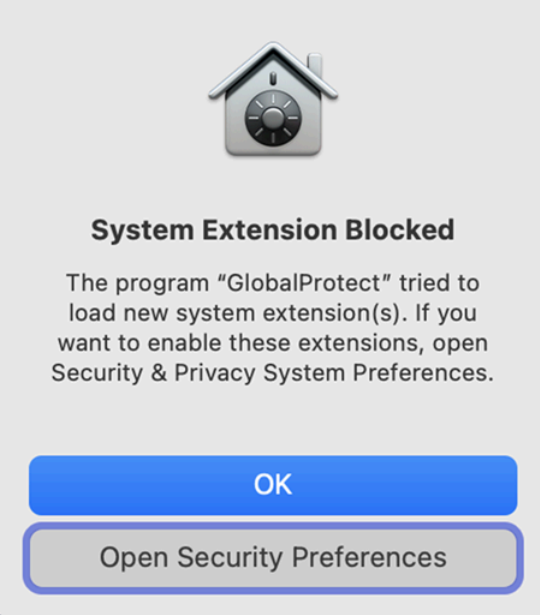
Continue（続行） をクリックします。



4. **[Install (**インストール)] をクリックして、GlobalProtectをインストールすることを確認します。
5. プロンプトが表示されたら、 ユーザー名とパスワードを入力し、[ソフトウェアのインストール]をクリックしてインストールを開始します。
6. インストール完了後、ウィザードを閉じます。
7. 管理者がGlobalProtectアプリのインストール時に自律型 DEM (ADEM)エンドポイントエージェントを初めてインストールするようにポータルを設定した場合は、次のポップアップ プロンプトで **OK** を選択して、再度表示しないようにします。

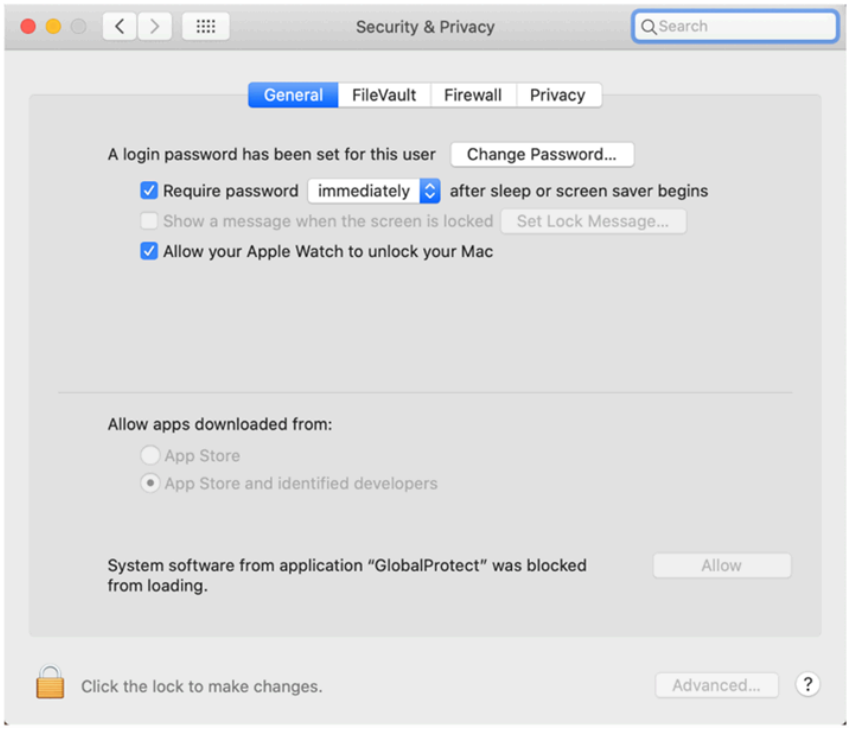


8. **GlobalProtect System Extensions** を有効にした場合は、**Open Security Preferences** を選択して、次の **System Extension Blocked** 通知でロードがブロックされた macOS のシステム拡張機能を有効にします。



管理者がサポートされているMobile Device Management System (MDM; モバイル デバイス管理システム) Jamf Pro を使用してこの通知を抑制している場合は、この通知を受信しなくても自動的にシステム拡張機能をロードできます。

9. **[Security & Privacy (セキュリティとプライ橋ー)]**ダイアログで、南京錠アイコンをクリックして変更を加え、**[Allow apps downloaded from (ダウンロードしたアプリを許可)]** 領域で**[App Store and identified developers (アプリストアと特定開発者)]**を選択します。**[Allow (許可)]** をクリックします。



GlobalProtect App for macOSの使用

どこで使用できますか?	何が必要ですか?
• macOS エンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

このトピックは、エンドポイントにログインした後で、セットアップでGlobalProtectログイン資格情報の入力が必要な場合にのみ適用されます(シングルサインオンは無効です)。

通常、組織にはGlobalProtectユーザーがアプリのインストール後に透過的にログインできるようにすることを推奨します。透過的なGlobalProtectログインでエンドポイントにログインすると、GlobalProtectアプリは自動的に起動し、さらなるユーザーの介入なしに企業ネットワークに接続します。

インストールが完了すると、**System Extension Blocked** (システム拡張機能がブロックされました)という通知メッセージが表示され、ロードがブロックされたmacOSのシステム拡張機能を有効にするように促されます。インストール中に **GlobalProtect System Extensions** オプションが選択されていない場合、ユーザがゲートウェイに接続すると、この通知メッセージが表示されます。この通知は、管理者が GlobalProtectゲートウェイでスプリットトンネルを設定した場合、GlobalProtect ポータルでネットワークアクセスにGlobalProtect接続を強制した場合(GlobalProtectアプリのカスタマイズを参照)、またはその両方を設定した場合に表示されます。どちらの機能も、ユーザがシステム拡張機能を有効にする必要があります。

設定でGlobalProtectの資格情報を入力する必要がある場合は、以下の適用可能な手順に従ってください。

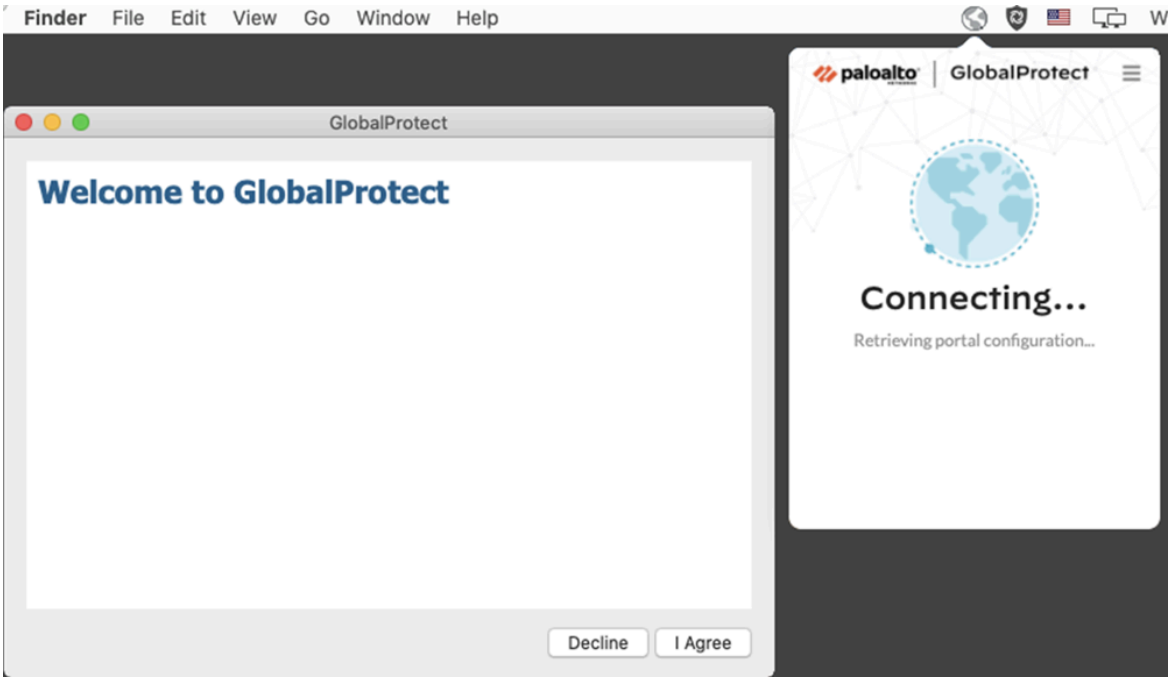
STEP 1 | GlobalProtect にログインします。

エンドポイントに初めてログインする場合、GlobalProtectアプリはログインに成功するとフレンドリーなウェルカムページを表示します。**[Get Started (開始する)]**をクリックしてください。

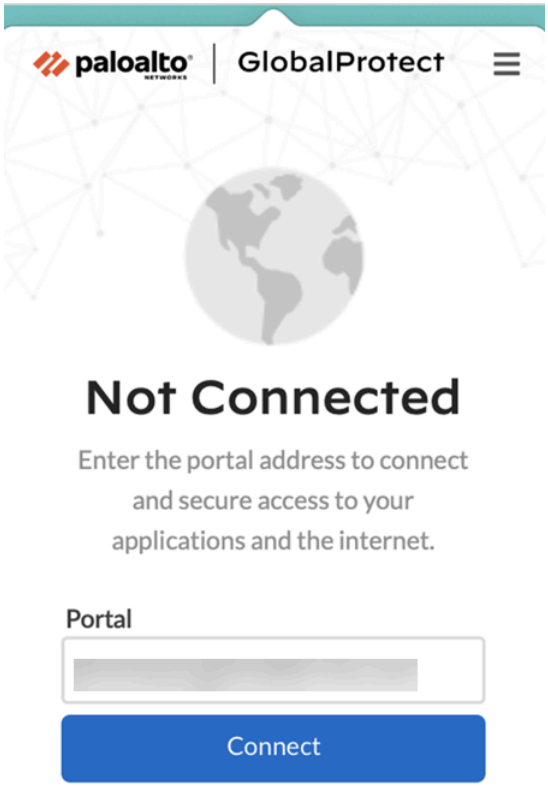
1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. (オプション)管理者から内部リソースにアクセスするページを表示するよう要求された場合は、GlobalProtectに接続する前に会社の利用規約を確認してください。

   利用規約に同意しない場合、GlobalProtectに接続できません。

   オプションで、キャンセルをクリックした場合は、GlobalProtectポータルのIPアドレス(またはドメイン)を入力し、接続をクリックして接続を開始する必要があります。



3. GlobalProtect管理者が指定したポータルのIPアドレスまたはドメインを入力し、接続をクリックします。



STEP 2 | GlobalProtectポータルまたはゲートウェイに接続します。

*GlobalProtect*システムトレイのアイコンを確認すると、接続しているかどうかを確認できます。接続していない場合、アイコンはグレー()で、アイコンにカーソルを合わせると未接続と表示されます。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. (オプション)GlobalProtectアプリに初めてログインする場合は、GlobalProtectポータルのFQDNまたはIPアドレスを入力し、**[Connect (接続)]**をクリックします。
3. (オプション)アプリに複数のポータルが保存されている場合は、ポータルの変更ドロップダウンからポータルを選択します。デフォルトでは、最後に接続したポータルがポータルの変更ドロップダウンから事前に選択されています。
4. （オプション）デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available**（利用可能な最適な接続）ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、ゲートウェイの変更ドロップダウンをクリックし、次のいずれかのオプションを使用します。
   - ゲートウェイを手動で選択します(外部ゲートウェイのみ)。このオプションは、管理者が手動ゲートウェイ選択を有効にした場合にのみ利用可能です。

- 優先ゲートウェイに割り当てて自動的に接続します:

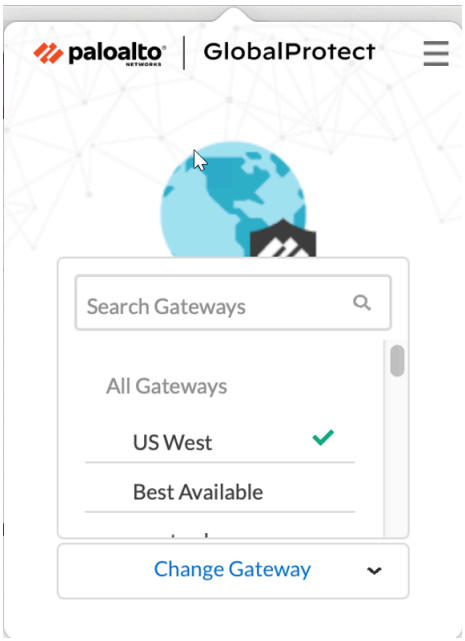
  1. ゲートウェイを優先として指定するには、星マーク(　)をクリックします。次回接続時には、この優先ゲートウェイに自動的に接続します。

     あとでゲートウェイを優先ゲートウェイにしたくないと判断した場合は、スターアイコンをクリアすることで、このゲートウェイを優先接続として解除できます。

  2. デフォルトでは、ゲートウェイ変更ドロップダウンからチェックマークで識別される利用可能な最適な接続ゲートウェイに自動的に接続します。優先ゲートウェ

イを設定すると、ゲートウェイの変更ドロップダウンから星付きゲートウェイの横に星が表示されます。

管理者がポータルエージェント設定で手動外部ゲートウェイを設定した場合は、ゲートウェイ検索フィールドを使用して特定のゲートウェイを選択できます。



5. （オプション）接続モードに応じて、**Connect**（接続）をクリックして接続を開始します。
6. (オプション)プロンプトが表示されたら、**Username** (ユーザー名)と**Password** (パスワード)を入力して**Sign In** (サインイン)をクリックします。

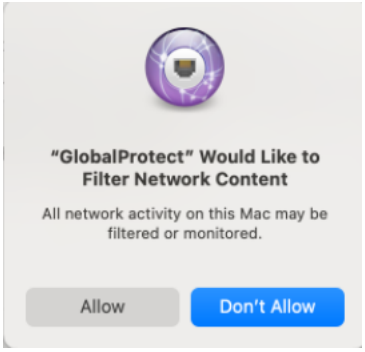
   管理者が生体認証(指紋)情報を使用してサインインすることを許可している場合は、最初にユーザ名とパスワードを使用して2回(1回は保存して再度認証)サインインする必要があります。その後、生体認証情報を使用してサインインできます。

   システム管理者が **GlobalProtect System Extensions** を有効にしている場合は、ロードをブロックされたmacOSのシステム拡張機能を有効にして、スプリットトンネルとEnforce GlobalProtect for Network Access機能を使用する必要があります。

   ネットワーク拡張構成の両方のポップアッププロンプトを許可するために、ユーザーは管理者権限を必要としません。管理者は、*Jamf Pro*などのモバイルデバイス管理システム*(MDM)*を使用して、これらのメッセージプロンプトを受信しなくても、ネットワーク拡張を自動的にロードすることで、これらのメッセージプロンプトを抑止できます。Jamf Pro を使用してシステム拡張とネットワーク拡張を有効にする 方法については、ナレッジベース記事 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000HAW8 を参照してください

   1. (macOS Catalina 10.15.4以降およびmacOS Big Sur 11以降のみ)システム管理者がGlobalProtectゲートウェイのドメインとアプリケーションに基づいてスプリットトンネルを設定した場合、または[ネットワークアクセスにGlobalProtect接続を強

制]機能を有効にしている場合は、次のポップアッププロンプトで許可を選択します。



許可しないを選択した場合、スプリットトンネル機能はGlobalProtectアプリで使用できず、[ネットワークアクセスにGlobalProtect接続を強制]機能は機能せず、ネットワークアクセスにGlobalProtect接続を強制できません。このポップアッププロンプトは、ポータルまたはゲートウェイに次回接続するとき、または許可を選択するまで表示されます。

アプリが外部モードで接続すると、GlobalProtectシステムトレイアイコンにシールド()が表示され、アイコンにカーソルを合わせると接続済みが表示されます。アプリが内部モードで接続すると、GlobalProtectシステムトレイのアイコンに家()が表示され、アイコンにカーソルを合わせると内部ネットワークが表示されます。

STEP 3 | GlobalProtectアプリケーションを開きます。

GlobalProtectシステム トレイ アイコンをクリックして、アプリ インターフェースを起動します。

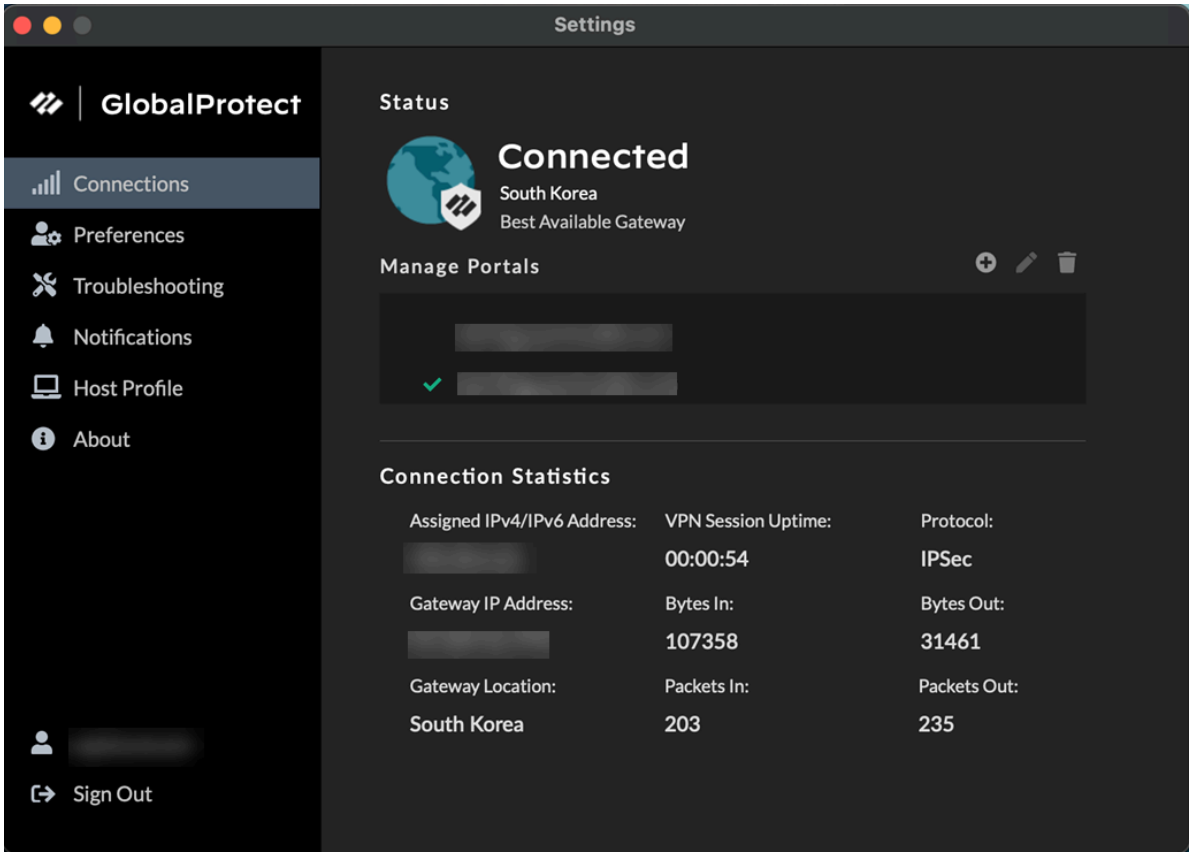
GlobalProtect アプリのインストール中に、管理者がAutonomous DEM (ADEM)エンドポイントエージェントをインストールするようにポータルを設定し、テストを有効にすることを許可しているか、または許可していない場合、通知が表示されます。管理者がADEMエンドポイント エージェントをすでにインストールしていて、後でADEMエンドポイント エージェントをアンインストールするようにポータルを設定している場合は、次回のログイン時に通知が表示されます。

STEP 4 | ネットワーク接続に関する情報を表示します。

アプリを起動したら、ステータスパネルのハンバーガーメニューをクリックして設定メニューを開きます。設定を選択して**GlobalProtect**設定パネルを開き、次のいずれかの設定を選択してGlobalProtectアプリを表示および変更します。

- 接続–接続タブには、GlobalProtectアカウントに関連付けられたポータルが表示されます。このタブからポータルを追加、編集、または削除できます。このタブには、接続しているゲートウェイも表示されます。管理者が GlobalProtect ポータルエージェントの設定で高度なビューを許可するをはいに設定すると、ゲートウェイに関する接続統計(ゲート

ウェイのIPアドレス、場所、VPNセッションの稼働時間など)を表示できます。接続タブを選択すると、ログイン有効期間のカウントダウンタイマーが表示されます。



GlobalProtect for Always-On Internet Security 機能の[Explicit Proxy Connectivity]がPrisma Accessを通じてアプリで有効になっている場合、接続タブにプロキシの詳細が表示されます。

プロキシモード:

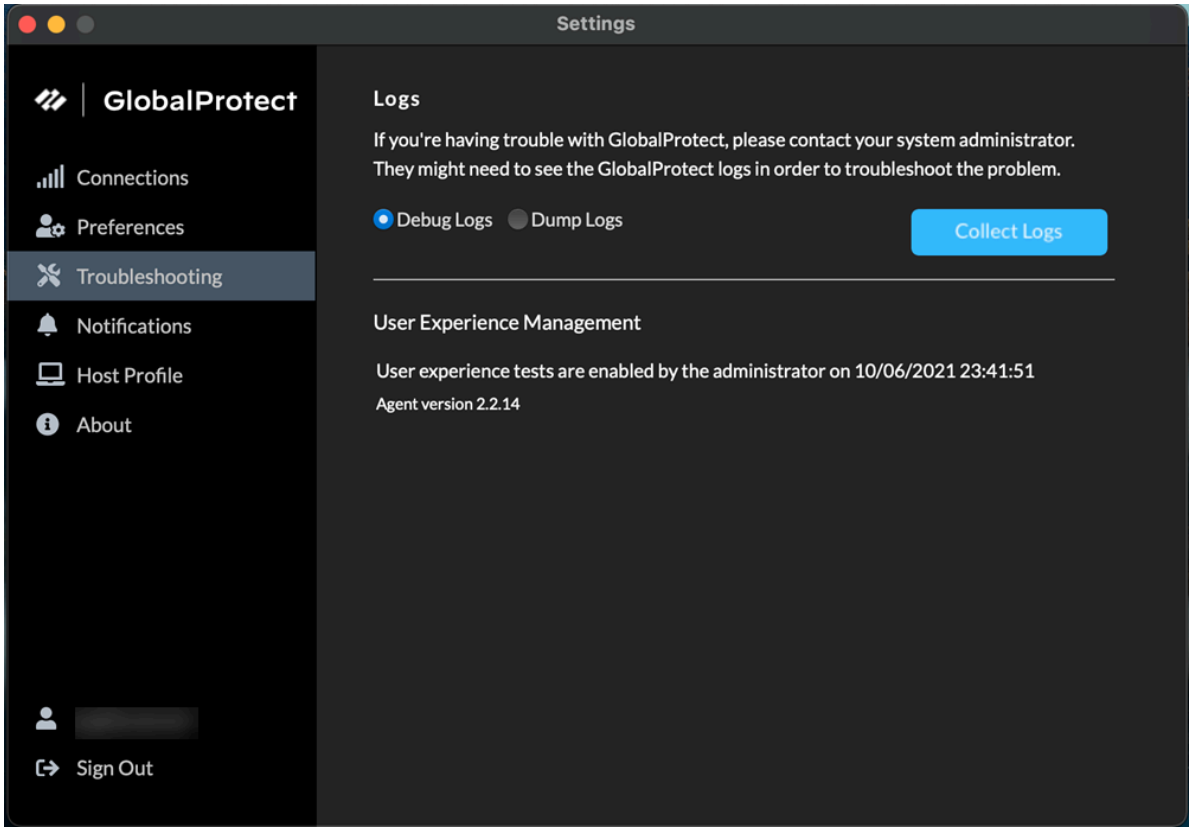
- プリファレンス–管理者が次のオプションの少なくとも1つを設定した場合にのみ、プリファレンスタブを使用できるようになりました。
  - 生体認証サインインを有効にする–生体認証(指紋)情報を使用してサインインすることを選択できます。このオプションは、管理者がGlobalProtectエージェント構成でユーザー資格情報を保存をユーザーフィンガープリントでのみに構成している場合にのみ使用できます。GlobalProtectポータルとゲートウェイへの認証の際に、保存されたパスワードを認証に使用するために、エンドポイントの信頼できる指紋テンプレートと一致する指紋を提供する必要があります。
  - 接続が成功するたびにウェルカムページを表示しない:ログインが成功したときにウェルカムページを表示するように選択できます。このオプションは、管理者がGlobalProtect ポータルエージェント設定でようこそページを工場出荷時に設定している場合にのみ使用できます。

- **SSL**で接続–SSLを使用するか、IPSecのままにするかを選択できます。このオプションは、管理者がGlobalProtectポータルエージェントの設定で**SSL**のみ接続をユーザーが変更できるに設定している場合にのみ使用できます。
- 常に診断テストを実行し、ログを含める–GlobalProtectアプリが診断テストを実行できるようにするか、診断ログを含めるかを選択できます。このオプションは、管理者がGlobalProtectポータルでトラブルシューティングのためのGlobalProtectアプリログ収集を有効にしている場合にのみ使用できます。

- トラブルシューティングートラブルシューティングタブでは、ログの収集、ログレベルの設定(デバッグ ログまたはダンプ ログ)、およびオプションでユーザ エクスペリエンス テストの有効化を行うことができます。

  詳細な分析のために、*GlobalProtect*アプリがトラブルシューティング ログ、診断ログ、またはその両方をStrata Logging Serviceに送信するには、トラブルシューティング用の GlobalProtect アプリログコレクションを有効にするようにGlobalProtectポータルを構成する必要があります。また、 HTTPS ベースの送信先 URL を構成 には、プローブする *Web* サーバー/リソースの *IP* アドレスまたは完全修飾ドメイン名を含めることができ、エンド ユーザーのエンドポイントでの待機時間やネットワーク パフォーマンスなどの問題を特定できます。

  詳細設定をクリックすると、エンドポイントに関する詳細情報を表示できます。



  ログの詳細設定ウィンドウには、ネットワーク設定、ルート設定、アクティブな接続、およびログに関する情報が表示されます。

  GlobalProtectが接続されているときに、GlobalProtectアプリに[ユーザーエクスペリエンステストを有効にする]チェックボックスが表示されている場合は、ADEMエンドポイントエージェントがユーザーエクスペリエンステストを実行できるかどうかを確認してください。または、管理者がGlobalProtectアプリのインストール中にADEMエンドポイントエージェントをインストールしたが、GlobalProtectアプリからユーザーエクスペリエンステストを有効または無効にすることができない場合、メッセージが表示されることを確認でき

ます。デフォルトでは、GlobalProtectが無効または切断された場合でも、ハートビートアラートはADEMに転送されます。

管理者がGlobalProtectアプリのインストール中に自律型 DEM エンドポイントエージェントをインストールするようにポータルを構成し、テストを有効にすることを許可している場合は 、GlobalProtectアプリでユーザーエクスペリエンステストを有効にするチェックボックスをオンにします。このチェックボックスは、管理者がGlobalProtectアプリからユーザーエクスペリエンステストの有効化または無効化を許可していない場合には表示されません。代わりにメッセージが表示され、アプリがユーザーエクスペリエンステストを実行できるように設定されていることを確認します。

ユーザーエクスペリエンステストを有効にするチェックボックスをオンにしない場合でも、ハートビートアラートはADEMに転送されます。

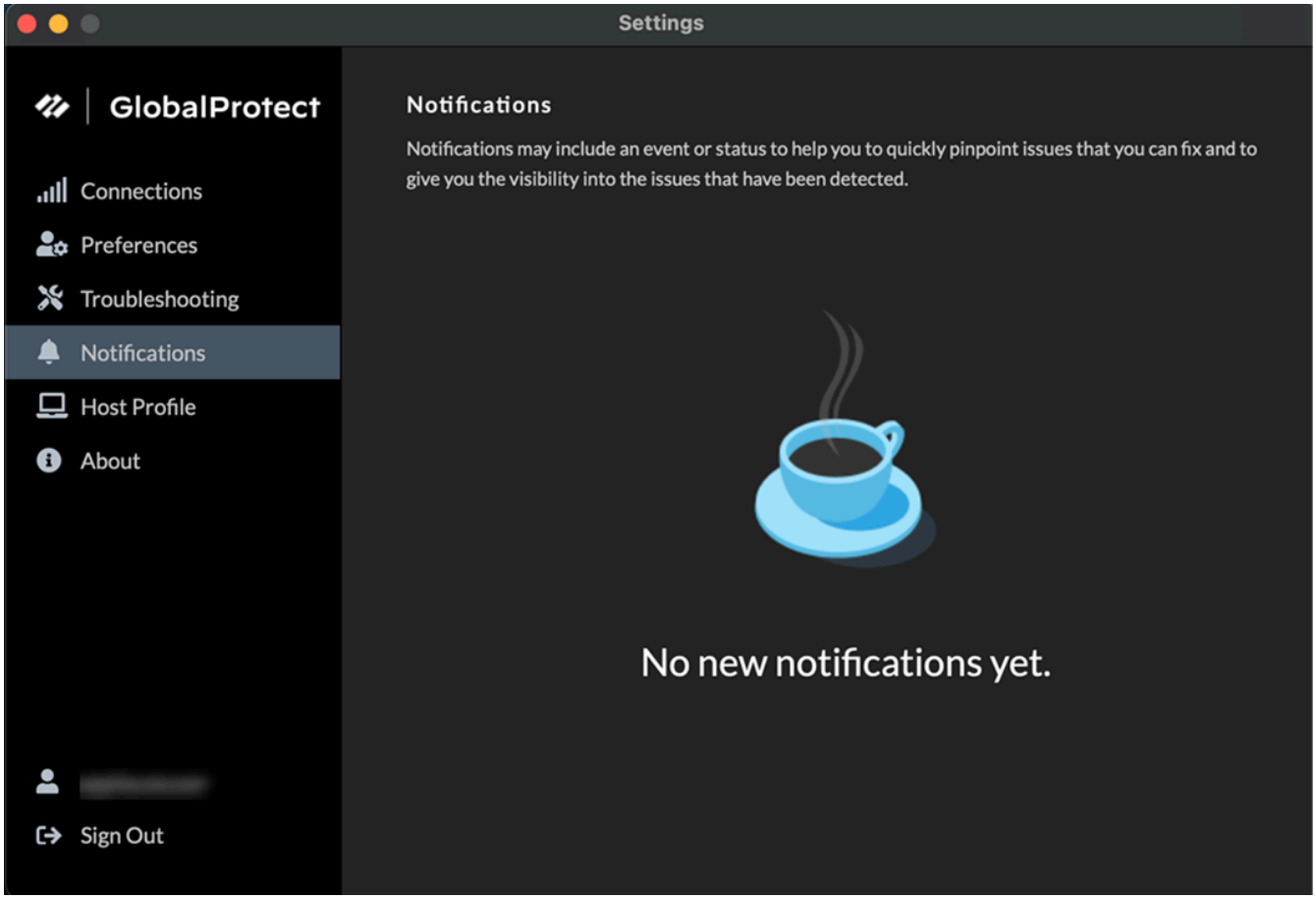
- 通知—通知タブには、GlobalProtectアプリでトリガーされた特定の通知に関する詳細情報が表示されます。ゲートウェイでGlobalProtectアプリセッションの有効期限に関するエンドユーザー通知を構成し、アプリ上でこれらのカスタム通知の表示をスケジュールできます。

GlobalProtectアプリバージョン6.2.3から、常時接続方式ではセッションタイムアウトメッセージとアイドルタイムアウトメッセージは抑制されます。

GlobalProtectアプリのバージョン6.2から、GlobalProtectアプリのログイン有効期間セッションを期限切れ前に延長して、アプリセッションの突然のログアウトを回避できるようになりました。ログイン有効期間満了通知は、アプリセッションの有効期限が近づくと事前に通知し、セッションから突然ログアウトされないようにユーザーセッションの期間

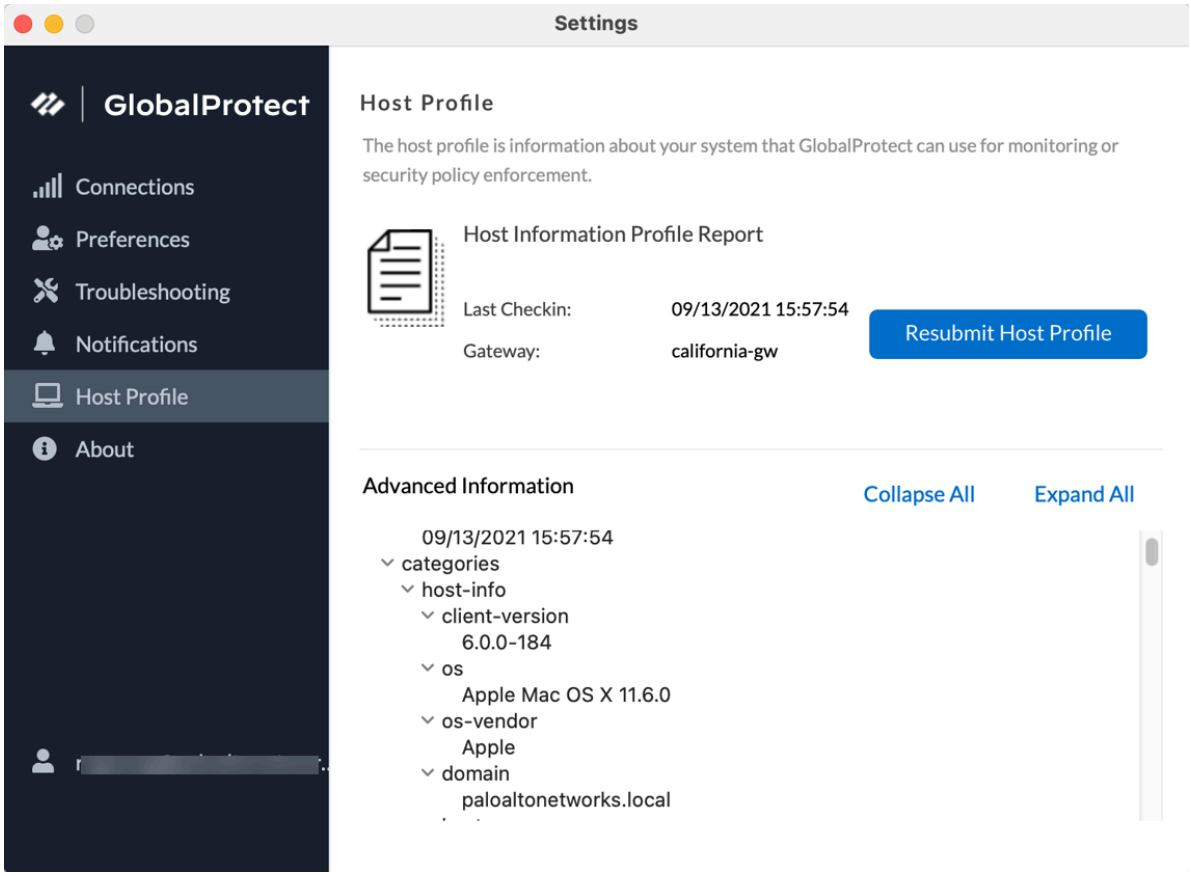
を延長するオプションを提供します。管理者がセッション延長の通知設定を行っている場合、アプリはユーザーセッション延長オプション付きの期限切れ通知を表示します。

GlobalProtectアプリでトリガーされた新しい通知がない場合も通知されます。



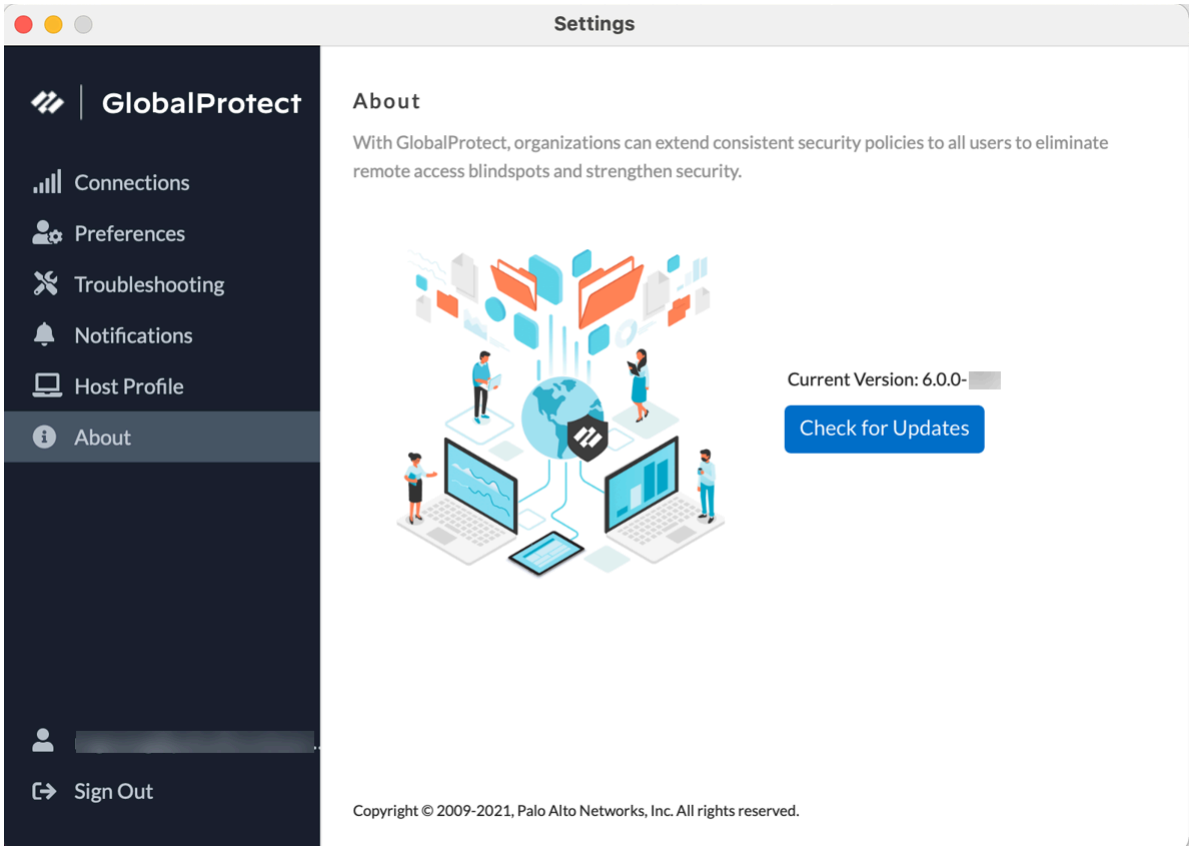
- ホストプロファイル–ホストプロファイルタブは、GlobalProtectがホスト情報プロファイルを使用してセキュリティポリシーを監視および実施するために使用するエンドポイン

ト データを表示します。HIP データをゲートウェイに手動で再送信するには、ホストプロファイルの再送信をクリックします。



管理者が複数の内部ゲートウェイを非トンネルモードで設定し、内部ホスト検出を行っている場合は、詳細をクリックして、各ゲートウェイのHost Information Profile (HIP)レポート提出を中央から監視し、HIP関連の問題の迅速なトラブルシューティングに役立てることができます。

- バージョン情報–バージョン情報タブには、エンドポイントに現在インストールされているGlobalProtectのバージョンが表示され、エンド・ユーザーは更新をチェックできます。



STEP 5 | (オプション)新しいパスワードを使用してログインします。

*GlobalProtect*管理者が*GlobalProtect*ポータルエージェントをユーザー資格情報を保存に設定すると、資格情報は自動的に*GlobalProtect*アプリに保存されます。企業ネットワークにアクセスするためのパスワードが変更された場合、新しいパスワードを使用して*GlobalProtect*にログインする必要があります。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. ハンバーガーメニューをクリックして設定メニューを開きます。
3. **Settings**（設定）を選択して、**GlobalProtect Settings**（**GlobalProtect** 設定）パネルを開きます。
4. **GlobalProtect**設定パネルで、サインアウトして、保存したユーザー資格情報をGlobalProtectアプリからクリアします。
5. ユーザー資格情報をクリアした後、新しいユーザー名とパスワードでGlobalProtectに再接続できます。

STEP 6 | (オプション) GlobalProtectから切断します。

管理者がオンデマンド接続方法でGlobalProtectを設定した場合、ステータスパネルの切断をクリックすることでGlobalProtectから切断できます。

macOS用のGlobalProtectアプリから問題を報告する

どこで使用できますか?	何が必要ですか?
• macOS エンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

ネットワーク パフォーマンスが低下したり、ポータルやゲートウェイとの接続が確立されなかったりするなどの異常な動作が発生した場合は、管理者がアクセスできるStrata Logging Serviceに直接問題を報告できます。GlobalProtectアプリのログを手動で収集してメールで送信したり、クラウドドライブに保存したりする必要はなくなりました。

*GlobalProtect*アプリに問題を報告するオプションを表示するには、管理者が*GlobalProtect*ポータルでトラブルシューティングのためのGlobalProtectアプリログ収集を有効にする必要があります。

STEP 1 | GlobalProtectポータルまたはゲートウェイに接続します。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. (オプション)GlobalProtectアプリに初めてログインする場合は、GlobalProtectポータルのFQDNまたはIPアドレスを入力し、**[Connect (接続)]**をクリックします。
3. (任意)複数のポータルがアプリに保存されている場合は、[ポータル]ドロップダウンからポータルを選択します。デフォルトでは、最後に接続されたポータルが[ポータル]ドロップダウンから事前に選択されています。
4. （オプション）デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available**（利用可能な最適な接続）ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、ゲートウェイのドロップダウンをクリックします。

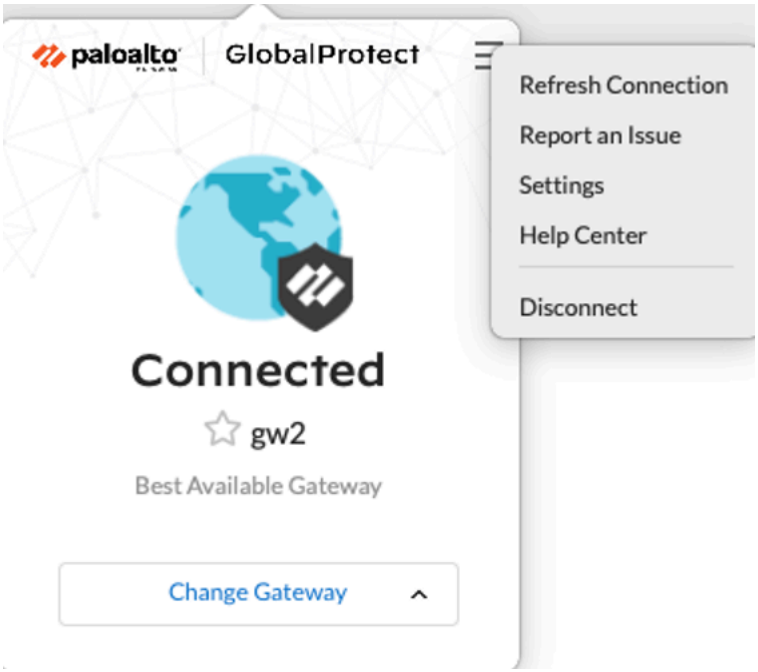
STEP 2 | GlobalProtectアプリケーションを開きます。

GlobalProtectシステム トレイ アイコンをクリックして、アプリ インターフェースを起動します。

STEP 3 | エンドポイントからGlobalProtectアプリケーションから問題を報告します。

アプリを起動したら、ステータスパネルのハンバーガーメニューをクリックして管理者に問題を報告してください。

1. **Report an Issue (**問題の報告**)**を選択します。



2. GlobalProtectアプリが診断テストを実行し、診断ログを含めることを有効にします。診断ログとトラブルシューティングログの両方が収集され、コンパクトなトラブルシューティングレポートとしてStrata Logging Serviceに送信されます。

   診断テストが正常に完了した後、GlobalProtectデバッグログファイルがエンドポイントからStrata Logging Serviceにアップロードされます。

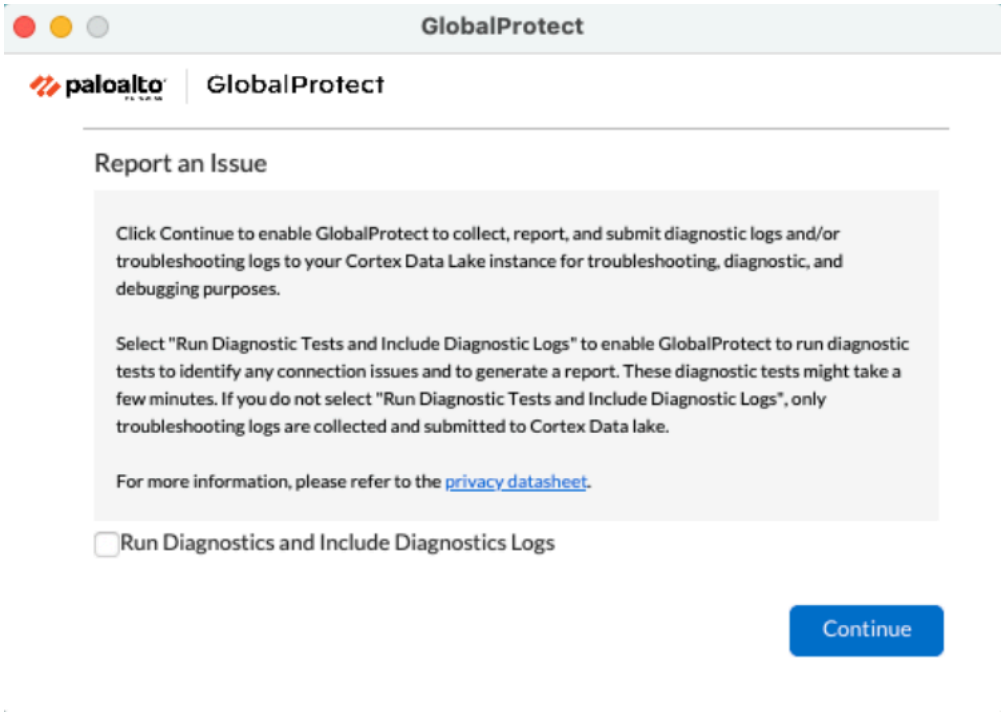
   アプリが診断テストを実行し、診断ログを含めることを有効にしない場合、トラブルシューティングログのみが収集され、コンパクトなトラブルシューティングレポートとして*Strata Logging Service*に送信されます。*GlobalProtect*アプリは、`.json`形式で自動的に生成されたレポートファイル*(pan_gp.trb.log*または*pan_gp_trbl.log)*をチェックします。トラブルシューティングログに問題が見つからなかった場合、通知メッセージが表示されます。再試行をクリックして、*pan_gp.trb*.log*ファイルが存在するか確認します。

3. **Run Diagnostic Tests and Include Diagnostic Logs(**診断テストを実行して診断ログを含める**)**チェックボックスを選択します。
4. 続行をクリックして、アプリがトラブルシューティング ログを作成し、管理者のStrata Logging Serviceインスタンスにレポートを送信できるようにします。

   エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。

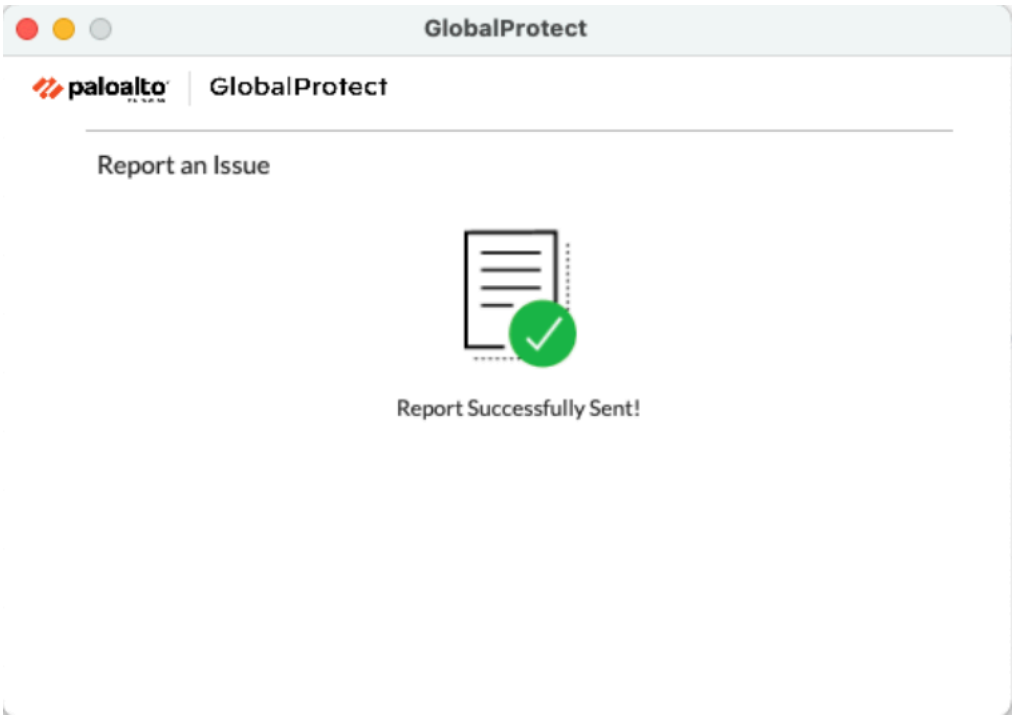
エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。GlobalProtectアプリは、トンネルありまたはトンネルなしで診断テスト

を実行できます。例えば、アプリが接続してトンネルを通じて診断テストを実行する前に、GlobalProtectのログイン資格情報を入力したいかもしれません。



アプリが診断テストを実行していることを確認するメッセージがポップアップしますが、これは**Run Diagnostic Tests and Include Diagnostic Logs (**診断テストを実行して診断ログを含める)チェックボックスを選択した場合のみです。

5. 閉じる]をクリックして、アプリがレポートをStrata Logging Serviceに正常に送信したことを確認します。この確認メッセージには、レポートが処理および送信された日時が表示されます。



GlobalProtectアプリをmacOSから接続解除する

どこで使用できますか?	何が必要ですか?
• macOS エンドポイントのみの場合:	❑ GlobalProtect アプリのバージョン 6.3 以降

管理者がGlobalProtectの接続方法を常時接続に設定している場合、GlobalProtectアプリを切断できます。たとえば、ホテルでGlobalProtect仮想プライベートネットワーク（VPN）が機能しておらず、VPN障害によってインターネットに接続できない場合、アプリを切断したい場合があります。GlobalProtectアプリを切断した後は、セキュアでない通信（VPNなし）を使用してインターネットに接続できます。

GlobalProtectアプリを切断できる方法、時間、回数は、管理者がGlobalProtectサービス(PanGPS)をどのように構成するかによって異なります。この構成では、アプリを完全に切断できないようにしたり、チャレンジに正しく応答した後にのみアプリを切断したりすることができます。

構成にチャレンジが含まれている場合、GlobalProtectアプリは次のいずれかを求めるプロンプトを表示します。

- アプリを切断したい理由
- インターネット速度が遅いやアプリが動作しないなどの理由に応答します(必要な場合)
- パスコード
- チケット番号

チャレンジにパスコードやチケット番号が含まれている場合は、電話でGlobalProtect管理者またはヘルプデスクの担当者に連絡することをお勧めします。

通常、管理者は事前にパスコードを電子メール(GlobalProtectの新規ユーザー用)または組織のウェブサイトに掲載して提供します。また、システム停止やシステム障害が発生した場合には、管理者が電話でパスコードを提供することもあります。

有効なチケット番号を取得する前に、エンドポイントはGlobalProtect管理者またはヘルプデスクの担当者に伝える必要があるチケットリクエスト番号を表示します。切断リクエストが承認されると、GlobalProtectを切断するために使用できる有効なチケット番号が届きます。

次の手順では、アプリを切断してチャレンジを渡す方法について説明します。

STEP 1 | GlobalProtectアプリの接続を解除します。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. ハンバーガーメニューをクリックして設定メニューを開きます。
3. **[Disconnect (接続解除)]**を選択します。

> ***[Disconnect (接続解除)]***オプションは、*GlobalProtect*エージェント構成でアプリケーションの切断が許可されている場合にのみ表示されます。構成で、チャレンジに応答することなく *GlobalProtect* アプリを切断できる場合、*GlobalProtect* アプリは追加のアクションを必要とせずに終了します。

STEP 2 | 必要に応じて、1つ以上の課題に対応します。

プロンプトが表示されたら、次の情報を入力します。

- 問題を教えてください–GlobalProtectアプリを切断する理由。
- 切断する理由を選択してください–構成により、1つ以上の理由に応答する必要がある場合や別の理由を入力する必要がある場合、GlobalProtectアプリは接続解除を選択するとすぐに理由を表示します。
- **Passcode (パスコード)**: 通常は、アプリを切断する必要がある既知の問題やイベントに基づいて、管理者が事前に提供するパスコードです。
- チケット–構成によりチケット番号を提供する必要がある場合、GlobalProtectアプリは接続解除を選択するとすぐに8文字の16進数のチケットリクエスト番号を表示します。チケット番号でアプリを接続解除するには、管理者またはヘルプデスクの担当者(電話)に連絡し、チケットリクエスト番号を提供してください。リクエストが承認された後、管理者またはヘルプデスクの担当者が8文字の16進数のチケット番号を提供します。チケット番号をチケットフィールドに入力し、次に**OK**をクリックします。

macOS用のGlobalProtect Appをアンインストールする

どこで使用できますか?	何が必要ですか?
• macOS エンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

、以下の手順に従って、macOS エンドポイントからGlobalProtectアプリをアンインストールします。アプリをアンインストールすると、企業ネットワークへのVPNアクセスがなくなり、エンドポイントは会社のセキュリティポリシーによって保護されなくなることに注意してください。

管理者権限を持つユーザーのみが、*macOS*エンドポイントから*GlobalProtect*アプリをアンインストールできます。

macOSエンドポイントでは、macOSのインストールプログラム(この場合はGlobalProtectインストーラ)を使用してプログラムをアンインストールできます。エンドポイントからGlobalProtectアプリをアンインストールするには、GlobalProtectソフトウェアパッケージをインストールし、その後GlobalProtectインストーラーを起動します。GlobalProtectインストーラーは、**GlobalProtect** をアンインストールパッケージを選択するように促します。管理者がGlobalProtectアプリのインストール中にmacOSエンドポイントのシステム拡張を有効にした場合、GlobalProtectアプリはアンインストール中にシステム拡張を削除するように促します。**GlobalProtect**アンインストールパッケージが正常にインストールされた後、GlobalProtectアプリはエンドポイントから削除されます。

*macOS*エンドポイントに*GlobalProtect*インストーラーがない場合は、コマンドラインから次のコマンドを実行して*GlobalProtect*をアンインストールできます:

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

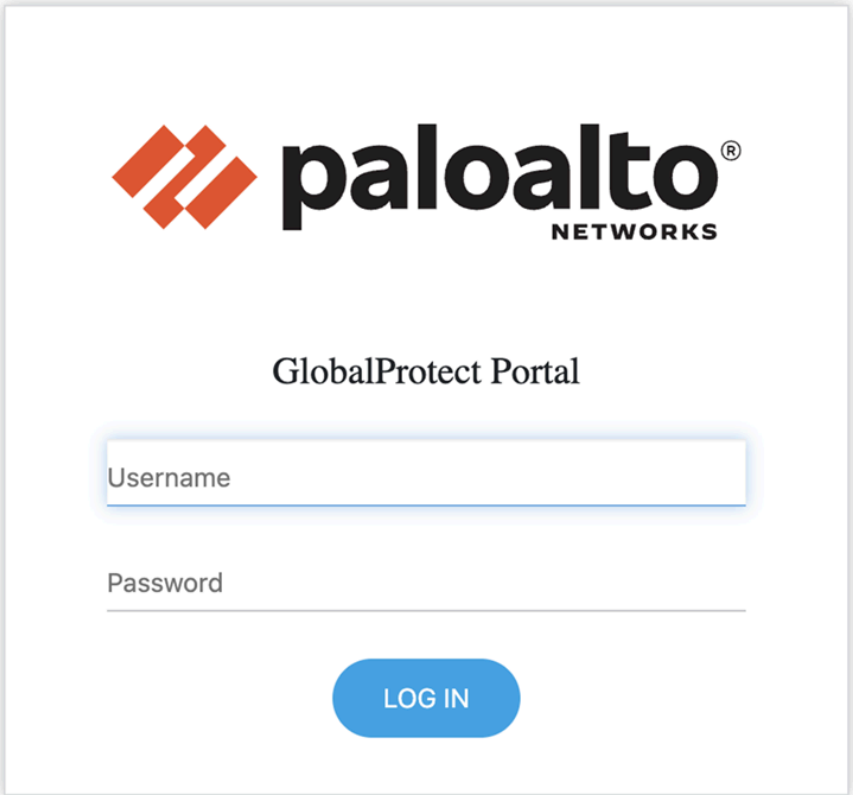
STEP 1 | GlobalProtect ポータルにログインします。

1. Web ブラウザを起動し、以下の URL に移動します。

   https://<portal address or name>

   例: **http://gp.acme.com**

2. ポータル ログイン ページで、**[Name (名前)]**と **[Password (パスワード)]**に入力し、**LOG IN (ログイン)]**をクリックします。ほとんどの場合、企業ネットワークに接続するときに使用するのと同じユーザー名とパスワードを使用できます。



STEP 2 | アプリのダウンロード ページに移動します。

ほとんどの場合、ポータルへのログイン後にアプリのダウンロード ページがすぐに表示されます。

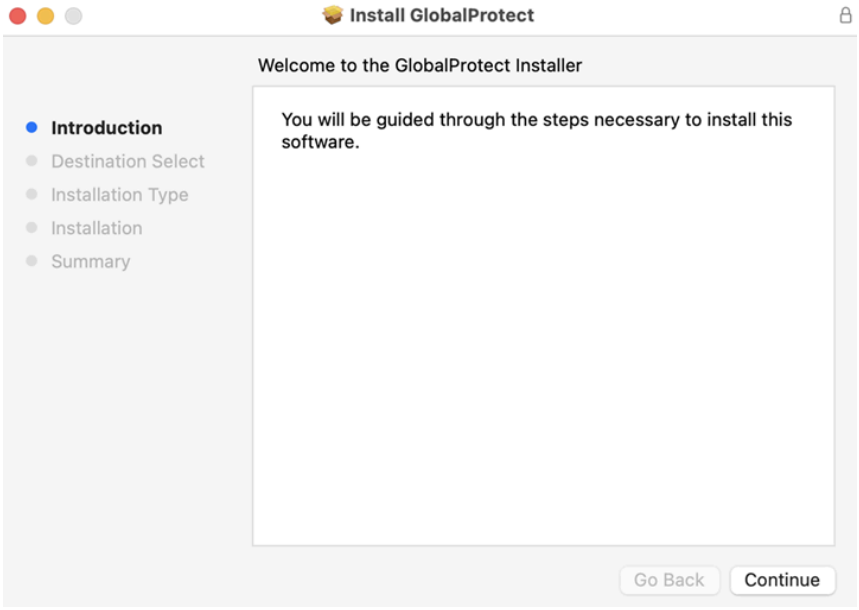
システム管理者が*GlobalProtect*クライアントレス*VPN*アクセスを有効にしている場合、ポータルにログインするとアプリケーションページが開きます(アプリのダウンロードページではなく)。***GlobalProtect Agent***（***GlobalProtect*** エージェント）を選択してダウンロード ページを選択します。

STEP 3 | アプリをダウンロードします。

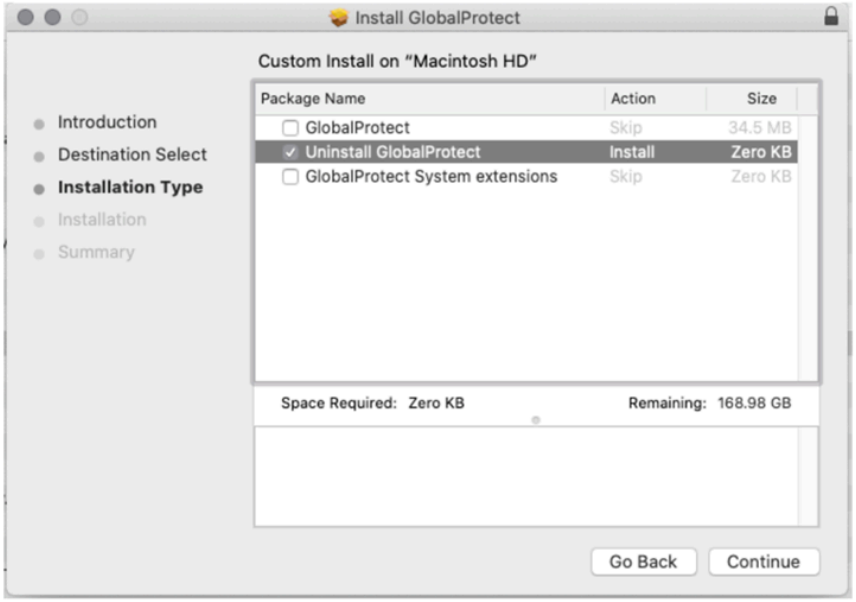
1. **[Download Mac 32/64 bit GlobalProtect agent (Mac 32/64 bit GlobalProtect**エージェントのダウンロード**)]**をクリックします。
2. プロンプトが表示されたら、ソフトウェアを実行します。
3. 再度プロンプトが表示されたら、GlobalProtect Installerを実行します。

STEP 4 | GlobalProtectをアンインストールします。

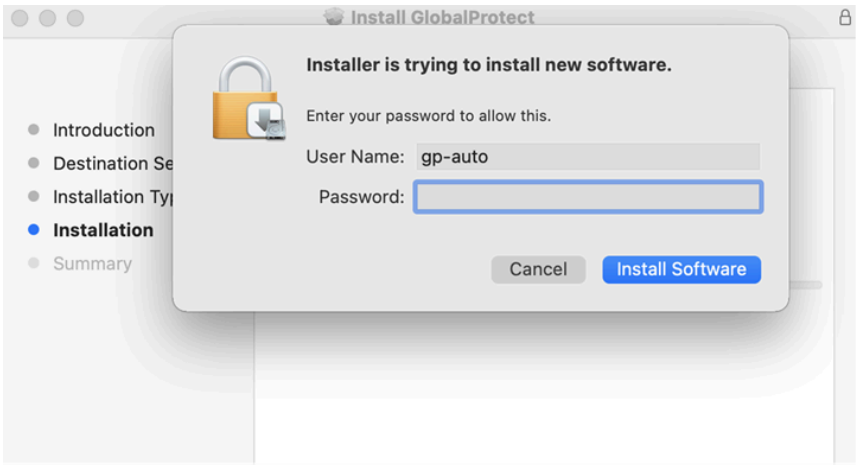
1. GlobalProtect Installerで、**Continue (**続行**)**をクリックします。



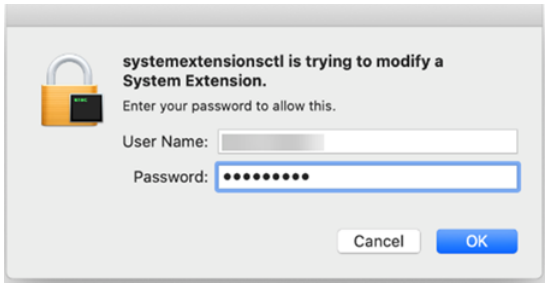
2. 宛先選択画面で、続行をクリックします。
3. インストールタイプ画面で、**GlobalProtect**をアンインストールチェックボックスを選択し、続行をクリックします。



4. GlobalProtect アプリを削除することを確認するには、インストールをクリックします。
5. プロンプトが表示されたら、ユーザー名とパスワードを入力し、ソフトウェアのインストールをクリックしてGlobalProtectをアンインストールします。

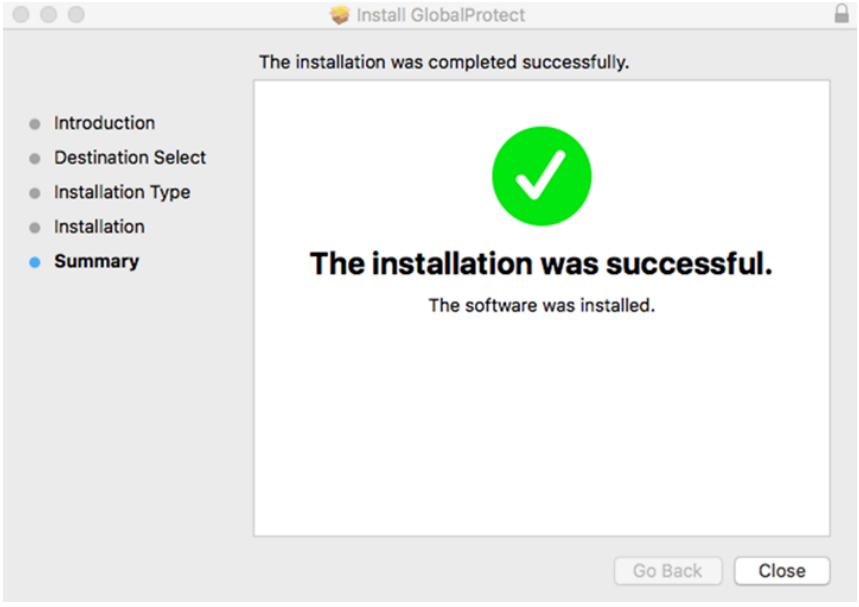


6. システム管理者がmacOS Catalina 10.15.4以降のGlobalProtectアプリ5.1.4インストール中にmacOSシステム拡張を有効にした場合、システム拡張をアンインストールするためのポップアッププロンプトが表示されます。プロンプトが表示されたら、ユーザー名とパスワードを入力し、**OK**をクリックしてシステム拡張機能を削除します。



STEP 5 | GlobalProtectアプリがもはやインストールされていないことを確認してください。

メッセージがポップアップし、**GlobalProtect**のアンインストールパッケージが正常にインストールされたことを確認します。この確認は、GlobalProtectアプリがエンドポイントから削除されたことを示しています。



GlobalProtect Enforcer カーネル拡張機能の削除

どこで使用できますか?	何が必要ですか?
• macOS エンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

macOS用GlobalProtect アプリケーションをアンインストールしてから、アプリケーションの新しいインスタンスをインストールする場合、GlobalProtectエンフォーサー カーネル拡張が正しく更新されないと、接続の問題が発生する可能性があります。カーネル拡張 (kext) は、アプリケーションを管理するmacOSオペレーティングシステム用のプラグインです。アプリケーションの新しいインスタンスをインストールした後にGlobalProtectに接続できない場合は、以下の手順を使用してGlobalProtectエンフォーサー カーネル拡張機能を探して削除します。

STEP 1 | Mac用GlobalProtect Appをアンインストールします。

STEP 2 | GlobalProtect エンフォーサーカーネル拡張機能がエンドポイントに存在するかどうかを確認します。

macOS エンドポイントで、**Applications** > **Utilities**フォルダの下にあるターミナルアプリケーションを開き、次のコマンドを入力します。

```
kextstat | grep gplock
```

STEP 3 | 拡張機能が存在する場合は、エンフォーサーをアンロードします。

ターミナル アプリケーションで次のコマンドを入力して、エンフォーサーをアンロードします。

```
sudo kextunload -b com.paloaltonetworks.GlobalProtect.gplock
```

STEP 4 | 再起動後にエンフォーサーがリロードされないようにします。

ターミナル アプリケーションで次のコマンドを入力して、macOS ハード ディスクからエンフォーサーを削除します。

```
sudo rm -r "/System/Library/Extensions/gplock*.kext"
```

STEP 5 | Mac用GlobalProtectアプリケーションをダウンロードおよびインストールします。

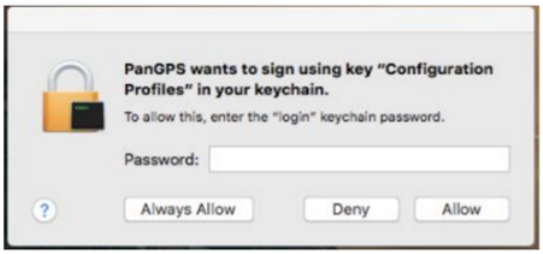
GlobalProtect App for macOSでクライアント証明書を認証に使用できるようにする

どこで使用できますか?	何が必要ですか?
• macOS エンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtectアプリをmacOSエンドポイントに初めてインストールし、ポータルまたはゲートウェイでクライアント証明書認証を有効にすると、キーチェーンポップアッププロンプトが表示され、GlobalProtectがログインキーチェーンからクライアント証明書にアクセスして使用できるようにパスワードの入力を求められます。キーチェーンポップアッププロンプトは、以前の証明書が期限切れになったために新しい証明書をインストールした場合にも表示される場合があります。

macOS用のGlobalProtectアプリが認証にクライアント証明書を使用できるようにするには、以下の手順を使用する必要があります。

STEP 1 | 次のキーチェーンポップアッププロンプトで、macOSエンドポイントとのログインキーチェーンアクセスを許可するパスワードを入力します。



STEP 2 | GlobalProtect に VPN トンネルを確立させるには、常に許可を選択します。キーチェーンポップアッププロンプトは、クライアント証明書の有効期限が切れるまで表示されません。このポップアッププロンプトは、クライアント証明書が更新されたときに再び表示される場合があります。

許可を選択すると、ユーザーが*GlobalProtect*に接続するたびにキーチェーンポップアッププロンプトが表示されます。拒否を選択すると、*GlobalProtect*は*VPN*トンネルを確立できず、キーチェーンポップアッププロンプトが表示されます。*GlobalProtect*は、ログインキーチェーンへのアクセスを許可した後にのみ*VPN* トンネルを確立できます。

iOS 用 GlobalProtect アプリ

どこで使用できますか?	何が必要ですか?
• iOSエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.1 以降が必要です。

GlobalProtect™は、デスクトップコンピュータ、ラップトップ、タブレット、またはスマートフォンなどのエンドポイントで実行され、企業ネットワーク内の機密リソースを保護するのと同じセキュリティポリシーを使用してあなたを保護するアプリケーションです。GlobalProtect™は、イントラネット、プライベートクラウド、パブリッククラウド、インターネットトラフィックを保護し、世界中のどこからでも会社のリソースにアクセスできるようにします。

iOS用GlobalProtectアプリケーションのダウンロードおよびインストール

どこで使用できますか?	何が必要ですか?
• iOSエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.1 以降が必要です。

iOSエンドポイントをGlobalProtectネットワークに接続する前に、アプリをダウンロードしてインストールする必要があります。iOSエンドポイントがモバイルデバイス管理(MDM)システムで管理されている場合、管理者はGlobalProtectアプリを自動的にエンドポイントにプッシュし、VPN設定を構成している可能性があります。iOSエンドポイントにGlobalProtectアプリがまだインストールされていない場合は、App Storeからダウンロードできます。

アプリをダウンロードする前に、管理者からGlobalProtectポータルのIPアドレスまたはFQDNを取得する必要があります。さらに、管理者は、ポータルおよびゲートウェイへの接続に使用できるユーザ名とパスワードを確認する必要があります。これは通常、企業ネットワークに接続するときに使用するユーザ名とパスワードと同じです。管理者が生体認証(指紋認証、またはmacOS XデバイスのみFace ID)情報を使用してサインインすることを許可している場合は、まずユーザー名とパスワードで2回(1回は保存して認証を受ける)サインインする必要があります。その後、生体認証情報を使用してサインインできます。

必要な情報を収集したら、次の手順でアプリをダウンロードしてインストールできます。

STEP 1 | アプリストアを起動します。

STEP 2 | **`GlobalProtect`** を検索します。

STEP 3 | 検索結果から、**GlobalProtect™**を選択します。

STEP 4 | GlobalProtectアプリの製品ページから 、**GET**をタップします。

STEP 5 | アプリをインストールします。

STEP 6 | プロンプトが表示されたら、Apple IDでサインインします。

iOS用のGlobalProtectアプリの使用

どこで使用できますか?	何が必要ですか?
• iOSエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.1 以降が必要です。

このトピックは、エンドポイントにログインした後にGlobalProtectのログイン資格情報を入力する必要がある場合にのみ適用されます(シングルサインオンは無効です)。

通常、組織にはGlobalProtectユーザーがアプリのインストール後に透過的にログインできるようにすることを推奨します。透過的なGlobalProtectログインでエンドポイントにログインすると、GlobalProtectアプリは自動的に起動し、さらなるユーザーの介入なしに企業ネットワークに接続します。

設定でGlobalProtectの資格情報を入力する必要がある場合は、以下の適用可能な手順に従ってください。

STEP 1 | GlobalProtectポータルまたはゲートウェイに接続します。

以下のワークフローのいずれかを使用してGlobalProtectポータルまたはゲートウェイに接続します:

- 初回接続体験:
  1. GlobalProtect アプリの使用
  2. (オプション)エンドポイントでGlobalProtect通知を有効にしていない場合は、通知許可ダイアログが表示されます。GlobalProtect からの通知の送信を許可します。

     GlobalProtectによる通知の送信を許可しないと、次回アプリを起動するとリマインダーが表示されます。設定→**GlobalProtect**リンクをタップして通知の許可画面に移動

すると、通知を有効にできます。それでも通知を有効にしない場合は、この画面をスキップします。

3. GlobalProtectポータルのアドレスを入力してください。

4. (オプション)接続モードに応じて、**Connect (**接続)をクリックして接続を開始します。
5. 「GlobalProtect」Would to AddVPN Configurationsメッセージが表示されたら、以下の手順に従ってエンドポイントにVPN構成を追加します。
   1. GlobalProtectがエンドポイントにVPN構成を追加することを許可します。この設定により、VPNを使用しているときにGlobalProtectがエンドポイントのネットワークアクティビティをフィルタリングおよび監視できるようになります。

   2. VPN構成をエンドポイントに追加することを確認するために、iPhoneまたはiPadのパスコードを入力してください。

6. (オプション) エンドポイントがポータルサーバー証明書を使用してGlobalProtectポータルのアイデンティティを確認できない場合、サーバーアイデンティティを確認できませんというメッセージが表示されます。証明書を信頼する場合は、続行をタップして接続を続行します。
7. (オプション)プロンプトが表示されたら、**Username (**ユーザー名と **Password (**パスワード)を入力して **Sign In (**サインイン)をクリックします。

   管理者が生体認証(指紋認証、またはiOS XデバイスのみFace ID)情報を使用してサインインすることを許可している場合は、最初にユーザー名とパスワードで2回(1回は保存、もう1回は認証)サインインする必要があります。その後、生体認証情報を使用してサインインできます。

8. (オプション)マルチファクター認証を使用している場合、サインイン後にエンドポイントに送信されるGlobalProtect検証コードを入力し、次に続行をタップします。
9. (オプション)管理者がGlobalProtectアプリにウェルカムメッセージを表示するように設定している場合、接続が成功するとウェルカムメッセージが表示されます。ようこそメッセージを閉じてホーム画面に進みます。

10. (オプション)アプリに通知がある場合、接続が成功すると通知ダイアログが表示されます。通知ダイアログを閉じてホーム画面に進みます。

11. ホーム画面が表示されたら、接続が正常に確立されたことを確認してください。接続が成功した場合、ホーム画面には接続済みの状態が表示されます。

12. (オプション)デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available (**利用可能な最適な接続)ゲートウェイに自

動的に接続します。別のゲートウェイに接続するには、ホーム画面の下部にあるゲートウェイのドロップダウンをタップしてから、次のいずれかのオプションを使用します。

- ゲートウェイを手動で選択します(外部ゲートウェイのみ)。管理者がポータルエージェントの設定で手動の外部ゲートウェイを10個以上設定している場合は、ゲートウェイ検索オプションを使用して特定のゲートウェイを検索することもできます。

- 優先ゲートウェイとして設定するゲートウェイの[その他のオプション] ()アイコンをタップし、優先に設定を選択して優先ゲートウェイに割り当て、自動的に接続します。または、ゲートウェイを長押し(長押し)し、優先設定を選択します。

  優先ゲートウェイの割り当てを削除するには、優先ゲートウェイの[その他のオプション] ()アイコンをタップし、優先を削除をクリックします。または、ゲートウェイを長押し(長押し)してから、優先を削除することもできます。

- オンデマンド(リモートアクセスVPN)接続エクスペリエンス:

  GlobalProtect管理者がオンデマンド接続方式でGlobalProtectを構成する場合、GlobalProtectアプリを起動して手動で接続を開始する必要があります。接続が開始された後、接続するにはタップしてGlobalProtect接続を確立できます。管理者がGlobalProtectにユーザー資格情報を保存するように設定している場合、接続はさらなるユーザーの操作を必要とせずに確立されます。管理者がGlobalProtectにユーザー資格情報を保存するように設定していない場合、接続を確立するためにサインインする必要があります。

- 常時接続のエクスペリエンス

  GlobalProtectの管理者が常時接続接続方法でGlobalProtectを構成すると、接続は自動的に開始されます。管理者がGlobalProtectアプリをユーザー資格情報を保存するように設定するかどうかに応じて、アプリを起動せずにGlobalProtect接続を確立できます。管理者がGlobalProtectにユーザー資格情報を保存するように設定している場合、接続は自動的に確立され、ユーザーの操作は必要ありません。管理者がGlobalProtectにユーザー資格情報を保存するように設定していない場合、接続を確立するためにアプリを通じてサインインする必要があります。
- (オプション)管理者が常時接続接続方法でGlobalProtectを設定している場合、接続は自動的に開始されます。ホーム画面は接続中の状態を表示します。

  常時接続接続方法を使用すると、ホーム画面は接続中の状態を表示し、接続アイコンをタップしようとしたときに切断を防ぐための切断メッセージが表示されます。

STEP 2 | GlobalProtect接続に関する情報を表示します。

GlobalProtect接続を確立した後、GlobalProtectアプリを起動します。設定アイコンをタップして設定メニューを開きます。設定メニューから設定をタップして、接続に関する情報(ポータルアドレスや接続状態を含む)を表示します。

- 別のGlobalProtectポータルに接続したい場合は、ポータルアドレスをタップします。プロンプトが表示されたら、新しいポータルアドレスを入力し、接続をタップします。
- 外部ゲートウェイに接続している場合は、接続ステータスをタップして接続に関する追加の詳細を表示します(ネットワークSSIDおよびゲートウェイIPアドレス/FQDNを含む)。

STEP 3 | (オプション)保存したパスワードを変更します。

GlobalProtect管理者がGlobalProtectポータルエージェントをユーザー資格情報を保存に設定すると、資格情報は自動的にGlobalProtectアプリに保存されます。パスワードが期限切れになったり、RADIUSまたはAD管理者が次回のログイン時にパスワードの変更を要求した場合、アプリでパスワードを更新できます。この機能は、保護された拡張認証プロトコルMicrosoftチャレンジハンドシェイク認証プロトコルバージョン2 (PEAP-MSCHAPv2)を使用してRADIUSサーバーで認証されている場合にのみ有効です。

1. GlobalProtect アプリの使用
2. ホーム画面から、接続するにはタップします。
3. (オプション)プロンプトが表示されたら、古い ユーザー名とパスワードを入力し、サインインします。
4. GlobalProtectアプリがパスワードを更新するように促した場合、現在のパスワードを入力し、その後に新しいパスワードを入力します。
5. パスワードを再入力して新しいパスワードを確認します。
6. サインインして新しいパスワードでGlobalProtectに再接続します。

STEP 4 | (オプション) GlobalProtectから切断します。

管理者がオンデマンド接続方法でGlobalProtectを設定した場合、ホーム画面から切断するにはタップできます。

iOS用のGlobalProtectアプリから問題を報告する

どこで使用できますか?	何が必要ですか?
• iOSエンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.1 以降が必要です。

ネットワーク パフォーマンスが低下したり、ポータルやゲートウェイとの接続が確立されなかったりするなどの異常な動作が発生した場合は、管理者がアクセスできるStrata Logging Serviceに直接問題を報告できます。GlobalProtectアプリのログを手動で収集してメールで送信したり、クラウドドライブに保存したりする必要はなくなりました。

*GlobalProtect*アプリに問題を報告するオプションを表示するには、管理者が*GlobalProtect*ポータルでトラブルシューティングのためのGlobalProtectアプリログ収集を有効にする必要があります。

STEP 1 | GlobalProtectポータルまたはゲートウェイに接続します。

1. GlobalProtect アプリの使用
2. GlobalProtectポータルのアドレスを入力してください。
3. (オプション)接続モードに応じて、**Connect (**接続)をクリックして接続を開始します。
4. GlobalProtectがエンドポイントにVPN構成を追加することを許可します。この設定により、VPNを使用しているときにGlobalProtectがエンドポイントのネットワークアクティビティをフィルタリングおよび監視できるようになります。
5. VPN構成をエンドポイントに追加することを確認するために、iPhoneまたはiPadのパスコードを入力してください。
6. (オプション)プロンプトが表示されたら、**Username (**ユーザー名と **Password (**パスワード)を入力して **Sign In (**サインイン)をクリックします。
7. ホーム画面が表示されたら、接続が正常に確立されたことを確認してください。接続が成功した場合、ホーム画面には接続済みの状態が表示されます。
8. (オプション)デフォルトでは、エンドポイントは管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、Best Available(利用可能な最適な接続)ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、ホーム画面の下部にあるゲートウェイのドロップダウンをタップし、リストからゲートウェイを選択します (外部ゲートウェイのみ)。

STEP 2 | GlobalProtect接続に関する情報を表示します。

GlobalProtect接続を確立した後、GlobalProtectアプリを起動します。設定アイコンをタップして設定メニューを開きます。設定メニューから設定をタップして、接続に関する情報(ポータルアドレスや接続状態を含む)を表示します。

STEP 3 | エンドユーザーのエンドポイントからGlobalProtectから問題を報告します。

アプリを起動した後、ヘルプをタップしてエンドポイントから問題を報告します。

1. 問題を報告をタップします。

2. GlobalProtectアプリが診断テストを実行し、診断ログを含めることを有効にします。診断ログとトラブルシューティングログの両方が収集され、コンパクトなトラブルシューティングレポートとしてStrata Logging Serviceに送信されます。

   診断テストが正常に完了した後、GlobalProtectデバッグログファイルがエンドポイントからStrata Logging Serviceにアップロードされます。

   アプリが診断テストを実行し、診断ログを含めることを有効にしない場合、トラブルシューティングログのみが収集され、コンパクトなトラブルシューティングレポートとして*Strata Logging Service*に送信されます。*GlobalProtect*アプリは、`.json`形式で自動的に生成されたレポートファイル*(pan_gp.trb.log*または*pan_gp_trbl.log)*をチェックします。トラブルシューティングログに問題が見つからなかった場合、通知メッセージが表示されます。再試行をクリックして、*pan_gp.trb*.log*ファイルが存在するか確認します。

3. **Run Diagnostic Tests and Include Diagnostic Logs(**診断テストを実行して診断ログを含める**)**チェックボックスを選択します。
4. アプリがトラブルシューティングログを作成し、管理者のStrata Logging Serviceインスタンスにレポートを送信できるようにするには、**CONTINUE**をタップしてください。

   エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。

   エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。GlobalProtectアプリは、トンネルありまたはトンネルなしで診断テストを実行できます。例えば、アプリが接続してトンネルを通じて診断テストを実行する前に、GlobalProtectのログイン資格情報を入力したいかもしれません。

   アプリが診断テストを実行していることを確認するメッセージがポップアップしますが、これは**Run Diagnostic Tests and Include Diagnostic Logs (**診断テストを実行して診断ログを含める**)**チェックボックスを選択した場合のみです。

   アプリがStrata Logging Serviceにレポートを送信していることを確認するメッセージがポップアップします。

5. アプリがStrata Logging Serviceにレポートを正常に送信したことを確認するには、**DONE**をタップしてください。

iOS用 GlobalProtectアプリケーションのアンインストール

どこで使用できますか?	何が必要ですか?
• iOSエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.1 以降が必要です。

は、次の手順を使用してiOSエンドポイントからGlobalProtectアプリをアンインストールします。アプリをアンインストールすると、企業ネットワークへのVPNアクセスがなくなり、エンドポイントは会社のセキュリティポリシーによって保護されなくなることに注意してください。

STEP 1 | GlobalProtectアプリアイコンをアイコンが揺れるまで長押しします。

STEP 2 | アイコンの左上にある**×**をタップします。

STEP 3 | プロンプトが表示されたら、GlobalProtectを削除します。

STEP 4 | 完了をタップするか、ホームボタンを押してホーム画面に戻ります。

Android 用 GlobalProtect アプリ

どこで使用できますか?	何が必要ですか?
• Androidエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtect™は、デスクトップコンピュータ、ラップトップ、タブレット、またはスマートフォンなどのエンドポイントで実行され、企業ネットワーク内の機密リソースを保護するのと同じセキュリティポリシーを使用してあなたを保護するアプリケーションです。GlobalProtect™は、イントラネット、プライベートクラウド、パブリッククラウド、インターネットトラフィックを保護し、世界中のどこからでも会社のリソースにアクセスできるようにします。

次のトピックでは、GlobalProtect app for Androidをインストールして使用する方法を説明します。

- Android用GlobalProtectアプリケーションのダウンロードおよびインストール
- ChromebooksのAndroid用GlobalProtectアプリケーションのダウンロードおよびインストール
- Android用 GlobalProtectアプリケーションを使用する
- Android用GlobalProtectアプリからの問題を報告する
- Android用GlobalProtectアプリケーションの接続を解除する
- Android用GlobalProtectアプリケーションのアンインストール
- ChromebookからAndroid用GlobalProtectアプリをアンインストールします。

Android用GlobalProtectアプリケーションのダウンロードおよびインストール

どこで使用できますか?	何が必要ですか?
• Androidエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

AndroidエンドポイントをGlobalProtectネットワークに接続する前に、アプリをダウンロードしてインストールする必要があります。Androidエンドポイントがモバイルデバイス管理（MDM）システムで管理されている場合、管理者はGlobalProtectアプリを自動的にエンドポイントにプッシュし、VPN設定を構成した可能性があります。AndroidエンドポイントにGlobalProtectアプリがまだない場合は、Google Playからダウンロードできます。

アプリをダウンロードする前に、管理者からGlobalProtectポータルのIPアドレスまたはFQDNを取得する必要があります。さらに、管理者は、ポータルおよびゲートウェイへの接続に使用できるユーザ名とパスワードを確認する必要があります。これは通常、企業ネットワークに接続するときに使用するユーザ名とパスワードと同じです。

必要な情報を収集したら、次の手順でアプリをダウンロードしてインストールできます。

STEP 1 | Google Playを起動します。

STEP 2 | **`GlobalProtect`** を検索します。

STEP 3 | 検索結果から、**GlobalProtect**を選択します。

STEP 4 | GlobalProtectアプリの製品ページから インストールをタップします。

STEP 5 | プロンプトが表示されたら、GlobalProtectがアクセスする必要がある情報を確認し、同意します。

ChromebooksのAndroid用GlobalProtectアプリケーションのダウンロードおよびインストール

どこで使用できますか?	何が必要ですか?
• Android (Chromebook) エンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

ChromebookでAndroid版GlobalProtectアプリを使用するには、アプリをダウンロードしてインストールする必要があります。ChromebookがWorkspace ONEまたはGoogle管理コンソールで管理されている場合、管理者がGlobalProtectアプリを自動的にエンドポイントにプッシュし、VPN設定を行っている可能性があります。ChromebookにAndroid用のGlobalProtectアプリがまだインストールされていない場合は、Google Playストアからダウンロードできます。

アプリをダウンロードする前に、管理者からGlobalProtectポータルのIPアドレスまたはFQDNを取得する必要があります。さらに、管理者は、ポータルおよびゲートウェイへの接続に使用できるユーザ名とパスワードを確認する必要があります。これは通常、企業ネットワークに接続するときに使用するユーザ名とパスワードと同じです。

必要な情報を収集したら、次の手順でアプリをダウンロードしてインストールできます。

Android 用 *GlobalProtect* アプリケーションは特定の Chromebook でのみサポートされています。*Chrome OS*用の*GlobalProtect*アプリのバージョン*4.1.x*を使用していた場合、アプリは利用できなくなりました。*Android*アプリをサポートする*Chrome OS*システムへのアップグレードを検討し、*Android*用の*GlobalProtect*アプリを使用してください。

STEP 1 | ChromebookでGoogle Playストアアプリを有効にします。

1. (オプション) Chrome OSバージョン52以前を実行しているChromebookの場合は、Chromebookオペレーティングシステムをアップデートします。
2. Chromebookから、画面右下のアカウント写真をクリックします。
3. **Settings**[設定]を選択します。
4. Google Playストアエリアで、**Chromebook**の**Google Play**ストアを有効にします。

   このオプションが利用できない場合、*Chromebook*は*Android*アプリをサポートしていません。
5. メッセージが表示されたら、**[Get Started (**はじめに**)]**をクリックしてGoogle Playストアを起動します。
6. サービス利用規約に同意します。
7. ようこそページで、Google Playストアにサインインします。
8. Google Playの利用規約に同意します。

STEP 2 | Androidエンドポイント用のGlobalProtectアプリをChromebookにダウンロードしてインストールします。

1. Google Playストアアプリを開きます。
2. **GlobalProtect App**を検索します。
3. GlobalProtectアプリのアイコンをクリックします。
4. **INSTALL**をクリックし、画面の指示に従ってアプリのインストールを完了します。

Android用 GlobalProtectアプリケーションを使用する

どこで使用できますか?	何が必要ですか?
• Androidエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

このトピックは、エンドポイントにログインした後にGlobalProtectのログイン資格情報を入力する必要がある場合にのみ適用されます(シングルサインオンは無効です)。

通常、組織にはGlobalProtectユーザーがアプリのインストール後に透過的にログインできるようにすることを推奨します。透過的なGlobalProtectログインでエンドポイントにログインすると、GlobalProtectアプリは自動的に起動し、さらなるユーザーの介入なしに企業ネットワークに接続します。

設定でGlobalProtectの資格情報を入力する必要がある場合は、以下の適用可能な手順に従ってください。

STEP 1 | GlobalProtectポータルまたはゲートウェイに接続します。

以下のワークフローのいずれかを使用してGlobalProtectポータルまたはゲートウェイに接続します:

- 初回接続体験:
  1. GlobalProtect アプリの使用
  2. GlobalProtectポータルのアドレスを入力してください。
  3. (オプション)接続モードに応じて、**Connect (接続)**をクリックして接続を開始します。
  4. (オプション) エンドポイントがポータルサーバー証明書を使用してGlobalProtectポータルのアイデンティティを確認できない場合、サーバーアイデンティティを確認できませ

んというメッセージが表示されます。証明書を信頼する場合は、続行をタップして接続を続行します。

5. (オプション)プロンプトが表示されたら、**Username (**ユーザー名と **Password (**パスワード)を入力して **Sign In (**サインイン)をクリックします。

   管理者が生体認証(指紋)情報を使用してサインインすることを許可している場合、最初にユーザー名とパスワードでサインインする必要があります。その後、生体情報を使用してサインインできます。

6. 接続要求メッセージが表示されたら、**OK**をタップしてGlobalProtectがエンドポイントにVPN接続を設定できるようにします。

7. (オプション)マルチファクター認証を使用している場合、サインイン後にエンドポイントに送信されるGlobalProtect検証コードを入力し、次に続行をタップします。
8. (オプション)管理者がGlobalProtectアプリにウェルカムメッセージを表示するように設定している場合、接続が成功するとウェルカムメッセージが表示されます。ウェルカムメッセージの外をタップしてホーム画面に進みます。

9. (オプション)アプリに通知がある場合、接続が成功すると通知ダイアログが表示されます。通知ダイアログを閉じてホーム画面に進みます。

10. ホーム画面が表示されたら、接続が正常に確立されたことを確認してください。接続が成功した場合、ホーム画面には接続済みの状態が表示されます。

11. (オプション)管理者が常時接続接続方法でGlobalProtectを設定している場合、接続は自動的に開始されます。ホーム画面は接続中の状態を表示します。

    常時接続接続方法を使用すると、ホーム画面は接続中の状態を表示し、接続アイコンをタップしようとしたときに切断を防ぐための切断メッセージが表示されます。

12. (オプション)デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available (**利用可能な最適な接続)ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、ホーム画面の下部にあるゲートウェイのドロップダウンをタップし、リストからゲートウェイを選択します (外部ゲートウェイのみ)。

- オンデマンド(リモートアクセスVPN)接続体験:

  GlobalProtectの管理者がオンデマンド接続方法でGlobalProtectを構成すると、接続を手動で開始するためにGlobalProtectアプリを起動する必要があります。接続が開始された後、接続するにはタップしてGlobalProtect接続を確立できます。管理者がGlobalProtectにユーザー資格情報を保存するように設定している場合、接続はさらなるユーザーの操作を必要とせずに確立されます。管理者がGlobalProtectにユーザー資格情報

を保存するように設定していない場合、接続を確立するためにサインインする必要があります。

- 常時接続体験:

  GlobalProtectの管理者が常時接続接続方法でGlobalProtectを構成すると、接続は自動的に開始されます。管理者がGlobalProtectアプリをユーザー資格情報を保存するように設定するかどうかに応じて、アプリを起動せずにGlobalProtect接続を確立できます。管理者がGlobalProtectにユーザー資格情報を保存するように設定している場合、接続は自動的に確立され、ユーザーの操作は必要ありません。管理者がGlobalProtectにユーザー資格情報を保存するように設定していない場合、接続を確立するためにアプリを通じてサインインする必要があります。

STEP 2 | GlobalProtect接続に関する情報を表示します。

GlobalProtect接続を確立した後、GlobalProtectアプリを起動します。設定アイコンをタップして設定メニューを開きます。設定メニューから設定をタップして、接続に関する情報(ポータルアドレスや接続状態を含む)を表示します。

- 別のGlobalProtectポータルに接続したい場合は、ポータルアドレスをタップします。プロンプトが表示されたら、新しいポータルアドレスを入力し、接続をタップします。

- 外部ゲートウェイに接続している場合は、接続ステータスをタップして接続に関する追加の詳細を表示します(ネットワークSSIDおよびゲートウェイIPアドレス/FQDNを含む)。

STEP 3 | (オプション)保存したパスワードを変更します。

GlobalProtect管理者がGlobalProtectポータルエージェントをユーザー資格情報を保存に設定すると、資格情報は自動的にGlobalProtectアプリに保存されます。パスワードが期限切れになったり、RADIUSまたはAD管理者が次回のログイン時にパスワードの変更を要求した場合、アプリでパスワードを更新できます。この機能は、保護された拡張認証プロトコルMicrosoftチャレンジハンドシェイク認証プロトコルバージョン2 (PEAP-MSCHAPv2)を使用してRADIUSサーバーで認証されている場合にのみ有効です。

1. GlobalProtect アプリの使用
2. ホーム画面から、接続するにはタップします。
3. (オプション)プロンプトが表示されたら、古い ユーザー名とパスワードを入力し、サインインします。
4. GlobalProtectアプリがパスワードを更新するように促した場合、現在のパスワードを入力し、その後に新しいパスワードを入力します。
5. パスワードを再入力して新しいパスワードを確認します。
6. サインインして新しいパスワードでGlobalProtectに再接続します。

STEP 4 | (オプション) GlobalProtectから切断します。

管理者がオンデマンド接続方法でGlobalProtectを設定した場合、ホーム画面から切断するにはタップできます。

Android用GlobalProtectアプリからの問題を報告する

どこで使用できますか?	何が必要ですか?
• Androidエンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

ネットワーク パフォーマンスが低下したり、ポータルやゲートウェイとの接続が確立されなかったりするなどの異常な動作が発生した場合は、管理者がアクセスできるStrata Logging Serviceに直接問題を報告できます。GlobalProtectアプリのログを手動で収集してメールで送信したり、クラウドドライブに保存したりする必要はなくなりました。

*GlobalProtect*アプリに問題を報告するオプションを表示するには、管理者が*GlobalProtect*ポータルでトラブルシューティングのためのGlobalProtectアプリログ収集を有効にする必要があります。

STEP 1 | GlobalProtectポータルまたはゲートウェイに接続します。

1. GlobalProtect アプリの使用
2. GlobalProtectポータルのアドレスを入力してください。
3. (オプション)接続モードに応じて、**Connect (**接続)をクリックして接続を開始します。
4. (オプション)プロンプトが表示されたら、**Username (**ユーザー名と **Password (**パスワード)を入力して **Sign In (**サインイン)をクリックします。
5. 接続要求メッセージが表示されたら、**OK**をタップしてGlobalProtectがエンドポイントにVPN接続を設定できるようにします。
6. ホーム画面が表示されたら、接続が正常に確立されたことを確認してください。接続が成功した場合、ホーム画面には接続済みの状態が表示されます。
7. (オプション)デフォルトでは、エンドポイントは管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、Best Available(利用可能な最適な接続)ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、ホーム画面の下部にあるゲートウェイのドロップダウンをタップし、リストからゲートウェイを選択します (外部ゲートウェイのみ)。

STEP 2 | GlobalProtect接続に関する情報を表示します。

GlobalProtect接続を確立した後、GlobalProtectアプリを起動します。設定アイコンをタップして設定メニューを開きます。設定メニューから設定をタップして、ポータルアドレスや接続状況を含む接続に関する情報を表示します。

STEP 3 | エンドユーザーのエンドポイントからGlobalProtectから問題を報告します。

アプリを起動した後、ヘルプをタップしてエンドポイントから問題を報告します。

1. 問題を報告をタップします。

2. GlobalProtectアプリが診断テストを実行し、診断ログを含めることを有効にします。診断ログとトラブルシューティングログの両方が収集され、コンパクトなトラブルシューティングレポートとしてStrata Logging Serviceに送信されます。

   診断テストが正常に完了した後、GlobalProtectデバッグログファイルがエンドポイントからStrata Logging Serviceにアップロードされます。

   アプリが診断テストを実行し、診断ログを含めることを有効にしない場合、トラブルシューティングログのみが収集され、コンパクトなトラブルシューティングレポートとして*Strata Logging Service*に送信されます。*GlobalProtect*アプリは、`.json`形式で自動的に生成されたレポートファイル*(pan_gp.trb.log*または*pan_gp_trbl.log)*をチェックします。トラブルシューティングログに問題が見つからなかった場合、通知メッセージが表示されます。再試行をクリックして、*pan_gp.trb*.log*ファイルが存在するか確認します。

3. **Run Diagnostic Tests and Include Diagnostic Logs(**診断テストを実行して診断ログを含める**)**チェックボックスを選択します。
4. アプリがトラブルシューティングログを作成し、管理者のStrata Logging Serviceインスタンスにレポートを送信できるようにするには、**CONTINUE**をタップしてください。

   エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。

   エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。GlobalProtectアプリは、トンネルありまたはトンネルなしで診断テストを実行できます。例えば、アプリが接続してトンネルを通じて診断テストを実行する前に、GlobalProtectのログイン資格情報を入力したいかもしれません。

   アプリが診断テストを実行していることを確認するメッセージがポップアップしますが、これは**Run Diagnostic Tests and Include Diagnostic Logs (**診断テストを実行して診断ログを含める**)**チェックボックスを選択した場合のみです。

   アプリがStrata Logging Serviceにレポートを送信していることを確認するメッセージがポップアップします。

5. アプリがStrata Logging Serviceにレポートを正常に送信したことを確認するには、**DONE**をタップしてください。

Android用GlobalProtectアプリケーションの接続を解除する

どこで使用できますか?	何が必要ですか?
• Androidエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

管理者がGlobalProtectの接続方法を常時接続に設定している場合、GlobalProtectアプリを切断できます。たとえば、ホテルでGlobalProtect仮想プライベートネットワーク（VPN）が機能しておらず、VPN障害によってインターネットに接続できない場合、アプリを切断したい場合があります。GlobalProtectアプリを切断した後は、セキュアでない通信（VPNなし）を使用してインターネットに接続できます。

GlobalProtectアプリを切断できる方法、時間、回数は、管理者がGlobalProtectサービス(PanGPS)をどのように構成するかによって異なります。この構成では、アプリを完全に切断できないようにしたり、チャレンジに正しく応答した後にのみアプリを切断したりすることができます。

構成にチャレンジが含まれている場合、GlobalProtectアプリは次のいずれかを求めるプロンプトを表示します。

- アプリを切断したい理由
- パスコード

チャレンジにパスコードが含まれる場合は、GlobalProtect管理者またはヘルプデスク担当者に電話で問い合わせることをお勧めします。通常、管理者は事前にパスコードを電子メール(GlobalProtectの新規ユーザー用)または組織のウェブサイトに掲載して提供します。また、システム停止やシステム障害が発生した場合には、管理者が電話でパスコードを提供することもあります。

次の手順では、アプリを切断してチャレンジを渡す方法について説明します。

STEP 1 | GlobalProtectアプリの接続を解除します。

1. GlobalProtect アプリの使用
2. 設定アイコンをタップして設定メニューを開きます。
3. 設定メニューから**DISCONNECT**をタップします。

[Disconnect (接続解除***)]***オプションは、*GlobalProtect*エージェント構成でアプリケーションの切断が許可されている場合にのみ表示されます。構成で、チャレンジに応答することなく *GlobalProtect* アプリを切断できる場合、*GlobalProtect* アプリは追加のアクションを必要とせずに終了します。

STEP 2 | 必要に応じて、1つ以上の課題に対応します。

プロンプトが表示されたら、次の情報を入力します。

- **Reason (**理由**):** GlobalProtectアプリを切断した理由。

- **Passcode (**パスコード**):** 通常は、アプリを切断する必要がある既知の問題やイベントに基づいて、管理者が事前に提供するパスコードです。

Android用GlobalProtectアプリケーションのアンインストール

どこで使用できますか?	何が必要ですか?
• Androidエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtect設定で場合、AndroidエンドポイントからGlobalProtectアプリケーションをアンインストールするには、以下の手順を実行します。アプリをアンインストールすると、企業ネットワークへのVPNアクセスがなくなり、エンドポイントは会社のセキュリティポリシーによって保護されなくなることに注意してください。

STEP 1 | 設定アプリを起動します。

STEP 2 | **[Apps & notifications (アプリケーションと通知)]**をタップします。

STEP 3 | **GlobalProtect**をタップします。

STEP 4 | **[Uninstall (アンインストール)]**をタップします。

ChromebookからAndroid用GlobalProtectアプリをアンインストールします。

どこで使用できますか?	何が必要ですか?
• Android (Chromebook) エンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

、ChromebookからAndroid用GlobalProtectアプリをアンインストールするには、次の手順を使用します。アプリをアンインストールすると、企業ネットワークへのVPNアクセスがなくなり、エンドポイントは会社のセキュリティポリシーによって保護されなくなることに注意してください。

STEP 1 | Google Playストアアプリを開きます。

STEP 2 | Google Play検索バーの隣にあるメニューボタン()をクリックします。

STEP 3 | **[Apps & games (アプリとゲーム)]** > **[My apps & games (イアプリとゲーム)]**を選択します。

STEP 4 | **[INSTALLED (インストール済み)]**を選択します。

STEP 5 | このデバイスの領域から、**GlobalProtect**を選択します。

STEP 6 | **[UNINSTALL (アンインストール)]**をクリックします。

Linux用GlobalProtectアプリ

どこで使用できますか?	何が必要ですか?
• Linuxエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtect™は、エンドポイント(デスクトップコンピュータ、ノートパソコン、またはサーバ)上で実行されるプログラムで、企業ネットワーク内の機密リソースを保護するのと同じセキュリティポリシーを使用してお客様を保護します。GlobalProtect™は、イントラネット、プライベートクラウド、パブリッククラウド、インターネットトラフィックを保護し、世界中のどこからでも会社のリソースにアクセスできるようにします。

以下のセクションでは、Linux 用のGlobalProtectアプリをインストールして使用する手順について説明します。

- Linux用GlobalProtectアプリケーションのダウンロードおよびインストール
- GlobalProtect App for Linuxの使用
- Linux用GlobalProtectアプリケーションからの問題の報告
- GlobalProtect App for Linuxを無効にする
- Linux用のGlobalProtect Appをアンインストールする

Linux用GlobalProtectアプリケーションのダウンロードおよびインストール

どこで使用できますか?	何が必要ですか?
• Linuxエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtect では、Linux デバイスに GlobalProtect アプリをインストールする方法として、GUI ベースのインストールバージョンと CLI バージョンの 2 つが用意されています。グラフィカルインタフェースをサポートするサポートされているLinuxオペレーティングシステムを使用している場合は、GUIバージョンのGlobalProtectをインストールできます。それ以外の場合は、CLIバージョンのGlobalProtectアプリをダウンロードしてインストールします。

- GlobalProtect for LinuxのGUIバージョンをダウンロードしてインストールする
- GlobalProtect for LinuxのCLIバージョンのダウンロードとインストール

GlobalProtect for LinuxのGUIバージョンをダウンロードしてインストールする

Linuxデバイスがグラフィカルユーザーインターフェースをサポートしている場合は、以下の手順を実行してGUIバージョンのGlobalProtect for Linuxをインストールします。

STEP 1 | Linux用GlobalProtectアプリケーションをダウンロードします。

1. カスタマーサポート ポータルにログインします。ユーザー名とパスワードの認証情報を入力すると、認証が行われ、サポートサイトにログインします。
2. **Updates**（更新） > **Software Updates**（ソフトウェア更新）を選択します。
3. GlobalProtect Agent for Linux でフィルタリングし、関連する TGZ ファイルをダウンロードします。
4. パッケージからファイルを展開します。

```
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
```

サポートされるオペレーティングシステムのバージョンに対応した複数のインストールパッケージが表示されます。DebianとUbuntuの場合はDEB、CentOSとRed Hatの場合はRPMです。GUIバージョンのパッケージはGlobalProtect_UIプレフィックスで表記される。

STEP 2 | (オプション) Linuxエンドポイントで手動でプロキシサーバー構成を使用する必要がある場合は、プロキシ設定を構成します。

*Linux*用の*GlobalProtect*アプリは、基本的なプロキシサーバー構成のみをサポートしていますが、プロキシ自動構成*(PAC)*ファイルの使用とプロキシ認証はサポートしていません。

Linux用のGlobalProtectアプリは、`/etc/environment`ファイル内のHTTP_PROXY、HTTPS_PROXY、NO_PROXY環境変数からプロキシ設定を取得します。後でシステムプロキシ構成を変更する場合は、GlobalProtectの実行元端末がプロキシ環境変数を使用していることを確認します。新しい設定が表示されない場合は、ログアウトしてから再度ログインして新しい設定を有効にしてください。

*HTTP__PROXY*変数または*HTTPS__PROXY*変数を設定している場合は、*GlobalProtect*ポータルが*NO__PROXY*変数に設定されている設定と一致することを確認してください。

1. Linuxエンドポイントにプロキシを設定するには、HTTP_PROXY環境変数またはHTTPS_PROXY環境変数を編集します(たとえば、`HTTPS_PROXY="https: / / yourproxy.local:8080"`)。
2. プロキシから除外するIPアドレスまたはドメイン名を設定するには、NO_PROXY環境変数を編集します(例：`NO_PROXY="www.gpqa.com"`)。

   複数のIPアドレスまたはドメイン名を区切るには、カンマを使用します。GlobalProtectアプリ5.1.6以降、IPアドレスまたはドメイン名にワイルドカード文字(*)を使用できます(例：`NO_PROXY= " * .domain.com "`)。

STEP 3 | Linux用のGlobalProtectアプリのGUIバージョンをインストールします。

GlobalProtectアプリUI配布パッケージをインストールするには、**`$ . / gp_install.sh`**コマンドを使用します。

```
$ ./gp_install.sh --help Usage: $ sudo ./gp_install [--cli-only |
 --arm | --help] --cli-only:CLIのみ --arm:ARMオプションなし:UI
```

インストールが完了すると、GlobalProtectアプリが自動的に起動します。

STEP 4 | 使用したインストール方法に応じて、Linuxオペレーティングシステムまたは SSHセッションからログアウトし、ログインし直します。

この手順は、インストール中の新しいパッケージの更新がGlobalProtectアプリに適用されるようにするために必要です。

STEP 5 | ポータルアドレスを指定し、接続プロセスを開始するように求められたら資格情報を入力します。

STEP 6 | (オプション)証明書をインポートするには、次の手順を実行します。

証明書ベースの認証のためにクライアント証明書をエンドポイントに事前デプロイする場合は、証明書をエンドポイントにコピーしてインポートし、GlobalProtect アプリで使用することができます。**globalprotect import-certificate --location *<location>*** コマンドを使用して、エンドポイントに証明書をインポートします。プロンプトが表示されたら、証明書パスワードを指定する必要があります。

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12 パスコードを入力してください:証明書のインポートに成功しました。
```

GlobalProtect for LinuxのCLIバージョンのダウンロードとインストール

Linux デバイスが GUI をサポートしていない場合は、次の手順を実行して Linux 用の GlobalProtect アプリをインストールします。Linux版GlobalProtectアプリは、DEB、RPM、TARのインストールパッケージをサポートしています。

STEP 1 | Linux用GlobalProtectアプリケーションをダウンロードします。

1. IT管理者からアプリパッケージを入手し、TGZファイルをLinuxエンドポイントにコピーします。

   たとえば、macOSのエンドポイントにパッケージをダウンロードした場合、ターミナルを開いてからファイルをコピーすると、

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

   ここで、***<DestinationFolder>***はTGZファイルを保存する~/pkgs/などの場所です。

2. Linuxエンドポイントから、パッケージを解凍します。

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

   パッケージを解凍すると、インストールパッケージ(Ubuntu用のDEBとCentOSとRed Hat用のRPM)と、パッケージをインストールおよびアンインストールするためのスクリプトが表示されます。

STEP 2 | (オプション) Linuxエンドポイントで手動でプロキシサーバー構成を使用する必要がある場合は、プロキシ設定を構成します。

Linux用のGlobalProtectアプリは、基本的なプロキシサーバー構成のみをサポートしていますが、プロキシ自動構成(PAC)ファイルの使用とプロキシ認証はサポートしていません。

Linux用のGlobalProtectアプリは、`/etc/environment`ファイル内のHTTP_PROXY、HTTPS_PROXY、NO_PROXY環境変数からプロキシ設定を取得します。後でシステムプロキシ構成を変更する場合は、GlobalProtectの実行元端末がプロキシ環境変数を使用していることを確認します。新しい設定が表示されない場合は、ログアウトしてから再度ログインして新しい設定を有効にしてください。

HTTP__PROXY変数またはHTTPS__PROXY変数を設定している場合は、GlobalProtectポータルがNO__PROXY変数に設定されている設定と一致することを確認してください。

1. Linuxエンドポイントにプロキシを設定するには、HTTP_PROXY環境変数またはHTTPS_PROXY環境変数を編集します(たとえば、`HTTPS_PROXY="https: / / yourproxy.local:8080"`)。
2. プロキシから除外するIPアドレスまたはドメイン名を設定するには、NO_PROXY環境変数を編集します(例：`NO_PROXY="www.gpqa.com"`)。

   複数のIPアドレスまたはドメイン名を区切るには、カンマを使用します。GlobalProtectアプリ5.1.6以降、IPアドレスまたはドメイン名にワイルドカード文字(*)を使用できます(例：`NO_PROXY= " * .domain.com "`)。

STEP 3 | **CLI Only**コマンドを使用してアプリパッケージをインストールします。

```
$ ./gp_install.sh --help Usage: $ sudo ./gp_install [--cli-only |
 --arm | --help] --cli-only:CLIのみ --arm:ARMオプションなし:UI
```

STEP 4 | (オプション)CLI モードを変更します。

コマンドは、コマンドラインモードまたはプロンプトモードで実行できます。コマンドラインモードでは、完全な GlobalProtect コマンドを指定する必要があります。プロンプトモードは、コマンドのみを指定し(アプリ名は指定せず) 、 コマンドラインモードよりも詳細な出力を表示します。

1. プロンプトモードに切り替えるには、引数を指定せずに **globalprotect**と入力します。

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

2. プロンプトモードを終了するには、**quit**と入力します。

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


STEP 5 | Linux用GlobalProtectアプリのヘルプを表示します。

プロンプトモード:

```
>> help 使用方法: 次のコマンドのみサポートされています。 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 reddiscovery remove-user -- clear
 credential resubmit-hip -- resubmit hip information set-log -- set
 debug level show -- show information
```

コマンドラインモード:

```
user@linuxhost:~$ globalprotect help 使用方法:次のコマンドのみサポートさ
れます。 collect-log -- collect log information connect -- connect
 to server disconnect -- disconnect 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
```

STEP 6 | Linux用のGlobalProtectアプリのCLIバージョンを使用します。

GlobalProtect App for Linuxの使用

どこで使用できますか?	何が必要ですか?
• Linuxエンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

GlobalProtectはLinux用のGlobalProtectアプリの2つのバージョンをサポートしています:Linuxデバイスが GUIをサポートしている場合の1つのバージョンと、GUIをサポートしていない場合のCLIバージョン。

- Linux用のGlobalProtectアプリのGUIバージョンを使用する
- Linux用のGlobalProtectアプリのCLIバージョンを使用します。

Linux用のGlobalProtectアプリのGUIバージョンを使用する

Linux用のGlobalProtectアプリのGUIバージョンを使用するには、これらの手順を完了してください。

STEP 1 | GlobalProtectウィンドウにFQDNまたはGlobalProtectポータルのIPアドレスを入力し、接続をクリックします。

GUIバージョンのGlobalProtectアプリをダウンロードしてインストールした後、GlobalProtectアプリが自動的に起動します。

1. (任意)複数のポータルがアプリに保存されている場合は、[ポータル]ドロップダウンからポータルを選択します。デフォルトでは、最後に接続されたポータルが[ポータル]ドロップダウンから事前に選択されています。

2. ポータルの **Username** (ユーザー名)と **Password** (パスワード)を入力し、**Sign in** (サインイン)をクリックします。

   ほとんどの場合、企業ネットワークに接続するときに使用するのと同じユーザー名とパスワードを使用できます。サインインすると、GlobalProtectポータルのステータスが**Connected** (接続済み)と表示されます。

3. （オプション）デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available**（利用可能な最適な接続）ゲートウェイ

に自動的に接続します。別のゲートウェイに接続するには、ゲートウェイドロップダウンをクリックし、次のオプションのいずれかを使用します:

- ゲートウェイを手動で選択します(外部ゲートウェイのみ)。

  このオプションは、管理者が手動ゲートウェイ選択を有効にした場合にのみ利用可能です。

- 優先ゲートウェイに割り当てて自動的に接続します:

  1. アプリのステータスパネルの右上のメニューから、優先ゲートウェイを選択してGlobalProtectを開きます:優先ゲートウェイダイアログ。
  2. 利用可能なゲートウェイのリストから、優先ゲートウェイとして設定したいゲートウェイを選択し、優先として設定をクリックします。
  3. ダイアログを閉じます。

  ゲートウェイに自動的に接続したくない場合は、優先ゲートウェイの割り当てを削除することもできます:

  1. アプリのステータスパネルの右上のメニューから、優先ゲートウェイを選択してGlobalProtectを開きます:優先ゲートウェイダイアログ。
  2. 利用可能なゲートウェイのリストから、優先ゲートウェイを選択し、優先を削除をクリックします。
  3. ダイアログを閉じます。

STEP 2 | GlobalProtectアプリケーションを開きます。

GlobalProtectシステム トレイ アイコンをクリックして、アプリ インターフェースを起動します。

STEP 3 | ネットワーク接続に関する情報を表示します。

アプリを起動した後、アプリのパネルの右上にあるメニュー(　)を選択し、設定を選択してGlobalProtect設定パネルを開き、ネットワーク接続に関する情報を表示するために次のタブのいずれかを選択します：

- **General**（一般）—GlobalProtect アカウントに関連付けられているユーザー名とポータルを表示します。このタブからポータルを追加、削除、または変更することもできます。

- **Connection (接続)**—GlobalProtectアプリ用に設定されたゲートウェイを表示し、各ゲートウェイに関する次の情報を提供します。
  - Gateway Name（ゲートウェイ名）
  - トンネルのステータス
  - 認証状態
  - 接続タイプ
  - ゲートウェイ IP アドレスまたは FQDN（外部モードでのみ使用可能）

  内部モードの場合、***Connection***（接続）タブには使用可能なゲートウェイ一覧が表示されます。外部モードの場合、***Connection (接続)***タブには接続先のゲートウェイと、ゲートウェイに関する追加の詳細(ゲートウェイの*IP*アドレス、位置、稼働時間など)が表示されます。

- トラブルシューティング—あなたがログを収集することを可能にし、ログレベルを設定します。

  詳細な分析のために、*GlobalProtect*アプリがトラブルシューティング ログ、診断ログ、またはその両方をStrata Logging Serviceに送信するには、トラブルシューティング用の GlobalProtect アプリログコレクションを有効にするようにGlobalProtectポータルを構成する必要があります。また、 HTTPS ベースの送信先 URL を構成 には、プローブする *Web* サーバー/リソースの *IP* アドレスまたは完全修飾ドメイン名を含めることができ、エンド ユーザーのエンドポイントでの待機時間やネットワーク パフォーマンスなどの問題を特定できます。

STEP 4 | (オプション)新しいパスワードを使用してログインします。

*GlobalProtect*管理者が*GlobalProtect*ポータルエージェントをユーザー資格情報を保存に設定すると、資格情報は自動的に*GlobalProtect*アプリに保存されます。企業ネットワークにアクセスするためのパスワードが変更された場合、新しいパスワードを使用して*GlobalProtect*にログインする必要があります。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. アプリのパネルの右上にあるメニュー(　)を選択し、次に設定を選択して**GlobalProtect**設定パネルを開きます。
3. **GlobalProtect**設定パネルの一般タブで、サインアウトしてGlobalProtectアプリから保存されたユーザー資格情報をクリアします。
4. ユーザー資格情報をクリアした後、新しいユーザー名とパスワードでGlobalProtectに再接続できます。

STEP 5 | (オプション) GlobalProtectから切断します。

管理者がオンデマンド接続方法でGlobalProtectを設定した場合、ステータスパネルの切断をクリックすることでGlobalProtectから切断できます。

Linux用のGlobalProtectアプリのCLIバージョンを使用します。

Linux用のGlobalProtect™アプリのコマンドラインインターフェース(CLI)を使用すると、GlobalProtectアプリに共通のタスクを実行できます。以下の例は、コマンドラインモードでの出力を表示します。プロンプトモードで同じコマンドを実行するには、**globalprotect**プレフィックスなしで入力します（詳細については、Linux用GlobalProtectアプリのダウンロードとインストールを参照してください）。

GlobalProtectポータルに接続します:

globalprotect connect --portal *<gp-portal>*コマンドを使用します。ここで***<gp-portal>***は、GlobalProtectポータルのIPアドレスまたはFQDNです。

以下に例を示します。

```
user@linuxhost:~$ globalprotect connect --portal
 myportal.example.com 設定を取得中...myportal.example.comから切断 -
 portal:local:ログイン資格情報を入力してください ユーザー名:user1 パスワード:設定を取得中...ネットワークを発見中...接続中...接続済み
```

証明書ベースの認証を使用する場合、ルートCA証明書なしで初めて接続すると、GlobalProtectアプリとGlobalProtectポータルが証明書を交換します。GlobalProtectアプリは証明書エラーを表示します。このエラーを認識しないと認証できません。次回接続すると、証明書エラーメッセージは表示されません。

```
user@linuxhost:~$ globalprotect connect
 --portal myportal.example.com 設定を取得
```

```
中...                                                    切断されまし
た。セキュリティ証明書に問題があるため、10.3.188.61のアイデンティティ
を確認できません。問題を解決するために、組織のヘルプデスクに連絡してく
ださい。警告:10.3.188.61との通信が危険にさらされている可能性がありま
す。この接続を続行しないことをお勧めします。エラーの詳細:続行しますか(y/
n)?y 設定を取得中...
  切断されました 10.3.188.61 - portal:local:ログイン資格
情報を入力してください ユーザー名:user1 パスワード:設定を取得
中...                                                    ネットワークを発見
中...接続中...接続済み
```

コマンドでユーザー名を指定することもできます。***--username <username>***オプションを使用します。*GlobalProtect*アプリは認証を促し、ユーザー名オプションを指定した場合はユーザー名を確認します。

証明書をインポートします。

証明書ベースの認証のためにクライアント証明書をエンドポイントに事前デプロイする場合は、証明書をエンドポイントにコピーしてインポートし、GlobalProtect アプリで使用することができます。**globalprotect import-certificate --location *<location>*** コマンドを使用して、エンドポイントに証明書をインポートします。プロンプトが表示されたら、証明書パスワードを指定する必要があります。

```
user@linuxhost:~$ globalprotect import-certificate --location /
home/mydir/Downloads/cert_client_cert.p12 パスコードを入力してくださ
い:証明書のインポートに成功しました。
```

ゲートウェイに接続します:

1. (オプション) **globalprotect show --manual-gateway**コマンドを使用して接続できる手動ゲートウェイを表示します。
2. **globalprotect connect --gateway *<gp-gateway>***コマンドを使用してゲートウェイに接続します。ここで***<gp-gateway>***はGlobalProtectゲートウェイのIPアドレスまたはFQDNです。
3. **globalprotect show --details**コマンドを使用して接続の詳細を表示します。

```
user@linuxhost:~$ globalprotect show --manual-gateway 名前 アドレス
 ------------------------------ gw1 192.168.1.180 gw2 192.168.1.181
 user@linuxhost:~$ globalprotect connect --gateway 192.168.1.180 設
定を取得中...ネットワークを発見中...接続中...接続済み
```


GlobalProtect接続のステータスを確認し、詳細を表示します:

接続のステータスを確認するには、**globalprotect show --status**コマンドを使用します。

接続の詳細を表示するには、**globalprotect show --details**コマンドを使用します。

```
user@linuxhost:~$ globalprotect show --status グローバルプロテクトのステータス:接続済み user@linuxhost:~$ globalprotect show --details 割り当てられたIPアドレス:192.168.1.132 ゲートウェイのIPアドレス:192.168.1.180 プロトコル:IPSec稼働時間(秒):231
```

ネットワークを再発見します:

globalprotect rediscover-networkコマンドを使用して、グローバルプロテクトから切断し再接続します。

```
user@linuxhost:~$ globalprotect rediscover-network 切断中...設定を取得中...設定を取得中...ネットワークを発見中...接続中...接続中...GlobalProtectの状態:接続済み
```

現在のユーザーの資格情報をクリアします:

ポータルおよびゲートウェイで認証するために使用される資格情報をクリアするには、**globalprotect remove-user**コマンドを使用します。GlobalProtectアプリケーションが資格情報をクリアする必要があることを確認した後、GlobalProtectアプリケーションはトンネルを切断し、次回接続する際に資格情報の入力を要求します。

```
user@linuxhost:~$ globalprotect remove-user 資格情報がクリアされ、現在のトンネルが終了します。続行しますか(y/n)?y クリアが正常に完了しました。
 user@linuxhost:~$ globalprotect connect --portal 192.168.1.179 構成を取得中...切断済み 192.168.1.179 - ポータル:local:ログイン資格情報を入力してください ユーザー名:user1 パスワード:設定を取得中...ネットワークを発見中...接続中...接続済み
```

ホスト情報をゲートウェイに再送信します。

エンドポイントに関する現在のホスト情報を表示するには、**globalprotect show --host-state**コマンドを使用します。エンドポイントに関する情報をゲートウェイに再送信するには、**globalprotect resubmit-hip**コマンドを使用します。これは、HIPベースのセキュリティポリシーがユーザーのリソースへのアクセスを妨げる場合に役立ちます。なぜなら、ユーザーがエンドポイント上のコンプライアンスの問題を修正し、その後HIPを再送信できるからです。

```
user@linuxhost:~$ globalprotect show --host-state 生成時間:2017年9月28日 11:24:07 カテゴリ ホスト情報 クライアントバージョン:4.1.0
 OS:Linux Ubuntu 16.04.3 LTS OSベンダー:Linux ドメイン: ホスト名:
 linuxhost ホストID:4C4C4544-0034-4D10-804C-************ ネットワーク
```



```
インターフェース enp0s31f6 説明: enp0s31f6 MACアドレス:D4:81:D7:D4:5A:A5
 wlp2s0 説明: wlp2s0 MACアドレス:user@linuxhost:~$ globalprotect
 resubmit-hip 再送信が成功しました。
```

GlobalProtectの通知を表示します。

globalprotect show --notification コマンドを使用して通知を表示します。

GlobalProtectのシステムトレイアイコンを表示します。

globalprotect launch-ui コマンドを使用してデスクトップにシステムトレイアイコンを表示します。システム トレイのアイコンをクリックするとGlobalProtectアプリケーションを起動できます。

ウェルカムページを表示します。

globalprotect show --welcome-page コマンドを使用します。GlobalProtectアプリは、ウェルカムページが存在する場合はブラウザにウェルカムページを表示し、存在しない場合は通知を表示します。

エラーを表示します。

globalprotect show --error コマンドを使用してアプリによって報告されたエラーを表示します。

```
user@linuxhost:~$ globalprotect show --error エラー:GlobalProtectポータルに接続できません
```

ログを収集する

アプリは、/home/<*user*>/.Globalprotect ディレクトリにPanGPAおよびPanGPIログファイルを保存します。**globalprotect collect-logs** コマンドを使用して、Linux用のGlobalProtectアプリがこれらのログとその他の有用な情報をパッケージ化できるようにします。ログを使用して問題をトラブルシューティングしたり、専門的な分析のためにサポートエンジニアに転送したりできます。

```
user@linuxhost:~$ globalprotect collect-log ログ収集を開始し
ています... ネットワーク情報を収集中... マシン情報を収集中... ファイ
ルをコピー中... 最終結果ファイルを生成中...サポートファイルは /home/
user/.GlobalProtect/Collect.tgz に保存されました。
```

Linux用のGlobalProtectアプリのバージョンを表示します。

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


Linux用GlobalProtectアプリケーションからの問題の報告

どこで使用できますか?	何が必要ですか?
• Linuxエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

ネットワーク パフォーマンスが低下したり、ポータルやゲートウェイとの接続が確立されなかったりするなどの異常な動作が発生した場合は、管理者がアクセスできるStrata Logging Serviceに直接問題を報告できます。GlobalProtectアプリのログを手動で収集してメールで送信したり、クラウドドライブに保存したりする必要はなくなりました。

Linux用GlobalProtectアプリケーションの GUI バージョンを使用してのみ、管理者に問題を報告できます。

GlobalProtectアプリに問題を報告するオプションを表示するには、管理者がGlobalProtectポータルでトラブルシューティングのためのGlobalProtectアプリログ収集を有効にする必要があります。

STEP 1 | GlobalProtectポータルまたはゲートウェイに接続します。

1. GlobalProtect ウィンドウで、GlobalProtect ポータルの FQDN または IP アドレスを入力し、**[Connect (接続)]**をクリックします。

   GUIバージョンのGlobalProtect app for Linuxをダウンロードしてインストールすると、GlobalProtectアプリが自動的に起動します。
2. (任意)複数のポータルがアプリに保存されている場合は、[ポータル]ドロップダウンからポータルを選択します。デフォルトでは、最後に接続されたポータルが[ポータル]ドロップダウンから事前に選択されています。
3. ポータルの **Username (ユーザー名)**と **Password (パスワード)**を入力し、**Sign in (サインイン)**をクリックします。

   ほとんどの場合、企業ネットワークに接続するときに使用するのと同じユーザー名とパスワードを使用できます。サインインすると、GlobalProtectポータルのステータスが**Connected (接続済み)**と表示されます。
4. （オプション）デフォルトでは、管理者が定義する構成と利用可能なゲートウェイの応答時間に基づいて決定される、**Best Available**（利用可能な最適な接続）ゲートウェイに自動的に接続します。別のゲートウェイに接続するには、ゲートウェイのドロップダウンをクリックします。

STEP 2 | GlobalProtectアプリケーションを開きます。

GlobalProtectシステム トレイ アイコンをクリックして、アプリ インターフェースを起動します。

STEP 3 | エンドポイントからGlobalProtectアプリケーションから問題を報告します。

アプリケーションを起動したら、アプリケーションのパネルの右上にあるメニュー(　)を選択して、管理者に問題を報告します。

1. **Report an Issue (**問題の報告**)**を選択します。

2. GlobalProtectアプリが診断テストを実行し、診断ログを含めることを有効にします。診断ログとトラブルシューティングログの両方が収集され、コンパクトなトラブルシューティングレポートとしてStrata Logging Serviceに送信されます。

   診断テストが正常に完了した後、GlobalProtectデバッグログファイルがエンドポイントからStrata Logging Serviceにアップロードされます。

   アプリが診断テストを実行し、診断ログを含めることを有効にしない場合、トラブルシューティングログのみが収集され、コンパクトなトラブルシューティングレポートとして*Strata Logging Service*に送信されます。*GlobalProtect*アプリは、`.json`形式で自動的に生成されたレポートファイル*(pan_gp.trb.log*または*pan_gp_trbl.log)*をチェックします。トラブルシューティングログに問題が見つからなかった場合、通知メッセージが表示されます。再試行をクリックして、*pan_gp.trb*.log*ファイルが存在するか確認します。

3. **Run Diagnostic Tests and Include Diagnostic Logs(**診断テストを実行して診断ログを含める**)**チェックボックスを選択します。
4. 続行をクリックして、アプリがトラブルシューティング ログを作成し、管理者のStrata Logging Serviceインスタンスにレポートを送信できるようにします。

   エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。

   エンドツーエンドの診断テストの結果は、`.json`形式のpan_gp_diag.logファイルに保存され、pan_gp.trb*.logファイルと共に管理者のStrata Logging Serviceインスタンスに送信されます。GlobalProtectアプリは、トンネルありまたはトンネルなしで診断テスト

を実行できます。例えば、アプリが接続してトンネルを通じて診断テストを実行する前に、GlobalProtectのログイン資格情報を入力したいかもしれません。

アプリが診断テストを実行していることを確認するメッセージがポップアップしますが、これは**Run Diagnostic Tests and Include Diagnostic Logs (**診断テストを実行して診断ログを含める**)**チェックボックスを選択した場合のみです。

アプリがStrata Logging Serviceにレポートを送信していることを確認するメッセージがポップアップします。

5. 閉じる]をクリックして、アプリがレポートをStrata Logging Serviceに正常に送信したことを確認します。この確認メッセージには、レポートが処理および送信された日時が表示されます。

Linux用のグローバル保護アプリの接続を解除

どこで使用できますか?	何が必要ですか?
• Linuxエンドポイントのみ	☐ GlobalProtect アプリのバージョン 6.3 以降

管理者がGlobalProtectの接続方法を常時接続に設定している場合、GlobalProtectアプリを切断できます。たとえば、ホテルでGlobalProtect仮想プライベートネットワーク（VPN）が機能しておらず、VPN障害によってインターネットに接続できない場合、アプリを切断したい場合があります。GlobalProtectアプリを切断した後は、セキュアでない通信（VPNなし）を使用してインターネットに接続できます。

GlobalProtectアプリを切断できる方法、時間、回数は、管理者がGlobalProtectサービスをどのように構成するかによって異なります。この構成では、アプリを完全に切断できないようにしたり、チャレンジに正しく応答した後にのみアプリを切断したりすることができます。

構成にチャレンジが含まれている場合、GlobalProtectアプリは次のいずれかを求めるプロンプトを表示します。

- アプリを切断したい理由
- パスコード

チャレンジにパスコードが含まれる場合は、GlobalProtect管理者またはヘルプデスク担当者に電話で問い合わせることをお勧めします。通常、管理者は事前にパスコードを電子メール(GlobalProtectの新規ユーザー用)または組織のウェブサイトに掲載して提供します。また、システム停止やシステム障害が発生した場合には、管理者が電話でパスコードを提供することもあります。

GlobalProtectはLinux用のGlobalProtectアプリの2つのバージョンをサポートしています:Linuxデバイスが GUIをサポートしている場合の1つのバージョンと、GUIをサポートしていない場合のCLIバージョン。

- GUIバージョンを使用してLinux用のGlobalProtectアプリの接続を解除する
- CLIバージョンを使用してLinux用GlobalProtectアプリを接続解除する

GUIバージョンを使用してLinux用のGlobalProtectアプリの接続を解除する

(常時接続モードのみで利用可能) GUIバージョンを使用してLinux用のGlobalProtectアプリを切断するには、これらの手順を完了します。

STEP 1 | GlobalProtectアプリの接続を解除します。

1. システム トレイのアイコンをクリックして GlobalProtect アプリを起動します。ステータス パネルが開きます。
2. アプリのパネルの右上にあるメニュー(　)を選択して設定メニューを開きます。
3. **[Disconnect (接続解除)]**を選択します。

> ***[Disconnect (接続解除)]***オプションは、*GlobalProtect*エージェント構成でアプリケーションの切断が許可されている場合にのみ表示されます。構成で、チャレンジに応答することなく *GlobalProtect* アプリを切断できる場合、*GlobalProtect* アプリは追加のアクションを必要とせずに終了します。

STEP 2 | 必要に応じて、1つ以上の課題に対応します。

プロンプトが表示されたら、次の情報を入力します。

- **Reason (理由)**: GlobalProtectアプリを切断した理由。
- **Passcode (パスコード)**: 通常は、アプリを切断する必要がある既知の問題やイベントに基づいて、管理者が事前に提供するパスコードです。

CLIバージョンを使用してLinux用GlobalProtectアプリを接続解除する

CLIバージョンを使用してLinux用GlobalProtectアプリを接続解除するには、次の手順を完了してください。

(オンデマンドモードのみで利用可能) GlobalProtectから接続解除:

`globalprotect disconnect`コマンドを使用してGlobalProtectから切断します。

```
user@linuxhost:~$ globalprotect disconnect GlobalProtectのステータス:切断
```

(常時接続モードのみで利用可能) GlobalProtectを接続解除:

globalprotect disconnectコマンドを使用してGlobalProtectアプリを接続解除し、無効にします。構成が必要な場合、プロンプトが表示されたときに理由またはパスコードを指定する必要があります。

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

```
user@linuxhost:~$ globalprotect disconnect 接続解除する理由を入力してください：これが私の接続解除理由です
```

```
user@linuxhost:~$ globalprotect disconnect 接続解除するためのパスコードを入力してください:ITp@ssw0rd
```


Linux用のGlobalProtect Appをアンインストールする

どこで使用できますか?	何が必要ですか?
• Linuxエンドポイントのみ	❑ GlobalProtect アプリのバージョン 6.3 以降

次のコマンドを使用して、Linux用のGlobalProtectアプリをアンインストールできます。

```
$ ./gp_uninstall.sh --help 使い方: $ sudo ./gp_uninstall [--cli-only |
 --arm | --help] --cli-only:CLIのみ --arm:ARMオプションなし:UI
```

IoTデバイス向けGlobalProtect

どこで使用できますか?	何が必要ですか?
• iOTデバイスのみ	❑ GlobalProtect アプリのバージョン 6.1 以降が必要です。

GlobalProtect™は、エンドポイント(デスクトップコンピュータ、ノートパソコン、またはサーバー、またはIoTデバイス)上で実行されるアプリケーションです。企業ネットワーク内の機密リソースを保護するのと同じセキュリティポリシーを使用して、ユーザーを保護します。IoTデバイスの場合、GlobalProtect™は、インターネット上または企業ネットワーク内の任意の場所で、デバイスから任意の送信元または宛先へのトラフィックを保護します。

GlobalProtectは、以下のオペレーティングシステム内に組み込まれているIoTデバイスにインストールできます。

- AndroidのIoT
- RaspbianのIoT
- UbuntuのIoT
- WindowsのIoT