paloalto TECHDOCS

GlobalProtect 管理者ガイド

9.1

docs.paloaltonetworks.com

お問い合わせ先

本社：

Palo Alto Networks

3000 タネリーウェイ

サンタクララ, CA 95054

www.paloaltonetworks.com/company/contact-support.html

ドキュメントについて

- このガイドの最新バージョン、または関連ドキュメントにアクセスするには、テクニカル ドキュメント ポータル docs.paloaltonetworks.com を参照してください。
- 特定のトピックを検索するには、検索ページ docs.paloaltonetworks.com/search.html に移動します。
- フィードバックやご質問はありますか?ポータルの任意のページにコメントを残すか、documentation@paloaltonetworks.com で私たちに書いてください。

Last Revised

June 4, 2020

Table of Contents

GlobalProtect の概要

自宅での電子メール チェック、または空港での会社のドキュメント更新など、今日の従業員の多くは社外で作業を行っています。こうした労働者のモビリティの向上により、生産性や柔軟性は高まりますが、同時に重大なセキュリティ リスクを招きます。ユーザーがノートパソコンやスマートフォンを社外に持ち出すたびに、企業ファイアウォール、およびユーザーとネットワークの両方を保護するように設計されている関連ポリシーがバイパスされます。GlobalProtect™ では、どこにいるかに関わらずすべてのユーザーに対して、物理的ペリメータ内で適用されるポリシーと同じ次世代ファイアウォール ベースのポリシーを拡張することで、ローミング ユーザーのセキュリティ上の課題を解決します。

以下のセクションでは、Palo Alto Networks GlobalProtect 製品の概念的な情報を提供し、GlobalProtect のコンポーネントとさまざまなデプロイ シナリオについて説明します。

- GlobalProtect コンポーネントについて
- GlobalProtect でサポートされている OS バージョン
- GlobalProtect がサポートしている機能について
- GlobalProtect ライセンスの概要

GlobalProtect コンポーネントについて

GlobalProtect はモバイル ユーザーを管理する完全なインフラストラクチャを提供し、使用しているエンドポイントや場所に関わらず、すべてのユーザーが安全にアクセスできるようにします。このインフラストラクチャには、以下のコンポーネントが含まれています。

- GlobalProtect Portal（GlobalProtect ポータル）
- GlobalProtect ゲートウェイ
- GlobalProtect アプリケーション

GlobalProtect Portal（GlobalProtect ポータル）

GlobalProtect ポータルは、GlobalProtect インフラストラクチャの管理機能を提供します。GlobalProtect ネットワークに参加するすべてのエンドポイントは、ポータルから設定情報を受信します。これには、使用可能なゲートウェイ、GlobalProtect ゲートウェイへの接続に必要になる可能性のあるクライアント証明書などの情報が含まれます。さらに、ポータルはMacOS と Windows の両方のエンドポイントに対する GlobalProtect アプリケーション ソフトウェアの動作と配布を制御します（GlobalProtect アプリケーションは、iOS エンドポイント用 Apple App Store、Android エンドポイントおよびChromebooks用 Google Play、 Windows 10 UWP エンドポイント用Microsoft Storeからモバイルエンドポイントに配布されます）。ホスト情報プロファイル（HIP）機能を使用している場合、必要なすべてのカスタム情報など、ホストから収集する情報もポータルで定義します。Palo Alto Networks 次世代ファイアウォールのインターフェイスでGlobalProtect ポータルへのアクセスのセットアップが可能です。

GlobalProtect ゲートウェイ

GlobalProtect ゲートウェイは、GlobalProtect アプリケーションからのトラフィックに対するセキュリティ処理を提供します。さらに、HIP 機能が有効になっている場合、ゲートウェイはアプリが送信した生ホスト データから HIP レポートを生成し、この情報をポリシーの適用に使用できます。さまざまなゲートウェイのタイプを設定し、リモート ユーザー向けにセキュリティ処理や仮想プライベート ネットワーク（VPN）へのアクセスを提供したり、アクセスに関するセキュリティ ポリシーを内部リソースに適用したりできます。

GlobalProtect ゲートウェイの設定は、Palo Alto Networks 次世代ファイアウォールのインターフェイスで行うことができます。同じファイアウォールでゲートウェイとポータルの両方を実行できます。または、企業全体で複数の分散ゲートウェイを設定することも可能です。

GlobalProtect アプリケーション

GlobalProtect アプリ ソフトウェアは、エンドポイント上で実行され、デプロイした GlobalProtect ポータルとゲートウェイを介してネットワーク リソースにアクセスできるようにします。

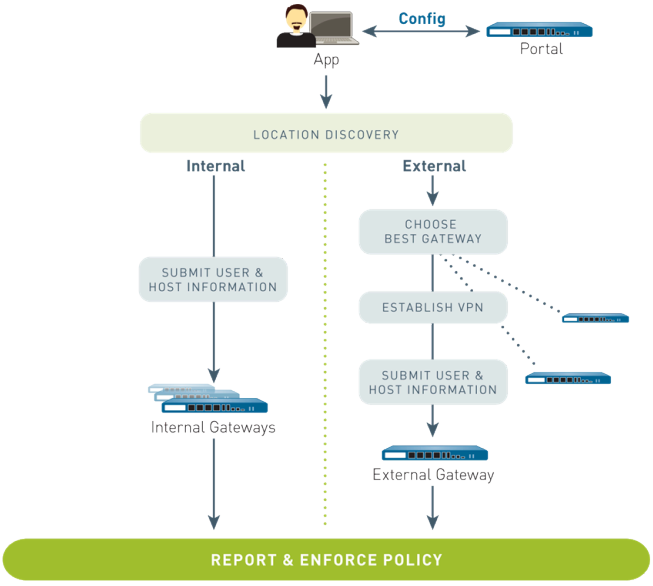
GlobalProtect for Windows および macOS エンドポイントは、GlobalProtect ポータルからデプロイされます。ポータルで定義するクライアント設定を使用し、ユーザーに表示するタブなど、アプリの動作を設定します。詳細については、GlobalProtect エージェント設定の定

義、GlobalProtect アプリのカスタマイズ、およびGlobalProtect アプリ ソフトウェアのデプロイを参照してください。

モバイル エンドポイント用の GlobalProtect アプリケーション（iOS、Android、Windows UWP）は、公式ストアで入手可能です。(iOS 用 Apple App Store、Android 用 Google Play、Windows UWP用 Microsoft Store)。あるいは、 サードパーティのモバイル エンドポイント管理システムである、AirWatch を使用した GlobalProtect モバイル アプリケーションのデプロイが可能です。

詳細については、GlobalProtect でサポートされている OS バージョンを参照してください。

以下の図は、GlobalProtect ポータル、ゲートウェイ、およびアプリケーションが連携し、使用するエンドポイントや場所に関わらず、すべてのユーザーに安全なアクセスを提供する方法を示しています。



GlobalProtect でサポートされている OS バージョン

GlobalProtect アプリは一般的なデスクトップ、ノートパソコン、タブレット、スマートフォンをサポートします。PAN-OS 6.1 以降のリリース上で動作するファイアウォールにて GlobalProtect を設定すること、さらにエンドユーザーがサポートされているリリースの GlobalProtect アプリケーションのみをエンドポイントにインストールすることが推奨されます。GlobalProtect アプリの最低リリース要件はオペレーティング システムによって異なります。特定のオペレーティング システムにおける GlobalProtect アプリの最低リリース要件を確認するには、Palo Alto Networks® CompatibilityMatrixにある以下のトピックを参照してください。

- GlobalProtect アプリケーションをインストールできる場所
- サポートされている X-Auth IPSec クライアント

古いバージョンの GlobalProtect アプリケーションについては、それがリリースされた時点の PAN-OS やオペレーティングシステムでは、まだサポートされています。GlobalProtect のリリースに対する PAN-OS のサポートの最低リリース要件については、ソフトウェア更新サイトを参照してください。

GlobalProtect ライセンスの概要

GlobalProtect を安全なリモート アクセスまたは 1 つまたは複数の内部/外部ゲートウェイを介した仮想プライベート ネットワーク（VPN）ソリューションの提供に使用する場合、GlobalProtect ライセンスは必要ありません。ただし、さらに上級のいくつかの機能（HIP チェックや関連コンテンツの更新、GlobalProtect モバイル アプリのサポート、または IPv6 のサポートなど）を使用するには、GlobalProtect の年間サブスクリプションの購入が必要です。このライセンスは、以下のゲートウェイを実行している各ファイアウォールにインストールする必要があります。

- HIP チェックを実行する
- モバイル エンドポイント用の GlobalProtect アプリをサポート
- Linux エンドポイント用の GlobalProtect アプリをサポート
- IPv6 接続を提供する
- 宛先ドメイン、アプリケーション プロセス名、または HTTP / HTTPS ビデオ ストリーミング アプリケーションに基づいて、トンネル トラフィックを分割します。

GlobalProtect クライアントレス VPN の場合、GlobalProtect ポータルからクライアントレス VPN をホストしているファイアウォールに GlobalProtect サブスクリプションをインストールする必要もあります。この機能を使用するには、**GlobalProtect** クライアントレス **VPN** の動的更新も必要です。

機能	必要なサブスクリプション
単一、外部ゲートウェイ（Windows および macOS）	—
単一または複数の内部ゲートウェイ	—
複数の外部ゲートウェイ	—
Internet of things (IoT)デバイス	—
HIP チェック	✓
エンドポイントマシンの証明書、エンドポイントのシリアルナンバー、ソフトウェアとアプリケーションの設定に基づくエージェント設定 (GlobalProtectサブスクリプションは、HIPチェックの使用時にのみ必要となります)	✓
エンドポイントのステータスを基にしたHIP-ベースのポリシー施行	✓
Windows および macOS を実行するエンドポイント向けアプリ	—

機能	必要なサブスクリプション
iOS、Android、Chrome OS、およびWindows 10 UWP を実行するエンドポイント向けモバイルアプリ	✓
Linux を実行するエンドポイント向けアプリ	✓
外部ゲートウェイ向けの IPv6	✓
内部ゲートウェイ向けの IPv6 （デフォルトの動作の変更—GlobalProtect アプリケーション 4.1.3 から、このユースケースでは GlobalProtect サブスクリプションが不要になります）	—
クライアントレス VPN	✓
宛先ドメイン、クライアント プロセス、およびビデオ ストリーミング アプリケーションに基づくスプリット トンネリング	✓

ファイアウォールでのラインセンスのインストールの詳細は、ライセンスのアクティベーションを参照してください。

始めましょう

GlobalProtect™ を実行するために、すべてのコンポーネントの通信を可能にするインフラストラクチャをセットアップする必要があります。基本レベルでは、これは GlobalProtect エンド ユーザーがポータルおよびゲートウェイを介してネットワークにアクセスするために接続する、インターフェイスおよびゾーンをセットアップする作業になります。GlobalProtect コンポーネントが安全なチャネルを経由して通信するため、必要な SSL 証明書を取得してさまざまなコンポーネントにデプロイする必要があります。以下のセクションでは、GlobalProtect インフラストラクチャのセットアップについて説明します。

> GlobalProtect のインターフェイスおよびゾーンの作成
> GlobalProtect コンポーネント間の SSL の有効化

GlobalProtect のインターフェイスおよびゾーンの作成

GlobalProtect インフラストラクチャに以下のインターフェイスおよびゾーンを設定する必要があります。

- **GlobalProtect** ポータル – GlobalProtect アプリの接続用にレイヤー 3 またはループバック インターフェイスが必要です。ポータルおよびゲートウェイが同じファイアウォールにある場合、同一のインターフェイスを使用することができます。ポータルは、ネットワークの外部からアクセス可能なゾーンにある必要があります（DMZなど）。
- **GlobalProtect** ゲートウェイ – ゲートウェイのインターフェイスおよびゾーンの要件は、以下のように、外部ゲートウェイまたは内部ゲートウェイのどちらを設定しているかによって異なります。
  - 外部ゲートウェイ – アプリが接続を確立する、レイヤー 3 またはループバック インターフェイスと、論理トンネル インターフェイスが必要になります。レイヤー 3 またはループバック インターフェイスは、DMZ などの外部ゾーンにある必要があります。トンネル インターフェイスは、内部リソース（**trust** など）に接続するインターフェイスと同じゾーン内に配置できます。セキュリティや可視性を高めるために、**corp-vpn** など、個別のゾーンを作成することができます。トンネル インターフェイスに別のゾーンを作成する場合は、トラフィックが VPN ゾーンと信頼されたゾーンの間を通過できるようにするセキュリティ ポリシーを作成する必要があります。
  - 内部ゲートウェイ – 信頼されたゾーンにレイヤー 3 またはループバック インターフェイスが必要になります。内部ゲートウェイにアクセスするためのトンネル インターフェイスを作成することもできますが、必須ではありません。

さまざまなポートとアドレスの *GlobalProtect* へのアクセスを可能にするループバック インターフェイスの使用方法に関するヒントとして、GlobalProtect ポータル ページをどのポートからもアクセスできるように設定できるかどうかを参照してください。

ポータルおよびゲートウェイについての詳細は、GlobalProtect コンポーネントについてを参照してください。

STEP 1 | デプロイする予定の各ポータルやゲートウェイのレイヤー 3 インターフェイスを設定します。

ゲートウェイおよびポータルが同じファイアウォールにある場合、両方に対して *1* つのインターフェイスを使用できます。

ベスト プラクティスとして、ポータルおよびゲートウェイには静的 *IP* アドレスを使用します。

GlobalProtect ポータルまたはゲートウェイを設定したインターフェイスで *HTTP*、*HTTPS*、*Telnet*、または *SSH* を許可するインターフェイス管理プロファイルを追加すると、インターネットからの管理インターフェイスへのアクセスを許可することになるため、追加しないでください。管理アクセスの保護のベストプラクティスに従い、攻撃を阻止するようにファイアウォールへの管理アクセスを保護してください。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）または **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Loopback**（ループバック）の順に選択し、GlobalProtect を設定する必要があるインターフェイスを選択します。この例では、**`ethernet1/1`** をポータル インターフェイスとして設定します。
2. （イーサネットのみ） **Interface Type**（インターフェイス タイプ）を **Layer3**（レイヤー **3**）に設定します。
3. 以下のように、**Config**（設定）タブで、ポータルまたはゲートウェイ インターフェイスが属する **Security Zone**（セキュリティ ゾーン）を選択します。
   - **`l3-untrust`** など、ネットワークの外部のホストからアクセスできるように、信頼されていないゾーンにポータルおよび外部ゲートウェイを配置します。
   - **`l3-trust`** などの内部ゾーンに内部ゲートウェイを配置します。
   - ゾーンをまだ作成していない場合は、 **New Zone**（新規ゾーン）を追加します。Zone （ゾーン）ダイアログの **Name**（名前）で名前をつけて新しいゾーンを定義し、**OK** をクリックします。
4. デフォルトの**Virtual Router**（仮想ルーター）を選択します。
5. IP アドレスをインターフェイスに割り当てます。
   - IPv4 アドレスの場合、**IPv4** を選択して、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例: 203.0.11.100/24）。
   - IPv6 アドレスの場合、**IPv6** を選択して、**Enable IPv6 on the interface**（インターフェースでの **IPv6** の有効化）を行い、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例：2001:1890:12f2:11::10.1.8.160/80）。
6. **OK** をクリックして、インターフェイス設定を保存します。

STEP 2 | GlobalProtect ゲートウェイをホストするファイアウォールで、GlobalProtect アプリによって確立される VPN トンネルを終端する論理トンネル インターフェイスを設定します。

動的ルーティングの必要がない場合、*IP* アドレスはトンネル インターフェイスで必須ではありません。なお、トンネル インターフェイスに *IP* アドレスを割り当てると、接続の問題のトラブルシューティングに利用できます。

VPN トンネルの終端となるゾーンで必ずユーザー *ID* を有効にしてください。

1. **Network**（ネットワーク） > **Interfaces (**インターフェイス**)** > **Tunnel**（トンネル） を選択してトンネル インターフェイスを**Add**（追加） します。
2. **Interface Name (**インターフェイス名**)** フィールドで、**.2** などの数値のサフィックスを入力します。
3. **Config (**設定**)** タブで、VPN トンネルの終端の **Security Zone (**セキュリティ ゾーン**)** を選択して以下のようにゾーンを定義します。
   - トンネルの終端点として Trust ゾーンを使用するには、ドロップダウン リストからゾーンを選択します。
   - （推奨）VPN トンネルの終端のゾーンを別に作成するには、**New Zone**（新規ゾーン）を追加します。ゾーン ダイアログで、新しいゾーンの **Name**（名前）を定義して（**corp-vpn** など）、**Enable User Identification**（ユーザー **ID** を有効にする）を実行し、**OK** をクリックします。
4. **Virtual Router**（仮想ルーター）を **None**（なし）に設定します。
5. IP アドレスをインターフェイスに割り当てます。
   - IPv4 アドレスの場合、**IPv4** を選択して、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例: 203.0.11.100/24）。
   - IPv6 アドレスの場合、**IPv6** を選択して、**Enable IPv6 on the interface**（インターフェースでの **IPv6** の有効化）を行い、インターフェイスに割り当てる IP アドレスとネットワーク マスクを **Add**（追加）します（例：2001:1890:12f2:11::10.1.8.160/80）。
6. **OK** をクリックして、インターフェイス設定を保存します。

STEP 3 | VPN 接続のトンネルの終端のために別のゾーンを作成した場合、VPN ゾーンと Trust ゾーンの間をトラフィックが通過できるセキュリティ ポリシーを作成します。

たとえば、以下のポリシー ルールは、**corp-vpn** ゾーンと **l3-trust** ゾーンの間のトラフィックを有効にします。

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

STEP 4 | 設定を **Commit**（コミット）します。

GlobalProtect コンポーネント間の SSL の有効化

GlobalProtect コンポーネント間のすべての相互作用は SSL/TLS 接続を介して行われます。そのため、設定で適切な証明書を参照できるように、各コンポーネントを設定する前に、必要な証明書の生成やインストールを行う必要があります。以下のセクションでは、サポートされる証明書のデプロイ方法、説明、さまざまな GlobalProtect 証明書のベスト プラクティス ガイドラインについて説明し、必要な証明書を生成してデプロイする手順を紹介します。

- GlobalProtect 証明書のデプロイメントについて
- GlobalProtect 証明書のベスト プラクティス
- GlobalProtect コンポーネントへのサーバー証明書のデプロイ

GlobalProtect 証明書のデプロイメントについて

GlobalProtect コンポーネントへのサーバー証明書のデプロイを行う方法は基本的に3つあります。

- （推奨）サードパーティ証明書および自己署名証明書の組み合わせ – GlobalProtect アプリは、GlobalProtect 設定の前にポータルにアクセスするため、HTTPS 接続を確立するために、証明書を信頼する必要があります。
- エンタープライズ認証局 – 独自のエンタープライズ認証局がすでにある場合は、この内部 CA を使用して、各 GlobalProtect コンポーネントの証明書を発行し、ポータルおよびゲートウェイをホストしているファイアウォールにインポートできます。この場合はまた、エンドポイントやモバイル デバイスが、接続対象の GlobalProtect サービスの証明書の発行に使用されるルート CA 証明書を信頼していることを確認する必要もあります。
- 自己署名証明書 – ポータルで自己署名 CA 証明書を生成し、これを使用してすべての GlobalProtect コンポーネントの証明書を発行できます。ただし、このソリューションはその他のオプションほど安全でないため、お勧めできません。万が一このオプションを選択した場合、エンド ユーザーが初めてポータルに接続すると証明書エラーが表示されます。これを防ぐには、手動で、または Active Directory の グループ ポリシー オブジェクト（GPO）などの中央管理されたデプロイメントを使用して、自己署名ルート CA 証明書をすべてのエンドポイントにデプロイします。

GlobalProtect 証明書のベスト プラクティス

以下の表に、使用する機能に応じて必要となる SSL/TLS の概要を示します。

Certificate（証明書）	使用率	発行プロセス/ベスト プラクティス
CA 証明書	GlobalProtect コンポーネントに対して発行された証明書の署名に使用します。	自己署名証明書を使用する予定の場合は、専用の CA サーバーまたは Palo Alto Networks ファイアウォールを使用して CA 証明書を生成し、CA または中間 CA によって署名された

Certificate（証明書）	使用率	発行プロセス/ベスト プラクティス
		GlobalProtectポータルおよびゲートウェイ証明書を発行します。
ポータル サーバー証明書	GlobalProtect アプリでポータルとの HTTPS 接続を確立できるようにします。	• この証明書は SSL/TLS サービス プロファイルで特定されます。ポータルのサーバー証明書は、それに関連するサービスプロファイルをポータル設定で選択することで割り当てます。 • 一般的なサードパーティ CA からの証明書を使用します。これは最も安全な方法で、ルート CA 証明書をデプロイすることなく、ユーザーのエンドポイントが確実にポータルとの信頼関係を確立できます。 • 一般的なパブリック CA を使用しない場合、ポータルのサーバー証明書を生成するために使用されたルート CA 証明書を、GlobalProtect アプリを実行するすべてのエンドポイントにエクスポートする必要があります。この証明書をエクスポートすることにより、エンドユーザーがポータルに初めてログインする際、証明書の警告が表示されるのを回避できます。 • 証明書のCommon Name (共通名 - CN)フィールドとSubject Alternative Name (サブジェクトの別名 - SAN)フィールドが、ポータルをホストするインターフェースの IPアドレスまたは FQDN と一致する必要があります。 • 通常、ポータルには独自のサーバー証明書が必要です。しかし、同じインターフェイスの単一ゲートウェイとポータルをデプロイしている場合、ゲートウェイとポータルの両方で同じ証明書を使用する必要があります。 • ゲートウェイとポータルを同じインターフェイス上で設定する場合、ゲートウェイとポータルに同じ証明書プロファイルおよび SSL/TLS サービス プロファイルを使用することも推奨します。証明書プロファイルおよび SSL/TLS サービス プロファイルが異なる場合、SSL ハンドシェーク中はゲートウェイの設定がポータルの設定より優先されます。

Certificate（証明書）	使用率	発行プロセス/ベスト プラクティス
ゲートウェイ サーバー証明書	GlobalProtect アプリでゲートウェイとの HTTPS 接続を確立できるようにします。	• この証明書は SSL/TLS サービス プロファイルで特定されます。ゲートウェイのサーバー証明書は、それに関連するサービスプロファイルをゲートウェイ設定で選択することで割り当てます。 • ファイアウォールまたは CA サーバーで CA 証明書を生成し、その CA 証明書を使用してすべてのゲートウェイ証明書を生成します。 • 証明書の CN フィールドと SAN フィールドが、ゲートウェイを設定するインターフェースの FQDN または IPアドレスと一致する必要があります。 • ポータルは、設定（Portal configuration Agent（ポータル設定エージェント）タブ内の信頼されたルートCA リスト）に基づいて、ゲートウェイルート CA 証明書を GlobalProtect アプリケーションに配布できます。ただし、ゲートウェイルートCA 証明書がユーザーの信頼できる証明書ストアに事前にインストールされていること、またはゲートウェイ証明書がパブリック CA によって発行されていることは必須ではありません。 • 通常、各ゲートウェイに独自のサーバー証明書が必要です。しかし、基本的な VPN アクセス用に同じインターフェース上に単一ゲートウェイとポータルをデプロイしている場合、両方のコンポーネントに対して 1 つのサーバー証明書を使用する必要があります。ベスト プラクティスとして、パブリック CA の署名よって発行された証明書を使用します。 • ゲートウェイとポータルを同じインターフェイス上で設定する場合、ゲートウェイとポータルに同じ証明書プロファイルおよび SSL/TLS サービス プロファイルを使用することも推奨します。証明書プロファイルおよび SSL/TLS サービス プロファイルが異なる場合、SSL ハンドシェーク中はゲートウェイの設定がポータルの設定より優先されます。

Certificate（証明書）	使用率	発行プロセス/ベスト プラクティス

（任意）クライアント証明書	GlobalProtect アプリとゲートウェイ/ポータル間で HTTPS セッションを確立する際に相互認証を可能にするために使用します。これにより、有効なクライアント証明書を持っているエンドポイントだけが、認証を行ってネットワークに接続できるようになります。	• クライアント証明書のデプロイメントを簡略化するため、次のいずれかの方法でログインに成功したときにアプリがクライアント証明書をデプロイするようにポータルを設定します。
		  • 同じ設定を受信するすべての GlobalProtect アプリに対して、単一のクライアント証明書を使用します。**Local**（ローカル）クライアント証明書は、証明書をポータルにアップロードし、ポータルのエージェント設定でそれを選択することで割り当てます。
		  • Simple Certificate Enrollment Protocol（**SCEP**）を使用し、GlobalProtect ポータルが一意のクライアント証明書を GlobalProtect アプリにデプロイできるようにします。これは、SCEP プロファイルを設定し、そのプロファイルをポータルのエージェント設定で選択することで有効化します。
		• GlobalProtect エンドポイント用のクライアント証明書を生成する際は、ダイジェスト アルゴリズム（sha1, sha256, sha384, or sha512）のいずれかを使用します。
		• エンド ユーザーを認証する時に各エンドポイントに一意のクライアント証明書をデプロイするには、他のメカニズムを使用します。
		• 最初にクライアント証明書なしで設定をテストし、その他すべての設定が正しいことを確認してからクライアント証明書を追加することを検討してください。

（任意）マシン証明書	マシン証明書は、ローカル マシン ストアまたはシステム キーチェーンにあるエンドポイントに発行されるクライアント証明書です。各マシン証明書は、ユーザーではなくサブジェクト フィールドを使用してエンドポイン	• GlobalProtect エンドポイント用のクライアント証明書を生成する際は、ダイジェスト アルゴリズム（sha1, sha256, sha384, or sha512）のいずれかを使用します。 • プレ ログオン機能を使用する場合、GlobalProtect へのアクセスを許可する前に、独自の PKI インフラストラクチャを使用して各エンドポイントにマシン証明書をデプ

Certificate（証明書）	使用率	発行プロセス/ベスト プラクティス
	トを識別します（例えば、CN=laptop1.example.com）この証明書により、信頼できるエンドポイントのみがゲートウェイあるいはポータルに接続できるようになります。 プレ ログオン接続方法を使用して構成されたユーザーには、マシン証明書が必要です	ロイしてください。これは、セキュリティを確保する上で重要なアプローチです。 詳細については、プレ ログオンを使用したリモート アクセス VPNを参照してください。

表：GlobalProtect 証明書の要件

GlobalProtect エンドポイント、ポータル、ゲートウェイ間の安全な通信を行うために使用するキーのタイプの詳細は、リファレンス:GlobalProtect アプリの暗号化機能

GlobalProtect コンポーネントへのサーバー証明書のデプロイ

GlobalProtect コンポーネントに SSL/TLS 証明書をデプロイする手順のベスト プラクティスは、以下の表の通りです。

一般的なサードパーティ CA からサーバー証明書をインポートします。

GlobalProtect ポータルに対して、一般的なサードパーティ *CA* によって発行されたサーバー証明書を使用します。これにより、信頼できない証明書に関する警告が表示されることなく、エンドユーザーが *HTTPS* 接続を確立できるようになります。

CN フィールドと、該当する場合は、*SAN* フィールドが、サードパーティのモバイル エンドポイント管理システムのポータルまたはデバイス チェックイン インターフェイスを設定する予定であるインターフェイスの *FQDN* または *IP* アドレスと完全に一致する必要があります。ワイルドカード一致がサポートされています。

証明書をインストールする前に、証明書とキー ファイルが管理システムからアクセス可能で、秘密鍵を復号化するパスフレーズを持っていることを確認します。

1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから、新しい証明書を **Import**（インポート）します。
2. **Local**（ローカル）の証明書タイプ（デフォルト）を使用します。
3. **Certificate Name**（証明書名）を入力します。
4. **Certificate File**（証明書ファイル） に CA から受信したファイルのパスと名前を入力するか、**Browse**（参照） でファイルを見つけます。
5. **File Format**（ファイル フォーマット）を **Encrypted Private Key and Certificate (PKCS12)**（暗号化された秘密鍵と証明書（**PKCS12**））に設定します。
6. **Key File**（キー ファイル）に PKCS#12 ファイルのパスと名前を入力するか、**Browse**（参照）でファイルを見つけます。
7. 秘密鍵の暗号化に使用した **Passphrase**（パスフレーズ） に入力して、再入力します。
8. **OK** をクリックして、証明書およびキーをインポートします。

GlobalProtect コンポーネントの自己署名証明書を発行するためのルート CA 証明書を作成します。

ポータルでルート *CA* 証明書を作成し、その証明書を使用して、ゲートウェイおよび必要に応じてクライアントに対してサーバー証明書を発行します。

自己署名証明書をデプロイする前に、GlobalProtect コンポーネントの証明書に署名するルート CA 証明書を作成する必要があります。

1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから、新しい証明書を **Generate**（生成）します。
2. **Local**（ローカル）の証明書タイプ（デフォルト）を使用します。
3. **Certificate Name**（証明書名）に「GlobalProtect_CA」などの名前を入力します。証明書名にスペースを含めることはできません。
4. **Signed By**（署名者）フィールドでは値を選択しないでください。**Signed By**（署名者）を未選択にすることで、自己署名の証明書になります。
5. **Certificate Authority**（証明書認証局） オプションを有効にします。
6. **OK** をクリックして証明書を生成します。

ポータルでルート CA を使用して自己署名サーバー証明書を生成します。

デプロイする各ゲートウェイ用のサーバー証明書を生成し、必要に応じてサードパーティのモバイル エンドポイント管理システムの管理インターフェイス（ゲートウェイがこのインターフェイスから *HIP* レポートを取得する場合）用のサーバー証明書を生成します。

ゲートウェイ サーバー証明書では、*CN* および *SAN* フィールドの値が同じでなければなりません。値が異なる場合、*GlobalProtect* エージェントは不一致を検出し、証明書を信頼しなくなります。証明書の***Host Name***（ホスト名）属性を追加した場合のみ、自己署名証明書には *SAN* フィールドが含まれます。

別の方法として、Simple Certificate Enrollment Protocol（SCEP）を使用してエンタープライズ CA のサーバー証明書をリクエストすることもできます。

1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから、新しい証明書を **Generate**（生成）します。
2. **Local**（ローカル）の証明書タイプ（デフォルト）を使用します。
3. **Certificate Name**（証明書名）を入力します。この名前にはスペースを含められません。
4. **Common Name**（共通名）フィールドに、ゲートウェイを設定するインターフェイスの FQDN（推奨）または IP アドレスを入力します。
5. **Signed By**（署名者）フィールドで、作成した GlobalProtect_CA を選択します。
6. Certificate Attributes（証明書の属性）領域で、**Add**（追加）を実行してゲートウェイを一意に識別する属性を定義します。**Host Name**（ホスト名）属性（証明書の SAN フィールドに入力される）を追加する場合、この値は **Common Name**（共通名）に定義した値と同じにする必要があります。
7. 暗号化**Algorithm**（アルゴリズム）、キーの長さ（**Number of Bits**（ビット数））、**Digest**（ダイジェスト）アルゴリズム、**Expiration**（有効期間）（日数）など、サーバー証明書の暗号設定を行います。
8. **OK** をクリックして証明書を生成します。

Simple Certificate Enrollment Protocol（SCEP）を使用してエンタープライズ CA のサーバー証明書をリクエストします。

デプロイする予定の各ポータルおよびゲートウェイに対し、別々の *SCEP* プロファイルを設定します。次に、各 *GlobalProtect* コンポーネントに対し、特定の *SCEP* プロファイルを使用してサーバー証明書を生成します。

ポータルおよびゲートウェイのサーバー証明書では、ポータルまたはゲートウェイを設定する予定のインターフェイスの *FQDN*（推奨）または *IP* アドレスが *CN* フィールドの値に含まれており、かつこれが *SAN* フィールドと同一でなければなりません。

連邦情報処理標準（*FIPS*）に準拠するため米国の連邦情報処理標準（*FIPS*）に準拠するために、*SCEP* サーバーと *GlobalProtect* ポータルの間の相互 *SSL* 認証を有効にする必要もあります。（*FIPS-CC* の実施についてはファイアウォールのログインページおよびそのステータスバーに表示されます）

設定のコミット後、ポータルは SCEP プロファイル内の設定を使って CA 証明書をリクエストしようと試みます。これが成功したら、ポータルをホストしているファイアウォールが CA 証明書を保存し、それを**Device Certificates**（デバイス証明書）のリストにデプロイします。

1. 各 GlobalProtect ポータルまたはゲートウェイ用の SCEP プロファイルを設定します。
   1. サーバー証明書をデプロイするコンポーネント、および SCEP プロファイルを識別する **Name**（名前）を入力します。このプロファイルが複数の仮想システム容量のあるファイアウォール用であれば、仮想システムを選択するか、そのプロファイルを利用できる **Location**（場所）として **Shared**（共有）を選択します。
   2. （任意）各証明書のリクエスト用に、PKI およびポータル間の **SCEP Challenge**（**SCEP** チャレンジ）レスポンス機構を設定します。SCEP サーバーから得られる **Fixed**（固定）チャレンジ パスワード、またはポータル-クライアントがユーザー名および指定した OTP を SCEP サーバーに送信する **Dynamic**（動的）パスワードを使用します。動的 SCEP チャレンジの場合、PKI 管理者の認証情報をこれに使用できます。
   3. PKI 内の SCEP サーバーにアクセスするためにポータルが使用する**Server URL**（サーバー **URL**）を設定します（例：**`http://10.200.101.1/certsrv/mscep/`**）。
   4. SCEP サーバーを識別するための文字列（255 文字まで）を **CA-IDENT Name**（**CA-IDENT** 名）に入力します。
   5. SCEP サーバーが生成する証明書に使用する **Subject**（サブジェクト）名を入力します。サブジェクトには、**`CN=<value>`**という形（**`<value>`**はポータルあるいはゲートウェイのFQDNまたはIPアドレス）で共通名（CN）キーが含まれていなければなりません。
   6. **Subject Alternative Name Type**（サブジェクトの別名タイプ）を選択します。証明書のサブジェクトまたは Subject Alternative Name（サブジェクト代替名）拡張子にメールの名前を入力するには、**RFC 822 Name**（**RFC 822** 名）を選択します。また、証明書の評価に使用する **DNS Name**（**DNS** 名）を入力するか、クライアントが証明書を取得する元となるリソースを特定する **Uniform Resource Identifier**（**URI**）を入力することもできます。

7. キーの長さ（**Number of Bits**（ビット数））、および証明書署名要求に使用する **Digest**（ダイジェスト）アルゴリズムなど、他の暗号設定を行います。
8. 許可される証明書の利用方法を、署名（**Use as digital signature**（デジタル署名として使用））または暗号化（**Use for key encipherment**（キーの暗号化に使用））のいずれかに設定します。
9. ポータルが正しい SCEP サーバーに確実に接続されるようにするために、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）を入力します。SCEP サーバーインターフェイスの Thumbprint（指紋）のフィールドからフィンガープリントを入手してください。
10. SCEP サーバーと GlobalProtect ポータルの間の相互 SSL 認証を有効にします。
11. **OK** をクリックし、設定を **Commit**（コミット）します。

2. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから **Generate**（生成）をクリックします。
3. **Certificate Name**（証明書名）を入力します。この名前にはスペースを含められません。
4. エンタープライズ CA が署名するサーバー証明書をポータルまたはゲートウェイに発行するプロセスを自動化するために使用する **SCEP Profile**（**SCEP** プロファイル）を選択し、**OK** をクリックして証明書を生成します。GlobalProtect ポータルは SCEP プロファイル内の設定を使用し、エンタープライズ PKI に CSR を送信します。

インポートまたは生成したサーバー証明書を SSL/TLS サービス プロファイルへ割り当てます。

1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）の順に選択し、SSL/TLS サービス プロファイルを **Add**（追加）します。
2. **Name**（名前）を入力してプロファイルを判別し、インポートまたは生成したサーバー **Certificate**（証明書）を選択します。
3. GlobalProtect コンポーネントとの通信に使用する SSL/TLS バージョン（**Min Version**（最低バージョン）から **Max Version**（最高バージョン））の範囲を定義します。

   最も強力なセキュリティを提供するには、***Min Version***（最低バージョン）を ***TLSv1.2*** に設定します。
4. **OK** をクリックして SSL/TLS サービス プロファイルを保存します。
5. 変更を **Commit**（コミット）します。

自己署名サーバー証明書をデプロイします。

- ポータルでルート *CA* によって発行された自己署名サーバー証明書をエクスポートし、それをゲートウェイにインポートします。
- 各ゲートウェイに対して一意のサーバー証明書を発行します。
- 自己署名証明書を指定している場合、ポータルのクライアント設定でエンドクライアントにルート *CA* 証明書を配布します。

証明書をポータルからエクスポートします。

1. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択します。
2. デプロイするゲートウェイ証明書を選択し、**Export Certificate**（証明書のエクスポート）をクリックします。
3. **File Format**（ファイル フォーマット）を **Encrypted Private Key and Certificate (PKCS12)**（暗号化された秘密鍵と証明書（**PKCS12**））に設定します。
4. 秘密鍵の暗号化に使用する **Passphrase**（パスフレーズ）を入力して確認します。
5. **OK** をクリックして PKCS12 ファイルを任意の場所にダウンロードします。

証明書をゲートウェイにインポートします。

1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから **Import**（インポート）をクリックします。
2. **Certificate Name**（証明書名）を入力します。
3. 前の手順でダウンロードした **Certificate File**（証明書ファイル）を **Browse**（参照）して選択します。
4. **File Format**（ファイル フォーマット）を **Encrypted Private Key and Certificate (PKCS12)**（暗号化された秘密鍵と証明書（**PKCS12**））に設定します。
5. ポータルからエクスポートしたときに秘密鍵の暗号化に使用した **Passphrase**（パスフレーズ）を入力して確認します。
6. **OK** をクリックして、証明書およびキーをインポートします。
7. **Commit**（コミット） をクリックして変更内容をゲートウェイにコミットします。

認証

GlobalProtect™ ポータルおよびゲートウェイは、エンドユーザーを認証してからでないと GlobalProtect へのアクセスを許可できません。そのため、ポータルおよびゲートウェイのセットアップする前に認証メカニズムを構成しておく必要があります。以下のセクションでは、サポートされている認証メカニズムおよびその設定方法について説明します。

GlobalProtect ユーザー認証について

GlobalProtect アプリが初めてポータルに接続する際、ユーザーはポータルへの認証を求められます。認証が成功すると、GlobalProtect ポータルはアプリが接続できるゲートウェイのリストが含まれた GlobalProtect 設定、および任意で、そのゲートウェイに接続するためのクライアント証明書を送信します。設定が正常にダウンロードされてキャッシュされたら、アプリは設定で指定されたゲートウェイのいずれかへの接続を試みます。これらのコンポーネントはネットワーク リソースおよび設定へのアクセスを提供するため、エンド ユーザーが認証する必要があります。

ポータルおよびゲートウェイに求められる適切なセキュリティ レベルは、ゲートウェイが保護するリソースの重要度によって異なります。GlobalProtect は柔軟な認証フレームワークを採用しているため、コンポーネント毎に適切な認証プロファイルおよび証明書プロファイルを選択できるようになっています。

- サポートされている GlobalProtect 認証方法
- アプリが提供する認証情報を識別する仕組み

サポートされている GlobalProtect 認証方法

以下のトピックでは、GlobalProtect がサポートしている認証方法について説明し、各方式の使用に関するガイドラインを示します。

- ローカル認証
- 外部認証
- クライアント証明書認証
- 2重認証
- 非ブラウザベースのアプリケーションの多要素認証
- シングルサインオン

ローカル認証

ユーザー アカウント認証情報と認証メカニズムの両方がファイアウォールに対してローカルです。この認証メカニズムは、すべての GlobalProtect ユーザーに対するアカウントが必要であるためスケーラブルではありません。そのため、非常に小規模のデプロイ環境の場合のみ妥当な手段になります。

外部認証

ユーザー認証機能は、外部の LDAP、Kerberos、TACACS+、SAML、または RADIUS サービス (1 回限りのパスワード (OTP) 認証などの 2 要素トークン ベースの認証サポートを含む) によって実行されます。外部認証を有効化する方法：

- 外部認証サービスにアクセスするための設定を含むサーバープロファイルを作成します。
- 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。

- ポータルおよびゲートウェイ設定でクライアント認証を指定し、さらにその設定を使用するエンドポイントの OS を任意で指定します。

GlobalProtect コンポーネントごとに異なる認証プロファイルを使用できます。指示内容については外部認証のセットアップを参照してください。構成例についてはリモート アクセス VPN（認証プロファイル）を参照してください。

SAML 認証を通じてポータルあるいはゲートウェイがユーザーを認証するよう設定する場合、*GlobalProtect* アプリケーション *4.1.8* 以前のリリースを実行しているユーザーは、シングル ログアウト *(SLO)* を無効化すると、アプリから ***Sign Out (***サインアウト*)* するオプションを使用できません。*GlobalProtect* アプリケーション *4.1.9* 以降のリリースを実行しているユーザーは、*SLO* が有効か無効かに関わらず、アプリから ***Sign Out (***サインアウト*)* するオプションを使用できます。

Kerberos を通じてユーザーを認証するようポータルあるいはゲートウェイを設定する場合、この認証方法を使ってユーザーが正常に認証すると、*GlobalProtect* アプリケーションから ***Sign Out (***サインアウト*)* するオプションが表示されなくなります。

GlobalProtect アプリケーションが ***Save User Credentials (***ユーザー認証情報を保存*)* するのを許可しない場合 ***(Network (***ネットワーク*) > GlobalProtect > Portals (***ポータル*) > <portal-config> > Agent (***エージェント*) > <agent-config> > Authentication (***認証*))***、*LDAP*、*TACACS+*、あるいは *RADIUS* 認証を使ってユーザーが認証を成功させると、ユーザーはアプリから ***Sign Out (***サインアウト*)* するオプションを使用できません。

クライアント証明書認証

ポータルまたはゲートウェイがクライアント証明書を使用してユーザー名を取得し、システムへのアクセス権を付与する前にユーザーを認証させるようにすることで、セキュリティを高めることができます。

- ユーザー認証を行うには、いずれかの証明書フィールド（Subject Name （サブジェクト名）フィールドなど）でユーザー名を指定する必要があります。
- エンドポイントを認証する場合は、証明書の Subject （サブジェクト）フィールドでユーザー名ではなくデバイスタイプを指定する必要があります。（接続方法がプレ ログオンである場合、ポータルあるいはゲートウェイはユーザーがログインする前にエンドポイントの認証を行います）

クライアント証明書認証を通じてユーザーを認証するようポータルあるいはゲートウェイを設定する場合、クライアント証明書だけを使ってユーザーが正常に認証すると、*GlobalProtect* アプリケーションから ***Sign Out (***サインアウト*)* するオプションが表示されなくなります。

クライアント証明書を指定するエージェント設定プロファイルの場合、各ユーザーがクライアント証明書を受け取ります。証明書を提供するメカニズムによって、各ユーザーに対して一意な証

明書を使用するか、そのエージェント設定に属するすべてのユーザーで同一の証明書を使用するかが決まります。

- 各ユーザーやエンドポイントに対して一意なクライアント証明書をデプロイする場合は、**SCEP** を使用します。ユーザーが最初にログインする際、ポータルがその企業の PKI から得られる証明書をリクエストします。ポータルがその一意な証明書を取得し、エンドポイントのもとにデプロイします。
- 単一のエージェント設定を受け取るすべてのユーザーに対して同じクライアント証明書をデプロイする場合は、ファイアウォールのローカルにある証明書をデプロイします。

また任意で、エンドポイントが接続をリクエストする際に提示するクライアント証明書を検証する証明書プロファイルを使用できます。この証明書プロファイルは、ユーザー名およびユーザードメインのフィールドの中身を指定したり、CA 証明書をリストアップしたり、セッションをブロックする基準を指定したりするとともに、CA 証明書の失効状態を判断する方法を提供します。証明書は新しいセッションのエンドポイントまたはユーザーの認証の一部であるため、ユーザーが最初にポータルにログインする前に、証明書プロファイルで使用される証明書をエンドポイントに対して事前にデプロイしておく必要があります。

また、証明書プロファイルはユーザー名を含める証明書フィールドを指定します。証明書プロファイルの Username（ユーザー名）フィールドで Subject（サブジェクト）が指定されている場合、エンドポイントから提示される証明書に、そのエンドポイントが接続を行うための共通名が含まれている必要があります。証明書プロファイルで Username（ユーザー名）フィールドとして Subject-Alt（サブジェクト代替名）に Email（電子メール）または Principal Name（プリンシパル名）が指定されている場合、エンドポイントから提示される証明書には対応するフィールドが含まれている必要があります。このフィールドは、GlobalProtect アプリがポータルまたはゲートウェイに対して認証するときにユーザー名として使用されます。

GlobalProtect は、証明書プロファイルに依存する共通アクセス カード（CAC）およびスマート カードによる認証もサポートしています。これらのカードの場合、証明書をスマート カード/CAC に発行したルート CA 証明書が証明書プロファイルに含まれている必要があります。

クライアント証明書認証を指定する場合、ユーザーの接続時にエンドポイントが証明書を提供するため、ポータル設定でクライアント証明書を設定しないでください。クライアント証明書認証の設定方法の例は、リモート アクセス VPN（証明書プロファイル）を参照してください。

2重認証

2 要素認証では、メカニズムワンタイムパスワードと Active Directory（AD）ログイン認証情報など、2 つのメカニズムを通してユーザーを認証する際にポータルまたはゲートウェイで認証します。2 要素認証を有効にするには、証明書プロファイルと認証プロファイルの両方を設定し、ポータルまたはゲートウェイの設定に追加します。

また、ポータルおよびゲートウェイが同じ認証方法を使用するように設定することも、別の認証方法を使うように設定することもできます。ユーザーは、ネットワークリソースへのアクセスを得る前に、コンポーネントが要求する 2 つのメカニズムを通じて正常に認証する必要があります。

GlobalProtect がユーザー名を取得できる **Username Field**（ユーザー名フィールド）が証明書プロファイルに指定されている場合、外部認証サービスは、認証プロファイルで指定されている外部認証サービスにユーザーを認証する際に自動的にそのユーザー名を使用します。たとえば、証明書プロファイルの **Username Field**（ユーザー名フィールド）が **Subject**（サブジェクト）に

設定されている場合、認証サーバーがユーザーの認証を試みる際、証明書の共通名フィールドの値がユーザー名として使用されます。ユーザーに証明書内のユーザー名での認証を強制しない場合、証明書プロファイルの **Username Field**（ユーザー名フィールド） が **None**（なし）に設定されていないことを確認してください。構成例については2 要素認証を使用したリモート アクセス VPNを参照してください。

非ブラウザベースのアプリケーションの多要素認証

(Windows および macOS エンドポイントのみ) 追加の認証が必要なこともある機密性の高い非ブラウザベースのネットワーク リソース (財務アプリケーションやソフトウェア開発アプリケーションなど) について、GlobalProtect アプリケーションはユーザーに通知し、こうしたリソースにアクセスするために必要な多要素認証をタイミング良く実行するよう要求できます。

シングルサインオン

(Windows のみ) シングル サインオン (SSO) を有効化すると、GlobalProtect アプリはユーザーの Windows ログイン認証情報を使用して、GlobalProtect ポータルおよびゲートウェイに対する認証と接続を自動的に行います。また、アプリがサードパーティの証明書をラップして、Windows ユーザーがサードパーティの認証情報プロバイダであっても認証して接続できるように設定することもできます。

シングル サインオンを有効化する場合、*GlobalProtect* アプリケーション *4.1.9* 以降のリリースを実行しているユーザーは、*SSO* を使用して認証を成功させた場合、アプリから ***Sign Out*** *(*サインアウト*)* するオプションを使用できません。

アプリが提供する認証情報を識別する仕組み

デフォルトでは、GlobalProtect アプリはポータル ログインに使用したものと同じログイン認証情報をゲートウェイに使用しようとします。ゲートウェイとポータルが同じ認証プロファイルや証明書プロファイルを使用している最も単純な状況では、アプリは透過的にゲートウェイに接続します。

アプリ毎に設定を別けることで、別の認証情報（一意の OTP など）を必要とする GlobalProtect ポータルおよびゲートウェイ（内部、外部、または手動専用）を指定するといったカスタマイズも可能です。これにより、GlobalProtect ポータルまたはゲートウェイが認証プロファイルで指定された認証情報を初めに求めるのではなく、一意の OTP を求めるようにすることができます。

アプリのエージェント認証動作を変更して強固かつ高速な認証を行う方法は 2 つあります。

- ポータルまたはゲートウェイでの Cookie 認証
- 一部またはすべてのゲートウェイへの認証情報の転送

ポータルまたはゲートウェイでの **Cookie** 認証

Cookie 認証により、エンド ユーザーがポータルとゲートウェイの両方に立て続けにログインしたり、それぞれの認証に複数の OTP を入力したりする必要がなくなるため、認証プロセスが簡略化されます。これによりユーザーに認証情報の入力を求める回数が最少化されるため、ユーザー体験が向上します。また Cookie により、一時的なパスワードを使用して、パスワードの有効期限が切れた後に VPN アクセスを再度有効にすることも可能になります。

ポータルおよび個々のゲートウェイ毎に個別の Cookie 認証を設定することができます（たとえば、機密性の高いリソースを保護しているゲートウェイについては、Cookie の有効期限を短くすることができます）。ポータルまたはゲートウェイが認証用 Cookie をエンドポイントにデプロイしたら、ポータルおよびゲートウェイはどちらも同じ Cookie を使用してユーザーを認証するようになります。アプリが Cookie を提示する際、ポータルまたはゲートウェイは指定された Cookie の有効期限に基づき、その有効性を判断します。Cookie の有効期限が切れたら、ポータルまたはゲートウェイへの認証を行うよう、GlobalProtect が自動的にユーザーに指示を出します。認証が成功したら、ポータルまたはゲートウェイは更新用の認証用 Cookie をエンドポイントに対して発行し、有効期間がまた一から始まります。

以下は、機密性の高い情報を保護していないポータルに対しては 15 日間、機密性の高い情報を保護するゲートウェイに対しては 24 時間の有効期限を Cookie に指定する例です。ユーザーが初めてポータルに認証する際、ポータルが認証用 Cookie を発行します。5 日後にユーザーがポータルに接続しようとする時点では、まだ認証用 Cookie は有効です。しかし、5日後にユーザーがゲートウェイに接続しようとすると、ゲートウェイはCookieの有効期限を評価し、有効期限切れであると判断します（5日＞24時間）。すると、ゲートウェイへの認証を行って認証成功後に更新用の認証用 Cookie を受信するよう、エージェントが自動的にユーザーに促します。この新しい認証用 Cookie は、ポータルに対しては 15 日間、ゲートウェイに対しては 24 時間、有効になります。

このオプションの使用方法の例は、2 要素認証のセットアップを参照してください。

一部またはすべてのゲートウェイへの認証情報の転送

2 要素認証では、独自の認証情報のセットを求めるポータルやゲートウェイのタイプ（内部、外部、または手動専用）を指定できます。この方法では、ポータルとゲートウェイで異なる認証情報が必要な場合（OTP が異なる場合またはログイン認証情報が完全に異なる場合）、認証プロセスが高速化されます。アプリが自動的に認証情報を転送しないポータルまたはゲートウェイを選択できるため、GlobalProtect コンポーネントごとにセキュリティをカスタマイズできます。たとえば、ポータルと内部的なゲートウェイのセキュリティは同じになりますが、最も機密性の高いリソースへのアクセスを提供するゲートウェイへのアクセスには 2 要素目として OTP または異なるパスワードを求めることができます。

このオプションの使用方法の例は、2 要素認証のセットアップを参照してください。

アプリが提供する証明書を識別する仕組み

macOS または Windows エンドポイントで認証にクライアント証明書を使用するように GlobalProtect を設定する場合、GlobalProtect はポータルやゲートウェイに対して認証するために有効なクライアント証明書を提示する必要があります。

クライアント証明書を有効にするには、以下の要件を満たす必要があります。

- ポータルおよびゲートウェイの設定で定義した認証局（CA）が発行した証明書であること。
- 証明書がクライアント認証の目的を指定していること。この目的は、証明書管理者が証明書を作成するときに指定します。
- 証明書が GlobalProtect ポータルのエージェント設定で設定されるように証明書ストアにあること。デフォルトでは、GlobalProtect アプリは最初にユーザー ストア内の有効な証明書を探します。存在しない場合、アプリケはマシン ストアを検索します。ユーザー ストアのほうが優先されるため、GlobalProtect アプリが証明書をユーザー ストアで見つけた場合、マシ

ン ストアでの検索は実行しません。強制的に GlobalProtect アプリが唯一の証明書ストアで証明書を検索するようにするには、適切な GlobalProtect ポータルのエージェント設定で **Client Certificate Store Lookup**（クライアントの証明ストアの検索）オプションを設定します。

- 証明書は、GlobalProtect ポータルエージェントの設定で指定された追加の目的に一致します。その他の目的を指定するには、証明書のオブジェクト識別子（OID）を識別し、適切な GlobalProtect ポータルのエージェント設定で **Extended Key Usage OID**（拡張キー使用 **OID**）値を設定する必要があります。OID とは、証明書を使用するアプリケーションまたはサービスを識別する数値であり、認証局（CA）が証明書を作成するときに自動的に証明書に付加されます。一般的な OID またはカスタム OID の指定の詳細は、OID による証明書選択を参照してください。

上記の要件を満たすクライアント証明書が 1 つしかない場合、アプリは自動的にそのクライアント証明書を認証に使用します。ただし、上記の要件を満たすクライアント証明書が複数ある場合は、GlobalProtect はエンドポイントで有効なクライアント証明書のリストからクライアント証明書を選択するようにユーザーに要求します。GlobalProtect がクライアント証明書を選択するようユーザーに要求するのはユーザーが最初に接続したときだけですが、どの証明書を選択すべきかユーザーが判断できない場合もあります。この場合、証明書の目的（OID によって指定）と証明書ストアによって、選択できるクライアント証明書のリストを絞り込むことを推奨します。アプリをカスタマイズするために可能なさまざまな設定の詳細は、GlobalProtect エージェントのカスタマイズを参照してください。

外部認証のセットアップ

以下のワークフローは、GlobalProtect ポータルおよびゲートウェイで外部認証サービスを利用する際のセットアップ方法を示しています。サポートされる認証サービスには、LDAP、Kerberos、RADIUS、SAML、および TACACS+ が含まれます。

GlobalProtect はローカル認証もサポートしています。ローカル認証を使用するには、*GlobalProtect* 接続を許可するユーザーおよびグループを含むローカルユーザーデータベース（***Device***（デバイス） > ***Local User Database***（ローカル ユーザー データベース)を作成し、次に認証プロファイルからそのデータベースを参照します。

詳細についてはサポートされている GlobalProtect 認証方法を参照してください。

外部認証をセットアップするためのオプションには、以下のようなものがあります。

- LDAP 認証のセットアップ
- SAML 認証のセットアップ
- Kerberos 認証のセットアップ
- RADIUS または TACACS+ 認証のセットアップ

LDAP 認証のセットアップ

LDAP は、認証サービスとしての組織やユーザー情報の中央リポジトリとしてよく使用されます。LDAP を使用して、アプリケーション ユーザーのロール情報を保存することもできます。

STEP 1 | サーバー プロファイルを作成します。

サーバー プロファイルによって外部認証サービスが識別され、その外部認証サービスに接続してユーザーの認証情報にアクセスする方法がファイアウォールに指示されます。

Active Directory（*AD*）への接続に *LDAP* を使用している場合、すべての *AD* ドメインに対して個別の *LDAP* サーバー プロファイルを作成する必要があります。

1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **LDAP** を選択して LDAP サーバー プロファイルを **Add (追加)** します。
2. **GP-User-Auth** などの **Profile Name**（プロファイル名）を入力します。
3. このプロファイルが複数の仮想システム容量のあるファイアウォール用であれば、仮想システムを選択するか、そのプロファイルを利用できる **Location**（場所）として **Shared**（共有）を選択します。
4. **Server List**（サーバー リスト）エリアの **Add**（追加）をクリックし、サーバーの **Name**（名前）、**LDAP Server**（**LDAP** サーバー）の IP address（IP アドレス）または

FQDN、および **Port**（ポート）といった、認証サービスへの接続に必要な情報を入力します。

5. LDAP サーバーの **Type (タイプ)** を選択します。
6. **Bind DN** と **Password**（パスワード）を入力して、ファイアウォールを認証するための認証サービスを有効にします。
7. （LDAP のみ）ディレクトリサーバーとの保護された接続のためにエンドポイントで SSL または TLS を使いたい場合は、 **Require SSL/TLS secured connection**（**SSL/TLS** で保護された接続を要求）オプションを有効にしてください（デフォルトで有効）。サーバー ポートによってエンドポイントが使用するプロトコル：
   - 389（デフォルト） – TLS（具体的には、デバイスは StartTLS 操作を使用して、最初のプレーンテキスト接続を TLS にアップグレードします）
   - 636 – SSL
   - その他の任意のポート – デバイスはまず TLS を使用しようとします。ディレクトリサーバーで TLS がサポートされていない場合は、SSL にフォールバックします。
8. （LDAP のみ）保護を強化するには、**Verify Server Certificate for SSL sessions**（**SSL** セッションのサーバー証明書を確認）オプションを有効化します。すると、エンドポイントは SSL/TLS 接続にディレクトリサーバーが提示する証明書を確認します。この検証を有効にする場合は、**Require SSL/TLS secured connection**（**SSL/TLS**で保護された接続を要求）オプションを有効化する必要があります。進めるための確認において、証明書は次のいずれかの条件に合う必要があります。
   - デバイス証明書のリストにある：**Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）。必要に応じて、証明書をデバイスにインポートします。
   - 証明書の署名者は信頼できる証明機関のリストにあること：**Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Default Trusted Certificate Authorities**（デフォルトの信頼できる証明機関）
9. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | (任意) 認証プロファイルを作成します。

認証プロファイルは、ポータルまたはゲートウェイがユーザーを認証する際に使用するサーバー プロファイルを指定します。ポータルまたはゲートウェイ上で、1 つまたは複数のクライアント認証プロファイルに 1 つまたは複数の認証プロファイルを割り当てることができます。クライアント認証プロファイル内の認証プロファイルで細かなユーザー認証を行う方法

の詳細は、GlobalProtect ゲートウェイの設定および GlobalProtect ポータルへのアクセスのセットアップを参照してください。

管理者の操作なしでユーザーが接続後、有効期限の切れたパスワードを変更できるようにするには、プレ ログオン付属リモートアクセス VPN の使用することを検討してください。

ユーザーのパスワードが期限切れになった場合、一時的な *LDAP* パスワードを割り当てて、ユーザーが *GlobalProtect* にログインできるようにすることもできます。この場合、一時的なパスワードを使用してポータルに対する認証を行うことはできますが、一時的なパスワードを再利用することはできないため、ゲートウェイのログインに失敗する可能性があります。この問題を回避するには、ポータル設定（***Network***（ネットワーク） **> *GlobalProtect* > *Portal***(ネットワーク > *GlobalProtect* > ポータル)）で認証のオーバーライドを構成し、*GlobalProtect* アプリが *Cookie* を使用してポータルに対する認証を行い、一時的なパスワードでゲートウェイに対する認証を行うことができるようにします。

1. **Device** > **Authentication Profile**(デバイス > 認証プロファイル) の順に選択し、新しいプロファイルを**Add**(追加) します。
2. プロファイルの**Name**（名前）を入力します。
3. **Authentication**（認証） **Type**（タイプ）を **LDAP** に設定します。
4. ステップ1 で作成した Kerberos 認証 **Server Profile**（サーバー プロファイル）を選択します。
5. **Login Attribute**（ログイン属性）として **sAMAccountName** と入力します。
6. **Password Expiry Warning**（パスワード失効の警告）を設定し、パスワードの失効をユーザーに通知するまでの日数を指定します。デフォルトでは、パスワードの有効期限（範囲は 1～255）が切れる 7 日前にユーザーへの通知が行われます。ユーザー有効期限前にはパスワードを変更する必要があるため、ユーザーが GlobalProtect のアクセスを続けられるように十分な通知を送ることを確認してください。この機能を使用するには、LDAP サーバープロファイルにて次のいずれかの LDAP サーバー タイプを指定する必要があります：**active-directory**, **e-directory**, or **sun**.

   プレログオンを有効にしない限り、ユーザーはパスワードの有効期限が切れたときに GlobalProtect にアクセスすることはできません。
7. **User Domain**（ユーザー ドメイン）と**Username Modifier**（ユーザー名修飾子）を指定します。エンドポイントは、**User Domain**（ユーザー ドメイン）と **Username Modifier**（ユーザー名修飾子）の値を結合して、ユーザーがログイン時に入力するドメイン/ユーザー名の文字列を変更します。エンドポイントは、変更した文字列を認証に、**User Domain**（ユーザー ドメイン） の値を User-ID グループ マッピングに使用します。認証サービスが特定の書式でドメイン/ユーザー名文字列を必要とする場合や、

ユーザーに正確にドメインを入力することが不確実な場合、ユーザー入力の変更は有用です。以下のオプションから選択します：

- 未変更のユーザー入力のみを送信するには、**User Domain**[ユーザー ドメイン] を空白 (デフォルト) のままにして、**Username Modifier**[ユーザー名修飾子] を変数 **%USERINPUT%** (デフォルト) に設定します。
- ユーザー入力の前にドメインを追加するには、**User Domain**（ユーザー ドメイン）を入力して、**Username Modifier**（ユーザー名修飾子）を **%USERDOMAIN%\%USERINPUT%** に設定します。
- ユーザー入力の後にドメインを追加するには、**User Domain**（ユーザー ドメイン）を入力して、**Username Modifier**（ユーザー名修飾子）を **%USERINPUT%@%USERDOMAIN%** に設定します。

> ***Username Modifier***（ユーザー名修飾子）に ***%USERDOMAIN%*** 変数が含まれている場合、ユーザーが入力したドメイン文字列は ***User Domain***（ユーザー ドメイン）の値に置き換わります。***User Domain***（ユーザー ドメイン）が空白の場合、デバイスがどのユーザーが入力したドメイン文字列でも削除します。

8. **Advanced**（詳細）タブで、**Allow List**（許可リスト）を **Add**（追加）して、このプロファイルで認証できるユーザーとユーザー グループを選択します。**all**（すべて） オプションを使用すれば、すべてのユーザーがこのプロファイルで認証できます。デフォルトでは、リストにエントリはありませんので、どのユーザーも認証できません。
9. <239>OK</239> をクリックします。

STEP 3 | 設定をコミットします。

Commit（コミット）をクリックします。

SAML 認証のセットアップ

Security Assertion Markup Language (SAML) は、パーティ間、特に ID プロバイダ (IdP) とサービス プロバイダ間で認証および認可データを交換するために使用される XML ベース、オープンスタンダードのデータ フォーマットです。SAML は OASIS Security Services Technical Committee の製品です。

STEP 1 | サーバー プロファイルを作成します。

サーバー プロファイルによって外部認証サービスが識別され、その外部認証サービスに接続してユーザーの認証情報にアクセスする方法がファイアウォールに指示されます。

次のステップでは、IdP から SAML メタデータ ファイルをインポートし、ファイアウォールが自動的にサーバープロファイルを作成し、接続、登録、IdP 情報の入力を自動で行えるようにする方法を説明します。IdP がメタデータ ファイルを提供しない場合は、**Device (**デバイ

ス) > **Server Profiles (**サーバー プロファイル**)** > **SAML Identity Provider (SAML** アイデンティティ プロバイダ**)**、を選択し、サーバー プロファイルを **Add (**追加**)** します。

1. SAML メタデータ ファイルを IdP から、ファイアウォールがアクセスできるエンドポイントにエクスポートします。

   ファイルのエクスポート方法については、IdP のドキュメントを参照してください。
2. **Device (**デバイス**)** > **Server Profiles (**サーバー プロファイル**)** > **SAML Identity Provider (SAML** アイデンティティ プロバイダ**)** を選択します。
3. メタデータ ファイルをファイアウォールに **Import (**インポート**)** します。
4. **GP-User-Auth** などの、サーバー プロファイルを識別する **Profile Name** (プロファイル名) を入力します。
5. メタデータ ファイルを **Browse (**参照**)** します。
6. （推奨）**Validate Identity Provider Certificate (**アイデンティティ プロバイダ証明書の検証**)**（デフォルト）を選択し、ファイアウォールに idP 証明書を検証させます。

   検証は、サーバー プロファイルを認証プロファイルに割り当てて変更を **Commit**（コミット）した後にのみ行われます。ファイアウォールは認証プロファイル内の証明書プロファイルを使用して証明書を検証します。
7. **Maximum Clock Skew**（最大クロック スキュー）、を入力します。これは、ファイアウォールが IdP メッセージを検証するときに、IdP とファイアウォール間で許容されるシステム時間差（秒）です。デフォルト値は60秒で、範囲は1～900秒です。差がこの値を超えると、認証は失敗します。
8. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | (任意) 認証プロファイルを作成します。

認証プロファイルは、ポータルまたはゲートウェイがユーザーを認証する際に使用するサーバー プロファイルを指定します。ポータルまたはゲートウェイ上で、1 つまたは複数のクライアント認証プロファイルに 1 つまたは複数の認証プロファイルを割り当てることができます。クライアント認証プロファイル内の認証プロファイルで細かなユーザー認証を行う方法の詳細は、GlobalProtect ゲートウェイの設定および GlobalProtect ポータルへのアクセスのセットアップを参照してください。

GlobalProtect アプリケーション *5.0* 以降のリリースでは、*SAML* 認証がプレ ログオンを伴うリモート アクセス VPN をサポートしています。

1. **Device** > **Authentication Profile**(デバイス > 認証プロファル) の順に選択し、新しい認証プロファイルを**Add**(追加) します。
2. 認証プロファイルの **Name**（名前）を入力します。
3. **Authentication**（認証） **Type**（タイプ）を **SAML** に設定します。
4. ステップ1 で作成した SAML **IdP Server Profile**（**IdP** サーバー プロファイル）を選択します。

5. 以下のオプションを構成して、ファイアウォールと SAML IDP プロバイダ間の証明書認証を有効化します。詳細は、SAML 2.0 認証を参照してください。
   - ファイアウォールが IdP に送信するメッセージに署名するために使用する **Certificate for Signing Requests**（署名要求の証明書）。
   - ファイアウォールが IdP 証明書を検証するために使用する **Certificate Profile**（証明書プロファイル）。
6. ユーザー名および管理ロールのフォーマットを指定します。
   - **Username Attribute**（ユーザー名属性）および **User Group Attribute**（ユーザー グループ属性）を指定します。

     その他の外部認証タイプとは異なり、*SAML* 認証プロファイルには ***User Domain***（ユーザー ドメイン） 属性がありません。

   - (任意) このプロファイルを使用して、IdP アイデンティティ ストアで管理する管理アカウントを認証する場合、**Admin Role Attribute**（管理者ロール属性）および **Access Domain Attribute**（アクセス ドメイン属性）を指定します。
7. **Advanced**（詳細）タブで、**Allow List**（許可リスト）を **Add**（追加）して、このプロファイルで認証できるユーザーとグループを選択します。**all**（すべて） オプションを使用すれば、すべてのユーザーがこのプロファイルで認証できます。デフォルトでは、リストにエントリはありませんので、どのユーザーも認証できません。

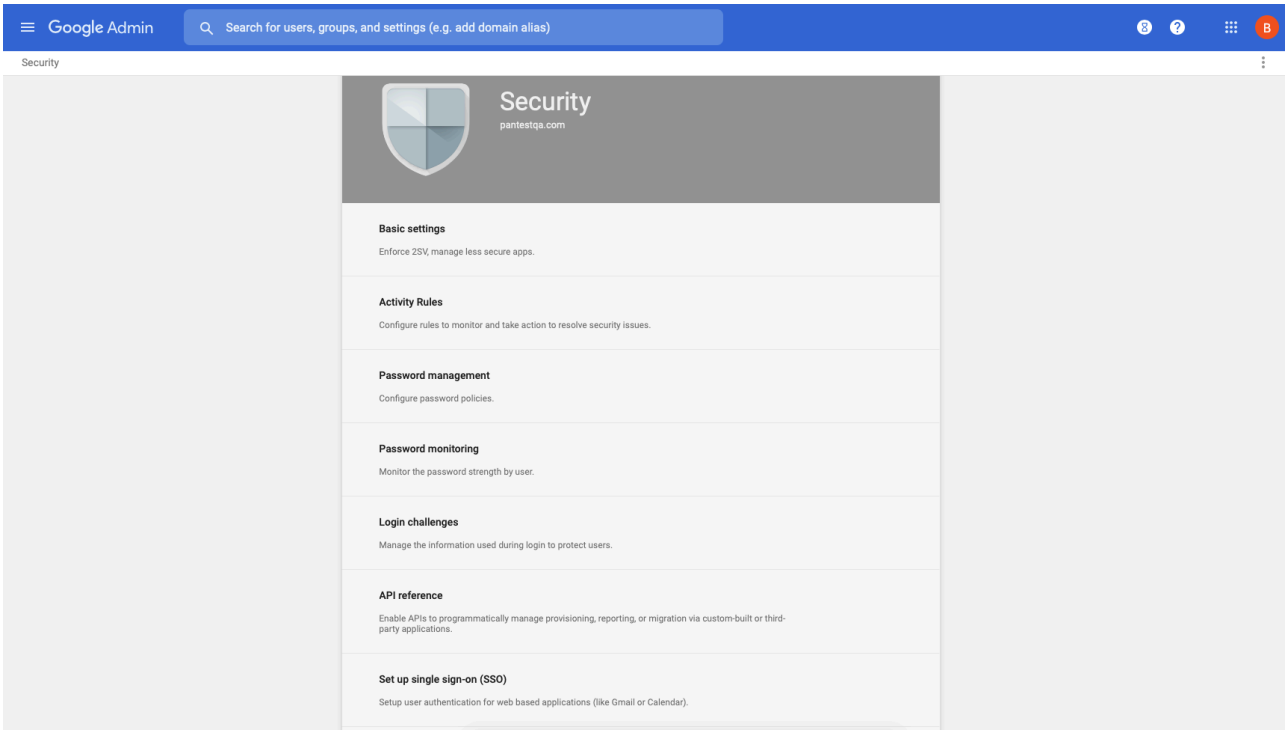
   Allow List（許可リスト）のユーザー名が SAML IdP サーバーから返されたユーザー名と一致することを確認してください。
8. <239>OK</239> をクリックします。

STEP 3 | 設定を **Commit**（コミット）します。

STEP 4 | (Chromebooks のみ) Chromebook の SAML SSO を有効にします。

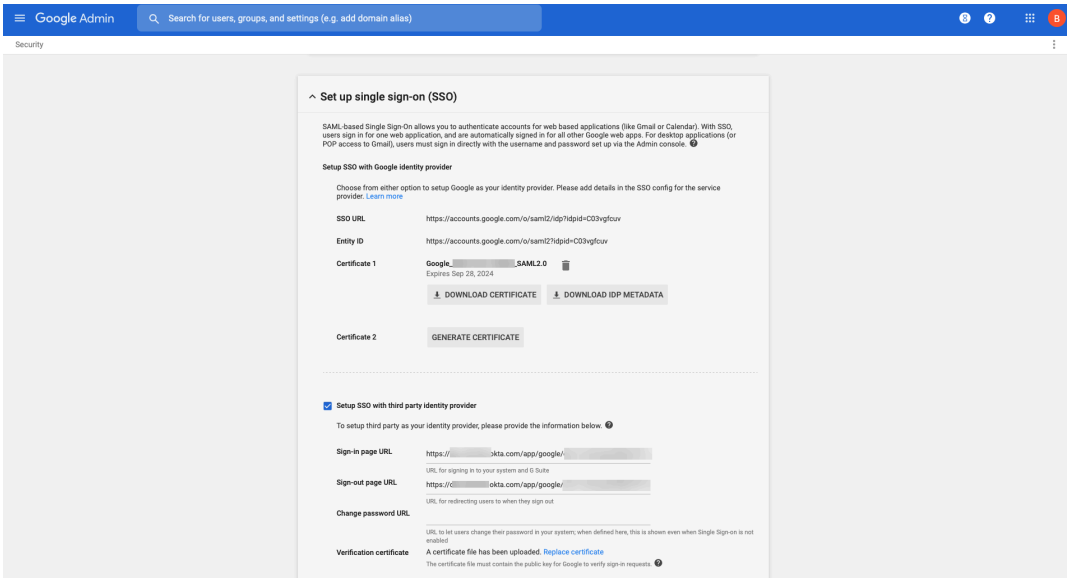
これらの手順を実行すると、 Chromebooks 上の Android の GlobalProtect アプリケーションに SAML SSO をセットアップすることができます。

1. Google 管理者コンソールにサインインして、**Security**（セキュリティ）を選択します。



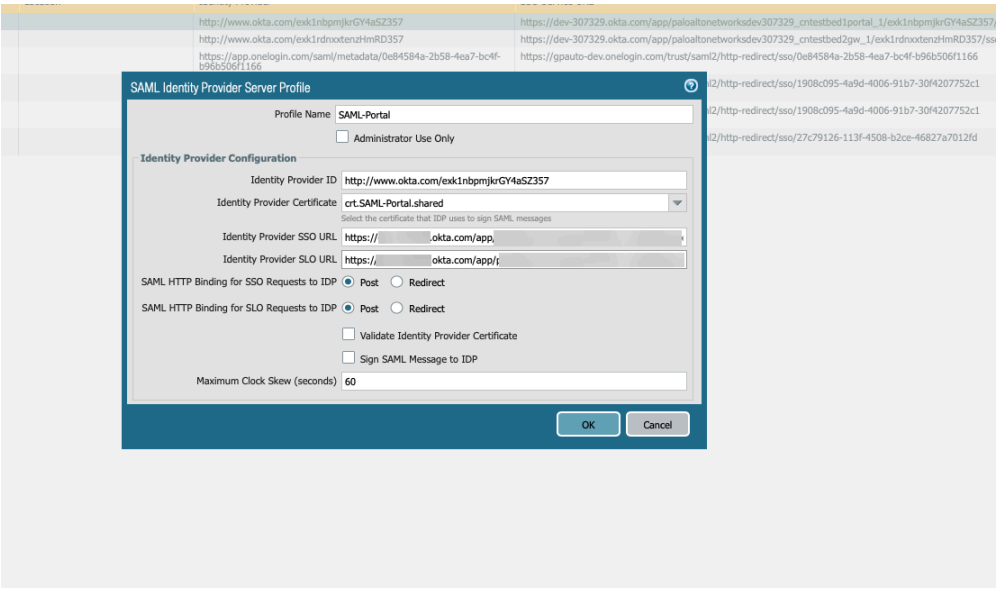
2. **Set up single sign-on (SSO)**（シングル・サインオン**(SSO)** のセットアップ）を選択します。
3. (オプション) Google 以外のプロバイダーで SSO をセットアップする場合は、**Setup SSO with third party identity provider**（サードパーティの識別プロバイダで **SSO** をセットアップ）を選択して、**Sign-in page URL**（サインイン ページ **URL**） と **Sign-out**

page URL（サインアウト ページ **URL**） を指定し、有効な**Verification certificate**（検証証明書）をアップロードします。



4. GlobalProtect 内で SAML アイデンティティ プロバイダを設定します。

   1. GlobalProtect コンソール内で、**Device**（デバイス） > **Server Profiles**（サーバーのプロファイル） > **SAML Identity Provider**（**SAML** アイデンティティ プロバイダ）を選択します。
   2. Google 管理者コンソール内の IdP に入力した値を一致させます。



Kerberos 認証のセットアップ

Kerberos は、チケットを使用して、保護されていないネットワークを介して通信するノードが、身元を互いに安全に証明できるようにするコンピュータネットワーク認証プロトコルです。

*Kerberos*認証は、*Windows*（*7*、*8*、および　*10*）および *macOS*（*10.10* 以降のリリース）エンドポイントでサポートされています。*macOS* エンドポイントの *Kerberos* 認証には、最小限の *GlobalProtect* アプリ バージョン *4.1.0* が必要です。

STEP 1 | サーバー プロファイルを作成します。

サーバー プロファイルによって外部認証サービスが識別され、その外部認証サービスに接続してユーザーの認証情報にアクセスする方法がファイアウォールに指示されます。

1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **Kerberos** を選択して Kerberos サーバー プロファイルを **Add (追加)** します。
2. **GP-User-Auth** などの **Profile Name**（プロファイル名）を入力します。
3. このプロファイルが複数の仮想システム容量のあるファイアウォール用であれば、仮想システムを選択するか、そのプロファイルを利用できる **Location**（場所）として **Shared**（共有）を選択します。
4. **Servers**（サーバー）エリアの **Add**（追加）をクリックして、認証サーバーへの接続用に次の情報を入力してください：
   - サーバーの **Name**（名前）
   - **Kerberos Server**（**Kerberos** サーバー）の IP アドレスまたは FQDN を入力してください
   - ポート
5. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | (任意) 認証プロファイルを作成します。

認証プロファイルは、ポータルまたはゲートウェイがユーザーを認証する際に使用するサーバー プロファイルを指定します。ポータルまたはゲートウェイ上で、1 つまたは複数のクライアント認証プロファイルに 1 つまたは複数の認証プロファイルを割り当てることができます。クライアント認証プロファイル内の認証プロファイルで細かなユーザー認証を行う方法の詳細は、GlobalProtect ゲートウェイの設定および GlobalProtect ポータルへのアクセスのセットアップを参照してください。

管理者の操作なしでユーザーが接続後、有効期限の切れたパスワードを変更できるようにするには、プレ ログオン付属リモートアクセス VPN の使用することを検討してください。

1. **Device** > **Authentication Profile**(デバイス > 認証プロファル) の順に選択し、新しいプロファイルを**Add**(追加) します。
2. プロファイルの **Name**（名前）を入力し、認証の **Type**（タイプ）として **Kerberos** を選択します。
3. ステップ1 で作成した Kerberos 認証 **Server Profile**（サーバー プロファイル）を選択します。
4. **User Domain**（ユーザー ドメイン）と**Username Modifier**（ユーザー名修飾子）を指定します。エンドポイントはこれらの値を組み合わせて、ユーザーがログイン時に入力するドメイン/ユーザー名の文字列を変更します。エンドポイントは、変更した文字列を認証に、**User Domain**（ユーザー ドメイン） の値を User-ID グループ マッピングに使

用します。認証サービスが特定の書式でドメイン/ユーザー名文字列を必要とする場合や、ユーザーに正確にドメインを入力することが不確実な場合、ユーザー入力の変更は有用です。以下のオプションから選択します：

- 未変更のユーザー入力を送信するには、**User Domain**（ユーザー ドメイン）を空白（デフォルト）のままにして、**Username Modifier**（ユーザー名修飾子）を変数 **%USERINPUT%**（デフォルト）に設定します。
- ユーザー入力の前にドメインを追加するには、**User Domain**（ユーザー ドメイン）を入力して、**Username Modifier**（ユーザー名修飾子）を **%USERDOMAIN%\%USERINPUT%** に設定します。
- ユーザー入力の後にドメインを追加するには、**User Domain**（ユーザー ドメイン）を入力して、**Username Modifier**（ユーザー名修飾子）を **%USERINPUT%@%USERDOMAIN%** に設定します。

> ***Username Modifier***（ユーザー名修飾子）に ***%USERDOMAIN%*** 変数が含まれている場合、ユーザーが入力したドメイン文字列は ***User Domain***（ユーザー ドメイン）の値に置き換わります。***User Domain***（ユーザー ドメイン）が空白の場合、デバイスがどのユーザーが入力したドメイン文字列でも削除します。

5. ネットワークが対応していれば、Kerberos シングル サインオン（SSO）を設定します。
   - **Kerberos Realm**（**Kerberos** レルム）を入力して（最大 127 文字）、ユーザーのログイン名のホスト名部分を指定します。例: ユーザー アカウント名が user@EXAMPLE.LOCAL の場合、レルムは EXAMPLE.LOCAL になります。
   - **Kerberos Keytab**（**Kerberos** キータブ） ファイルを **Import**（インポート）します。入力を促されたら、キータブ ファイルの **Browse**（参照）を行い、**OK** をクリックします。認証中は、エンドポイントは最初にキータブを使用して SSO の確立を試みます。これに成功した場合、アクセスを試行しているユーザーが **Allow List**（許可リスト）に含まれていれば、認証は即座に成功します。含まれていない場合、認証プロセスは、指定した認証 **Type**（タイプ）を使用する手動（ユーザー名/パスワード）認証にフォールバックします。**Type**（タイプ）は Kerberos 以外でも構いません。この挙動を変更し、ユーザーが Kerberos だけを使用して認証できるようにするには、GlobalProtect ポータル エージェント設定にて **Use Default Authentication on Kerberos Authentication Failure**（**Kerberos** 認証の失敗時にはデフォルトの認証を使用）を **No**（いいえ）に設定します。
6. **Advanced**（詳細）タブで、**Allow List**（許可リスト）を **Add**（追加）して、このプロファイルで認証できるユーザーとユーザー グループを選択します。**all**（すべて） オプションを使用すれば、すべてのユーザーがこのプロファイルで認証できます。デフォルトでは、リストにエントリはありませんので、どのユーザーも認証できません。
7. <239>OK</239> をクリックします。

STEP 3 | 設定をコミットします。

Commit（コミット）をクリックします。

RADIUS または TACACS+ 認証のセットアップ

RADIUS は、リモート アクセス サーバーが中央のサーバーと通信し、ダイアルイン ユーザーを認証して必要なシステムまたはサービスへのアクセスを承認するためのクライアント/サーバー プロトコルおよびソフトウェアです。TACACS+ とは、リモート アクセス サーバーがユーザーのログイン パスワードを認証サーバーに転送して指定されたシステムへのアクセスを許可するかどうか判断するための UNIX ネットワークに一般的な定評のある認証プロトコルです。

STEP 1 | サーバー プロファイルを作成します。

サーバー プロファイルによって外部認証サービスが識別され、その外部認証サービスに接続してユーザーの認証情報にアクセスする方法がファイアウォールに指示されます。

クライアント VSA を RADIUS サーバーに受け渡す機能を有効化する場合は、*RADIUS* サーバープロファイルを作成しなければなりません。

1. **Device**（デバイス） > **Server Profiles**（サーバー プロファイル）の順に選択してから、プロファイルのタイプ（**RADIUS** または **TACACS+**）を選択します。
2. 新しい RADIUS または TACACS+ サーバー プロファイルを**Add**（追加）します。
3. **GP-User-Auth** などの **Profile Name**（プロファイル名）を入力します。
4. このプロファイルが複数の仮想システム容量のあるファイアウォール用であれば、仮想システムを選択するか、そのプロファイルを利用できる **Location**（場所）として **Shared**（共有）を選択します。
5. 以下の **Server Settings**（サーバー設定）を指定します。
   - **Timeout (sec)**（タイムアウト（秒））—認証サーバーからの応答がないことが原因でサーバー接続要求がタイムアウトになるまでの秒数。
   - **Authentication Protocol**（認証プロトコル）—認証サーバーへの接続に使用するプロトコルを選択します。オプションには、**CHAP**、**PAP**、**PEAP-MSCHAPv2**、**PEAP**

with GTC（**GTC** 付属の **PEAP**）、または **EAP-TTLS with PAP**（**PAP** 付属の **EAP-TTLS**）が含まれます。

> 認証プロトコルとして ***PEAP-MSCHAPv2***（*Protected Extensible Authentication Protocol Microsoft Challenge Handshakie Authentication Protocol version 2*）を構成すると、リモート ユーザーは、パスワードの有効期限が切れたときに *GlobalProtect* アプリケーションを使用して *RADIUS* または *Active Directory*（*AD*）パスワードを変更できます。 管理者は次のログイン時にパスワードを変更しなければなりません。

- （RADIUS のみ）**Retries**（再試行）–ファイアウォールが要求をドロップするまでに認証サーバーへの接続を試みる回数。
- （TACACS+ のみ）**Use single connection for all authentication**（すべての認証に単一接続を使用）–リクエストごとに個別のセッションを使用するのではなく、単一の TCP セッションを経由してすべての TACACS+ 認証リクエストを行います。

6. **Servers**（サーバー）エリアの **Add**（追加）をクリックして、認証サーバーへの接続用に次の情報を入力してください：
   - 名前
   - **RADIUS** または **TACACS+ Server**（サーバー）（IP アドレスまたはサーバーの FQDN）
   - **Secret**（シークレット）（認証サービスでファイアウォールの認証を可能にする共有シークレット）
   - ポート
7. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | (任意) 認証プロファイルを作成します。

認証プロファイルは、ポータルまたはゲートウェイがユーザーを認証する際に使用するサーバー プロファイルを指定します。ポータルまたはゲートウェイ上で、1 つまたは複数のクライアント認証プロファイルに 1 つまたは複数の認証プロファイルを割り当てることができます。クライアント認証プロファイル内の認証プロファイルで細かなユーザー認証を行う方法の詳細は、GlobalProtect ゲートウェイの設定および GlobalProtect ポータルへのアクセスのセットアップを参照してください。

> 管理者の操作なしでユーザーが接続後、有効期限の切れた自分のパスワードを変更できるようにするには、プレ ログオン付属リモートアクセス VPN の使用することを検討してください。

1. **Device** > **Authentication Profile**(デバイス > 認証プロファル) の順に選択し、新しいプロファイルを**Add**(追加) します。
2. プロファイルの**Name**（名前）を入力します。
3. **Authentication**（認証） **Type**（タイプ） （**RADIUS** または **TACACS+**）を選択します。
4. ドロップダウンからステップ 1 で作成した RADIUS または TACACS+ 認証の **Server Profile**（サーバー プロファイル）を選択します。

5. （RADIUS のみ）この情報を認証プロファイルに含める場合は、**Retrieve user group from RADIUS**（**RADIUS** からユーザー グループを取得） を有効にします。
6. **User Domain**（ユーザー ドメイン）と**Username Modifier**（ユーザー名修飾子）を指定します。エンドポイントはこれらの値を組み合わせて、ユーザーがログイン時に入力するドメイン/ユーザー名の文字列を変更します。エンドポイントは、変更した文字列を認証に、**User Domain**（ユーザー ドメイン） の値を User-ID グループ マッピングに使用します。認証サービスが特定の書式でドメイン/ユーザー名文字列を必要とする場合や、ユーザーに正確にドメインを入力することが不確実な場合、ユーザー入力の変更は有用です。以下のオプションから選択します：
   - 未変更のユーザー入力を送信するには、**User Domain**（ユーザー ドメイン）を空白（デフォルト）のままにして、**Username Modifier**（ユーザー名修飾子）を変数 **%USERINPUT%**（デフォルト）に設定します。
   - ユーザー入力の前にドメインを追加するには、**User Domain**（ユーザー ドメイン）を入力して、**Username Modifier**（ユーザー名修飾子）を **%USERDOMAIN%\%USERINPUT%** に設定します。
   - ユーザー入力の後にドメインを追加するには、**User Domain**（ユーザー ドメイン）を入力して、**Username Modifier**（ユーザー名修飾子）を **%USERINPUT%@%USERDOMAIN%** に設定します。

   Username Modifier（ユーザー名修飾子） に ***%USERDOMAIN%*** 変数が含まれている場合、ユーザーが入力したドメイン文字列は ***User Domain***（ユーザー ドメイン）の値に置き換わります。***User Domain***（ユーザー ドメイン）が空白の場合、デバイスがどのユーザーが入力したドメイン文字列でも削除します。
7. **Advanced**（詳細）タブで、**Allow List**（許可リスト）を **Add**（追加）して、このプロファイルで認証できるユーザーとユーザー グループを選択します。**all**（すべて） オプションを使用すれば、すべてのユーザーがこのプロファイルで認証できます。デフォルトでは、リストにエントリはありませんので、どのユーザーも認証できません。
8. <239>OK</239> をクリックします。

STEP 3 | 設定を **Commit**（コミット）します。

クライアント証明書認証のセットアップ

任意のクライアント証明書認証では、ユーザーは GlobalProtect ポータルまたはゲートウェイへの接続をリクエストする際にクライアント証明書を提示します。ポータルあるいはゲートウェイは共有/固有のクライアント証明書を使用し、ユーザーやエンドポイント自分の組織に属したものかどうかを検証します。

クライアント証明書をデプロイする方法は、お客様の組織のセキュリティ要件によって異なります。

- 認証用の共有クライアント証明書のデプロイ
- 認証用のマシン証明書をデプロイ
- 認証用のユーザー固有のクライアント証明書のデプロイ

認証用の共有クライアント証明書のデプロイ

エンドポイント ユーザーが組織に属するかどうかを検証するために、すべてのエンドポイントに対して 1 つのクライアント証明書を使用するか、特定のクライアント設定と共にデプロイする個別の証明書を生成します。ここでは、自己署名クライアント証明書を発行し、ポータルからデプロイする作業を行います。

STEP 1 | 複数の GlobalProtect エンドポイントにデプロイする証明書を生成します。

1. GlobalProtect コンポーネントの自己署名証明書を発行するためのルート CA 証明書を作成します。
2. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから、新しい証明書を **Generate**（生成）します。
3. **Certificate Type**（証明書タイプ）を **Local**（ローカル）に設定します（デフォルト）。
4. **Certificate Name**（証明書名）を入力します。この名前にはスペースを含められません。
5. この証明書をアプリ証明書（**GP_Windows_App** など）として識別する **Common Name**（共通名） を入力します。この証明書は、同じエージェント設定を使用するすべてのアプリに配布されるため、特定のユーザーまたはエンドポイントを一意に識別する必要はありません。
6. **Signed By**（署名者）フィールドで、ルート CA を選択します。
7. **OCSP Responder**（**OCSP** レスポンダ）を選択し、証明書の失効状態を確認します。
8. **OK** をクリックして証明書を生成します。

STEP 2 | 2 要素認証のセットアップを行います。

GlobalProtect ポータル エージェント設定で認証設定を行い、ポータルがファイアウォールの **Local**（ローカル）にあるアプリ証明書を、その設定を受け取るクライアントに透過的にデプロイできるようにします。

認証用のマシン証明書をデプロイ

エンドポイントが組織に属するかどうかを確認するには、独自の公開鍵インフラストラクチャ（PKI）を使用して、各エンドポイントに対してマシン証明書を発行および配布する（推奨）か、エクスポート用の自己署名マシン証明書を生成します。プレ ログオン接続方式ではマシン証明書が必要であり、エンドポイントに事前にインストールされていなければ GlobalProtect コンポーネントがアクセスを許可しません。

自分の組織に属したエンドポイントであることを確認するために、ユーザー認証用の認証プロファイルを設定する必要もあります（2 要素認証を参照してください）。

以下の作業を行ってクライアント証明書を作成し、手動でエンドポイントにデプロイします。詳細については、GlobalProtect ユーザー認証についてを参照してください。設定例については、リモート アクセス VPN（証明書プロファイル）を参照してください。

STEP 1 | GlobalProtect アプリおよびエンドポイントに対してクライアント証明書を発行します。

これにより、GlobalProtect ポータルおよびゲートウェイが、そのエンドポイントが自分の組織に属したものであることを検証できるようになります。

1. GlobalProtect コンポーネントの自己署名証明書を発行するためのルート CA 証明書を作成します。
2. **Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから **Generate**（生成）をクリックします。
3. **Certificate Name**（証明書名）を入力します。証明書名にスペースを含めることはできません。
4. 証明書に表示される IP アドレスまたは FQDN を **Common Name**（共通名） フィールドに入力します。
5. **Signed By**（署名者） ドロップダウンからルート CA を選択します。
6. **OCSP Responder**（**OCSP** レスポンダ）を選択し、証明書の失効状態を確認します。
7. 証明書の **Cryptographic Settings**（暗号化設定）を設定します。これには、暗号化 **Algorithm**（アルゴリズム）、キーの長さ（**Number of Bits**（ビット数））、**Digest**（ダイジェスト）アルゴリズム（sha1、sha256、または sha384 を使用。クライアント証明書では sha512 はサポートされていない）、および **Expiration**（有効期間）（日数）などが含まれます。

   ファイアウォールが FIPS-CC モードで、鍵生成のアルゴリズムが RSA の場合、RSA キーは 2048 ビットまたは 3072 ビットである必要があります。
8. **Certificate Attributes**（証明書の属性）領域で、その エンドポイントが自分の組織に所属していることを一意に識別できる属性を**Add**（追加）および定義します。**Host Name**（ホスト名）属性（証明書の SAN フィールドに入力される）を追加する場合、この値は **Common Name**（共通名）に定義した値と同じにする必要があります。
9. **OK** をクリックして証明書を生成します。

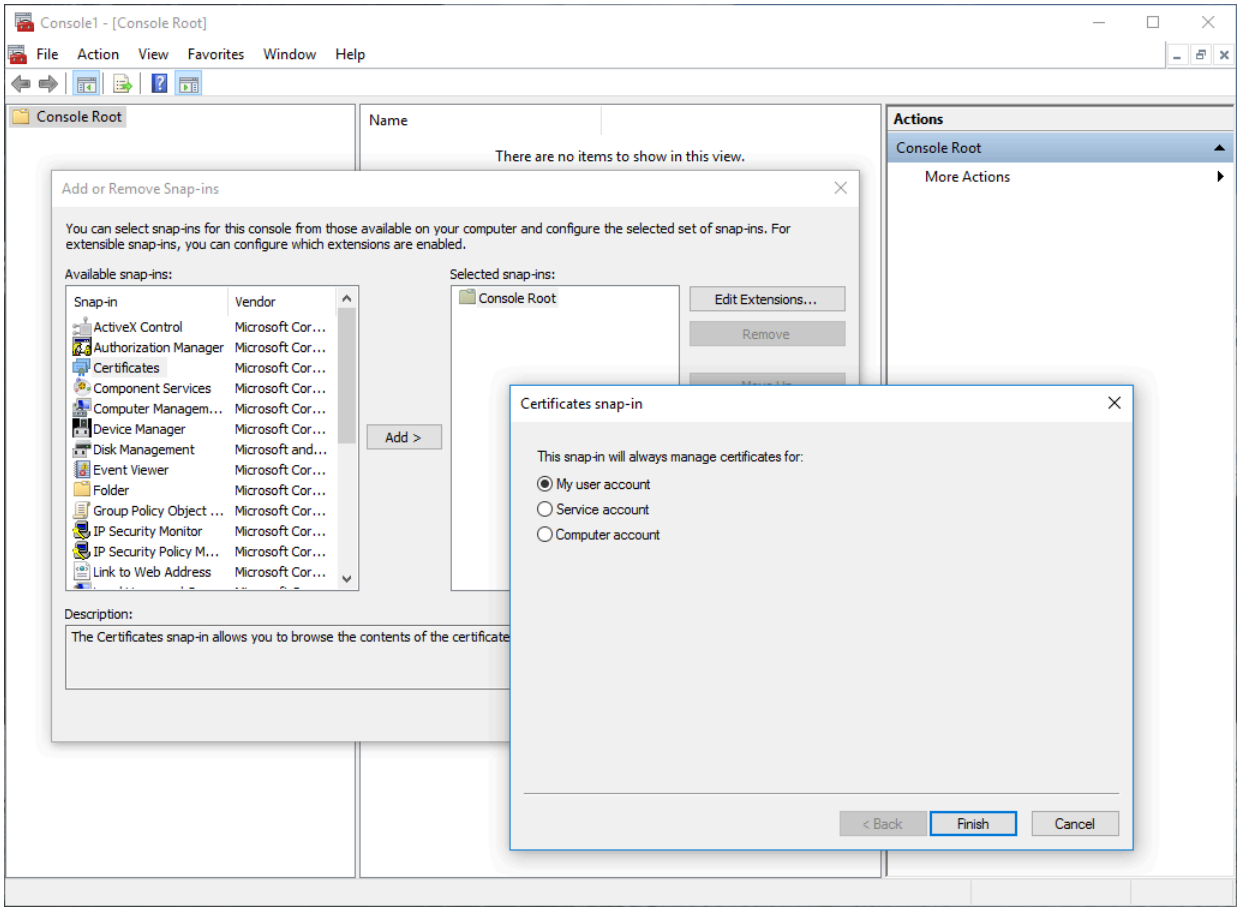
STEP 2 | エンドポイントの個人用証明書ストアに証明書をインストールします。

一意のユーザー証明書またはマシン証明書を使用している場合、ポータルあるいはゲートウェイに最初に接続する前に、エンドポイントの個人用証明書ストアに各証明書をインストールしておく必要があります。マシン証明書を Windows のローカル コンピュータの証明書ストアおよび macOS のシステム キーチェーンにインストールします。ユーザー証明書を Windows の現在のユーザーの証明書ストアおよび macOS のキーチェーンにインストールします。

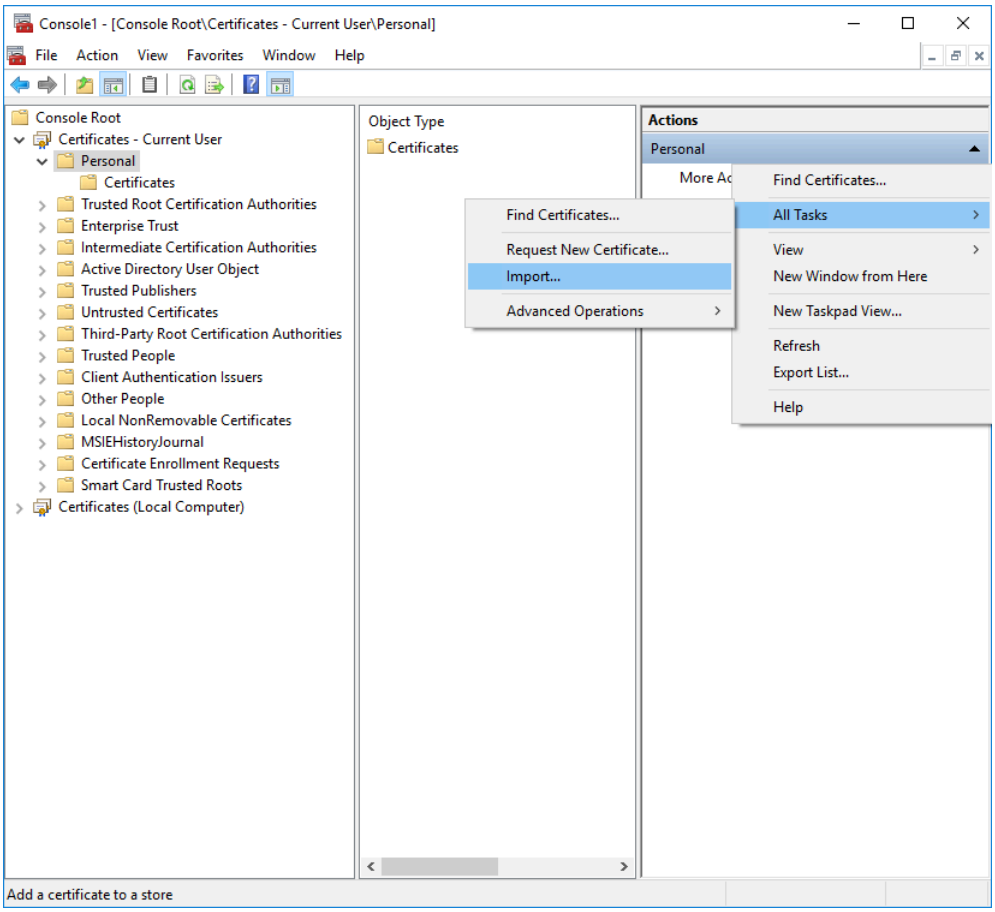
たとえば、Microsoft 管理コンソールを使用して Windows システムに証明書をインストールするには、以下の手順を実行します。

1. コマンド プロンプトから、「`mmc`」と入力して Microsoft 管理コンソール を起動します。
2. **[ファイル]** > **[スナップインの追加と削除]** の順に選択します。

3. **Available snap-ins**（利用可能なスナップイン） のリストから、**Certificates**（証明書）を選択し、**Add**（追加）して、インポートする証明書の種類に応じて、次の証明書スナップインのいずれかを選択します。
   - **Computer account**（コンピュータ アカウント） – マシン証明書をインポートする場合はこのオプションを選択します。
   - **My user account**（ユーザー アカウント） – ユーザー証明書をインポートする場合はこのオプションを選択します。



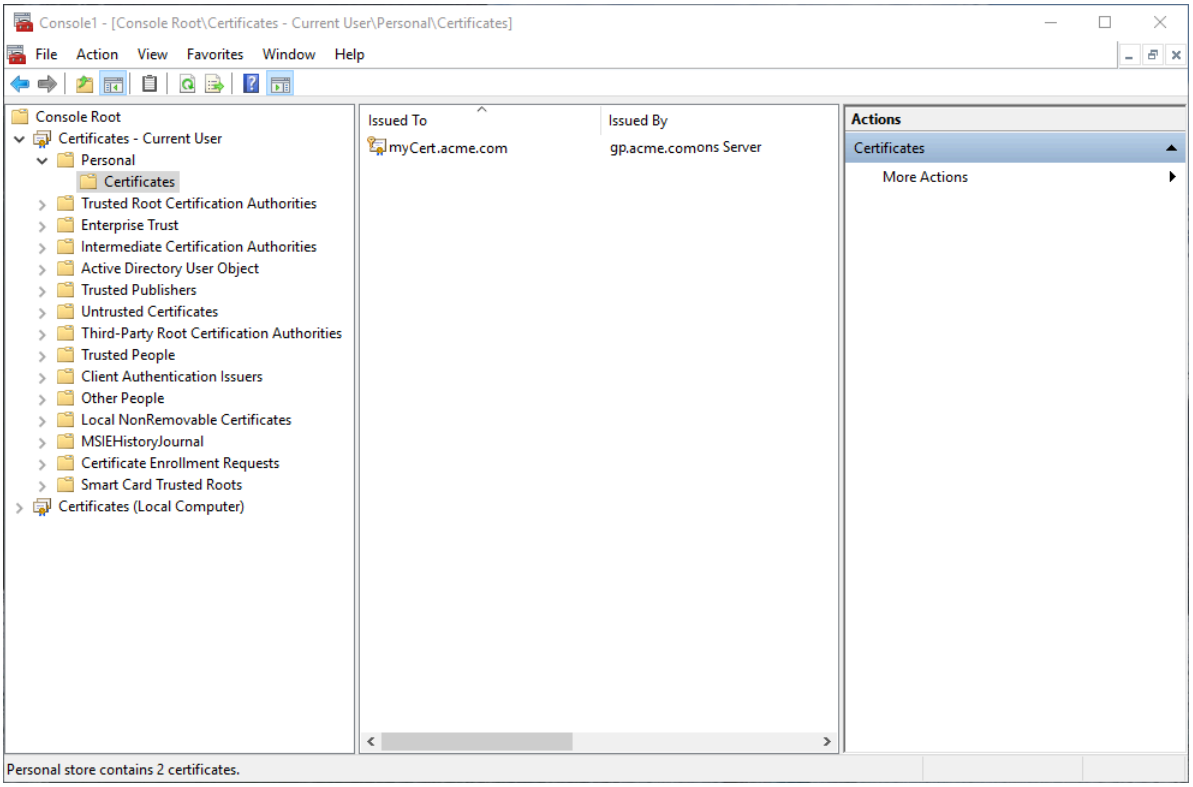
4. **Console Root**（コンソール ルート）から、**Certificates**（証明書）を展開して、**Personal**（個人）を選択します。
5. **Actions**（操作）列で **Personal**（個人） > **More Actions**（他の操作） > **All Tasks**（すべてのタスク） > **Import**（インポート）の順に選択し、証明書のインポート ウィザードの手順に従って CA から受信した PKCS ファイルをインポートします。



6. インポートする .p12 証明書ファイルを**Browse**（参照）し（参照するファイル タイプとして **Personal Information Exchange** を選択）、**Password**（パスワード）に秘密鍵の暗号化に使用したパスワードを入力します。**Certificate store**（証明書ストア）を **Personal**（個人）に設定します。

STEP 3 | 証明書が個人用証明書ストアに追加されたことを確認します。

Console Root（コンソール ルート） から個人証明書ストアへ移動します（**Certificates**（証明書） > **Personal**（個人） > **Certificates**（証明書）：



STEP 4 | クライアント証明書の発行に使用されたルート CA 証明書をファイアウォールにインポートします。

パブリック CA またはエンタープライズ PKI CA といったクライアント証明書を発行したのが外部の CA である場合のみ、このステップが必要になります。自己署名証明書を使用している場合、ルート CA はポータルおよびゲートウェイによってすでに信頼されています。

1. クライアント証明書の発行に使用されたルート CA 証明書（Base64 形式）をダウンロードします。
2. クライアント証明書を生成した CA からファイアウォールに、ルート CA 証明書をインポートします。
   1. **[Device]** > **[証明書の管理]** > **[証明書]** > **[デバイス証明書]** の順に選択し、**[インポート]** をクリックします。
   2. **Certificate Type**（証明書タイプ）を **Local**（ローカル）に設定します（デフォルト）。
   3. **Certificate Name**（証明書名）フィールドに、クライアント CA 証明書であることを識別できる名前を入力します。
   4. **Browse**（参照）をクリックして、CA からダウンロードした **Certificate File**（証明書ファイル）を選択します。
   5. **File Format**（ファイル フォーマット）を **Base64 Encoded Certificate (PEM)**（**Base64** エンコード済み証明書 **(PEM)**）に設定して、**OK** をクリックします。
   6. **Device Certificates**（デバイス証明書）タブで、証明書情報を開くためにインポートする証明書を選択します。
   7. **Trusted Root CA**（信頼されたルート **CA**）を選択して **OK** をクリックします。

STEP 5 | クライアント証明書プロファイルを作成します。

1. **Device**（デバイス） > **Certificates**（証明書） > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）の順に選択し、新しい証明書プロファイルを **Add(追加)**します。
2. プロファイル **Name**（名前）を入力します。
3. **Username Field**（ユーザー名フィールド）の値を選択し、ユーザーの ID 情報が含まれる証明書内のフィールドを指定します。

   ポータルまたはゲートウェイが証明書だけを使ってユーザーを認証するように設定する予定の場合、**Username Field**（ユーザー名フィールド）を指定する必要があります。これにより、GlobalProtect がユーザー名を証明書と関連付けられるようになります。

   ポータルまたはゲートウェイを 2 要素認証用にセットアップする予定の場合、**None**（なし）というデフォルトの値をそのまま残すか、またはセキュリティの層をもう一つ加えるために、ユーザー名を指定することができます。ユーザー名を指定する場合、クライアント証明書内のユーザー名が認証をリクエストしているユーザーの

名前にマッチしているかどうかが、外部認証サービスによって確認されます。これにより、証明書の発行対象のユーザー本人であることが約束されます。

ユーザーは、証明書に含まれているユーザー名を変更することができません。

4. **CA Certificates**（**CA** 証明書）領域で、**Add**（追加）をクリックします。**CA Certificates**（**CA** 証明書）ドロップダウンから、ステップ 4 でインポートした信頼されたルート CAを選択してから、**OK** をクリックします。

STEP 6 | 設定を保存します。

変更を **Commit**（コミット）します。

認証用のユーザー固有のクライアント証明書のデプロイ

個々のユーザーを認証するためには、各 GlobalProtect ユーザーに対して一意のクライアント証明書を発行し、GlobalProtect を有効にする前にそのクライアント証明書をエンドポイントにデプロイする必要があります。ユーザー固有のクライアント証明書の生成およびデプロイメントを自動化するために、GlobalProtect ポータルをお客様のエンタープライズ PKI 内の SCEP サーバーへの SCEP（Simple Certificate Enrollment Protocol）クライアントとして動作させることができます。

エンタープライズ PKI はポータルからリクエストを受けた際にユーザー固有の証明書を生成し、その証明書をポータルに送信します。つまり、SCEP のオペレーションは動的なものになります。その後、ポータルが証明書をアプリに透過的にデプロイできるようになります。ユーザーがアクセスを求めると、アプリがクライアント証明書を提示し、ポータルあるいはゲートウェイに認証できるようになります。

GlobalProtect ポータルまたはゲートウェイは、エンドポイントおよびユーザーを特定できる情報を使用し、そのユーザーへのアクセスを許可するかどうか評価します。ホスト ID がデバイス ブロックリストに載っている、または証明書プロファイルで指定されているブロック オプションにそのセッションがマッチする場合、GlobalProtect はアクセスをブロックします。SCEP ベースのクライアント証明書が無効なために認証が失敗した場合、GlobalProtect アプリは、認証プロファイルの設定に基づいて、ポータルの認証と証明書の取得を試みます。アプリがポータルから証明書を取得できない場合、エンドポイントは接続を行うことができません。

STEP 1 | SCEP プロファイルを作成します。

1. **Device**（デバイス） > **Certificate Management**（証明書管理） > **SCEP**の順に選択し、**Add**（追加）をクリックして新しい SCEP プロファイルを追加します。
2. SCEP プロファイルを識別する **Name**（名前）を入力します。
3. このプロファイルが複数の仮想システム容量のあるファイアウォール用であれば、仮想システムを選択するか、そのプロファイルを利用できる **Location**（場所）として **Shared**（共有）を選択します。

STEP 2 | （任意）SCEP ベースの証明書発行をより安全に行いたい場合は、各回の証明書要求について PKI およびポータルとの間に SCEP チャレンジレスポンス機能を設定します。

この機能の設定後はバックグラウンドで動作するため、追加の入力が必要になることはありません。

連邦情報処理標準（FIPS）に準拠するため連邦情報処理標準（FIPS）に準拠するため、**Dynamic (動的) SCEP**要求を使用し、HTTPSを利用する**Server URL (サーバー URL)** を指定します（ステップ 7を参照）。

以下のいずれかの**SCEP** チャレンジオプションを選択します。

- **None**（なし）– （デフォルト）SCEP サーバーは証明書の発行前にポータルとのチャレンジを行いません。
- **Fixed**（固定）–PKI インフラストラクチャ内の SCEP サーバーから取得した登録チャレンジ **Password**（パスワード） を入力します。
- **Dynamic**（動的） – 任意の **Username**（ユーザー名）および**Password**（パスワード）（多くの場合は PKI 管理者の認証情報となります）と、ポータルのクライアントがこれらの認証情報を送信する SCEP **Server URL**（サーバー **URL**）を入力します。認証情報は、各証明書要求時にポータルの OTP パスワードを透過的に生成する SCEP サーバーで認証するために使用されます (各証明書要求の後`The enrollment challengepassword is` フィールドの画面の更新後にこの OTP 変更が表示されます)。PKI はそれぞれの新しいパスワードをポータルへ透過的に受け渡し、また、証明書要求に対してそれらのパスワードを使用します。

STEP 3 | SCEP サーバーとポータル間の接続設定を指定し、ポータルがクライアント証明書をリクエスト・受信できるようにします。

証明書の**Subject**（サブジェクト）名でトークンを指定することで、エンドポイントまたはユーザーに関する補足的な情報を含めることができます。

SCEP サーバーに対する CSR の **Subject**（サブジェクト）フィールドでは、ポータルには **CN** としてトークン値が、**SerialNumber**（シリアル番号）としてホスト ID が含まれます。ホスト ID は、エンドポイントのタイプによって異なります。GUID（Windows）、インターフェースの MAC アドレス（macOS）、Android ID（Android エンドポイント） 、UDID（iOS エンドポイント）、GlobalProtect が割り当てる一意の名前（Chrome）。

1. **Configuration**（設定）エリアで、PKI 内の SCEP サーバーにアクセスするためにポータルが使用する **Server URL**（サーバー **URL**）を設定します（例：`http://10.200.101.1/certsrv/mscep/`）。
2. SCEP サーバーを識別するための **CA-IDENT Name**（**CA-IDENT** 名）を入力します（最大 255 文字）。
3. SCEP サーバーが生成する証明書に使用する **Subject**（サブジェクト）名を入力します。サブジェクトは、**<attribute>=<value>** の形式で識別される名前にして、共通名（CN）属性（**CN=<variable>**）を含める必要があります。CN は次のような動的なトークンをサポートしています。
   - `$USERNAME`–このトークンは、ポータルに特定のユーザーの証明書の要求を許可するために使用します。この変数を使用するには、グループ マッピングの有効化も行

う必要があります。ユーザーが入力したユーザー名は user-group マッピング テーブルの名前と一致する必要があります。

- `$EMAILADDRESS`—このトークンは、特定の電子メール アドレスに関連付けられた証明書を要求するために使用します。この変数を使用するには、グループ マッピングの有効化を行い、Server Profile（サーバー プロファイル）の**Mail Domains**（メール ドメイン）領域で **Mail Attributes**（メール属性）を設定する必要もあります。GlobalProtect がユーザーの電子メール アドレスを識別できない場合、一意の ID を生成してその値を含む CN を入力します。
- `$HOSTID`—エンドポイントのみに対する証明書をリクエストするには、ホスト ID のトークンを指定します。ユーザーがポータルにログインしようと試みると、エンドポイントはホスト ID の値を含む、ユーザーを識別できる情報を送信します。

GlobalProtect ポータルがアプリに SCEP 設定をプッシュする際、サブジェクト名の CN の部分は、証明書の所有者が持つ実際の値（ユーザー名、ホスト ID、または電子メール アドレス）に置き換えられます（例： **`O=acme,CN=johndoe`**）。

4. **Subject Alternative Name Type**（サブジェクトの別名タイプ）を選択します。
   - **RFC 822 Name**（**RFC822** 名）— 証明書のサブジェクトまたはサブジェクト代替名拡張子に電子メールアドレス名を入力します。
   - **DNS Name**（**DNS** 名）— 証明書の検証に使用する DNS 名を入力します。
   - **Uniform Resource Identifier**（ユニフォームリソース識別子）— アプリが証明書を取得する URI リソース名を入力します。
   - **None**（なし）— 証明書の属性を指定しません。

STEP 4 | （任意）証明書の **Cryptographic Settings**（暗号設定）を行います。

- 証明書の **Number of Bits**（ビット数）（鍵長）を選択します。

  ファイアウォールが FIPS-CC モードで鍵生成アルゴリズムが RSA の場合。RSA キーは 2,048 ビット以上でなければなりません。
- 証明書署名要求（CSR）用のダイジェスト アルゴリズムを示す **Digest for CSR**（**CSR** 用ダイジェスト）を選択します（ sha1, sha256, sha384, or sha512）。

STEP 5 | （任意）許可される証明書の用途を設定します（署名用または暗号化用）。

- この証明書を署名のために使用する場合、**Use as digital signature**（デジタル署名として使用）のチェックボックスを選択します。このオプションより、デジタル署名の検証を行う際にエンドポイントが証明書に含まれる秘密鍵を使用するようになります。
- この証明書を暗号化のために使用する場合、**Use for key encipherment**（鍵の暗号化のために使用）のチェックボックスを選択します。このオプションにより、SCEP サーバーが発行する証明書を通して確立された HTTPS 接続を経由して交換されたデータをアプリのエンドポイントで暗号化する際に、証明書に含まれる秘密鍵を使用するようになります。

STEP 6 | （任意）ポータルが正しい SCEP サーバーに確実に接続されるようにするために、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）を入力します。このフィンガープ

リントは、SCEP サーバー インターフェイスの **Thumbprint**（指紋）フィールドから取得します。

1. SCEPサーバーの管理UIのURLを入力します（例：**http://<ホスト名あるいはIP>/CertSrv/mscep_admin/**）。
2. Thumbprint（指紋）をコピーし、**CA Certificate Fingerprint**（**CA** 証明書フィンガープリント）に入力します。

STEP 7 | SCEP サーバーと GlobalProtect ポータルの間の相互 SSL 認証を有効にします。米国の連邦情報処理標準（FIPS）に準拠するためにこれが必須になります。Federal Information Processing Standard (連邦情報処理標準 - FIPS)

FIPS-CC の実施についてはファイアウォールのログインページおよびそのステータスバーに表示されます。

SCEP サーバーのルート**CA Certificate**（**CA** 証明書）を選択します。また、必要に応じて**Client Certificate**（クライアント証明書）を選択し、SCEP サーバーと GlobalProtect ポータルの間の相互 SSL 認証を有効にすることも可能です。

STEP 8 | 設定を保存・コミットします。

1. **OK** をクリックして設定を保存します。
2. 設定を **Commit**（コミット）します。

ポータルが SCEP プロファイルの設定を使用して CA 証明書をリクエストしようと試み、それをファイアウォールがホストするポータルに保存します。正しく実行されると、CA証明書が**Device** > **Certificate Management** > **Certificates**(デバイス > 証明書管理 > 証明書)に表示されます。

STEP 9 | （任意）SCEP プロファイルを保存した後にポータルが証明書の取得に失敗した場合は、ポータルから証明書署名要求（CSR）を手動で生成できます。

1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから、新しい証明書を **Generate**（生成）します。
2. **SCEP** を **Certificate Type**（証明書タイプ）として選択します。
3. **Certificate Name**（証明書名）を入力します。この名前にはスペースを含められません。
4. お客様のエンタープライズ PKI に CSR を送信する際に使用する **SCEP Profile**（**SCEP** プロファイル）を選択します。
5. **OK** をクリックしてリクエストを送信し、証明書を生成します。

STEP 10 | 2 要素認証のセットアップを行います。

SCEP プロファイルを GlobalProtect ポータル エージェント設定に割り当て、設定を受信するアプリに対してポータルがクライアント証明書を透過的にリクエスト・デプロイできるようにします。

2 要素認証のセットアップ

重要なデータを保護するため、または PCI、SOX、HIPAA といった規制の要件を満たすために強固な認証手段が必要な場合、2 要素認証スキームを使用した認証サービスを使用するように GlobalProtect を構成することができます。2 要素認証スキームでは、エンド ユーザーが把握しているもの（暗証番号やパスワードなど）と、エンド ユーザーが所有しているもの（ハードウェアまたはソフトウェア トークン/OTP、スマート カード、証明書など）の 2 つが必要です。また、複数の外部認証サービスを組み合わせて、またはクライアントと証明書プロファイルを使う 2 要素認証を有効化することもできます。

以下のトピックでは、GlobalProtect に 2 要素認証をセットアップする方法例を紹介します。

- 証明書および認証プロファイルを使用した 2 要素認証の有効化
- 1 回限りのパスワード（OTP）を使用した 2 要素認証の有効化
- スマート カードを使用した 2 要素認証の有効化
- ソフトウェアトークンアプリケーションを使用して2要素認証を有効にする

証明書および認証プロファイルを使用した 2 要素認証の有効化

次のワークフローでは、ユーザが証明書プロファイルと認証プロファイルの両方を認証するように GlobalProtect を設定する方法について説明します。ユーザーがポータル/ゲートウェイに接続するには、両方の方法を使用して認証に成功する必要があります。この設定の詳細については、2 要素認証を使用したリモート アクセス VPN を参照してください。

STEP 1 | 認証サーバープロファイルを作成します。

この認証サーバープロファイルによって、ファイアウォールが外部認証サービスに接続してユーザーの認証情報を取得する方法が決定されます。

Active Directory（*AD*）への接続に *LDAP* を使用している場合、すべての *AD* ドメインに対して個別の *LDAP* サーバー プロファイルを作成する必要があります。

1. **Device(デバイス）** > **Server Profiles**（サーバー プロファイル）の順に選択し、プロファイルのタイプ（**LDAP**、**Kerberos**、**RADIUS**、または **TACACS+**）を選択します。
2. 新しいサーバー プロファイルを**Add**（追加）します。
3. **gp-user-auth** などの **Profile Name**（プロファイル名）を入力します。
4. （LDAP のみ）LDAP サーバーの **Type**（タイプ）を選択します（**active-directory**、**e-directory**、**sun**、または **other**（その他））。
5. サーバープロファイルの種類に応じて **Servers**（サーバー）または **Servers List**（サーバー リスト）領域で **Add**（追加）をクリックし、認証サービスへの接続に次の情報を入力します。
   - サーバーの **Name**（名前）
   - **Server**（サーバー）の FQDN の IP アドレス
   - ポート
6. （RADIUS、TACACS+ および LDAP のみ）ファイアウォールで認証サービスによる認証を可能にする設定を以下のように指定します。
   - RADIUS および TACACS+ — サーバー エントリを追加するときに共有の **Secret**（シークレット）を入力します。
   - LDAP — **Bind DN**（バインド **DN**）および **Password**（パスワード）を入力します。
7. （LDAP のみ）ディレクトリサーバーとの保護された接続のためにエンドポイントで SSL または TLS を使いたい場合は、 **Require SSL/TLS secured connection**（**SSL/TLS** で保護された接続を要求）オプションを有効にしてください（デフォルトで有効）。エンドポントが使用するプロトコルは、**Server list**（サーバーリスト）内の **Port**（ポート）によって異なります。
   - 389（デフォルト） — TLS（具体的には、エンドポイントは StartTLS 操作を使用して、TLS への最初のプレーンテキスト接続をアップグレードします）。
   - 636—SSLです。
   - その他の任意のポート — エンドポイントはまず TLS の使用を試みます。ディレクトリ サーバーで TLS がサポートされていない場合、エンドポイントは SSL を使用します。
8. （LDAP のみ）保護を強化するには、**Verify Server Certificate for SSL sessions**（**SSL** セッションのサーバー証明書を確認）オプションを有効化します。すると、エンドポイントは SSL/TLS 接続にディレクトリサーバーが提示する証明書を確認します。この検証を有効にする場合は、**Require SSL/TLS secured connection**（**SSL/TLS**で保護された

接続を要求）オプションを有効化する必要があります。次のいずれかの条件が真でなければ、検証が成功しません。

- 証明書がデバイス証明書のリストにある：**Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）。必要に応じて、証明書をエンドポイントにインポートします。
- 証明書の署名者は信頼できる証明機関のリストにあること：**Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Default Trusted Certificate Authorities**（デフォルトの信頼できる証明機関）。

9. **OK** をクリックしてサーバー プロファイルを保存します。

STEP 2 | ユーザーを認証するサービスを特定する認証プロファイルを作成します。後で、プロファイルをポータルおよびゲートウェイに割り当てるオプションを利用できます。

1. **Device** > **Authentication Profile**(デバイス > 認証プロファル) の順に選択し、新しいプロファイルを**Add**(追加) します。
2. プロファイルの**Name**（名前）を入力します。
3. **Authentication**（認証）**Type**（タイプ）を選択します。
4. **Server Profile**（サーバー プロファイル）で、ステップ 1 で作成したプロファイルを選択します。
5. （LDAP のみ）**Login Attribute**（ログイン属性）として **sAMAccountName**を入力します。
6. **OK** をクリックして認証プロファイルを保存します。

STEP 3 | ポータルがユーザーのエンドポイントから得たクライアント証明書の認証に使用するクライアント証明書プロファイルを作成します。

2 要素認証でクライアント証明書を使用するように設定すると、クライアント証明書で指定されていれば、外部認証サービスはユーザー名の値を使用してユーザーを認証します。これにより、ログインしているユーザーは確実に証明書が発行されているユーザーになります。

1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）の順に選択し、新しい証明書プロファイルを **Add(追加)**します。
2. プロファイルの**Name**（名前）を入力します。
3. 以下のいずれかの **Username Field**（ユーザー名欄）値を選択します：
   - クライアント証明書に個々のユーザーを認証させたい場合は、ユーザーを識別する証明書フィールドを選択します。
   - ポータルからクライアント証明書をデプロイしている場合、**None**（なし）を選択します。
   - プレ ログオンの接続方式で使用する証明書プロファイルをセットアップしている場合、 **None**（なし）を選択します。
4. プロファイルを割り当てる **CA Certificates**（**CA** 証明書） を **Add**（追加） してから、次の設定を構成します：
   1. **CA certificate**（**CA** 証明書）として、信頼できるルート CA 証明書、または SCEP サーバーから得られる CA 証明書を選択します。必要に応じて証明書をインポートしてください。
   2. （任意）**Default OCSP URL**（デフォルト **OCSP URL**）を入力します。
   3. （任意）**OCSP Verify Certificate**（**OCSP** 検証証明書字）用の証明書を選択します。
   4. (任意) 証明書の署名に使用したテンプレートの **Template Name (テンプレート名)** を入力します。
5. （任意）ユーザーが要求したセッションをいつブロックするかを指定するには、次のオプションを選択します：
   1. 証明書のステータスが未知（unknown）の場合。
   2. **Certificate Status Timeout**（証明書ステータスのタイムアウト）にある秒数の間に、GlobalProtect コンポーネントが証明書ステータスを取得しない場合。
   3. クライアント証明書のサブジェクトのシリアル番号属性が、GlobalProtect アプリがエンドポイントについてレポートするホスト ID に一致しない場合。
   4. 証明書の有効期限が切れました。
6. <239>OK</239> をクリックします。

STEP 4 | （任意）GlobalProtect クライアントおよびエンドポイントに対してクライアント証明書を発行します。

クライアント証明書を透過的にデプロイするには、ポータルが共有クライアント証明書をエンドポイントに配布するよう設定するか、ポータルが SCEP を使用して各ユーザーに対して一意のクライアント証明書をリクエスト、デプロイするように設定します。

1. エンタープライズ PKI またはパブリック CA を使用して、クライアント証明書を各 GlobalProtect ユーザーに発行します。
2. プレ ログオン接続方式の場合は、エンドポイントで個人用証明書ストアに証明書をインストールします。

STEP 5 | GlobalProtect の設定を保存します。

Commit（コミット）をクリックします。

1 回限りのパスワード（OTP）を使用した 2 要素認証の有効化

ポータルおよびゲートウェイ上でワンタイムパスワード（OTP）を使用する 2 要素認証を設定する流れを説明します。ユーザーがアクセスを求めた際、ポータルまたはゲートウェイはユーザーに OTP を入力するよう求めます。認証サービスは OTP をトークンとしてユーザーの RSA デバイスに送信します。

2 要素認証方式を設定することは、他のタイプの認証を設定することに似ています。2 要素認証スキームでは、次の設定を行う必要があります：

- 認証プロファイルに割り当てられたサーバープロファイル（通常、2 要素認証用の RADIUS サービスに対して）。
- これらのコンポーネントが使用するサービス用の認証プロファイルを含むクライアント認証プロファイル。

デフォルトでは、アプリはポータルおよびゲートウェイへのログインに使用されたものと同じ認証情報を提供します。OTP 認証の場合、この動作によってゲートウェイでの最初の認証に失敗し、ユーザーへのログイン要求に遅延が発生するため、ユーザーの OTP が期限切れになる可能性があります。これを回避するには、同じ認証情報を使用するのではなく、OTP を求めるポータルおよびゲートウェイをアプリ単位で設定する必要があります。

また、認証のオーバーライドを設定することで、ユーザーに OTP を求める頻度を減らすこともできます。これにより、ポータルおよびゲートウェイが安全に暗号化された Cookie を生成・承認し、一定時間の間、ユーザーを認証することができるようになります。ポータルおよび/またはゲートウェイは、Cookie の有効期限が切れたことによってユーザーが OTP を提供しなければならない回数が減るまで、新しい OTP を必要としません。

STEP 1 | バックエンドの RADIUS サービスが OTP 用のトークンを生成するよう設定し、さらにユーザーが必要なデバイス（ハードウェア トークンなど）を持っている状態にした後で、ファイアウォールとやり取りを行う RADIUS サーバーをセットアップします。

具体的な手順は、RADIUS サーバーのドキュメントを参照してください。ほとんどの場合、RADIUS サーバーに認証エージェントおよびクライアント設定をセットアップし、ファイアウォールと RADIUS サーバー間の通信を有効にする必要があります。さらに、ファイア

ウォールと RADIUS サーバー間のセッションを暗号化する際に使用する共有シークレットを定義しなければなりません。

STEP 2 | ゲートウェイおよび/またはポータルをホストする各ファイアウォール上で、RADIUS サーバー プロファイルを作成します。（小規模なデプロイ環境の場合、単一のファイアウォールがポータルおよびゲートウェイをホストできます）

1. **Device (デバイス)** > **Server Profiles (サーバープロファイル)** > **Syslog** の順に選択します。
2. 新しいプロファイルを **Add**（追加）します。
3. この RADIUS プロファイルの **Profile Name**（プロファイル名前）を入力します。
4. **Servers**（サーバー）エリアで RADIUS インスタンスを **Add**（追加）し、以下を入力します：
   - この RADIUS サーバーを識別できる分かりやすい**Name**（名前）。
   - **RADIUS Server**（**RADIUS** サーバー）の IP アドレス。
   - ファイアウォールと RADIUS サーバー間のセッションを暗号化する共有**Secret**（シークレット）。
   - RADIUS サーバーが認証要求をリッスンする **Port**（ポート）番号（デフォルトは 1812）。
5. **OK** をクリックしてプロファイルを保存します。

STEP 3 | 認証プロファイルを作成します。

1. **Device** > **Authentication Profile**(デバイス > 認証プロファル) の順に選択し、新しいプロファイルを**Add**(追加) します。
2. プロファイルの**Name**（名前）を入力します。この名前にはスペースを含められません。
3. 認証サービス **Type**（タイプ）として **RADIUS** を選択します。
4. **Server Profile**（サーバー プロファイル）で、RADIUS サーバーへのアクセス用に作成したプロファイルを選択します。
5. **User Domain**（ユーザー ドメイン）名を入力します。ファイアウォールでは、認証しているユーザーと許可リストのエントリの照合、および User-ID のグループ マッピングにこの値を使用します。
6. **Username Modifier**（ユーザー名修飾子）を選択して、RADIUS サーバーが想定するユーザー名/ドメインのフォーマットを変更します。
7. **OK** をクリックして認証プロファイルを保存します。

STEP 4 | 認証プロファイルを GlobalProtect ゲートウェイ/ポータルに割り当てます。

ポータルおよびゲートウェイ用に、クライアント認証設定を複数用意できます。各クライアント認証設定に対し、特定の OS のエンドポイントに適用する認証プロファイルを指定できます。

このステップでは、ポータルまたはゲートウェイの設定に認証プロファイルを追加する方法について説明します。これらのコンポーネントをセットアップする方法についての詳細は、GlobalProtect ポータルおよび GlobalProtect ゲートウェイを参照してください。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）または **Gateways**（ゲートウェイ）を選択します
2. 既存のポータルまたはゲートウェイ設定を選択するか、新しく **Add**（追加）します。新しいポータルまたはゲートウェイを追加する場合は、名前、場所、およびネットワークパラメーターを指定します。
3. **Authentication**（認証）タブで**SSL/TLS service Profile**（**SSL/TLS** サービス プロファイル）を選択するか、新しいプロファイルを **Add**（追加）します。
4. 新しい **Client Authentication**（クライアント認証）を **Add**（追加）し、以下の設定を構成します。
   - このクライアント認証設定の **Name**（名前）。
   - この設定を適用するエンドポイントの **OS** を選択します。
   - 認証プロファイルの作成で作成した **Authentication Profile**（認証プロファイル）。
   - （任意）カスタム**Username Label**（ユーザー名ラベル）。
   - （任意）カスタム**Pasword Label**（パスワード ラベル）。
   - （任意）カスタム **Authentication Message**（認証メッセージ）。
5. **OK** をクリックして設定を保存します。

STEP 5 | （任意）ユーザーログインする度に、ユーザー名およびパスワード、またはパスワードのみを求めるよう、ポータルまたはゲートウェイを設定します。OTP を使用する 2 要素認証の場合、ユーザーはログインする度にダイナミックパスワードを入力しなければならないため、パスワードは保存できません。

このステップでは、ポータルのエージェント設定でパスワードを設定する方法を説明します。詳細については、GlobalProtect アプリのカスタマイズを参照してください。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） の順に選択し、既存のポータルの設定を選択します。
2. GlobalProtect ポータル設定ダイアログで **Authentication**（認証）を選択します。
3. 既存のエージェント設定を選択するか、新しく **Add**（追加）します。
4. **Authentication**（認証）タブで、**Save User Credentials**（ユーザー認証情報の保存）を**Save Username Only**（ユーザー名のみ保存）または **No**（保存しない）に設定します。この設定により、次のステップで選択する各コンポーネント用に、GlobalProtect がダイナミックパスワードをユーザーに求めるようにすることができます。
5. **OK** を 2 回クリックして設定を保存します。

STEP 6 | OTP のようなダイナミックパスワードを求める GlobalProtect コンポーネント（ポータルおよびゲートウェイの種類）を選択します。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） の順に選択し、既存のポータルの設定を選択します。
2. GlobalProtect ポータル設定ダイアログで **Authentication**（認証）を選択します。
3. 既存のエージェント設定を選択するか、新しく **Add**（追加）します。
4. **Authentication**（認証）タブで、**Components that Require Dynamic Passwords (Two-Factor Authentication)**（ダイナミックパスワードが必要なコンポーネント（**2** 要素認証））を選択します。選択した種類のポータルおよび/またはゲートウェイで OTP の入力が求められるようになります。

   > *SAML* 認証を使用するすべてのコンポーネントに対して、***Components that Require Dynamic Passwords (Two-Factor Authentication)***（ダイナミックパスワードが必要なコンポーネント（**2** 要素認証））オプションを選択しないでください。

5. **OK** を 2 回クリックして設定を保存します。

STEP 7 | シングル サインオン（SSO）が有効になっているのであれば、無効にしてください。エージェント設定は RADIUS を認証サービスとして指定するため、Kerberos SSO はサポートされていません。

このステップでは、SSO を無効化する方法を説明します。詳細については、GlobalProtect エージェント設定の定義を参照してください。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） の順に選択し、既存のポータルの設定を選択します。
2. GlobalProtect ポータル設定ダイアログで **Authentication**（認証）を選択します。
3. 既存のエージェント設定を選択するか、新しく **Add**（追加）します。
4. **App**（アプリ）タブで、**Use Single Sign-On**（シングル サインオンの使用）を **No**（いいえ）に設定します。
5. **OK** を 2 回クリックして設定を保存します。

STEP 8 | （任意）ユーザーが認証情報を入力する回数を減らすには、認証のオーバーライドを設定します。

デフォルトでは、ポータルまたはゲートウェイは認証プロファイルと任意で証明書プロファイルを使用してユーザーを認証します。認証のオーバーライドを行うと、ポータルまたはゲートウェイは、エンドポイントにデプロイ済みの暗号化された Cookie を使用してユーザーを認証するようになります。Cookie が有効な間、ユーザーは通常の認証情報や OTP を入力す

ることなくログインすることができます。詳細は、ポータルまたはゲートウェイでの Cookie 認証を参照してください。

Cookie の有効期限が切れていないエンドポイントへのアクセスを即刻ブロックする必要がある場合（たとえば、エンドポイントを紛失したり、盗まれたりした場合）、そのエンドポイントをブロックリストに追加することでエンドポイントのアクセスをブロックすることができます。

詳細は、GlobalProtect ポータルおよび GlobalProtect ゲートウェイを参照してください。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）または **Gateways**（ゲートウェイ）を選択します
2. 既存のポータルまたはゲートウェイ設定を選択するか、新しく **Add**（追加）します。
3. ポータルまたはゲートウェイを設定するかどうかに応じて、次のいずれかを選択します。
   - **GlobalProtect** ポータル設定—GlobalProtect ポータル設定ダイアログで、**Agent**（エージェント） > ***<agent-config>*** > **Authentication**（認証）を選択します。
   - **GlobalProtect** ゲートウェイ設定—GlobalProtect ゲートウェイ設定ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定） > ***<client-setting>*** > **Authentication Override**（認証のオーバーライド）を選択します。
4. 以下の**Authentication Override**（認証のオーバーライド）を設定します：
   - 認証のオーバーライドの **Name**（名前）。
   - **Generate cookie for authentication override**（認証オーバーライド用 **Cookie** を生成） — ポータルまたはゲートウェイで暗号化されたエンドポイント固有の Cookie を生成できるようにします。ユーザーの認証が成功すると、ポータルまたはゲートウェイによってエンドポイントに対して認証用 Cookie が発行されます。
   - **Accept cookie for authentication override**（**Cookie** による認証オーバーライドを許可） — 暗号化された有効な Cookie を使用してポータルまたはゲートウェイでユーザーを認証できるようになります。有効な Cookie がエンドポイントで提示された場

合、ポータルまたはゲートウェイではそれぞれが暗号化された Cookie であることを確認し、復号化を行ってユーザーを認証します。

GlobalProtect アプリケーションが関連する認証用 *Cookie* をユーザーのエンドポイントにマッチさせて取得するためには、接続するユーザーのユーザー名を知る必要があります。*Cookie* を取得した後、アプリはそれをポータルあるいはゲートウェイに送信してユーザー認証を行います。

(Windows のみ) ポータルのエージェント設定でシングル サインオンを使用するオプションを***Yes (***はい*)* に設定 *(SSO* を有効化*)* すると *(****Network (***ネットワーク*) > GlobalProtectPortals > (***ポータル*) > <portal-config> Agent (***エージェント*) > <agent-config>. > App (***アプリ*))***、*GlobalProtect* アプリケーションが *Windows* のユーザー名を使用してユーザーのローカル認証用 *Cookie* を取得するようになります。***Use Single Sign-On (***シングル サインオンを使用*)* するオプションを ***No (***いいえ*)* に設定 *(SSO* を無効化*)* する場合、アプリがユーザーの認証用 *Cookie* を取得できるようにするために、*GlobalProtect* アプリケーションがユーザー認証情報を保存できるようにする必要があります。***Save User Credentials (***ユーザー認証情報の保存*)* オプションを ***Yes (***はい*)* に設定するとユーザー名およびパスワードの両方が、***Save Username Only (***ユーザー名のみ保存*)* に設定するとユーザー名だけが保存されます。

(macOS のみ) macOS エンドポイントはシングル サインオンをサポートしていないため、ユーザーの認証 *cookie* を取得できるようにするには、*GlobalProtect* アプリケーションが ***Save User Credentials (***ユーザー認証情報を保存*)* を有効にする必要があります。***Save User Credentials (***ユーザー認証情報の保存*)* オプションを ***Yes (***はい*)* に設定するとユーザー名およびパスワードの両方が、***Save Username Only (***ユーザー名のみ保存*)* に設定するとユーザー名だけが保存されます。

- **Cookie Lifetime**（**Cookie** の有効期間） — Cookie が有効な時間数、日数、または週数を指定します。一般的な有効期間は、（機密性の高い情報を保護する）ゲートウェイの場合は 24 時間、ポータルの場合は 15 日間です。範囲は、時間が 1～72、週が 1～52、日数が 1～365 です。ポータルまたはゲートウェイのいずれか（最初に切れた方）で Cookie が失効すると、そのポータルまたはゲートウェイではユーザーが認証を求められ、その後新しい Cookie が暗号化されてエンドポイントに送信されます。

- **Certificate to Encrypt/Decrypt Cookie**（**Cookie** 暗号化/復号化時の証明書） — Cookie を暗号化および複合化するために使用する RSA 証明書を指定します。ポータルおよびゲートウェイで同じ証明書を使う必要があります。

  RSA 証明書がネットワークでサポートされている最も強固なダイジェスト アルゴリズムを使うように設定することが推奨されます。

  ポータルおよびゲートウェイは RSA 暗号化パディング スキーム PKCS#1 V1.5 を使用して Cookie を生成（証明書の公開鍵を使用）し、Cookie を復号化します（証明書の秘密鍵を使用）。

5. **OK** を 2 回クリックして設定を保存します。

STEP 9 | 設定を **Commit**（コミット）します。

STEP 10 | 設定を確認します。

GlobalProtect アプリを実行しているエンドポイントから、OTP 認証を有効にしたゲートウェイまたはポータルへの接続を試みます。以下のようなプロンプトが表示されます。

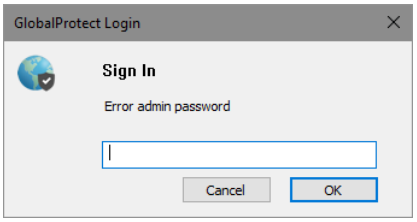


図 **1 : OTP** ポップアップ プロンプト

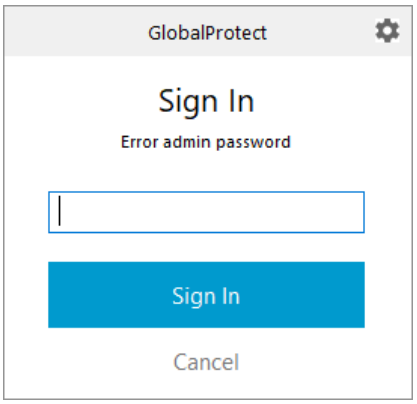


図 **2 : GlobalProtect** ステータス パネルの **OTP** プロンプト

スマート カードを使用した 2 要素認証の有効化

エンド ユーザーがスマート カードまたは共通アクセス カード（CAC）を使用して認証できるようにするには、CAC またはスマート カードに含まれる証明書を発行したルート CA 証明書をポータルおよびゲートウェイにインポートする必要があります。次に、そのルート CA を含む証明書プロファイルを作成してポータル/ゲートウェイ設定に適用し、認証プロセスでのスマート カードの使用を有効にします。

STEP 1 | スマート カード インフラストラクチャをセットアップします。

この手順は、エンド ユーザーにスマート カードおよびスマート カード リーダーをデプロイ済みであることを前提としています。

具体的な手順は、認証プロバイダ ソフトウェアのドキュメントを参照してください。

ほとんどの場合、スマート カード インフラストラクチャのセットアップでは、参加するエンド ユーザーおよびサーバー（このユースケースでは GlobalProtect ポータルおよびゲートウェイ）に対して証明書を生成することになります。

STEP 2 | エンド ユーザーのスマート カードに含まれるクライアント証明書を発行したルート CA 証明書をインポートします。

証明書が管理システムからアクセス可能なことを確認してから、以下の手順を実行します。

1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから、**Import**（インポート）をクリックします。
2. **Certificate Name**（証明書名）を入力します。
3. CA から受信した **Certificate File**[証明書ファイル] のパスと名前を入力するか、**Browse**[参照] してファイルを検索します。
4. **File Format** [ファイル フォーマット]ドロップダウン リストから **Base64 Encoded Certificate (PEM)** [Base64 エンコード済み証明書（PEM）]を選択してから、**OK** をクリックして証明書をインポートします。

STEP 3 | CAC またはスマート カード認証を使用する各ポータル/ゲートウェイで証明書プロファイルを作成します。

CRL と *OCSP* のどちらを使用するかなど、その他の証明書プロファイル フィールドの詳細は、オンライン ヘルプを参照してください。

1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificate Profile (証明書プロファイル)** を選択します。
2. 既存の証明書プロファイルを選択するか、新しく **Add**（追加）します。
3. 証明書プロファイルの **Name**（名前）を入力します。
4. **Username Field**（ユーザー名欄）で、User-ID の IP アドレスを照合するために PAN-OS が使用する証明書を選択します。たとえば、共通名を使用する場合は **Subject**（サブジェクト） を、電子メール アドレスを使用する場合は **Subject Alt:**（サブジェクト代替名:）を選択します。**(追加)**で電子メールアドレスを使うか、**(サブジェクト代替名: Principal Name**(プリンシパル名)でプリンシパル名を使います。
5. **CA Certificates (証明書)** エリアで、**Add (追加)** をクリックし、ステップ 2 でインポートした信頼されたルート CA 証明書を証明書プロファイルにインポートします。プロンプトが表示されたら、**Authorization Code**（認証コード）を選択して、**OK** をクリックします。
6. **OK** をクリックして、証明書プロファイルを保存します。

STEP 4 | 証明書プロファイルをポータルまたはゲートウェイに割り当てます。このステップでは、ポータルまたはゲートウェイの設定に証明書プロファイルを追加する方法について説明します。これらのコンポーネントをセットアップする方法についての詳細は、GlobalProtect ポータルおよび GlobalProtect ゲートウェイを参照してください。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）または **Gateways**（ゲートウェイ）を選択します
2. 既存のポータルまたはゲートウェイ設定を選択するか、新しく **Add**（追加）します。
3. GlobalProtect ゲートウェイ設定ダイアログで、**Authentication**（認証）を選択します。
4. 作成した **Certificate Profile**（証明書プロファイル）を選択します。
5. **OK** をクリックして設定を保存します。

STEP 5 | 設定を **Commit**（コミット）します。

STEP 6 | 設定を確認します。

GlobalProtect アプリを実行しているエンドポイントから、スマート カード対応の認証をセットアップしたゲートウェイまたはポータルへの接続を試みます。プロンプトが表示されたら、スマート カードを挿入して正常に GlobalProtect に対して認証できることを確認します。

ソフトウェアトークンアプリケーションを使用して2要素認証を有効にする

ご所属の組織が RSA SecurID などのソフトウェアトークン（ソフトトークン）アプリケーションを使用して二要素認証を実装する場合、ユーザーは最初にソフトウェア トークン アプリケーションを開き、PIN を入力してパスコードを取得し、**Password**（パスワード）フィールド内のGlobalProtect アプリケーションにパスコードを入力することを要求されます。この二段階プロセスにより、ログイン プロセスが複雑になります。

ログインプロセスを簡略化してユーザーエクスペリエンスを向上させる目的で、GlobalProtect はシームレスなソフト トークン認証を提供します。ユーザーが RSA PIN を GlobalProtect の **Password**（パスワード）フィールドを入力すると、 GlobalProtect は RSA から該当のパスコードを取得し、ユーザーが RSA アプリケーションを開くための別段の手順を実行することなく、接続を処理します。

この機能は3つすべての RSA モードでサポートされています。PinPad Style (トークンコードを含む PIN 統合型)、Fob Style (トークン コードに PIN が続く) および Pinless モード。PinPad と Fob Style の場合、ユーザーは **Password**（パスワード） フィールドに PIN を入力し、GlobalProtect は該当のパスコードを取得します。Pinless モードでは、Password（パスワード）フィールドはグレー色で表示され、ユーザーは自分のユーザー名を入力します。

この機能は *Windows* デバイスでサポートされており、 *GlobalProtect™* アプリケーション*5.1*以降に対応します。

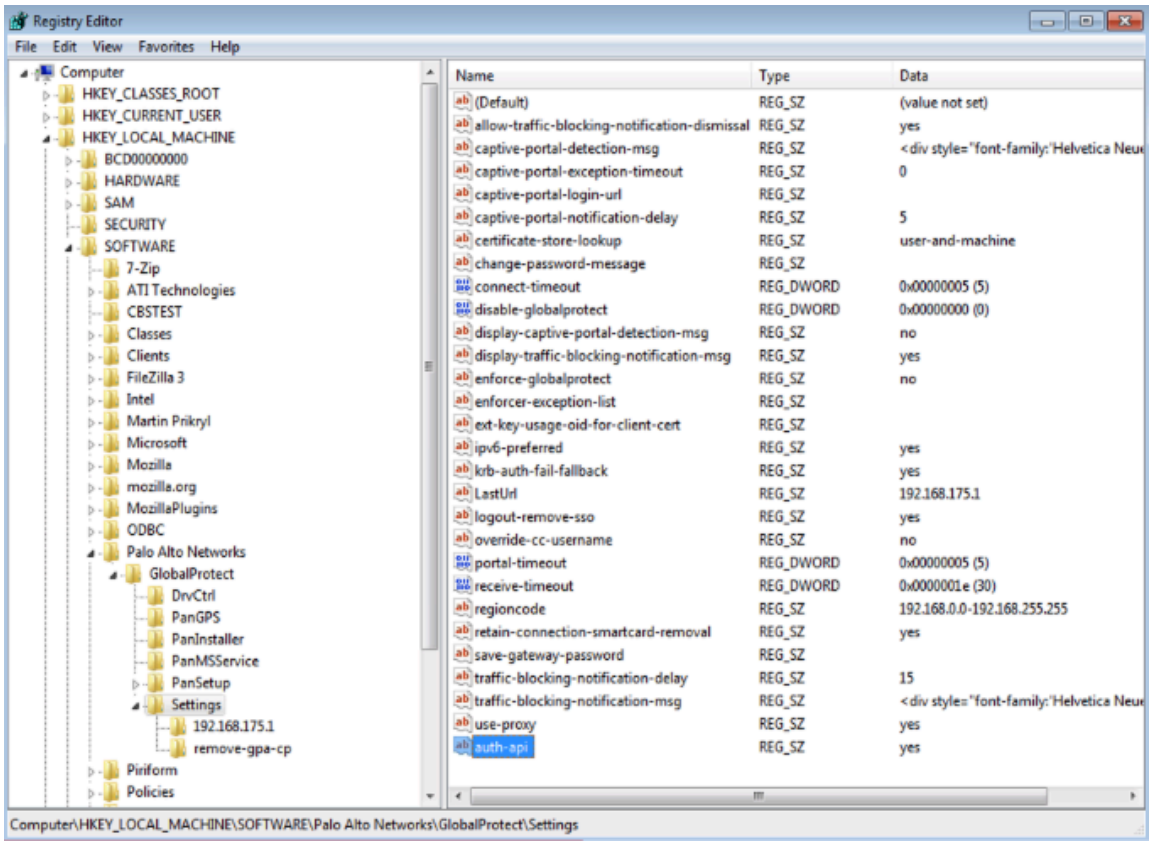
STEP 1 | クライアントの Windows デバイスのレジストリ キーを変更して、シームレスなソフト トークン認証を有効にします。

シームレスなソフト トークン認証を有効にするには、クライアントの Windows デバイスで Windows レジストリを変更する必要があります。GlobalProtect は、GlobalProtect アプリケーションの初期化時にこのレジストリ エントリを1回だけ取得します。

1. Windows Registry Editor（Windows レジストリ エディタ） を開き、**HKEY_LOCAL_MACHINE** > **SOFTWARE** > **PALO Also Networks** > **GlobalProtect** > **Settings**（設定）を選択します。
2. **auth-api** 値を **yes** に変更します。

auth-api はクライアントのマシン内で ***yes*** に設定されるため、*RSA* ベースの認証を含むポータルとゲートウェイを設定することが推奨されます。*GlobalProtect* はパスコードの取得を試行するため、他の認証プロファイルはサポートされていません。

ポータルとゲートウェイは *RSA* 認証を使用するため、ゲートウェイで *cookie* ベースの認証を有効にすることをお勧めします。*GlobalProtect* がゲートウェイのパスコードの取得を試行するときに、ポータル用に取得されたトークンが有効なままであると、パスコードがすでに使用されていたために認証が失敗する場合があります。したがって、ポータルで *Authentication Override*（認証オーバーライド）*cookie* を生成し、ゲートウェイで *cookie* を承認することをお勧めします。

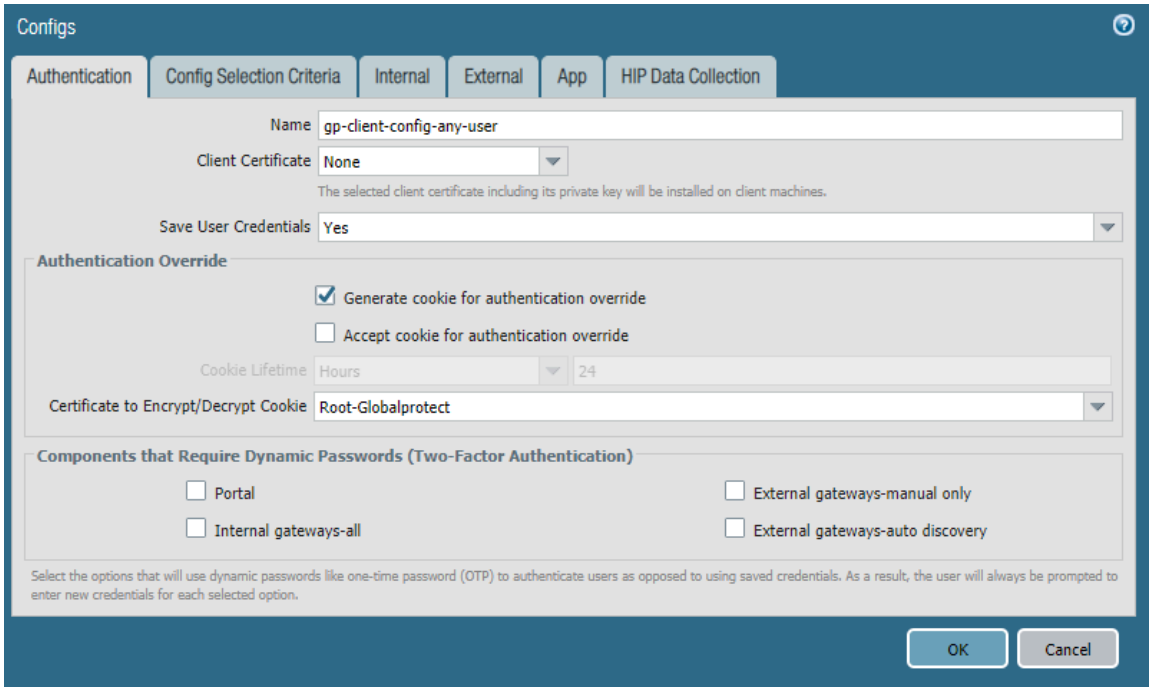


STEP 2 | RSA ベースの認証を使用してポータルとゲートウェイを設定します。

STEP 3 | GlobalProtect ポータルで cookieベースの認証を有効にします。

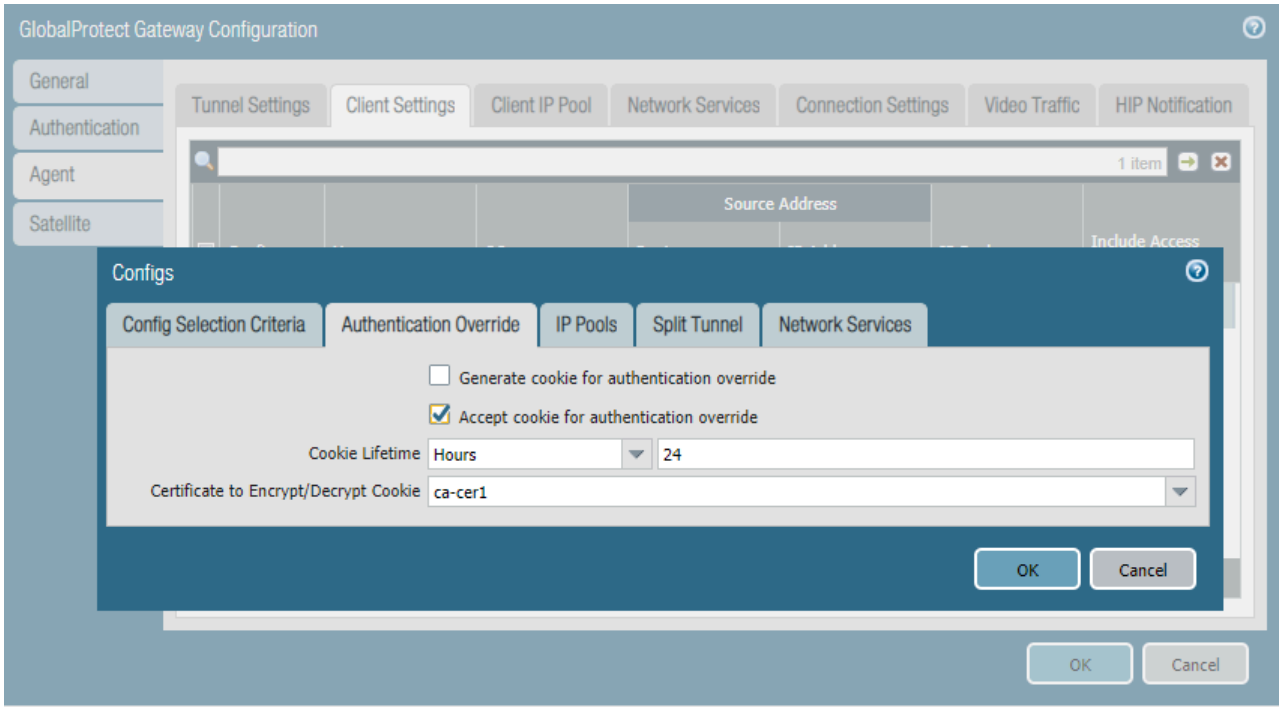
GlobalProtect を指定して既存の認証をオーバーライドすると、GlobalProtect は既存のパスコードを新しく作成したパスコードで上書きできます。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > ***<portal-config>***の順に選択し、**Agent**（エージェント）タブを選択します。
2. Agent（エージェント）設定を **Add**（追加）するか、既存の設定を選択します。
3. **Generate cookie for authentication override**（**cookie**を生成して認証をオーバーライド）を選択します。



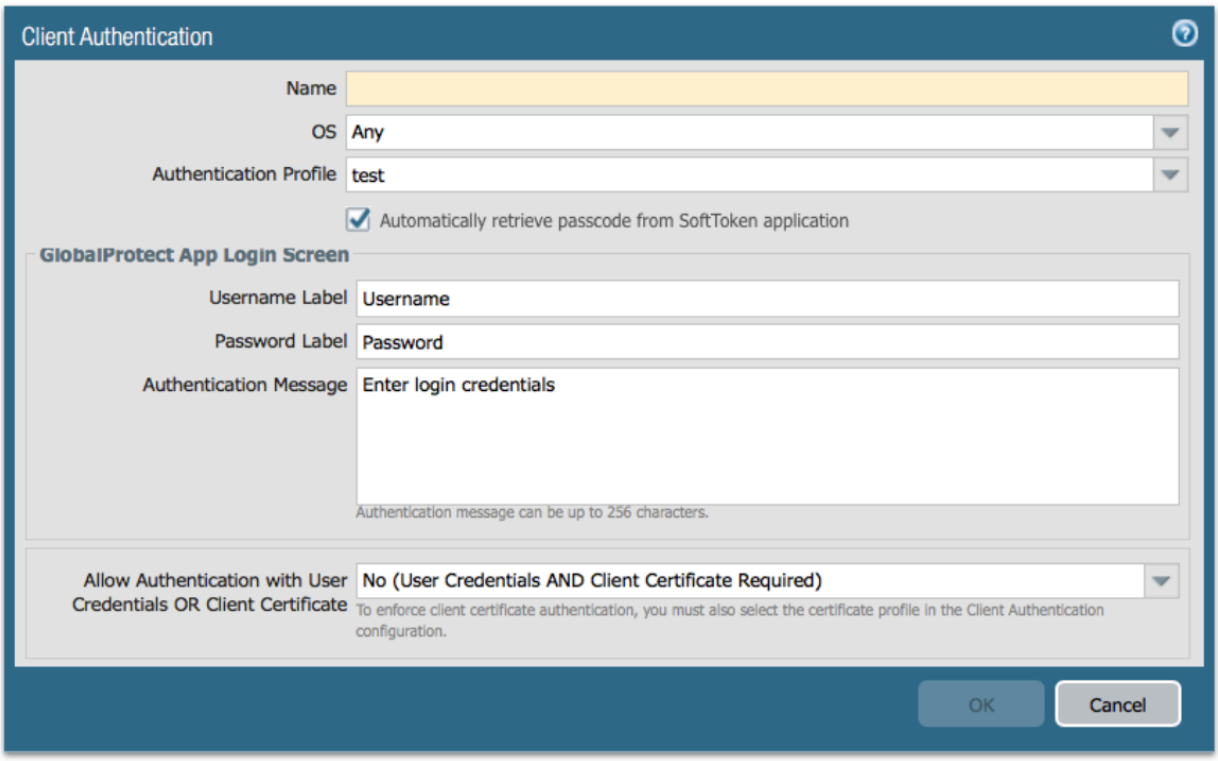
STEP 4 | GlobalProtect ゲートウェイが cookie による認証オーバーライドを許可できるようにします。

1. **Network**（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ） > ***<gateway>*** の順に選択し、**Agent**（エージェント）タブを選択します。
2. **Client Settings**（クライアント設定）を選択してから、GlobalProtect クライアント設定を選択するか新しい設定を追加します。
3. **Authentication Override**（認証オーバーライド）を選択してから、**Accept cookie for authentication override**（認証オーバーライド用の **cookie** を承認）を選択します。



STEP 5 | **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > ***<portal-config>***の順に選択し、**Authentication**（認証）タブを選択します。

STEP 6 | 新しいクライアント認証プロファイルを **Add**（追加）するか、既存のプロファイルを選択します。 次に、 **Automatically retrieve passcode from SoftToken application**（**SoftToken**アプリケーションからパスコードを自動的に取得）を選択します。



strongSwan Ubuntu および CentOS エンドポイントの認証のセットアップ

GlobalProtect アクセスを strongSwan Ubuntu および CentOS エンドポイントに拡張するには、これらのエンドポイントの認証をセットアップします。

Ubuntu Linux および *CentOS* の *strongSwan* をサポートする最小 *GlobalProtect* リリース バージョンを確認するには、「GlobalProtect でサポートされている OS バージョン」を参照してください。

GlobalProtect ゲートウェイに接続するには、ユーザーは認証が終わっている必要があります。以下のワークフローは、 strongSwan エンドポイントの認証を有効化する方法を示します。strongSwan についての詳細な説明は、strongSwan wiki を参照してください。

- 証明書プロファイルを使用した認証の有効化
- 認証プロファイルを使用した認証の有効化
- 2 要素認証を使用した認証の有効化

証明書プロファイルを使用した認証の有効化

次のワークフローは、証明書プロファイルを使用し strongSwan クライアントを認証可能にする方法を示します。

STEP 1 | GlobalProtect ゲートウェイ用 IPsec トンネルを strongSwan クライアントとの接続に設定します。

1. **Network** > **GlobalProtect** > **Gateways** (ネットワーク > GlobalProtect > ゲートウェイ)を選択します。
2. 既存のゲートウェイを選択するか、新しく **Add**（追加）します。
3. GlobalProtect ゲートウェイ設定ダイアログの **Authentication**（認証）タブで、使用する **Certificate Profile**（証明書プロファイル）を選択します。
4. **Agent**（エージェント） > **Tunnel Settings**（トンネル設定） を選択して **Tunnel Mode**（トンネル モード）を有効にして、トンネルを設定する以下の設定を指定します。
   - このインターフェイスを有効にする **Enable X-Auth Support**（**X-Auth** サポートを有効にする）には、このチェック ボックスをオンにします。
   - **Group Name**（グループ名）と **Group Password**（グループパスワード）がすでに設定済みであれば、それらを削除します。
   - **OK** をクリックして設定を保存します。

STEP 2 | IPsec トンネル設定ファイル（**ipsec.conf**）の conn %default セクションのデフォルト接続設定が strongSwan クライアント用に正しく定義されています。

ipsec.conf ファイルは通常 /etc フォルダにあります。

この手順の設定は以下のリリース用にテストされ確認されます。

- *Ubuntu 14.0.4 with strongSwan 5.1.2 and CentOS 6.5 with strongSwan 5.1.3 for PAN-OS 6.1.*
- *Ubuntu 14.0.4 with strongSwan 5.2.1 for PAN-OS 7.0.*

この手順の設定は異なるバージョンの *strongSwan* をお使いの場合は参考にお使いいただけます。詳細は、strongSwan wiki を参照してください。

ipsec.conf ファイル内の **conn %default** セクションをこれらの推奨設定に変更します。

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

STEP 3 | strongSwan client\xd5 s IPsec 設定ファイル（**ipsec.conf**）と IPsec ファイルを（**ipsec.secrets**）変更して推奨設定を使用します。

ipsec.secrets ファイルは通常 /etc フォルダにあります。

strongSwan クライアントユーザー名を証明書の共通名として使用します。

ipsec.conf ファイル内の以下の項目をこれらの推奨設定に変更します。

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

```
auto=add
```

`ipsec.conf` ファイル内の以下の項目をこれらの推奨設定に変更します。

```
:RSA
<private key file> “<passphrase if used>”
```

STEP 4 | strongSwan IPsec サービスを開始し、strongSwan クライアントが GlobalProtect ゲートウェイに対する認証に使用する IPsec トンネルに接続します。

`config <name>` 変数をトンネル設定の名前に使用します。

- Ubuntu:

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

- CentOS:

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

STEP 5 | トンネルが正しくセットアップされていて VPN 接続が strongSwan クライアントと GlobalProtect の両方に確立されていることを確認します。

1. 特定の接続の詳細な状態情報（接続名を指定）や strongSwan クライアントからのすべての接続の状態情報を確認します。
   - Ubuntu:

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

   - CentOS:

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

2. **Network** > **GlobalProtect** > **Gateways**（ネットワーク > GlobalProtect > ゲートウェイ）を選択します。**Info**（情報）カラムで、strongSwan クライアントへの接続用に設定されたゲートウェイの **Remote Users**（リモートユーザー）を選択します。strongSwan クライアントは **Current Users**（現在のユーザー）の下にリスト表示されなければなりません。

認証プロファイルを使用した認証の有効化

次のワークフローは、認証プロファイルを使用し strongSwan クライアントを認証可能にする方法を示します。認証プロファイルは、strongSwan クライアントを認証認する時に使用するサーバー プロファイルを指定します。

STEP 1 | GlobalProtect ゲートウェイ用 IPsec トンネルを strongSwan クライアントとの接続にセットアップします。

1. **Network** > **GlobalProtect** > **Gateways** (ネットワーク > GlobalProtect > ゲートウェイ)を選択します。
2. 既存のゲートウェイを選択するか、新しく **Add**（追加）します。
3. GlobalProtect ゲートウェイ設定ダイアログの **Authentication**（認証）タブで、使用する **Authentication Profile**（認証プロファイル）を選択します。
4. **Agent**（エージェント） > **Tunnel Settings**（トンネル設定） を選択して **Tunnel Mode**（トンネル モード）を有効にして、トンネルを設定する以下の設定を指定します。
   - このインターフェイスを有効にする **Enable X-Auth Support**（**X-Auth** サポートを有効にする）には、このチェック ボックスをオンにします。
   - **Group Name**（グループ名）と **Group Password**（グループパスワード）がまだ設定されていなければ入力します。
   - **OK** をクリックして、これらの設定を保存します。

STEP 2 | IPsec トンネル設定ファイル（`ipsec.conf`）の conn %default セクションのデフォルト接続設定が strongSwan クライアント用に正しく定義されています。

`ipsec.conf` ファイルは通常 /etc フォルダにあります。

この手順の設定は以下のリリース用にテストされ確認されます。

- *Ubuntu 14.0.4 with strongSwan 5.1.2 and CentOS 6.5 with strongSwan 5.1.3 for PAN-OS 6.1.*
- *Ubuntu 14.0.4 with strongSwan 5.2.1 for PAN-OS 7.0.*

この手順の設定は異なるバージョンの *strongSwan* をお使いの場合は参考にお使いいただけます。詳細は、strongSwan wiki を参照してください。

`ipsec.conf` ファイル内の `conn %default` セクションで、これらの推奨設定にします。

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

STEP 3 | strongSwan client\xd5 s IPsec 設定ファイル（**ipsec.conf**）と IPsec ファイルを（**ipsec.secrets**）変更して推奨設定を使用します。

ipsec.secrets ファイルは通常 /etc フォルダにあります。

strongSwan クライアントユーザー名を証明書の共通名として使用します。

ipsec.conf ファイル内で以下の推奨設定を設定します。

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

ipsec.secrets ファイル内で以下の推奨設定を設定します。

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

STEP 4 | strongSwan IPsec サービスを開始し、strongSwan クライアントが GlobalProtect ゲートウェイに対する認証に使用する IPsec トンネルに接続します。

- Ubuntu:

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

- CentOS:

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


STEP 5 | トンネルが正しくセットアップされていて VPN 接続が strongSwan クライアントと GlobalProtect の両方に確立されていることを確認します。

1. 特定の接続の詳細な状態情報（接続名を指定）や strongSwan クライアントからのすべての接続の状態情報を確認します。

   - Ubuntu:

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

   - CentOS:

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

2. **Network** > **GlobalProtect** > **Gateways** (ネットワーク > GlobalProtect > ゲートウェイ)を選択します。**Info**（情報）カラムで、strongSwan クライアントへの接続用に設定されたゲートウェイの **Remote Users**（リモートユーザー）を選択します。strongSwan クライアントは **Current Users**（現在のユーザー）の下にリスト表示されなければなりません。

2 要素認証を使用した認証の有効化

2 要素認証では、GlobalProtect ゲートウェイに接続するために、strongSwan クライアントは証明書プロファイルと認証プロファイルの両方を使用した認証に成功する必要があります。次のワークフローは、2 要素認証を使用し strongSwan クライアントを認証可能にする方法を示します。

STEP 1 | GlobalProtect ゲートウェイ用 IPsec トンネルを strongSwan クライアントとの接続にセットアップします。

1. **Network** > **GlobalProtect** > **Gateways** (ネットワーク > GlobalProtect > ゲートウェイ)を選択します。
2. 既存のゲートウェイを選択するか、新しく **Add**（追加）します。
3. GlobalProtect ゲートウェイ設定ダイアログの **Authentication**（認証）タブで、使用する **Certificate Profile**（証明書プロファイル） と **Authentication Profile**（認証プロファイル）を選択します。
4. **Agent**（エージェント） > **Tunnel Settings**（トンネル設定） を選択して **Tunnel Mode**（トンネル モード）を有効にして、トンネルを設定する以下の設定を指定します。

   - このインターフェイスを有効にする **Enable X-Auth Support**（**X-Auth** サポートを有効にする）には、このチェック ボックスをオンにします。
   - **Group Name**（グループ名）と **Group Password**（グループパスワード）がすでに設定済みであれば、それらを削除します。
   - **OK** をクリックして、これらの設定を保存します。

STEP 2 | IPsec トンネル設定ファイル（**ipsec.conf**）の conn %default セクションのデフォルト接続設定が strongSwan クライアント用に正しく定義されています。

ipsec.conf ファイルは通常 **/etc** フォルダにあります。

この手順の設定は以下のリリース用にテストされ確認されます。

- *Ubuntu 14.0.4 with strongSwan 5.1.2 and CentOS 6.5 with strongSwan 5.1.3 for PAN-OS 6.1.*
- *Ubuntu 14.0.4 with strongSwan 5.2.1 for PAN-OS 7.0.*

異なるバージョンの *strongSwan* をお使いの場合、この手順の設定を参考にお使いいただけます。詳細は、strongSwan wiki を参照してください。

ipsec.conf ファイル内で以下の推奨設定を設定します。

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

STEP 3 | strongSwan client\xd5 s IPsec 設定ファイル（**ipsec.conf**）と IPsec ファイルを（**ipsec.secrets**）変更して推奨設定を使用します。

ipsec.secrets ファイルは通常 /etc フォルダにあります。

strongSwan クライアントユーザー名を証明書の共通名として使用します。

ipsec.conf ファイル内で以下の推奨設定を設定します。

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

```
auto=add
```

ipsec.secrets ファイル内で以下の推奨設定を設定します。

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

STEP 4 | strongSwan IPsec サービスを開始し、strongSwan クライアントが GlobalProtect ゲートウェイに対する認証に使用する IPsec トンネルに接続します。

- Ubuntu:

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

- CentOS:

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

STEP 5 | トンネルが正しくセットアップされていて VPN 接続が strongSwan クライアントと GlobalProtect の両方に確立されていることを確認します。

1. 特定の接続の詳細な状態情報（接続名を指定）や strongSwan クライアントからのすべての接続の状態情報を確認します。
   - Ubuntu:

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

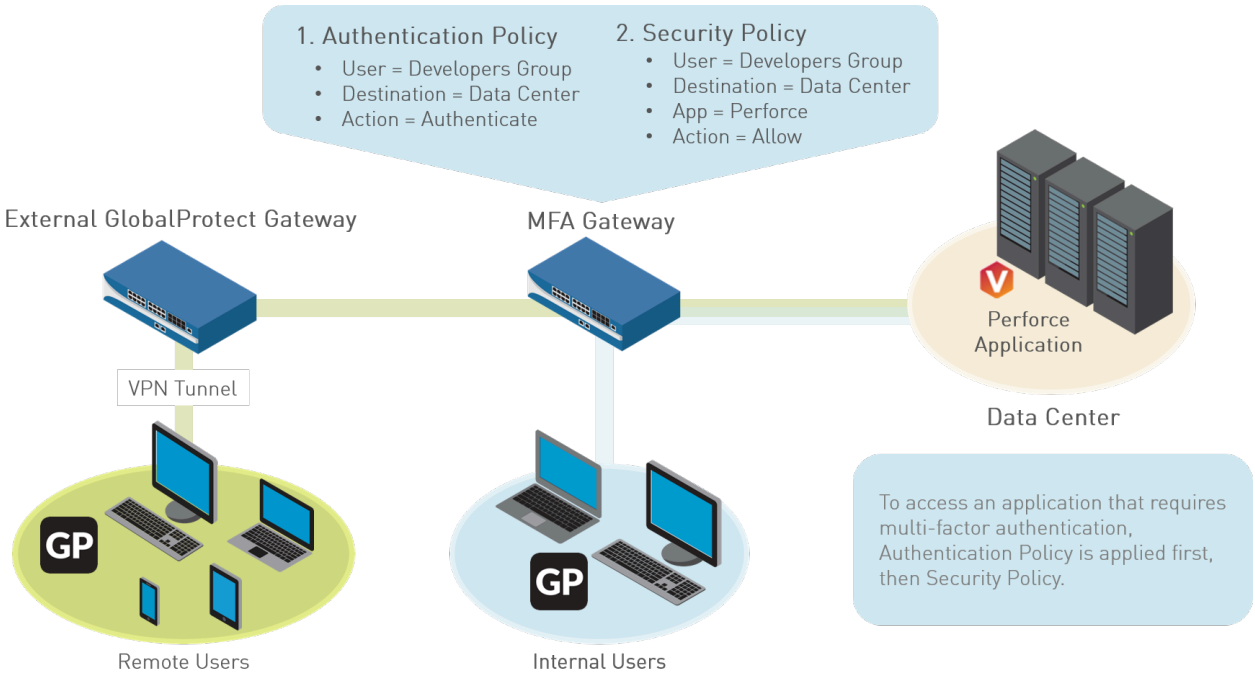
   - CentOS:

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

2. **Network** > **GlobalProtect** > **Gateways** (ネットワーク > GlobalProtect > ゲートウェイ)を選択します。**Info**（情報）カラムで、strongSwan クライアントへの接続用に設定されたゲートウェイの **Remote Users**（リモートユーザー）を選択します。strongSwan クライアントは **Current Users**（現在のユーザー）の下にリスト表示されなければなりません。

多要素認証の通知をスムーズに行うための GlobalProtect の設定

重要なアプリケーションを保護して、攻撃者が盗んだ認証情報を使用してネットワークを縦横無尽に動き回るのを阻止するために、ポリシーベースの多要素認証（MFA）を設定できます。これにより、各ユーザーはさまざまなタイプ（要素）の複数の認証チャレンジに対応してからでないと機密性の高いサービスやアプリケーションにアクセスできません。



ユーザー セッションが認証ポリシーに一致する場合、アプリケーションまたはサービスのタイプによって、認証チャレンジに関する通知のユーザー体験が決まります。

- （Windows または macOS エンドポイントのみ）非ブラウザベースのアプリケーション — Windows または macOS エンドポイントの非 HTTP アプリケーション（Perforce など）で MFA 通知をスムーズに行うには、GlobalProtect アプリが必要です。セッションが認証ポリシー ルールに一致する場合、ファイアウォールは認証ポータル ページへの埋め込み URL リンクが含まれる UDP 通知を GlobalProtect アプリに送信します。その後、GlobalProtect アプリでこのメッセージがユーザーへのポップアップ通知として表示されます。
- ブラウザベースのアプリケーション — ブラウザベースのアプリケーションでは、通知メッセージをユーザーに表示するために GlobalProtect が必要ありません。ファイアウォールがセッションを Web ブラウジング トラフィック（App-ID に基づく）として識別すると、ファイアウォールは自動的に認証ポリシー ルールで指定された認証ポータル ページ（以前のキャプティブ ポータル ページ）をユーザーに表示します。詳細は、多要素認証の設定を参照してください。

非ブラウザベースのアプリケーションについて MFA 通知を表示するように GlobalProtect を設定するには、以下のワークフローに従います。

STEP 1 | GlobalProtect を設定する前に、ファイアウォールで多要素認証を設定します。

ゲートウェイまたはポータルに対する認証に *GlobalProtect* で *2* 要素認証を使用している場合、*RADIUS* サーバー プロファイルが必要です。*GlobalProtect* を使用して認証ポリシーの一致に関する通知をユーザーに行っている（*UDP* メッセージ）場合、多要素認証サーバー プロファイルで十分です。

機密性の高いリソースを保護するために多要素認証を使用するための最も簡単なソリューションは、ネットワークで既に確立済みの MFA ベンダーとファイアウォールを統合することです。MFA 構築の準備ができたら、認証ポリシーのコンポーネントの設定を開始できます。詳細は、多要素認証の設定を参照してください。

- キャプティブ ポータルで認証タイムスタンプを記録し、ユーザー マッピングを更新できるようにします。
- ファイアウォールのユーザーを認証するサービスへの接続方法を定義するサーバー プロファイルを作成します。
- サーバー プロファイルを、認証パラメータを指定する認証プロファイルに割り当てます。
- ユーザーが認証を必要とするリソースにアクセスできるように、セキュリティ ポリシー ルールを設定します。

STEP 2 | （外部ゲートウェイのみ）GlobalProtect が外部ゲートウェイで多要素認証をサポートできるようにするには、ファイアウォールの ingress トンネル インターフェイス用に応答ページを設定する必要があります。

1. **Device** > **Response Pages**（応答ページ） > **MFA Login Page**（**MFA** ログイン ページ）の順に選択します。
2. **Predefined**（事前定義済み）テンプレートを選択して、任意の場所に **Export**（エクスポート）します。
3. エンドポイントで、HTML エディタを使用してダウンロードした応答ページをカスタマイズして、一意のファイル名を付けて保存します。
4. ファイアウォールの **MFA Login Page**（**MFA** ログイン ページ）ダイアログに戻り、カスタマイズしたページを **Import**（インポート）して、**Import File**（インポート ファイル）を **Browse**（参照）して選択し、**Destination**（宛先）を選択します（仮想システムまたは共有の場所）。**OK**をクリックした後、**Close**（閉じる）をクリックします。

STEP 3 | （外部ゲートウェイのみ）**Interface Mgmt**（インターフェイス管理）プロファイルで許可されるサービスとして **Response Pages**（応答ページ）を有効にします。

1. **Network**（ネットワーク） > **Network Profiles**（ネットワーク プロファイル） > **Interface Mgmt**（インターフェイス管理）の順に選択し、プロファイルを選択します。
2. **Permitted Services** エリアで、**Response Pages**（応答ページ）を選択して **OK** をクリックします。

STEP 4 | （外部ゲートウェイのみ）**Interface Mgmt**（インターフェイス管理）プロファイルをトンネル インターフェイスに追加します。

1. **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Tunnel**（トンネル）の順に選択し、応答ページを使用するトンネル インターフェイスを選択します。
2. **Advanced**（詳細）を選択してから、前のステップで **Management Profile**（管理プロファイル） として設定した **Interface Mgmt**（インターフェイス管理）プロファイルを選択します。

STEP 5 | （外部ゲートウェイのみ）トンネル インターフェースに関連付けられたゾーンで **Enable User Identification**（ユーザー **ID** の有効化）を行います（**Network**（ネットワーク） > **Zones**（ゾーン） > **<tunnel-zone** ）。

STEP 6 | 非ブラウザベースのアプリケーションの多要素認証通知をサポートするように GlobalProtect クライアントを設定します。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択し、ポータル設定を選択します（または新しいポータルを **Add**（追加）します）。
2. **Agent (**エージェント**)** を選択し、さらに既存のエージェント設定を選択するか、新しい物を **Add (**追加**)** します。
3. **App**（アプリケーション）タブで、以下を指定します。
   - **Enable Inbound Authentication Prompts from MFA Gateways**（**MFA** ゲートウェイからのインバウンド認証プロンプトを有効にします） を **Yes**（はい）に設定します。多要素認証（MFA）をサポートするには、GlobalProtect アプリはゲートウェイからのインバウンド UDP プロンプトを受信および承認する必要がありま

す。GlobalProtect アプリがプロンプトを受け取り、受信確認できるようにする場合は **Yes**（はい）を選択します。デフォルトでは、この値は **No**（いいえ）になっています。この場合、GlobalProtect はゲートウェイからの UDP プロンプトをブロックします。

- **Network Port for Inbound Authentication Prompts (UDP)**（インバウンド認証プロンプト用の **GlobalProtect** ネットワーク ポート（**UDP**））フィールドで、MFA ゲートウェイからのインバウンド認証プロンプトの受け取りに GlobalProtect アプリが使用するポート番号を指定します。デフォルト ポートは 4501 です。ポートを変更するには、1 ～ 65535 の数値を指定します。
- **Trusted MFA Gateways (**信頼された **MFA** ゲートウェイ**)** フィールドで、GlobalProtect アプリケーションが多要素認証で信頼するリダイレクト URL のポート番号 (6082 など、デフォルト以外のポートでのみ必須) およびゲートウェイのアドレスを指定します。指定されたネットワーク ポートに向かうリダイレクト URL を伴う UDP 認証プロンプトを GlobalProtect アプリケーションが受信すると、GlobalProtect はリダイレクト URL を信頼できる場合にのみ認証メッセージを表示します。
- **Default Message for Inbound Authentication Prompts**（インバウンド認証プロンプト用のデフォルト メッセージ）を設定します。ユーザーが追加認証が必要なリソースにアクセスしようとすると、GlobalProtect はインバウンド認証プロンプトを含む UDP パケットを受信し、このメッセージを表示します。UDP パケットには、多要素認証の設定で指定した認証ポータル ページの URL も含まれています。GlobalProtect は自動的に URL をメッセージに付加します。たとえば、このトピックの最初に示した通知を表示するには、以下のメッセージを入力します。

  追加の認証が必要となる、保護されたリソースにアクセスしようとしています。`Proceed to authenticate at:` （以下に進んで認証を受けてください。）

4. エージェント設定を保存（**OK** を 2 回クリック）し、変更内容を **Commit**（コミット）します。

VSA を RADIUS サーバーに受け渡す機能の有効化

ポータルまたはゲートウェイと通信する際、GlobalProtect エンドポイントはエンドポイントの IP アドレス、操作システム (OS) 、ホスト名、ユーザードメイン、GlobalProtect アプリのバージョンを含む情報を送信します。ファイアウォールをオンにしてベンダー固有属性（VSA）をサーバーの認証中に RADIUS サーバーに送ることができます（デフォルトでは、ファイアウォールは VSA を送信しません。）RADIUS 管理者はこれらの VSA に基づき管理タスクを実行します。例えば、RADIUS 管理者は OS 属性を使って Microsoft Windows ユーザー用の通常のパスワード認証と Google Android ユーザー用のワンタイム パスワード (OTP) を必須とするポリシーを定義するかもしれません。

以下はこの工程の前提条件です：

- Palo Alto Networks RADIUS ディクショナリ をお使いの RADIUS サーバーにインポートします。
- RADIUS サーバープロファイルを設定し認証プロファイルへ割り当てます。詳細については外部認証のセットアップを参照してください。
- 認証プロファイルを GlobalProtect ポータルまたはゲートウェイをへ割り当てます。詳細は GlobalProtect ポータルへのアクセスのセットアップ またはGlobalProtect ゲートウェイの設定を参照してください。

STEP 1 | ファイアウォール CLI へのログイン

STEP 2 | 送信したい各 VSA のコマンドを入力します：

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

ファイアウォールが特定の *VSA* を送信するのを停止するには、***radius-vsa-on*** の代わりに ***radius-vsa-off*** オプションを使用して同じコマンドを実行します。

グループ マッピングの有効化

エンド ユーザーのシステムで実行しているエージェントまたはアプリケーションでは、GlobalProtect にアクセスするにはユーザーが認証に成功する必要があるため、各 GlobalProtect ユーザーの ID は把握されています。ただし、グループ メンバーシップに基づいて GlobalProtect 設定またはセキュリティ ポリシーを定義する場合、ファイアウォールがディレクトリ サーバーからグループのリストおよび対応するメンバーのリストを取得する必要があります。これはグループ マッピングと呼ばれます。

この機能を有効にするには、LDAP サーバー プロファイルを作成する必要があります。このプロファイルからファイアウォールに対して、ディレクトリ サーバーへの接続および認証方法と、ディレクトリでユーザーおよびグループの情報を検索する方法に関する命令が行われます。ファイアウォールがグループ マッピングを取得する LDAP サーバーに接続されたら、エージェント設定およびセキュリティポリシーを定義する際にグループを選択できるようになります。ファイアウォールは、Microsoft Active Directory（AD）、Novell eDirectory、Sun ONE Directory Server を含む、さまざまな LDAP ディレクトリ サーバーをサポートしています。

以下の手順により LDAP ディレクトリに接続し、ファイアウォールでユーザー対グループのマッピング情報を取得できるようにします。

STEP 1 | LDAP サーバー プロファイルを作成し、ファイアウォールがグループ マッピング情報の取得に使用するディレクトリ サーバーへの接続方法を指定します。

1. **Device** > **Server Profiles** > **LDAP**(デバイス > サーバー プロファイル > LDAP) の順に選択し、**Add**(追加) をクリックします。
2. サーバー プロファイルを識別する **Profile Name**（プロファイル名）を入力します。
3. このプロファイルが複数の仮想システム容量のあるファイアウォール用であれば、仮想システムを選択するか、そのプロファイルを利用できる **Location**（場所）として **Shared**（共有）を選択します。
4. 各 LDAP サーバー（最大 4）については、**Add**（追加）を実行し **Name**（名前）（サーバーを識別するために）、サーバー IP アドレス（**LDAP Server**（**LDAP** サーバー）フィールド）、サーバー **Port**（ポート）（デフォルト 389）を入力します。
5. LDAP サーバーの **Type**（タイプ）を選択します （**active-directory**, **e-directory**, **sun**、または**other**（その他））。
6. ディレクトリサーバーとの保護された接続のためにデバイスで SSL または TLS を使いたい場合は、 **Require SSL/TLS secured connection**（**SSL/TLS** で保護された接続を要求）チェックボックスを選択してください。（デフォルトでは選択されています）。サーバー **Port**（ポート）によってデバイスが使用するプロトコル：
   - 389（デフォルト） – TLS（具体的には、デバイスは StartTLS 操作を使用して、最初のプレーンテキスト接続を TLS にアップグレードします）
   - 636 – SSL
   - その他の任意のポート – デバイスはまず TLS を使用しようとします。ディレクトリサーバーで TLS がサポートされていない場合は、SSL にフォールバックします。
7. さらに保護を強化するには、**Verify Server Certificate for SSL sessions**（**SSL** セッションのサーバー証明書を確認）チェックボックス（デフォルトでクリア）を選びます。そう

すればデバイスは SSL/TLS 接続にディレクトリサーバーが提示する証明書を確認します。この検証を有効にするには、**Require SSL/TLS secured connection**（**SSL/TLS** で保護された接続を要求）チェック ボックスをオンにする必要もあります。進めるための確認において、証明書は次のいずれかの条件に合う必要があります。

- デバイス証明書のリストにある：**Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）。必要に応じて、証明書をデバイスにインポートします。
- 証明書の署名者は信頼できる証明機関のリストにあること：**Device** > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Default Trusted Certificate Authorities**（デフォルトの信頼できる証明機関）

8. <239>OK</239> をクリックします。

STEP 2 | LDAP サーバー プロファイルを User-ID のグループ マッピング設定に追加します。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **Group Mapping Settings (グループ マッピング設定)** の順に選択し、新しいグループ マッピング設定を **Add (追加)** します。
2. **Server Profile (サーバープロファイル)** を選択します。
3. **Name (名前)** にグループ マッピング設定の名前を入力します。
4. 作成した **Server Profile**（サーバー プロファイル）を選択します。
5. ファイアウォール ポリシーが使用するグループの更新情報を取得するため、ファイアウォールが LDAP ディレクトリ サーバーとの接続を開始する **Update Interval (更新間隔)** を秒数で指定します (範囲は 60 ～ 86,400 秒)。
6. グループ マッピング用にサーバープロファイルが **Enabled (有効)** になっていることを確認します。

STEP 3 | (任意) GlobalProtect を有効化し、ディレクトリ サーバーからシリアル番号を取得します。

GlobalProtect は接続中のエンドポイントのステータスを識別子、エンドポイントのシリアル番号の有無に基づいて HIP ベースのセキュリティ ポリシーを適用できます。エンドポイントが管理対象である場合、エンドポイントのシリアル番号をディレクトリ サーバー内のエンドポイントのマシン アカウントと紐付けることができます。その後、ファイアウォールがディレクトリ サーバーからグループ マッピング情報を取得する際、これらの管理対象のエンドポイントのシリアル番号を事前に取得できるようになります。

1. グループ マッピング設定で **Server Profile (サーバープロファイル)** を選択します。
2. **Fetch list of managed devices (管理対象デバイスのリストを取得)** するオプションを有効化します。

STEP 4 | (任意) ユーザーおよびユーザーグループを識別する属性を指定します。

1. グループ マッピング設定で **User and Group Attributes (**ユーザーおよびグループ属性**)** を選択します。
2. User Attributes (ユーザー属性) エリアで個々のユーザーを識別するために使用する **Primary Username (**プライマリ ユーザー名**)**、**E-Mail (**メール**)**、および **Alternate Username 1-3 (**代替ユーザー名 **1**～**3)** を指定します。
3. Group Attributes (グループ属性) エリアで個々のユーザーグループを識別するために使用する **Group Name (**グループ名**)**、**Group Member (**グループ メンバー**)**、および **E-Mail (**メール**)** を指定します。

STEP 5 | （任意）ポリシールールで選択できるグループを制限します。

デフォルトでは、グループを指定しないと、ポリシー ルールですべてのグループを使用できます。

1. ディレクトリサービスから既存グループを追加します。
   1. グループ マッピング設定で **Group Include List (**グループ許可リスト**)** を選択します。
   2. Available Groups (利用可能なグループ)リスト内で、ポリシールールに表示するグループを選択して Add (追加) アイコン (⊕) をクリックし、グループを Included Groups (許可するグループ) のリストに移動させます。
2. 既存のユーザー グループに一致しないユーザー属性に基づいてポリシー ルールを作成する場合、LDAP フィルタに基づいてカスタム グループを作成します。
   1. グループ マッピング設定で **Custom Group (**カスタム グループ**)** を選択します。
   2. 新しいカスタム グループを **Add (**追加**)** します。
   3. 現在のファイアウォールまたは仮想システムにおけるグループマッピング設定の中で一意のグループの **Name**（名前）を入力します。**Name**（名前）に既存の AD グループ ドメインの識別名（DN）と同じ値があると、ファイアウォールは、その名前が参照されるすべての場所（たとえば、ポリシーやログ内）でカスタム グループを使用します。
   4. 最高 2,048 UTF-8 文字の **LDAP Filter**（**LDAP** フィルタ）を指定し、それから **OK** をクリックします。ファイアウォールは、LDAP フィルタを検証しません。

      LDAP 検索を最適化し、*LDAP* ディレクトリ サーバーのパフォーマンスへの影響を最小限にするには、索引付き属性を使用し、検索範囲を縮小して、ポリシーまたは可視性に必要なユーザーおよびグループ オブジェクトを含めます。また、*LDAP*フィルタに基づいてカスタムグループを作成することもできます。

STEP 6 | 変更をコミットします。

OK、**Commit (**コミット**)** の順にクリックします。

paloalto TECHDOCS

GlobalProtect ゲートウェイ

GlobalProtect ゲートウェイの概要

アプリケーションに配信される GlobalProtect ポータル設定には、エンドポイントが接続できるゲートウェイのリストが含まれているため、ポータルを設定する前にゲートウェイを設定することをお勧めします。

GlobalProtect ゲートウェイは、以下の 2 つのメイン機能を提供するように設定されます。

- 接続される GlobalProtect のセキュリティ ポリシーをゲートウェイに適用します。また、セキュリティ ポリシーをより詳細に設定するため、ゲートウェイで HIP 収集を有効にすることもできます。HIP チェックの有効化の詳細は、ホスト情報を参照してください。
- 企業内部ネットワークに仮想プライベート ネットワーク（VPN）アクセスを提供する。VPN アクセスは、ゲートウェイをホストしているファイアウォール上のエンドポイントとトンネル インターフェイス間の IPsec または SSL トンネルを通じて提供されます。

AWS クラウドにデプロイされた *VM-Series* ファイアウォールで *GlobalProtect* ゲートウェイを設定することもできます。通常、このインフラストラクチャをセットアップする場合、コストや *IT* 機器の負担が生じますが、*VM-Series* ファイアウォールを *AWS* クラウドにデプロイすると、このような負担を負うことなく、*GlobalProtect* ゲートウェイを任意の領域にすばやく簡単にデプロイできます。詳細は、使用例:AWS の *GlobalProtect* ゲートウェイとしての *VM-Series* ファイアウォールを参照してください。

GlobalProtect ゲートウェイのコンセプト

以下のセクションでは、複数ゲートウェイの設定でのゲートウェイ接続の優先順位および GlobalProtect ゲートウェイの MIB サポートについて説明します。

- ゲートウェイのタイプ
- 複数ゲートウェイ構成時のゲートウェイの優先順位
- GlobalProtect MIB サポート

ゲートウェイのタイプ

GlobalProtect ゲートウェイは、GlobalProtect アプリケーションからのトラフィックに対するセキュリティ処理を提供します。さらに、ホスト情報 プロファイル (HIP) 機能が有効になっている場合、ゲートウェイはエンドポイントが送信する生ホスト データから HIP レポートを生成し、この情報をポリシーの適用に使用できます。

GlobalProtect ゲートウェイの設定は、Palo Alto Networks 次世代ファイアウォールで行います。同じファイアウォールでゲートウェイとポータルの両方を実行できます。または、企業全体で複数の分散ゲートウェイを設定することも可能です。

GlobalProtect では、以下のゲートウェイタイプがサポートされています。

- 内部—内部ゲートウェイは、内部リソースへのアクセスに対するセキュリティ ポリシーを適用する、GlobalProtect ゲートウェイとして設定された内部ネットワークのインターフェイスです。内部ゲートウェイを User-ID や HIP チェックと併用すると、ユーザーやデバイス状態を基準にトラフィックを識別して制御することができます。内部ゲートウェイは、重要なリソースへの認証済みアクセスが必要な機密環境で役立ちます。内部ゲートウェイは、トンネル モードまたは非トンネル モードのいずれかで設定できます。GlobalProtect アプリはエンドポイントの位置を判断するために、内部ホスト検出を実行した後で内部ゲートウェイに接続します。
- 外部ゲートウェイ（自動検出）—外部ゲートウェイは企業ネットワーク外にあり、リモート ユーザー向けにセキュリティ処理や仮想プライベート ネットワーク（VPN）アクセスを提供します。デフォルトでは、 GlobalProtect アプリはゲートウェイに割り当てた優先順位、送信元地域、応答時間に基づいて、自動的に **Best Available (**利用可能な最適な接続**)** 外部ゲートウェイに接続します (複数ゲートウェイ構成時のゲートウェイの優先順位を参照)。
- 外部ゲートウェイ（手動）—手動の外部ゲートウェイも企業ネットワーク外にあり、リモート ユーザー向けにセキュリティ処理や VPN アクセスを提供します。自動検出の外部ゲートウェイと手動の外部ゲートウェイの違いは、ユーザーが接続を開始したときに GlobalProtect アプリが手動の外部ゲートウェイにしか接続しないという点にあります。手動の外部ゲートウェイに異なる認証要件を設定することもできます。手動のゲートウェイを設定するには、GlobalProtect ポータルのエージェント設定の定義を行う時にゲートウェイを **Manual**（手動）として識別する必要があります。

複数ゲートウェイ構成時のゲートウェイの優先順位

追加の Palo Alto Networks 次世代ファイアウォールを戦略的にデプロイし、それらを GlobalProtect ゲートウェイとして設定すれば、従業員がどこからアクセスしようと、モバイル端

末からのアクセスを保護できるようになります。エージェントが接続する適切なゲートウェイを決定するために、ゲートウェイをポータルのアプリ設定に追加し、各ゲートウェイに接続の優先順位を割り当てます。GlobalProtect エージェント設定の定義を参照してください。

GlobalProtect ポータルのアプリ設定に複数のゲートウェイが含まれている場合、エージェントはエージェント設定に含まれるすべてのゲートウェイとの通信を試みます。次に、アプリは優先順位と応答時間を使用して、接続するゲートウェイを決定します。GlobalProtect アプリ 4.0.2 以前のリリースの場合、アプリは、優先順位が高いゲートウェイの応答時間が全ゲートウェイの応答時間の平均よりも長い場合にのみ、優先順位が低いゲートウェイに接続します。

例えば、gw1 および gw2 の応答時間が次のようになる場合を検討してみましょう。

名前	優先順位	応答時間
gw1	最高	80 ms
gw2	High（高）	25 ms

アプリは、優先順位が最も高い（数値が大きい）ゲートウェイの応答時間が両方のゲートウェイの平均応答時間（52.5 ms）よりも長いと判断し、gw2 に接続します。この例では、応答時間 80 ms というのは両方の平均よりも長いため、gw1 の優先順位が高くても、アプリは gw1 に接続しませんでした。

それでは、gw1、gw2、そして 3 つ目のゲートウェイである gw3 の応答時間が以下のようになる場合を検討してみましょう。

名前	優先順位	応答時間
gw1	最高	30 ms
gw2	High（高）	25 ms
gw3	Medium（中）	50 ms

この例では、すべてのゲートウェイの平均応答時間は 35 ms です。アプリはどのゲートウェイが平均応答時間よりも早く応答したか評価し、gw1 と gw2 の応答時間は両方とも早いことを確認します。そうするとアプリは、優先順位が高いいずれかのゲートウェイに接続します。この例では、応答時間が平均よりも早かったすべてのゲートウェイの内、gw1 の優先順位が最も高いため、アプリは gw1 に接続します。

ゲートウェイの優先順位に加えて、外部ゲートウェイ構成に 1 つまたは複数の送信元地域を追加できます。GlobalProtect は送信元地域を認識して、その地域に設定されたゲートウェイに対してのみユーザーの接続を許可します。ゲートウェイの選択については、送信元地域が考慮されてから、ゲートウェイの優先順位が考慮されます。

GlobalProtect アプリ 4.0.3 以降のリリースでは、GlobalProtect アプリは応答時間に関係なく、low（低）または lowest（最低）の優先順位が割り当てられたゲートウェイよりも

highest（最高）、high（高）、medium（中）の優先順位が割り当てられたゲートウェイを優先します。その後、GlobalProtect アプリは low（低）または lowest（最低）の優先順位が割り当てられたゲートウェイをゲートウェイのリストに追加します。これにより、アプリは必ず高い優先順位で設定したゲートウェイへの接続を最初に試みます。

GlobalProtect MIB サポート

Palo Alto Networks のエンドポイントは、標準仕様およびエンタープライズ向けの管理情報ベース（MIB）をサポートしており、エンドポイントの物理的状態、使用状況の統計、トラップ、その他の有益な情報を監視することができます。大抵の MIB は、シンプル ネットワーク管理プロトコル（SNMP）フレームワークを用いてエンドポイントの特性を表すために、オブジェクト グループを使用します。これらの MIB を SNMP マネージャにロードして、MIB で定義されているオブジェクト（エンドポイント統計情報およびトラップ）を監視する必要があります (詳細は、PAN-OS 8.1 管理者ガイドのSNMP マネージャを使用して MIB およびオブジェクトを調査を参照)。

エンタープライズ MIB に含まれている PAN-COMMON-MIB は、panGlobalProtect オブジェクト グループを使用します。panGlobalProtect オブジェクト グループを構成するオブジェクトは、次の表の通りです。

オブジェクト	説明
panGPGWUtilizationPct	GlobalProtect ゲートウェイの使用状況（パーセント値として）
panGPGWUtilizationMaxTunnels	許可されているトンネルの最大数
panGPGWUtilizationActiveTunnels	アクティブなトンネルの数

これらの SNMP オブジェクトを使用して GlobalProtect ゲートウェイの使用状況を監視し、必要に応じて変更を加えます。例えば、アクティブなトンネルの数が 80% に達している、または許可されているトンネルの最大数を超えている場合、ゲートウェイを追加することを検討するべきです。

GlobalProtect ゲートウェイを設定するための前提条件となるタスク

GlobalProtect ゲートウェイを設定する前に、以下のタスクを完了している必要があります。

- 各ゲートウェイを設定する予定のファイアウォールのインターフェイス（およびゾーン）を作成します。トンネル接続が必要なゲートウェイの場合、物理インターフェイスと仮想トンネル インターフェイスの両方を設定する必要があります。GlobalProtect のインターフェイスおよびゾーンの作成を参照してください。
- GlobalProtect アプリがゲートウェイとの SSL 接続を確立するために必要なゲートウェイ サーバー証明書と SSL/TLS サービスプロファイルをセットアップします。GlobalProtect コンポーネント間の SSL の有効化を参照してください。
- GlobalProtect ユーザーの認証に使用される認証プロファイル/証明書プロファイルを定義します。認証を参照してください。

GlobalProtect ゲートウェイの設定

前提条件となるタスクを完了した後に、GlobalProtect ゲートウェイを設定します。

STEP 1 | ゲートウェイを追加します。

1. 新しいゲートウェイを **Add (追加)** します (**Network (ネットワーク)** > **GlobalProtect** > **Gateways (ゲートウェイ)**)。
2. ゲートウェイの **Name (名前)** を付けます。

   ゲートウェイ名にスペースを含めることはできず、各virtual system(仮想システム-vsys)に固有のものである必要があります。ベスト プラクティスとして、ユーザーや管理者がゲートウェイを識別できるように、場所やその他の分かりやすい情報を含めます。
3. (任意) このゲートウェイが属している仮想システムの **Location (場所)** を選択します。

STEP 2 | エンドポイントがゲートウェイに接続できるようにするネットワーク情報を指定します。

すでに存在しない場合は、ゲートウェイ用のネットワークインターフェイスを作成 します。

> 設定を行うインターフェイスで *HTTP*、*HTTPS*、*Telnet*、または *SSH* を許可するインターフェイス管理プロファイルを追加すると、インターネットからの管理インターフェイスへのアクセスを許可することになるため、プロファイルを追加しないでください。管理アクセスの保護のベスト プラクティスに従い、攻撃を阻止するようにファイアウォールへの管理アクセスを保護してください。

1. エンドポイントがゲートウェイとの通信に使用する **Interface (インターフェイス)** を選択します。
2. ゲートウェイ Web サービスの **IP Address Type**（**IP** アドレス タイプ）と **IP address**（**IP** アドレス）を指定します。
   - （**IP Address Type**）**IP** アドレス タイプは、**IPv4 Only**（**IPv4** のみ）、**IPv6**（**IPv6** のみ）、あるいは **IPv4 and IPv6 (IPv4** および **IPv6)** に設定できます。ネットワークがデュアル スタック構成をサポートしているときは、**IPv4 and IPv6**（**IPv4** および **IPv6**）を使用します。これにより IPv4 と IPv6 が同時に動作します。
   - IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 アドレス の場合は `172.16.1/0`、IPv6 アドレスの場合は `21DA:D3:0:2F3b` のように指定します。デュアル スタック構成の場合は、IPv4 アドレスと IPv6 アドレスの両方を入力します。

STEP 3 | ゲートウェイがユーザーを認証する方法を指定します。

ゲートウェイ用の SSL/TLS サービス プロファイルが存在しない場合は、サーバー証明書を GlobalProtect コンポーネントにデプロイします。

認証プロファイルあるいは証明書プロファイルが存在しない場合は、認証セットアップ作業を行ってゲートウェイ用にこれらのプロファイルを設定します。

次のゲートウェイの **Authentication**（認証）設定を構成します（**Network**（ネットワーク）> **GlobalProtect** > **Gateways**（ゲートウェイ） > ***<gateway-config>*** > **Authentication**（認証））：

- ゲートウェイと GlobalProtect 間でセキュアな通信を行うために、ゲートウェイ用の **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）を選択します。

  最も強力なセキュリティを提供するには、***SSL/TLS*** サービス プロファイルの ***Min Version***（最低バージョン）を ***TLSv1.2*** に設定します。

- ローカル ユーザー データベース、または LDAP、Kerberos、TACACS+、SAML、RADIUS などの外部認証サービス（OTP を含む）を使用してユーザーを認証する場合、以下の設定と共に **Client Authentication**（クライアント認証）設定を **Add**（追加）します。
  - このクライアント認証設定を識別する **Name**（名前）を入力します。
  - この設定を適用する **OS**（オペレーティングシステム）の種類を識別します。デフォルトでは、設定は、**Any**（指定なし）のオペレーティングシステムに適用されます。
  - ゲートウェイへのアクセスを求めるエンドポイントの認証に使用する**Authentication Profile**（認証プロファイル）を選択または追加します。
  - ゲートウェイ ログイン用のカスタム **Username Label**（ユーザー名ラベル）を入力します（電子メール アドレス **(username@domain**等）。
  - ゲートウェイ ログイン用のカスタム **Password Label**（パスワード ラベル） を入力します（2 要素認証、トークンベースの認証の場合はパスコード）。
  - エンドユーザーがログイン時に使用する証明書を理解しやすくなるように、**Authentication Message**（認証メッセージ）を入力します。メッセージの最大長は 256 文字です。（デフォルトは `Enter login credentials`です）。
  - 次のいずれかのオプションを選択し、ユーザーが認証情報かつ/またはクライアント証明書を使用してゲートウェイに認証できるかどうかを定義します：
    - ユーザーがユーザー認証情報およびクライアント証明書の両方を使ってゲートウェイに認証することを求める場合、**Allow Authentication with User Credentials OR Client Certificate (**ユーザー認証情報あるいはクライアント証明書による認証を許可**)** するオプションを **No (User Credentials AND Client Certificate Required) (**いいえ**(**ユーザー認証情報およびクライアント証明書が必要**))** (デフォルト) に設定します。
    - ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってゲートウェイに認証することを許可する場合、**Allow Authentication with User Credentials OR Client Certificate (**ユーザー認証情報あるいはクライアント証明書による認証を許可**)**するオプションを **Yes (User Credentials OR Client Certificate**

Required) (はい **(**ユーザー認証情報あるいはクライアント証明書が必要**))** に設定します。

このオプションを **Yes (**はい**)** に設定すると、ゲートウェイはまずエンドポイントのクライアント証明書をチェックします。エンドポイントがクライアント証明書を持っていない、あるいはクライアント認証設定用の証明書プロファイルを設定していない場合、エンドポイントのユーザーは自身のユーザー認証情報を使用してゲートウェイに認証する必要があります。

- クライアント証明書またはスマート カード/CAC に基づいてユーザーを認証するには、対応する **Certificate Profile**（証明書プロファイル）を選択します。クライアント証明書を事前にデプロイするか、Simple Certificate Enrollment Protocol（SCEP）を使用して 認証用のユーザー固有のクライアント証明書のデプロイする必要があります。
  - ユーザーがユーザー認証情報およびクライアント証明書の両方を使ってゲートウェイに認証することを求める場合、**Certificate Profile (**証明書プロファイル**)** および認証プロファイルの両方を指定する必要があります。
  - ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってゲートウェイに認証するのを許可し、ユーザー認証用の **Authentication Profile (**認証プロファイル**)** を指定する場合、**Certificate Profile (**証明書プロファイル**)** は任意項目になります。
  - ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってゲートウェイに認証するのを許可し、ユーザー認証用の 認証プロファイル を選択しない場合、**Certificate Profile (**証明書プロファイル**)** は必須項目になります。

- 特定の OS にマッチする **Authentication Profile** (認証プロファイル) を一切設定しない場合、**Certificate Profile** (証明書プロファイル) が必須項目になります。

ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使用してゲートウェイに認証することを許可する場合、***Username Field*** (ユーザー名フィールド) を ***None*** (なし) に設定した ***Certificate Profile*** (証明書プロファイル) を選択しないでください。

- 2 要素認証を使用するには、**Authentication Profile** (証明書プロファイル) と **Certificate Profile** (証明書プロファイル) の両方を選択します。この場合、ユーザーが両方の方法を使って認証を成功させなければ、アクセスできなくなります。

(Chrome のみ) ゲートウェイがクライアント証明書および *LDAP* を使用して *2* 要素認証を行うように設定する場合、*Chrome OS 47* 以降のバージョンを実行する *Chromebook* で、クライアント証明書を選択するために過剰なプロンプトが発生します。この過剰なプロンプトを防止するために、*Google* 管理コンソールでクライアント証明書を指定する設定を行ってから、ポリシーを管理対象の *Chromebook* にデプロイします。

1. Google 管理コンソールにログインし、***Device management*** (デバイス マネージャ) > ***Chrome management*** (*Chrome* 管理) > ***User settings*** (ユーザー設定) を選択します。
2. *Client Certificates* (クライアント証明書) セクションで次の *URL* パターンを入力し、***Automatically Select Client Certificate for These Sites*** (これらのサイトに対して自動的にクライアント証明書を選択) します：

   ```
   {"pattern": "https://[*.]","filter":{}}
   ```

3. ***Save***（保存）をクリックします。*Google* 管理コンソールが数分以内にすべてのデバイスにポリシーをデプロイします。

STEP 4 | トンネルを有効化して、トンネルのパラメーターを設定します。

外部ゲートウェイの場合はトンネル パラメータが必須です。内部ゲートウェイの場合は任意項目になります。

SSL-VPN トンネル モードの使用を強制する場合、***Enable IPSec (IPSec* の有効化*)*** オプションを無効化 *(*クリア*)* します。デフォルトでは、*SSL-VPN* はエンドポイントが *IPSec* トンネルの確立に失敗した場合にのみ使用されます。

Extended Authentication（*X-Auth*）は、*IPSec* トンネルのみでサポートされています。

Enable X-Auth Support（***X-Auth*** サポートの有効化）を行う場合、*GlobalProtect* の *IPSec* 暗号化プロファイルは利用できません。

サポートされている暗号化アルゴリズムの詳細については、GlobalProtect アプリの暗号化機能 を参照してください。

1. GlobalProtect Configuration Gateway (GlobalProtect 設定ゲートウェイ)ダイアログで、**Agent** > **Tunnel Settings** (エージェント > トンネル設定)の順に選択します。
2. **Tunnel Mode**（トンネル モード）を有効にして、トンネリングの分割を有効にします。
3. ゲートウェイ用のネットワークインターフェイスを作成する際に定義した **Tunnel Interface (**トンネル インターフェイス**)** を選択します。
4. (任意) 認証、HIP 更新、および GlobalProtect エージェント更新のために同時にゲートウェイにアクセスできるユーザーの最大数 (**Max User (**最大ユーザー数**)**) を指定します。値の範囲は、フィールドが空でプラットフォームによって異なる場合に表示されます。
5. **Enable IPSec**（**IPSec** の有効化）を行い、次に**GlobalProtect IPSec Crypto**（**GlobalProtect IPSec**暗号化）プロファイルを選択して GlobalProtect アプリとゲートウェイ間の VPN トンネルを保護します。**default**（デフォルト）プロファイルでは、AES-128-CBC 暗号化と sha1 認証が使用されます。

   *IPSecはWindows 10 UWP*エンドポイントでサポートされていません。

   New GlobalProtect IPSec Crypto (新規 **GlobalProtect IPsec** 暗号化**)** プロファイルを作成 (**GlobalProtect IPSec Crypto (GlobalProtect IPsec** 暗号化プロファイル**)**ドロップダウンメニュー) してから、次の設定を構成することもできます。

   1. プロファイルを識別する **Name**（名前）を入力します。

   2. VPN ピアがトンネル内のデータを保護するためのキーをネゴシエートするために使用する **Authentication**（認証）および **Encryption**（暗号化）アルゴリズムを **Add**（追加）します。

   - **Encryption**（暗号化） — VPN ピアがどの暗号化をサポートするか不明な場合は、次のように保護強度が高い順に複数の暗号アルゴリズムを追加できます: **aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**.ピアはトンネルを確立するための最も強固なアルゴリズムを判別します。

- **Authentication**（認証） — データの整合性および認証の保護を維持する認証アルゴリズム（**sha1**）を選択します。プロファイルには認証アルゴリズムが必要ですが、この設定は AES-CBC 暗号（**aes-128-cbc**）にのみ適用されます。AES-GCM 暗号化アルゴリズム（**aes-256-gcm** or **aes-128-gcm**）を使用する場合、これらの暗号はネイティブで ESP 整合性保護機能をサポートしているため、設定が無視されます。

3. **OK** をクリックしてプロファイルを保存します。

6. （任意）サードパーティ VPN（Linux 上で実行されている VPNC クライアントなど）を使用してゲートウェイに接続する必要があるエンドポイントが存在する場合、**Enable X-Auth Support**（**X-Auth** サポートの有効化）を行います。X-Auth を有効にした場合、エンドポイントに必要な場合は**Group**（グループ） 名と **Group Password**（グループパスワード）を入力する必要があります。デフォルトでは、IPSec トンネルの確立に使用されたキーの有効期限が切れた場合、ユーザーに再認証は要求されません。ユーザーに再認証を要求する場合は、**Skip Auth on IKE Rekey**（**IKE** キー再生成での認証をスキップ）するオプションの選択を無効化します。

   strongSwan エンドポイントでは *IKE SA* ネゴシエーション中に再認証が必要であるため、それ用に ***Enable X-Auth Support (X-Auth*** サポートを有効化**)** するためには、***Skip Auth on IKE Rekey (IKE*** のキー再発行時に認証をスキップ**)** するオプションを無効化する必要もあります。さらに、**`closeaction=restart`** 設定を *strongSwan IPSec* 設定ファイルの **`conn %default`** セクションに追加しなければなりません。*(StrongSwan IPSec* 設定の詳細については、strongSwan Ubuntu および CentOS エンドポイントの認証のセットアップを参照してください*)*。

   X-Auth アクセスは *iOS* および *Android* エンドポイントでサポートされていますが、これらのエンドポイントで利用できる *GlobalProtect* 機能は制限されています。*GlobalProtect* アプリケーションを使用すれば、*GlobalProtect* によって *iOS* および *Android* エンドポイントに提供されるすべてのセキュリティ機能に簡単にアクセスできるようになります。*iOS* 用 *GlobalProtect* アプリケーションは *Apple* 社の *App Store* で入手できます。*Android* 用 *GlobalProtect* アプリケーションは *Google Play* で入手できます。

STEP 5 | （トンネル モードのみ）クライアント設定用の選択条件を指定します。

ゲートウェイは、どの設定を接続する GlobalProtect アプリに配信するかを決定するために、指定されているユーザー/ユーザー グループの設定を使用します。複数の設定がある場合は、設定を適切な順序に並べる必要があります。ゲートウェイがマッチを見つけると (**Source User (**送信元ユーザー**)**、**OS**、および **Source Address (**送信元アドレス**)** に基づき)、関連する設定をユーザーに配信します。そのため、より具体的な設定が、一般的な設定よりも優先される必要があります。ステップ 13 を参照してください。 クライアント設定のための設定リストの順序に関する指示。

1. GlobalProtect Configuration Gateway（GlobalProtect 設定ゲートウェイ）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定）の順に選択します。
2. 既存のクライアント設定の構成を選択するか、新しく **Add**（追加）します。

3. 次の **Config Selection Criteria (設定選択条件)** を設定します：
   - この設定を特定のユーザーあるいはユーザーグループにデプロイする場合、**Source User (送信元ユーザー)** (あるいはユーザーグループ) を **Add (追加)** します。この設定をプレ ログオンモードのアプリケーションを使用しているユーザーにのみデプロイする場合は、**Source User (送信元ユーザー)** のドロップダウンリストで **pre-logon (プレ ログオン)** を選択します。この設定をすべてのユーザーにデプロイする場合は **any (すべて)** を選択します。

     この設定を特定のグループにデプロイする場合は、グループ マッピングの有効化で説明されているように、まずはユーザーをグループにマッピングする必要があります。
   - エンドポイントのオペレーティングシステムに基づいてこの設定をデプロイする場合は、**OS** (Android、Chrome など) を **Add (追加)** します。この設定をすべてのオペレーティングシステムにデプロイする場合は、**Any (すべて)** を選択します。
   - ユーザーの場所に基づいてこの設定をデプロイする場合は、送信元の**Region (地域)**あるいはローカル **IP Address (IP アドレス)** (IPv4 および IPv6) を**Add (追加)**します。この設定をすべてのユーザーの場所にデプロイする場合、**Region (地域)** や **IP Address (IP アドレス)** は指定しないでください。
4. **OK** をクリックして、設定の選択条件を保存します。

STEP 6 | (トンネル モードのみ) 認証のオーバーライドを設定し、ゲートウェイが安全に暗号化された Cookie を生成・承認してユーザーを認証できるようにします。この機能により、指定した期間（たとえば、24 時間毎）中にユーザーにログイン認証情報を求めるのが 1 度で済むようになります。

デフォルト設定では、ゲートウェイは認証プロファイルと任意で証明書プロファイルを使用してユーザーを認証します。認証のオーバーライドが有効な場合、GlobalProtect は成功したログインの結果をキャッシュし、ユーザーに認証情報を求める代わりに Cookie を使用してユーザーを認証するようになります。詳細は、ポータルまたはゲートウェイでの Cookie 認証を参照してください。クライアント証明書が必要な場合、エンドポイントが有効な証明書も提示しなければ、アクセスが許可されません。

Cookie の有効期限が切れていないデバイスへのアクセスを即刻ブロックする必要がある場合（たとえば、デバイスを紛失したり、盗まれたりした場合）、そのエンドポイントをブロックリストに即座に追加することでエンドポイントのアクセスをブロックすることができます。

1. GlobalProtect Configuration Gateway（GlobalProtect 設定ゲートウェイ）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定）の順に選択します。
2. 既存のクライアント設定の構成を選択するか、新しく **Add**（追加）します。

3. 以下の**Authentication Override**（認証のオーバーライド）を設定します：
   - **Name**（名前）—設定を識別します。
   - **Generate cookie for authentication override**（認証オーバーライド用 **Cookie** を生成） — ゲートウェイが暗号化されたエンドポイント固有の Cookie を生成し、その認証用 Cookie をエンドポイントに発行できるようにします。
   - **Accept cookie for authentication override**（**Cookie** による認証オーバーライドを許可） — ゲートウェイが暗号化された有効な Cookie を使用してユーザーを認証できるようにします。有効な Cookie をアプリが提示した場合、ゲートウェイはポータルまたはゲートウェイが暗号化した Cookie であることを確認し、復号化を行ってユーザーを認証します。

     GlobalProtect アプリケーションが関連する認証用 *Cookie* をユーザーのエンドポイントにマッチさせて取得するためには、接続するユーザーのユーザー名を知る必要があります。*Cookie* を取得した後、アプリはそれをポータルあるいはゲートウェイに送信してユーザー認証を行います。

     (Windows のみ) ポータルのエージェント設定でシングル サインオンを使用するオプションを***Yes*** *(*はい*)* に設定 *(SSO* を有効化*)* すると *(****Network*** *(*ネットワーク*) > GlobalProtectPortals >* *(*ポータル*) > <portal-config> > Agent (*エージェント*) > <agent-config> > App (*アプリ*))*、*GlobalProtect* アプリケーションが *Windows* のユーザー名を使用してユーザーのローカル認証用 *Cookie* を取得するようになります。***Use Single Sign-On*** *(*シングル サインオンを使用*)* するオプションを ***No*** *(*いいえ*)* に設定 *(SSO* を無効化*)* する場合、アプリがユーザーの認証用 *Cookie* を取得できるようにするために、*GlobalProtect* アプリケーションがユーザー認証情報を保存できるようにする必要があります。***Save User Credentials*** *(*ユーザー認証情報の保存*)* オプションを ***Yes*** *(*はい*)* に設定するとユーザー名およびパスワードの両方が、***Save Username Only*** *(*ユーザー名のみ保存*)* に設定するとユーザー名だけが保存されます。
   - **Cookie Lifetime**（**Cookie** の有効期間） — Cookie が有効な時間数、日数、または週数を指定します（デフォルトは 24 時間）。範囲は、時間が 1～72、週が 1～52、日数が 1～365 です。Cookie が失効した場合、ユーザーはログイン認証情報を再度入力する必要があり、この入力をうけ、ゲートウェイは新しい Cookie を暗号化してアプリに送信します。この値は、ポータル用に設定した**Cookie Lifetime**（**Cookie** の有効期間）と同じにすることも、別の値にすることも可能です。

- **Certificate to Encrypt/Decrypt Cookie**（**Cookie** 暗号化/復号化時の証明書） — Cookie を暗号化および複合化するために使用する RSA 証明書を選択します。ポータルおよびゲートウェイで同じ証明書を使う必要があります。

  RSA 証明書がネットワークでサポートされている最も強固なダイジェスト アルゴリズムを使うように設定することが推奨されます。

  ポータルおよびゲートウェイは RSA 暗号化パディング スキーム PKCS#1 V1.5 を使用して Cookie を生成（証明書の公開鍵を使用）し、Cookie を復号化します（証明書の秘密鍵を使用）。

STEP 7 | （トンネル モードのみ）（任意）IPv4 または IPv6 アドレスを、ゲートウェイに接続するエンドポイントの仮想ネットワーク アダプタに割り当てるために使用するクライアント レベルの IP プールを設定します。

IP プールの構成は、クライアント レベル（***Network***（ネットワーク） > ***GlobalProtect*** > ***Gateways***（ゲートウェイ） > ***<gateway-config>*** > ***GlobalProtect Gateway Configuration***（***GlobalProtect*** ゲートウェイ設定） > ***Agent***（エージェント） > ***Client Settings***（クライアント設定） > ***<client-setting>*** > ***Configs***（設定） > ***IP Pools***（***IP*** プール））またはゲートウェイ レベル（***Network***（ネットワーク） > ***GlobalProtect*** > ***Gateways***（ゲートウェイ） > ***<gateway-config>*** > ***GlobalProtect Gateway Configuration***（***GlobalProtect*** ゲートウェイ設定） > ***Agent***（エージェント） > ***Client IP Pool***（クライアント ***IP*** プール））のいずれかでのみ行わなければなりません。

非トンネル モードの内部ゲートウェイ設定では、アプリは物理ネットワーク アダプタに割り当てられたネットワーク設定を使用するため、*IP* プールおよびスプリット トンネル設定は不要です。

ゲートウェイ*IP*アドレスプールの設定時にアドレスオブジェクトを使用することはサポートされていません。

1. GlobalProtect Configuration Gateway（GlobalProtect 設定ゲートウェイ）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定）の順に選択します。
2. 既存のクライアント設定の構成を選択するか、新しく **Add**（追加）します。
3. 次のいずれかの **IP Pools (IP** プール**)** 設定を行います。
   - 静的 IP アドレスを要求するエンドポイント用に認証サーバーの IP アドレス プールを指定するには、 **Retrieve Framed-IP-Address attribute from authentication server**（フレーム済-**IP**-アドレス属性を認証サーバーから検索する）チェックボックスをオンにし、サブネットまたは IP アドレス範囲を**Add**（追加）して**Authentication Server IP Pool**（認証サーバー **IP** プール）まで含むようにします。トンネルが確立されると、リモートユーザーのコンピューターにインターフェイス

が作成されます 認証サーバーの Framed-IP 属性にマッチする IP 範囲あるいはサブネット内のアドレスを伴います。

認証サーバーの *IP* アドレス プールには、すべての同時接続ユーザーをサポートするのに十分な *IP* アドレスが含まれている必要があります。*IP* アドレスは静的に割り当てられ、ユーザーの接続が切断された後も保持されます。

- ゲートウェイに接続するエンドポイントに IPv4 または IPv6 アドレスを割り当てるために使用する**IP Pools**（**IP** プール）を指定するには、IPアドレスサブネット/範囲を **Add**（追加）追加します。IPv4またはIPv6のサブネットまたは範囲、あるいはその2つの組み合わせを追加できます。

  ゲートウェイへの適切なルーティングを確実に行うには、ゲートウェイ上の既存の IP プール（該当する場合）および LAN に物理的に接続されているエンドポイントに割り当てられたものとは異なる範囲の IP アドレスを使用する必要があります。プライベート IP アドレッシング スキームを使用することを推奨します。

4. **OK** をクリックして IP プール設定を保存します。

STEP 8 | (トンネル モードのみ—任意) スプリット トンネルを無効化し、すべてのトラフィック (ローカル サブネット トラフィックを含む) が VPN トンネルを経由して検査され、ポリシーを適用されるようにする必要があります。

STEP 9 | （トンネル モードのみ）（任意）アクセスルートに基づいてスプリットトンネル設定を設定します。

STEP 10 | （トンネル モードのみ）（任意）アクセスルートに基づいてスプリットトンネル設定を設定します。

STEP 11 | （トンネル モードのみ）（任意）アプリケーションルートに基づいてスプリットトンネル設定を設定します。

STEP 12 | (トンネル モードのみ—任意) クライアント設定用の DNS を設定します。

クライアント設定で一つ以上の *DNS* サーバーあるいは *DNS* サフィックスを設定すると (***Network*** (ネットワーク) > ***GlobalProtect*** > ***Gateways*** (ゲートウェイ) > ***<gateway-config>*** > ***Agent*** (エージェント) > ***Client Settings*** (クライアント設定) > ***<client-settings-config>*** > ***Network Services*** (ネットワーク サービス))、*DNS* サーバーと *DNS* サフィックスの両方について、ゲートウェイがエンドポイントに設定を送信します。これは、グローバル (ゲートウェイ単位) *DNS* サーバーおよび *DNS* サフィックスを設定する際にも該当します。

クライアント設定で *DNS* サーバーや *DNS* サフィックスを設定しない場合、設定済み (***Network*** (ネットワーク) > ***GlobalProtect*** > ***Gateways*** (ゲートウェイ) > ***<gateway-config>*** > ***Agent*** (エージェント) > ***Network Services*** (ネットワーク サービス)) であれば、ゲートウェイが グローバル *DNS* サーバーおよび *DNS* サフィックスをエンドポイントに送信します。

1. GlobalProtect Configuration Gateway（GlobalProtect 設定ゲートウェイ）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定）の順に選択します。
2. 既存のクライアント設定の構成を選択するか、新しく **Add**（追加）します。
3. 次のいずれかの **Network Services (ネットワーク サービス)** 設定を行います。
   - このクライアント設定を持つ GlobalProtect アプリケーションが DNS クエリを送る先となる **DNS Server (DNS サーバー)** の IP アドレスを指定します。各 IP アドレスをコンマで区切れば最大 10 件の DNS サーバーを追加できます。
   - エンドポイントが解決できない非修飾ホスト名に遭遇したときにエンドポイントがローカルで使用する **DNS Suffix (DNS サフィックス)** を指定します。

STEP 13 | （トンネル モードのみ）適切な設定が各 GlobalProtect アプリにデプロイされるように、ゲートウェイのエージェント設定を配置します。

アプリに接続すると、ゲートウェイは、パケットの送信元の情報を、定義したエージェント設定と比較します（**Agent**（エージェント） > **Client Settings**（クライアント設定））。セキュリティ ルール評価によって、ゲートウェイはリストの先頭から一致を検索します。一致が見つかると、ポータルは対応する設定をアプリに配信します。

- ゲートウェイ設定を設定のリストの上に移動するには、設定を選択して **Move Up**（上へ）をクリックします。
- ゲートウェイ設定を設定のリストの下に移動するには、設定を選択して **Move Down**（下へ）をクリックします。

STEP 14 | （トンネル モードのみ）（任意）IPv4 または IPv6 アドレスを、ゲートウェイに接続するすべてのエンドポイントの仮想ネットワーク アダプタに割り当てるために使用するグローバル IP アドレス プールを設定します。

このオプションを使用すると、ゲートウェイ設定で各クライアント設定の IP プールを定義するのではなく、ゲートウェイ レベルで IP プールを定義することで設定を簡素化できます。

IP プールの構成は、ゲートウェイ レベル（***Network***（ネットワーク） > ***GlobalProtect*** > ***Gateways***（ゲートウェイ） > ***<gateway-config>*** > ***Agent***（エージェント） > ***Client IP Pool***（クライアント ***IP*** プール））またはクライアント レベル（***Network***（ネットワーク） > ***GlobalProtect*** > ***Gateways***（ゲートウェイ） > ***<gateway-config>*** > ***Agent***（エージェント） > ***Client Settings***（クライアント設定） > ***<client-setting>*** > ***IP Pools***（***IP*** プール））のいずれかでのみ行う必要があります。

ゲートウェイ*IP*アドレスプールの設定時にアドレスオブジェクトを使用することはサポートされていません。

1. GlobalProtect Configuration Gateway（GlobalProtect 設定ゲートウェイ）ダイアログで、**Agent**（エージェント） > **Client IP Pool**（クライアント **IP** プール）の順に選択します。
2. ゲートウェイに接続するすべてのエンドポイントに IPv4 または IPv6 アドレスを割り当てるために使用する IP アドレス サブネットまたは範囲を **Add**（追加）します。IPv4またはIPv6のサブネットまたは範囲、あるいはその2つの組み合わせを追加できます。

   ゲートウェイへの適切なルーティングを確実に行うには、ゲートウェイ上の既存の IP プール（該当する場合）および LAN に物理的に接続されているエンドポイントに割り当てられたものとは異なる範囲の IP アドレスを使用する必要があります。プライベート IP アドレッシング スキームを使用することを推奨します。

STEP 15 | （トンネルモードのみ）エンドポイントのネットワーク設定を指定します。

非トンネル モードの内部ゲートウェイ設定では、*GlobalProtect* アプリは物理ネットワーク アダプタに割り当てられたネットワーク設定を使用するため、このネットワーク設定は不要です。

GlobalProtect Gateway Configuration (GlobalProtect ゲートウェイ設定) ダイアログ上で、**Agent (エージェント)** > **Network Services (ネットワーク サービス)** を選択してから、次のいずれかのネットワーク構成設定を行います：

- DHCP クライアントとして設定されたインターフェイスがファイアウォールにある場合、**Inheritance Source**（継承ソース）をそのインターフェイスに設定することで、DHCP クライアントで受信したものと同じ設定が GlobalProtect アプリに割り当てられます。また、オプションを有効化すると、継承元から **Inherit DNS Suffixes (DNS** サフィックスの継承**)** をすることこともできます。
- **Primary DNS**（プライマリ **DNS**）サーバー、 **Secondary DNS**（セカンダリ **DNS**）サーバー、**Primary WINS**（プライマリ **WINS**）サーバー、**Secondary WINS**（セカンダリ

WINS）サーバー、および**DNS Suffix**（**DNS** サフィックス）を手動で割り当てます。カンマで区切って複数の DNS サフィックス（最大100個）を入力できます。

DNS Suffix（***DNS*** サフィックス）に *ASCII* 以外の文字を含めることはできません。

STEP 16 | （任意）エンドポイントのデフォルトのタイムアウト設定を変更します。

GlobalProtect Gateway Configuration (GlobalProtect ゲートウェイ設定) ダイアログ上で、**Agent (エージェント)** > **Connection Settings (接続設定)** を選択し、Timeout Configuration (タイムアウト設定) エリアで次の設定を行います：

- 1 回のゲートウェイ ログイン セッションの最大 **Login Lifetime**（ログイン ライフタイム）を変更します（デフォルトのログインの有効期間は 30 日間です）。この期間中、**Inactivity Logout**（アイドル タイムアウト）の期間中にゲートウェイがエンドポイントから HIP チェックを受信する限り、ユーザーのログイン状態は保持されます。この期間が過ぎると、ログインセッションが自動的にログアウトされます。
- **Inactivity Logoutt**（アイドル タイムアウト）期間を変更して、非アクティブなセッションが自動的にログアウトするまでの時間を指定します（デフォルト期間は 3 時間です）。設定された時間内にゲートウェイがエンドポイントから HIP チェックを受信しなかった場合、ユーザーは GlobalProtect からログアウトされます。
- **Disconnect on Idle**（アイドル状態での切断）を変更して、アイドル状態のユーザがGlobalProtectからログアウトするまでの時間（分）を指定します（デフォルトの時間は180分です）。設定された時間内に GlobalProtect アプリが VPN トンネルを介してトラフィックをルーティングしなかった場合、ユーザーは GlobalProtect からログアウトされます。この設定は、オンデマンド接続方式のみを使用する GlobalProtect アプリに適用されます。

STEP 17 | (任意) SSL VPN トンネルの自動復旧を設定します。

SSL VPN トンネルの自動復旧を設定したことでネットワークが不安定、あるいはエンドポイントの状態が変わり、それにより GlobalProtect 接続が解除された場合、特定のゲートウェイのために GlobalProtect アプリケーションが VPN トンネルを自動的に確立し直すことを許可あるいは拒否することができます。

1. GlobalProtect Configuration Gateway（GlobalProtect 設定ゲートウェイ）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定）の順に選択します。
2. Authentication Cookie Usage Restrictions (認証用 Cookie 使用制限) で次のいずれかオプションを設定します：
   - このゲートウェイについて、GlobalProtect アプリケーションが VPN トンネルを自動的に復旧するのを防ぐ場合は、**Disable Automatic Restoration of SSL VPN (SSL VPN の自動復元を無効化)** します。
   - このゲートウェイについて、GlobalProtect アプリケーションが VPN トンネルを自動的に確立し直すことを許可する場合は、**Disable Automatic Restoration of SSL VPN (SSL VPN の自動復元を無効化)** を無効化 (クリア) します (デフォルト)。

STEP 18 | (任意) 認証用 Cookie に対して送信元 IP アドレスを強制するよう設定します。

エンドポイントの IP アドレスが Cookie の発効対象である元の送信元 IP アドレスに一致する場合、あるいはエンドポイントの IP アドレスが特定のネットワーク IP アドレス範囲に一致する場合にのみ、エンドポイントからの Cookie を GlobalProtect ポータルあるいはゲートウェイが許可するよう、設定を行うことができます。/24 あるいは /32 など、CIDR サブネット マスクを使用してネットワークの IP アドレス範囲を定義できます。例えば、公開送信元 IP アドレスが 201.109.11.10 であり、ネットワークの IP アドレス範囲のサブネット マスクが /24 に設定されているエンドポイントに対して認証用 Cookie がすでに発効されていた場合、ネットワーク IP アドレス範囲 201.109.11.0/24 内の公開送信元 IP アドレスを持つエンドポイントで認証用 Cookie が有効になります。

1. GlobalProtect Configuration Gateway（GlobalProtect 設定ゲートウェイ）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定）の順に選択します。
2. Authentication Cookie Usage Restrictions (認証用 Cookie 使用制限) セクションで **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override) (認証用 Cookie の使用を制限 (VPN トンネルあるいは認証のオーバーライドの自動復旧用))** してから、次のいずれかを設定します：
   - **The original Source IP for which the authentication cookie was issued (認証用 Cookie の元の発効対象である送信元 IP)** を選択すると、Cookie を使用しようとするエンドポイントの公開送信元 IP アドレスが、Cookie の元の発効対象であるエンドポイントの公開送信元 IP アドレスと同じである場合のみ、認証用 Cookie が有効になります。
   - **The original Source IP network range (元の送信元 IP ネットワーク範囲)** を選択すると、Cookie を使用しようとするエンドポイントの公開送信元 IP アドレスが、指定されたネットワークの IP アドレス範囲内である場合にのみ、認証用 Cookie が有効になります。**Source IPv4 Netmask (送信元 IPv4 ネットマスク)** あるいは **Source IPv6 Netmask (送信元 IPv6 ネットマスク)** を入力し、認証用 Cookie が有効であるネットワーク IP アドレス範囲のサブネット マスクを定義します (例えば、 **32** あるいは **128**)。

STEP 19 | (トンネル モードのみ) VPN トンネルから HTTP/HTTPS ビデオ ストリーミング トラフィックを除外します。

STEP 20 | （任意）ホスト情報プロファイル（HIP）を含むセキュリティ ルールが適用されるときにエンド ユーザーに表示される通知メッセージを定義します。

このステップは、ホスト情報プロファイルを作成して、セキュリティ ポリシーに追加した場合にのみ適用されます。HIP 機能の設定および HIP 通知メッセージの作成に関する詳細は、ホスト情報を参照してください。

1. GlobalProtect Configuration Gateway（GlobalProtect 設定ゲートウェイ）ダイアログで、**Agent**（エージェント） > **HIP Notification**（**HIP** 通知）の順に選択します。
2. 既存の HIP 通知設定を選択するか、新しく **Add**（追加）します。
3. 以下の設定を指定します。
   - このメッセージを適用する **Host Information**（ホスト情報）オブジェクトまたはプロファイルを選択します。
   - 対応するHIPプロファイルがポリシーで一致したときにメッセージを表示するかどうか、または一致しない場合は、**Match Message**（メッセージの一致）または**Not Match Message**（一致しないメッセージ）を選択し、通知を **Enable**（有効にする）を選択します。場合によっては、マッチの対象となるオブジェクトおよびポリシーの対象を基準に、一致する場合と一致しない場合の両方でメッセージの作成が必要になることがあります。**Match Message**（一致メッセージ）の場合、**Include Mobile App List**（一致したアプリケーションのリストをメッセージに含める）オプションを有効化して、どのアプリケーションが HIP マッチをトリガーできるのか指定することもできます。
   - **System Tray Balloon**（システム トレイ バルーン ）または **Pop Up Message**（ポップアップ メッセージ）のいずれでメッセージを表示するのかを選択します。
   - **Template (テンプレート)** にメッセージのテキストを入力してフォーマットしてから、**OK** をクリックします。
   - 定義する各メッセージについて、ここでの手順を繰り返します。

STEP 21 | ゲートウェイの設定を保存します。

1. **OK** をクリックして設定を保存します。
2. 変更を **Commit**（コミット）します。

STEP 22 | (任意) エンドユーザーの接続中にこのゲートウェイの位置を示すラベルを表示するよう GlobalProtect アプリケーションを設定する場合は、このゲートウェイを設定するファイアウォールの物理的な場所を指定します。

ネットワークのパフォーマンス低下など、エンドユーザーが異常な挙動を体験した場合、この位置情報をサポートやヘルプデスクの担当者に提供してトラブルシューティングをスムーズに進めることができます。また、この位置情報を使用してゲートウェイとの近さを判断す

ることもできます。この近さに基づき、より近いゲートウェイに切り替える必要があるかどうかを判断できます。

ゲートウェイの位置を指定しない場合、*GlobalProtect* アプリケーションの位置フィールドは空になります。

- **CLI** にて—次の CLI コマンドを使用し、ゲートウェイを設定したファイアウォールの物理的な位置を指定します：

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- **XML API** にて—次の XML API を使用し、ゲートウェイを設定したファイアウォールの物理的な位置を指定します：
  - デバイス—ゲートウェイを設定したファイアウォールの名前
  - ロケーション—ゲートウェイを設定したファイアウォールの位置

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

GlobalProtectゲートウェイでのスプリット トンネル トラフィック

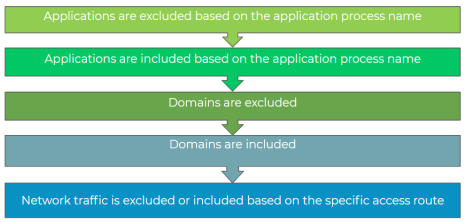
アクセスルート、宛先ドメイン、アプリケーション、HTTP / HTTPS ビデオ ストリーミング アプリケーションに基づいて、スプリット トンネル トラフィックを設定できます。

GlobalProtect サブスクリプションを活用すれば、スプリットルールを *Windows* および *macOS* エンドポイントに施行または適用できます。

スプリット トンネル機能により、帯域幅を節約し、トラフィックを以下にルーティングできます:

- エンタープライズ SaaS とパブリック クラウド アプリケーションをトンネルし、包括的な SaaS アプリケーションの可視性と制御を実現し、すべてのトラフィックをトンネリングできない環境でのシャドウ IT に関連するリスクを回避します。
- VoIP などのレイテンシの影響を受けやすいトラフィックを VPN トンネルの外に送信し、他のすべてのトラフィックは VPN を通過して、GlobalProtect ゲートウェイによる検査とポリシーの適用を行います。
- VPN トンネルから HTTP/HTTPS ビデオ ストリーミング トラフィックを除外します。YouTube や Netflix などのビデオストリーミング アプリケーションは、大量の帯域幅を消費します。VPN トンネルから低リスクのビデオ ストリーミング トラフィックを除外することで、ゲートウェイの帯域幅消費を減らすことができます。

スプリット トンネル ルールは、次の順番で Windows と macOS エンドポイントに適用されます:



ゲートウェイでスプリット トンネル トラフィックを設定する方法については、次のセクションを参照してください:

- アクセスルートベースのスプリット トンネルを設定する
- ドメインおよびアプリケーションベースのスプリット トンネルを設定する
- GlobalProtect VPNトンネルからのビデオトラフィックを除外する

アクセスルートベースのスプリット トンネルを設定する

ルートを包含または除外しない場合、すべての要求は VPNトンネル経由でルーティングされます（スプリット トンネルなし）。特定の宛先 IP サブネットトラフィックをVPNトンネル経由で送信しないようにしたり、除外したりできます。VPN トンネルを介して送信するルートは、トンネルに含めるルートとして、またはトンネルから除外するルートとして、あるいはその両方として定義できます。たとえば、スプリット トンネルを設定し、リモート ユーザーが VPN トンネ

ルを経由せずにインターネットに直接アクセスできるようにすることができます。具体性の高いルートのほうが具体性の低いルートよりも優先されます。

アクセスルートを追加するためにスプリットトンネルトラフィックを定義するとき、ゲートウェイがこれらのルートをリモート ユーザーのエンドポイントにプッシュするため、VPN トンネル経由で送信できるユーザーのエンドポイントが決まります。スプリットトンネルトラフィックを定義してアクセスルートを除外すると、これらのルートは、仮想アダプタ（トンネル）を介して GlobalProtect VPN トンネルを介して送信されるのではなく、エンドポイント上の物理アダプタを介して送信されます。 アクセスルートでスプリットトンネルトラフィックを除外することで、 VPN トンネルの外部に遅延の影響を受けやすいトラフィックや高帯域幅を消費するトラフィックを送信し、他のすべてのトラフィックを VPN 経由でルーティングして、GlobalProtect ゲートウェイによる検査とポリシーの適用を行うことができます。

ゲートウェイから送信されるルートよりも、ローカルのルートが優先されます。スプリット トンネルを有効化すると、ユーザーが VPN トンネル経由でローカル サブネット トラフィックを送信しなくても、直にプロキシおよびローカル リソース (ローカルのプリンターなど) に到達できるようになります。スプリット トンネルを無効化することで、ユーザーが GlobalProtect に接続されている時は常にすべてのトラフィックが必ず VPN トンネルを経由して検査され、ポリシーが適用されるようになります。ローカルネットワークへの直接アクセスオプションを有効化するか無効化するかに応じて、以下の IPv4 および IPv6 トラフィックの動作を検討します：

表 **1 : IPv4** トラフィックの動作

ローカル サブネットへの **IPv4** トラフィック	「ローカルネットワークへの直接アクセスなし」が有効		「ローカルネットワークへの直接アクセスなし」が無効	
	トンネルを確立する前	トンネルを確立した後	トンネルを確立する前	トンネルを確立した後
新しいインバウンド トラフィック	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	トラフィックが VPN トンネル経由で送信されます。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。
新しいアウトバウンド トラフィック	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	トラフィックが VPN トンネル経由で送信されます。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。
既存のトラフィック	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	トンネルを終了します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。

表 **2 : IPv6** トラフィックの動作

ローカル サブネットへの **IPv6** トラフィック	「ローカルネットワークへの直接アクセスなし」が有効		「ローカルネットワークへの直接アクセスなし」が無効	
	トンネルを確立する前	トンネルを確立した後	トンネルを確立する前	トンネルを確立した後
新しいインバウンド トラフィック	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。
新しいアウトバウンド トラフィック	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。
既存のトラフィック	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。	物理アダプタ経由でローカル サブネットのトラフィックを許可します。

アクセスルートを基準にスプリット トンネルを設定するには、以下の手順を実行します。

STEP 1 | 開始する前に：

1. GlobalProtect ゲートウェイの設定を行います。
2. **Network**（ネットワーク） > **GlobalProtect** > **Gateways(**ゲートウェイ**)** > ***<gateway-config>***を選択して既存のゲートウェイを変更するか、新しいゲートウェイを追加します。

STEP 2 | スプリット トンネルを有効化します。

1. **GlobalProtect Configuration Gateway (GlobalProtect** ゲートウェイの設定**)**ダイアログで **Agent** > **Tunnel Settings**（エージェント > トンネル設定)の順に選択して、**Tunnel Mode**（トンネルモード）を有効化します。
2. GlobalProtectアプリケーションのトンネル パラメータを設定します。

STEP 3 | （トンネル モードのみ）スプリット トンネルを無効化し、すべてのトラフィック (ローカル サブネット トラフィックを含む) が VPN トンネルを経由して検査され、ポリシーを適用されるようにする必要があります。

1. **GlobalProtect Gateway Configuration**（**GlobalProtect** ゲートウェイ設定）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定） > ***<client-setting-config>***を選択して、既存のクライアント設定を選択するか新しい設定を追加します。
2. **Split Tunnel (**スプリット トンネル**)** > **Access Route (**アクセス ルート**)** を選択してから、**No direct access to local network (**ローカルネットワークへの直接アクセスなし**)** オプションを有効化します。

   このオプションを有効化するとスプリット トンネル トラフィックが無効になり、ユーザーはトラフィックをプロキシまたはローカルリソースに *GlobalProtect* と接続中は送信できません。

STEP 4 | （トンネル モードのみ）アクセス経路に基づくスプリットトンネル設定を設定します。

スプリット トンネルの設定は、GlobalProtect アプリケーションがゲートウェイとトンネルを確立するときに、エンドポイント上の仮想ネットワーク アダプタに割り当てられます。

包含アクセス ルートと除外アクセス ルートで同じアクセス ルートを指定すると、間違った設定と認識されるため、同じアクセス ルートを指定しないでください。

宛先サブネットまたはアドレスオブジェクト（タイプ **IP Netmask**（**IP**ネットマスク））を指定することにより、特定のトラフィックをトンネルにルーティングしたり、トンネルから除外したりすることができます。

1. **GlobalProtect Gateway Configuration**（**GlobalProtect** ゲートウェイ設定）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定） > ***<client-setting-config>***を選択して、既存のクライアント設定を選択するか新しい設定を追加します。
2. 次のアクセス ルートベースの **Split Tunnel**（スプリット トンネル）設定（（**Split Tunnel**スプリット トンネル） > **Access Route**（アクセス ルート））を設定します：
   - （任意）GlobalProtect に一部のLAN を宛先にしているトラフィックなどをルーティングするには、**Includes**（包含）エリアで宛先のサブネットまたはアドレス オブジェクト（タイプは**IP Netmask**（ **IP** ネットマスク））を **Add**（追加）します。IPv6 または IPv4 サブネットを含めることができます。

     On PAN-OS 8.0.2以降のリリースでは、最大100のアクセスルートを使用して、スプリットトンネルゲートウェイ設定にトラフィックを含めることができます。GlobalProtectアプリケーションのバージョン4.1.x以降と組み合わせない限り、最大1,000件のアクセスルートを使用できます。
   - （任意）**Excludes**（除外）エリアで、アプリに除外させたい宛先のサブネットまたはアドレス オブジェクト（タイプは **IP Netmask**（IP ネットマスク））を **Add**（追加）します。除外するルートは、想定外のトラフィックが除外されることのないように、包含するルートよりも細かく指定してください。IPv6 または IPv4 サブネットを除外できます。ファイアウォールは、スプリット トンネル ゲートウェイ設定で最大100の除外アクセスルートをサポートします。GlobalProtectアプリケーションの

バージョン4.1.x以降と組み合わせない限り、最大200件の除外アクセスルートを使用できます。

Chromebook で *Android* を実行しているエンドポイントのアクセスルートを除外することはできません。*Chromebook* では *IPv4* ルートのみがサポートされています。

3. **OK** をクリックしてスプリット トンネルの設定を保存します。

STEP 5 | ゲートウェイの設定を保存します。

1. **OK** をクリックして設定を保存します。
2. 変更を **Commit**（コミット）します。

ドメインおよびアプリケーションベースのスプリット トンネルを設定する

宛先ドメインとポート（オプション）またはアプリケーションに基づくすべてのトラフィック（IPv4 および IPv6）を含むようにスプリット トンネルを設定すると、その特定のドメインまたはアプリケーションに向かうすべてのトラフィックは、検査とポリシーの実施のために VPN トンネルを介して送信されます。例えば、すべての Salesforce トラフィックが ***Salesforce.com** 宛先ドメインを使用して、 VPN トンネルを通過できるようにすることが可能です。VPN トンネルにすべての Salesforce トラフィックを含めることにより、Salesforceドメイン全体とサブドメインへの安全なアクセスを提供できます。宛先 IP アドレス サブネットを指定しなくても、スプリット トンネルを設定できるため、スプリット トンネル機能をドメインやアプリケーションに拡張することができます（SaaS やパブリック クラウド アプリケーションなどの動的なパブリック IP アドレス）。

宛先ドメインとポート（オプション）またはアプリケーションに基づいてトラフィック（IPv4 および IPv6）を除外するようにスプリット トンネルを設定すると、その特定のアプリケーションまたはドメインのすべてのトラフィックは、検査なしでエンドポイントの物理アダプタに直接送信されます。例えば、**C:\Program Files (x86)\Skype\Phone\Skype** アプリケーションプロセス名を使用して、すべてのSkype トラフィックを VPN トンネルから除外することができます。

Windows 7 Service Pack 2 以降のリリースおよび *macOS 10.10* 以降のリリースのエンドポイントでサポートされています。

次の手順を使用して、宛先ドメインまたはアプリケーションプロセス名に基づいてトラフィックを含めるか除外するようにスプリット トンネルを構成します。

STEP 1 | 開始する前に：

1. GlobalProtect ゲートウェイの設定を行います。
2. **Network**（ネットワーク） > **GlobalProtect** > **Gateways(ゲートウェイ)** > ***<gateway-config>*** を選択して既存のゲートウェイを変更するか、新しいゲートウェイを追加します。

STEP 2 | スプリット トンネルを有効化します。

1. **GlobalProtect Configuration Gateway (GlobalProtect** ゲートウェイの設定)ダイアログで **Agent** > **Tunnel Settings**（エージェント > トンネル設定)の順に選択して、**Tunnel Mode**（トンネルモード）を有効化します。
2. GlobalProtectアプリケーションのトンネル パラメータを設定します。

STEP 3 | （トンネル モードのみ）アクセス経路に基づいて分割トンネル設定を構成します。これらの設定は、GlobalProtect アプリがゲートウェイとトンネルを確立するときに、エンドポイント上の仮想ネットワーク アダプタに割り当てられます。

このスプリットトンネル設定は *macOS* エンドポイント上の *Sophos* と互換性がないため、宛先ドメインに基づいてスプリット トンネルを設定することはできません。この互換性がない問題を回避するには、

1. GlobalProtect Gateway Configuration（GlobalProtect ゲートウェイ設定）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定） > ***<client-setting-config>***を選択して、既存のクライアント設定を選択するか新しい設定を追加します。
2. （任意）宛先ドメインとポートを使用して、VPN 接続経由で GlobalProtect にルーティングしたいSaaS またはパブリック クラウド アプリケーションを **Add**（追加）します（**Split Tunnel**（スプリット トンネル） > **Domain and Application**（ドメインとアプリケーション） > **Include Domain**（ドメインを含む））。エントリを最大 200 個まで追加することができます。たとえば、**`*.gmail.com`** を追加すると、すべての Gmail トラフィックが VPN トンネルを通過できるようになります。
3. （任意）宛先ドメインとポートを使用して、VPN トンネルから除外する SaaS またはパブリッククラウドアプリケーションを **Add**（追加）します（**Split Tunnel**（スプリット トンネル） > **Domain and Application**（ドメインとアプリケーション） > **Exclude Domain**（ドメインを除外する））。エントリを最大 200 個まで追加することができます。たとえば、**`*.target.com`** を追加すると、すべての Target トラフィックが VPN トンネルから除外されます。
4. **OK** をクリックしてスプリット トンネルの設定を保存します。

STEP 4 | （トンネル モードのみ）アプリケーションに基づいてスプリットトンネル設定を構成します。

Safari トラフィックを *macOS* エンドポイントのアプリケーションベールのスプリット トンネル ルールに追加することはできません。

環境変数を使用して、*Windows* および *macOS* エンドポイント上のアプリケーションに基づいてスプリット トンネルを設定できます。

1. GlobalProtect Gateway Configuration（GlobalProtect ゲートウェイ設定）ダイアログで、**Agent**（エージェント） > **Client Settings**（クライアント設定） > ***<client-setting-config>***を選択して、既存のクライアント設定を選択するか新しい設定を追加します。
2. （任意）アプリケーションのプロセス名を使用して、VPN 接続経由で GlobalProtect にルーティングする SaaS またはパブリック クラウド アプリを **Add**（追加）します（**Split Tunnel**（スプリット トンネル） > **Domain and Application**（ドメインとアプリ

ケーション） > **Include Client Application Process Name**（クライアント アプリケーションのプロセス名を含む））。エントリを最大 200 個まで追加することができます。例えば、すべての RingCentral-based トラフィックが macOs エンドポイント上で VPN トンネルを通過できるようにするには、**/Applications/RingCentral for Mac.app/Contents/MacOS/Softphone** を追加します。

3. （任意）アプリケーションのプロセス名を使用して、VPN トンネルから除外する SaaS またはパブリック クラウド アプリケーションを **Add**（追加）します（**Split Tunnel**（スプリット トンネル） > **Domain and Application**（ドメインとアプリケーション） > **Exclude Client Application Process Name**（クライアント アプリケーションのプロセス名を除外））。エントリを最大 200 個まで追加することができます。たとえば、**/Applications/Microsoft Lync.app/Contents/MacOS/Microsoft Lync** を追加すると、すべての Microsoft Lync アプリケーション トラフィックが VPN トンネルから除外されます。
4. **OK** をクリックしてスプリット トンネルの設定を保存します。

STEP 5 | ゲートウェイの設定を保存します。

1. **OK** をクリックしてゲートウェイ設定を保存します。
2. 変更を **Commit (コミット)** します。

GlobalProtect VPNトンネルからのビデオトラフィックを除外する

特定のドメインへの HTTP/HTTPS ビデオ ストリーミング トラフィックが VPN トンネル経由で送信されないように、スプリット トンネルを設定できます。これにより、ビデオ トラフィックはエンドポイントの物理インターフェースから直接送信されます。ファイアウォールの App-ID 機能は、トラフィックをスプリット トンネリングする前にビデオ ストリームを識別します。VPN トンネルから低リスクのビデオ ストリーミング トラフィック（YouTube や Netflixなど）を除外することで、ゲートウェイの帯域幅消費を減らすことができます。

すべてのビデオ トラフィック タイプは、次のビデオ ストリーミング アプリケーション用にリダイレクトされます。

- YouTube
- Dailymotion
- Netflix

他のビデオ ストリーミング アプリケーションを VPN トンネルから除外すると、それらのアプリケーションでは次のビデオ トラフィック タイプのみがリダイレクトされます。

- MP4
- WebM
- MPEG

以下の手順を使用して、VPN トンネルからビデオ ストリーミング トラフィックを除外するスプリット トンネルを設定します。

STEP 1 | 開始する前に：

1. 以下の前提条件を満たしてください:
   - Windows 7 Service Pack 2 以降のリリースおよび macOS 10.10 以降のリリースのエンドポイントでサポートされています。
   - この場合、これらのエンドポイントの仮想ネットワークアダプタに IP アドレスを割り当てるために使用される IP プールに、IPv6 アドレスが含まれていないことを確認します。Windows または macOS エンドポイントの物理アダプタが IPv4 アドレスのみをサポートしている場合、エンドポイントの仮想ネットワーク アダプタに IPv6 アドレスを割り当てるように GlobalProtect ゲートウェイを設定すると、エンドポイント ユーザーは VPN トンネルから除外するビデオ ストリーミング アプリケーションにアクセスできず、 ゲートウェイに接続します。
   - VPN トンネルからビデオ ストリーミング トラフィックを除外する場合は、Firefox や Chrome などのウェブブラウザ アプリケーションを VPN トンネルに含めないでください。これにより、スプリット トンネル設定で競合するロジックがなくなり、ユーザーが Web ブラウザからビデオをストリーミングできるようになります。
   - Sling TV アプリケーションのトラフィックを VPN トンネルから除外するには、アプリケーションに基づきスプリット トンネルを設定してください。
2. GlobalProtect ゲートウェイの設定を行います。
3. **Network**（ネットワーク） > **GlobalProtect** > **Gateways(ゲートウェイ)** > ***<gateway-config>***を選択して既存のゲートウェイを変更するか、新しいゲートウェイを追加します。

STEP 2 | スプリット トンネルを有効化します。

1. **GlobalProtect Configuration Gateway (GlobalProtect** ゲートウェイの設定)ダイアログで **Agent** > **Tunnel Settings**（エージェント > トンネル設定)の順に選択して、**Tunnel Mode**（トンネルモード）を有効化します。
2. GlobalProtectアプリケーションのトンネル パラメータを設定します。

STEP 3 | (トンネル モードのみ) VPN トンネルから HTTP/HTTPS ビデオ ストリーミング トラフィックを除外します。

1. **GlobalProtect Gateway Configuration**（**GlobalProtect** ゲートウェイ設定）ダイアログで、**Agent**（エージェント） > **Video Traffic**（ビデオ トラフィック） の順に選択します。
2. **Exclude video applications from the tunnel**（トンネルから動画アプリケーションを除外）へのオプションを有効にします。

   このオプションを有効にしても、*VPN* トンネルから特定のビデオ ストリーミング アプリケーションを除外しないと、すべてのビデオ ストリーミング トラフィックが除外されます。
3. （任意）**Applications**（アプリケーション）リストを **Browse**（参照）参照すると、VPN トンネルから除外できるすべてのビデオ ストリーミング アプリケーションが表示されます。除外するアプリケーションの追加 ( ) アイコンをクリックします。た

とえば、**directv** の追加アイコンをクリックすると、VPN トンネルから DIRECTV ビデオ ストリーミング トラフィックが除外されます。

4. **Applications (アプリケーション)**ドロップダウン - 短縮版 **Applications (アプリケーション)** リストを使用して、VPN トンネルから除外するビデオ ストリーミング アプリケーションを **Add (追加)** します。リストには最大 200 のビデオ アプリケーション エントリを追加できます。たとえば、**youtube-streaming** を選択すると、すべての YouTube ベースのビデオ ストリーミング トラフィックが VPN トンネルから除外されます。

STEP 4 | ゲートウェイの設定を保存します。

1. **OK** をクリックしてゲートウェイ設定を保存します。
2. 変更を **Commit (コミット)** します。

paloalto TECHDOCS

GlobalProtect ポータル

GlobalProtect ポータルの概要

GlobalProtect ポータルは、GlobalProtect インフラストラクチャの管理機能を提供します。GlobalProtect ネットワークに参加するすべてのエンドポイントは、ポータルから設定情報を受信します。これには、使用可能なゲートウェイ、ゲートウェイへの接続に必要になる可能性のあるクライアント証明書などの情報が含まれます。ポータルは更に、macOS および Windows エンドポイント両方の GlobalProtect アプリ ソフトウェアの動作と配布を制御しています。

ポータルは、モバイル エンドポイントで使用する *GlobalProtect* アプリケーションを配布しません。モバイル エンドポイント用の *GlobalProtect* アプリケーションを取得するには、エンド ユーザーはデバイスのストアからアプリケーションをダウンロードする必要があります。*iOS* は *App Store*、*Android* は *Google Play*、*Chromebook* は *Chrome* ウェブストア、*Windows 10 UWP* は *Microsoft* ストア。しかし、モバイル エンドポイントがアクセスするゲートウェイを制御するのは、モバイル アプリケーションのユーザーに対してデプロイされるエージェント設定です。サポートされているバージョンの詳細については、GlobalProtect でサポートされている OS バージョンを参照してください。

GlobalProtect アプリ ソフトウェアを配布すると共に、GlobalProtect ポータルを設定すれば、HTML、HTML5、JavaScript テクノロジを使用する一般的なエンタープライズ Web アプリケーションへの安全なリモート アクセスを提供できます。ユーザーは GlobalProtect アプリ ソフトウェアをインストールすることなく、SSL 対応の Web ブラウザから安全なアクセスを利用できます。これは、パートナーや契約業者をアプリケーションにアクセスできるようにしたり、個人エンドポイントなどの管理対象外のアセットを安全に利用できるようにしたりしなければならない状況に便利です。GlobalProtect クライアントレス VPN を参照してください。

GlobalProtect ポータルを設定するための前提条件となるタスク

GlobalProtect ポータルを設定する前に、以下のタスクを完了する必要があります。

- ポータルを設定する予定のファイアウォールのためのインターフェイス（およびゾーン）を作成します。GlobalProtect のインターフェイスおよびゾーンの作成を参照してください。
- ポータル サーバー証明書、ゲートウェイ サーバー証明書、SSL/TLS サービス プロファイル、さらに必要に応じて、GlobalProtect™ サービスの SSL/TLS 接続を確立するためにエンド ユーザーにデプロイするクライアント証明書をセットアップします。GlobalProtect コンポーネント間の SSL の有効化を参照してください。
- ポータルが GlobalProtect ユーザーの認証に使用する任意の認証プロファイルおよび証明書プロファイルを定義します。認証を参照してください。
- GlobalProtect ゲートウェイの設定を行い、複数ゲートウェイ構成時のゲートウェイの優先順位を把握します。

GlobalProtect ポータルへのアクセスのセットアップ

GlobalProtect ポータルを設定するための前提条件となるタスクを完了した後に、以下のように GlobalProtect ポータルを設定します。

STEP 1 | ポータルを追加します。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択し、ポータルを**Add(追加)** します。
2. ポータルの **Name**（名前）を入力します。

   ゲートウェイ名にスペースを含めることはできず、各virtual system(仮想システム-vsys)に固有のものである必要があります。
3. （任意）**Location**（場所）フィールドから、このポータルが属する仮想システムを選択します。

STEP 2 | GlobalProtect アプリがポータルと通信できるように、ネットワークを設定します。

ポータル用のネットワーク インターフェイスをまだ作成していない場合は、GlobalProtect のインターフェイスおよびゾーンの作成を参照してください。ポータル用の SSL/TLS サービス プロファイルをまだ作成していない場合は、GlobalProtect コンポーネントへのサーバー証明書のデプロイを参照してください。

> *GlobalProtect* ポータルまたはゲートウェイを設定したインターフェイスで *HTTP*、*HTTPS*、*Telnet*、または *SSH* を許可するインターフェイス管理プロファイルを追加すると、インターネットからの管理インターフェイスへのアクセスを許可することになるため、追加しないでください。管理アクセスの保護のベスト プラクティスに従い、攻撃を阻止するようにファイアウォールへの管理アクセスを保護してください。

1. **General (全般)** を選択します。
2. Network Settings (ネットワーク設定) エリアで **Interface (インターフェイス)** を選択します。
3. ポータル Web サービスの **IP Address Type**（**IP** アドレス タイプ）と **IP address**（**IP** アドレス）を指定します。
   - IP アドレス タイプは、**IPv4**（のみ）、**IPv6**（のみ）、あるいは **IPv4 and IPv6 (IPv4** および **IPv6)** にできます。ネットワークがデュアル スタック構成をサポートしているときは、**IPv4 and IPv6**（**IPv4** および **IPv6**）を使用します。これにより IPv4 と IPv6 が同時に動作します。
   - IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 アドレス の場合は `172.16.1/0`、IPv6 アドレスの場合は `21DA:D3:0:2F3b` のように指定します。デュアル スタック構成の場合は、IPv4 アドレスと IPv6 アドレスの両方を入力します。
4. **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）を選択します。

STEP 3 | カスタムログインとヘルプページを選択するか、ログインページとヘルプページを完全に無効にします。カスタムログインページおよびヘルプページの作成についての詳細は、GlobalProtect ポータル ログイン、ウェルカム ページ、およびヘルプ ページのカスタマイズ を参照してください。

1. **General (全般)** を選択します。
2. Appearance (表示) エリアで次のいずれかを設定します：
   - ポータルへのユーザー アクセス用の **Portal Login Page**（ポータル ログイン ページ）を設定するには、**factory-default**（出荷時のデフォルト）ログインページを選択し、カスタム ログイン ページを **Import**（インポート）するか、ログイン ページへのアクセスを **Disable**（無効化）します。
   - **App Help Page**（アプリのヘルプ ページ）設定してGlobalProtectアプリユーザーを支援するには、**factory-default**（出荷時のデフォルト）ヘルプページを選択するか、カスタムヘルプページを**Import**（インポート）するか、**None**（なし）を選択して GlobalProtect ステータス パネルの設定メニューから**Help**（ヘルプ）オプションを削除します。

STEP 4 | ポータルがユーザーを認証する方法を指定します。

1. **Authentication**（認証）を選択します。
2. 次のいずれかのポータル認証を設定します：

   ポータルのサーバー証明書をまだ作成しておらず、ゲートウェイ証明書を発行していない場合は、GlobalProtect コンポーネントへのサーバー証明書のデプロイを参照してください。

   - ポータルと GlobalProtect アプリ間でセキュアな通信を行うために、そのポータル用に設定した **SSL/TLS Service Profile**（**SSL/TLS** サービス プロファイル）を選択します。
   - ローカル ユーザー データベース、または LDAP、Kerberos、TACACS+、SAML、RADIUS などの外部認証サービス（OTP を含む）でユーザーを認証する場合、GlobalProtect クライアント認証設定の定義を行います。
   - クライアント証明書またはスマート カード/CAC に基づいてユーザーを認証するには、対応する **Certificate Profile**（証明書プロファイル）を選択します。クライアント証明書を事前にデプロイするか、Simple Certificate Enrollment Protocol（SCEP）を使用して 認証用のユーザー固有のクライアント証明書のデプロイする必要があります。
     - ユーザーがユーザー認証情報およびクライアント証明書の両方を使ってポータルに認証することを求める場合、**Certificate Profile (証明書プロファイル)** および 認証プロファイル の両方が必要になります。
     - ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってポータルに認証するのを許可する場合、ユーザー認証用の認証プロファイルを選択します。**Certificate Profile (証明書プロファイル)**は任意項目になります。

- ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってポータルに認証するのを許可し、ユーザー認証用の認証プロファイルを選択しない場合、**Certificate Profile** (証明書プロファイル) は必須項目になります。
- 特定の OS にマッチする認証プロファイルを一切設定しない場合、**Certificate Profile** (証明書プロファイル) が必須項目になります。

ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使用してポータルに認証することを許可する場合、***Username Field*** (ユーザー名フィールド) を ***Subject*** (サブジェクト) あるいは ***Subject Alt*** (サブジェクト代替) に設定して ***Certificate Profile*** (証明書プロファイル) を選択します。

STEP 5 | ユーザーが正常にポータルに認証した後、接続中のエンドポイントから GlobalProtect アプリケーションが収集するデータを定義します。

GlobalProtect アプリケーションはこのデータをポータルに送信し、各ポータルのエージェント設定用に設定した選択条件と照合します。ポータルはこの条件に基づき、接続する GlobalProtect アプリケーションに特定のエージェント設定を配信します。

1. **Portal Data Collection** (ポータル データ収集) を選択します。
2. 次のいずれかのデータ収集を設定します：
   - GlobalProtect アプリケーションに接続中のエンドポイントからマシン証明書を収集させる場合、収集するマシン証明書を指定する **Certificate Profile** (証明書プロファイル) を選択します。
   - GlobalProtect アプリケーションに接続中のエンドポイントからカスタム ホスト情報を収集させる場合、Custom Checks (カスタム チェック) エリアで次のレジストリあるいは plist のデータを定義します：
     - Windows エンドポイントからレジストリ データを収集する場合、**Windows** を選択してから **Registry Key** (レジストリキー) および対応する **Registry Value** (レジストリ値) を **Add** (追加) します。
     - macOS エンドポイントから plist データを収集する場合、**Mac** を選択してから **Plist**キーおよび対応する **Key** (キー) の値を **Add** (追加) します。

STEP 6 | ポータルの設定を保存します。

1. **OK** をクリックして設定を保存します。
2. 変更を **Commit**（コミット）します。

GlobalProtect クライアント認証設定の定義

ユーザーによる GlobalProtect ポータルへの認証を可能にする設定は、各 GlobalProtect クライアント認証設定で指定します。各 OS 用に設定をカスタマイズするか、あらゆるエンドポイントを対象にした設定を行うことが可能です。例えば、Android ユーザーは RADIUS 認証を、Windows ユーザーは LDAP 認証を使用するように設定することができます。また、Web ブラウザからポータルに（GlobalProtect アプリをダウンロードするために）アクセスするユーザー用、または GlobalProtect ゲートウェイへのサードパーティの IPsec VPN（X-Auth）アクセス用のクライアント認証をカスタマイズすることもできます。

STEP 1 | GlobalProtect ポータルへのアクセスのセットアップを行います。

STEP 2 | ポータルがユーザーを認証する方法を指定します。

ローカル ユーザー データベース、または LDAP、Kerberos、TACACS+、SAML、RADIUS などの外部認証サービス（OTP を含む）でユーザーを認証するように GlobalProtect ポータルを設定できます。認証プロファイル/証明書プロファイルをまだセットアップしていない場合は、認証の指示を参照してください。

GlobalProtect ポータル設定のダイアログで（**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > ***<portal-config>***）、**Authentication**（認証）を選択して、以下の設定を含んだ新しい **Client Authentication**（クライアント認証）を**Add**（追加）します。

- このクライアント認証設定を識別する **Name**（名前）を入力します。
- この設定をデプロイするエンドポイントを指定します。この設定をすべてのエンドポイントに適用する場合は、**Any (すべて)** のデフォルトの **OS** を許可します。この設定を特定のオペレーティングシステムを実行しているエンドポイントに適用する場合は、**Android** などの **OS** を選択します。あるいは、ウェブ **Browser (ブラウザ)** から クライアントレス VPN ポータル に接続するエンドポイントにこの設定を適用することができます。
- ユーザーが自身のユーザー認証情報を使用してポータルあるいはゲートウェイに認証できるようにする場合は、**Authentication Profile (認証プロファイル)** を選択あるいは追加します。
  - ユーザーがユーザー認証情報およびクライアント証明書の両方を使ってポータルあるいはゲートウェイに認証することを求める場合、**Authentication Profile (認証プロファイル)** および 証明書プロファイルの両方が必要になります。
  - ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってポータルあるいはゲートウェイに認証するのを許可する場合、ユーザー認証用の認証プロファイルを選択します。**Authentication Profile (認証プロファイル)** は任意項目になります。
  - ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってポータルあるいはゲートウェイに認証するのを許可するものの、ユーザー認証用の認証プロファ

イルを選択しない (あるいは **Certificate Profile (**認証プロファイル**)** を **None (**なし**)** に設定する) 場合、**Authentication Profile (**認証プロファイル**)** が必須です。

- （任意） GlobalProtect ポータル ログインのカスタム **Username Label**（ユーザー名ラベル）を入力します（電子メール アドレス **(username@domain**等）。
- （任意）GlobalProtect ポータル ログイン用のカスタム **Password Label**（パスワード ラベル） を入力します（2 要素認証、トークンベースの認証の場合はパスコード）。
- (Optional) エンドユーザーがログイン時に使用する証明書を理解しやすくなるように、**Authentication Message**（認証メッセージ）を入力します。メッセージの最大長は 256 文字です。（デフォルトは `Enter login credentials`です）。
- 次のいずれかのオプションを選択し、ユーザーが認証情報かつ/またはクライアント証明書を使用してポータルに認証できるかどうかを定義します：
  - ユーザーがユーザー認証情報およびクライアント証明書の両方を使ってポータルに認証することを求める場合、**Allow Authentication with User Credentials OR Client Certificate (**ユーザー認証情報あるいはクライアント証明書による認証を許可**)** するオプションを **No (User Credentials AND Client Certificate Required) (**いいえ **(**ユーザー認証情報およびクライアント証明書が必要**))** (デフォルト) に設定します。
  - ユーザーがユーザー認証情報あるいはクライアント証明書のいずれかを使ってポータルに認証することを許可する場合、**Allow Authentication with User Credentials OR Client Certificate (**ユーザー認証情報あるいはクライアント証明書による認証を許可**)** するオプションを **Yes (User Credentials OR Client Certificate Required) (**はい **(**ユーザー認証情報あるいはクライアント証明書が必要**))** に設定します。

    このオプションを **Yes (**はい**)** に設定すると、GlobalProtect ポータルはまずエンドポイントのクライアント証明書を検索します。エンドポイントがクライアント証明書を持っていない、あるいはクライアント認証設定用の証明書プロファイルを設定していない場合、エンドユーザーは自身のユーザー認証情報を使用してポータルに認証する必要があります。

STEP 3 | リストの一番上にある**Any**（指定なし）の OS 固有の設定と、リストの一番下（**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > **<portal-config>** > **Authentication**（認証））にあるすべての OS に適用される設定で、クライアント認証構成を配置します。セキュリティ ルール評価によって、ポータルはリストの先頭から一致を検索します。一致が見つかると、ポータルは対応する設定をアプリに配信します。

- 設定のリストの上部にクライアントの認証設定を移動するには、設定を選択し、**Move Up**（上へ）をクリックします。
- 設定のリストの下部にクライアントの認証設定を移動するには、設定を選択し、**Move Down**（下へ）をクリックします。

STEP 4 | （任意）認証プロファイルおよび証明書プロファイルを使用する 2 要素認証を有効にするには、このポータル設定を両方とも構成します。

ユーザーがアクセスを得るためには、ポータルが事前に両方の方法を使ってエンドポイントを認証する必要があります。

(*Chrome のみ*) ポータルがクライアント証明書および *LDAP* を使用して *2* 要素認証を行うように設定する場合、*Chrome OS 47* 以降のバージョンを実行する *Chromebook* で、クライアント証明書を選択するために過剰なプロンプトが発生します。この過剰なプロンプトを防止するために、*Google* 管理コンソールでクライアント証明書を指定する設定を行ってから、ポリシーを管理対象の *Chromebook* にデプロイします。

1. Google 管理コンソールにログインし、***Device management*** (デバイス マネージャ) > ***Chrome management*** (*Chrome* 管理) > ***User settings*** (ユーザー設定) を選択します。
2. *Client Certificates* (クライアント証明書) セクションで次の *URL* パターンを入力し、***Automatically Select Client Certificate for These Sites*** (これらのサイトに対して自動的にクライアント証明書を選択) します：

   ```
   {"pattern": "https://[*.]","filter":{}}
   ```

3. ***Save***（保存）をクリックします。*Google* 管理コンソールが数分以内にすべてのデバイスにポリシーをデプロイします。

GlobalProtect Portal 設定ダイアログ（**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > ***<portal-config>***）で、**Authentication**（認証）を選択して **Certificate Profile**（証明書プロファイル）を選択し、クライアント証明書またはスマートカードに基づいてユーザーを認証します。

証明書の共通名（*CN*）フィールドと、該当する場合は、サブジェクトの別名（*SAN*）フィールドが、ポータルを設定するインターフェイスの *IP* アドレスまたは *FQDN* と完全に一致する必要があります。一致しない場合、ポータルへの *HTTPS* 接続を確立できなくなります。

STEP 5 | ポータルの設定を保存します。

1. **OK** をクリックして、設定を保存します。
2. 変更を **Commit**（コミット）します。

GlobalProtect エージェント設定の定義

GlobalProtect ユーザーがポータルに接続し、GlobalProtect ポータルによって認証されると、ポータルは定義した設定に基づいて、アプリにエージェント設定を送信します。固有の設定が必要なユーザーあるいはグループ用に別々のロールがある場合、各ユーザーのタイプあるいはユーザーグループ用に個別のエージェント設定を作成することができます。ポータルは、エンドポイ

ントの OS、およびユーザー名またはグループ名を使用して、デプロイするエージェント設定を判断します。他のセキュリティルールの評価と同じく、ポータルはリストの先頭から一致する項目を検索します。一致が見つかると、ポータルは設定をアプリに送信します。

設定には以下の情報を含めることができます。

- エンドポイントが接続できるゲートウェイのリスト。
- 外部ゲートウェイのうち、そのセッション用にユーザーが手動で選択できるいずれかのゲートウェイ。
- アプリが GlobalProtect ゲートウェイとの SSL 接続を確立できるようにするために必要なルート CA 証明書。
- SSL フォワード プロキシ復号化用のルート CA 証明書。
- 接続時にエンドポイントがゲートウェイに提示するクライアント証明書。アプリとポータルあるいはゲートウェイ間の相互認証が必要な場合のみ、この設定が必須になります。
- 接続時にエンドポイントがポータルまたはゲートウェイに提示しなければならない、安全に暗号化された Cookie。ポータルに生成を許可した場合にのみ、この Cookie が含められます。
- ローカル ネットワークまたは外部ネットワークのどちらに接続するかを決定するためにエンドポイントが使用する設定。
- エンドユーザーが表示される内容、ユーザーが GlobalProtect のパスワードを保存できるかどうか、ユーザーにソフトウェアのアップグレードを促すかどうかなどのアプリの動作設定。

ポータルがダウンまたは到達不能になっている場合、アプリは、最後に成功したポータル接続のアプリ設定（キャッシュされたバージョン）を使用して、アプリが接続できるゲートウェイ、ゲートウェイとの安全な通信を確立するために使用するルート CA 証明書、および使用する接続方式などの設定を取得します。

エージェント設定を作成するには、以下の手順を実行します。

STEP 1 | 1 つ以上の信頼されたルート CA 証明書をポータル エージェント設定に追加し、GlobalProtect アプリがポータルおよびゲートウェイの ID を確認できるようにします。

ポータルが証明書をデプロイする証明書ファイルは、GlobalProtect のみが読み取ります。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します
2. エージェント設定を追加するポータル設定を選択し、さらに**Agent**（エージェント）タブを選択します。
3. **Trusted Root CA**（信頼されたルート **CA**）フィールドで、ゲートウェイやポータルのサーバー証明書の発行に使用された CA 証明書を **Add**（追加）し、それを選択します。

   Web インターフェイスに、GlobalProtect ポータルとなるファイアウォールにインポートされる CA 証明書のリストが表示されます。Web インターフェイスは、選択できる

証明書のリストからエンドエンティティ証明書（リーフ証明書とも呼ばれる）も除外します。新しい CA 証明書を **Import**（インポート）することもできます。

証明書の作成と追加に関しては、以下のベスト プラクティスに従ってください。

- すべてのゲートウェイの証明書の発行に同じ証明書発行者を使用します。
- 証明書チェーン全体（信頼されたルート *CA* および中間 *CA* 証明書）をポータル エージェント設定に追加します。

4. （任意）GlobalProtect 以外の目的で追加の CA 証明書をデプロイします（たとえば、SSL フォワード プロキシ復号化）。

   このオプションにより、ポータルを使用して証明書をエンドポイントおよびエージェントにデプロイし、ローカルのルート証明書ストアにインストールできます。これは、他にこれらのサーバー証明書を配布する方法がない場合や、証明書の配布にポータルを使用するのが好ましい場合に便利な場合があります。

   SSL フォワード プロキシ復号化のためには、HTTPS 接続の終了、ポリシーに対するトラフィックの遵守状況の調査、暗号化されたトラフィックを転送するための HTTPS 接続の再確立にファイアウォールが使用するフォワード トラスト証明書を指定します（Windows および macOS エンドポイントのみ）。

   1. 前のステップで説明したように証明書を追加します。
   2. **Install in Local Root Certificate Store**（ローカルのルート証明書ストアにインストール）オプションを有効にします。

      ユーザーがポータルにログインする際にポータルが自動的にその証明書を送信し、エンドポイントのローカル ストアにインストールするため、ユーザーが証明書を手動でインストールする必要はありません。

STEP 2 | エージェント設定を追加します。

エージェントの設定によって、接続しているアプリにデプロイする GlobalProtect 設定が指定されます。少なくとも 1 つのエージェント設定を定義する必要があります。

1. ポータル設定（**Network (ネットワーク)** > **GlobalProtect** > **Portals (ポータル)** > ***<portal-config>***）で新しいエージェント設定を **Add (追加)** します。
2. 設定を識別する **Name**（名前）を入力します。複数の設定を作成する予定がある場合は、各設定に対して定義した名前が、それらを区別するのに十分に分かりやすいことを確認してください。

STEP 3 | （任意）この設定を持つユーザーがポータルに認証する方法を指定する設定を行います。

ゲートウェイがクライアント証明書を使用してエンドポイントを認証する場合は、証明書を配布するソースを選択する必要があります。

次のいずれかの **Authentication (認証)** 設定を行います。

- クライアント証明書を使用してポータルへのユーザー認証を行えるようにする場合、証明書およびその秘密鍵をエンドポイントに配布する**Client Certificate**（クライアント証明書）のソースを選択します（**SCEP**、**Local**、または**None**（なし））。内部 CA を使用して証明書をエンドポイントに配布する場合、**None(なし)** を選択します（デフォルト）。アプリがローカル証明書ストアに保存できるよう、ポータルがマシン証明書を生成・送信し、ポータルおよびゲートウェイの認証にその証明書を使用できるようにする場合、**SCEP** を選択し、さらに関連する SCEP プロファイルを選択します。これらの証明書はデバイス固有のものであり、発行の対象となったエンドポイント上でのみ使用できます。すべてのエンドポイントで同じ証明書を使用する場合、ポータルの **Local**（ローカル） にある証明書を選択します。**None**（なし）の場合、ポータルは証明書をエンドポイントにプッシュ送信しませんが、別の方法を用いて証明書をエンドポイントに提供できます。
- **Save User Credentials**（ユーザー認証情報を保存）するかどうかを指定します。**Yes**（はい）を選択するとユーザー名とパスワードを保存します（デフォルト）。ユーザー名のみ保存するには、**Save Username Only**（ユーザー名のみ保存）を選択します。ユーザーの生体情報（指紋）を保存するには**Only with User Fingerprint**（ユーザーの指紋のみ保存）、またiOS X エンドポイント専用で face ID credentials (顔 ID 認証)を選択します。また証明書を保存しない場合は**No(**いいえ） を選択します。

  ポータルまたはゲートウェイでワンタイムパスワード（OTP）などのダイナミックパスワードが求められるように設定した場合、ユーザーはログインするたびに新しいパスワードを入力する必要があります。この場合、GlobalProtect アプリでは、ユーザー名とパスワードの両方が保存されているセクションが指定されていても無視され、ユーザー名だけが保存されます。詳細については、1 回限りのパスワード（OTP）を使用した 2 要素認証の有効化を参照してください。

  GlobalProtect で**Save User Credentials**（ユーザー証明書を保存） **Only with User Fingerprint**（ユーザーの指紋のみ）を選択する場合、GlobalProtect は、GlobalProtect で認証を許可する前に、アプリケーションのユーザー検証用に、アプリケーションのオペレーティング システム機能を利用することができます。エンドユーザーは、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。iOS X 上で、GlobalProtect は Face ID による顔認証にも対応します。GlobalProtect は、認証に使用される指紋または顔のテンプレートを保存しませんが、オペレーティングシステムのスキャン機能を使用して、スキャンの一致の有効性を判断します。

STEP 4 | 内部ネットワーク内の GlobalProtect エンドポイントにトンネル接続を求めない場合は、内部ホスト検出を設定します。

1. **Internal (内部)** を選択します。
2. **Internal Host Detection (内部ホスト検出)** (**IPv4** あるいは **IPv6** のいずれか) を有効化します。
3. **IP Address**（**IP** アドレス） に内部ネットワークからのみ到達できるホストの IP アドレスを入力します。指定する IP アドレスは IP アドレス タイプ（(**IPv4** または**IPv6**）に対

応するものでなければなりません。たとえば、IPv4 の場合は 172.16.1.0、IPv6 の場合は 21DA:D3:0:2F3b のように指定します。

4. 入力した IP アドレス用の DNS **Hostname**（ホスト名）を入力します。GlobalProtect に接続するエンドポイントは、指定されたアドレスでリバース DNS ルックアップを試みます。このルックアップが失敗すると、エンドポイントはそれが外部ネットワーク上にあると判断し、外部ゲートウェイのリストにあるゲートウェイに向けてトンネル接続を開始します。

STEP 5 | サードパーティのモバイル エンドポイント管理システムへのアクセスをセットアップします。

この手順は、この設定を使用しているモバイル エンドポイントが サードパーティーのモバイル エンドポイント管理システムで管理される場合に必要になります。すべてのエンドポイントが最初にポータルに接続します。サードパーティーのモバイル エンドポイント管理システムが、対応するポータル エージェント設定で設定されている場合、エンドポイントは登録のためにリダイレクトされます。

1. モバイル エンドポイント管理システムに関連付けられているエンドポイント チェックイン インターフェイスの IP アドレスまたは FQDN を入力します。ここに入力する値は、エンドポイント チェックイン インターフェイスに関連付けられたサーバー証明書の値に厳密に一致する必要があります。IPv6 または IPv4 アドレスを指定できます。
2. モバイル エンドポイント管理システムが登録要求をリスンするポートを **Enrollment Port**（登録ポート）に指定します。この値はモバイル エンドポイント管理システムに設定された値と一致する必要があります（デフォルト = 443）。

STEP 6 | ポータルのエージェント設定の選択条件を指定します。

ポータルは、指定されているユーザー/ユーザー グループの設定を使用して、どの設定を接続する GlobalProtect アプリに配信するかを決定します。そのため、複数の設定がある場合は、設定を適切な順序に並べる必要があります。ポータルが一致を認めるとすぐに、設定が配信されます。そのため、より具体的な設定が、一般的な設定よりも優先される必要があります。エージェント設定のリストの順序付けの手順については、ステップ 12 を参照してください。

Config Selection Criteria (設定の選択条件**)** を選択してから次のいずれかのオプションを設定します：

- この設定を適用するユーザー、ユーザーグループ、オペレーティングシステムを指定するには、**User/User Group (**ユーザー**/**ユーザーグループ**)** を選択してから次のいずれかのオプションを設定します：
  - 特定のオペレーティング システム上で実行されているアプリにこの設定を配布するには、設定を適用する **OS** (**Android**、**Chrome**、**iOS**、**Linux**、**Mac**、**Windows**、または **WindowsUWP**) を **Add (**追加**)** して選択します。**OS** を **Any (**すべて**)** に設定し、設定をすべてのオペレーティングシステムにデプロイします。
  - この設定を特定のユーザーおよび/またはグループに制限するには、この設定を追加する **User/User Group**（ユーザー/ユーザー グループ）を **Add**（追加）して選択します。追加するユーザー/グループごとにこの手順を繰り返します。エンドポイントにまだログインしていないユーザーへの設定を制限するには、**User/User Group** (ユーザー/ユーザー グループ) ドロップダウン リストから **pre-logon** (プレ ログオン)を選択します。ロ

グイン ステータスに関わらず、すべてのユーザー (ログオン前およびログイン済みユーザーの両方) に設定をデプロイするには、**User/User Group (ユーザー/ユーザーグループ)** のドロップダウンリストで **any (任意)** を選択します。

特定のグループへの設定を制限するには、グループ マッピングの有効化で説明されているように、ユーザーをグループにマッピングする必要があります。

- 特定のデバイス属性に基づいてこの設定をアプリに配信するためには、**Device Checks (デバイス チェック)** を選択してから次のいずれかのオプションを設定します：
  - アクティブディレクトリあるいは Azure AD 内にエンドポイントのシリアル番号があるかどうかに基づいてこの設定を配信するためには、**Machine account exists with device serial number (デバイスのシリアル番号を持つマシン アカウントが存在)** のドロップダウンリストでオプションを選択します。このオプションを **Yes (はい)** に設定すると、存在するシリアル番号を持つエンドポイント (管理対象のエンドポイント) にのみエージェント設定が適用されるようになります。このオプションを **No (いいえ)** に設定すると、シリアル番号が存在しないエンドポイント (管理対象外のエンドポイント) にのみエージェント設定が適用されるようになります。このオプションを **None (なし)** に設定すると、エンドポイントのシリアル番号に基づいてアプリに設定が配信されなくなります。
  - エンドポイントのマシン証明書に基づいてこの設定を配信するためには、エンドポイントにインストールされたマシン証明書にマッチさせる **Certificate Profile (証明書プロファイル)** を選択します。
- カスタム ホスト情報に基づいてこの設定を配信するためには、**Custom Checks (カスタム チェック)** を選択します。**Custom Checks (カスタム チェック)** を有効化してから、次のいずれかのレジストリおよび plist データを定義します：
  - Windows エンドポイントが特定のレジストリキーを持っているかどうかを確認するには、次のいずれかのステップを使用します：
    1. 新しいレジストリキーを **Add (追加)** します (**Custom Checks (カスタム チェック)** > **Registry Key (レジストリキー)**)。
    2. 入力を求められたらマッチさせる **Registry Key (レジストリキー)** を入力します。
    3. (任意) エンドポイントが指定されたレジストリキーあるいはキー値を持っていない場合にのみこの設定を配信する場合は、**Key does not exist or match the specified value data (キーが存在しないか、指定した値データと一致しない)** を選択します。
    4. (任意) 特定のレジストリ値に基づいてこの設定を配信するためには、**Registry Value (レジストリ値)** および対応す る **Value Data (値データ)** を **Add (追加)** します。特定の

Registry Value (レジストリ値) あるいは **Value Data (値データ)** を持たないエンドポイントにのみこの設定を配信する場合は、**Negate (反転)** を選択します。

- 次のいずれかのステップで、macOS エンドポイントの plist 内に特定のエントリーがあるかどうかを確認できます：
  1. 新しい plist を **Add (追加)** します (**Custom Checks (カスタム チェック)** > **Plist**)。
  2. 入力を求められたら **Plist** の名前を入力します。
  3. (任意) エンドポイントが指定された plist を持っていない場合にのみこの設定を配信するためには、**Plist does not exist (plist** が存在しない**)** を選択します。
  4. (任意) plist 内の特定のキーと値ペアに基づいてこの設定を配信するには、**Add (追加)** をクリックして **Key (キー)** と対応する **Value (値)** を入力します。指定されたキーまたは値を明示的に持たないエンドポイントを照合する場合は、 **Negate (除外)** を選択します。

STEP 7 | この設定が行われたユーザーが接続できる外部ゲートウェイを指定します。

ゲートウェイを設定する際は、次の推奨設定を検討してください。

- 内部ゲートウェイと外部ゲートウェイの両方を同じ設定に追加している場合、***Internal Host Detection***（内部ホスト検出）を必ず有効にしてください（ステップ *4*）。
- *GlobalProtect* アプリが接続先のゲートウェイを判断する方法についての詳細は、複数ゲートウェイ構成時のゲートウェイの優先順位を参照してください。

1. **External (外部)** を選択します。
2. ユーザーが接続できる **External Gateways (外部ゲートウェイ)** を **Add (追加)** します。
3. **Name**（名前）フィールドに分かりやすいゲートウェイ名を入力します。ここに入力する名前は、ゲートウェイを設定したときに定義した名前と一致する必要があり、ユーザーが接続しているゲートウェイの場所を知ることができるように分かりやすい名前にする必要があります。
4. ゲートウェイが設定されているインターフェイスの FQDN または IP アドレスを **Address**（アドレス）フィールドに入力します。IPv4 または IPv6 アドレスを設定できます。指定するアドレスは、ゲートウェイ サーバー証明書に記載された共通名（CN）と完全に一致する必要があります。
5. ゲートウェイの 1 つ以上の **Source Regions**（送信元地域）を **Add**（追加）するか、**Any**（任意）を選択してゲートウェイをすべての地域で使用できるようにします。GlobalProtect はユーザーが接続した際に地域を認識して、その地域に設定された

ゲートウェイに対してのみユーザーの接続を許可します。ゲートウェイの選択では、送信元地域が考慮されてから、ゲートウェイの優先順位が考慮されます。

6. フィールドをクリックし、次のいずれかの値を選択して、ゲートウェイの **Priority**（優先順位）を設定します。
   - 1 つの外部ゲートウェイのみを使用している場合、**Highest**（最高）（デフォルト）に設定しておくことができます。
   - 複数の外部ゲートウェイを使用している場合、この設定が適用される特定のユーザー グループの選択を指示するために、優先順位の値を変更することができます（**Highest**（最高）から **Lowest**（最低）までの範囲）。たとえば、ローカル ゲートウェイよりもユーザー グループ接続を優先する場合、地理的に遠いゲートウェイよりも高い優先順位を設定します。優先順位の値は、エージェントのゲートウェイ選択アルゴリズムの重みづけに使用されます。
   - アプリがゲートウェイとの接続を自動的に確立する必要がない場合、**Manual only**（手動のみ）を選択します。この設定は、環境のテストに役立ちます。
7. **Manual**（手動）チェック ボックスをオンにして、ゲートウェイに手動で切り替えることをユーザーに許可します。

STEP 8 | この設定が行われたユーザーが接続できる内部ゲートウェイを指定します。

設定に内部ゲートウェイが含まれる場合、接続方式にオンデマンドを使用しないようにしてください。

1. **Internal (**内部**)** を選択します。
2. ユーザーが接続できる **Internal Gateways (**内部ゲートウェイ**)** を **Add (**追加**)** します。
3. **Name**（名前）フィールドに分かりやすいゲートウェイ名を入力します。ここに入力する名前は、ゲートウェイを設定したときに定義した名前と一致する必要があり、ユーザーが接続しているゲートウェイの場所を知ることができるように分かりやすい名前にする必要があります。
4. ゲートウェイが設定されているインターフェイスの FQDN または IP アドレスを **Address**（アドレス）フィールドに入力します。IPv4 または IPv6 アドレスを設定できます。指定するアドレスは、ゲートウェイ サーバー証明書に記載された共通名（CN）と完全に一致する必要があります。
5. （任意）ゲートウェイ設定に 1 つ以上の **Source Addresses**（送信元アドレス）を **Add**（追加）します。送信元アドレスには、IP サブネット、範囲、事前定義されたアドレスを使用できます。GlobalProtect は IPv6 アドレスと IPv4 アドレスの両方をサポートしています。GlobalProtect はユーザーが接続した際にエンドポイントの送信元アドレスを認識して、そのアドレスに設定されたゲートウェイに対してのみユーザーの接続を許可します。
6. **OK** をクリックして変更内容を保存します。
7. （任意）ゲートウェイ設定に **DHCP Option 43 Code**（**DHCP** オプション **43** コード）を **Add**（追加）します。DHCP サーバーがクライアントに提供するように設定されたベンダー固有の情報 （オプション 43）に関連付けられた 1 つ以上のサブオプショ

ン コードを含めることができます。たとえば、192.168.3.1 の IP アドレスに関連付けられたサブオプション コード 100 を含めることもできます。

GlobalProtect ポータルは、ユーザーが接続した際に GlobalProtect アプリにポータル設定に含まれるオプション コードのリストを送信し、アプリはオプションで指定されたゲートウェイを選択します。

送信元アドレスと DHCP オプションの両方を設定した場合、アプリに提示される使用可能なゲートウェイのリストは 2 つの設定の組み合わせ（結合）に基づきます。

DHCP オプションは *Windows* および *macOS* エンドポイントでのみサポートされています。*DHCP* オプションを使用して *IPv6* アドレス指定を使用するゲートウェイを選択することはできません。

8. （任意）企業ネットワークの内側にいるかどうかを GlobalProtect アプリが判断できるようにする場合は **Internal Host Detection**（内部ホスト検出）を選択します。ユーザーがログインを試みると、アプリは指定された **IP Address**（**IP** アドレス**)**）に対して内部 **Hostname**（ホスト名）のリバース DNS 検索を実行します。

   エンドポイントが企業ネットワーク内にある場合、ホストは到達可能なリファレンスポイントとなります。アプリがホストを検出したということは、エンドポイントがネットワーク内にあることを意味しており、アプリは内部ゲートウェイと接続します。アプリが内部ホストの検出に失敗した場合、アプリはネットワーク外にあることを意味しており、アプリは外部ゲートウェイに接続します。

   Internal Host Detection（内部ホスト検出）のアドレス指定の方法として **IPv4** または **IPv6** を設定できます。指定する IP アドレスは IP アドレス タイプに対応するものでなければなりません。たとえば、IPv4 の場合は 172.16.1.0、IPv6 の場合は 21DA:D3:0:2F3b のように指定します。

STEP 9 | この設定のユーザーに対して、GlobalProtect アプリケーションの動作をカスタマイズします。

必要に応じて **App (**アプリ**)** 設定を変更します。各オプションの詳細については、GlobalProtect アプリのカスタマイズを参照してください。

STEP 10 | （任意）アプリに収集または収集から除外させる必要がある HIP カテゴリのカスタム ホスト情報プロファイル（HIP）データを定義します。

この手順は、*HIP* 機能を使用する予定だが、標準 *HIP* オブジェクトを使用して収集できない情報を収集する必要がある場合、または収集と関係のない *HIP* 情報がある場合にのみ適用します。*HIP* 機能のセットアップおよび使用方法の詳細は、ホスト情報を参照してください。

カスタム *HIP* データの収集に関する詳細については、エンドポイントからのアプリケーションおよびプロセス データの収集を参照してください。

1. **HIP Data Collection (HIP** データ収集**)** を選択します。
2. GlobalProtect アプリケーションを有効化して **Collect HIP Data (HIP** データを収集**)** します。
3. アプリが HIP データの検索を行う **Max Wait Time (sec) (**最大待機時間 **(**秒**))**を 指定します。この時間が経過すると入手したデータが送信されます (範囲は 10～60 秒、デフォルトは 20 秒)。
4. GlobalProtect アプリケーションが送信するマシン証明書にマッチさせるために GlobalProtect ポータルが使用する **Certificate Profile (**証明書プロファイル**)** を選択します。
5. **Exclude Categories**（除外カテゴリ）を選択し、特定のカテゴリおよび/またはベンダー、アプリケーション、またはカテゴリ内のバージョンを除外します。詳細については、 HIP ベースのポリシー適用の設定 を参照してください。
6. **Custom Checks**（カスタム チェック）を選択し、このエージェント設定を実行しているホストから収集するカスタム データを定義し、カテゴリおよびベンダーを追加します。

STEP 11 | エージェント設定を保存します。

OK をクリックして、エージェント設定を保存します。

STEP 12 | 適切な設定が各アプリにデプロイされるように、エージェント設定を配置します。

アプリに接続すると、ポータルは、パケットの送信元の情報を、定義したエージェント設定と比較します。セキュリティ ルール評価によって、ポータルはリストの先頭から一致を検索します。一致が見つかると、ポータルは対応する設定をアプリに配信します。

- エージェント設定を設定のリストの上に移動するには、設定を選択して **Move Up**（上へ）をクリックします。
- エージェント設定を設定のリストの下に移動するには、設定を選択して **Move Down**（舌へ）をクリックします。

STEP 13 | ポータルの設定を保存します。

1. **[OK]** をクリックしてポータルの設定を保存します。
2. 変更を **Commit**（コミット）します。

GlobalProtect アプリのカスタマイズを定義する

ポータル エージェントの設定では、エンド ユーザ がエンドポイントにインストールされている GlobalProtect アプリと対話する方法をカスタマイズできます。アプリの表示と動作をカスタマイズしたり、作成したさまざまな GlobalProtect エージェント設定に異なるアプリ設定を定義することができます。たとえば、次の項目の指定が可能です。

- どのメニューとビューにユーザーがアクセスできるか。
- ユーザーがアプリケーションをアンインストールまたは無効にできるかどうか（ユーザー ログオン接続方式のみ）。
- 正常ログイン時にウェルカム ページを表示するかどうか。ユーザーがウェルカムページを閉じることができるかどうかを設定したり、GlobalProtect ポータルのログインページ、ウェルカムページ、ヘルプページをカスタマイズして、環境内で GlobalProtect を使用する方法を説明することもできます。
- GlobalProtect アプリが自動的にアップグレードされるか、ユーザーに手動でアップグレードするかを確認するかどうか。
- 機密ネットワーク リソースにアクセスするために多要素認証が必要かどうかをユーザーに確認するかどうか。

また、Windows レジストリ、Windows インストーラ（Msiexec）、およびグローバル macOS plist でアプリの設定を定義することもできます。Web インターフェイス（ポータルのエージェント設定）で定義された設定は、Windows レジストリ、Msiexec、および macOS plist で定義されている設定よりも優先されます。詳細については、アプリの設定の透過的なデプロイを参照してください。

Windows レジストリまたは Windows インストーラ（Msiexec）を介してのみ使用できる追加の設定では、次のことが可能になります。

- Windows SSO が失敗した場合、アプリがエンドユーザーに証明書を要求するかを指定します。
- デフォルトポータル IP アドレス（またはホスト名）を指定します。
- ユーザーがエンドポイントにログインする前に GlobalProtect が接続を開始できます。
- GlobalProtect が接続を確立する前後、または GlobalProtect が接続を解除した後に実行されるスクリプトをデプロイできます。
- サードパーティの証明書プロバイダを使用するときに SSO を有効にして、Windows エンドポイントでサードパーティの証明書をラップするように GlobalProtect アプリを構成します。

詳細情報は、カスタマイズ可能なアプリの設定を参照してください。

STEP 1 | カスタマイズするエージェント設定を選択します。

また、*Windows* レジストリ、*Windows Installer*（*Msiexec*）、および *macOS plist* からほとんどのアプリケーション設定を構成することもできます。ただし、*Web* インターフェイスで定義された設定は、*Windows* レジストリ、*Msiexec*、および *macOS plist* で定義されている設定よりも優先されます。詳細については、アプリの設定の透過的なデプロイを参照してください。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します
2. エージェント設定を追加するポータルを選択するか、新しいものを **Add**（追加）します。
3. **Agent**（エージェント）タブで、変更するクライアントの設定を選択します。または、新しい設定を **Add**（追加）します）。
4. **App**（アプリケーション）タブを選択します。

   App Configurations（アプリケーション設定）エリアには、各エージェント設定に対してカスタマイズ可能なアプリ設定がデフォルトの値と共に表示されます。デフォルトの動作を変更する際、テキスト色がグレイからデフォルトに切り替わります。

STEP 2 | アプリが GlobalProtect 接続に使用する **Connect Method**（接続方式）を指定します。

内部ゲートウェイを使用してネットワークにアクセスするには、接続方法として ***Pre-logon (Always On)***（ログオン前（常時オン））、***Pre-logon then On-demand***（ログオン前、次にオンデマンド）、または ***User-log on (Always On)***（ユーザー ログオン（常時オン））を使用します。

アプリ設定の領域で、次の **Connect Method**（接続方式）オプションのいずれかを選択します。

- **User-logon (Always On)**（ユーザー ログオン（常時オン）） – ユーザーがエンドポイント（またはドメイン）にログインすると、ただちに GlobalProtect アプリが自動的にポータルに接続します。SSO と併用されると（Windows エンドポイントのみ）、GlobalProtect ログインはエンド ユーザーに透過的になります。

  iOS エンドポイントでは、この設定により、*1* 回限りのパスワード（*OTP*）アプリケーションが機能しなくなります。これは、*GlobalProtect* が強制的にすべてのトラフィックでトンネルを経由させるためです。

- **Pre-logon (Always On)**（ログオン前（常時オン）） – GlobalProtect アプリが、ユーザーがエンドポイントにログインする前にユーザーを認証し、GlobalProtect ゲートウェイへの VPN トンネルを確立します。このオプションでは、この設定を受け取る各エンドポイントに対し、外部の PKI ソリューションを使用してマシン証明書を事前にデプロイしておくこ

とが必要になります。プレ ログオンの詳細についてはプレ ログオンを伴うリモート アクセス VPNを参照してください。

- **On-demand (Manual user initiated connection)**（オンデマンド（ユーザーによる手動接続））– ユーザーは、GlobalProtect に接続するために、アプリを手動で起動する必要があります。外部ゲートウェイのみの場合、この接続方式を使用します。
- **Pre-logon then On-demand**（ログオン前、次にオンデマンド）– **Pre-logon (Always On)**（ログオン前（常時オン））の接続方式と同じく、（コンテンツ リリース バージョン 590-3397 以降が必要な）この接続方式では、ユーザーがエンドポイントにログインする前に GlobalProtect アプリがユーザーを認証し、GlobalProtect ゲートウェイとの VPN トンネルを確立できます。プレ ログオン接続方式と異なり、エンドポイントにログインした後、接続が何らかの理由で切断された場合、ユーザーは手動でアプリを起動して GlobalProtect に接続する必要があります。このオプションの利点は、パスワードの有効期限が切れた後、またはパスワードを忘れた後にユーザーが新しいパスワードを指定できるようにすることができますが、ログイン後にユーザーが手動で接続を開始する必要があることです。

STEP 3 | ネットワーク アクセス用に GlobalProtect 接続を強制するかどうかを指定します。

ネットワークアクセスの際に *GlobalProtect* を強制する場合、***User-logon***（ユーザーログオン）または ***Pre-logon***（ログオン前）モードで接続するユーザーに対してのみこの機能を有効にすることを推奨します。***On-demand***（オンデマンド）モードで接続するユーザーは、猶予時間内に接続を確立できない可能性があります。

App Configurations（アプリケーション設定）エリアで以下のオプションのいずれかを設定します。

- すべてのネットワーク トラフィックに対して GlobalProtect トンネルの使用を強制する場合は、**Enforce GlobalProtect Connection for Network Access**（ネットワークアクセスの際に必ず **GlobalProtect** 接続を利用する）を **Yes**（はい）に設定します。デフォルトでは、GlobalProtect はネットワーク アクセスに必須ではありません。つまり、GlobalProtect が無効または切断されている状態でも、ユーザーはインターネットにアクセスすることができます。トラフィックがブロックされる前にユーザーに指示を出す場合、GlobalProtect を **Displays Traffic Blocking Notification Message**（トラフィック ブロックの通知メッセー

ジを表示する）に設定し、さらに任意でメッセージを表示するタイミングを指定します（**Traffic Blocking Notification Delay**（トラフィックブロックの通知遅延））。

> ***Enforce GlobalProtect Connection for Network Access***（ネットワークアクセスの際に必ず ***GlobalProtect*** 接続を利用する）を有効にする場合、ユーザーがパスコードで *GlobalProtect* アプリを無効にすることを許可するかどうか検討してください。***Enforce GlobalProtect Connection for Network Access***（ネットワークアクセスの際に必ず ***GlobalProtect*** 接続を利用する） 機能により、ネットワーク アクセスに *GlobalProtect* 接続が必要となるため、ネットワークの安全性が高まります。ごくまれに、エンドポイントが *VPN* への接続に失敗し、トラブルシューティングのためにリモート管理ログインが必要になることがあります。トラブルシューティング セッション中に管理者が提供したパスコードを使用して *GlobalProtect* アプリ（Windows 用または macOS 用）を無効にすると、管理者が遠隔操作でエンドポイントに接続することを許可することになります。

- **Enforce GlobalProtect Connection for Network Access**（ネットワークアクセスの**GlobalProtect** 接続を強制）が有効になっており、**GlobalProtect Connection**（**GlobalProtect** 接続）が確立されていない時に、特定のホスト/ネットワークへのトラフィックを許可するためには、これらの IP アドレスを入力して、特定のローカルアドレスまたはネットワークアクセスのネットワークセグメントの除外を設定します。ネットワークアクセスに GlobalProtect を強制していて、GlobalProtect が接続を確立できない場合に、アクセスを許可する IP アドレスまたはネットワークセグメントを最大10個指定します。

  > このオプションでは、コンテンツ リリース バージョン*8196-5685*以降が必要になります。

  除外を設定すると、GlobalProtectが切断されているときにユーザーがローカルリソースにアクセスできるようになり、ユーザーエクスペリエンスを向上させることができます。たとえば、GlobalProtectが 接続されていない場合、GlobalProtect はリンクローカルアドレスへのアクセスを許可できます。これにより、ユーザーはローカルネットワークセグメントまたはブロードキャストドメインにアクセスできます。

- ユーザーがインターネットにアクセスするためにキャプティブポータルにログインしなければならない場合、**Captive Portal Exception Timeout (sec) (**キャプティブポータルの例外タイムアウト **(**秒**))** を指定し、ユーザーがキャプティブポータルにログインできる期間 (秒単位) を示します (範囲は 0～3600 秒、デフォルトは 0 秒)。この期間中にユーザーがログインしない場合、キャプティブポータルのログインページがタイムアウトし、ユーザーがネットワークを使用できなくなります。

  GlobalProtect アプリケーションがキャプティブポータルを検出した際に通知メッセージを表示するには、**Display Captive Portal Detection Message (**キャプティブポータルの検知メッセージの表示**)** を **Yes (**はい**)** に設定します。**Captive Portal Notification Delay (sec) (**キャプティブポータルの通知遅延 **(**秒**))** フィールドに、GlobalProtect アプリケーションがこのメッセージを表示するまでの時間 (秒単位) を入力します (範囲は 1～120 秒、デフォルトは 5 秒)。キャプティブポータルが検出された後、しかしインターネットに到達可能になるまでに、GlobalProtect はこのタイマーを開始します。また、**Captive Portal Detection**

Message (キャプティブポータル検知メッセージ**)** を設定して追加の指示を出すこともできます。

キャプティブ ポータルの検出時にデフォルトのウェブブラウザを自動的に起動してユーザーがキャプティブ ポータルにシームレスにログインできるようにするには、**Automatically Launch Webpage in Default Browser Upon Captive Portal Detection**（キャプティブ ポータルの検出時にデフォルトのブラウザでウェブページを自動的に起動する）フィールドに完全修飾ドメイン名-FQDNまたはデフォルトのウェブブラウザの起動時にウェブトラフィックを開始する最初の接続試行に使用するウェブサイトの IP アドレス（最大長は256文字）を入力します。次に、キャプティブ ポータルはこのウェブサイト接続の試行を一旦遮断し、デフォルトのウェブブラウザをキャプティブ ポータルのログインページにリダイレクトします。このフィールドが空の場合（デフォルト）、GlobalProtect はキャプティブ ポータルの検出時にデフォルトのウェブブラウザを自動的に起動しません。

これらのオプションを使用するには、コンテンツ リリース バージョン *607-3486* 以降が必要になります。キャプティブポータルの通知遅延 では、コンテンツ リリース バージョン *8118-5277* 以降が必要になります。***Automatically Launch Webpage in Default Browser Upon Captive Portal Detection***（キャプティブ ポータルの検出時にデフォルトのブラウザでウェブページを自動的に起動する）オプションには、*2019*年*7*月*8*日以降にリリースされたコンテンツリリースバージョンが必須です。

STEP 4 | さらに GlobalProtect 接続設定を追加します。

シングル サインオン（*SSO*）が有効になっている場合（デフォルト）、*GlobalProtect* アプリはユーザーの *Windows* ログイン認証情報を使用して、*GlobalProtect* ポータルおよびゲートウェイに対する認証と接続を自動的に行います。これにより、*GlobalProtect* アプリはサードパーティの証明書をラップして、*Windows* ユーザーがサードパーティの認証情報プロバイダであっても認証して接続できるようにします。

App Configurations（アプリケーション設定）エリアで以下のオプションのいずれかを設定します。

- (Windows および macOS のみ; macOS のサポートには、コンテンツリリースのバージョン 8196-5685 以降が必要です) **Use Single Sign-On**（シングル サインオンの使用）

(Windows) または **Use Single Sign-On**（シングル サインオンの使用） **(macOS)** を **No**（いいえ）に設定すると、シングル サインオンが無効になります。

> SAML authentication (SAML 認証) を通じてユーザーを認証し、また認証をオーバーライドするために Cookie を生成して許可 するよう *GlobalProtect* ゲートウェイを設定する場合、ユーザーの *Windows* ユーザー名がその *SAML* ユーザー名と異なるとき (例えば、*Windows* ユーザー名が「*user*」であり、*SAML* ユーザー名が「*user123*」)、あるいはいずれかのユーザー名が完全修飾ドメイン名を含むとき (例えば、*Windows* ユーザー名が「*user*」であり、*SAML* ユーザー名が「*user@example.com*」)は ***Use Single Sign-On*** (シングル サインオンの使用) オプションを ***No*** (いいえ) に設定する必要があります。

- GlobalProtect アプリケーションに **Automatically Use SSL When IPSec Is Unreliable (IPSec を信頼できない場合に自動的に SSL を使用)** させる時間 (時間単位) を指定します (範囲は 0～168 時間)。このオプションを指定すると、GlobalProtect アプリケーションは指定された期間中、IPSec トンネルを確立しようとしなくなります。このタイマーは、トンネルのキープアライブがタイムアウトしたことで IPSec トンネルがダウンする度に開始されます。

  デフォルトの値である **0** を採用すると、アプリが IPSec トンネルを正常に確立できた場合に SSL トンネルを確立するというフォールバックが行われません。IPSec トンネルを確立できない場合にのみ SSL トンネルにフォールバックします。

  > このオプションでは、*2019*年*7*月*8*日以降にリリースされたコンテンツ リリース バージョンが必要になります。

- GlobalProtect アプリケーションの SSL 接続オプションを選択します。最高のユーザーエクスペリエンスを提供するために、SSL 接続のみを強制するか、SSL 接続を禁止するか、ま

たは地理的位置とネットワークパフォーマンスに応じてユーザーが SSL またはIPSec（デフォルト）を選択できるようにするかを選択できます。

App Configure（アプリケーション設定）領域で、許可した**Connect with SSL Only**（**SSL** のみで接続）オプションを選択します。

このオプションでは、コンテンツ リリース バージョン *8207-5750* 以降が必要になります。

- **Yes**（はい）—すべての GlobalProtect クライアントに SSL のみ使用することを要求します。
- **No**（いいえ）—VPN 接続用にゲートウェイで接続されたプロトコルで接続します。ゲートウェイ設定で IPSec が有効になっている場合、VPN 接続に IPSec が使用されます。ゲートウェイに SSL が設定されている場合は、VPN 接続に SSL を使用します。
- **User can Change**（ユーザーが変更可能）—ユーザーが GlobalProtect アプリケーションで SSL または IPSec のどちらを使用するか変更することを許可します。

  ユーザーはアプリケーション上で**Settings**（設定） > **General**（一般）を選択して、**Connect with SSL Only**（**SSL** のみで接続）と**Settings**（設定） > **Connection**（接続）を有効にして、**Protocol**（プロトコル）が **SSL** であることを検証できます。

- **Maximum Internal Gateway Connection Attempts**（内部ゲートウェイ接続の最大試行回数）を入力し、GlobalProtect アプリから内部ゲートウェイへの接続が失敗した場合に接続を試行できる回数を指定します（範囲は 0～100、4～5 を推奨、デフォルトは 0）。0 の場合、GlobalProtect アプリは接続の再試行を行いません。この値を大きくすることで、一時的にダウンしたり到達できないが、指定した回数の再試行が終わる前に復帰する内部ゲートウェイにアプリを接続できるようにすることができます。また、この値を増やすことで、内部ゲートウェイが最新のユーザー情報およびホスト情報を確実に受信できるようになります。
- **GlobalProtect App Config Refresh Interval**（**GlobalProtect** アプリ設定の更新間隔）を入力し、GlobalProtect ポータルがクライアントの設定を更新する間隔（時間数）を指定します（範囲は 1～168、デフォルトは 24）。
- （Windows のみ） セキュリティ要件に応じて、**Retain Connection on Smart Card Removal**（スマートカードの取り外し時に接続を維持）を指定します。デフォルトではこのオプションが **Yes**（はい）に設定されており、クライアント証明書が含まれたスマートカードをユーザーが取り外しても、GlobalProtect はトンネルを維持します。トンネルを切断するには、このオプションを **No**（いいえ）に設定します。

  この機能を使用するには、コンテンツ リリース バージョン *590-3397* 以降が必要になります。

- **Automatic Restoration of VPN Connection Timeout**（**VPN** 接続の自動復元のタイムアウト）を設定して、トンネルが切断されたときに GlobalProtect が実行するアクションを指定します。このオプションを **Yes**（はい）に設定すると、トンネルが切断された後に GlobalProtect が接続の再確立を試みます。このオプションを **No**（いいえ）に設定すると、トンネルが切断された後に GlobalProtect が再接続を試みるのを防ぎます。**Wait Time Between VPN Connection Restore Attempts**（**VPN** 再接続を試行するまでの待機時間） を

設定して、GlobalProtect が接続を復元しようとする間に待機する時間（秒単位）を調整します（範囲は1～60秒、デフォルトは 5 です）。

接続方式常時オンが機能しており、タイムアウト値が切れる前にユーザーが外部ネットワークから内部ネットワークに切り替えると、*GlobalProtect* はネットワーク探索を実行しません。そのため、*GlobalProtect* は最後に検出していた外部ゲートウェイへの接続を復元します。内部ホストの検出をトリガするには、*GlobalProtect* のステータスパネルの設定メニューから ***Refresh Connection***（リフレッシュ接続）を選択する必要があります。

STEP 5 | エージェント設定を持つユーザーが利用できるメニューおよび UI ビューを設定します。

App Configurations（アプリケーション設定）エリアで以下のオプションのいずれかを設定します。

- アプリケーションの基本的なステータス情報のみをユーザーに表示する場合は、**Enable Advanced View**（詳細ビューの有効化 ）を **No**（いいえ） に設定します。このオプションを無効にすると、ユーザーは以下のタブから情報を閲覧することができます:
  - **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。
  - **Notification**（通知）—GlobalProtect 通知を表示します。

  デフォルトは **Yes(**はい）です。このオプションを有効にすると、ユーザーは次の追加タブを閲覧できます:
  - **Connection**（接続）—GlobalProtect アプリケーション用に設定されたゲートウェイと、各ゲートウェイに関する情報を一覧表示します。
  - **Host Profile**（ホスト プロファイル）— GlobalProtect が HIP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。
  - **Troubleshooting**（トラブルシューティング）—ネットワーク設定、ルート設定、有効な接続、およびログに関する情報を表示します。GlobalProtect が生成したログを収集したり、ログ生成レベルを設定することもできます。
- エンドポイントで GlobalProtect システムトレイ アイコンを非表示にするには、**Display GlobalProtect Icon**（**GlobalProtect** アイコンの表示）を**No**（いいえ） に設定します。アイコンを非表示にすると、ユーザーは、パスワードの変更、ネットワークの再検出、ホスト情報の再送信、トラブルシューティング情報の表示、要求時接続の実行など、他のタスクを実行できません。しかし、必要に応じて、HIP 通知メッセージ、ログインプロンプト、および証明書ダイアログは表示されるようになっています。
- ユーザーがネットワーク検出を実行しないようにするには、**Enable Rediscover Network Option**（ネットワークオプションの再検出の有効化）を **No**（いいえ）に設定します。このオプションを無効にすると、GlobalProtect のステータスパネルの設定メニューで **Refresh Connection**（接続のリフレッシュ）オプションが灰色に表示されます。
- ユーザーに HIP データをゲートウェイに手動で再送信させないようにするには、**Enable Resubmit Host Profile Option**（ホスト プロファイルの再送信オプションの有効化）を **No**（いいえ）に設定します。このオプションはデフォルトで有効になっており、HIP ベースのセキュリティ ポリシーでユーザーがリソースにアクセスするのを防止するのに役立ち

ます。これにより、ユーザーがコンピュータのコンプライアンスの問題を解決し、HIP を再送信することが可能になるためです。

- （Windows のみ）GlobalProtect がシステムトレイに通知を表示できるようにするには、**Show System Tray Notifications**（システムトレイ通知の表示）を **Yes**（はい）に設定します。
- パスワードの有効期限が迫っている際にユーザーに表示するカスタム メッセージを作成するには、**Custom Password Expiration Message (LDAP Authentication Only)**（カスタム パスワードの失効メッセージ（**LDAP** 認証のみ） を入力します。メッセージの長さは最大 200 文字までです。
- ユーザーが Active Directory（AD）パスワードを変更したときにパスワードポリシーまたは要件を指定するカスタムメッセージを作成するには、**Change Password Message**（パスワード メッセージを変更）を入力します。メッセージの長さは最大 255 文字までです。

STEP 6 | この設定のエンド ユーザーがアプリ内で実行できることを定義します。

- **Allow User to Change Portal** Address（ユーザーによるポータルアドレスの変更を許可する）を **No**（いいえ）に設定し、GlobalProtect アプリのステータスの **Portal**（ポータル）フィールドを無効にします。その場合、ユーザーは接続先のポータルを指定できなくなるため、Windows レジストリ (`HKEY_LOCAL_MACHINE\SOFTWARE\PaloAlto Networks\GlobalProtect\PanSetup` でキー `Portal` を指定) または macOS plist (ディクショナリ `PanSetup` の `/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist` でキー `Portal` を指定) でデフォルトのポータル アドレスを指定する必要があります。詳細情報については、アプリの設定の透過的なデプロイを参照してください。
- ユーザーがウェルカム ページを省略できないようにするには、**Allow User to Dismiss Welcome Page**（ユーザーがウェルカムページを省略できるようにする）を **No**（いいえ）に設定します。オプションを **Yes**（はい）に設定した場合、ユーザーはウェルカム ページを省略し、以降のログイン時に GlobalProtect でウェルカム ページが表示されないようにすることができます。

STEP 7 | ユーザーが GlobalProtect アプリを無効化できるかどうかを指定します。

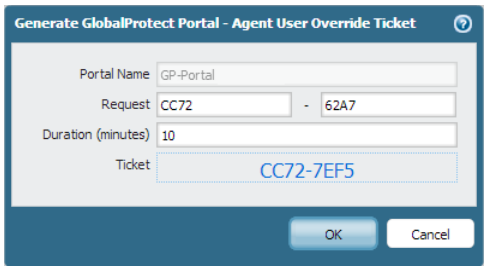
Allow User to Disable GlobalProtect（**GlobalProtect** の無効化を許可）オプションは、**Connect Method**（接続方式）付属の **User-Logon (Always On)**（ユーザー ログオン（常時オン））に設定されたエージェント設定に適用されます。ユーザー ログオン モードでは、ユーザーがエンドポイントにログインするとすぐに、アプリが自動的に接続されます。この

モードは、「常時オン」と呼ばれることがあります。その理由は、ユーザーが GlobalProtect アプリを無効化するためにこの動作をオーバーライドする必要があるからです。

デフォルトではこのオプションが**Allow**（許可）に設定されており、ユーザーはコメント、パスコード、またはチケット番号を提示することなく GlobalProtect を無効にできます。

GlobalProtect システムトレイアイコンが表示されない場合、ユーザーは *GlobalProtect* アプリを無効にすることはできません。詳細については、ステップ5を参照してください。

- ユーザー ログオン接続方式のユーザーが GlobalProtect を無効化できないようにするには、**Allow User to Disable GlobalProtect App**（**GlobalProtect** アプリケーションの無効化を許可）を **Disallow**（許可しない）に設定します。
- パスコードを入力したユーザーが GlobalProtect のみを無効化するのを許可するには、**Allow User to Disable GlobalProtect App**（**GlobalProtect** アプリケーションの無効化を許可）を **Allow with Passcode**（パスコードで許可）に設定します。次に、Disable GlobalProtect App （GlobalProtect アプリケーションの無効化）エリアで、エンドユーザーが入力する必要がある **Passcode**（パスコード）を入力（および確認入力）します。
- チケットを入力したユーザーが GlobalProtect のみを無効化するのを許可するには、**Allow User to Disable GlobalProtect**（**GlobalProtect** の無効化を許可）を **Allow with Ticket**（チケットで許可）に設定します。このオプションを使用すると、無効化アクションによってアプリが要求番号を生成し、エンドユーザーは管理者と通信する必要があります。管理者は、 **Network** > **GlobalProtect** > **Portals**(ネットワーク > GlobalProtect > ポータル) ページで **Generate Tickett**(チケットの生成) をクリックし、エンド ユーザーから通知された要求番号を入力してチケットを生成します。管理者はチケットをエンド ユーザーに提供します。エンド ユーザーはこのチケットを Disable GlobalProtect（GlobalProtect の無効化）ダイアログに入力して、アプリを無効化します。



- ユーザーが GlobalProtect アプリを無効化できる上限回数を設定するには、Disable GlobalProtect App（GlobalProtect アプリケーションの無効化）エリアにある **Max Times**

User Can Disable（無効にできる最大回数）フィールドに数値を指定します。0（デフォルト）の値は、ユーザーがアプリを無効化できる上限回数に制限がないことを示します。

この設定は、***Allow***（許可）、***Allow with Comment***（コメント付きで許可）、***Allow with Passcode***（パスコードで許可）の各オプションにのみ適用されます。

ユーザーが GlobalProtect アプリを最大回数無効にしてから、その後もアプリを無効にする必要がある場合は、

- GlobalProtect portal ポータル エージェント設定（**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > ***<portal-config>*** > **Agent**（エージェント） > ***<agent-config>*** > **App**（アプリケーション））で、**Max Times User Can Disable**（最大タイムユーザーの無効化）の値を増やすことができます。その後、GlobalProtect のステータスパネルの設定メニューから**Refresh Connection**（接続のリフレッシュ）を選択するか、新しい値を有効にするために新しい GlobalProtect 接続を確立する必要があります。
- ユーザーは、アプリを再インストールすることでカウンタをリセットできます。

- アプリケーションを無効にする時間を制限するには、GlobalProtect アプリの無効化領域に**Disable Timeout**（**min**）（タイムアウトを無効にする（分））値を入力します。0（デフォルト）の値は、ユーザーがアプリを無効化できる時間の長さが無制限であることを示します。

  この設定は、***Allow***（許可）、***Allow with Comment***（コメント付きで許可）、***Allow with Passcode***（パスコードで許可）の各オプションにのみ適用されます。

STEP 8 | ユーザーが GlobalProtect アプリケーションをアンインストールできるかどうかを指定します。

Allow User to Uninstall GlobalProtect App（ユーザーに **GlobalProtect** アプリケーションのアンインストールを許可する）オプションを使用して、ユーザーが GlobalProtect アプリケーションをアンインストールできるようにする/GlobalProtect アプリケーションをアンインス

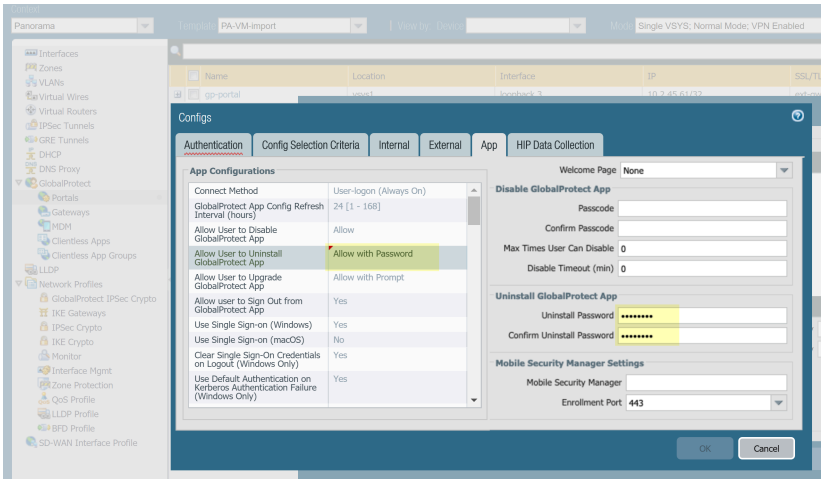
トールできないようにする、または指定されたパスワードを入力した場合はアンインストールできるようにします。

この設定は、ポータルに初めて接続するときにエンドポイントデバイスレジストリにプッシュされ、接続するポータルごとに保存されます。

このオプションでは、コンテンツ リリース バージョン *8207-5750* 以降が必要になります。

- ユーザーが制限なしで GlobalProtect アプケーションをアンインストールできるようにするには、 **Allow**（許可）を選択します。
- ユーザーが GlobalProtect アプリケーションをアンインストールしないようにするには、**Disallow**（許可しない）を選択します。

  Windows レジストリ内で **Disallow**（許可しない）に設定すると、該当のポータルの値は、`Computer\\HKEY_LOCAL_MACHINE\\SOFTWARE\\Palo Alto Networks\\GlobalProtect\\Settings\\ 'Uninstall = 1'`で「1」に設定されます。
- ユーザーがパスワードを入力して GlobalProtect アプリケーションのアンインストールすることを許可するには、**Allow with Password**（パスワードを入力させて許可）を選択します。次に、Uninstall GlobalProtect App（GlobalProtect アプリケーション のアンインストール）セクションで、**Uninstall Password**（アンインストール用パスワード）を入力し、**Confirm Uninstall Password**（パスワードのアンインストールを確定する）を実行します。



STEP 9 | ユーザーが GlobalProtect アプリをサインアウトできるかどうかを指定します。

ユーザーが GlobalProtect アプリからログアウトしないようにするには、App Configurations（アプリの設定）領域で、**Allow user to Sign Out from GlobalProtect App**（ユーザーの **GlobalProtect** アプリからのサインアウトを許可）を**No**（いいえ）に設定します。ユーザーのログアウトを許可するには、**Allow user to Sign Out from GlobalProtect App**（ユーザーの **GlobalProtect** アプリからのサインアウトを許可） を **Yes**（はい）に設定します。

このオプションでは、コンテンツ リリース バージョン*8196-5685*以降が必要になります。

STEP 10 | この設定を受け取るユーザー用に、証明書設定と動作を設定します。

App Configurations（アプリケーション設定）エリアで以下のオプションのいずれかを設定します。

- **Client Certificate Store Lookup**（クライアントの証明ストアの検索） – アプリがクライアント証明書の検索に使うストアを選択します。**User**（ユーザー）証明書は Windows の現在のユーザーの証明書ストアおよび macOS の個人用キーチェーンに保存されています。**Machine**（マシン）証明書は Windows の現在のローカルコンピュータの証明書ストアおよび macOS のシステム キーチェーンに保存されています。デフォルトでは、アプリは両方の場所で **User and machine**（ユーザーおよびマシン）証明書を検索します。
- **SCEP Certificate Renewal Period (days)**（**SCEP** 証明書更新期間（日）） – SCEP では、証明書が失効する前に、ポータルが新しいクライアント証明書をリクエストできます。この任意の時間は、証明書が失効する前の *SCEP* 証明書の更新期間を示します。クライアント証明書が失効する前の日数として設定可能なこの期間の間、ポータルはエンタープライズ PKI 内の SCEP サーバーから新しい証明書をリクエストできます（範囲は 0～30、デフォルトは 7）。0 を指定すると、ポータルはエージェント設定を更新する際に、クライアント証明書の自動更新を行いません。

  更新期間中に GlobalProtect アプリが新しい証明書を取得するには、ユーザーはアプリにログインする必要があります。たとえば、クライアント証明書の有効期間が 90 日で証明書の更新期間が 7 日であり、有効期間の最後の 7 日間にユーザーがログインしている場合、ポータルは新しい証明書を取得し、更新されたエージェント設定と共にデプロイします。詳細については、認証用のユーザー固有のクライアント証明書をデプロイを参照してください。
- **Extended Key Usage OID for Client Certificate**（クライアント証明向けの拡張キー使用 **OID**）（Windows および macOS エンドポイントのみ）– このオプションは、クライアント認証を有効にしていて、複数のクライアント証明書がエンドポイントに存在することが想定され、クライアント証明書をフィルタリングできるもう 1 つの目的が明らかになっている場合のみ使用します。このオプションを使用すると、関連付けられたオブジェクト識別子（OID）を使用するクライアント証明書のもう 1 つの目的を指定できます。たとえば、サーバー認証の目的もあるクライアント証明書のみを表示するには、OID 1.3.6.1.5.5.7.3.1 を入力します。GlobalProtect アプリが 2 つ目の目的に一致する唯一のクライアント証明書を見つけると、GlobalProtect は自動的に選択し、その証明書を使用して認証します。それ以外の場合、GlobalProtect は条件に一致するクライアント証明書のフィルタリング済みリストからクライアント証明書を選択するようユーザーに要求します。一般的な証明書の目的および OID のリストなどの詳細は、PAN-OS 7.1 新機能ガイドを参照してください。
- ポータル証明書が有効でない状態でアプリにポータルとの接続を確立させたくない場合は、**Allow User to Continue with Invalid Portal Server Certificate**（ユーザーが無効なポータルサーバー証明書で続行できるようにする）を **No**（いいえ）に設定します。ポータルで提供されるのはエージェント設定のみです。ポータルではネットワーク アクセスは提供されません。したがって、ポータルに対するセキュリティは、ゲートウェイに対するセキュリティよりも重要です。ただし、ポータルの信頼されたサーバー証明書をデプロイした場合、このオプションを無効にすると中間者攻撃（MITM）の回避に役立ちます。

STEP 11 | 機密性の高いネットワーク リソースにアクセスするために多要素認証が必要な場合にユーザーにログイン プロンプトを表示するかどうかを指定します。

内部ゲートウェイ接続では、機密性の高いネットワーク リソース（たとえば、財務アプリケーションやソフトウェア開発アプリケーション）で追加の認証が必要になる場合があります。これらのリソースへのアクセスが必要な多要素認証の通知をスムーズに行うための GlobalProtect の設定が可能です。

App Configurations（アプリケーション設定）エリアで以下のオプションのいずれかを設定します。

- **Enable Inbound Authentication Prompts from MFA Gateways**（**MFA** ゲートウェイからのインバウンド認証プロンプトを有効にします） を **Yes**（はい）に設定します。多要素認証（MFA）をサポートするには、GlobalProtect アプリはゲートウェイからのインバウンド UDP プロンプトを受信および承認する必要があります。GlobalProtect アプリがプロンプトを受け取り、受信確認できるようにする場合は **Yes**（はい）を選択します。デフォルトでは、この値は **No**（いいえ）になっています。この場合、GlobalProtect はゲートウェイからの UDP プロンプトをブロックします。
- **Network Port for Inbound Authentication Prompts (UDP)**（インバウンド認証プロンプト用の **GlobalProtect** ネットワーク ポート（**UDP**））を指定します。これは、GlobalProtect アプリが、MFA ゲートウェイからインバウンド認証プロンプトを受信するために使用します。デフォルト ポートは 4501 です。ポートを変更するには、1 ～ 65535 の数値を指定します。
- GlobalProtect アプリが多要素認証で信頼できる、**Trusted MFA Gateways**（信頼された **MFA** ゲートウェイ）を指定します。GlobalProtect アプリが指定されたネットワーク ポートで UDP メッセージを受信した場合、UDP プロンプトが信頼されたゲートウェイから来ているときにのみ、GlobalProtect は認証メッセージを表示します。
- **Inbound Authentication Message**（インバウンド認証メッセージ）を設定します。たとえば、`You have attempted to access a protected resource that requires additional authentication`（追加認証が必要な保護されたリソースにアクセスしようとしました）。`Proceed to authenticate at:` （以下に進んで認証を受けてください。）ユーザーが追加の認証を必要とするリソースにアクセスしようとすると、GlobalProtect は着信認証メッセージを受信して表示します。GlobalProtect は、多要素認証を設定したときに指定した認証ポータル ページの URL を自動的にインバウンド認証メッセージに付加します。

STEP 12 | （Windows のみ）この設定を受け取る Windows エンドポイント用に設定を行います。

- **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Windows Only)**（トンネルによって割り当てられた **DNS** サーバーを使用してすべての **FQDN** を解決（**Windows** のみ）） — GlobalProtect トンネルの DNS 解決設定を行います。**No**（いいえ）を選択すると、ゲートウェイで構成された DNS サーバーへの最初の照会が解決されない場合、Windows エンドポイントが物理アダプタに設定された DNS サーバーに DNS 照会を送信できるようになります。このオプションは、すべてのアダプタのすべての DNS サーバーを再帰的に照会するネイティブ Windows の動作を保持しますが、一部の DNS 照会を解決するための待機時間が長くなる可能性があります。**Yes**（はい）（デフォルト）を選択すると、一部の DNS クエリを物理アダプタで設定された DNS サーバーに送信すること

をエンドポイントに許可する代わりに、ゲートウェイで設定した DNS サーバーを使用してすべての DNS クエリを解決することを Windows エンドポイントに許可します。

この機能は *DNS over TCP* をサポートしていません。

この機能には、コンテンツ リリースバージョン *731* 以降のリリースと *GlobalProtect* アプリ *4.0.3* 以降のリリースが必要です。

- **Send HIP Report Immediately if Windows Security Center (WSC) State Changes**（**Windows** セキュリティーセンター（**WSC**）の状態が変更された場合に **HIP** レポートを即座に送信） — Windows セキュリティーセンター（WSC）の状態が変更された際に、GlobalProtect アプリが HIP データを送信しないようにするには、**No**（いいえ）を選択します。WSC の状態が変更された際に即座に HIP データを送信する場合は **Yes**（はい）（デフォルト）を選択します。
- **Clear Single Sign-On Credentials on Logout**（ログアウト時にサインオンの認証情報を消去） — ユーザーのログアウト後もサインオン認証情報を保存しておく場合は **No**（いいえ）を選択します。ユーザーのログアウト時に消去し、次回ログイン時に再度認証情報の入力を求める場合は **Yes**（はい）（デフォルト）を選択します。
- **Use Default Authentication on Kerberos Authentication Failure**（**Kerberos** 認証の失敗時にはデフォルトの認証を使用） — Kerberos 認証のみを使用する場合は **No**（いいえ）を選択します。Kerberos 認証が失敗した場合にデフォルトの認証方法を使って認証を再試行する場合は、**Yes**（はい）（デフォルト）を選択します。

STEP 13 | （Windows のみ）Windows エンドポイントの GlobalProtect を**Detect Proxy for Each Connection**（接続ごとにプロキシを検出）に設定します。

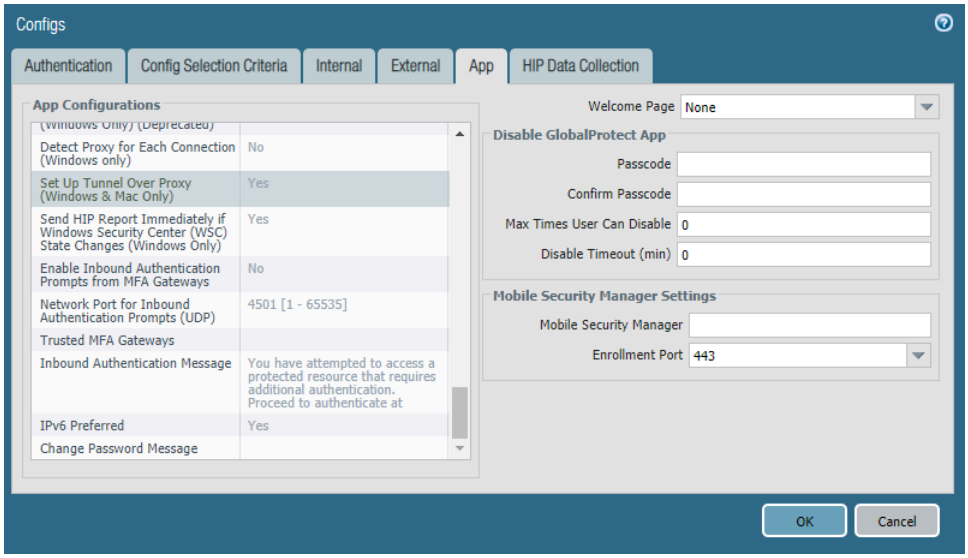
プロキシの使用に基づくネットワーク トラフィックの挙動の詳細については、プロキシを介したトンネル接続を参照してください。

- ポータル接続用のプロキシを自動検出し、以降の接続にそのプロキシを使用する場合は**No**（いいえ）を選択してください。
- 接続のたびにプロキシを自動検出する場合は **Yes**（はい）（デフォルト）を選択します。

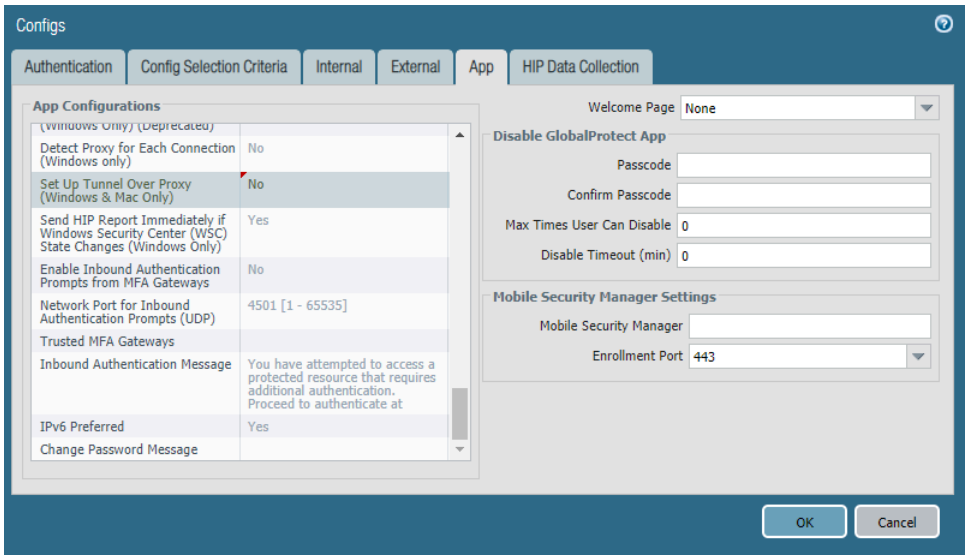
STEP 14 | (Windows および macOS のみ) GlobalProtect にプロキシを使用させるか、プロキシをバイパスさせるかを指定します。

この設定を使用すれば、GlobalProtect のプロキシの使用に基づいてネットワーク トラフィックの挙動を設定できます。詳細についてはプロキシを介したトンネル接続を参照してください。

- GlobalProtect にプロキシの使用を求める場合は、**Set Up Tunnel Over Proxy (Windows & Mac only)** (プロキシを介したトンネルのセットアップ **(Windows** および **Mac** のみ**)**) のオプションを **Yes** (はい) に設定します。



- GlobalProtect にプロキシをバイパスさせる場合は、**Set Up Tunnel Over Proxy (Windows & Mac only)** (プロキシを介したトンネルのセットアップ **(Windows** および **Mac** のみ**)**) のオプションを **No** (いいえ) に設定します。



STEP 15 | エンドポイントが GlobalProtect ポータルまたはゲートウェイに接続する際に頻繁に遅延や速度低下が発生する場合、ポータルおよび TCP のタイムアウトの値を調整することもできます。

エンドポイントがポータルまたはゲートウェイに接続するか、そこからデータを受信する際に許可する時間を延ばすには、必要に応じてタイムアウトの値を増やします。ただし、この値を増やすと GlobalProtect アプリが接続を確立できない場合に待機時間が長くなります。値を減らすと、ポータルまたはゲートウェイがタイムアウトの時間までに応答しない場合、GlobalProtect アプリが接続を確立できなくなることがあります。

App Configurations（アプリケーション設定）エリアで以下のタイムアウト オプションのいずれかを設定します。

- **Portal Connection Timeout (sec)**（ポータルの接続タイムアウト（秒））—ポータルへの接続要求に対し応答がなかった場合に、接続要求がタイムアウトするまでの秒数です（範囲は1 ～ 600、デフォルトは 30）。ファイアウォールが 777-4484 より前のアプリケーションおよび脅威のコンテンツ バージョンを実行している場合、デフォルトは 30 です。コンテンツ バージョン 777-4484 で始まる場合、デフォルトは 5 です。
- **TCP Connection Timeout (sec)**（**TCP** 接続タイムアウト（秒））— TCP 接続の両端のいずれかからの応答がない場合に、接続要求がタイムアウトするまでの秒数です（範囲は 1～600、デフォルトは 60）。ファイアウォールが 777-4484 より前のアプリケーションおよび脅威のコンテンツ バージョンを実行している場合、デフォルトは60 です。コンテンツ バージョン 777-4484 で始まる場合、デフォルトは 5 です。
- **TCP Receive Timeout (sec)**（**TCP** 受信のタイムアウト（秒））— TCP 要求が一部欠損している場合に、TCP 接続がタイムアウトするまでの秒数です（範囲は 1～600、デフォルトは 30）。

STEP 16 | **User Switch Tunnel Rename Timeout**（ユーザー スイッチ トンネルの名前変更のタイムアウト）を指定し、既存の VPN トンネルを介するリモート デスクトップ接続が可能かどうかを指定します。リモート デスクトップ プロトコル（RDP）を使用して新しいユーザーが Windows マシンに接続する際、ゲートウェイはその新しいユーザーに VPN トンネルを再び割り当てます。その後ゲートウェイは、その新しいユーザーに対してセキュリティ ポリシーを強制できるようになります。

VPN トンネルを介したリモート デスクトップ接続を許可することは、IT 管理者が RDP を使用してリモート エンドユーザー システムにアクセスする必要がある状況において有用です。

デフォルトでは、 **User Switch Tunnel Rename Timeout**（ユーザー スイッチ トンネルの名前変更のタイムアウト）値は 0 に設定されています。これは、GlobalProtect ゲートウェイが VPN トンネル上の新しいユーザー認証を終端とするということです。この動作を変更するには、タイムアウトの値を 1 から 600 秒に設定します。タイムアウトの値が切れる前に新規ユーザーがログインしない場合、GlobalProtect は最初のユーザーに割り当てられた VPN トンネルを切断します。

User Switch Tunnel Rename Timeout（ユーザー スイッチ トンネルの名前変更のタイムアウト）値のみの変更は *RDP* トンネルに影響しますが、設定時にすでにログオンしているトンネル名を変更することはできません。

STEP 17 | ユーザーがエンドポイントからログアウトした後に GlobalProtect が既存の VPN トンネルを保持できるようにするには、**Preserve Tunnel on User Logoff Timeout**（ユーザー トンネルのログアウト タイムアウトを保持）の値を指定します（範囲は0～600秒、デフォルトは0秒です）。デフォルト値の **0** を選択すると、GlobalProtect はユーザーのログアウト後にトンネルを保持しません。

このオプションでは、*2019*年*7*月*8*日以降にリリースされたコンテンツ リリース バージョンが必要になります。

VPN トンネルを保持するように GlobalProtect を設定するときは、以下の GlobalProtect の接続動作を考慮してください:

- 同じユーザーがログアウトした後、Always On（常時オン）またはOn-Demand（オンデマンド）モードのいずれかで、指定されたタイムアウト期間内にエンドポイントに再度ログインした場合、GlobalProtect はユーザーの操作（ポータルおよびゲートウェイ認証を含む）を必要とせずに接続されたままになります。 ユーザーが指定されたタイムアウト期間内に再度ログインしない場合、トンネルは切断されるので、GlobalProtect 接続を再確立する必要があります。
- ユーザーがエンドポイントからログアウトし、別のユーザーが Always On（常時オン）または On-Demand（オンデマンド）モードで同じエンドポイントにログインした場合、新規ユーザーが指定したタイムアウト期間内で GlobalProtect への認証に成功した場合にのみ、既存のトンネル名は新規ユーザーに合わせて変更されます。新規ユーザーがログインせず、指定されたタイムアウト期間内に正常に認証されない場合、既存のトンネルが切断され、新しい GlobalProtect 接続が確立される必要があります。新規ユーザーが Always On（常時オン）モードの場合、GlobalProtect は新しい接続の確立を自動的に試行します。新規ユーザーが On-Demand（オンデマンド）モードの場合は、手動で新しい GlobalProtect 接続を確立する必要があります。

STEP 18 | どのようにして GlobalProtect アプリのアップグレードを行うかを指定します。

ユーザーがいつアップグレードできるかを制御するために、設定ごとにアプリのアップグレードをカスタマイズできます。たとえば、あるリリースを全ユーザーにデプロイする前に小規模なユーザー グループでテストする場合、IT グループのユーザーのみに適用される設定を作成できます。これにより、このグループのユーザーにはアップグレードとテストを許可し、他のユーザー/グループ設定にはアップグレードを禁止します。新しいバージョンを完全にテストした後、残りのユーザーのエージェントの設定を変更し、アップグレードを許可できます。

デフォルトでは、**Allow User to Upgrade GlobalProtect App**（ユーザーによる **GlobalProtect** アプリのアップグレードを許可）オプションは、 **Allow with Prompt**（プロンプト付きで許可）するように設定されています。つまり、エンドユーザーは、ファイアウォール上で新しいバージョンのアプリが起動されたときにアップグレードを促されます。この動作を変更するには、以下のいずれかのオプションを選択します。

- **Allow Transparently**（メッセージを表示せずに実行）–アップグレードはユーザーの介入なしに自動的に行われます。アップグレードは、ユーザーが遠隔操作をしている場合にも企業ネットワーク内で接続している場合にも実行される場合があります。
- **Internal**（内部） – ユーザーが企業ネットワーク内で接続されている場合、アップグレードはユーザーの介入なしに自動的に行われます。帯域幅が狭い状況でアップグレードが遅

れるのを防ぐために、この設定を推奨します。ユーザーが企業ネットワークの外側から接続している場合、アップグレードは延期され、ユーザーが企業ネットワーク内から接続したときに再び開始されます。このオプションを使用するには、内部ゲートウェイと内部ホスト検出を設定する必要があります。

- **Disallow**（許可しない）—このオプションはアプリのアップグレードを防ぎます。
- **Allow Manually**（手動で許可）—エンドユーザーはアプリのアップグレードを開始します。この場合、ユーザーは、GlobalProtect のステータスパネルの設定メニューから **Check Version**（バージョンの確認） を選択して新しいエージェントのバージョンがあるかどうかを判定し、必要に応じてアップグレードします。アプリがユーザーに表示されない場合、このオプションは動作しません。**Display GlobalProtect Icon**（**GlobalProtect** アイコンの表示）設定の詳細は、ステップ 5 を参照してください。

> ***Allow Transparently***（メッセージを表示せずに実行）および ***Internal***（内部）でアップグレードが実行されるのは、ポータルの *GlobalProtect* ソフトウェア バージョンがエンドポイントの *GlobalProtect* ソフトウェア バージョンより新しい場合のみです。たとえば、*GlobalProtect 3.1.1* ポータルに接続している *GlobalProtect 3.1.3* エージェントはアップグレードされません。

STEP 19 | **Change Password Message**（パスワードの変更メッセージ）を追加して、ユーザーがパスワードを変更したときにユーザーが準拠しなければならないパスワード ポリシーまたは要件を指定します（たとえば、パスワードに少なくとも 1 つの数字と 1 つの大文字を含める必要があります）。

STEP 20 | 正常ログイン時にウェルカム ページを表示するかどうかを指定します。

ウェルカム ページは、イントラネットやその他の内部サーバーなどの、GlobalProtect に接続されているときのみアクセスできる内部リソースにユーザーを誘導するときに役立ちます。

デフォルトでは、アプリが正常に接続したことを示すのは、システム トレイ/メニュー バーに表示されるバルーン メッセージのみです。

ログインが成功した後にウェルカム ページを表示するには、**Welcome Page**（ウェルカム ページ）のドロップダウンリストで **factory-default**（出荷時のデフォルト）を選択します。GlobalProtect は、GlobalProtect アプリケーション内にウェルカム ページを表示します。（どのポータル設定がデプロイされるかに基づいて）ユーザーやユーザーの特定のグループ固有の情報を提供するカスタム ウェルカム ページを選択することができます。カスタム ページの作成についての詳細は、GlobalProtect ポータル ログイン、ウェルカム ページ、およびヘルプ ページのカスタマイズを参照してください。

STEP 21 | (Windows のみ) GlobalProtect アプリケーションの **Display Status Panel at Startup (**開始時にステータスパネルを表示**)** させるかどうかを指定します。

- **No (**いいえ**)**を選択すると、ユーザーが初めて接続を確立する際に GlobalProtect のステータスパネルが表示されません。
- **Yes (**はい**)**を選択すると、ユーザーが初めて接続を確立する際に自動的に GlobalProtect のステータスパネルを表示します。このオプションを使用すると、ステータスパネルを手動で閉じるには、パネルの外側をクリックする必要があります。

STEP 22 | エージェント設定を保存します。

1. エージェント設定のカスタマイズが完了したら、**OK** をクリックしてエージェント設定を保存します。保存しない場合は、 GlobalProtect ポータルのエージェント設定の定義に戻ってエージェント設定を完成します。
2. **OK** をクリックしてポータルの設定を保存します。
3. 変更を **Commit**（コミット）します。

GlobalProtect ポータル ログイン、ウェルカム ページ、およびヘルプ ページのカスタマイズ

GlobalProtect は、デフォルト ログイン、ウェルカム ページやヘルプ ページを提供します。ただし、コーポレート ブランディング、利用規定、内部リソースへのリンクを使用して独自のカスタム ページを作成できます。

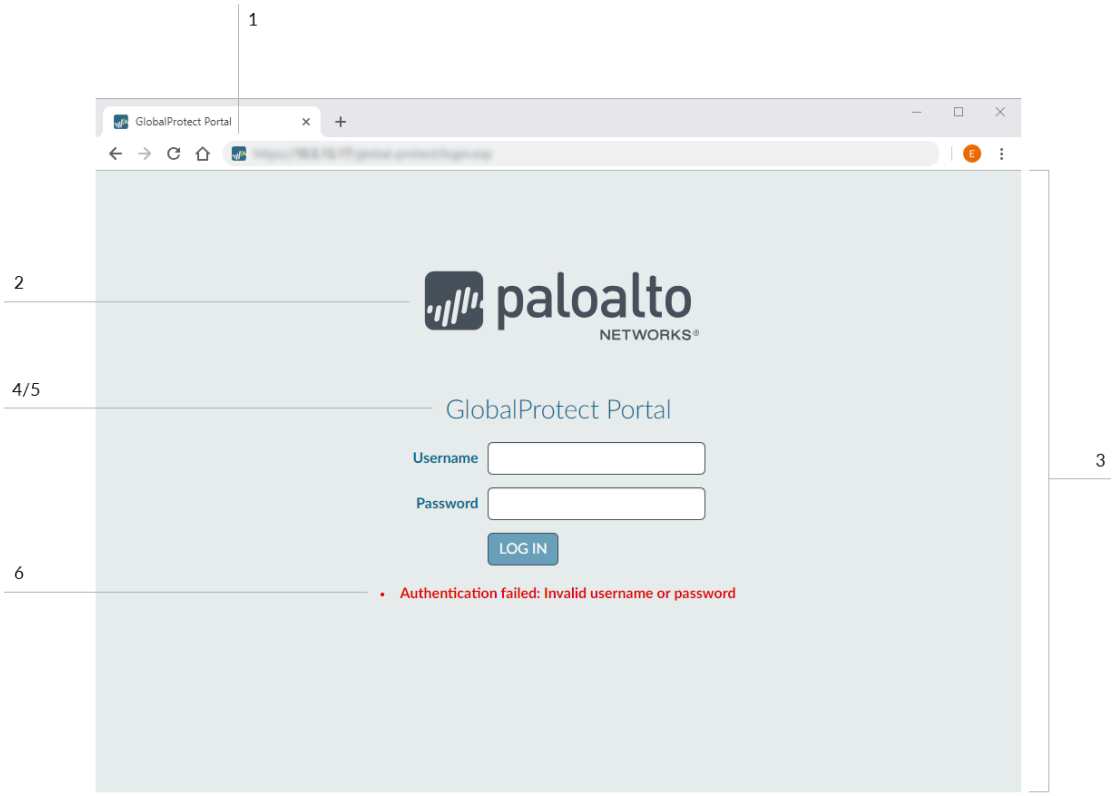
または、*GlobalProtect* ポータルへの不正な認証を防止するために、ポータルのログイン ページにブラウザからアクセスできなくすることもできます（***Network***（ネットワーク） > ***GlobalProtect*** > ***Portals***（ポータル） > ***<portal_config>*** > ***General***（一般）で ***Portal Login Page***（ポータルのログイン ページ） > ***Disable***（無効化）オプションを設定）。ポータル ログイン ページが無効になっている場合、代わりに *Microsoft System Center Configuration Manager*（*SCCM*）などのソフトウェア配布ツールを使用して、ユーザーが *GlobalProtect* アプリをダウンロードしてインストールできるようにすることができます。

STEP 1 | デフォルトのポータル ログイン ページ、ウェルカム ページ、あるいはヘルプページをエクスポートします。

1. **Device** > **Response Pages** (デバイス > 応答ページ) の順に選択します。
2. **GlobalProtect Portal Login Page**（**GlobalProtect** ポータルのログイン ページ）など、対応するGlobalProtectポータルページのリンクを選択します。
3. **Default**（デフォルト）で事前定義されたページを選択し、**Export**（エクスポート）をクリックします。

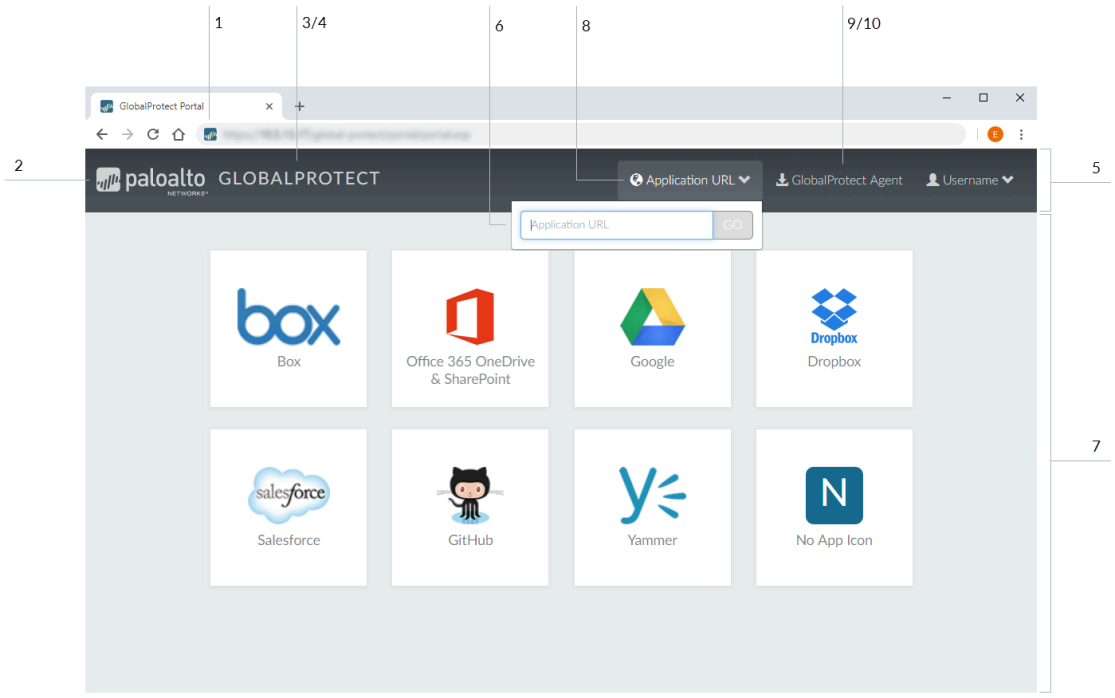
STEP 2 | エクスポートしたページを編集します。

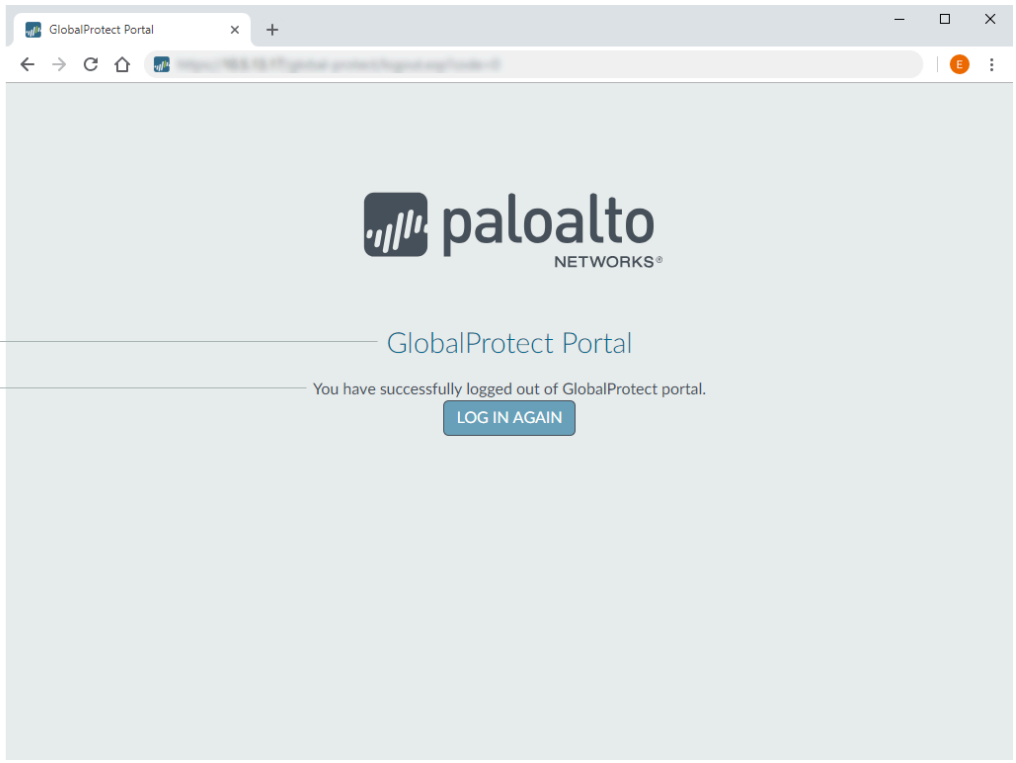
1. 任意の HTML テキスト エディタを使用して、ページを編集します。
2. ログインページあるいはホームページを編集するには、次のいずれかの変数を設定します：
   - **GlobalProtect** ポータルのログイン ページ



ラベル番号	変数	説明	例
1	favicon	ウェブ ブラウザのアドレスバーに表示される URL。	`var favicon = 'http://cdn.slidesharecdn.com/logo-24x24.jpg?3975762018';`
2	logo ロゴ	企業ロゴの URL。	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
3	bg_color	ログインページの背景色。	`var bg_color = '#D3D3D3';`
4	gp_portal_name	企業ロゴの下に表示されるテキスト。	`var gp_portal_name = 'GlobalProtect Portal';`
5	gp_portal_name_color	企業ロゴの下に表示されるテキストの色。	`var gp_portal_name_color = '#000000';`
6	error_text_color	ログオンのエラーメッセージのテキストの色。	`var error_text_color = '#196390';`

- **GlobalProtect** ポータルのホーム ページ





ラベル番号	変数	説明	例
1	favicon	ウェブ ブラウザのアドレスバーに表示される URL。	`var favicon = 'http://cdn.slidesharecdn.com/logo-24x24.jpg?3975762018';`
2	logo ロゴ	企業ロゴの URL。	`var logo = 'http://cdn.slidesharecdn.com/logo-96x96.jpg?1382722588';`
3	navbar_text	ナビゲーション バーのテキスト。	`var navbar_text = 'GlobalProtect';`
4	navbar_text_color	ナビゲーション バーのテキストの色。	`var navbar_text_color = '#D3D3D3';`
5	navbar_bg_color	ナビゲーション バーの背景色。	`var navbar_bg_color = '#A9A9A9';`
6	dropdown_bg_color	ドロップダウン メニューの背景色。	`var dropdown_bg_color = '#FFFFFF';`
7	bg_color	ホームページの背景色。	`var bg_color = '#D3D3D3';`
8	label_custom_app_url	カスタム/内部アプリケーションの URL のラベル。	`var label_custom_app_url =`

ラベル番号	変数	説明	例
			'Application URL' ;
9	表示 globalprotect_agent	GlobalProtect アプリケーションのダウンロード ボタンを表示/非表示にするオプション。ダウンロード ボタンを表示する場合は **1** を入力します。ダウンロード ボタンを表示しない場合は **0** を入力します。	var display_ globalprotect_agent = 1;
10	label_globalprotect_エージェント	GlobalProtect アプリケーションのダウンロード ボタンのラベル。	var label_ globalprotect_agent = 'GlobalProtect Agent';
11	gp_portal_name	ポータルのログアウト ページで企業ロゴの下に表示されるテキスト。	var gp_portal_name = 'GlobalProtect Portal';
12	gp_portal_name_color	ポータルのログアウト ページで企業ロゴの下に表示されるテキストの色。	var gp_portal_name_ color = '#000000' ;
13	logout_text_array	ユーザーがポータルからログアウトした後、ポータルのログアウト ページに表示されるメッセージ。	var logout_text_ array = ["You have successfully logged out of GlobalProtect portal.", "GlobalProtect

ラベル番号	変数	説明	例
		既存のメッセージしか編集できません。新しいメッセージを追加したり、既存のメッセージを削除したりすることはできません。	`Gateway is not licensed. Contact system administrator.", "User not authenticated to GlobalProtect portal.", "System error, contact system administrator.", "System error, failed to delete user session. Contact system administrator.", "Can not create user session. Max-capacity reached. Contact system administrator."];`
14	`logout_text_color`	ユーザーがポータルからログアウトした後、ポータルのログアウト ページに表示されるメッセージのテキストの色。	`var logout_text_color = '#000000';`

3. 編集したページを新しいファイル名で保存します。ページが UTF-8 エンコーディングのままであることを確認してください。

STEP 3 | 新しいページをインポートします。

1. **Device** > **Response Pages** (デバイス > 応答ページ) の順に選択します。
2. GlobalProtect ポータル ページに対応するリンクを選択します。
3. 新しいポータル ページを**Portals**（ポータル）します。**Import File**（インポート ファイル）フィールドにパスとファイル名を入力するか、**Browse**（参照）をクリックしてファイルを選択します。
4. （任意） **Destination**（宛先）ドロップダウン リストから、このページが使用される仮想システムを選択するか、すべての仮想システムから利用できるように**shared**（共有）（デフォルト）を選択します。
5. **OK** をクリックしてファイルをインポートします。

STEP 4 | 新しいページを使用するようにポータルを設定します。

- **Portal Login Page (**ポータルのログイン ページ**)**、**Portal Landing Page (**ポータルのランディング ページ**)**、および **App Help Page (**ポータルのヘルプページ**)**：
  1. **Network (**ネットワーク ） > **GlobalProtect** > **Portals**ポータル.を選択します。
  2. ログインまたはアプリのヘルプページを追加するポータルを選択します。
  3. **General**（全般）タブの Appearance（表示）エリアで、関連するドロップダウンリストから新しいページを選択します。
- **Custom Welcome Page**（カスタム ウェルカム ページ）：
  1. **Network (**ネットワーク ） > **GlobalProtect** > **Portals**ポータル.を選択します。
  2. ウェルカムページを追加するポータルを選択します。
  3. **Agent**（エージェント）タブで、ウェルカム ページを追加するエージェント設定を選択します。
  4. **App**（アプリ）タブで、**Welcome Page**（ウェルカム ページ）のドロップダウンリストから新しいページを選択します。
  5. **OK** をクリックして、エージェント設定を保存します。

STEP 5 | ポータルの設定を保存します。

OK をクリックしてポータル設定を保存し、変更を **Commit**（コミット）します。

STEP 6 | 新しいページが表示されることを確認します。

- ログインページのテスト – ブラウザを開き、ポータルの URL に移動します（「:4443」ポート番号を URL の末尾に追加しないでください。追加すると、ファイアウォールの Web インターフェイスに誘導されます）。たとえば、**`https://myportal:4443`**.ではなく **`https://myportal`** と入力します。新しいポータルのログイン ページが表示されます。
- ログインページのテスト – ブラウザを開き、ポータルの URL に移動します（「:4443」ポート番号を URL の末尾に追加しないでください。追加すると、ファイアウォールの Web インターフェイスに誘導されます）。たとえば、**`https://myportal:4443`**.ではなく **`https://myportal`** と入力します。**Username (**ユーザー名**)** および **Password (**パスワード**)** を入力してからポータルに **LOG IN (**ログイン**)** します。新しいポータルのホームページが表示されます。
- ヘルプページのテスト—GlobalProtect システム トレイ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 パネルが開いている時は、設定アイコン （⚙）をクリックして設定メニューを開きます。**Help**（ヘルプ）を選択して新しいヘルプページを閲覧します。
- ウェルカムページのテスト—GlobalProtect システム トレイ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 パネルが開いている時は、設定アイコン （⚙）をクリックして設定メニューを開きます。**Welcome Page**（ウェルカム ページ）を選択して新しいウェルカムページを閲覧します。

GlobalProtect アプリケーション

GlobalProtect アプリケーションをエンドユーザーにデプロイする

GlobalProtect™ に接続するには、エンドポイントが GlobalProtect アプリケーションを実行している必要があります。ソフトウェアのデプロイメント方法は、以下のようにエンドポイントのタイプによって異なります。

プラットフォーム	デプロイメントのオプション
macOS および **Windows** エンドポイント	macOS および Windows エンドポイントにソフトウェアを配布およびインストールするために使用できるオプションは複数あります。 • ポータルから直接 – エンド ユーザーがポータルに接続するときに更新をインストールできるように、ポータルをホストしているファイアウォールにアプリ ソフトウェアをダウンロードし、アクティベーションします。このオプションによって、エンド ユーザーは、それぞれのユーザー、グループ、オペレーティング システムに定義するエージェントの設定に基づいて更新を受信する方法やタイミングを柔軟に制御することができます。ただし、更新が必要なアプリが大量にある場合、ポータルに過剰な負荷がかかる可能性があります。アプリ更新のポータルへのホストの記載をご確認ください。 • **Web** サーバーから – アプリを同時にアップグレードする必要があるエンドポイントが大量にある場合、ファイアウォールの負荷を軽減するために、アプリ更新を Web サーバーにホストすることを検討してください。アプリ更新の Web サーバーへのホストの記載をご確認ください。 • コマンド ラインから透過的に – Windows エンドポイントでは、Windows インストーラー（MSIEXEC）を使用してアプリの設定を自動的にデプロイできます。ただし、MSIEXEC を使用して新しいアプリ バージョンにアップグレードするには、既存のアプリを最初にアンインストールする必要があります。さらに、MSIEXEC は、Windows レジストリに値を設定することによって、エンドポイントでアプリの設定を直接デプロイすることを可能にします。同様に、macOS plist の設定を構成することで、macOS エンドポイントにアプリケーション設定をデプロイすることもできます。アプリの設定の透過的なデプロイを参照してください。 • グループ ポリシー ルールの使用 – Active Directory 環境で、Active Directory グループ ポリシーを使用して、GlobalProtect アプリをエンド ユーザーに配布することもできます。AD グループ ポリシーでは、Windows エンドポイント設定とソフトウェアの自動修正が可能です。プログラムをエンドポイントやユーザーに自動的に配布するため

プラットフォーム	デプロイメントのオプション
	にグループ ポリシーを使用する方法に関する情報は、http://support.microsoft.com/kb/816102 で記事を参照してください。 • モバイル エンドポイント管理システムから—MDMあるいはEMMといったモバイル管理システムを使ってモバイル エンドポイントを管理する場合、そのシステムを使って GlobalProtect アプリケーションをデプロイおよび設定することができます。モバイル エンドポイント管理を参照してください。
Windows 10 フォンおよび **Windows 10 UWP**	• モバイル エンドポイント管理システムから—MDM や EMM といったモバイル管理システムを使って Windows 10 エンドポイントを管理する場合、そのシステムを使って GlobalProtect アプリケーションをデプロイおよび設定することができます。モバイル エンドポイント管理を参照してください。 • **Microsoft** ストアから—エンドユーザーは、Microsoft Store から直接 GlobalProtect アプリをダウンロードしてインストールすることもできます。GlobalProtect アプリをダウンロードしてテストする方法は、GlobalProtect モバイル アプリケーションのダウンロードおよびインストールを参照してください。
iOS および **Android** エンドポイント	• モバイル エンドポイント管理システムから—MDM や EMM といったモバイル管理システムを使う場合、そのシステムを使って GlobalProtect アプリケーションをデプロイおよび設定することができます。モバイル エンドポイント管理を参照してください。 • アプリストアから—エンドユーザーは、Apple App Store（iOS エンドポイント）または Google Play（Android エンドポイント）から直接 GlobalProtect アプリをダウンロードしてインストールすることもできます。GlobalProtect アプリをダウンロードしてテストする方法は、GlobalProtect モバイル アプリケーションのダウンロードおよびインストールを参照してください。
Chromebook	• **Google** 管理者コンソールから—Google 管理コンソールを使用すれば、Webベースのロケーションから一元的に Chromebook の設定やアプリケーションを管理できます。Google 管理者コンソールを使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイするには、Google 管理コンソールを使用して管理対象 Chromebook 上で Android

プラットフォーム	デプロイメントのオプション
	用 GlobalProtect アプリケーションをデプロイを参照してください。 *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。*Android* アプリケーションをサポートしていない *Chromebook* では、*Chromebook* 用 *GlobalProtect* アプリケーションを引き続き実行する必要があります。*Chromebook* は *GlobalProtect* アプリ *5.0*以降のバージョンではサポートしていません。 • **AirWatch** から—AirWatch で登録した管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイできるようになっています。アプリケーションをデプロイしたら、VPN プロファイルを構成、デプロイし、エンドユーザー用の GlobalProtect アプリケーションを自動的にセットアップします。AirWatch を使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイするには、AirWatch を使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイを参照してください。
Linux Linux	サポート サイトから Linux 用 GlobalProtect アプリをダウンロードした後、アプリを配布してインストールできます： • **Linux** アプリ配布ツールの使用—Linux アプリの配布は通常、Chef や Puppet などのサードパーティのツールを使用して管理するか、Linux オペレーティングシステム用のローカル リポジトリ（Ubuntu リポジトリ や RHEL リポジトリなど）を使用して管理します。詳しくは、ご使用の Linux オペレーティングシステムの資料を参照してください。 • 手動インストール—ソフトウェアをエンドユーザーが利用できるようにする場合は、**apt** や **dpkg** などの Linux ツールを使用してソフトウェアを手動でインストールできます。Linux GlobalProtect アプリのインストール方法については、GlobalProtect アプリのユーザーガイドを参照してください。

GlobalProtect アプリ ソフトウェアをデプロイする代わりに、*GlobalProtect* ポータルを設定すれば、*HTML*、*HTML5*、*JavaScript* テクノロジを使用する一般的なエンタープライズ *Web* アプリケーションへの安全なリモート アクセスを提供できます。ユーザーは *GlobalProtect* アプリ ソフトウェアをインストールすることなく、*SSL* 対応の *Web* ブラウザから安全なアクセスを利用できます。GlobalProtect クライアントレス VPN を参照してください。

GlobalProtect アプリケーションのダウンロード

お客様がエンドユーザーである場合、*IT* 管理者に連絡してサポートされている最新の *GlobalProtect* ソフトウェアを求めてください。

エンドユーザーのために GlobalProtect アプリをデプロイする前に、新しいアプリ インストール パッケージを、ポータルをホストしているファイアウォールにアップロードし、ポータルに接続しているアプリにダウンロードするためにソフトウェアをアクティベーションする必要があります。このデプロイ方法は、すべての非モバイル アプリケーションのバージョンで利用できます。GlobalProtect アプリケーションのモバイル バージョンをダウンロードするには、お使いのモバイル デバイスのアプリ ストアを参照してください (詳細については GlobalProtect モバイル アプリケーションのダウンロードおよびインストールを参照)。

ファイアウォールに直接最新のアプリケーションをダウンロードするためには、Palo Alto Networks 更新サーバーへのアクセスを可能にするサービス ルートを持つ必要があります (GlobalProtect アプリケーションをエンドユーザーにデプロイするを参照)。ファイアウォールがインターネットにアクセスできない場合、インターネットに接続されたコンピュータを使用して、Palo Alto Networks ソフトウェア更新 サポート サイトからアプリ ソフトウェア パッケージをダウンロードした後に、ファイアウォールに手動でアップロードすることができます。

アプリ ソフトウェア パッケージを手動でダウンロードする方法：

STEP 1 | Palo Alto Networks カスタマー サポート ポータル (https://support.paloaltonetworks.com/) にログインします。

Software Updates (ソフトウェア更新) ページにログインしてソフトウェアをダウンロードするには、有効な *Palo Alto Networks* アカウントが必要になります。ログインできず、サポートが必要な場合は、https://www.paloaltonetworks.com/support/tabs/overview.htmlにアクセスしてください。

STEP 2 | **Updates**（更新） > **Software Updates**（ソフトウェア更新）を選択します。

STEP 3 | オペレーティングシステムに応じて GlobalProtect アプリケーションのバージョンを選択します。

STEP 4 | 対象のアプリ バージョンのリリースノートを確認してからダウンロード リンクを選択し、ダウンロードを進めます。

STEP 5 | GlobalProtect アプリケーションをエンドユーザーにデプロイする.

GlobalProtect アプリケーションの各リリースをインストール可能なオペレーティングシステムについては、Palo Alto Networks Compatibility Matrix（Palo Alto Networks 互換性マトリクス）を参照してください。

アプリ更新のポータルへのホスト

GlobalProtect アプリ ソフトウェアをデプロイする最も簡単な方法は、新しいアプリ インストール パッケージを、ポータルをホストしているファイアウォールにダウンロードし、ポータルに接続しているアプリにダウンロードするためにソフトウェアをアクティベーションします。自動的にこれを行うには、ファイアウォールが、Palo Alto Networks 更新サーバーへのアクセスを可

能にするサービス ルートを持つ必要があります。ファイアウォールがインターネットにアクセスできない場合、インターネットに接続されたコンピュータを使用して、Palo Alto Networks ソフトウェア更新 サポート サイトからソフトウェア パッケージをGlobalProtect アプリケーションのダウンロードした後に、ファイアウォールに手動でアップロードすることができます。

アプリ ソフトウェアの更新がポータルエージェント設定でどのようにデプロイされるかを定義します。つまり、アプリがポータルに接続するときに更新が自動的に行われるのか、アプリをアップグレードするプロンプトがユーザーに表示されるのか、エンド ユーザーが手動でチェックして新しいアプリ バージョンをダウンロードするのかを定義します。エージェント設定の作成について、詳細はGlobalProtect エージェント設定の定義を参照してください。

STEP 1 | GlobalProtect ポータルをホストするファイアウォールで、新しいアプリ ソフトウェアのイメージを確認します。

Device（デバイス） > **GlobalProtect Client**（**GlobalProtect** クライアント） を選択して、使用可能なアプリ ソフトウェアのイメージ一覧を閲覧します。

- ファイアウォールが更新サーバーにアクセスできる場合、**Check Now**（今すぐチェック）をクリックし、最新の更新をチェックします。**Action**（アクション）列の値が **Download**（ダウンロード）の場合は、最新バージョンのアプリが入手可能であることを示します。
- ファイアウォールが更新サーバーにアクセスできない場合は、手順 2 の説明に従って、Palo Alto Networks ソフトウェア更新サポート サイトから手動でソフトウェア イメージをダウンロードする必要があります。

STEP 2 | アプリ ソフトウェア イメージをダウンロードします。

- ファイアウォールが更新サーバーにアクセスできる場合は、目的のアプリ バージョンを見つけて、**Download**（ダウンロード）をクリックします。ダウンロードが完了すると、**Action**（アクション）列の値が **Activate**（アクティベーション）になります。
- ファイアウォールが更新サーバーにアクセスできない場合、GlobalProtect アプリケーションのダウンロード。ソフトウェア イメージをダウンロードしたら、ファイアウォールの **Device**（デバイス） > **GlobalProtect Client**（**GlobalProtect** クライアント） ページに戻り、 **Upload**（アップロード）します。

STEP 3 | エンド ユーザーがポータルからダウンロードできるように、アプリ ソフトウェア イメージをアクティベーションします。

一度にアクティベーションできるアプリ ソフトウェア イメージのバージョンは *1* つのみです。新しいバージョンをアクティベーションするが、以前にアクティベーションされたバージョンを必要とするアプリが別にある場合、必要なバージョンを再度ダウンロードできるようにするために、アクティベーションする必要があります。

- ソフトウェア イメージを更新サーバーから自動的にダウンロードした場合、**Activate**（アクティベーション）をクリックします。
- ソフトウェア イメージをファイアウォールに手動でアップロードした場合、**Activate From File**（ファイルからアクティベーション） をクリックし、ドロップダウン リストから、アップロードした **GlobalProtect Client File**（**GlobalProtect** クライアント ファイ

ル）を選択します。**OK** をクリックし、選択したイメージをアクティベーションします。バージョンに **Currently Activated**（現在アクティベーション済み）と表示するには、ページの更新が必要になる場合があります。

アプリ更新の Web サーバーへのホスト

GlobalProtect アプリ ソフトウェアのインストールや更新が必要なエンドポイントが大量にある場合、GlobalProtect アプリ ソフトウェア イメージを外部 Web サーバーにホストすることを検討してください。これは、ユーザーがアプリのダウンロードのために接続するときのファイアウォールの負荷の軽減に役立ちます。

STEP 1 | Web サーバーにホストする GlobalProtect アプリのバージョンをファイアウォールにダウンロードし、アクティベーションします。

ファイアウォールでアプリ ソフトウェアをダウンロードおよびアクティベーションするには、アプリ更新のポータルへのホストで説明されている手順を実行します。

STEP 2 | Web サーバーにホストする GlobalProtect アプリ ソフトウェア イメージをダウンロードします。

ポータルでアクティベーションしたのと同じイメージをダウンロードします。

ウェブ ブラウザからGlobalProtect アプリケーションのダウンロード。

STEP 3 | ソフトウェア イメージ ファイルを Web サーバーに公開します。

STEP 4 | エンド ユーザーを Web サーバーにリダイレクトします。

ポータルをホストしているファイアウォールで、次の CLI コマンドを操作モードで入力します：

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

ここで、*<path>* はイメージをホストしているフォルダへの URL のパスです (たとえば、**https://acme/GP**)。

STEP 5 | リダイレクトをテストします。

1. Web ブラウザから、以下の URL に移動します：

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

   例: **https://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、**Login**（ログイン）をクリックします。正常ログイン後に、ポータルがダウンロードのためにリダイレクトします。

アプリのインストールのテスト

GlobalProtect アプリのインストール状況をテストするには、以下の手順を実行します。

STEP 1 | アプリのインストール状況をテストするためのエージェント設定を作成します。

GlobalProtect アプリ ソフトウェアをエンドポイントに最初にインストールするとき、エンドユーザーは、管理者権限を持つアカウントを使用してシステムにログインする必要があります。この後のアプリ ソフトウェア更新では、管理者権限は不要です。

ファイアウォールを管理する責任を担う *IT* 部門の管理者などの小規模なユーザーのグループに制限したエージェントの設定を作成することをお勧めします。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します
2. 変更または **Add**（追加）する、既存のポータル構成を選択します
3. **Agent**（エージェント）タブで、既存の設定を選択するか、**Add**（追加）をクリックして、テスト ユーザー/グループにデプロイする新しい設定を追加します。
4. **User/User Group**（ユーザー/ユーザー グループ）タブで、アプリをテストする **User/User Group**（ユーザー/ユーザー グループ）を **Add**（追加）します。
5. **App**（アプリ）タブで、**Allow User to Upgrade GlobalProtect App**（ユーザーによる **GlobalProtect** アプリのアップグレードを許可）を **Allow with Prompt**（プロンプト付きで許可）に設定します。**OK** をクリックして設定を保存します。
6. （任意）**Agent**（エージェント）タブで、作成または変更したエージェントの設定を選択し、これまでに作成した一般的な設定の先頭になるように、**Move Up**（上へ）をクリックします。

   GlobalProtect アプリに接続すると、ポータルは、パケットの送信元の情報を、定義したエージェント設定と比較します。セキュリティルール評価によって、ポータルはリストの先頭から一致する項目を検索します。一致が見つかると、ポータルは対応する設定をアプリに配信します。
7. 変更を **Commit**（コミット）します。

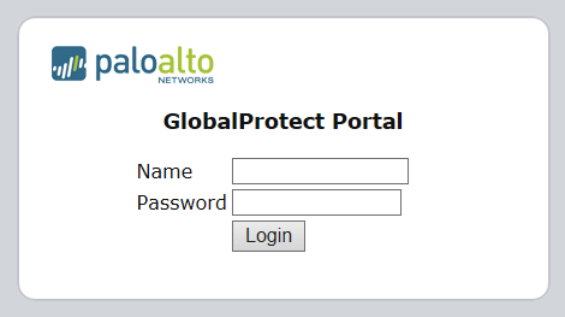
STEP 2 | GlobalProtect ポータルにログインします。

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: **https://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。

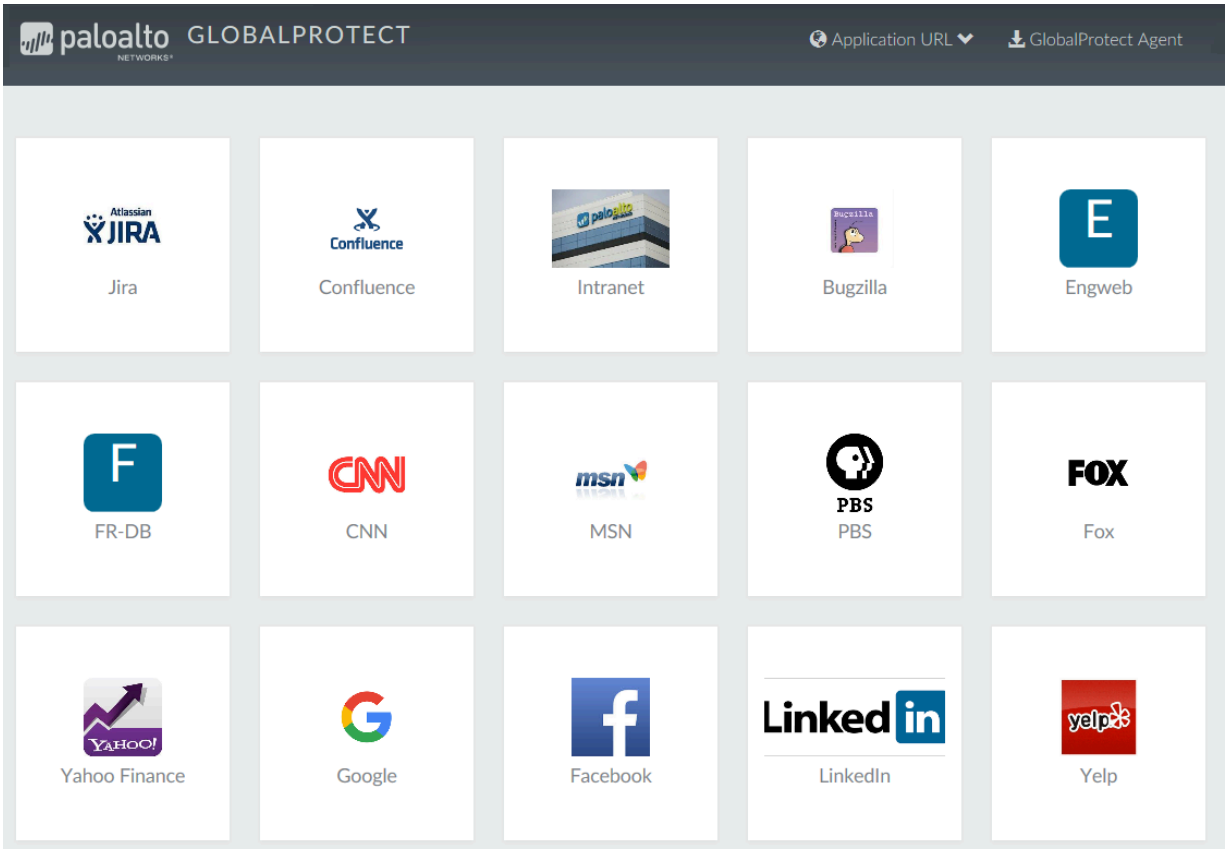


STEP 3 | アプリのダウンロード ページに移動します。

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。

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 4 | 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。

2. ソフトウェア インストール ファイルを開きます。
3. ソフトウェアの実行または保存のプロンプトが表示されたら、**Run**（実行）をクリックします。
4. プロンプトが表示されたら、**Run**（実行） をクリックして GlobalProtect セットアップ ウィザードを起動します。

> *GlobalProtect* アプリ ソフトウェアをエンドポイントに最初にインストールするとき、エンドユーザーは、管理者権限を持つアカウントを使用してシステムにログインする必要があります。この後のアプリ ソフトウェア更新では、管理者権限は不要です。

STEP 5 | GlobalProtect アプリ セットアップを完了します。

1. GlobalProtect セットアップ ウィザードから、**Next**（次へ） をクリックします。
2. **Next** (次へ)をクリックしてデフォルトのインスレーション フォルダ（`C:\Program Files\Palo Alto Networks\GlobalProtect`）を承認するか、**Browse(参照)** をクリックして新しい場所を選択し、**Next (次へ)** を 2 回クリックします。
3. インストール完了後、ウィザードを **Close**（閉じる）します。

STEP 6 | GlobalProtect にログインします。

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. Portal（ポータル）の FQDN または IP アドレスを入力してから **Connect**（接続）をクリックします。
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、**Gateway**（ゲートウェイ）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）。

   このオプションはマニュアル ゲートウェイ選択が有効な場合にのみ利用可能です。
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. （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。

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。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。

GlobalProtect モバイル 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 アプリケーションを使用すると、企業のセキュリティ ポリシーをモバイル エンドポイントまで容易に拡張することができます。GlobalProtect アプリを実行している他のリモート エンドポイントと同様に、モバイル アプリから IPsec や SSL VPN トンネルを介して、会社のネットワークに安全にアクセスすることができます。アプリが、エンド ユーザーの現在のロケーションに最も近いゲートウェイに自動で接続します。さらに、エンドポイントとの双方向のトラフィックには、会社のネットワーク上にある他のホストと同じセキュリティ ポリシーが自動的に適用されます。また、モバイル アプリはホスト設定に関する情報を収集し、この情報を使用して HIP ベースのセキュリティ ポリシーを強化することができます。

GlobalProtect アプリケーションをインストールするには、次のような主な 2 つの方法があります。サードパーティ製の MDM からアプリをデプロイし、そのアプリを管理対象のエンドポイントに透過的にプッシュすることができます。または、公式のストアからアプリを直接エンドポイントにインストールすることも可能です。

- iOS エンドポイント—App Store
- Android エンドポイントと Chromebooks—Google Play

  GlobalProtect アプリケーション 5.0 以降、Chrome OS 版 GlobalProtect アプリケーションはサポートされません。代わりに Android 用 GlobalProtect アプリケーションを使用してください。
- Windows 10 フォンおよび Windows 10 UWP エンドポイント—Microsoft ストア

ここでは、GlobalProtect アプリケーションをモバイル エンドポイントに直接インストールする流れをご説明します。AirWatch からの GlobalProtect アプリのデプロイ方法は、AirWatch を使用して GlobalProtect モバイル アプリケーションをデプロイを参照してください。

STEP 1 | アプリのインストール状況をテストするためのエージェント設定を作成します。

ファイアウォールを管理する責任を担う IT 部門の管理者などの小規模なユーザーのグループに制限したエージェントの設定を作成することをお勧めします。

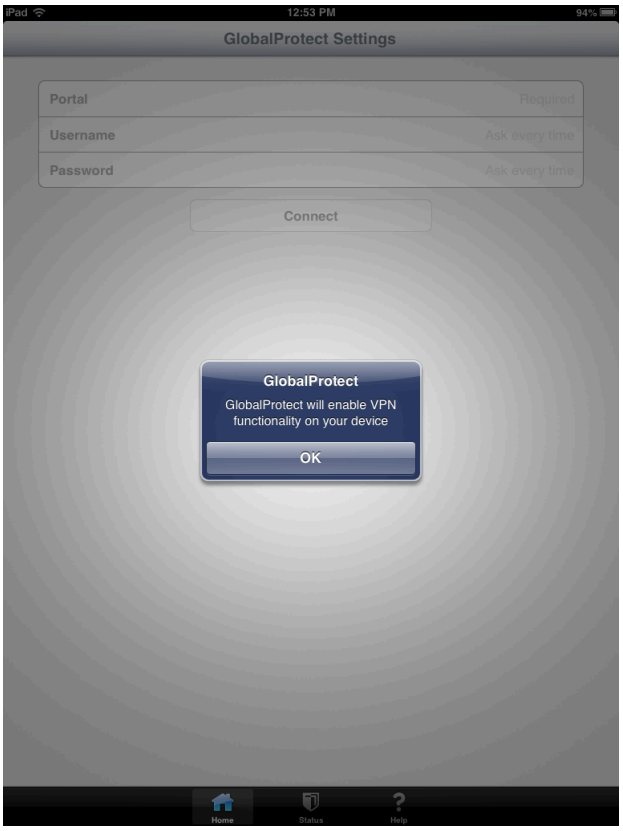
1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します
2. 既存のポータル設定を選択して変更するか、新しく **Add**（追加）します。
3. **Agent**（エージェント）タブで、既存の設定を選択するか、**Add**（追加）をクリックして、テスト ユーザー/グループにデプロイする新しい設定を追加します。
4. **User/User Group**（ユーザー/ユーザー グループ）タブで、アプリをテストする **User/User Group**（ユーザー/ユーザー グループ）を **Add**（追加）します。
5. テストしているアプリの **OS** を選択します（**iOS**、**Android**、または**WindowsUWP**）。
6. （任意）作成または変更したエージェントの設定を選択し、これまでに作成した一般的な設定の先頭になるように、**Move Up**（上へ）をクリックします。
7. 変更を **Commit**（コミット）します。

STEP 2 | エンドポイントから、プロンプトに従って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。

- Android エンドポイントでは、Google Play でアプリを検索します。
- iOS エンドポイントでは、App Store でアプリを検索します。
- Windows 10 UWP エンドポイントでは、Microsoft ストアでアプリを検索します。

STEP 3 | アプリケーションを起動します。

正常にインストールされると、GlobalProtect アプリケーション アイコンがエンドポイントのホーム画面に表示されます。アプリケーションを起動するには、このアイコンをタップします。GlobalProtect VPN 機能を有効にするプロンプトが表示されたら、**OK** をタップします。



STEP 4 | ポータルに接続します。

1. プロンプトが表示されると、**Portal**（ポータル）に名前またはアドレスを入力し、**Username**（ユーザー名）と **Password**（パスワード）を入力します。ポータル名は FQDN である必要がありますが、先頭に「https://」を入力しないでください。

2. **Connect**（接続）をタップして、アプリケーションが GlobalProtect との接続を正常に確立することを検証します。

   サードパーティーのモバイル エンドポイント管理システムが設定されている場合、アプリケーションから登録プロンプトが表示されます。

アプリ設定の透過的なデプロイ

ポータルの設定からアプリ設定をデプロイする代わりに、Windows レジストリやグローバル macOS plist、または Windows インストーラー（MSIEXEC）から、エンドポイントの設定を直接定義することができます。この利点は、GlobalProtect ポータルに初めて接続する前に、エンドポイントへの GlobalProtect アプリの設定のデプロイを有効にできることです。

ポータルの設定で定義されている設定は常に、Windows レジストリや macOS plist で定義されている設定をオーバーライドします。レジストリまたは plist で設定を定義するが、ポータル設定で異なる設定が指定されている場合、アプリがポータルから受け取る設定は、エンドポイントで定義された設定よりも優先されます。この上書きには、オンデマンドで接続するのか、シングルサイン オン（SSO ）を使用するのか、ポータル証明書が無効な場合にアプリが接続できるのかなどの、ログイン関連の設定が含まれます。つまり、設定に矛盾しない必要があります。また、ポータル設定はエンドポイントにキャッシュされ、GlobalProtect　アプリが再起動されるか、エンドポイントが再起動されるとキャッシュ設定が使用されます。

以下のセクションでは、使用できるカスタマイズ可能なアプリ設定と、Windows および macOS エンドポイントに透過的にこれらの設定をデプロイする方法について説明します。

- カスタマイズ可能なアプリの設定
- Windows エンドポイントへのアプリ設定のデプロイ
- macOS エンドポイントへのアプリ設定のデプロイ

Windows レジストリおよび *macOS plist* を使用して *GlobalProtect* アプリ設定をデプロイするだけでなく、*GlobalProtect* アプリがエンドポイントから特定の *Windows* レジストリまたは *macOS plist* 情報（エンドポイントにインストールされたアプリケーション、エンドポイントで実行されているプロセス、これらのアプリケーションやプロセスの属性またはプロパティに関するデータなど）を収集できるようにすることもできます。その後、データをモニターして、一致条件としてセキュリティ ルールに追加できます。定義したレジストリ設定に一致するエンドポイント トラフィックは、セキュリティ ルールに従って適用することができます。さらに、カスタム チェックをセットアップしてエンドポイントからのアプリケーションおよびプロセス データの収集を行うことができます。

カスタマイズ可能なアプリの設定

ポータル アドレスの事前のデプロイに加えて、アプリ設定も定義できます。Windows エンドポイントへのアプリ設定のデプロイを行うには、Windows レジストリ（`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect`）でキーを適宜します。macOS エンドポイントへのアプリ設定のデプロイを行うには、you define entries in the dictionary of the macOS plist （`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`）の `PanSetup` ディクショナリでエントリを定義します。Windows エンドポイントの場合のみ、Windows インストーラを使用してMsiexec からアプリ設定をデプロイすることもできます。

以下のトピックでは、カスタマイズ可能なアプリの設定について説明します。GlobalProtect ポータル エージェント設定で定義されている設定は、Windows レジストリや macOS plist で定義されている設定よりも優先されます。

一部の設定については、対応するポータル設定が *Web* インターフェイスにないため、*Windows* レジストリまたは *MSIEXEC* を使用して設定する必要があります。これらの *SSO* 設定には、*`can-prompt-user-credential`*、*`wrap-cp-guid`*、および*`filter-non-gpcp`* が含まれます。

- アプリの表示オプション
- ユーザー行動オプション
- アプリの動作オプション
- スクリプトの導入オプション

アプリの表示オプション

次の表は、GlobalProtect アプリの表示をカスタマイズするために Windows レジストリおよび macOS の plist で利用できるオプションを示します。

表 **3 :** 表：カスタマイズ可能なアプリの設定

ポータルのエージェントの設定	Windows レジストリ/ macOS Plist	Msiexec パラメータ	Default（フォルト）
詳細ビューの有効化	**enable-advanced-view yes | no**	**ENABLEADVANCEDVIEW=”yes | no”**	**yes**
GlobalProtect アイコンの表示	**show-agent-icon yes | no**	**SHOWAGENTICON=”yes | no”**	**yes**
ネットワーク オプションの再検出の有効化	**rediscover-network yes | no**	**REDISCOVERNETWORK=”yes | no”**	**yes**
ホストプロファイルオプションの再送信の有効化	**resubmit-host-info yes | no**	**RESUBMITHOSTINFO=”yes | no”**	**yes**
システム トレイ通知の表示	**show-system-tray-notifications yes | no**	**SHOWSYSTEMTRAYNOTIFICATIONS=”yes | no”**	**yes**

ユーザー行動オプション

ユーザーが GlobalProtect アプリとやり取りする方法をカスタマイズするために Windows レジストリおよび Mac の plist にて利用するオプションは、以下の表の通りです。

表 4 : 表：カスタマイズ可能なユーザー行動オプション

ポータルのエージェントの設定	Windows レジストリ/macOS Plist	Msiexec パラメータ	Default（フォルト）
ユーザーによるポータルアドレスの変更を許可する	**can-change-portal yes | no**	**CANCHANGEPORTAL=”yes | no”**	**yes**
ユーザーがウェルカムページを省略できるようにする	**enable-hide-welcome-page yes | no**	**ENABLEHIDEWELCOMEPAGE= ”yes | no”**	**yes**
ユーザーが無効なポータルサーバー証明書で続行できるようにする	**can-continue-if-portal-cert-invalid yes | no**	**CANCONTINUEIFPORTALCERTINVALID= ”yes | no”**	**yes**
ユーザーが **GlobalProtect** アプリを無効化できるようにする	**disable-allowed yes | no**	**DISABLEALLOWED="yes | no"**	**no**
ユーザー認証情報の保存 GlobalProtect が認証情報を保存するのを防止する場合は 0 を、ユーザー名およびパスワードを両方とも保存させる場合は 1 を、ユーザー名だけを保存させる場合は 2 を指定します。	**save-user-credentials 0 | 1 | 2**	**SAVEUSERCREDENTIALS 0 | 1 | 2**	n/a
ポータルにない **Allow user to save password**（パ	**can-save-password yes | no**	**CANSAVEPASSWORD=”yes | no”**	**yes**

ポータルのエージェントの設定	Windows レジストリ/macOS Plist	Msiexec パラメータ	Default（フォルト）
スワードの保存を許可）する設定は、PAN-OS 7.1 以降のリリースの Web インターフェイスでは非推奨になっていますが、Windows レジストリおよび macOS plist で設定することができます。**Save User Credentials**（ユーザー認証情報の保存）フィールドでいずれかの値を指定すると、ここで指定した値が上書きされます。			
Windows のみ/ポータルにない この設定により、GlobalProtect の認証情報プロバイダーが **Start GlobalProtect Connection (GlobalProtect 接続を開始)** ボタンを表示し、ユーザーが手動で GlobalProtect プレ ログオン接続を開始できるようになります。	**`ShowPrelogonButton yes | no`**	n/a	**`no`**

アプリの動作オプション

次の表は、GlobalProtect アプリの動作をカスタマイズするために Windows レジストリおよび macOS の plist で利用できるオプションを示します。

表 5 : 表：カスタマイズ可能なアプリの動作オプション

ポータルのエージェントの設定	Windows レジストリ/macOS Plist	Msiexec パラメータ	Default（フォルト）
接続手段	**connect-method on-demand | pre-logon | user-logon**	**CONNECTMETHOD="on-demand | pre-logon | user-logon"**	ユーザーログオン
GlobalProtect アプリ設定の更新間隔（時間）	**refresh-config-interval** <hours>	**REFRESHCONFIGINTERVAL="**<hours>**"**	**24**
接続時の DNS 設定の更新（Windows のみ）	**flushdns yes | no**	**FLUSHDNS="yes | no"**	**no**
Windows セキュリティーセンター（WSC）の状態が変更された場合には HIP レポートを即座に送信（Windows のみ）	**wscautodetect yes | no**	**WSCAUTODETECT="yes | no"**	**no**
接続ごとにプロキシーを検出（Windows のみ）	**ProxyMultipleAuto Detection yes | no**	**ProxyMultipleAuto Detection="yes | no"**	**no**
ログアウト時にサインオンの認証情報を消去（Windows のみ）	**LogoutRemoveSSO yes | no**	**LogoutRemoveSSO="yes | no"**	**yes**

ポータルのエージェントの設定	Windows レジストリ/macOS Plist	Msiexec パラメータ	Default（フォルト）
Kerberos 認証の失敗時にはデフォルトの認証を使用（Windows のみ）	**krb-auth-fail-fallback yes | no**	**KRBAUTHFAILFALLBACK= ”yes | no”**	**no**
カスタムパスワードの失効メッセージ（LDAP 認証のみ）	**PasswordExpiryMessage** <**message**>	**PasswordExpiryMessage “**<**message**>**”**	
ポータルの接続のタイムアウト（秒）	**PortalTimeout** <**portaltimeout**>	**PORTALTIMEOUT= ”**<**portaltimeout**>**”**	**5**
TCP 接続のタイムアウト（秒）	**ConnectTimeout** <**connecttimeout**>	**CONNECTTIMEOUT= ”**<**connecttimeout**>**”**	**5**
TCP 受信のタイムアウト（秒）	**ReceiveTimeout** <**receivetimeout**>	**RECEIVETIMEOUT= ”**<**receivetimeout**>**”**	**30**
クライアントの証明ストアの検索	**certificate-store-lookup user | machine | user and machine | invalid**	**CERTIFICATESTORELOOKUP= "user | machine | user and machine | invalid"**	**user and machine**
SCEP 証明書更新期間（日）	**scep-certificate-renewal-period** <**renewalPeriod**>	n/a	**7**
内部のゲートウェイ接続の最大試行回数	**max-internal-gateway-connection-attempts** <**maxValue**>	**MIGCA="**<**maxValue**>**"**	**0**
クライアント証明向けの拡張キー使用 OID	**ext-key-usage-oid-for-client-cert** <**oidValue**>	**EXTCERTOID=”**<**oidValue**>**”**	n/a

ポータルのエージェントの設定	Windows レジストリ/macOS Plist	Msiexec パラメータ	Default（フォルト）
ユーザースイッチトンネルの名前変更のタイムアウト（秒）	**user-switch-tunnel-rename-timeout** <**renameTimeout**>	n/a	**0**
シングル サインオンの使用 （**Windows** のみ）	**use-sso yes | no**	**USESSO="yes | no"**	**yes**
ポータルにない この設定により、デフォルトポータル IP アドレス（またはホスト名）を指定します。	**portal** <**IPaddress**>	**PORTAL="**<**IPaddress**>**"**	n/a
ポータルにない この設定により、ユーザーがデバイスにログインて GlobalProtect ポータルに接続する前に GlobalProtect が VPN トンネルを開始できます。	**prelogon 1**	**PRELOGON="1"**	**1**
Windows のみ/ポータルにない この設定はシングル サインオン（SSO）と併用され、SSO に失敗した場合に認証情報のプロンプトをユーザーに表示するかど	**can-prompt-user-credential yes | no**	**CANPROMPTUSERCREDENTIAL= ”yes | no”**	**yes**

ポータルのエージェントの設定	Windows レジストリ/macOS Plist	Msiexec パラメータ	Default（フォルト）
うかを示します。			
Windows のみ/ポータルにない この設定により、サードパーティ認証情報プロバイダのタイルが Windows ログインページからフィルタされ、ネイティブ Windows タイルのみが表示されます。*	**wrap-cp-guid {third party credential provider guid}**	**WRAPCPGUID="{guid_value]" FILTERNONGPCP="yes | no"**	**no**
Windows のみ/ポータルにない この設定は wrap-cp-guid 設定の追加オプションで、ネイティブ Windows ログオン タイルだけでなくサードパーティ認証情報プロバイダのタイルも Windows ログイン ページに表示できるようにします。*	**filter-non-gpcp no**	n/a	n/a
Windows のみ/ポータルにない この設定では、静的 IP アドレスを Windows エ	**reserved-ipv4 <reserved-ipv4>** **reserved-ipv6 <reserved-ipv6>**	**RESERVEDIPV4="<reserved-ipv4>"** **RESERVEDIPV6="<reserved-ipv6>"**	n/a

ポータルのエージェントの設定	Windows レジストリ/macOS Plist	Msiexec パラメータ	Default（フォルト）
ンドポイントに割り当てることができます。			

Windows レジストリまたは*Windows*インストーラ（*Msiexec*）を使用してこれらの設定を有効にする詳細な手順は、Windows エンドポイントのサードパーティ認証情報プロバイダの SSO ラッピングを参照してください。

スクリプトの導入オプション

接続前後と切断前に GlobalProtect がスクリプトを開始できるようにするオプションは、以下の表の通りです。これらのオプションはポータル内で利用できないため、必要なキーの値（pre-vpn-connect、post-vpn-connect、または pre-vpn-disconnect）を Windows レジストリまたは macOS の plist で定義する必要があります。スクリプトをデプロイする詳細な流れについては、Windows レジストリを使用したスクリプトのデプロイ、Msiexec を使用したスクリプトのデプロイ、またはmacOS Plist を使用したスクリプトのデプロイを参照してください。

表：カスタマイズ可能なスクリプトの導入オプション

ポータルのエージェントの設定	Windows レジストリ/macOS Plist	Msiexec パラメータ	Default（フォルト）
コマンド設定で指定したスクリプト（スクリプトに渡されるすべてのパラメータを含む）を実行します。 環境変数も対応されています。 コマンド内のパス全体を指定します。	**command <parameter1> <parameter2> [...]** Windows 例： **command %userprofile%\vpn_script.bat c:test_user** macOS 例： **command $HOME/vpn_script.sh /Users/test_user test_user**	**PREVPNCONNECTCOMMAND=”<parameter1> <parameter2> [...]”** **POSTVPNCONNECTCOMMAND=”<parameter1> <parameter2> [...]”** **PREVPNDISCONNECTCOMMAND=”<parameter1> <parameter2> [...]”**	**n/a**
（任意）コマンドを実行できる権限を指定	**context admin | user**	**PREVPNCONNECTCONTEXT=”admin | user”**	**user**

ポータルのエージェントの設定	Windows レジストリ/ macOS Plist	Msiexec パラメータ	Default（フォルト）
します（デフォルトは user であり、コンテキストを指定しない場合、コマンドは現在のアクティブ ユーザーを実行します）。		**POSTVPNCONNECTCONTEXT= ”admin | user”** **PREVPNDISCONNECTCONTEXT= ”admin | user”**	
（任意）GlobalProtect アプリがコマンドを実行するまでの間に待機する時間を秒で指定します（範囲は 0～120）。コマンドがタイムアウトするまでに完了しなければ、アプリは接続を確立または切断するための処理を続行します。値 0（デフォルト）とはアプリがコマンドを実行するまで待機しないということです。 *post-vpn-connect* には対応していません。	**timeout** <**value**> 例: **timeout 60**	**PREVPNCONNECTTIMEOUT= ”**<**value**>**”** **POSTVPNCONNECTTIMEOUT= ”**<**value**>**”** **PREVPNDISCONNECTTIMEOUT= ”**<**value**>**”**	**0**
（任意）コマンドで使用されているファイルのパス全体を指定します。GlobalProtect アプリは、checksum キー内に指定された値を確認することでファイルの整合性を確認します。 環境変数も対応されています。	**file** <**path_file**>	**PREVPNCONNECTFILE= ”**<**path_file**>**”** **POSTVPNCONNECTFILE= ”**<**path_file**>**”** **PREVPNDISCONNECTFILE= ”**<**path_file**>**”**	**n/a**

ポータルのエージェントの設定	Windows レジストリ/ macOS Plist	Msiexec パラメータ	Default（フォルト）
（任意）file キーで参照される、ファイルの sha256 チェックサムを指定します。チェックサムを指定すると、GlobalProtect アプリが生成したチェックサムがここで指定したチェックサム値と合致する場合にのみ、GlobalProtect アプリがそのコマンドを実行するようになります。	**checksum** <**value**>	**PREVPNCONNECTCHECKSUM= n/a ”<value>”** **POSTVPNCONNECTCHECKSUM= ”<value>”** **PREVPNDISCONNECTCHECKSUM =”<value>”**	
（任意）コマンドを実行できないか、またはコマンドがゼロ以外の戻りコードで終了したことをユーザーに知らせるエラー メッセージを指定します。 メッセージは *1,024* 文字以下の *ANSI* 文字とします。	**error-msg** <**message**> 例: **error-msg Failed executing pre-vpn-connect action!**	**PREVPNCONNECTERRORMSG= n/a ”<message>”** **POSTVPNCONNECTERRORMSG= ”<message>”** **PREVPNDISCONNECTERRORMSG =”<message>”**	

Windows エンドポイントへのアプリ設定のデプロイ

Windows レジストリまたは Windows インストーラ（Msiexec）を使用して、GlobalProtect アプリおよび設定を Windows エンドポイントに透過的にデプロイします。

- Windows レジストリでのエージェント設定のデプロイ
- エージェントの設定の MSIEXEC からのデプロイ
- Windows レジストリを使用したスクリプトのデプロイ
- Msiexec を使用したスクリプトのデプロイ
- Windows エンドポイントのサードパーティ認証情報プロバイダの SSO ラッピング

- Windows レジストリを使用したサードパーティ認証情報の SSO ラッピングの有効化
- Windows インストーラを使用したサードパーティ認証情報の SSO ラッピングの有効化

Windows レジストリでのアプリ設定のデプロイ

GlobalProtect ポータルに初めて接続する前に、Windows レジストリを使用して、Windows エンドポイントへの GlobalProtect アプリ設定のデプロイを有効にできます。以下の表で説明されているオプションを使用して、Windows レジストリを使用して Windows エンドポイントのアプリケーション設定をカスタマイズします。

Windows レジストリを使用して *GlobalProtect* アプリ設定をデプロイするだけでなく、*GlobalProtect* アプリが *Windows* エンドポイントから特定の *Windows* レジストリ情報を収集できるようにすることもできます。その後、データをモニターして、一致条件としてセキュリティ ルールに追加できます。定義したレジストリ設定に一致するエンドポイント トラフィックは、セキュリティ ルールに従って適用することができます。さらに、カスタム チェックをセットアップしてエンドポイントからのアプリケーションおよびプロセス データの収集を行うことができます。

STEP 1 | Windows レジストリで、GlobalProtect アプリのカスタマイズ設定を見つけます。

Windows レジストリを開き (コマンド プロンプトで **regedit** と入力する)、次の場所に移動します。

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

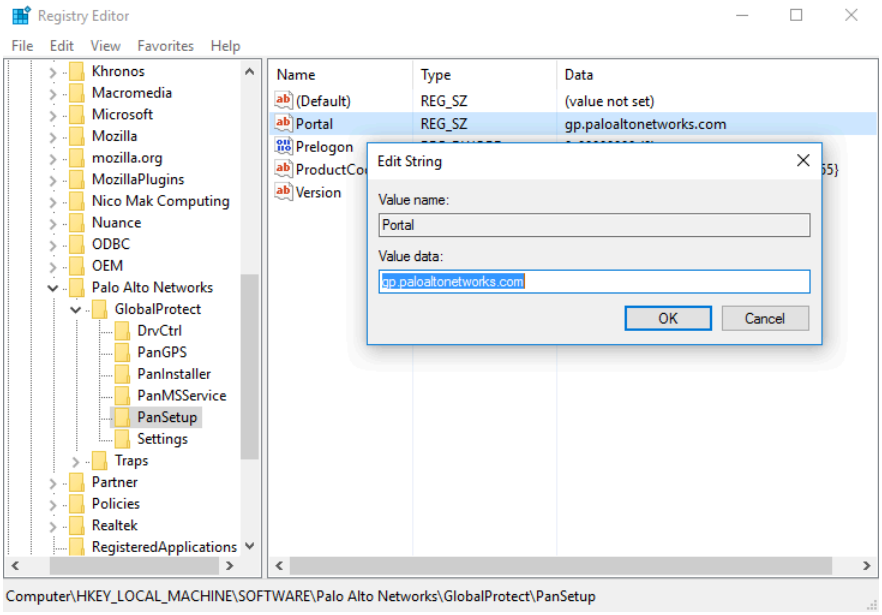
STEP 2 | ポータル名を設定します。

初めての接続であっても、エンド ユーザーがポータル アドレスを手動で入力せずに済むようにする場合、ポータル アドレスを Windows レジストリを介して事前にデプロイします。

1. Window レジストリで次に移動します：

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

2. **Portals**（ポータル）を右クリックして **Modify**（変更）を選択します。
3. **Value data**（値データ）フィールドにポータル名を入力して、**OK** をクリックします。



STEP 3 | GlobalProtect アプリとシングルサインオン（SSO）の接続方法など、Windows エンドポイントにさまざまな設定をデプロイします。

Windows レジストリを使用してセットアップできるコマンドおよび値の完全なリストは、カスタマイズ可能なアプリの設定を参照してください。

STEP 4 | GlobalProtect アプリが Windows エンドポイントのサードパーティ認証情報をラップできるようにします。これにより、サードパーティ認証情報プロバイダが使用されている場合でも SSO を使用できます。

Windows レジストリを使用したサードパーティ認証情報の SSO ラッピングの有効化を行います。

アプリ設定の MSIEXEC からのデプロイ

Windows エンドポイントでは、次の構文を使用して、Windows インストーラ（Msiexec）から GlobalProtect アプリとアプリ設定を自動的にデプロイするオプションがあります。

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec は実行可能なプログラムで、コマンドラインから製品をインストールまたは設定します。*Microsoft Windows XP* 以降の *OS* でエンドポイントが作動する際、コマンドプロンプトで使える文字列の最大長は *8,191* 文字です。

Msiexec の例	説明
`msiexec.exe /i GlobalProtect.msi /quiet PORTAL=”portal.acme.com”`	クワイエット モード（ユーザーの操作なし）で GlobalProtect をインストールし、ポータルのアドレスを設定します。
`msiexec.exe /i GlobalProtect.msi CANCONTINUEIFPORTALCERTINVALID= ”no”`	証明書が有効でない場合にユーザーがポータルに接続するのを拒否するオプションを付けて、GlobalProtect をインストールします。

すべての設定の一覧および対応するデフォルト値は、カスタマイズ可能なアプリの設定を参照してください。

indows インストーラを使用したサードパーティ認証情報の SSO ラッピングの有効化も可能です。

Windows レジストリを使用したスクリプトのデプロイ

Windows レジストリを用いて Windows エンドポイントへカスタム スクリプトをデプロイできます。

GlobalProtect アプリを、指定なしまたはすべての以下のイベントに対してスクリプトを開始し実行するよう設定できます：トンネル確立前後、トンネル切断前後。特定のイベントでスクリプトを実行するには、そのイベント用のコマンド レジストリ エントリからバッチ スクリプトを参照します。

構成設定に応じて、アプリがゲートウェイへの接続を確立する前と後で、そしてアプリの接続が切断される前に、GlobalProtect アプリはスクリプトを実行できます。Windows レジストリを使用して Windows エンドポイントのアプリ設定をカスタマイズするには、次のワークフローを使用します。

スクリプトの展開を可能にするレジストリ設定は、*GlobalProtect App 2.3* 以降のリリースを実行しているエンドポイントでサポートされています。

STEP 1 | Windows レジストリを開いて、GlobalProtect アプリのカスタマイズ設定を見つけます。

Windows レジストリを開いて（コマンド プロンプトで **regedit** と入力）、スクリプトを実行するタイミング（プリ/ポスト接続またはプリ切断）に応じて、次のキーのいずれかに移動します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
\pre-vpn-connect
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
\post-vpn-connect
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings
\pre-vpn-disconnect
```

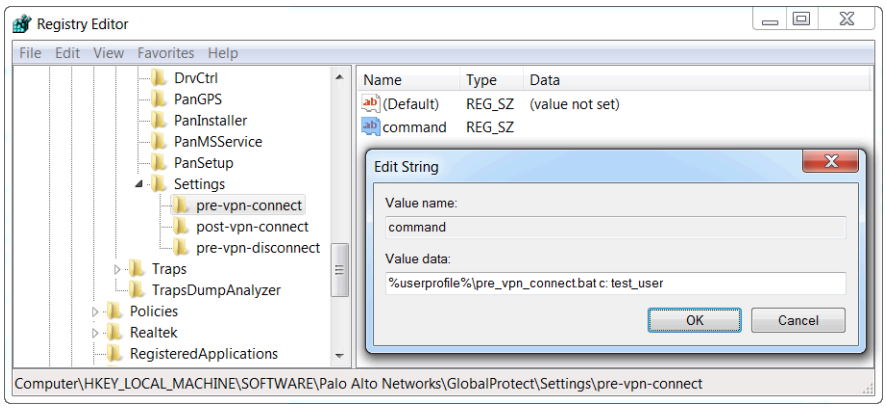
キーが***Settings***（設定）キーになければ、（***Settings***（設定）を右クリックし***New***（新規） > ***Key***（キー）を選択してそれを作ります。

STEP 2 | GlobalProtect アプリがスクリプトを実行できるように `command`（コマンド） という名前の新規文字列値を作ります。

ここで指定するバッチファイルには、デバイス上で実行する特定のスクリプト（スクリプトに渡されれる何らかのパラメータを含む）を含むようにします。

1. `command`（コマンド） 文字列がまだない場合、作成します（`pre-vpn-connect` キー、`post-vpn-connect` キー、または `pre-vpn-disconnect` キーを右クリックして、**New**（新規） > **String Value**（文字列値）を選択し、**command** と名付ける）。
2. `command`（コマンド）を右クリックして **Modify**（変更）を選択します。
3. GlobalProtect アプリが実行するコマンドまたは文字列を入力します。以下に例を示します。

```
%userprofile%\pre_vpn_connect.bat c:
test_user
```



STEP 3 | （任意）各コマンドに必要に応じて追加レジストリ エントリを追加します。

レジストリ文字列と対応する値を作成または変更します。これはcontext、timeout、file、checksum、または error-msg を含みます。詳しい情報については、カスタマイズ可能なアプリの設定を参照してください。

Msiexec を使用したスクリプトのデプロイ

Windows エンドポイント上で、Windows Installer (Msiexec) を使って GlobalProtect アプリ、アプリ設定、アプリが自動で実行するスクリプトをデプロイできます（カスタマイズ可能なアプリの設定を参照してください）。これを行うには、以下の構文を使用します：

```
msiexec.exe /i GlobalProtect.msi <SETTING>="<value>"
```

Msiexec は実行可能なプログラムで、コマンドラインから製品をインストールまたは設定します。*Microsoft Windows XP* 以降でシステムが作動する際、 コマンドプロンプトで使える文字列の最大長は *8,191* 文字です。

この制限はコマンドライン、他のプロセスに引き継がれる個々の環境変数（*USERPROFILE* 変数など）、すべての環境変数拡張子に適用されます。バッチファイルをコマンドラインから実行する場合、制限はまたバッチファイル処理に適用されます。

例えば、特定の接続または切断イベントで実行するスクリプトをデプロイするには、以下の例に類似する構文を使用できます。

例:接続イベント前に実行するスクリプトをデプロイするための **Msiexec** の使用

こちらにコピーアンドペーストができるスクリプトがあります。

```
msiexec.exe /i GlobalProtect.msi
PREVPNCONNECTCOMMAND="%userprofile%\pre_vpn_connect.bat c:
 test_user"
PREVPNCONNECTCONTEXT="user"
PREVPNCONNECTTIMEOUT="60"
PREVPNCONNECTFILE="C:\Users\test_user\pre_vpn_connect.bat"
PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf599"
PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
```

すべての設定の一覧および対応するデフォルト値は、カスタマイズ可能なアプリの設定を参照してください。

例:事前接続、事後接続、事前切断イベント時に実行するスクリプトをデプロイするための **Msiexec** の使用

こちらにコピーアンドペーストができるスクリプトがあります。

```
msiexec.exe /i GlobalProtect.msi
PREVPNCONNECTCOMMAND="%userprofile%\pre_vpn_connect.bat c:
 test_user"
PREVPNCONNECTCONTEXT="user"
PREVPNCONNECTTIMEOUT="60"
PREVPNCONNECTFILE="C:\Users\test_user\pre_vpn_connect.bat"
PREVPNCONNECTCHECKSUM="a48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf599"
PREVPNCONNECTERRORMSG="Failed executing pre-vpn-connect action."
POSTVPNCONNECTCOMMAND="c:\users\test_user\post_vpn_connect.bat c:
 test_user"
POSTVPNCONNECTCONTEXT="admin"
POSTVPNCONNECTFILE="%userprofile%\post_vpn_connect.bat"
POSTVPNCONNECTCHECKSUM="b48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b011
8647ccf598"
POSTVPNCONNECTERRORMSG="Failed executing post-vpn-connect action."
PREVPNDISCONNECTCOMMAND="%userprofile%\pre_vpn_disconnect.bat c:
 test_user"
PREVPNDISCONNECTCONTEXT="admin"
PREVPNDISCONNECTTIMEOUT="0"
PREVPNDISCONNECTFILE="C:\Users\test_user\pre_vpn_disconnect.bat"
PREVPNDISCONNECTCHECKSUM="c48ad33695a44de887bba8f2f3174fd8fb01a46a19e3ec9078b0
118647ccf597"
PREVPNDISCONNECTERRORMSG="Failed executing pre-vpn-disconnect
 action."
```

すべての設定の一覧および対応するデフォルト値は、カスタマイズ可能なアプリの設定を参照してください。

Windows エンドポイントのサードパーティ認証情報プロバイダの SSO ラッピング

Windows 7 のエンドポイント上では、GlobalProtect アプリは Microsoft Credential Provider フレームワークを活用してシングル サインオン（SSO）をサポートします。SSO では GlobalProtect の認証情報プロバイダーが Windows のネイティブの Credential Provider をラップすることで、GlobalProtect が Windows のログイン情報を使用して自動的に認証を行い、GlobalProtect ポータルおよびゲートウェイに接続できるようになっています。さらに、Windows 10 ユーザーは、SSO ラッピングにより、パスワードの有効期限が切れたとき、または次回のログイン時に管理者がパスワードの変更を要求したときに、GlobalProtect 資格情報プロバイダを使用して Active Directory（AD）パスワードを更新できます。

エンドポイントに他のサードパーティ認証情報プロバイダも存在する場合は、GlobalProtect の認証情報プロバイダはユーザーの Windows ログイン情報を収集できません。その結果、GlobalProtect が GlobalProtect ポータルおよびゲートウェイに自動接続できなくなります。SSO が失敗する場合は、サードパーティ認証情報プロバイダを特定し、GlobalProtect アプリがそのサードパーティによる認証情報をラップするように設定することで、Windows ログイ

ン情報のみを使って Windows、GlobalProtect、そのサードパーティ認証情報プロバイダへの認証を行えるようになります。

また任意で、Windows にて別のログイン タイル（認証情報プロバイダー毎に 1 つ、ネイティブの Windows ログイン用にもう 1 つ）を表示するように設定することもできます。これは、サードパーティ認証情報プロバイダが、GlobalProtect に適用されない機能を追加している場合に役立ちます。

Windows エンドポイントから *GlobalProtect* の認証情報プロバイダーを削除するには、コマンドプロンプトで ***GlobalProtectPanGPS.exe -u*** コマンドを実行します。

Windows レジストリまたは Windows インストーラ（`msiexec`）を使用して、GlobalProtect がサードパーティ認証情報をラップできるようにすることができます。

- Windows レジストリを使用したサードパーティ認証情報の SSO ラッピングの有効化
- Windows インストーラを使用したサードパーティ認証情報の SSO ラッピングの有効化

サードパーティ認証情報プロバイダ（*CP*）の *GlobalProtect SSO* ラッピングはサードパーティ *CP* 設定に依存しています。一部のケースでは、サードパーティ *CP* の実装により *GlobalProtect* が *CP* を正常にラップができるようになっている場合、*GlobalProtect SSO* ラッピングが正常に機能しない可能性があります。

Windows レジストリを使用したサードパーティ認証情報の SSO ラッピングの有効化

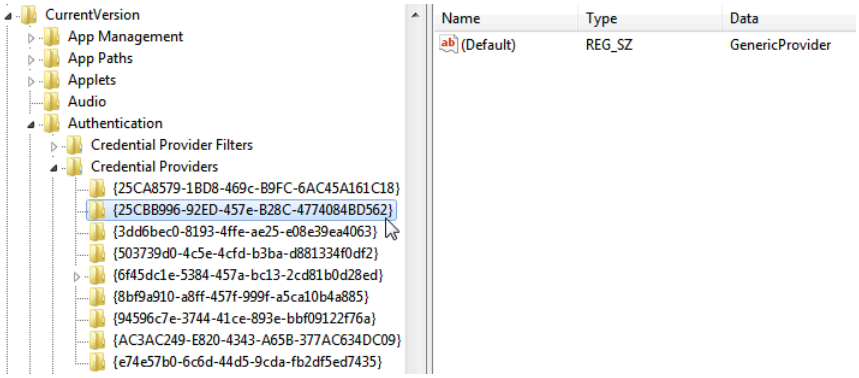
Windows レジストリで以下の手順を実行して、SSO で Windows 7 エンドポイントのサードパーティ認証情報をラップできるようにすることができます。

STEP 1 | Windows レジストリを開いて、ラップするサードパーティ認証情報プロバイダのグローバル一意識別子（GUID）を見つけます。

1. コマンド プロンプトで **regedit** コマンドを入力し、Windows レジストリ エディタを開きます。
2. 現在インストールされている証明書プロバイダのリストを表示するには、次の Windows レジストリの場所に移動します：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion
   \Authentication\Credential Providers.
   ```

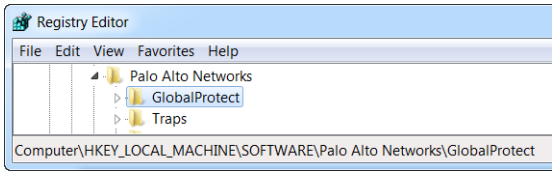
3. ラップする認証情報プロバイダの GUID キー（GUID の両端の波かっこ { および } を含む）をコピーします。



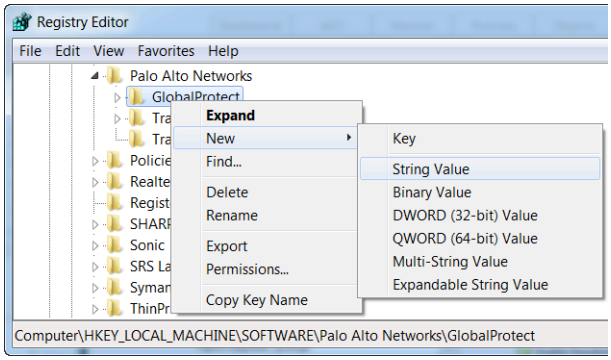
STEP 2 | **wrap-cp-guid** 設定を GlobalProtect レジストリに追加して、サードパーティ認証情報プロバイダの SSO ラッピングを有効にします。

1. Windows レジストリの以下の場所に移動します。

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



2. **GlobalProtect** フォルダを右クリックしてから、**New**（新規） > **String Value**（文字列値）を選択して新しい文字列値を選択します：



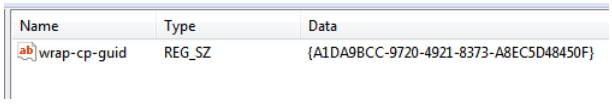
3. 次の **String Value**（文字列値）フィールドを設定します：
   - 名前: **wrap-cp-guid**
   - 値のデータ: {<**third-party credential provider GUID**>}

     [値のデータ] フィールドに入力する *GUID* 値は、波かっこ *{* および *}* で囲む必要があります。

     以下に、**Value data**（値のデータ）フィールドのサードパーティ認証情報プロバイダ GUID の例を示します。

```
{A1DA9BCC-9720-4921-8373-A8EC5D48450F}
```

新しい**String Value**（文字列値）の場合、文字列値の **Name**（名前）として `wrap-cp-guid`が表示され、**Value Data**（値データ）として GUID が表示されます。



STEP 3 | 次のステップ：

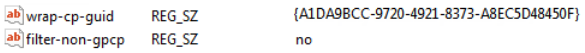
- このセットアップにより、ログオン画面にネイティブ Windows ログオン タイルがユーザーに表示されます。ユーザーはタイルをクリックして自身の Windows 認証情報でシス

テムにログインすると、そのシングルログインでユーザーは Windows、GlobalProtect、サードパーティーの認証情報プロバイダの認証を受けます。

- （任意）ログオン画面に複数のタイル（たとえば、ネイティブの Windows タイルとサード パーティの証明書プロバイダ用のタイル）を表示する場合は、ステップ 4 に進みます。
- （オプション）ユーザーにデフォルトの証明書プロバイダを割り当てる場合は、ステップ 5 に進みます。
- （オプション）ログオン画面でユーザーにデフォルトの証明書プロバイダ タイルを非表示にする場合は、ステップ 6 に進みます。

STEP 4 | （任意）サードパーティ認証情報プロバイダのタイルをログイン時にユーザーに表示できるようにします。

`filter-non-gpcp` という **Name**（名前）の 2 つ目の **String Value**（文字列値）を追加して、文字列の **Value data**（値のデータ）として **no** と入力します。



この文字列値を GlobalProtect の設定に追加すると、Windows のログオン画面で、ネイティブ Windows タイルとサードパーティの証明書プロバイダのタイルの 2 つのログイン オプションがユーザーに表示されます。

STEP 5 | ユーザー ログイン用にデフォルトの証明書プロバイダを割り当てます。

1. Windows レジストリを開いて、デフォルトの証明書プロバイダとして割り当てるサードパーティ認証情報プロバイダのグローバル一意識別子（GUID）を見つけます。
   1. コマンド プロンプトで `regedit` コマンドを入力し、Windows レジストリ エディタを開きます。
   2. 現在インストールされている証明書プロバイダのリストを表示するには、次の Windows レジストリの場所に移動します：

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion
      \Authentication\Credential Providers.
      ```
   3. 認証情報プロバイダの完全な GUID キー（GUID の両端の波かっこ **{** および **}** を含む）をコピーします。
2. ローカル グループ ポリシー エディタを開き、デフォルトの証明書プロバイダを有効にして割り当てます。
   1. コマンド プロンプトで `gpedit.msc` コマンドを入力し、ローカル グループ ポリシー エディタを開きます。
   2. **Computer Configuration**（コンピュータ設定） > **Administrative Templates**（管理用テンプレート） > **System**（システム） > **Logon**（ログオン）の順に選択します。
   3. **Setting**（設定）で、**Assign a default credential provider**（デフォルトの証明書プロバイダの割り当て）を右クリックして、**Assign a default credential provider**（デフォルトの証明書プロバイダの割り当て）ウィンドウを開きます。
   4. 該当するポリシーを **Enabled**（有効）にします。
   5. **Assign the following credential provider as the default credential provider**（次の証明書プロバイダをデフォルトの証明書プロバイダに割り当てる）で、（Windows レジストリからコピーされた）証明書プロバイダの GUID を入力します。
   6. **Apply**（適用）をクリックして **OK** をクリックすると変更内容が保存されます。

STEP 6 | （オプション）Windows のログオン画面からサード パーティの証明書プロバイダのタイルを非表示にします。

1. Windows レジストリを開いて、非表示するサードパーティ認証情報プロバイダのグローバル一意識別子（GUID）を見つけます。
   1. コマンド プロンプトで `regedit` コマンドを入力し、Windows レジストリ エディタを開きます。
   2. 現在インストールされている証明書プロバイダのリストを表示するには、次の Windows レジストリの場所に移動します：

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion
      \Authentication\Credential Providers.
      ```
   3. 非表示にする認証情報プロバイダの完全な GUID キー（GUID の両端の波かっこ **{** および **}** を含む）をコピーします。
2. ローカル グループ ポリシー エディタを開き、サードパーティの証明書プロバイダを非表示にします。
   1. コマンド プロンプトで `gpedit.msc` コマンドを入力し、ローカル グループ ポリシー エディタを開きます。
   2. **Computer Configuration**（コンピュータ設定） > **Administrative Templates**（管理用テンプレート） > **System**（システム） > **Logon**（ログオン）の順に選択します。
   3. **Setting**（設定）で、**Exclude credential providers**（証明書プロバイダを除外する）を右クリックして、**Exclude credential providers**（証明書プロバイダを除外する）ウィンドウを開きます。
   4. 該当するポリシーを **Enabled**（有効）にします。
   5. **Exclude credential providers**（証明書プロバイダを除外する）で、非表示にする（Windowsレジストリからコピーされた）証明書プロバイダの GUID を入力します。

      複数の証明書プロバイダを非表示にするには、各 *GUID* をカンマで区切ります。
   6. **Apply**（適用）をクリックして **OK** をクリックすると変更内容が保存されます。

STEP 7 | 変更内容を最終確定します。

最終確定後にシステムを再起動すると、変更内容が反映されます。

Windows インストーラを使用したサードパーティ認証情報の SSO ラッピングの有効化

Windows インストーラ MSIEXEC で以下のオプションを使用して、SSO で Windows 7 エンドポイントのサードパーティ認証情報プロバイダをラップできるようにすることができます。

サードパーティ認証情報をラップして、ログイン時にユーザーにネイティブ タイルを表示します。ユーザーは、タイルをクリックし、ネイティブ Windows 認証情報を使用でエンドポ

イントにログインできます。ユーザーは 1 回のログインで Windows、GlobalProtect、およびサードパーティの証明書プロバイダに対して認証を受けることができます。

Windows インストーラ（MSIEXEC）で以下の構文を使用します。

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}"
 FILTERNONGPCP="yes"
```

上記の構文の **FILTERNONGPCP** パラメータでは、サードパーティ認証情報を使用してシステムにログオンするオプションをフィルタし、ユーザーの認証を簡略化します。

ユーザーがサードパーティ認証情報を使用してログインできるようにするには、Windows Installer（MSIEXEC）で以下の構文を使用します。

```
msiexec.exe /i GlobalProtect.msi WRAPCPGUID="{guid_value}"
FILTERNONGPCP="no"
```

上記の構文の **FILTERNONGPCP** パラメータは **"no"** に設定されているため、サードパーティ認証情報プロバイダのログオン タイルを除外してネイティブ タイルのみを表示します。この場合、Windows システムにログオンするときに、ネイティブ Windows タイルとサードパーティ認証情報プロバイダのタイルの両方がユーザーに表示されます。

macOS エンドポイントへのアプリ設定のデプロイ

macOS グローバル plist（プロパティ リスト）ファイルを使用して、GlobalProtect アプリのカスタマイズ設定を設定するか、または macOS エンドポイントにスクリプトをデプロイします。

- macOS Plist でのアプリ設定のデプロイ
- macOS Plist を使用したスクリプトのデプロイ

macOS Plist でのアプリ設定のデプロイ

macOS グローバル plist（プロパティ リスト）ファイルで GlobalProtect アプリのカスタマイズ設定を行うことができます。これにより、GlobalProtect ポータルに初めて接続する前に、macOS エンドポイントへの GlobalProtect アプリの設定のデプロイが有効になります。

macOS エンドポイントでは、plist ファイルは `/Library/Preferences` または `~/Library/Preferences` のいずれかにあります。波型（~）シンボルは、場所が現在のユーザーのホームフォルダにあることを示します。macOS エンドポイントの GlobalProtect アプリは、最初に使用する GlobalProtect plist 設定をチェックします。この場所に plist がない場合、GlobalProtect アプリは `~/Library/Preferences` で plist 設定を検索します。

macOS plist を使用して *GlobalProtect* アプリ設定をデプロイするだけでなく、*GlobalProtect* アプリがエンドポイントから特定の *macOS plist* 情報を収集できるようにすることもできます。その後、データをモニターして、一致条件としてセキュリティ ルールに追加できます。定義したレジストリ設定に一致するエンドポイント トラフィックは、セキュリティ ルールに従って適用することができます。さらに、カスタム チェックをセットアップしてエンドポイントからのアプリケーションおよびプロセス データの収集を行うことができます。

STEP 1 | GlobalProtect plist ファイルを開いて、GlobalProtect アプリのカスタマイズ設定を見つけます。

Xcode または代わりとなる plist エディタを使用して plist ファイルを開きます。

`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`

次に、

`/Palo Alto Networks/GlobalProtect/Settings` に移動します。

`Settings` ディクショナリが存在しない場合は、作成します。各キーを文字列として `Settings` ディクショナリに追加します。

STEP 2 | ポータル名を設定します。

初めての接続であっても、エンド ユーザーがポータル アドレスを手動で入力せずに済むようにする場合、ポータル アドレスを plist を介して事前にデプロイします。`PanSetup` ディクショナリにおいて、 `Portal` のエントリを設定します。

STEP 3 | GlobalProtect アプリの接続方法など、macOS エンドポイントにさまざまな設定をデプロイします。

macOS plist を使用して設定できるキーおよび値の完全なリストは、カスタマイズ可能なアプリの設定を参照してください。

macOS Plist を使用したスクリプトのデプロイ

ユーザーが初めて GlobalProtect ゲートウェイに接続する場合、 GlobalProtect アプリが設定ファイルをダウンロードし、GlobalProtect Mac プロパティ ファイル (plist) にアプリ設定を保存します。アプリ設定の変更に加えて、plist を使っていずれまたはすべての以下のイベントに対してスクリプトをデプロイできます：トンネル確立前後、トンネル切断前後。以下のワークフローを使って、スクリプトを macOS エンドポイントにデプロイするために Mac plist を使います。

スクリプトの展開を可能にする *macOS plist* 設定は、*GlobalProtect App 2.3* 以降のリリースを実行しているエンドポイントでサポートされています。

STEP 1 | (エンドポイントが実行する Mac OS X 10.9 以降の OS) 設定キャッシュを点滅します。これにより plist への変更後 OS がキャッシュした preference を使わなくなります。

デフォルトの preferences キャッシュをクリアするには、**`killall cfprefsd`** コマンドを macOS 端末から実行します。

STEP 2 | GlobalProtect plist ファイルを開き、 接続または切断イベントに関連する GlobalProtect ディクショナリを見つけるか作成します。設定を追加するディクショナリは GlobalProtect アプリがスクリプトを実行するタイミングを決定します。

Xcode または代替 plist エディタを使って plist ファイル（`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`）を開き、次のディクショナリのいずれかの場所に移動します。

- `/PaloAlto Networks/GlobalProtect/Settings/pre-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/post-vpn-connect`
- `/Palo Alto Networks/GlobalProtect/Settings/pre-vpn-disconnect`

Settings ディクショナリが存在しない場合は、作成します。それから、*Settings*で、スクリプトを実行するイベント用の新規ディクショナリを作ります。

STEP 3 | **command** という名前の新規 `String`（文字列）を作成して、GlobalProtect アプリがスクリプトを実行できるようにします。

ここで指定する値には、お使いのエンドポイント上で実行するシェルスクリプト（スクリプトに渡される何らかのパラメータ）を参照するようにします。

`command`（コマンド） 文字列がまだ存在していない場合は、ディクショナリに追加してスクリプトとパラメータを**Value**（値）フィールドで次のように指定します：以下に例を示します。

```
$HOME\pre_vpn_connect.sh
/Users/username username
```

環境変数も対応されています。

ベストプラクティスとして、コマンド内のパス全体を指定します。

STEP 4 | （任意）管理者権限、スクリプトのタイムアウト値、バッチファイルのチェックサム値、コマンドが実行に失敗した際表示されるエラーメッセージを含む、コマンドに関する追加設定を追加します。

plist 内のその他の文字列 (`context`、`timeout`、`file`、`checksum`、`error-msg`) を作成または変更し、対応する値を入力します。詳しい情報については、カスタマイズ可能なアプリの設定を参照してください。

STEP 5 | plist ファイルに変更を保存します。

plist を保存します。

GlobalProtect クライアントレス VPN

GlobalProtect クライアントレス VPN を使用すれば、一般的なエンタープライズ Web アプリケーションに安全にリモート アクセスできます。ユーザーは GlobalProtect ソフトウェアをインストールすることなく、SSL 対応の Web ブラウザから安全なアクセスを利用できます。これは、パートナーや契約業者をアプリケーションにアクセスできるようにしたり、個人エンドポイントなどの管理対象外のアセットを安全に利用できるようにしたりしなければならない状況に便利です。ユーザーおよびユーザー グループに基づいて Web アプリケーションへのアクセスを提供するように GlobalProtect ポータルのランディング ページを設定でき、SAML 対応のアプリケーションへのシングルサインオンを許可することもできます。以下のトピックでは、クライアントレス VPN を設定してトラブルシューティングする方法を説明しています。

クライアントレス VPN の概要

GlobalProtect クライアントレス VPN を設定すると、リモート ユーザーは Web ブラウザを使用して GlobalProtect ポータルにログインし、公開された Web アプリケーションを起動できます。ユーザーまたはユーザー グループに基づいて、ユーザーに一連のアプリケーションへのアクセスを許可したり、カスタム アプリケーション URL を入力することによるその他の企業アプリケーションへのアクセスを許可したりできます。

ユーザーがポータルにログインすると、起動できる Web アプリケーションのリストと共に公開されたアプリケーション ページが表示されますGlobalProtect ポータルでアプリケーションのデフォルトのランディング ページを使用することも、自社用にカスタム ランディング ページを作成することもできます。

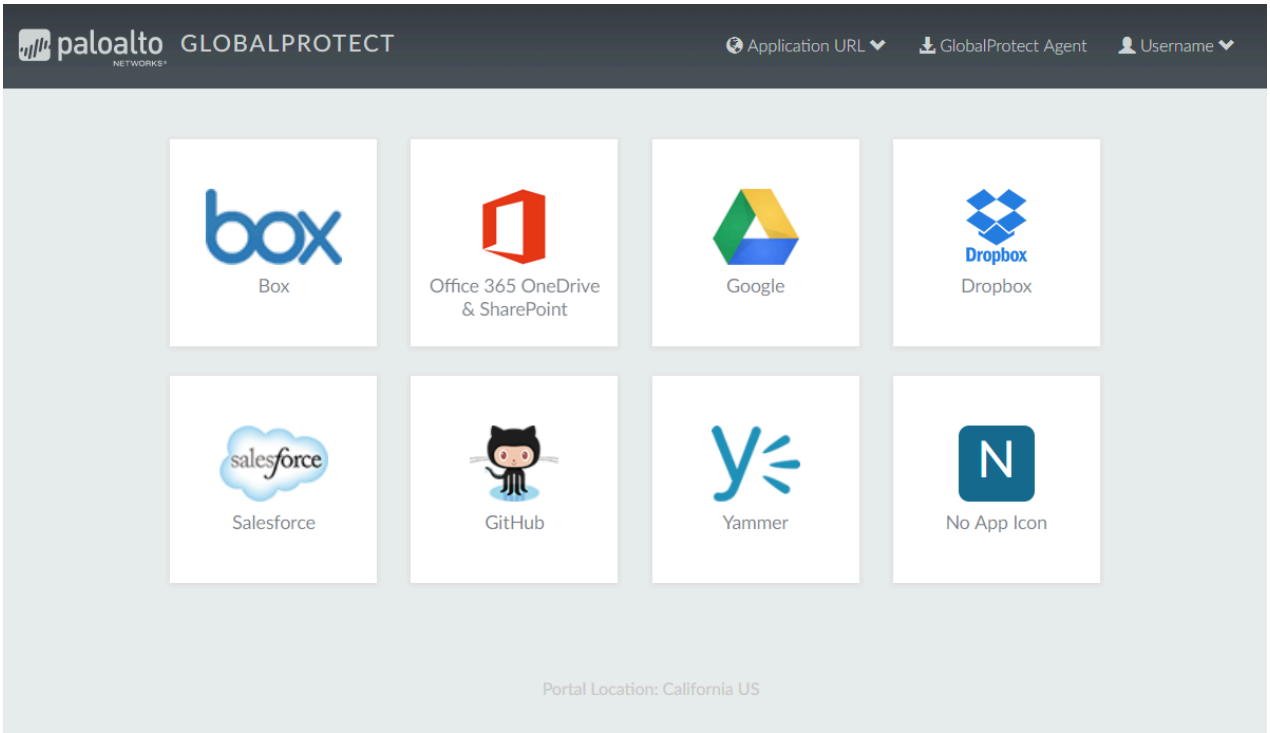


図 **3 :** クライアントレス **VPN** のアプリケーションのランディング ページ

このページはポータルのデフォルトのランディング ページからの置き換えとなるため、GlobalProtect アプリのダウンロード ページへのリンクが含まれます。設定している場合、ユーザーは **Application URL**（アプリケーション **URL)** を選択して URL を入力し、公開されていないその他の企業 Web アプリケーションを起動することもできます。

公開されたアプリケーション ページを表示する代わりに 1 つの Web アプリケーションのみを設定した場合（かつ公開されていないアプリケーションへのアクセスを禁止した場合）、ユーザーがログインすると直ちにそのアプリケーションが自動的に起動します。GlobalProtect クライアン

トレス VPN を設定していない場合、ユーザーがポータルにログインするとアプリ ソフトウェアのダウンロード ページが表示されます。

GlobalProtect クライアントレス VPN を設定する場合、セキュリティ ポリシーで GlobalProtect エンドポイントから公開されたアプリケーション ランディング ページをホストする GlobalProtect ポータルに関連付けられたセキュリティ ゾーンへのトラフィックと、GlobalProtect ポータル ゾーンから公開されたアプリケーション サーバーがホストされるセキュリティ ゾーンへのユーザーベースのトラフィックを許可する必要があります。定義するセキュリティ ポリシーによって、公開された各アプリケーションを使用する権限をどのユーザーに付与するかが決まります。

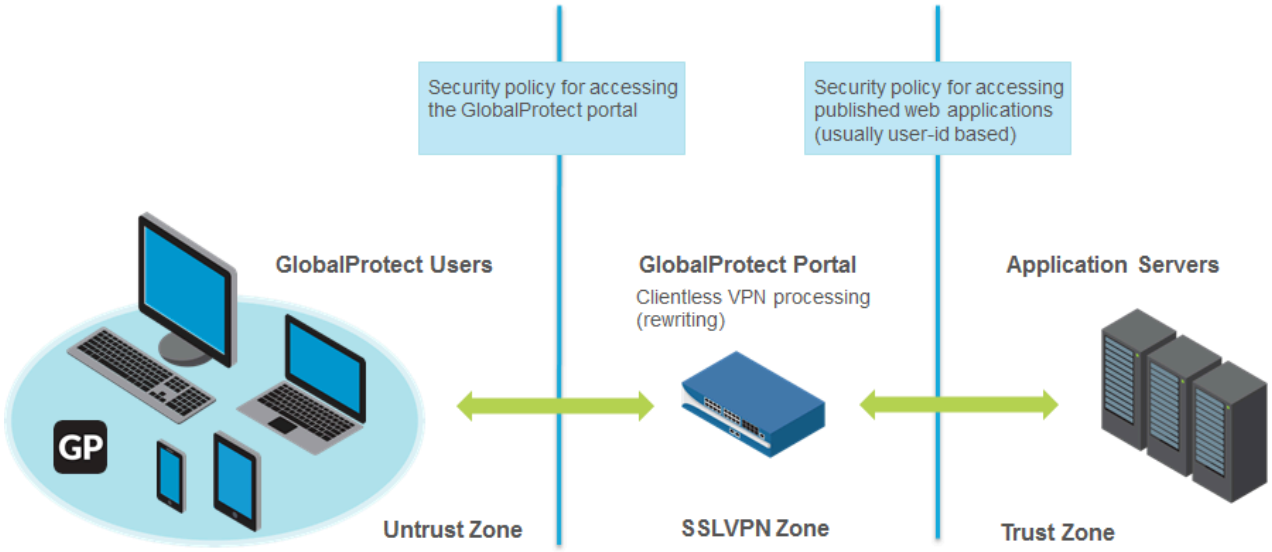


図 **4 :** クライアントレス **VPN** のゾーンおよびセキュリティ ポリシー

サポートされるテクノロジ

一般的なエンタープライズ Web アプリケーションへの安全なリモート アクセスを提供するように GlobalProtect ポータルを設定できます。最適な結果を得るには、必ずデプロイまたは多数のユーザーへの使用を許可する前に、制御された環境でクライアントレス VPN アプリケーションを徹底的にテストしてください。

Technology（テクノロジ）	サポートされるバージョン

Web アプリケーション テクノロジ	• HTML
	• HTML5
	• HTML5-Web-Sockets
	• Javascript
	• リモートデスクトップ プロトコル（RDP）、VNC、または SSH
	  • Citrix XenApp および XenDesktop あるいは VMWare Horizon および Vcenter のような仮想デスクトップ インフラストラクチャ（VDI）および仮想マシン（VM）環境は、HTML5 経由のアクセスをネイティブでサポートしています。サードパーティ製のミドルウェアを追加することなく、クライアントレス VPN 経由でこれらのマシンにRDP、VNC、SSH接続できます。
	  • HTML5や、クライアントレス VPN がサポートしている他のウェブアプリケーション技術がネイティブでサポートされていない環境では、HOBLink、Thinfinity などのサードパーティのベンダーを使ってクライアントレス VPN 経由で RDP 接続できます。
	• Adobe Flash—クライアントレス VPN を使用すれば、ブラウザは Adobe Flash、Microsoft Word ドキュメント、Adobe PDF を使用するコンテンツを提供できます。しかし、クライアントレス VPN は Adobe Flash、Microsoft Word ドキュメント、Adobe PDF 内の HTML、URL、リンクを書き換えられないため、そのようなコンテンツが正しく表示されない場合があります。
	その他の技術（Microsoft Sliverlight や XML/XSLT など）はサポートされていません。

オペレーティング システム	• Windows • macOS • iOS • Android • Chrome

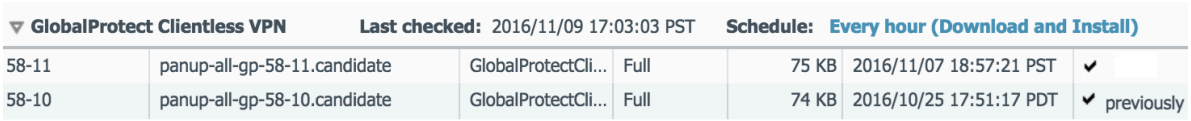
Technology（テクノロジ）	サポートされるバージョン
	• Linux Linux
サポートされるブラウザ	• Chrome • エッジ • Internet Explorer • Safari • Firefox

クライアントレス VPN の設定

GlobalProtect クライアントレス VPN を設定するには、以下の手順を実行します。

STEP 1 | 開始する前に：

- GlobalProtect ポータルからクライアントレス VPN をホストするファイアウォールに GlobalProtect サブスクリプションをインストールします。アクティブなライセンスとサブスクリプションを参照してください。
- 最新バージョンの GlobalProtect Clientless VPN ダイナミック更新をインストールして（Install Content and Software Updates（コンテンツとソフトウェア更新のインストール）を参照）、新しいダイナミックコンテンツ更新のインストールのスケジュールを設定します。ベストプラクティスとして、GlobalProtect Clientless VPN の最新のコンテンツ更新を常にインストールすることをお勧めします。



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

- ベスト プラクティスとしては、クライアントレス VPN をホストする GlobalProtect ポータル用に個別の FQDN を設定します。PAN-OS Web インターフェイスと同じ FQDN は使用しないでください。
- 標準 SSL ポート（TCP ポート 443）で GlobalProtect ポータルをホストします。非標準ポートはサポートされません。

STEP 2 | GlobalProtect クライアントレス VPN を使用できるアプリケーションを設定します。GlobalProtect ポータルでは、ユーザーがログインしたときにこれらのアプリケーションがランディング ページに表示されます（アプリケーション ランディング ページ）。

1. **Network**（ネットワーク） > **GlobalProtect** > **Clientless Apps**（クライアントレス アプリ）の順に選択して 1 つ以上のアプリケーションを **Add**（追加）します。各アプリケーションについて、以下を指定します。
   - **Name**（名前） – アプリケーションの分かりやすい名前（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
   - **Location**（場所）（マルチ仮想システム モードに設定されているファイアウォール） – クライアントレス VPN アプリケーションを使用可能な仮想システム

（vsys）。マルチ仮想システム モードに設定されていないファイアウォールの場合、**Location**（場所）フィールドは表示されません。

- **Application Home URL**（プリケーションのホーム **URL**） – Web アプリケーションが配置されている URL（最大 4095 文字）。
- **Application Description**（アプリケーションの説明）（任意） – アプリケーションの簡単な説明（最大 255 文字）。
- **Application Icon**（アプリケーションのアイコン）（任意） – 公開されたアプリケーション ページでアプリケーションを識別するためのアイコン。アイコンを参照してアップロードすることができます。

2. <239>OK</239> をクリックします。

STEP 3 | （任意）一連の Web アプリケーションを管理するためのグループを作成します。

アプリケーションの集合を複数管理し、ユーザー グループに基づいてアクセスを提供する場合には、クライアントレス アプリケーション グループが便利です。たとえば、G&A チームの財務アプリケーション、エンジニアリング チームの開発アプリケーションなどです。

1. **Network**（ネットワーク） > **GlobalProtect** > **Clientless App Groups**（クライアントレス アプリ グループ）の順に選択します。新しいクライアントレス VPN アプリケーション グループを **Add**（追加）して以下を指定します。
   - **Name**（名前） – アプリケーション グループの分かりやすい名前（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
   - **Location**（場所）（マルチ仮想システム モードに設定されているファイアウォール） – クライアントレス VPN アプリケーション グループを使用可能な仮想システム（vsys）。マルチ仮想システム モードに設定されていないファイアウォールの場合、**Location**（場所）フィールドは表示されません。
2. **Applications**（アプリケーション）エリアで、グループにアプリケーションを **Add**（追加）します。既存のクライアントレス VPN アプリケーションのリストから選択することも、**New Clientless App**（新しいクライアントレス アプリ）を定義することもできます。
3. <239>OK</239> をクリックします。

STEP 4 | クライアントレス VPN サービスを提供するように GlobalProtect ポータルを設定します。

1. **Network (ネットワーク)** > **GlobalProtect** > **Portals (ポータル)** の順に選択し、既存のポータル設定を選択するか、新しいものを **Add (追加)** します。 GlobalProtect ポータルへのアクセスのセットアップ：
2. **Authentication**（認証）タブでは、以下の操作を行うことができます。
   - （任意）クライアントレス VPN 用の新しいクライアント認証を作成できます。この場合、**Client Authentication**（クライアントの認証）の **OS** として **Browser**（ブラウザ）を選択します。
   - 既存のクライアント認証を使用できます。
3. **Clientless**（クライアントレス） > **General**（全般）で、**Clientless VPN**（クライアントレス **VPN**）を選択してポータル サービスを有効にして以下を設定します。
   - アプリケーションのランディング ページをホストする GlobalProtect ポータルの **Hostname (ホスト名)** (IP アドレスまたは FQDN) を指定します。このホスト名は、アプリケーション URL の書き換えに使用されます。（URL の書き換えの詳細は、ステップ 8 を参照）。

     ネットワーク アドレス変換（*NAT*）を使用して *GlobalProtect* ポータルへのアクセスを提供する場合、入力する *IP* アドレスまたは *FQDN* は *GlobalProtect* ポータルの *NAT IP* アドレス（公開 *IP* アドレス）と一致するものであるか、*NAT IP* アドレスに解決できるものである必要があります。ユーザーはカスタム ポートの *GlobalProtect* ポータルにアクセスできないため、*NAT* 以前のポートも *TCP* ポート *443* である必要があります。

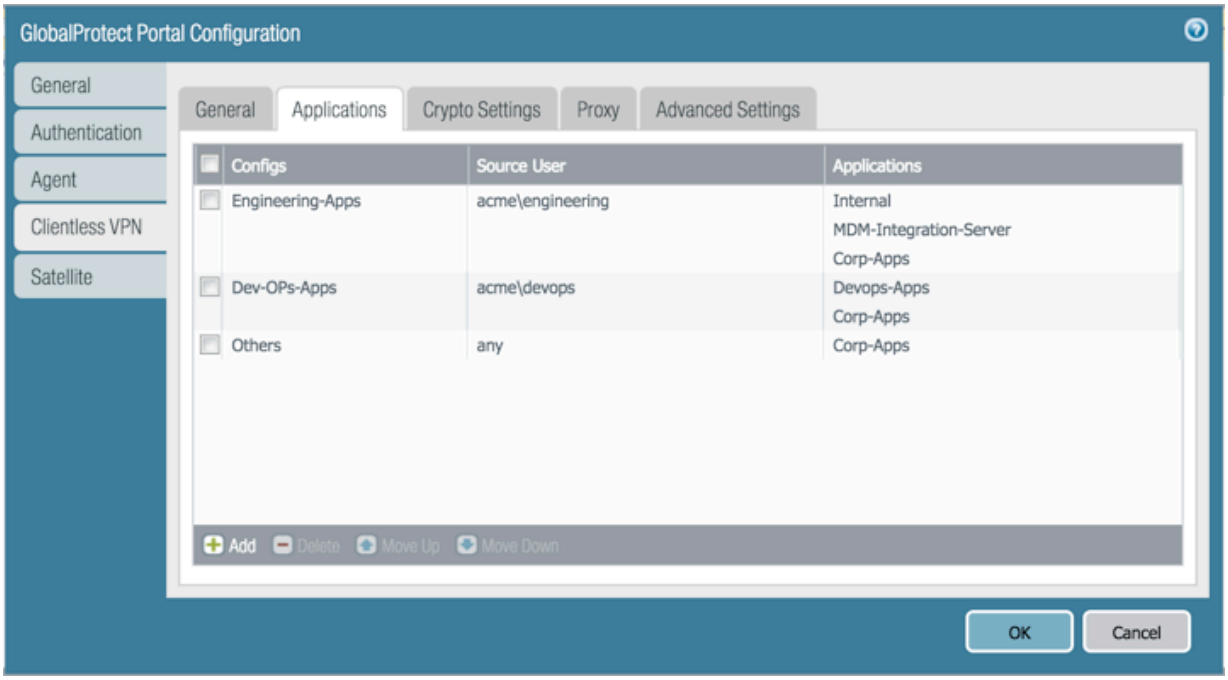
   - **Security Zone**（セキュリティ ゾーン）を指定します。このゾーンは、ファイアウォールとアプリケーション間のトラフィックの送信元ゾーンとして使用されます。このゾーンからアプリケーション ゾーンに定義されるセキュリティ ルールによって、アクセスできるアプリケーションが決まります。
   - **DNS Proxy**（**DNS** プロキシ）サーバーを選択するか、**New DNS Proxy**（新しい **DNS** プロキシ）を設定します。GlobalProtect はアプリケーション名を解決するためにこのプロキシを使用します。DNS プロキシ オブジェクトを参照してください。
   - **Login Lifetime**（ログイン ライフタイム)） — クライアントレス VPN セッションが有効な最大時間数または最大分数を指定します。一般的なセッション期間は 3 時間です。時間数を指定する場合の範囲は 1 ～ 24 時間、分数を指定する場合の範囲は60 ～ 1440 分です。セッションが失効すると、ユーザーは再認証して、新しいクライアントレス VPN セッションを開始する必要があります。
   - **Inactivity Timeout**（アイドル タイムアウト） — クライアントレス VPN セッションがアイドル状態を維持できる時間数または分数を指定します。一般的なアイドル タイムアウトは 30 分です。時間数を指定する場合の範囲は 1 ～ 24 時間、分数を指定する場合の範囲は 5 ～ 1440 分です。指定した時間内にユーザーのアクティビティがない場合、ユーザーは再認証して、新しいクライアントレス VPN セッションを開始する必要があります。
   - **Max User**（最大ユーザー） — 同時にポータルにログインできるユーザーの最大数を指定します。値を指定しない場合、エンドポイントの上限が使用されます。エンド

ポイントの上限が不明な場合、上限は 50 ユーザーとなります。ユーザー数の上限に達した場合、以降のクライアントレス VPN ユーザーはポータルにログインできません。

STEP 5 | ユーザーおよびユーザー グループをアプリケーションにマッピングします。

このマッピングによって、GlobalProtect クライアントレス VPN セッションから起動できるアプリケーション ユーザーまたはユーザー グループが決まります。

GlobalProtect ポータルは、指定されているユーザー/ユーザー グループの設定を使用して、どの設定を接続する GlobalProtect クライアントレス VPN ユーザーに配信するかを決定します。複数の設定がある場合、ポータルはリストの上から順に一致する設定を探すため、必ず適切な順序を決めて、必要なアプリケーションすべてにマッピングしてください。ポータルが一致する設定を見つけると、すぐにその設定を GlobalProtect クライアントレス VPN ユーザーに配信します。



アプリケーションをユーザー/ユーザー グループに配信するか、公開されていないアプリケーションの起動をユーザー/ユーザー グループに許可したとしても、そのアプリケーショ

ンにアクセスできるとは限りません。セキュリティ ポリシーを使用してアプリケーション (公開されているかによらず) へのアクセスを制御します。

グループを選択する前にグループ マッピングを設定する必要があります（***Device***（デバイス） > ***User Identification***（***User-ID***） > ***Group Mapping Settings***（グループ マッピング設定））。

1. **Applications**（アプリケーション）タブで、ユーザーを公開されたアプリケーションに照合する **Applications to User Mapping**（アプリケーションからユーザーへのマッピング）を **Add**（追加）します。
   - **Name**（名前） – マッピングの名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
   - **Display application URL address bar**（アプリケーション **URL** のアドレス バーを表示） – このオプションを選択するとアプリケーション URL のアドレス バーが表示され、ユーザーはアプリケーション ランディング ページで公開されていないアプリケーションをこのバーから起動できます。有効な場合、ユーザーは **Application URL (**アプリケーションの **URL)** を選択できます。
2. **Source Users**（送信元ユーザー）を指定します。現在のアプリケーション設定の適用対象に個別のユーザーやユーザー グループを **Add**（追加）できます。これらのユーザーは、GlobalProtect クライアントレス VPN を使用して、設定対象のアプリケーションを起動する権限を持ちます。ユーザーやグループだけでなく、これらの設定をユーザーやグループに適用するタイミングを指定できます。
   - **any**（すべて） – アプリケーション設定はすべてのユーザーに適用されます（対象ユーザーやユーザー グループを **Add**（追加）する必要はありません）。
   - **select**（対象指定） – アプリケーション設定はこのリストに **Add**（追加）したユーザーおよびユーザー グループにのみ適用されます。
3. 個別のアプリケーションまたはアプリケーション グループをマッピングに **Add**（追加）します。設定に追加した **Source Users**（送信元ユーザー）は、GlobalProtect クライアントレス VPN を使用して、追加済みのアプリケーションにリンクできます。

STEP 6 | クライアントレス VPN セッションのセキュリティ設定を指定します。

1. **Crypto Settings**（暗号化設定）タブで、ファイアウォールと公開されているアプリケーション間の SSL セッションで使用する認証および暗号化アルゴリズムを指定します。
   - **Protocol Versions**（プロトコル バージョン） – 必要な TLS/SSL バージョンの下限と上限を選択します。TLS バージョンが大きいほど、接続の安全性は高くなります。選択肢には、**SSLv3**、**TLSv1.0**、**TLSv1.1**、**TLSv1.2** が含まれます。
   - **Key Exchange Algorithms**（キー交換アルゴリズム） – キー交換用のサポート対象アルゴリズム タイプを選択します。選択肢は次の通りです。**RSA**、Diffie-Hellman（**DHE**）、エフェメラル楕円曲線 Diffie-Hellman（**ECDHE**）です。
   - **Encryption Algorithms**（暗号化アルゴリズム） – サポート対象の暗号化アルゴリズムを選択します。**AES128** 以上が推奨されます。
   - **Authentication Algorithms**（認証アルゴリズム） – サポート対象の認証アルゴリズムを選択します。選択肢は次の通りです。（**MD5**、**SHA1**、**SHA256**、または **SHA384**）。**SHA256** 以上をお勧めします。
2. アプリケーションが提示するサーバー証明書に問題がある場合に実行するアクションを選択します。
   - **Block sessions with expired certificate**（証明書が期限切れのセッションをブロック） – サーバー証明書の期限が切れている場合、アプリケーションへのアクセスをブロックします。
   - **Block sessions with untrusted issuers**（発行者が信頼されていないセッションをブロック） – サーバー証明書が信頼されていない認証局から発行されたものである場合、アプリケーションへのアクセスをブロックします。
   - **Block sessions with unknown certificate status**（証明書の状態が不明なセッションをブロック） – OCSP または CRL サービスが **unknown**（不明）の証明書失効状態を返す場合、アプリケーションへのアクセスをブロックします。
   - **Block sessions on certificate status check timeout**（証明書の状態のチェックがタイムアウトしたセッションをブロック） – 証明書の状態のサービスからの応答を受信する前に、証明書の状態のチェックがタイムアウトした場合、アプリケーションへのアクセスをブロックします。

STEP 7 | （任意）アプリケーションにアクセスするために 1 つ以上のプロキシ サーバー設定を指定します。

プロキシに対しては基本的な認証のみがサポートされています（ユーザー名とパスワード）。

ユーザーがプロキシ サーバーを経由してアプリケーションにアクセスする必要がある場合、**Proxy Server**（プロキシ サーバー）を指定します。ドメインのセットごとに 1 つずつ、複数のプロキシ サーバー設定を追加できます。

- **Name**（名前） – プロキシ サーバー設定を識別するラベル（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
- **Domains**（ドメイン） – プロキシ サーバーがサービスを提供するドメインを追加します。複数のドメインを示すためにドメイン名の先頭にワイルドカード文字（*）を使用できます。
- **Use Proxy**（プロキシを使用） – ドメインへのアクセスを提供するためにプロキシ サーバーを割り当てる場合に選択します。
- **Server**（サーバー） – プロキシ サーバーの IP アドレスまたはホスト名を指定します。
- **Port**（ポート） – プロキシ サーバーとの通信用ポートを指定します。
- **User**（ユーザー）と **Password**（パスワード） – プロキシ サーバーへのログインに必要な認証情報である **User**（ユーザー）と **Password**（パスワード）を指定します。確認のためにパスワードはもう一度指定します。

STEP 8 | （任意）アプリケーション ドメインの特記事項があれば指定します。

クライアントレス VPN はリバース プロキシとして機能し、公開されている Web アプリケーションが返す Web ページが変更されます。すべての URL を書き換え、書き換えられたページをリモート ユーザーに表示します。そのため、リモート ユーザーがこれらのいずれかの URL にアクセスすると、要求は GlobalProtect ポータルを経由します。

場合によって、アプリケーションにはポータル経由でアクセスする必要ががないページが含まれていることもあります（たとえば、アプリケーションに yahoo.finance.com の株式相場表示機能が含まれている場合があります）。このようなページは除外できます。

Advanced Settings（詳細設定）タブで、**Rewrite Exclude Domain List**（再書き込み除外ドメイン リスト）にドメイン名、ホスト名、または IP アドレスを **Add**（追加）します。これらのドメインは書き換えルールから除外され、書き換えられません。

ホストおよびドメイン名では、パスはサポートされません。ホスト名およびドメイン名のワイルドカード文字（*） は、名前の先頭でのみ使用できます（*.etrade.com など）。

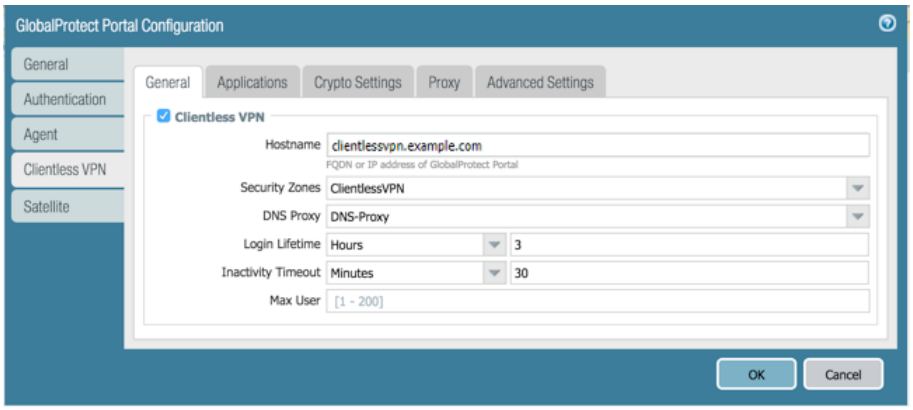
STEP 9 | ポータルの設定を保存します。

1. **OK** を 2 回クリックします。
2. 変更を **Commit (コミット)** します。

STEP 10 | ユーザーが公開されたアプリケーションにアクセスできるように、セキュリティ ポリシー ルールを設定します。

セキュリティ ポリシーは以下の目的で必要です。

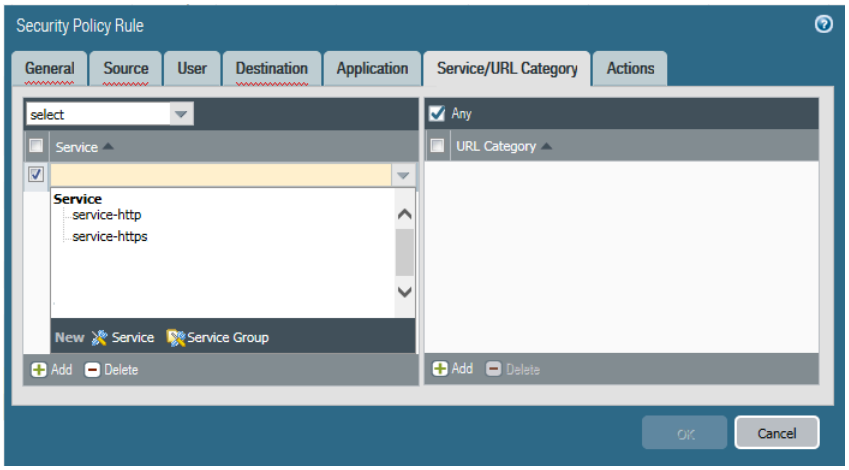
- クライアントレス VPN をホストする GlobalProtect ポータルにインターネットからアクセスできるようにするため。これは、信頼されていないゾーンまたはインターネット ゾーンからクライアントレス VPN ポータルをホストするゾーンへのトラフィックです。
- クライアントレス VPN ユーザーにインターネットへのアクセスを許可するため。これは、クライアントレス VPN ゾーンから信頼されないゾーンまたはインターネット ゾーンへのトラフィックです。



- クライアントレス VPN ユーザーに企業リソースへのアクセスを許可するため。これは、クライアントレス VPN ゾーンからラスト ゾーンまたは企業ゾーンへのトラフィックです。定義するセキュリティ ポリシーによって、公開された各アプリケーションを使用する権限をどのユーザーに付与するかが決まります。公開されたアプリケーションサーバーをホストしているセキュリティ ゾーンの場合、必ず **Enable User Identification (ユーザー ID を有効化)** してください。

  デフォルトでは、**Security Policy Rule**（セキュリティ ポリシー ルール）の **Service/URL**（サービス/URL）は **application-default** に設定されています。クライアントレス

VPN は、このデフォルト設定の HTTPS サイトでは機能しません。**service-http** と **service-https** の両方が含まれるように **Service/URL**（サービス/URL）を変更します。



- クライアントレス VPN アプリケーションにアクセスするためにプロキシ サーバーを設定する場合、必ずセキュリティ ポリシー定義にプロキシ IP アドレスとポートを含めてください。プロキシ サーバー経由でアプリケーションにアクセスする場合、プロキシ IP アドレスとポートについて定義したセキュリティ ポリシーのみが適用されます。

STEP 11 | (任意) クライアントレス VPN のユーザーが接続しているポータルの位置をクライアントレス VPN ポータルのランディング ページで表示するよう設定するために、ポータルを設定したファイアウォールの物理的な位置を指定します。

ネットワークのパフォーマンス低下など、クライアントレス VPN のユーザーが異常な挙動を体験した場合、この位置情報をサポートやヘルプデスクの担当者に提供してトラブルシューティングをスムーズに進めることができます。また、この位置情報を使用してポータルとの近さを判断することもできます。この近さに基づき、より近いポータルに切り替える必要があるかどうかを判断できます。

ポータルの位置を指定しない場合、クライアントレス *VPN* ポータルのランディング ページの位置フィールドは空になります。

- **CLI** にて—次の CLI コマンドを使用し、ポータルを設定したファイアウォールの物理的な位置を指定します：

```
<username@hostname> set deviceconfig setting global-protect
 location <location>
```

- **XML API** にて—次の XML API を使用し、ポータルを設定したファイアウォールの物理的な位置を指定します：
  - デバイス—ポータルを設定したファイアウォールの名前
  - ロケーション—ポータルを設定したファイアウォールの位置

```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?
key=<apikey>&type=config&action=set&xpath=/config/devices/
```

```
entry[@name='<device-name>']/deviceconfig/setting/global-
protect&element=<location>location-string</location>'
```

クライアントレス *VPN* トラフィックの送信元 *IP* アドレス（アプリケーションに提示されるもの）は、ポータルがアプリケーションに到達するために使用する出力インターフェイスの *IP* アドレス、あるいはソース *NAT* が使用中である場合は変換後の *IP* アドレスのいずれかになります。

クライアントレス VPN のトラブルシューティング

この機能では HTML アプリケーションのダイナミックな書き換えを伴うため、一部のアプリケーションの HTML コンテンツはアプリケーションを正しく書き変えられず、破損する場合があります。問題が発生した場合、以下の表に示したコマンドを使用し、原因を特定してください。

表 **6 :** 表：書き換えエンジン統計

Action（アクション）	コマンド
CLI コマンド	
使用するクライアントレス VPN ダイナミック コンテンツのバージョンを一覧にする **Device** > **Dynamic Updates**（ダイナミック更新） > **GlobalProtect Clientless VPN**（GlobalProtect クライアントレス VPN）からダイナミック更新バージョンを表示することもできます。	**show system setting ssl-decrypt memory** proxy uses shared allocator SSL certificate cache: Current Entries: 1 Allocated 1, Freed 0 Current CRE (61-62) : 3456 KB (Actual 3343 KB) Last CRE (60-47) : 3328 KB (Actual 3283 KB) この例では、現在のダイナミック更新はバージョン 61-62 で、最後にインストールされたダイナミック更新はバージョン 60-47 です。
クライアントレス VPN のアクティブな（現在の）ユーザーを一覧にする	**show global-protect-portal current-user portal GP ClientlessPortal filter-user all-users** GlobalProtect Portal : GPClientlessPortal Vsys-Id : 1 User : paloaltonetworks.com\johndoe Session-id : 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0 Client-IP : 5.5.5.5 Inactivity Timeout : 1800 Seconds before inactivity timeout : 1750 Login Lifetime : 10800 Seconds before login lifetime : 10748

Action（アクション）	コマンド
	Total number of user sessions: 1
DNS 解決の結果を表示する これは、DNS に問題があるかどうかを判断する場合に役立ちます。DNS に問題がある場合、FQDN に対する問い合わせを CLI の出力で解決できなかったことがわかります。	**show system setting ssl-decrypt dns-cache** Total DNS cache entries: 89 Site IP Expire(secs) Interface bugzilla.panw.local 10.0.2.15 querying 0 www.google.com 216.58.216.4 Expired 0 stats.g.doubleclick.net 74.125.199.154 Expired 0
すべてのクライアントレス VPN ユーザーセッションおよび保存されている Cookie を表示する	**show system setting ssl-decrypt gp-cookie-cache** User: johndoe, Session-id: 1SU2vrPIDfdopGf-7gahMTCiX8PuL0S0, Client-ip: 199.167.55.50
書き換え統計を表示する これは、クライアントレス VPN 書き換えエンジンの状態を識別する場合に役立ちます。 書き換え統計およびその意味や目的の詳細は、表:書き換えエンジン統計を参照してください。	**show system setting ssl-decrypt rewrite-stats** Rewrite Statistics initiate_connection : 11938 setup_connection : 11909 session_notify_mismatch : 1 reuse_connection : 37 file_end : 4719 packet : 174257 packet_mismatch_session : 1 peer_queue_update_rcvd : 167305 peer_queue_update_sent : 167305 peer_queue_update_rcvd_failure: 66 setup_connection_r : 11910 packet_mismatch_session_r : 22 pkt_no_dest : 23 cookie_suspend : 2826 cookie_resume : 2826 decompress : 26 decompress_freed : 26 dns_resolve_timeout : 27 stop_openend_response : 43 received_fin_for_pending_req : 26 Destination Statistics To mp : 4015 To site : 12018

Action（アクション）	コマンド
	To dp : 17276 Return Codes Statistics ABORT : 18 RESET : 30 PROTOCOL_UNSUPPORTED : 7 DEST_UNKNOWN : 10 CODE_DONE : 52656 DATA_GONE : 120359 SWITCH_PARSER : 48 INSERT_PARSER : 591 SUSPEND : 2826 Total Rewrite Bytes : 611111955 Total Rewrite Useconds : 6902825 Total Rewrite Calls : 176545
デバッグ コマンド	
クライアントレス VPN ポータルを実行するファイアウォールでデバッグ ログを有効にする	**debug dataplane packet-diag set log feature ssl all** **debug dataplane packet-diag set log feature misc all** **debug dataplane packet-diag set log feature proxy all** **debug dataplane packet-diag set log feature flow basic** **debug dataplane packet-diag set log on**
クライアントレス VPN ポータルを実行するファイアウォールでパケット キャプチャを有効にする	**debug dataplane packet-diag set capture username *<portal-username>*** **debug dataplane packet-diag set capture stage clientless-vpn-client file *<clientless-vpn-client-file>*** **debug dataplane packet-diag set capture stage clientless-vpn-server file *<clientless-vpn-server-file>*** **debug dataplane packet-diag set capture stage firewall file *<firewall-file>*** **debug dataplane packet-diag set capture stage receive file *<receive-file>*** **debug dataplane packet-diag set capture stage transmit file *<transmit-file>*** **debug dataplane packet-diag set capture on**

Action（アクション）	コマンド
	パケット キャプチャ コマンドを実行する際、エンド ユーザーがクライアントレス *VPN* ポータルにログインした後に同意ページが表示され、ユーザー セッション中に暗号化されない *(*クリア テキストの*)* データもキャプチャされるということが伝えられます。ユーザーがパケット キャプチャ セッションに同意すると、アプリケーションのランディング ページへと進み、そこでパケット キャプチャが始まります。パケット キャプチャ セッションに同意しないユーザーはクライアントレス *VPN* ポータルからログアウトされ、管理者に連絡しなければ通常の *(*パケット キャプチャなしの*)* ユーザー セッションを継続できなくなります。 すでに進行中のユーザー セッションに対してパケット キャプチャ コマンドを実行すると、そのユーザーはクライアントレス *VPN* ポータルから自動的にログアウトされ、ログインし直してパケット キャプチャ セッションを許可あるいは拒否することになります。
パケット キャプチャ ファイルを表示	**debug dataplane packet-diag show setting** -- --------- Packet diagnosis setting: -- --------- Packet filter Enabled: no Match pre-parsed packet: no -- --------- Logging Enabled: no Log-throttle: no Sync-log-by-ticks: yes Features: Counters: -- --------- Packet capture Enabled: yes Snaplen: 0 Username: test1 Stage clientless-vpn-client: file client.pcap Captured: packets - 3558 bytes - 11366322 Maximum: packets - 0 bytes - 0 Stage clientless-vpn-server: file server.pcap Captured: packets - 1779 bytes - 5651923

Action（アクション）	コマンド
	Maximum: packets - 0 bytes - 0 --- ---
パケット キャプチャ ファイルを Secure Copy (SCP) サーバーにエクスポート	**scp export filter-pcap** + remote-port SSH port number on remote host + source-ip Set source address to specified interface address * from from * to Destination (username@host:path) **scp export filter-pcap from <*source-file*>** <scp-server> Destination (username@host:path)

表 **7 :** 表：書き換えエンジン統計

統計	説明
initiate_connection_failure	バックエンド ホストに対する接続の初期化に失敗しました
setup_connection_failure	接続のセットアップに失敗しました
setup_connection_duplicate	重複するピア セッションが存在しています
session_notify_mismatch	ほとんど無効のセッションです
packet_mismatch_session	受信したパケットに適切なセッションが見つかりませんでした
peer_queue_update_rcvd_failure	パケット更新がピアによって受信されたときにセッションが無効でした
peer_queue_update_sent_failure	パケット更新をピアに送信できなかったか、パケット キュー長の更新をピアに送信できませんでした
exceed_pkt_queue_limit	キューに入っているパケットが多すぎます
proxy_connection_failure	プロキシ接続に失敗しました
setup_connection_r	ピア セッションをアプリケーション サーバーにインストールしています。この値は、**initiate_connection** および **setup_connection** の値と一致している必要があります。
setup_connection_duplicate_r	プロキシに重複するセッションが既にあります

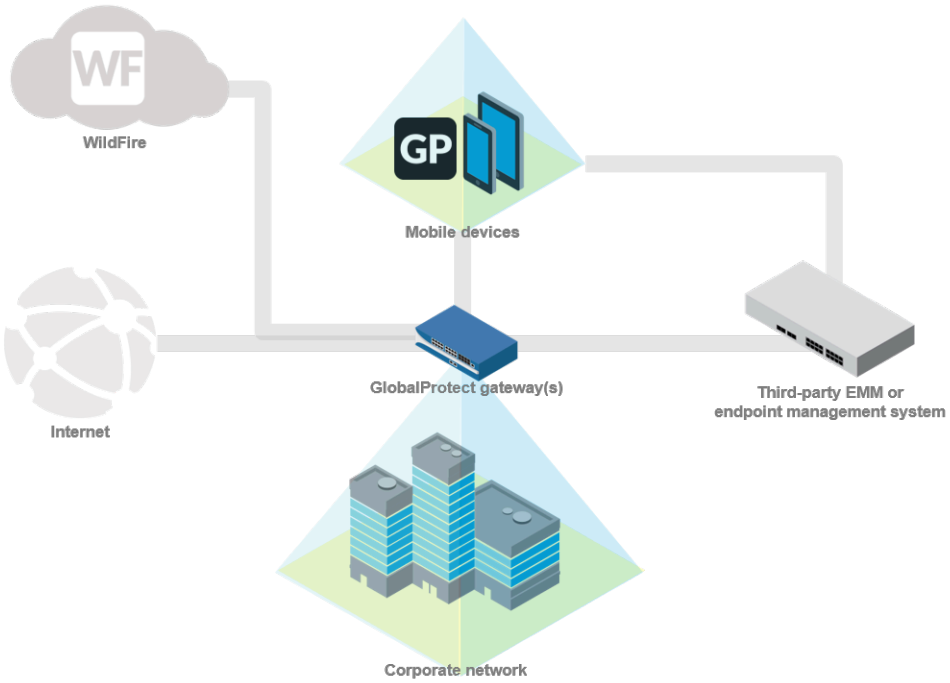
統計	説明
setup_connection_failure_r	ピア セッションをセットアップできませんでした
session_notify_mismatch_r	ピア セッションが見つかりません
packet_mismatch_session_r	パケットを取得しようとしたときにピア セッションが見つかりませんでした
exceed_pkt_queue_limit_r	保留中のパケットが多すぎます
unknown_dest	宛先ホストが見つかりませんでした
pkt_no_dest	このパケットの宛先がありません
cookie_suspend	Cookie を取得するセッションが中断されました
cookie_resume	MP から更新された Cookie を含む応答を受信しました。この値は、通常 cookie_suspend の値に一致します。
decompress_failure	解凍できませんでした
memory_alloc_failure	メモリを割り当てられませんでした
wait_for_dns_resolve	DNS 要求を解決するセッションを中断しました
dns_resolve_reschedule	応答がないため、DNS クエリのスケジュールを再設定しました (タイムアウト前に再試行)
dns_resolve_timeout	DNS クエリのタイムアウト
setup_site_conn_failure	サイト (プロキシ、DNS) への接続をセットアップできませんでした
site_dns_invalid	DNS の解決に失敗しました
multiple_multipart	複数パートのコンテンツタイプが処理されました
site_from_referer	リファラーからバックエンド ホストを受信しました。これは、クライアントレス VPN が書き換えない Flash などのコンテンツからの書き換えリンクに問題があることを示している場合があります。
received_fin_for_pending_req	クライアントからの保留中の要求についてサーバーから FIN を受信しました

統計	説明
unmatched_http_state	予期しない HTTP コンテンツです。これは、http ヘッダーまたは本文の解析に問題があることを示している場合があります。

モバイル機器管理(MDM)

モバイルデバイス管理の概要

モバイル エンドポイントがより高機能になるにつれ、エンド ユーザーがそれらを利用してビジネス タスクを行う頻度が増えています。しかし、企業ネットワークにアクセスするこれらのデエンドポイントは、脅威や脆弱性に対する保護がない状態でインターネットにも接続しています。



モバイルデバイス管理システムを使用すれば、コンプライアンスが必要なエンドポイントに企業のアカウント設定や VPN 設定を自動的にデプロイすることが可能になり、モバイル エンドポイントの管理が簡素化されます。また、このモバイルデバイス管理システムを使用してすでに攻撃を受けているエンドポイントに対処することで、セキュリティ違反の影響を緩和することができます。これにより、企業データと個人用のエンド ユーザー データの両方が保護されます。例えばエンドユーザーがエンドポイントを紛失したら、モバイルデバイス管理システムから遠隔操作でそのエンドポイントをロックしたり、さらにはエンドポイントを削除（完全に、あるいは部分的に）してしまったりすることも可能です。

モバイルデバイス管理システムに備わっているアカウントのプロビジョニングとリモート デバイス管理機能を利用できるだけでなく、既存の GlobalProtect™ VPN インフラストラクチャと統合すれば、エンドポイントが報告するホスト情報を使用して、GlobalProtect ゲートウェイを介したアプリへのアクセスにセキュリティ ポリシーを適用できます。また、Palo Alto の次世代型ファイアウォールに組み込まれている監視ツールを使用してモバイル エンドポイントのトラフィックを監視することも可能です。

MDM あるいは EMM システムと GlobalProtect を統合

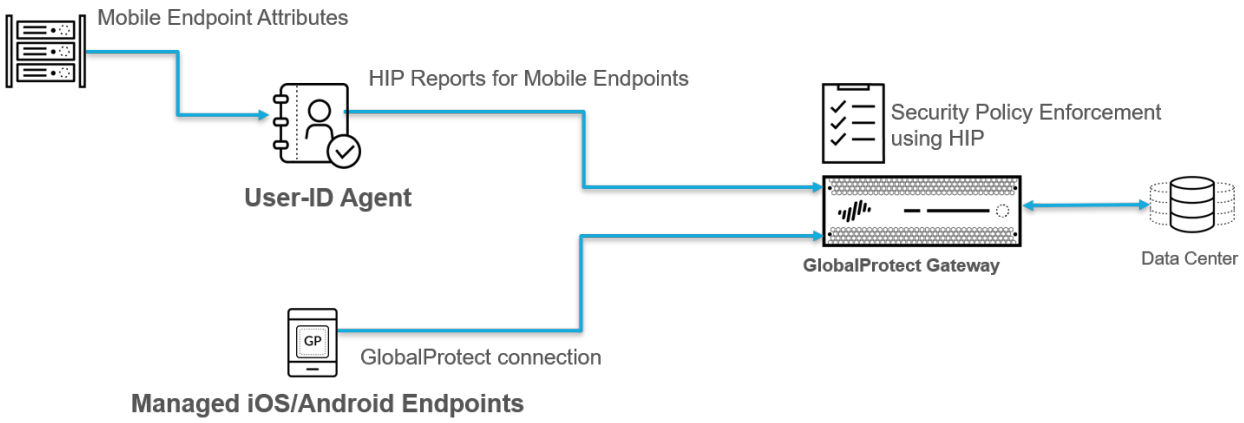
次のいずれかの方法で、GlobalProtect デプロイメントを MDM あるいは EMM システムと統合することができます：

MDM あるいは EMM システムとファイアウォールを統合 (AirWatch のみ)

Windows User-ID エージェントを設定し、AirWatch MDM サーバーと通信して接続中のエンドポイントからホスト情報を収集するよう設定することができます。User-ID エージェントは、HIP ベースのポリシーを適用するために HIP レポートの一部としてこのホスト情報を GlobalProtect ゲートウェイに送信します。

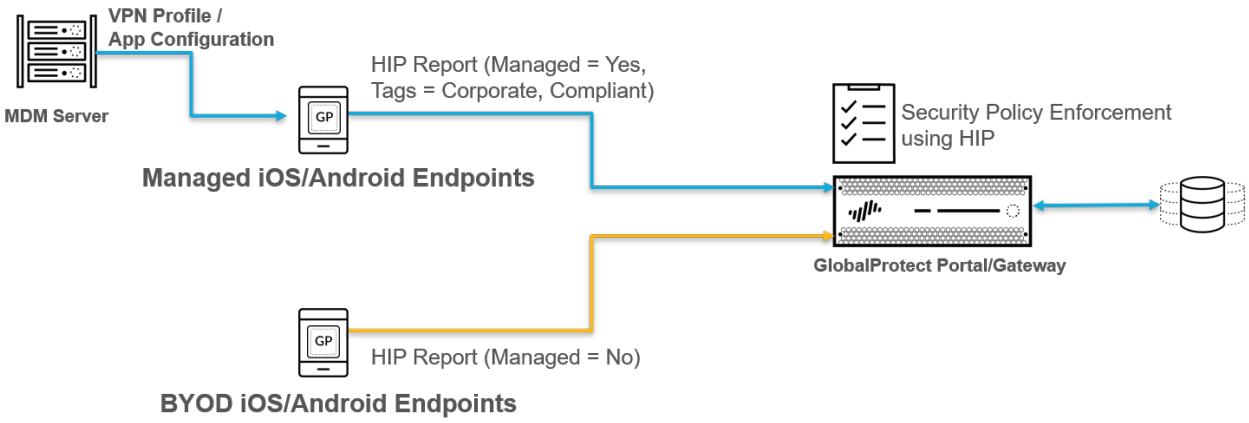
ファイアウォールの統合は、*PAN-OS 8.0* 以降のリリースでサポートされています。

ファイアウォールの統合は *VMware AirWatch* でのみサポートされています。



MDM あるいは EMM システムと GlobalProtect アプリケーションを統合

バージョン 5.0 から、iOS および Android エンドポイント用 GlobalProtect アプリケーションが、MDM システムからベンダー データ属性およびタグを取得できるようになっています。iOS エンドポイントの場合、MDM システムがこれらの属性を VPN プロファイルの一部として GlobalProtect アプリケーションに送信します。Android エンドポイントの場合、MDM システムがこれらの属性をアプリ制限設定の一部として送信します。GlobalProtect アプリケーションはその後、HIP ベースのポリシーを適用するために HIP レポートの一部としてこの属性およびタグを GlobalProtect ゲートウェイに送信します。



GlobalProtect アプリケーションの統合は *VMware*、*AirWatch*、*MobileIron*、*Microsoft Intune* で承認されています。しかし、*VPN* プロファイル内のベンダー データ属性をサポートしているあらゆる *MDM* あるいは *EMM* システムでもこの統合方法がサポートされています。

次の表は、サポートされているベンダー データ属性を示しています：

MDM 属性	HIP レポート属性	HIP レポート カテゴリ	説明
`mobile_id`	ホスト**ID**	一般条項	エンドポイント固有のデバイス識別子 (UDID)。
管理対象	管理対象	一般条項	エンドポイントが管理対象であるかどうかを示す値。値が **Yes (**はい**)** である場合、エンドポイントが管理対象です。値が **No (**いいえ**)** である場合、エンドポイントが管理対象ではありません。
コンプライアンス	タグ	モバイル デバイス	エンドポイントが指定済みの MDM コンプライアンス ポリシーに準拠しているかどうかを示す、コンプライアンス状態 (例えば、**Compliant (**準拠**)**)。この値は HIP レポートの **Tag (**タグ**)** 属性に付加されます。

MDM 属性	HIP レポート属性	HIP レポート カテゴリ	説明
ownership	タグ	モバイル デバイス	エンドポイントの所有者カテゴリ (例えば、**Employee Owned (**従業員が所有**)**)。この値は HIP レポートの **Tag (**タグ**)** 属性に付加されます。
タグ	タグ	モバイル デバイス	他の MDM ベースの属性と照合するタグ。

GlobalProtect と MDM との統合をセットアップ

次のワークフローで GlobalProtect と MDM との統合をセットアップできます：

STEP 1 | GlobalProtect インフラストラクチャをセットアップします。

1. GlobalProtect のインターフェイスおよびゾーンの作成.
2. GlobalProtect コンポーネント間の SSL の有効化.
3. GlobalProtect ユーザー認証をセットアップします。GlobalProtect ユーザー認証についてを参照してください。
4. グループ マッピングの有効化.
5. GlobalProtect ゲートウェイの設定.
6. モバイル エンドポイント用の GlobalProtect アプリケーションをサポートしているゲートウェイを動作させるそれぞれのファイアウォールで使用するライセンスをアクティベートします。
7. GlobalProtect ポータルへのアクセスのセットアップ.

STEP 2 | モバイルデバイス管理システムをセットアップし、企業が発行したエンドポイントのみ、あるいは企業が発行したものと個人のエンドポイントを両方ともサポートするのか決定します。

お使いのモバイルデバイス管理（MDM）システム、あるいはエンタープライズ モビリティ管理（EMM）システムの指示を確認します。

STEP 3 | モバイル エンドポイント用の GlobalProtect アプリを入手します。

- App store– GlobalProtect モバイル アプリケーションのダウンロードおよびインストール
- サポートされている mobile device management (モバイルデバイス管理 - MDM) システム–GlobalProtect モバイル アプリケーションのデプロイ
- サードパーティ製の他のモバイルデバイス管理システム–アプリケーションを管理対象のエンドポイントにデプロイする方法については、ベンダーによる指示をご確認ください。

STEP 4 | MDM の統合を設定します。

次のいずれかの方法を使用し、MDM の統合を設定します。

- MDM あるいは EMM システムとファイアウォールを統合：
  - ホスト情報を収集するための Windows User-ID エージェントの設定
- MDM あるいは EMM システムと GlobalProtect アプリケーションを統合：
  - 承認済みのサードパーティ製の MDM による GlobalProtect アプリケーションの管理
  - 他のサードパーティ製の MDM を使用した GlobalProtect アプリケーションの管理

STEP 5 | ホスト情報を使用し、モバイル エンドポイントに割り当てるポリシーを設定します。

管理対象エンドポイントのHIP ベースのポリシー適用の設定

承認済みのサードパーティ製の MDM による GlobalProtect アプリケーションの管理

承認済みのサードパーティ製の MDM システムを使ってモバイル エンドポイント用の GlobalProtect アプリケーションをデプロイ・構成・管理する方法については、次の各セクションの情報を参照してください：

- 承認済みの MDM ベンダー
- GlobalProtect モバイル アプリケーションのデプロイ
- 常時オンの VPN 設定
- ユーザーが開始するリモート アクセス VPN 設定
- アプリ単位の VPN 設定
- WildFire と App Scan の統合の有効化
- macOSエンドポイントのGlobalProtectアプリケーションの通知を抑制する

承認済みのサードパーティ製の MDM システムを使用していない場合、他のサードパーティ製の MDM を使用した GlobalProtect アプリケーションの管理できます。

承認済みの MDM ベンダー

次の表では、GlobalProtect アプリケーションを構成・デプロイ・管理するために使用できる、承認済みの MDM ベンダーを OS 毎にリストアップしています。「—」は、その OS がサポートされていないことを示します。

承認されていない MDM ベンダーを使用したい場合は、他のサードパーティ製の MDM を使用した GlobalProtect アプリケーションの管理

サポートされている MDM ベンダー	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux Linux
AirWatch	✓（アプリ単位の VPN のみ）	✓	—	—	✓	—	—
Microsoft Intune	✓（常時オン、リモートアクセス、アプ	✓	—	—	✓（常時オンおよびアプリ単位の	—	—

サポートされている MDM ベンダー	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux Linux
	リケーションごとの VPN のみ)				VPN のみ)		
MobileIron	✓（常時オンの VPN のみ)	✓	—	—	—	—	—
Google 管理コンソール	✓ (Chromebook でサポートされている Android アプリの場合、アプリ開発のみ)	—	✓（アプリのデプロイのみ)	—	—	—	—

> *GlobalProtect* アプリケーションをデプロイする用途でのみ *Google* 管理コンソールを使用できます。コンソールを使って *VPN* 設定を構成することはできません。*Google* 管理コンソールを使ってアプリをデプロイする前に、GlobalProtect ポータルで *VPN* 設定を構成しておく必要があります。

GlobalProtect モバイル アプリケーションのデプロイ

GlobalProtect アプリケーションを使用すると、企業のセキュリティ ポリシーをモバイル エンドポイントまで容易に拡張することができます。GlobalProtect アプリを実行している他のリモート エンドポイントと同様に、モバイル アプリから IPsec や SSL VPN トンネルを介して、会社のネットワークに安全にアクセスすることができます。アプリケーションが、エンド ユーザーの現在のロケーションに最も近いゲートウェイに接続します。さらに、モバイル エンドポイントとの双方向のトラフィックには、会社のネットワーク上にある他のエンドポイントと同じセキュ

リティ ポリシーが自動的に適用されます。また、アプリはホスト設定に関する情報を収集し、この情報を使用して HIP ベースのセキュリティ ポリシーを強化することができます。

GlobalProtect アプリケーションをインストールするには、次のような主な 2 つの方法があります。App Storeから直接エンドポイントにアプリケーションをインストールするか（GlobalProtect モバイル アプリのダウンロードおよびインストールを参照）、あるいはモバイルデバイス管理システム（AirWatchなど）から管理対象のエンドポイントへとアプリケーションをデプロイ、透過的にプッシュします。

- AirWatch を使用した GlobalProtect モバイル アプリケーションのデプロイ
- AirWatch を使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイ
- Microsoft Intune を使用した GlobalProtect モバイル アプリケーションのデプロイ
- MobileIron を使用した GlobalProtect モバイル アプリケーションのデプロイ
- Google 管理コンソールを使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイ

AirWatch を使用した GlobalProtect モバイル アプリケーションのデプロイ

AirWatch で登録されている管理対象のエンドポイントに GlobalProtect アプリケーションをデプロイすることができます。iOS または Android を実行しているエンドポイントは、AirWatch エージェントをダウンロードして AirWatch MDM に登録する必要があります。Windows 10 のエンドポイントは AirWatch エージェントを必要としませんが、エンドポイント上で登録の設定を行う必要があります。アプリケーションをデプロイしたら、VPN プロファイルを構成、デプロイし、エンドユーザー用の GlobalProtect アプリケーションを自動的にセットアップします。

管理対象 *Chromebook* 上で *Android* 用 *GlobalProtect* アプリケーションを実行する場合、AirWatch を使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイすることができます。

STEP 1 | 作業を始める前に、GlobalProtect アプリケーションをデプロイするエンドポイントが AirWatch に登録されていることを確認してください。

- **Android** および **iOS**—AirWatch エージェントをダウンロードし、指示に従って登録を行います。
- **Windows**フォンおよび**Windows 10 UWP**—Windows 10 UWPエンドポイントをAirWatchに登録する設定を行います（エンドポイントから**Settings** > **Accounts** > **Work access** > **Connect** (設定 > アカウント > 業務アクセス > 接続)を選択）。

STEP 2 | AirWatch から **APPS & BOOKS**（アプリおよび本） > **Public**（公開） > **Add Application**（アプリを追加）を選択します。

STEP 3 | このアプリケーションを管理する組織グループを選択します。

STEP 4 | **Platform**（プラットフォーム）として **Apple iOS**、**Android**、または **Windows** フォンを選択します。

STEP 5 | エンドポイントのアプリ ストアで GlobalProtect アプリを検索するか、GlobalProtect アプリ ページに次のいずれかの URL を入力します。

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

STEP 6 | **Next**（次へ）をクリックします。そのエンドポイントのアプリストアでアプリを検索した場合、検索結果のリストからアプリを**Select**（選択）する必要もあります。

Android 用 *GlobalProtect* アプリを検索してもリストにそのアプリが表示されない場合は、*Android for Work* の管理者に連絡して、承認済みの会社アプリのリストに *GlobalProtect* を追加するか、*Google Play* ストアのアプリ *URL* を使用してください。

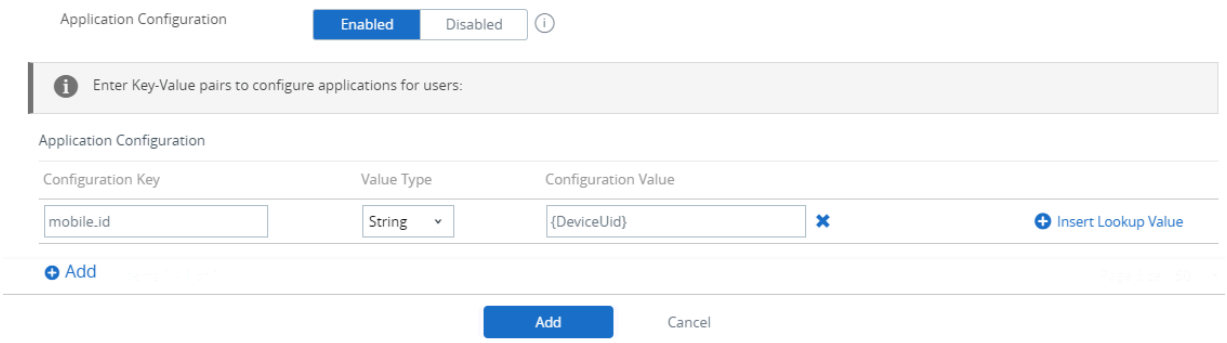
STEP 7 | **Assignment**（割り当て）タブで、このアプリケーションへのアクセスが許可される **Assigned Smart Group**（割り当てられたスマート グループ）を選択します。

STEP 8 | **App Delivery Method**（アプリ配信方法）を、アプリが自動でデバイスにプッシュされる **Auto**（自動） が、**On Demand**（オンデマンド）のいずれかに設定します。

STEP 9 | （Android 用 GlobalProtect アプリのみ）アプリ設定を **Enable**（有効）にして、UDID を使用してエンドポイントを識別できるようにします。

次のキー/値ペアを追加します。

- 設定キー—**mobile_id**
- 値タイプ—**String**
- 設定値—**{DeviceUid}**



STEP 10 | **Save & Publish**(保存して発行) を選択し**Assignment**(割り当て) セクションで割り当てた スマート グループ 内のエンドポイントへの App Catalog をプッシュします。

AirWatch を使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイ

GlobalProtect アプリケーション 5.0 から、AirWatch で登録した管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイできるようになっています。アプリケーションをデプロイしたら、VPN プロファイルを構成、デプロイし、エンドユーザー用の GlobalProtect アプリケーションを自動的にセットアップします。

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。*Android* アプリケーションをサポートしていない *Chromebook* では、*Chromebook* 用 *GlobalProtect* アプリケーションを引き続き実行する必要があります。*Chromebook* は *GlobalProtect* アプリ*5.0*以降のバージョンではサポートしていません。

Android 用 *GlobalProtect* アプリケーションと *Chromebook* 用 *GlobalProtect* アプリケーションの両方を同じ *Chromebook* にデプロイしないでください。

次のステップに従い、AirWatch を使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイします：

STEP 1 | Google 管理コンソールをセットアップします。

Google 管理コンソールを使用すれば、組織内のユーザーのために Google サービスを管理できます。AirWatch は Google 管理コンソールを使用して Chromebook との統合を行います。

1. 管理者として Google 管理コンソールにログインします。
2. コンソールで **Security (セキュリティ)** > **Advanced Settings (詳細設定)** > **Manage API client access (API クライアント アクセスの管理)** を選択します。
3. **Client Name (クライアント名)** フィールドに、AirWatch から得たクライアント ID を入力します。
4. **One or More API Scopes (一つ以上の API スコープ)** フィールドに、アプリケーション アクセスを制御する次の Google API のスコープを入力します：

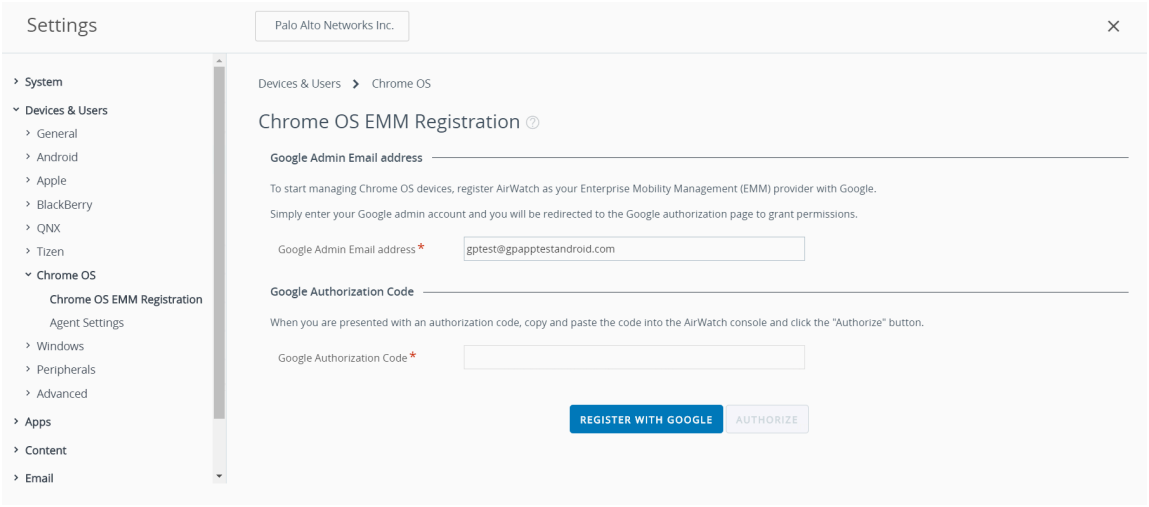
   各 *API* スコープをコンマで区切ってください。

   - https://www.googleapis.com/auth/chromedevicemanagementapi
   - https://www.googleapis.com/auth/admin.directory.user
   - https://www.googleapis.com/auth/admin.directory.device.chromeos
5. **Authorize (認証)** をクリックします。
6. デバイス ポリシー用の **Chrome Management - Partner Access (Chrome 管理 - パートナーアクセス)** (**Device Management (デバイス管理)** > **Device Settings (デバイス設定)** > **Chrome Management (Chrome 管理)** > **Device Settings (デバイス設定)**) およびユーザー ポリシー (**Device Management (デバイス管理)** > **Device Settings (デバイス設定)** > **Chrome Management (Chrome 管理)** > **User Settings (ユーザー設定)**) を有効化します。

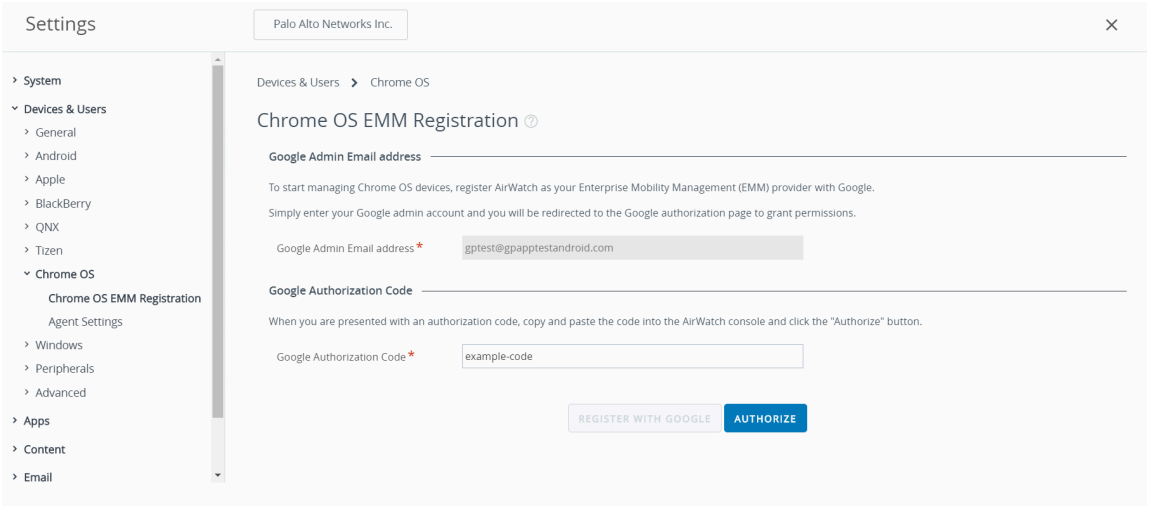
STEP 2 | Google 用のエンタープライズ モビリティ管理 (EMM) プロバイダーとして AirWatch を登録します。

AirWatch を使用して Chromebook を管理するには、Google 管理コンソールを使用して AirWatch を登録する必要があります。

1. AirWatch コンソールにログインします。
2. **Devices (デバイス)** > **Devices Settings (デバイス設定)** > **Devices & Users (デバイスおよびユーザー)** > **Chrome OS** > **Chrome OS EMM Registration (Chrome OS EMM 登録)** を選択します。
3. Google 管理コンソールにアクセスするために使用した **Google Admin Email address (Google** 管理者メールアドレス**)** を入力します。
4. **REGISTER WITH GOOGLE (GOOGLE** で登録**)** をクリックします。Google 認証ページにリダイレクトし、そこで Google 認証コードを取得できます。



5. Google 認証ページで取得した **Google Authorization Code (Google** 認証コード**)** を入力します。
6. **AUTHORIZE (**認証**)** をクリックして登録を完了させます。



STEP 3 | AirWatch で Chromebook を登録します。

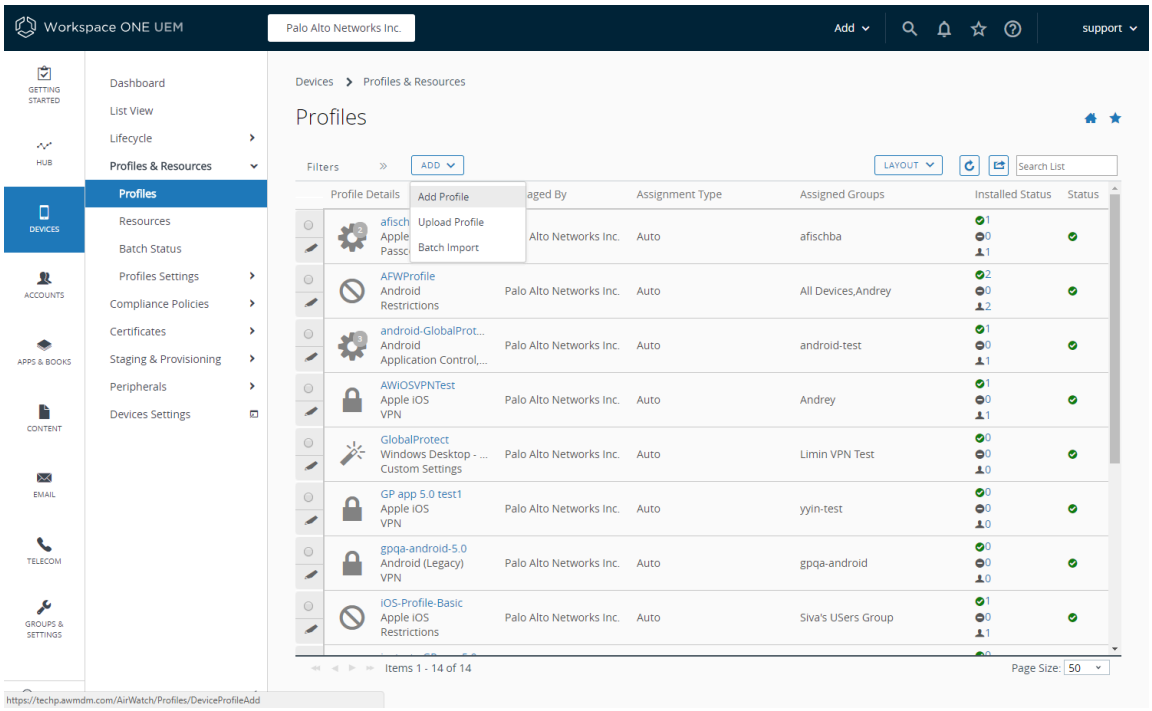
AirWatch を使って Chromebook を管理し始める前に、Chromebook を AirWatch に登録・同期する必要があります。

1. Chromebook で **CTRL+ALT+E** を押してエンタープライズ登録画面を開きます。
2. Google 管理者ウェルカムレターに記載されているユーザー名およびパスワードを入力するか、既存の G Suite ユーザー認証情報を入力します。
3. **Enroll device (デバイスを登録)** をクリックします。Chromebook が正常に登録されたら、確認メッセージを受け取ります。
4. AirWatch コンソールにログインします。
5. **Devices (デバイス)** > **Devices Settings & Users (デバイス設定およびユーザー)** > **Chrome OS** > を選択します。
6. **Device Sync (デバイス同期)** をクリックして登録済みのすべての Chromebook を AirWatch と同期させます。

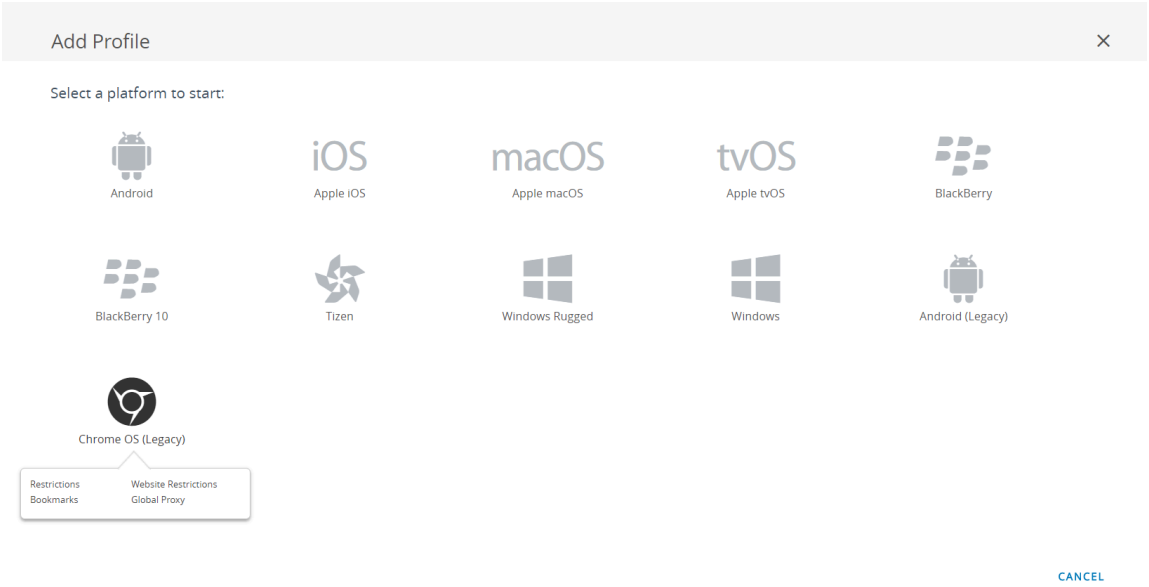
STEP 4 | Android 用 GlobalProtect アプリケーションを AirWatch 上の Chrome OS プロファイルに追加します。

Application Control (アプリケーション制御) プロファイルを使用すれば、Google Play および Chrome ウェブストアからアプリを追加できます。

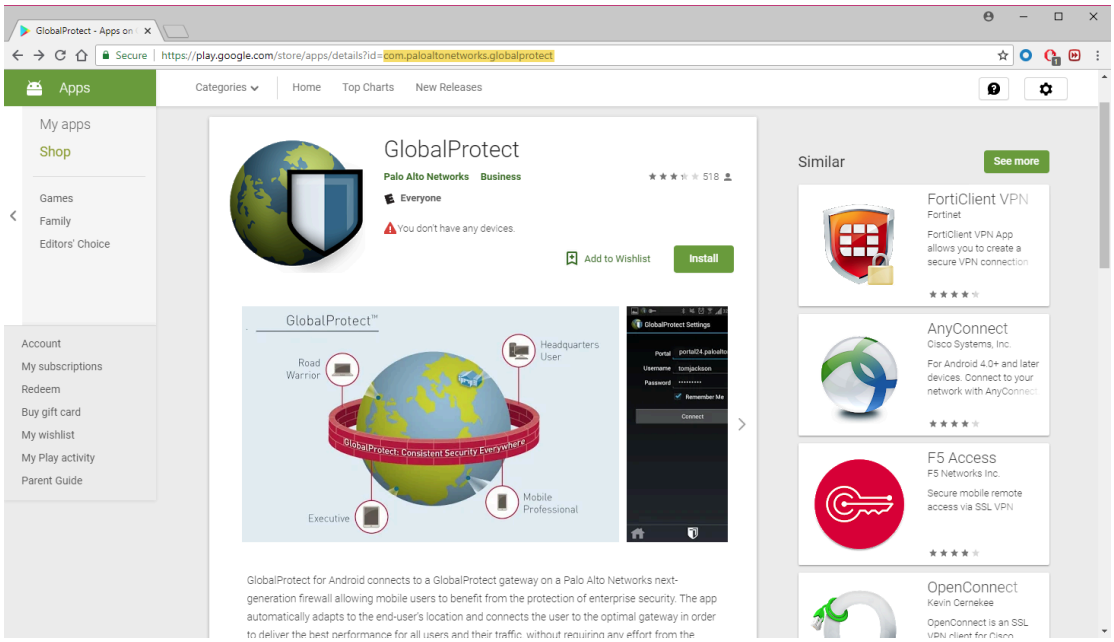
1. AirWatch コンソールにログインします。
2. **Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles (プロファイル)** を選択して新しい Chrome OS プロファイルを **ADD (追加)** します。



3. プラットフォームのリストで **Chrome OS (Legacy) (Chrome OS (レガシー))** を選択します。



4. **General (**一般**)**設定の設定を行います。
5. **Application Control (**アプリケーション制御**)** 設定を行います。
   1. Google Play の URL (com.paloaltonetworks.globalprotect) に表示される GlobalProtect **App ID** を入力します。



2. アプリの **Name (名前)** を入力します。

3. **Pin App to Shelf** (アプリをシェルフにピン留めする) かどうかを指定します。**Y** と入力してアプリを Chromebook のアプリ シェルフにピン留めします。
4. 変更を**SAVE & PUBLISH** (保存して公開)します。

Microsoft Intune を使用した **GlobalProtect** モバイル アプリケーションのデプロイ

Microsoft Intune で登録された管理対象のエンドポイント、あるいは Microsoft Intune を使ってエンドポイントを登録していないユーザー（iOS のみ）に GlobalProtect アプリケーションをデプロイできます。アプリケーションをデプロイしたら、VPN プロファイルを構成して管理対象のエンドポイントにデプロイし、エンドユーザー用の GlobalProtect アプリケーションを自動的にセットアップします。

STEP 1 | Microsoft Intune でエンドポイントを登録します。

GlobalProtect アプリケーションをエンドポイントにデプロイするために、エンドポイントが Microsoft Intune で登録されていることを確認します。

STEP 2 | Microsoft Intune に GlobalProtect アプリケーションを追加します。

GlobalProtect アプリケーションは、アプリを Microsoft Intune に追加した後でなければユーザーやエンドポイントに割り当てることができません。

STEP 3 | GlobalProtect アプリケーション用にアプリの割り当てタイプを設定します。

アプリをユーザーやエンドポイントに割り当てることで、GlobalProtect アプリケーションにアクセスできる人物を指定することができます。アプリを割り当てる前に、そのアプリの割り当てタイプを指定しておく必要があります。この割り当てタイプにより、アプリを利用可能にしたり、必須にしたり、アンインストールしたりできるようになります。

STEP 4 | GlobalProtect アプリケーションを特定のユーザーやエンドポイントに割り当てます。

GlobalProtect アプリケーションの割り当てタイプを設定したら、そのアプリを特定のユーザーやエンドポイントに割り当てられるようになります。

（*iOS のみ*）*Microsoft Intune* でエンドポイントを登録していないユーザーに、*GlobalProtect* アプリケーションを割り当てることができます。

MobileIron を使用した **GlobalProtect** モバイル アプリケーションのデプロイ

MobileIron で登録されている管理対象のエンドポイントに GlobalProtect アプリケーションをデプロイすることができます。アプリケーションをデプロイしたら、VPN プロファイルを構成、デプロイし、エンドユーザー用の GlobalProtect アプリケーションを自動的にセットアップします。

STEP 1 | ユーザーを MobileIron に追加します。

ユーザーが自身のエンドポイントを MobileIron に登録する前に、各ユーザーの項目を作成しておく必要があります。

STEP 2 | （任意）ユーザーをユーザーグループに割り当てます。

ユーザーを別々のユーザーグループに割り当てることで、個々のユーザーではなく参加しているグループに基づいて GlobalProtect アプリケーションをデプロイできます。

STEP 3 | エンドポイントを MobileIron で登録するよう、ユーザーに促します。

ユーザーを MobileIron に追加したら、エンドポイントを登録するよう、ユーザーに促すことができるようになります。

STEP 4 | GlobalProtect アプリケーションを MobileIron アプリ カタログに追加します。

ユーザーが利用できるモバイル アプリがアプリ カタログにリストアップされます。公開されているストア（Apple の App Store など）で GlobalProtect アプリケーションを検索して追加したり、社内用アプリとして MobileIron に直接アプリをアップロードしたりできます。その後、アプリの配信設定を行い、登録済みのエンドポイント上で GlobalProtect アプリケーションをインストール・設定する方法を指定します。

Google 管理コンソールを使用して管理対象 **Chromebook** 上で **Android** 用 **GlobalProtect** アプリケーションをデプロイ

Google 管理コンソールを使用すれば、ウェブベースのロケーションから一元的に Chromebook の設定やアプリケーションを管理できます。管理対象 Chromebook のコンソール上で Android 用 GlobalProtect アプリケーションをデプロイし、関連する VPN 設定を行えるようになっています。

ユーザー向けにアプリケーションを自動的に設定するには、オプションで Google Chromebook 管理コンソールを使用して、設定を構成し、管理対象の Chrome OS デバイスにデプロイできます。Google 管理コンソールを使用して、Chromebook の設定とアプリケーションを管理できます。

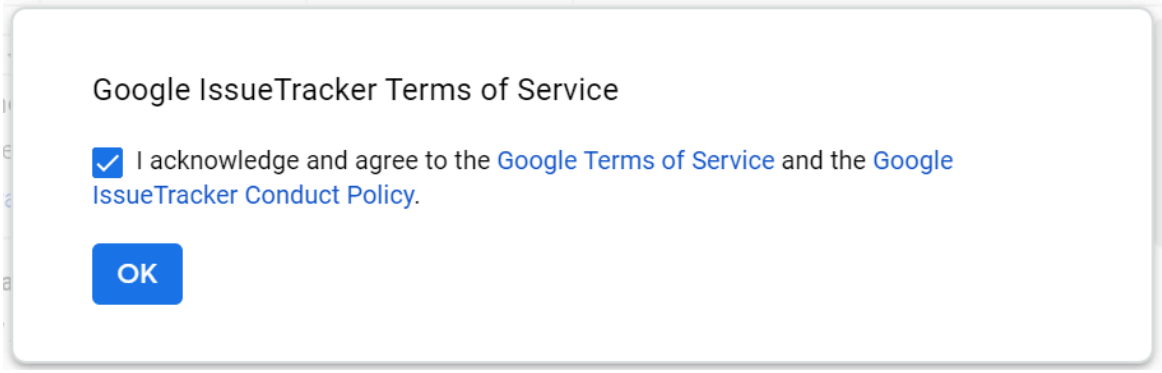
管理対象 *Chromebook* 上で *Android* 用 *GlobalProtect* アプリケーションをデプロイするための推奨事項に従ってください。

- *Google* 管理コンソールを使用して、認証用の一意の証明書をデバイスにプッシュすることはできません。
- お使いの *Chromebook* で、***CTRL+ALT+T*** キーを押すと、ターミナルのコマンドラインが開きます。`route` コマンドを使用して、デバイスにインストールされているルートを表示します。スプリット トンネリングのアクセスルートを含めるかどうかを決定できます。
- アプリケーションは多くの場合異なるファイル形式を使用するため、*OpenSSL* を使用して証明書を *PKCS # 12* 形式から *Base64* 形式に変換できます。`openssl base64 -A -in` *<certificate-in-p12-format>* `-out` *<cert.txt>* コマンドを使用します。

次のステップで、Google 管理コンソールを使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイします：

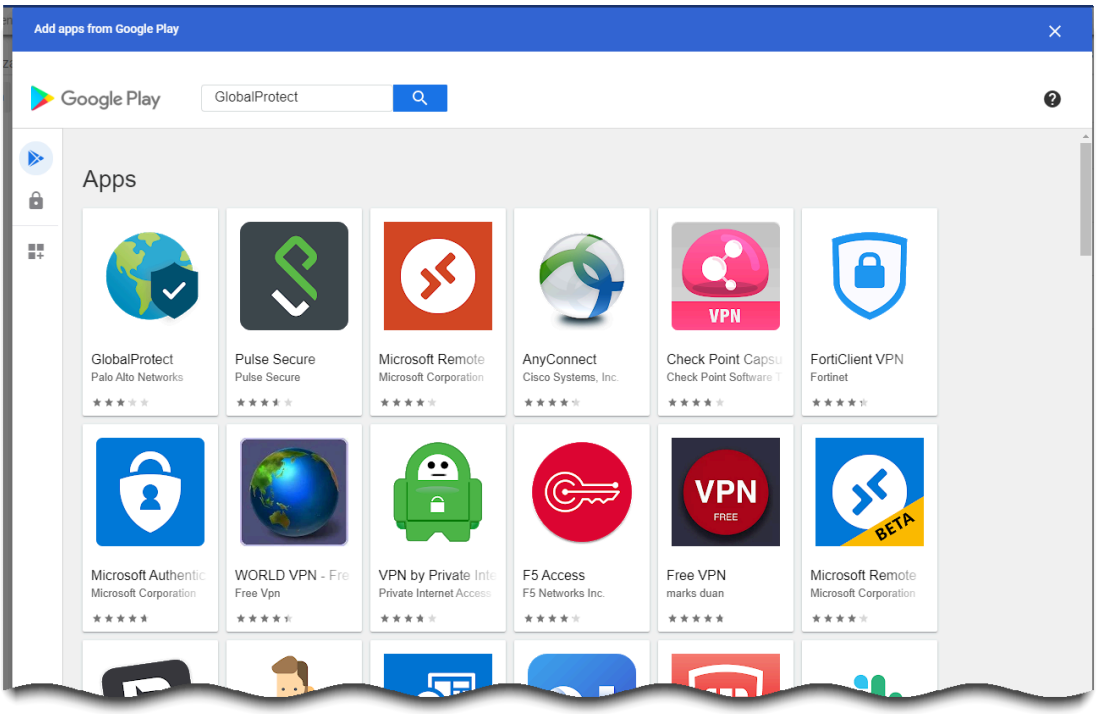
STEP 1 | 開始する前に：

- 管理対象の Chromebook の Android 用のGlobalProtect アプリケーションをサポートするように GlobalProtect ゲートウェイを設定します。GlobalProtect ゲートウェイの設定を参照してください。
- ポータルを設定し、管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをカスタマイズします。GlobalProtect アプリケーションが接続可能なゲートウェイを1つ以上設定する必要があります。GlobalProtect ポータルへのアクセスのセットアップを参照してください。Chrome OS 上の Android がサポートする機能の一覧を確認したい場合は、Palo Alto Networks 互換性マトリクスを参照してください。
- （推奨）シームレスな認証のために、Chromebook 上の Android 用 GlobalProtect アプリケーションの SAML SSO を有効にしてください。ユーザーが Chromebook にログインした後、GlobalProtect アプリケーションで認証情報を再入力しなくても自動的に接続できるように、SAML SSO を設定することをお勧めします。これにより、ユーザーは always on security（セキュリティ常時有効）にアクセスすることができます。SAML 認証のセットアップを参照してください。
- ユーザーが管理対象の Chromebook 上の Android で初めて GlobalProtect に接続する場合、トンネルを設定する前に、以下の VPN 抑制通知メッセージを確認する必要があります。



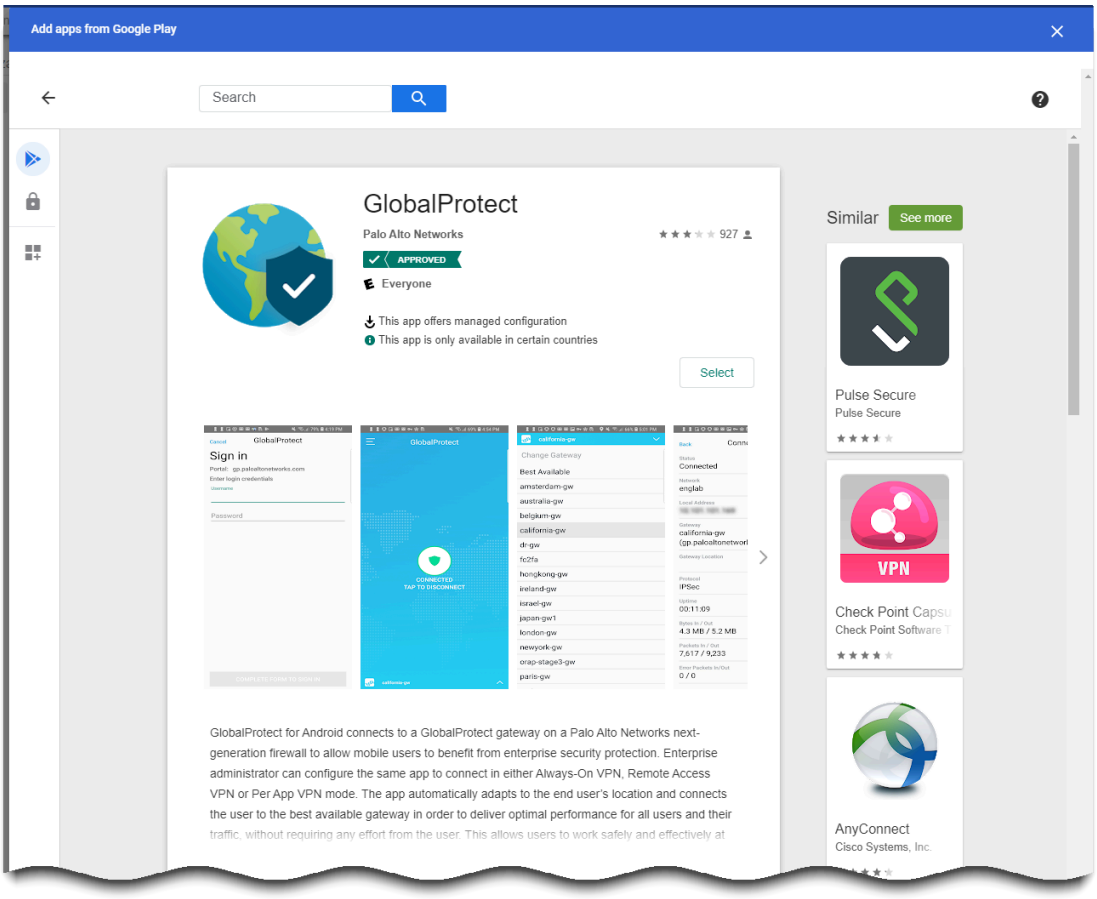
STEP 2 | Chromebook ユーザーのために GlobalProtect アプリケーションを許可します。

1. 管理者として Google 管理コンソールにログインします。
2. 管理者コンソールで **Device (デバイス)** > **Chrome management (Chrome 管理)** を選択して Chrome 管理設定を表示して修正します。
3. **Apps & extensions**（アプリケーションと拡張機能）を選択します。
4. Apps and extensions（アプリケーションと拡張）領域で、 **application settings page**（アプリケーション設定ページ）リンクをクリックします。
5. 追加 ( ) ボタンをクリックし、Google Playstore から承認済みの Android アプリケーションのリストに GlobalProtect を追加します。
6. Google Play ストアが起動する際、**`GlobalProtect`** を検索してから GlobalProtect アプリケーションのアイコンをクリックします。



7. GlobalProtect アプリケーションの追加を **Select (選択)** します。

   GlobalProtect アプリケーションの追加に成功すると、メッセージが表示されます。



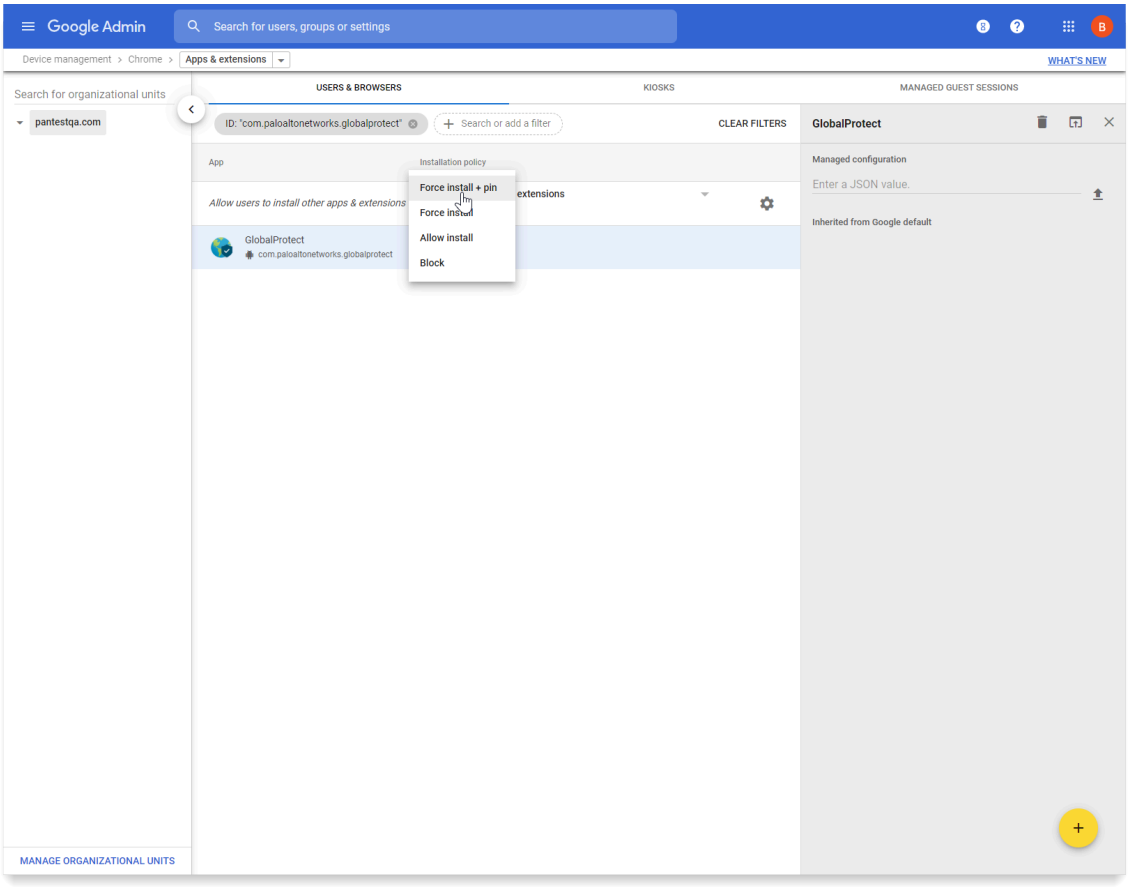
STEP 3 | GlobalProtect アプリケーションを Chromebook にインストールする方法を決定します。

GlobalProtect アプリケーションを許可したら、アプリケーションを Chromebook にインストールする方法を指定する必要があります。ユーザーがアプリをアンインストールすることで GlobalProtect を回避するのを防ぐために、ユーザーが Chromebook にログインする際にすべての Chromebook が自動的に GlobalProtect アプリケーションをインストールするよう強制します。

1. アプリケーション拡張機能管理設定 (**Device Management (デバイス管理)** > **Chrome** > **Apps & extensions (アプリケーションと拡張機能の管理)**) で、アプリケーション一覧から **GlobalProtect** を選択します。
2. ページの左端にあるリストから組織部門を選択します。
3. 以下のいずれかのオプションを選択します。
   - (推奨) **Force install + pin**（インストール + ピンを強制）–強制インストールされた GlobalProtect アプリケーションを有効にしてタスクバーに固定します。このオプションを選択すると、ユーザーはアプリケーションの Sign Out（サインアウト）オプションを利用できなくなります。
   - **Force install**（強制インストール）–ユーザーが Chromebook にログインしたときに GlobalProtect アプリケーションが各 Chromebook に自動的にインストールされるようにする場合は、このオプションを使用します。ユーザーが GlobalProtect アプリをア

ンインストールしてセキュリティとコンプライアンスの要件を回避できないようにするには、**Force install**（強制インストール）オプションを適用します。このオプションを選択すると、ユーザーはアプリケーションの Sign Out（サインアウト）オプションを利用できなくなります。

- **Allow install**（インストールを許可）—Google Playstore からアプリケーションを手動でインストールします。また、このオプションを選択した場合はユーザーが Chromebook から GlobalProtect アプリケーションをアンインストールできます。
- **Block**（ブロック）—ユーザーがこのアプリケーションをインストールすることをブロックします。



4. 変更を **SAVE**（保存）します。

STEP 4 | 管理設定を GlobalProtect アプリケーションに適用します。

GlobalProtect アプリケーションが強制インストールを行えるようにしたら、管理設定ファイルをアプリに適用できます。管理設定ファイルには、変更可能なアプリ設定の値が含まれます。

1. App Management（アプリケーション管理設定）（**Device Management (デバイス管理)** > **Chrome management (Chrome 管理)** > **Apps & Extensions (アプリケーションと拡張機能)**）の Apps (アプリケーション) リストで **GlobalProtect** を選択します。
2. ページの左端にあるリストから組織部門を選択します。
3. ページの右端にある**Upload from file**（ファイルからアップロード）アイコンをクリックして、管理対象の設定ファイルを選択してアップロードします。または、次のサンプル構成のように、JSON 形式のキー値の名前を入力します。

```
{
 "portal": "acme.portal.com",
 "username": "user123"
}
```

次のテーブルは、管理対象設定ファイルの設定例を示しています。お勤め先に関連する設定については、お勤め先の IT 管理者にお問い合わせください。

設定	説明	値タイプ	例
Portal（ポータル）	ポータルの IP アドレスまたは完全修飾ドメイン名（FQDN）。	文字列	**acme.portal.com**
ユーザー名	ポータル認証用のパスワード。	文字列	**user123**
パスワード	ポータル認証用のパスワード。	文字列	**password123**
client_certificate	ポータル認証用のクライアント証明書。	文字列（Base64）	**DAFDSaweEWQ23wDSAFD…**
client_certificate_passphrase	ポータル認証用のクライアント証明書のパスフレーズ。	文字列	**PA$$W0RD$123**
app_list	アプリ単位の VPN 設定 で VPN トンネルを経由できるアプリケーション トラフィックを制御できるブロックリ	文字列	**allow list| block list: com.google.calendar; com.android.email; com.android.chrome**

設定	説明	値タイプ	例
	ストあるいは許可リスト。		
connect_method	VPN 接続方式。	文字列	**user-logon | on-demand**
mobile_id	サードパーティの MDM システムで設定されている、モバイルエンドポイントを識別するのに使用する一意の識別子。	文字列	**5188a8193be43f42d332dde5cb2c941e**
remove_vpn_config_via_restriction	VPN 設定を削除するフラグ。	ブール値	**true | false**
allow_vpn_bypass	アプリケーション トラフィックが VPN トンネルをバイパスできるようにするフラグ。	ブール値	**true | false**
cert_alias	ポータルまたはゲートウェイ認証中にクライアント証明書を識別するために使用される一意の名前。	文字列	**Company User client**
管理対象	デバイスが MDM サーバーに登録されているかどうかを示すフラグ。	ブール値	**true | false**
ownership	デバイスの所有者カテゴリ (例えば、**Employee Owned** (従業員が所有))。	文字列	**byod**
コンプライアンス	デバイスが指定済みのコンプライアンス ポリシーに準拠しているかどうかを示す、コンプライアンスステータス。	文字列	**yes**

設定	説明	値タイプ	例
タグ	デバイスの識別を可能にするタグ。各タグをコンマで区切ってください。	文字列	**GuestAccount,SatelliteOffi**

4. 変更を **SAVE**（保存）します。

STEP 5 | 管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションに関するポリシーを施行します。

- 管理対象 Chromebook の Android に固有の**Host Info**（ホスト情報）を使用して Create HIP objects（HIP オブジェクトの作成）を実行します。次にそれをHost Information Profile（任意のホスト情報プロファイル、HIP）プロファイルの一致条件として使用します。
- HIP プロファイルをポリシールールの一致条件として使用して、対応するセキュリティポリシーを施行を実行します。アプリは、デフォルトで、ホストのセキュリティ状態の特定に役立つ以下の情報のカテゴリに関するデータを収集します。

常時オンの VPN 設定

常時オンの VPN 設定では、セキュアな GlobalProtect 接続が常にオンになります。ユーザーのログイン時に GlobalProtect アプリが GlobalProtect ポータルに接続し、ユーザーおよびホスト情報を送信してエージェント設定を取得します。アプリケーションはポータルからエージェント設定を受信した後、エージェント設定で指定されている GlobalProtect ゲートウェイに自動的に接続し、VPN トンネルを確立します。

サポートされているモバイルデバイス管理システムを使って常時オンの VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- AirWatchを使用した常時オンの VPN 設定
- Microsoft Intune を使用した常時オンの VPN 設定
- MobileIron を使用した常時オンの VPN 設定
- Google 管理コンソールを使用して常時オンの VPN を設定

AirWatchを使用した常時オンの VPN 設定

AirWatch とは、中央のコンソールから一元的にモバイル エンドポイントを管理できるようにする、エンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより、デバイス レベルあるいはアプリケーション レベルで、AirWatch が管理するモバイル エンドポイントおよびファイアウォール間で安全に接続を行えるようになります。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

AirWatch を使って常時オンの VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- AirWatch を使用した iOS エンドポイント用の常時オンの VPN 設定

- AirWatch を使用した Windows 10 UWP エンドポイント用の常時オンの VPN 設定

AirWatch を使用した *iOS* エンドポイント用の常時オンの *VPN* 設定

常時オンの VPN 設定では、セキュアな GlobalProtect 接続が常にオンになります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、必ず VPN トンネル経由でルーティングされます。

次の各作業により、AirWatch を使用して iOS エンドポイント用に常時オンの VPN 設定を構成することができます：

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

- AirWatch を使用して GlobalProtect モバイル アプリケーションをデプロイします。
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

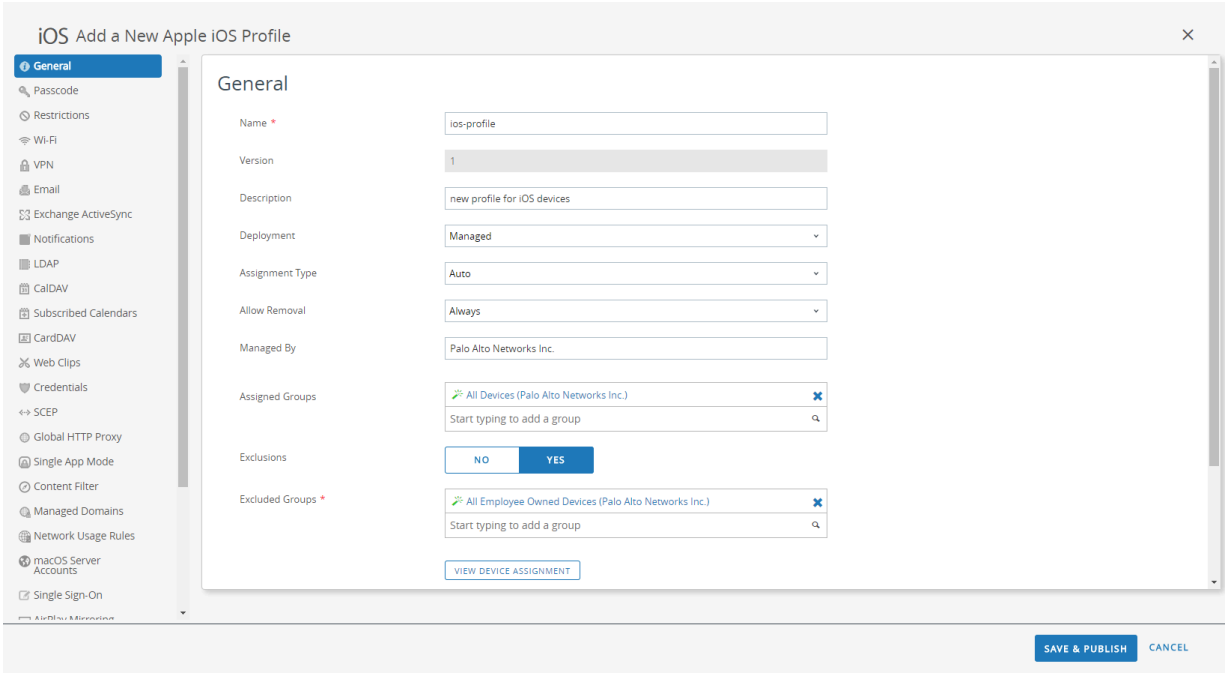
STEP 2 | AirWatch コンソールから、既存の Apple iOS プロファイルを編集するか、新しいプロファイルを追加します。

1. **Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles (プロファイル)**を選択して新しいプロファイルを**ADD (追加)**します。
2. プラットフォームのリストで**iOS**を選択します。

STEP 3 | **General (一般)設定の設定を行います。**

1. プロファイルの**Name**（名前）を入力します。
2. （任意）その目的を示すプロファイルの簡単な**Description (説明)**を入力します。
3. （任意）登録解除時にプロファイルを自動的に削除するかどうかを指定する**Deployment (デプロイメント)**方式として、**Managed**（管理対象）（プロファイルは削除されます）あるいは**Manual**（手動）（プロファイルはエンドユーザーが削除するまでインストールされたままになります）のいずれかを選択します。
4. （任意）プロファイルをエンドポイントにデプロイする方法として、**Assignment Type (割り当てタイプ)**を選択します。プロファイルをすべてのエンドポイントに自動的にデプロイするには、**Auto**（自動）を選択します。エンド ユーザーがプロファイルをセルフサービス ポータル（SSP）からインストールしたり、プロファイルを個別のエンドポイントに手動でデプロイできるようにするには、**Optional**（任意）を選択します。エンド ユーザーがエンドポイントに適用されるコンプライアンス ポリシーに違反した場合にプロファイルをデプロイするには、**Compliance**（コンプライアンス）を選択します。
5. （任意）エンドユーザーに対してプロファイルの**Allow Removal (削除を許可)**するかどうかを選択します。エンド ユーザーがいつでもプロファイルを手動で削除できるようにするには、**Always**（常に許可）を選択します。エンド ユーザーがプロファイルを削除できないようにするには、**Never**（拒否）を選択します。エンド ユーザーがプロファイルを削除するのに管理者の許可が必要になるようにするには、**With Authorization**（認証あり）を選択します。**With Authorization**（認証あり）を選択すると、必要なパスワードが追加されます。
6. （任意）**Managed By (管理者)**フィールドに、プロファイルへの管理アクセスを持つ組織グループを入力します。
7. （任意）**Assigned Groups (割り当てられたグループ)**フィールドに、プロファイルの追加先となるスマート グループを追加します。このフィールドには、最低限の OS、デバイス モデル、所有者カテゴリ、組織グループなどの仕様で設定できる新規スマート グループを作成するオプションが含まれます。
8. （任意）このプロファイルの割り当てに**Exclusions (除外)**を含めるかどうか指定します。**Yes (はい)**を選択すると**Excluded Groups (除外されたグループ)**フィールドが表示され、プロファイルの割り当てから除外するスマート グループを選択できるようになります。
9. （任意）**Install only on devices inside selected areas (選択した範囲に含まれるデバイスのみをインストール)**するオプションを有効化する場合は、特定のジオフェンスあるいは iBeacon リージョン内にあるエンドポイントにしかプロファイルをインストールできません。指示されたら、**Assigned Geofence Areas (割り当てられたジオフェンス エリア)**フィールドにジオフェンスあるいは iBeacon リージョンを追加します。
10. （任意）**Enable Scheduling and install only during selected time periods (スケジュールを有効化し、選択した期間中にのみインストール)**する場合、プロファイルのインストレーションにタイム スケジュール（**Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles Settings (プロファイル設定)** > **Time Schedules (タイム スケジュール)**）を適用し、プロファイルをエンドポイントにインストールできる期間を制限することができます。指示されたら、**Assigned Schedules (割り当てられたスケジュール)**フィールドにスケジュール名を入力します。

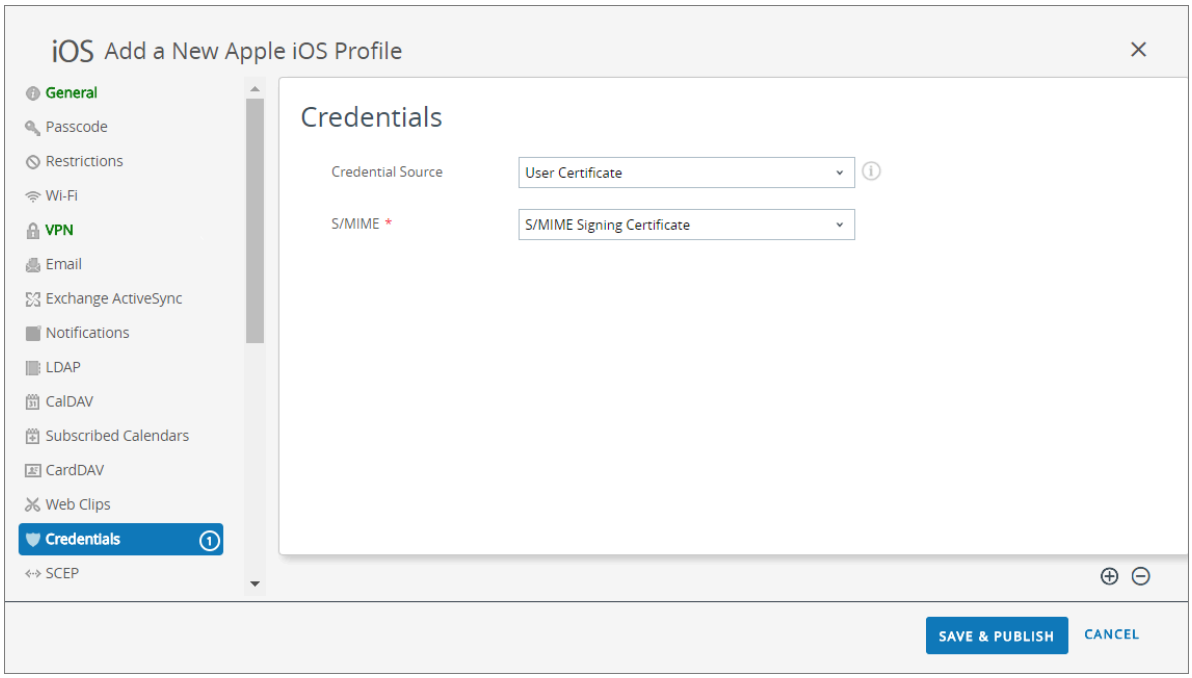
11. （任意）すべてのエンドポイントからプロファイルを削除する**Removal Date (**削除日**)**を選択します。



STEP 4 | （任意）GlobalProtect のデプロイメントでクライアント証明書認証が必要な場合、**Credentials (**認証情報**)**の設定を行います：

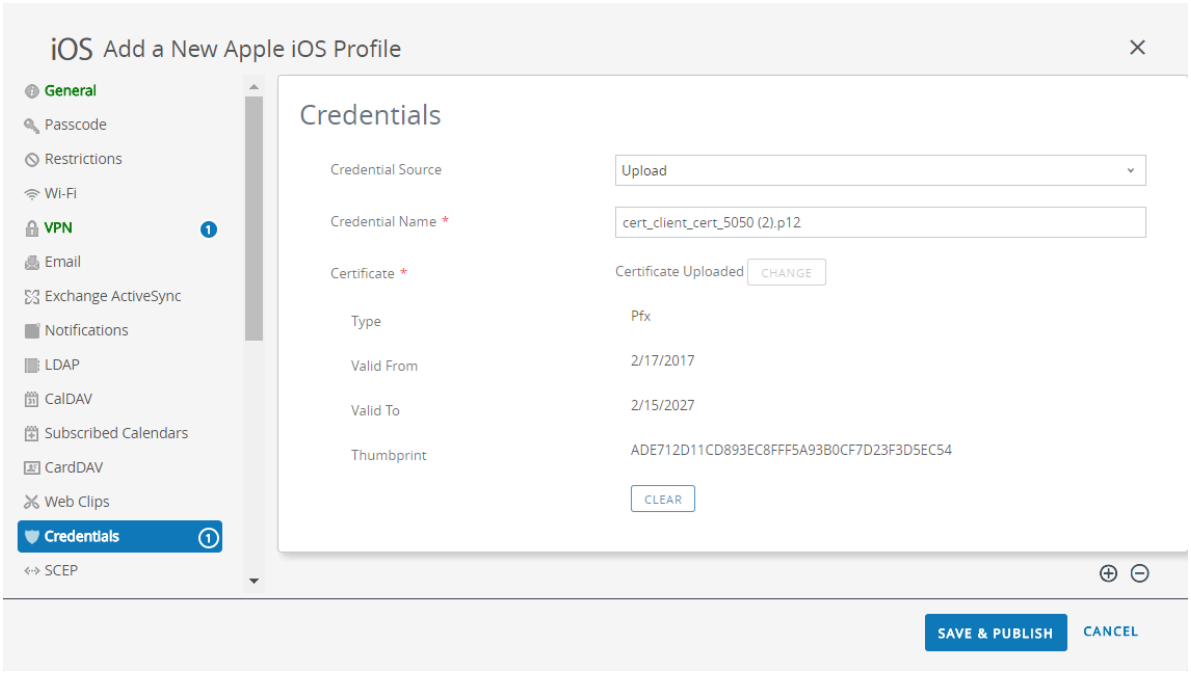
iOS 12 から、*GlobalProtect* クライアント認証用にクライアント証明書を使用する場合、*MDM* サーバーからプッシュされる *VPN* プロファイルの一部としてクライアント証明書をデプロイしなければならなくなります。その他の方式を使って *MDM* サーバーからクライアント証明書をデプロイする場合、*GlobalProtect* アプリケーションで証明書を使用することはできません。

- AirWatch ユーザーからクライアント証明書を取得する方法：
  1. **Credential Source (**認証情報ソース**)**を**User Certificate (**ユーザー証明書**)**に設定します。
  2. **S/MIME Signing Certificate (S/MIME** 署名証明書**)**（デフォルト）を選択します。

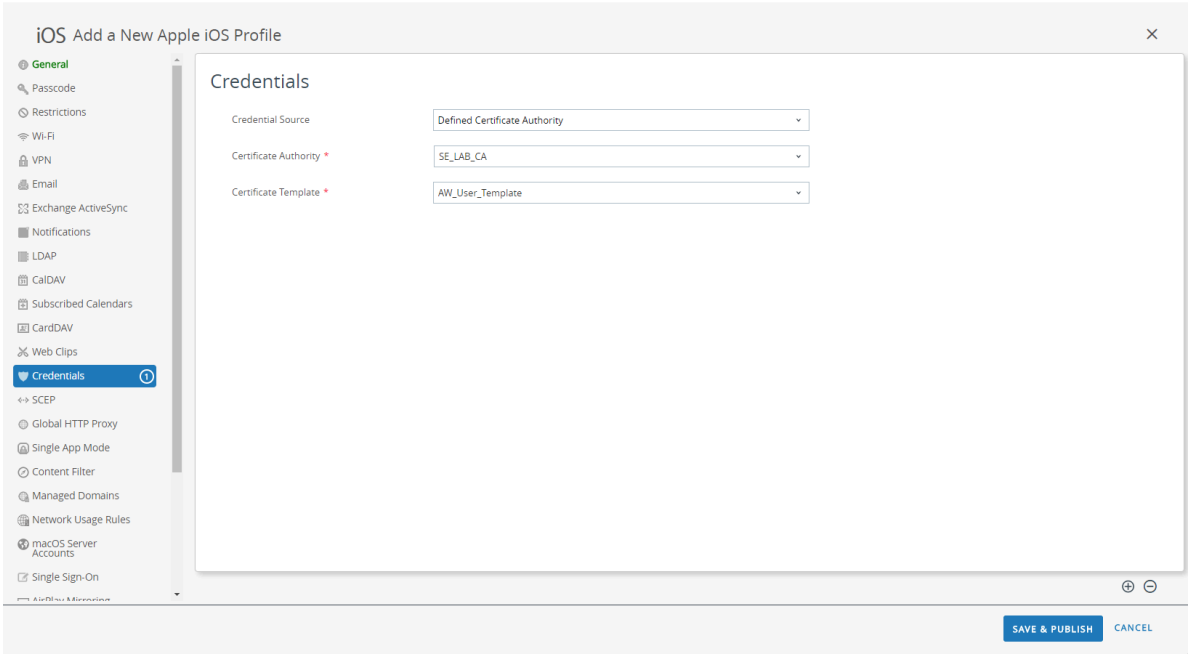


- 手動でクライアント証明書をアップロードする方法：
  1. **Credential Source (**認証情報ソース**)**を **(**アップロード**)**に設定します。
  2. **Credential Name (**認証情報名**)**を入力します。
  3. **UPLOAD (**アップロード**)**をクリックし、アップロードする証明書を参照して選択します。

4. 証明書を選択したら**SAVE (保存)**をクリックします。

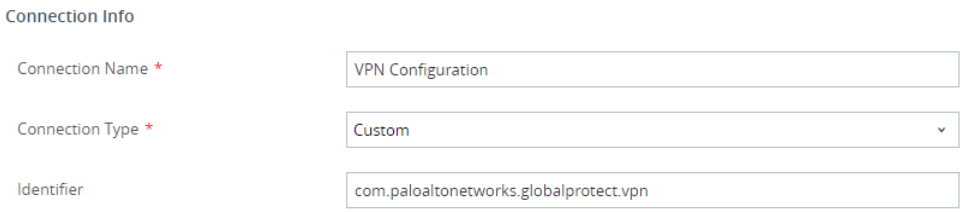


- 事前定義済みの認証局およびテンプレートを使用する方法：
  1. **Credential Source (**認証情報ソース)を**Defined Certificate Authority (**定義済みの認証局)に設定します。
  2. 証明書の取得元にする**Certificate Authority (**認証局)を選択します。
  3. その認証局で使用する**Certificate Template (**証明書テンプレート)を選択します。



STEP 5 | **VPN** の設定を行います。

1. エンドポイントが表示する**Connection Name (**接続名**)**を入力します。
2. ネットワーク**Connection Type (**接続タイプ**)**を選択します：
   - GlobalProtect アプリケーション 4.1.x 以前のリリースの場合、**Palo Alto Networks GlobalProtect**を選択します。
   - GlobalProtect アプリケーション 5.0 以降の場合は**Custom (**カスタム**)**を選択します。
3. （任意）**Connection Type (**接続タイプ**)**を**Custom (**カスタム**)**にセットする場合、GlobalProtect アプリケーションを識別する次のバンドル ID を**Identifier (**識別子**)**フィールドに入力します： **`com.paloaltonetworks.globalprotect.vpn`**



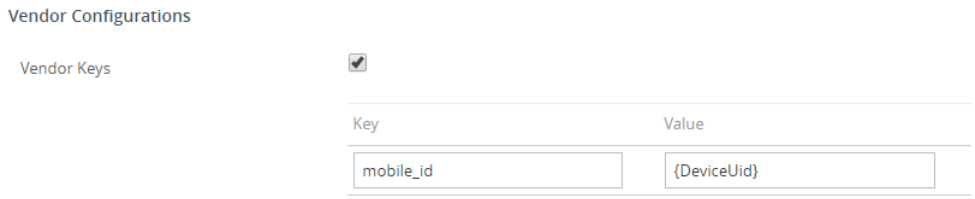
4. ユーザーが接続する GlobalProtect ポータルのホスト名または IP アドレスを**Server (**サーバー**)**フィールドに入力します。
5. （任意）VPN **Account (**アカウント**)**のユーザー名を入力するか、追加（**+**）ボタンをクリックして、サポートされている挿入可能なルックアップ値を見ます。
6. （任意）**Disconnect on idle (**アイドリング時に接続解除**)**フィールドで、アプリケーションがトラフィックを VPN トンネル経由でルーティングするのを停止した後、エンドポイントが GlobalProtect アプリケーションからログアウトするまでの時間（秒）を指定します。
7. Authentication (認証) 領域でユーザーの**Authentication (**認証**)**方式を選択します：**Password (**パスワード**)**、**Certificate (**証明書**)**、**Password + Certificate (**パスワード **+** 証明書**)**。
8. 指示されたら、**Password** （パスワード）の入力および/または GlobalProtect でユーザー認証に使用する **Identity Certificate**（**ID** 証明書）の選択を行います。**Identity Certificate (**アイデンティティ証明書**)**は、**Credentials (**認証情報**)**で設定した証明書と同じものです。
9. **Enable VPN On Demand**（**VPN**オンデマンドを有効にする）と**Use new on demand keys**（新規オンデマンドキーを使用する）を実行します。
10. 以下でオンデマンドルールを設定します: **Action:Connect**（アクション**:** 接続）。
11. （任意）**Proxy (**プロキシ**)**タイプを選択し、関連する設定を行います。

STEP 6 | （任意）（GlobalProtect アプリケーション 5.0 から）GlobalProtect のデプロイ環境で MDM と HIP の統合が必要な場合、一意のデバイス識別子（UDID）属性を指定します。

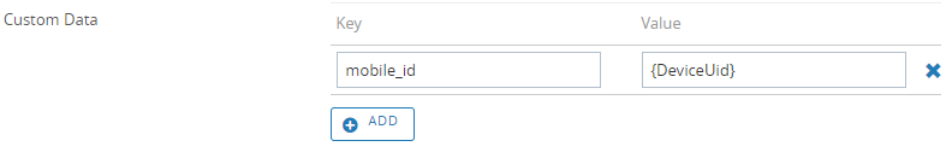
HIP ベースのポリシーを施行するのに使用するモバイル デバイス属性を MDM サーバーから取得するために、GlobalProtect に MDM を統合できるようになっています。GlobalProtect アプリケーションがエンドポイントの UDID を GlobalProtect ゲートウェイに提示しなければ、MDM の統合が機能しません。UDID 属性により、GlobalProtect アプリケーションが MDM ベースのデプロイ環境で UDID 情報を取得・使用できるようになります。プロファイ

ルから UDID 属性を削除すると、MDM の統合を利用できなくなります。GlobalProtect アプリケーションは新しい UDID を生成しますが、それを統合のために使用することはできません。

- **Palo Alto Networks GlobalProtect**ネットワーク**Connection Type (**接続タイプ**)**を使用している場合、**VPN**設定に移動して Vendor Configurations (ベンダー設定) 領域で **Vendor Keys (**ベンダーキー**)**を有効化してください。**Key (**キー**)**を**`mobile_id`**に、**Value (**値**)**を**`{DeviceUid}`**に設定します。



- **Custom (**カスタム**)**ネットワーク**Connection Type (**接続タイプ**)**を使用している場合、**VPN**設定に移動して Connection Info (接続情報) 領域で**Custom Data (**カスタム データ**)**を**ADD (**追加**)**してください。**Key (**キー**)**を**`mobile_id`**に、**Value (**値**)**を**`{DeviceUid}`**に設定します。



STEP 7 | 変更を**SAVE & PUBLISH (**保存して公開**)**します。

AirWatch を使用した *Windows 10 UWP* エンドポイント用の常時オンの *VPN* 設定

常時オンの VPN 設定では、セキュアな GlobalProtect 接続が常にオンになります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、必ず VPN トンネル経由でルーティングされます。セキュリティ要件がさらに厳しい場合、VPN ロックダウンを有効にして、安全な接続を常にオンにして接続状態を保つことを強制するだけでなく、さらにアプリケーションが接続されていない場合にネットワーク アクセスを無効化することができます。この設定は、通常 GlobalProtect ポータル設定で指定する **Enforce GlobalProtect for Network Access**（ネットワーク アクセスの際に必ず **GlobalProtect** を利用する）するオプションと同じです。

Windows エンドポイントについては *AirWatch* でまだ *GlobalProtect* が公式の接続プロバイダとしてリストされていないため、代わりとなる *VPN* プロバイダを選択し、*GlobalProtect* アプリケーションの設定を編集して、以下の手順に従って設定を *VPN* プロファイルにインポートし直す必要があります。

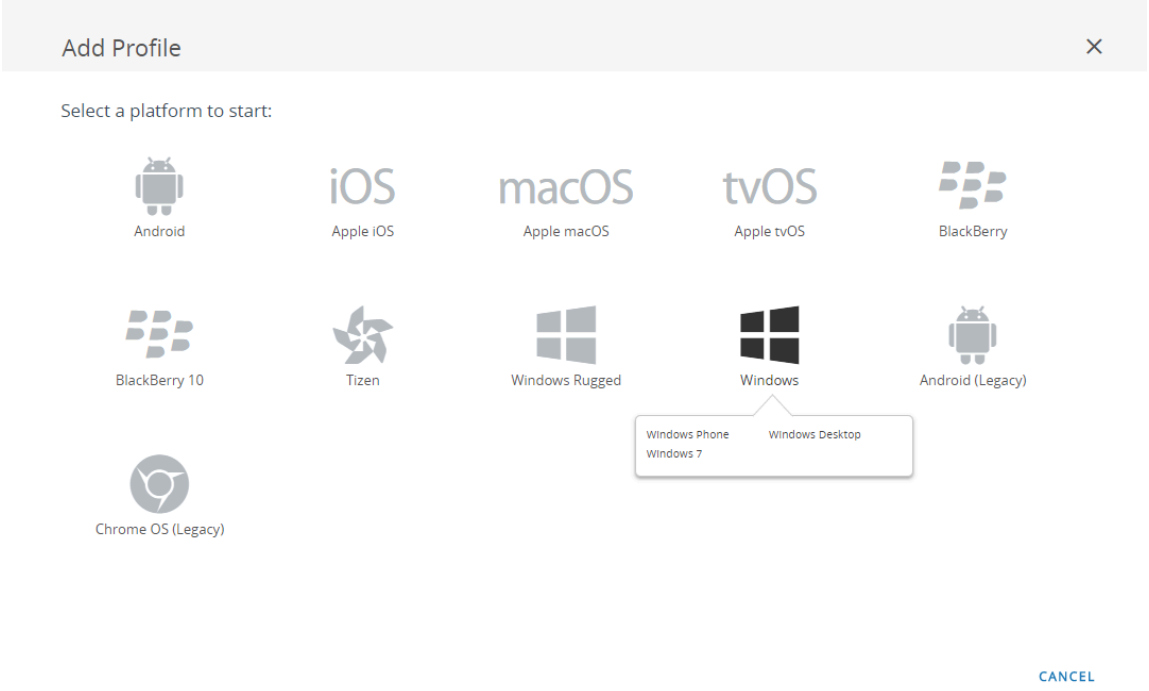
次の各作業により、AirWatch を使用して Windows 10 UWP エンドポイント用に常時オンの VPN 設定を構成することができます：

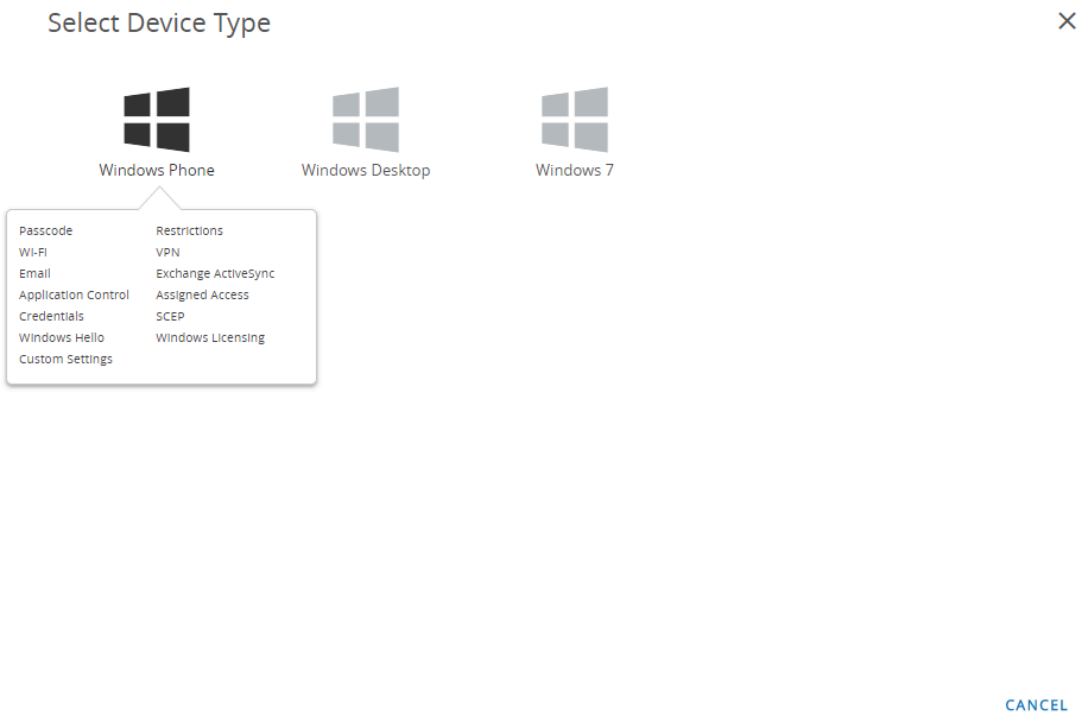
STEP 1 | Windows 10 UWP 用 の GlobalProtect アプリケーションをダウンロードします。

- AirWatch を使用して GlobalProtect モバイル アプリケーションをデプロイします。
- Microsoft ストアから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | AirWatch コンソールから、既存の Windows 10 UWP プロファイルを編集するか、新しいプロファイルを追加します。

1. **Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles (プロファイル)**を選択して新しいプロファイルを**ADD (追加)**します。
2. プラットフォームとして **Windows** を、デバイスタイプとして **Windows Phone**（**Windows** フォン）を選択します。





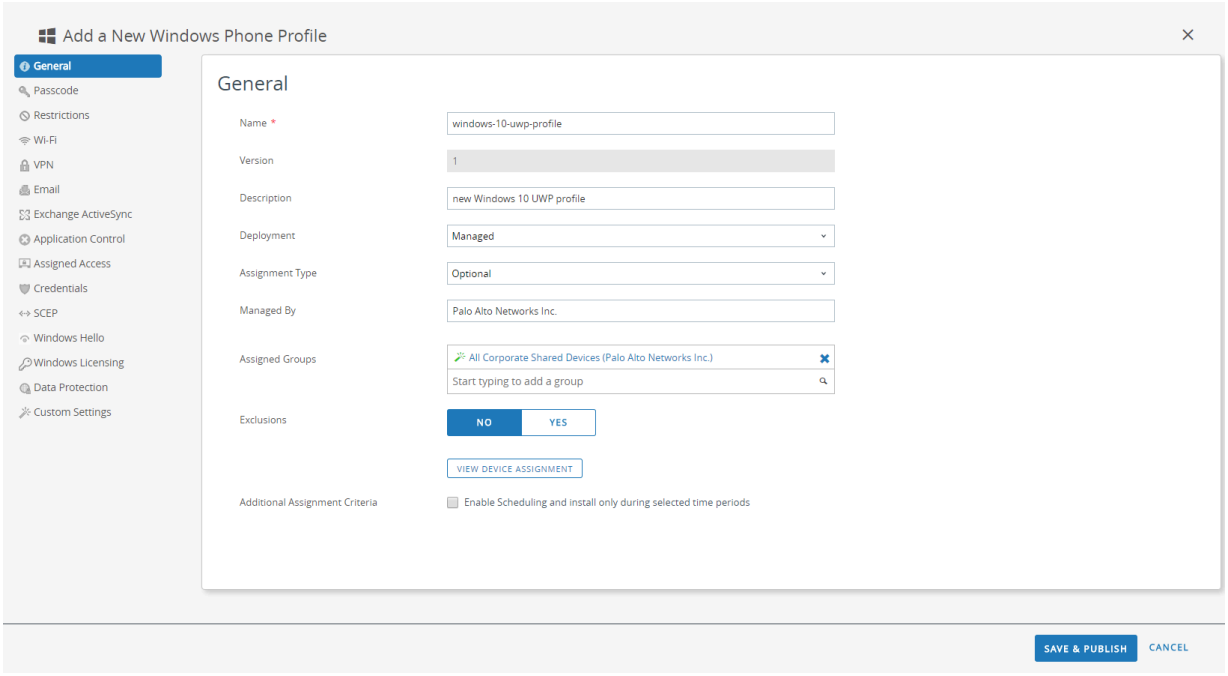
STEP 3 | **General (**一般**)**設定の設定を行います。

1. プロファイルの**Name**（名前）を入力します。
2. （任意）その目的を示すプロファイルの簡単な**Description (**説明**)**を入力します。
3. （任意）**Deployment (**デプロイ**)**方法を**Managed (**管理対象**)**に設定し、登録解除時にプロファイルを自動的に削除できるようにします
4. （任意）プロファイルをエンドポイントにデプロイする方法として、**Assignment Type (**割り当てタイプ**)**を選択します。プロファイルをすべてのエンドポイントに自動的にデプロイするには、**Auto**（自動）を選択します。エンド ユーザーがプロファイルをセルフサービス ポータル（SSP）からインストールしたり、プロファイルを個別のエンドポイントに手

動でデプロイできるようにするには、**Optional**（任意）を選択します。エンド ユーザーがエンドポイントに適用されるコンプライアンス ポリシーに違反した場合にプロファイルをデプロイするには、**Compliance**（コンプライアンス）を選択します。

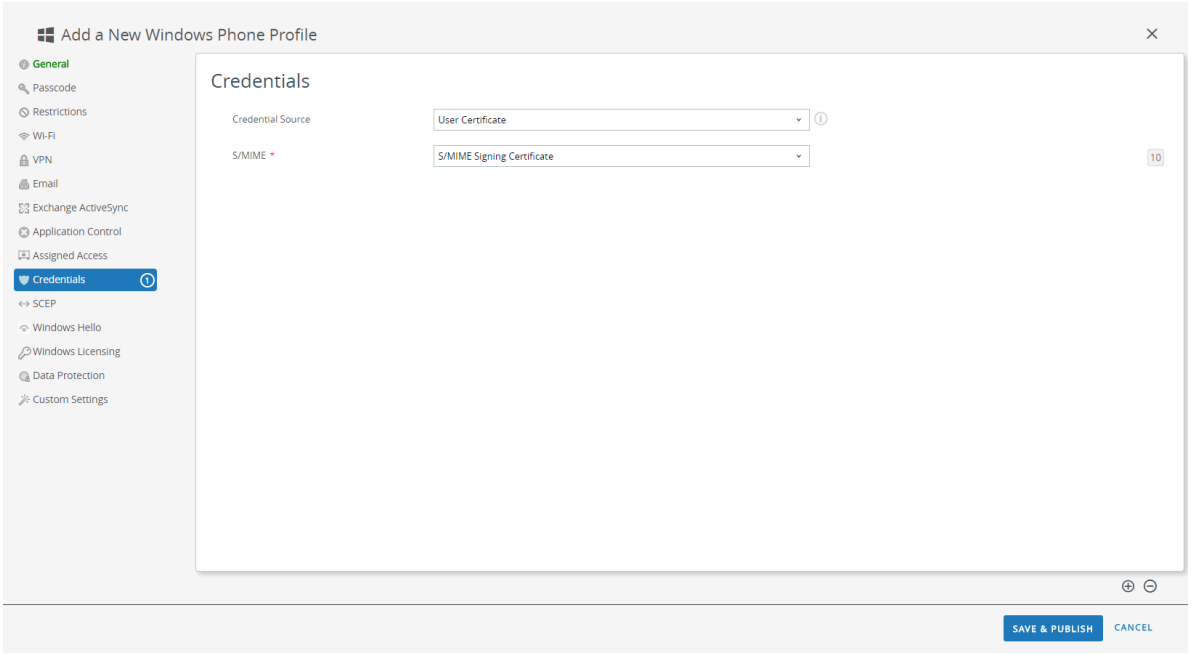
5. （任意）**Managed By (**管理者**)**フィールドに、プロファイルへの管理アクセスを持つ組織グループを入力します。
6. （任意）**Assigned Groups (**割り当てられたグループ**)**フィールドに、プロファイルの追加先となるスマート グループを追加します。このフィールドには、最低限の OS、デバイス モデル、所有者カテゴリ、組織グループなどの仕様で設定できる新規スマート グループを作成するオプションが含まれます。
7. （任意）このプロファイルの割り当てに**Exclusions (**除外**)**を含めるかどうか指定します。**Yes (**はい**)**を選択すると**Excluded Groups (**除外されたグループ**)**フィールドが表示され、プロファイルの割り当てから除外するスマート グループを選択できるようになります。
8. （任意）**Enable Scheduling and install only during selected time periods (**スケジュールを有効化し、選択した期間中にのみインストール**)**する場合、プロファイルのインストレーションにタイム スケジュール（**Devices (**デバイス**)** > **Profiles & Resources (**プロファイルおよびリソース**)** > **Profiles Settings (**プロファイル設定**)** > **Time Schedules (**タイム スケジュール**)**）を適用し、プロファイルをエンドポイントにインストールできる期間を制限すること

ができます。指示されたら、**Assigned Schedules (**割り当てられたスケジュール**)**フィールドにスケジュール名を入力します。



STEP 4 | （任意）GlobalProtect のデプロイメントでクライアント証明書認証が必要な場合、**Credentials (**認証情報**)**の設定を行います：

- AirWatch ユーザーからクライアント証明書を取得する方法：
  1. **Credential Source (**認証情報ソース**)**を**User Certificate (**ユーザー証明書**)**に設定します。
  2. **S/MIME Signing Certificate (S/MIME** 署名証明書**)**（デフォルト）を選択します。

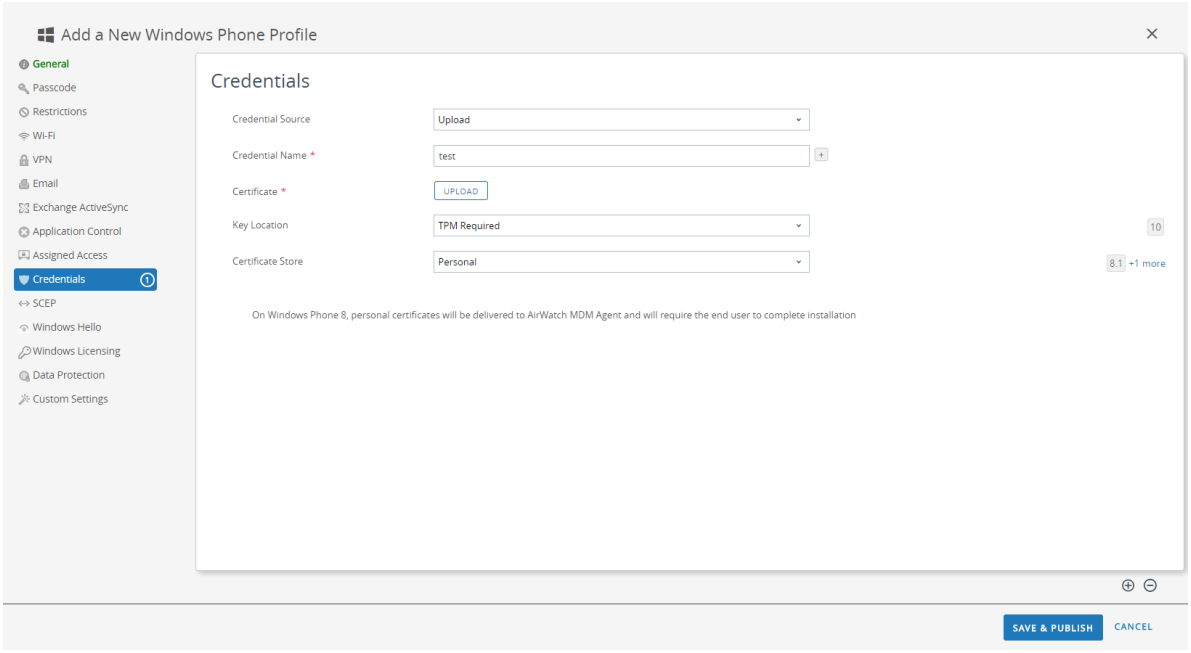


- 手動でクライアント証明書をアップロードする方法：
  1. **Credential Source (**認証情報ソース**)**を **(**アップロード**)**に設定します。
  2. **Credential Name (**認証情報名**)**を入力します。
  3. **UPLOAD (**アップロード**)**をクリックし、アップロードする証明書を参照して選択します。
  4. 証明書を選択したら**SAVE (**保存**)**をクリックします。
  5. 証明書の秘密鍵を保存する**Key Location (**キーの場所**)**を選択します：
     - **TPM Required (TPM** が必要**)**—Trusted Platform Module（信頼されたプラットフォーム モジュール）に秘密鍵を保存します。エンドポイントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵をインストールできません。
     - **TPM If Present (**存在する場合は **TPM)**—信頼されたプラットフォーム モジュールがエンドポイントに存在する場合、秘密鍵をそのモジュールに保存します。エンドポ

イントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵はエンドポイントのソフトウェアに保存されます。

- **Software (ソフトウェア)**—秘密鍵をエンドポイントのソフトウェアに保存します。
- **Passport (パスポート)**—秘密鍵を Microsoft Passport に保存します。このオプションを使用する場合、AirWatch 保護エージェントをエンドポイントにインストールしなければなりません。

6. **Certificate Store**（証明書ストア）を **Personal**（個人）に設定します。

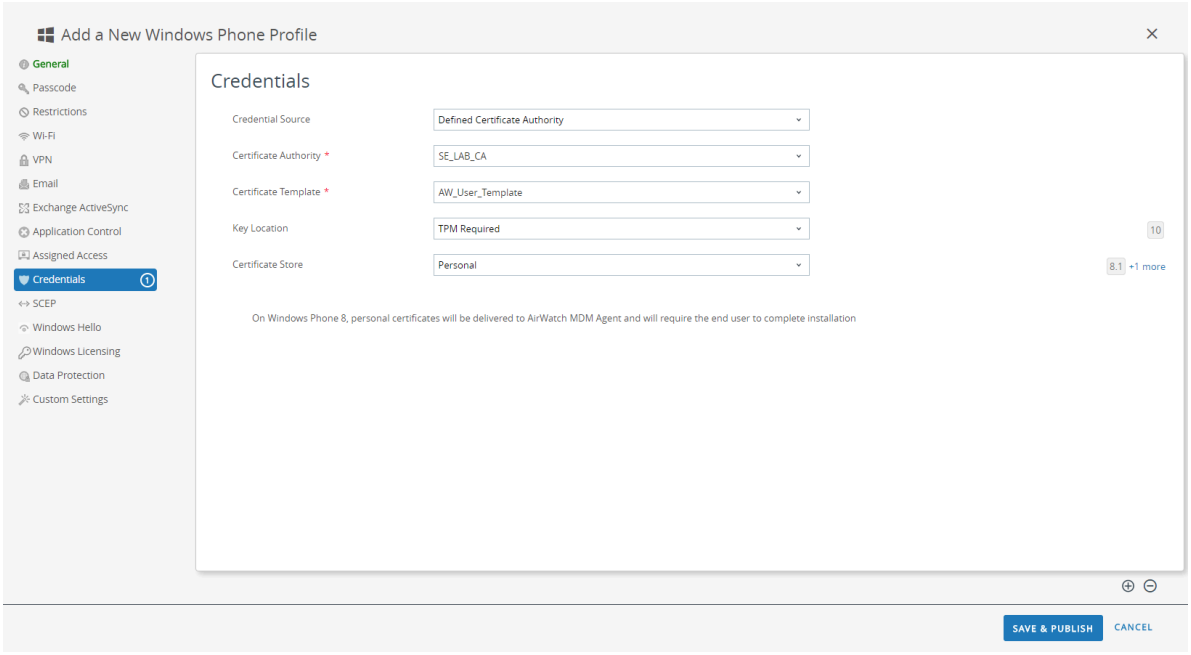


- 事前定義済みの認証局およびテンプレートを使用する方法：
  1. **Credential Source (**認証情報ソース**)**を**Defined Certificate Authority (**定義済みの認証局**)**に設定します。
  2. 証明書の取得元にする**Certificate Authority (**認証局**)**を選択します。
  3. その認証局で使用する**Certificate Template (**証明書テンプレート**)**を選択します。
  4. 証明書の秘密鍵を保存する**Key Location (**キーの場所**)**を選択します：
     - **TPM Required (TPM** が必要**)**—Trusted Platform Module（信頼されたプラットフォーム モジュール）に秘密鍵を保存します。エンドポイントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵をインストールできません。
     - **TPM If Present (**存在する場合は **TPM)**—信頼されたプラットフォーム モジュールがエンドポイントに存在する場合、秘密鍵をそのモジュールに保存します。エンドポ

イントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵はエンドポイントのソフトウェアに保存されます。

- **Software (ソフトウェア)**—秘密鍵をエンドポイントのソフトウェアに保存します。
- **Passport (パスポート)**—秘密鍵を Microsoft Passport に保存します。このオプションを使用する場合、AirWatch 保護エージェントをエンドポイントにインストールしなければなりません。

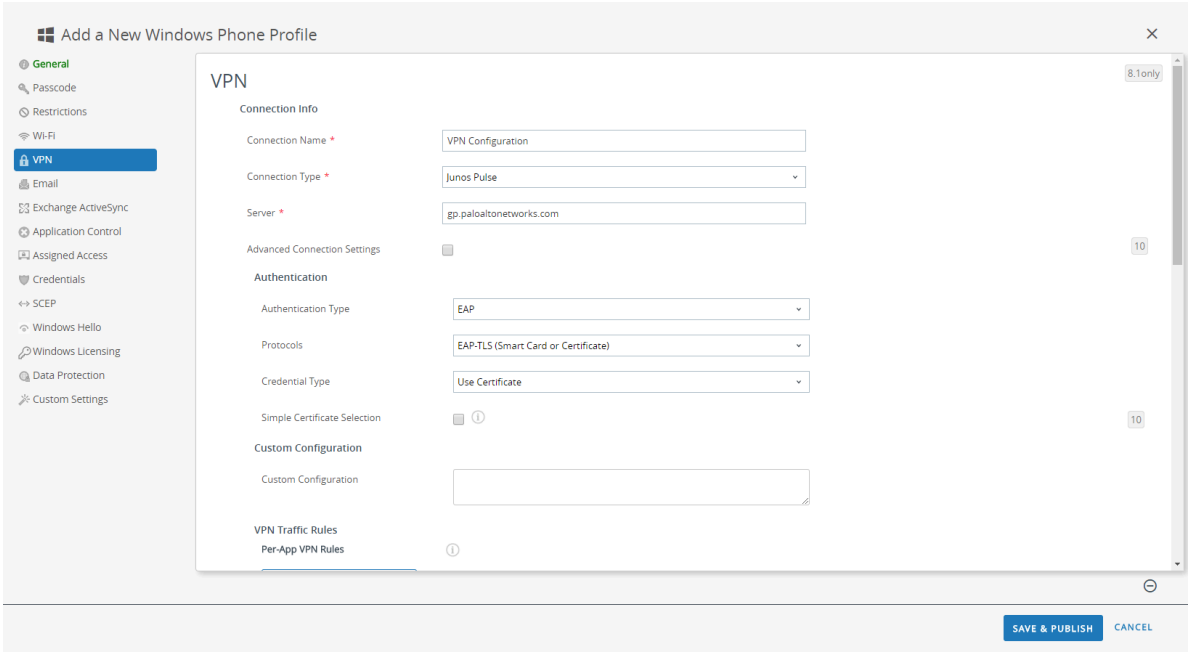
5. **Certificate Store**（証明書ストア）を **Personal**（個人）に設定します。



STEP 5 | **VPN** の設定を行います。

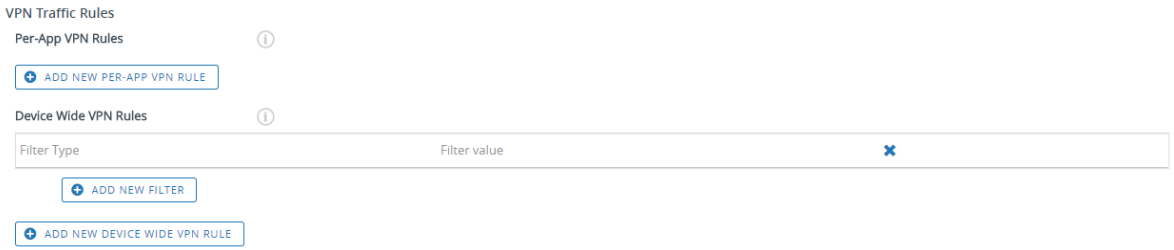
1. エンドポイントが表示する**Connection Name (**接続名**)**を入力します。
2. 別の**Connection Type (**接続タイプ**)**のプロバイダーを選択します（GlobalProtect VPN プロファイルに必要な関連するベンダー設定が含まれていないため、**IKEv2**、**L2TP**、**PPTP**、**Automatic**（自動）は選択しないでください）。

   Windows エンドポイントについては *AirWatch* がまだ *GlobalProtect* を公式の接続プロバイダとしてリストしていないため、代わりとなる *VPN* プロバイダを選択する必要があります。
3. ユーザーが接続する GlobalProtect ポータルのホスト名または IP アドレスを**Server (**サーバー**)**フィールドに入力します。
4. Authentication（認証）領域で**Authentication Type (**認証タイプ**)**を選択し、エンドユーザーを認証する方式を指定します。



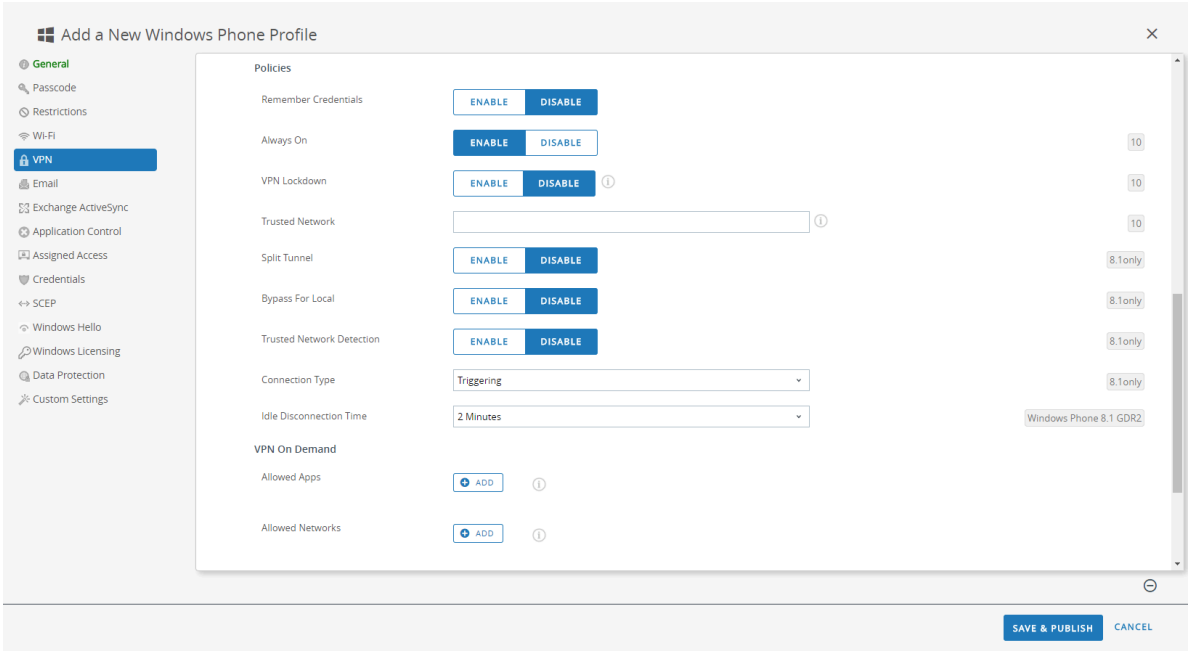
5. （任意）GlobalProtect がユーザーの認証情報を保存するのを許可するには、Policies（ポリシー）エリアにある **Remember Credentials**（認証情報の記憶）オプションを **ENABLE (**有効**)** にします。
6. （任意）VPN Traffic Rules (VPN トラフィック ルール) 領域で**ADD NEW DEVICE WIDE VPN RULE (**全デバイス対象の新しい **VPN** ルールを追加**)**して、特定のルートにマッチするトラフィックを VPN トンネル経由で送信します。このルールはアプリケーション単位に束縛されませんが、エンドポイント全体で評価されます。特定の一致条件にマッチするトラフィックは VPN トンネル経由でルーティングされます。

   ADD NEW FILTER (新規フィルターの追加**)**をクリックしてから**Filter Type (**フィルタータイプ**)**および関連する**Filter Value (**フィルターの値**)**を入力し、一致条件を追加します。



7. GlobalProtect の接続を常に維持するには、Policies (ポリシー) 領域で以下のオプションのいずれかを設定します。
   - **Always On (**常時オン**)**の**ENABLE (**有効化**)**は、安全な接続を常にオンにすることを強制します。
   - **ENABLE VPN Lockdown**（**VPN** ロックダウンの有効化）は安全な接続を常にオンにして接続状態を保つことを強制すると共に、アプリが接続されていない場合にネットワーク アクセスを無効化します。AirWatch の **VPN Lockdown**（**VPN** ロックダウン）オプションは、GlobalProtect ポータル設定で指定する **Enforce GlobalProtect for Network**

Access（ネットワーク アクセスの際に必ず **GlobalProtect** を利用する）オプションと同じです。



8. （任意）信頼されたネットワーク接続を検知した場合にのみ GlobalProtect が接続するようにするには、**Trusted Network**（信頼されたネットワーク）アドレスを指定します。

STEP 6 | 変更を**SAVE & PUBLISH (**保存して公開**)**します。

STEP 7 | GlobalProtect を接続タイプのプロバイダーとして設定する場合、XML 内の VPN プロファイルを編集します。

XML で直接行う追加の編集を最小限にするために、*VPN* プロファイルの設定をエクスポートする前に設定をレビューします。*VPN* プロファイルをエクスポートした後で設定を変更する必要が生じた場合、*XML* に直接変更を加えるか、*VPN* プロファイルの設定を更新して再度このステップを実施することができます。

1. **Devices** > **Profiles**（プロファイル） > **List View**（リスト ビュー） で、前述のステップで追加した新しいプロファイルの隣にあるラジオ ボタンを選択し、次に表の上部にある **</>XML** を選択します。AirWatch でプロファイルの XML ビューが開きます。
2. プロファイルを **Export**（エクスポート）した後、任意のテキスト エディタで開きます。
3. GlobalProtect の以下の設定を編集します。

- `PluginPackageFamilyName` を指定する `LoclURI` エレメントで、エレメントを次のように変更します:

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

- 続く `Data` エレメントで、値を次のように変更します：

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. エクスポートしたプロファイルに加えた変更を保存します。
2. AirWatch に戻り、**Devices**（デバイス） > **Profiles**（プロファイル） > **List View**（リストビュー） を選択します。
3. 新しいプロファイルを作成（**ADD** （追加） > **Add Profile** （プロファイルの追加） > **Windows** > **Windows Phone** （**Windows**フォン））して名前を付けます。
4. **Custom Settings** > **Configure** (カスタム設定 > 設定)を選択し、編集した設定をコピーアンドペーストします。
5. 変更を**SAVE & PUBLISH (**保存して公開**)**します。

STEP 8 | **Devices**（デバイス） > **Profiles**（プロファイル） > **List View**（リスト ビュー）からオリジナルのプロファイルを選択することでオリジナルのプロファイルを消去して、**More Actions**（他の操作） > **Deactivate**（無効化）を選択します。AirWatch により、プロファイルが Inactive（無効）のリストに移動されます。

STEP 9 | 設定のテストを行います。

Microsoft Intune を使用した常時オンの VPN 設定

Microsoft Intune とは、中央から一元的にモバイル エンドポイントを管理できるようにする、クラウド ベースのエンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより、デバイス レベルあるいはアプリケーション レベルで、Microsoft Intune が管理するモバイル エンドポイントおよびファイアウォール間で安全に接続を行えるようになります。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

Microsoft Intune を使って常時オンの VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- Microsoft Intune を使用した iOS エンドポイント用の常時オンの VPN 設定
- Microsoft Intune を使用した Windows 10 UWP エンドポイント用の常時オンの VPN 設定

Microsoft Intune を使用した *iOS* エンドポイント用の常時オンの *VPN* 設定

常時オンの VPN 設定では、セキュアな GlobalProtect 接続が常にオンになります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、必ず VPN トンネル経由でルーティングされます。

次の各作業により、Microsoft Intune を使用して iOS エンドポイント用に常時オンの VPN 設定を構成することができます：

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

- Microsoft Intune を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | （任意）証明書ベースの認証が必要なデプロイ環境の場合、証明書プロファイルの設定を行います。

STEP 3 | 新しい iOS VPN プロファイルを作成します。

- **Platform (プラットフォーム)**を**iOS**に設定します。

STEP 4 | iOS エンドポイント用に常時オンの VPN 設定を行います。

- **Connection type (接続タイプ)**を**Palo Alto Networks GlobalProtect** に設定します。

Microsoft Intune を使用した *Windows 10 UWP* エンドポイント用の常時オンの *VPN* 設定

常時オンの VPN 設定では、セキュアな GlobalProtect 接続が常にオンになります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、必ず VPN トンネル経由でルーティングされます。

次の各作業により、Microsoft Intune を使用して Windows 10 UWP エンドポイント用に常時オンの VPN 設定を構成することができます：

STEP 1 | Windows 10 UWP 用 の GlobalProtect アプリケーションをダウンロードします。

- Microsoft Intune を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- Microsoft ストアから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | （任意）証明書ベースの認証が必要なデプロイ環境の場合、証明書プロファイルの設定を行います。

STEP 3 | 新しい Windows 10 UWP の VPN プロファイルを作成します。

- **Platform (プラットフォーム)**を**Windows 10 and later (Windows 10 以降)**に設定します。

STEP 4 | Windows 10 UWP エンドポイント用に常時オンの VPN 設定を行います。

- **Connection type (接続タイプ)**を**Palo Alto Networks GlobalProtect** に設定します。
- **Always On (常時オン)**の VPN を有効化します。

MobileIron を使用した常時オンの **VPN** 設定

MobileIron とは、中央のコンソールから一元的にモバイル エンドポイントを管理できるようにする、エンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより、デバイス レベルあるいはアプリケーション レベルで、MobileIron が管理するモバイル エンドポイントおよびファイアウォール間で安全に接続を行えるようになります。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

MobileIron を使って常時オンの VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- MobileIron を使用した iOS エンドポイント用の常時オンの VPN 設定
- MobileIron を使用した Android エンドポイント用の常時オンの VPN 設定

MobileIron を使用した *iOS* エンドポイント用の常時オンの *VPN* 設定

常時オンの VPN 設定では、セキュアな GlobalProtect 接続が常にオンになります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、必ず VPN トンネル経由でルーティングされます。

次の各作業により、MobileIron を使用して iOS エンドポイント用に常時オンの VPN 設定を構成することができます：

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

- MobileIron を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | （任意）証明書ベースの認証が必要になるデプロイ環境の場合、証明書設定の追加を行ってから証明書設定を行います。

STEP 3 | 常時オンの VPN 設定を追加します。

- 設定タイプを**Always On VPN (常時オンの VPN)**.

STEP 4 | iOS 用に常時オンの VPN 設定を行います。

MobileIron を使用した *Android* エンドポイント用の常時オンの *VPN* 設定

常時オンの VPN 設定では、セキュアな GlobalProtect 接続が常にオンになります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、必ず VPN トンネル経由でルーティングされます。

次の各作業により、MobileIron を使用して Android エンドポイント用に常時オンの VPN 設定を構成することができます：

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

- MobileIron を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- Google Playから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | （任意）証明書ベースの認証が必要になるデプロイ環境の場合、証明書設定の追加を行ってから証明書設定を行います。

STEP 3 | 常時オンの VPN 設定を追加します。

- 設定タイプを**Always On VPN (**常時オンの **VPN)**.

STEP 4 | Android 用に常時オンの VPN 設定を行います。

Google 管理コンソールを使用して常時オンの **VPN** を設定

Google 管理コンソールとは、中央のコンソールから一元的に Chromebook を管理できるようにする、クラウド ベースのエンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより、デバイス レベルあるいはアプリケーション レベルで、Google 管理コンソールが管理する Chromebook およびファイアウォール間で安全に接続を行えるようになります。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

Google 管理コンソールを使用して *Chromebook* 用に常時オンの *VPN* を設定

Chromebook は Android 用 GlobalProtect アプリケーションの拡張サポートを通じて常時オンの VPN をサポートします。常時オンの VPN 設定では、セキュアな GlobalProtect 接続が常にオンになります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、必ず VPN トンネル経由でルーティングされます。エンドユーザーが自身の Chromebook 上で Android 用 GlobalProtect アプリケーションを起動できるようにすることで、必ずユーザーが常に GlobalProtect に接続され、常時オンのセキュリティを利用できるようにすることができます。

- *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。
- *Android* アプリケーションをサポートしていない *Chromebook* では、*Chromebook* 用 *GlobalProtect* アプリケーションを引き続き使用する必要があります。しかし、これらの *Chromebook* は常時オンの *VPN* をサポートしていません。
- *VPN* を常時オンする機能のために *Android* 用 *GlobalProtect* アプリケーションを *Chromebook* にインストールする場合、*Chromebook* 用 *GlobalProtect* アプリケーションを同じ *Chromebook* にインストールすることはできません。

以下の各作業により、Google 管理コンソールを使用して Chromebook 用にAlways On(常時オン)の VPN 設定を設定することができます。

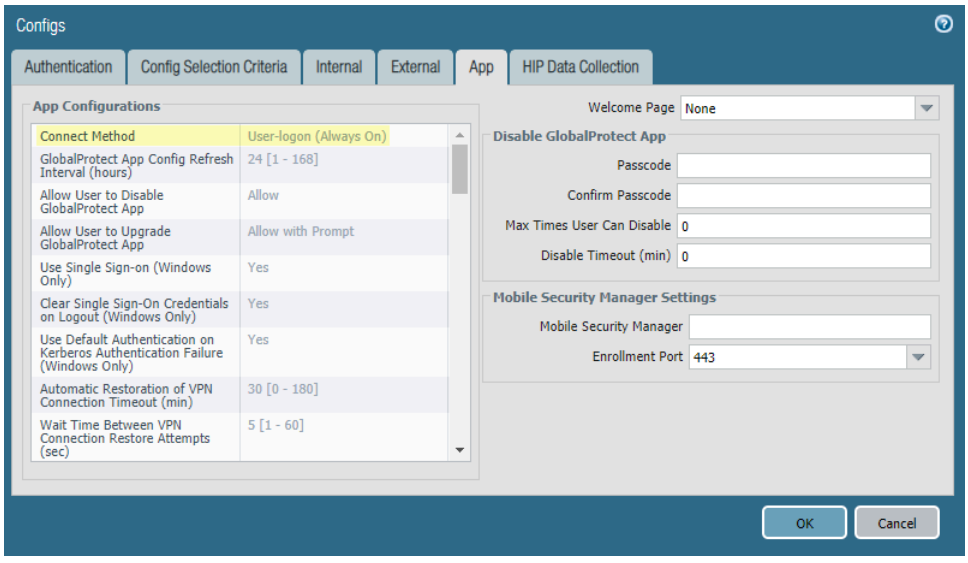
以下のステップは、Google 管理コンソールを使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイする場合にのみ適用されます。現在、AirWatch は管理対象 Chromebook における Android 用 GlobalProtect アプリケーションのための常時オンの VPN 設定をサポートしていません。

STEP 1 | Palo Alto Networks のファイアウォールから、GlobalProtect ポータルへのアクセスのセットアップします。

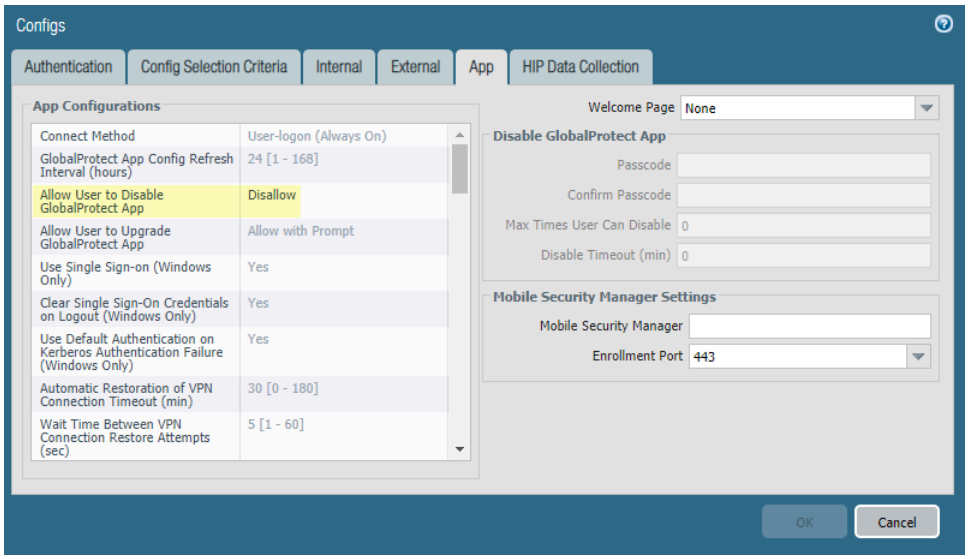
STEP 2 | GlobalProtect エージェント設定の定義.

STEP 3 | GlobalProtect アプリのカスタマイズを定義する.

- GlobalProtect 接続を常にオンにするよう構成するには、**Connect Method (**接続方式**)** を **User-logon (Always On) (**ユーザーログオン **(**常にオン**))** に設定します。



- ユーザーが GlobalProtect アプリケーションを無効化できないようにするために、**Allow User to Disable GlobalProtect App (**ユーザーが **GlobalProtect** アプリを無効化できるようにする**)** オプションを **Disallow (**許可しない**)** に設定します。

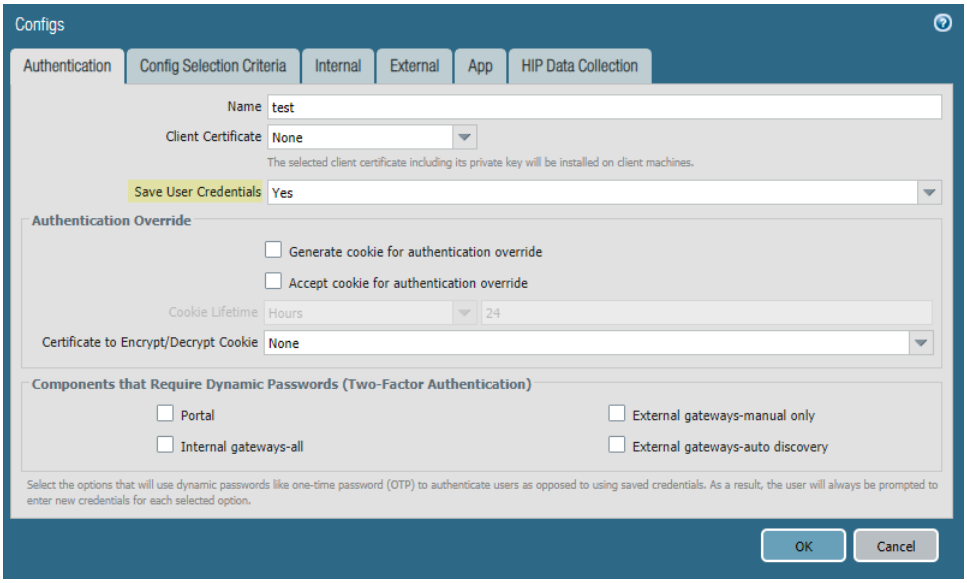


STEP 4 | GlobalProtect の透過的な認証を有効化します。

ユーザーが GlobalProtect 認証プロンプトを回避することで、GlobalProtect 接続が解除されたときに GlobalProtect 接続をバイパスするのを防ぐために、次のいずれかのオプションを設定して透過的な認証を行います：

- クライアント証明書認証を使用してユーザーが GlobalProtect に透過的に認証できるようにします。
- GlobalProtect アプリケーションが透過的なログインを行うためにユーザー名およびパスワードの両方を保存できるようにします。

1. ポータルのエージェント設定 (**Network (ネットワーク)** > **GlobalProtect** > **Portals (ポータル)** > ***<portal-config>*** > **Agent (エージェント)** > ***<agent-config>***) で **Authentication (認証)** を選択します。
2. **Save User Credentials (ユーザー認証情報の保存)** オプションを **Yes (はい)** に設定します。

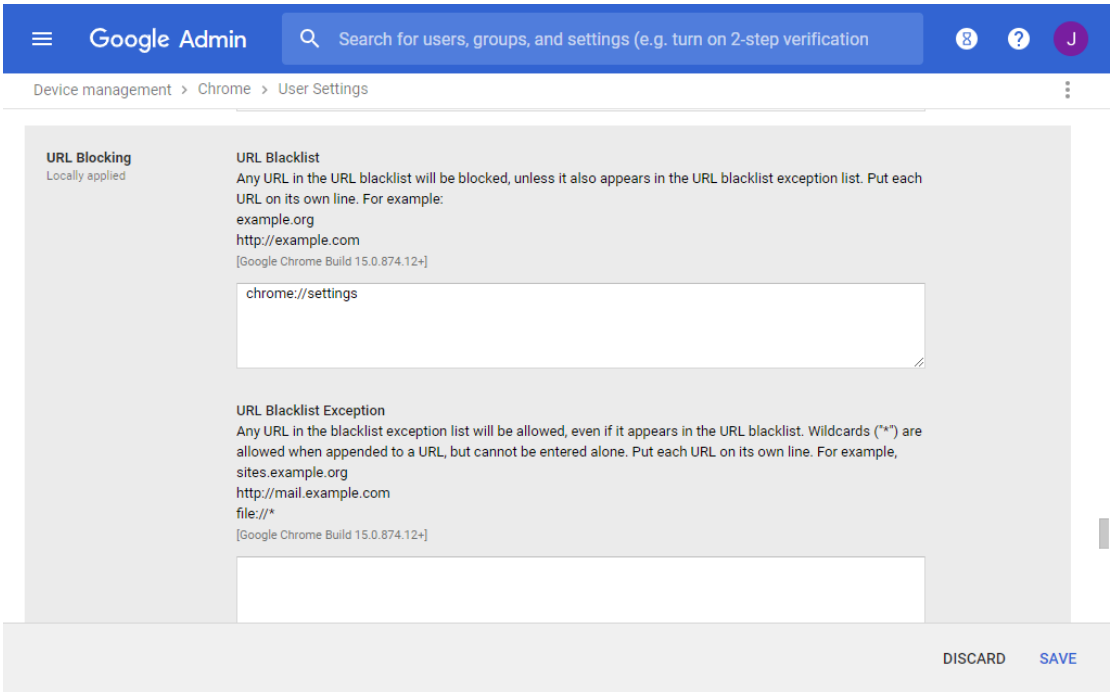


3. **OK** を 2 回クリックしてポータルの設定を保存します。

STEP 5 | ファイアウォールへの変更を **Commit**（コミット）します。

STEP 6 | Chromebook ユーザーが Chrome OS VPN 設定を使用して GlobalProtect をバイパスするのを防ぎます。

1. 管理者として Google 管理コンソールにログインします。
2. Google 管理コンソールを使用して管理対象 Chromebook 上で Android 用 GlobalProtect アプリケーションをデプロイすべての管理対象の Chromebooks 上。
3. Chrome 設定 (**chrome://settings**) をブラックリストに登録し、ユーザーが VPN 設定を変更するのを防ぎます：
   1. **Device Management (デバイス管理)** > **Chrome management (Chrome 管理)** > **User Settings (ユーザー設定)** を選択します。
   2. Content (コンテンツ) > URL Blocking (URL ブロック) 領域の **URL Blacklist (URL ブラックリスト)** テキストボックスに **chrome://settings** と入力します。



4. 変更を **SAVE**（保存）します。

ユーザーが開始するリモート アクセス **VPN** 設定

リモート アクセス（オンデマンド）による VPN の構成では、ユーザーが手動で GlobalProtect アプリケーションを起動して安全な GlobalProtect の接続を確立する必要があります。ユーザーのログイン時に GlobalProtect アプリが GlobalProtect ポータルに接続し、ユーザーおよびホスト情報を送信してエージェント設定を取得します。アプリケーションはポータルからエージェント設定を受信した後、エージェント設定で指定されている GlobalProtect ゲートウェイに接続し、VPN トンネルを確立します。

サポートされているモバイルデバイス管理システムを使ってユーザーが開始するリモート アクセス VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- AirWatch を使用してユーザーが開始するリモート アクセス VPN を設定
- Microsoft Intune を使用してユーザーが開始するリモート アクセス VPN を設定
- MobileIron を使用してユーザーが開始するリモート アクセス VPN を設定

AirWatch を使用してユーザーが開始するリモート アクセス **VPN** を設定

AirWatch とは、中央のコンソールから一元的にモバイル エンドポイントを管理できるようにする、エンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより AirWatch 管理モバイル エンドポイントとファイアウォール間の、デバイスまたはアプリケーションレベルでの保護された接続が実現します。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

AirWatch を使ってユーザーが開始するリモート アクセス VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- AirWatch を使用してユーザーが開始するリモート アクセス VPN を iOS エンドポイント用に設定
- AirWatch を使用してユーザーが開始するリモート アクセス VPN を Windows 10 UWP エンドポイント用に設定

AirWatch を使用してユーザーが開始するリモート アクセス *VPN* を *iOS* エンドポイント用に設定

リモート アクセス（オンデマンド）による VPN の構成では、ユーザーが手動でアプリを起動して安全な GlobalProtect の接続を確立する必要があります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、ユーザーが接続を開始・確立した後にのみ、必ず VPN トンネル経由でルーティングされます。

次の各作業により、AirWatch を使用して iOS エンドポイント用にユーザーが開始するリモート アクセス VPN 設定を構成することができます：

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

- AirWatch を使用して GlobalProtect モバイル アプリケーションをデプロイします。
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

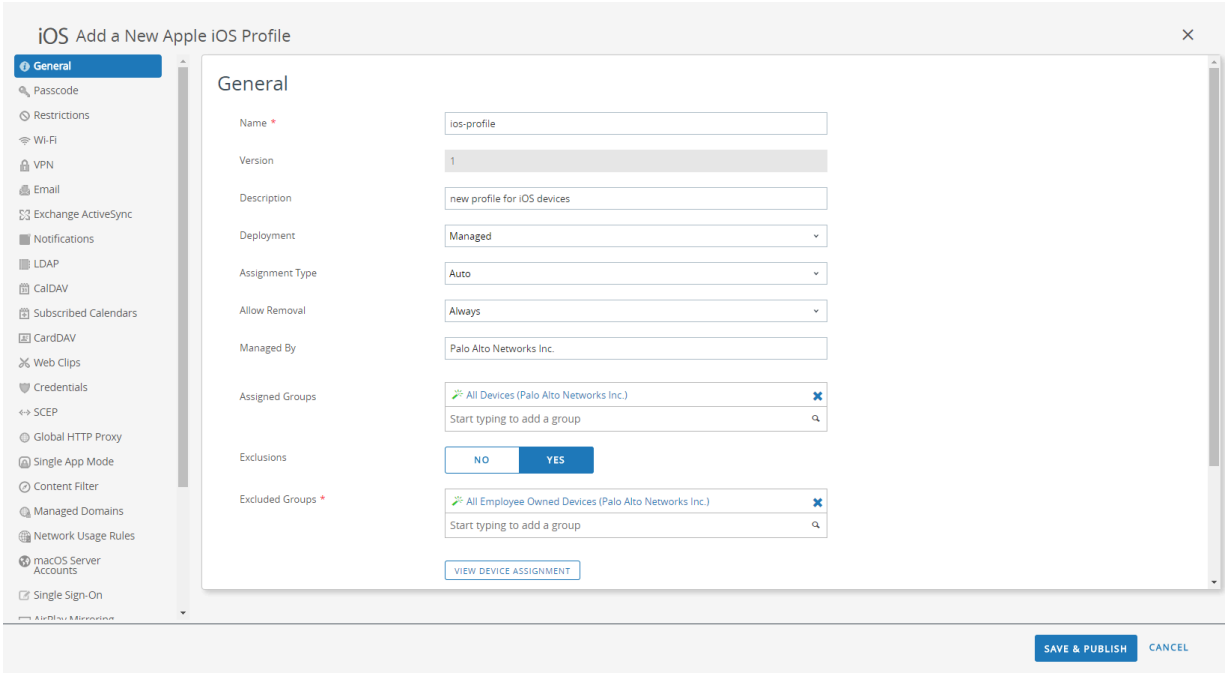
STEP 2 | AirWatch コンソールから、既存の Apple iOS プロファイルを編集するか、新しいプロファイルを追加します。

1. **Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles (プロファイル)**を選択して新しいプロファイルを**ADD (追加)**します。
2. プラットフォームのリストで**iOS**を選択します。

STEP 3 | **General (一般)設定の設定を行います。**

1. プロファイルの**Name**（名前）を入力します。
2. （任意）その目的を示すプロファイルの簡単な**Description (説明)**を入力します。
3. （任意）登録解除時にプロファイルを自動的に削除するかどうかを指定する**Deployment (デプロイメント)**方式として、**Managed**（管理対象）（プロファイルは削除されます）あるいは**Manual**（手動）（プロファイルはエンドユーザーが削除するまでインストールされたままになります）のいずれかを選択します。
4. （任意）プロファイルをエンドポイントにデプロイする方法として、**Assignment Type (割り当てタイプ)**を選択します。プロファイルをすべてのエンドポイントに自動的にデプロイするには、**Auto**（自動）を選択します。エンド ユーザーがプロファイルをセルフサービス ポータル（SSP）からインストールしたり、プロファイルを個別のエンドポイントに手動でデプロイできるようにするには、**Optional**（任意）を選択します。エンド ユーザーがエンドポイントに適用されるコンプライアンス ポリシーに違反した場合にプロファイルをデプロイするには、**Compliance**（コンプライアンス）を選択します。
5. （任意）エンドユーザーに対してプロファイルの**Allow Removal (削除を許可)**するかどうかを選択します。エンド ユーザーがいつでもプロファイルを手動で削除できるようにするには、**Always**（常に許可）を選択します。エンド ユーザーがプロファイルを削除できないようにするには、**Never**（拒否）を選択します。エンド ユーザーがプロファイルを削除するのに管理者の許可が必要になるようにするには、**With Authorization**（認証あり）を選択します。**With Authorization**（認証あり）を選択すると、必要なパスワードが追加されます。
6. （任意）**Managed By (管理者)**フィールドに、プロファイルへの管理アクセスを持つ組織グループを入力します。
7. （任意）**Assigned Groups (割り当てられたグループ)**フィールドに、プロファイルの追加先となるスマート グループを追加します。このフィールドには、最低限の OS、デバイス モデル、所有者カテゴリ、組織グループなどの仕様で設定できる新規スマート グループを作成するオプションが含まれます。
8. （任意）このプロファイルの割り当てに**Exclusions (除外)**を含めるかどうか指定します。**Yes (はい)**を選択すると**Excluded Groups (除外されたグループ)**フィールドが表示され、プロファイルの割り当てから除外するスマート グループを選択できるようになります。
9. （任意）**Install only on devices inside selected areas (選択した範囲に含まれるデバイスのみをインストール)**するオプションを有効化する場合は、特定のジオフェンスあるいは iBeacon リージョン内にあるエンドポイントにしかプロファイルをインストールできません。指示されたら、**Assigned Geofence Areas (割り当てられたジオフェンス エリア)**フィールドにジオフェンスあるいは iBeacon リージョンを追加します。
10. （任意）**Enable Scheduling and install only during selected time periods (スケジュールを有効化し、選択した期間中にのみインストール)**する場合、プロファイルのインストレーションにタイム スケジュール（**Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles Settings (プロファイル設定)** > **Time Schedules (タイム スケジュール)**）を適用し、プロファイルをエンドポイントにインストールできる期間を制限することができます。指示されたら、**Assigned Schedules (割り当てられたスケジュール)**フィールドにスケジュール名を入力します。

11. （任意）すべてのエンドポイントからプロファイルを削除する**Removal Date (**削除日**)**を選択します。

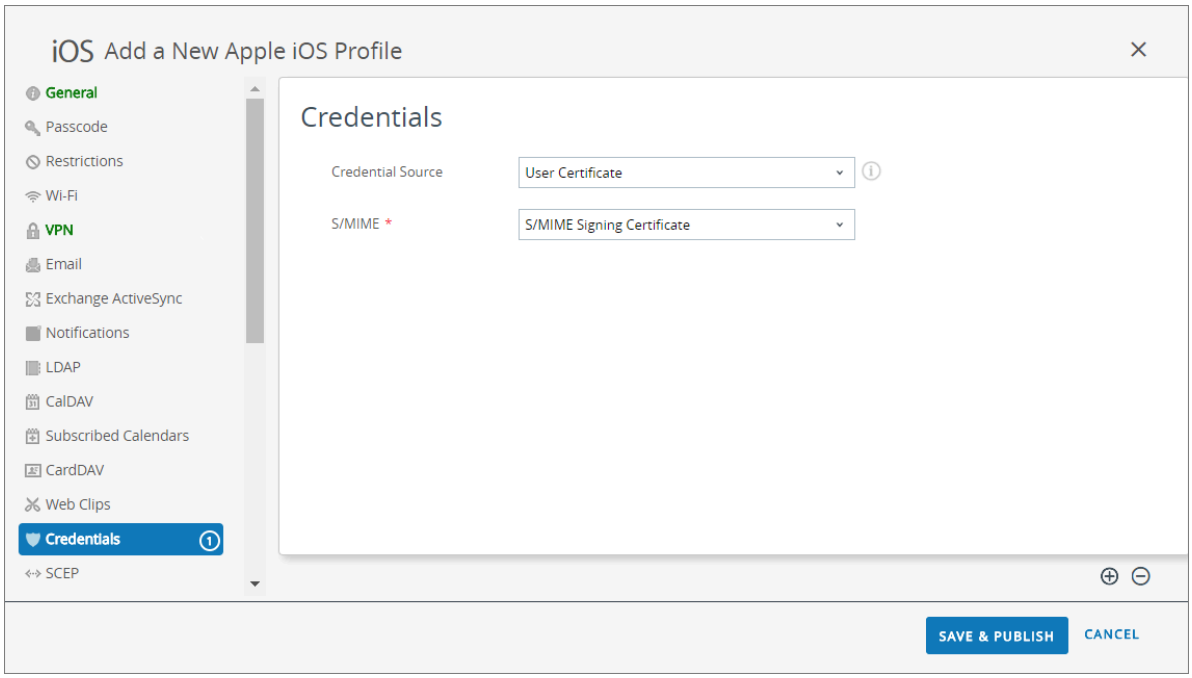


STEP 4 | **Credentials (認証情報)**の設定を行います：

iOS エンドポイント用のリモート アクセス *VPN* 設定では必ず証明書ベースの認証が求められます。

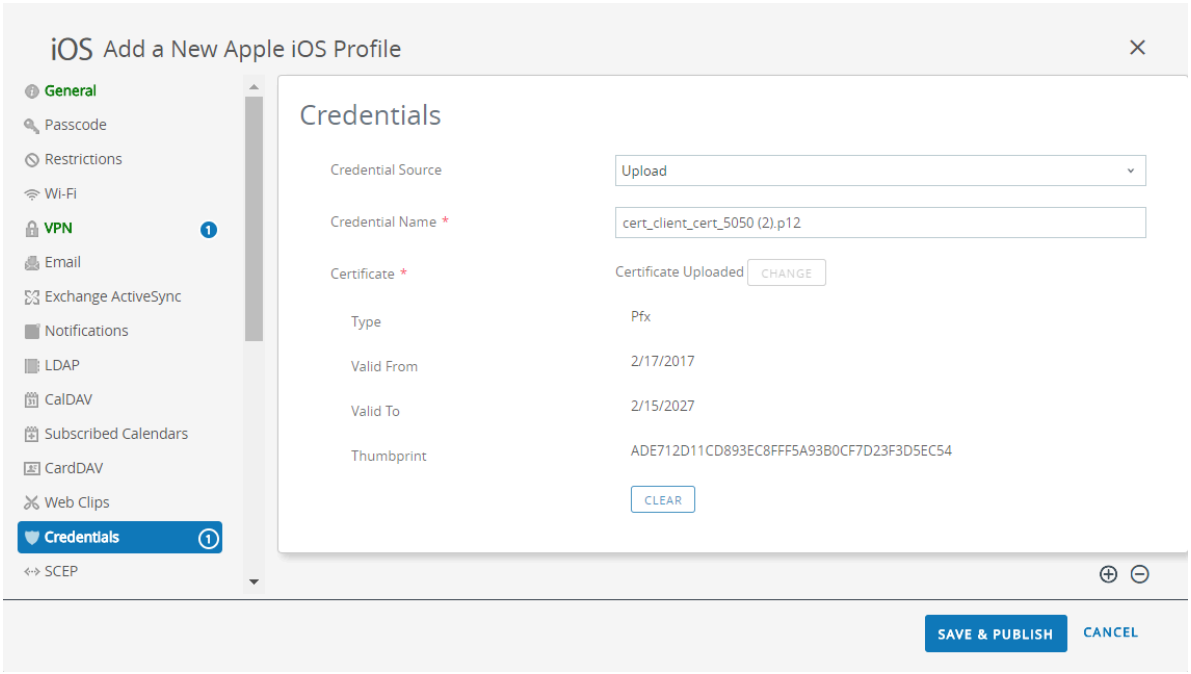
iOS 12 から、*GlobalProtect* クライアント認証用にクライアント証明書を使用する場合、*MDM* サーバーからプッシュされる *VPN* プロファイルの一部としてクライアント証明書をデプロイしなければならなくなります。その他の方式を使って *MDM* サーバーからクライアント証明書をデプロイする場合、*GlobalProtect* アプリケーションで証明書を使用することはできません。

- AirWatch ユーザーからクライアント証明書を取得する方法：
  1. **Credential Source (認証情報ソース)**を**User Certificate (ユーザー証明書)**に設定します。
  2. **S/MIME Signing Certificate (S/MIME 署名証明書)**（デフォルト）を選択します。

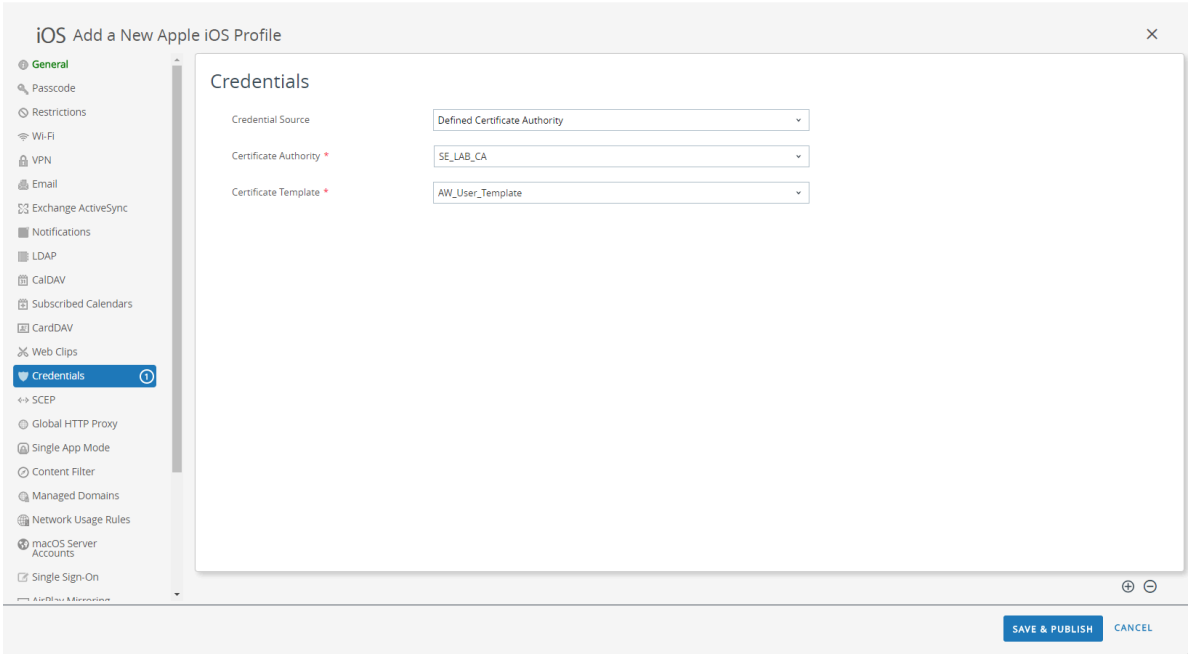


- 手動でクライアント証明書をアップロードする方法：
  1. **Credential Source (認証情報ソース)**を **(アップロード)**に設定します。
  2. **Credential Name (認証情報名)**を入力します。

3. **UPLOAD** (アップロード)をクリックし、アップロードする証明書を参照して選択します。
4. 証明書を選択したら**SAVE** (保存)をクリックします。



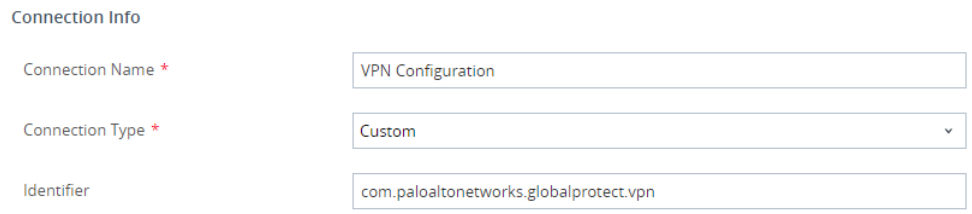
- 事前定義済みの認証局およびテンプレートを使用する方法：
  1. **Credential Source** (認証情報ソース)を**Defined Certificate Authority** (定義済みの認証局)に設定します。
  2. 証明書の取得元にする**Certificate Authority** (認証局)を選択します。
  3. その認証局で使用する**Certificate Template** (証明書テンプレート)を選択します。



STEP 5 | **VPN** の設定を行います。

1. エンドポイントが表示する**Connection Name (**接続名**)**を入力します。
2. ネットワーク**Connection Type (**接続タイプ**)**を選択します：
   - GlobalProtect アプリケーション 4.1.x 以前のリリースの場合、**Palo Alto Networks GlobalProtect**を選択します。
   - GlobalProtect アプリケーション 5.0 以降の場合は**Custom (**カスタム**)**を選択します。
3. （任意）**Connection Type (**接続タイプ**)**を**Custom (**カスタム**)**にセットする場合、GlobalProtect アプリケーションを識別する次のバンドル ID を**Identifier (**識別子**)**フィールドに入力します：

   com.paloaltonetworks.globalprotect.vpn

4. ユーザーが接続する GlobalProtect ポータルのホスト名または IP アドレスを**Server (**サーバー**)**フィールドに入力します。
5. （任意）VPN **Account (**アカウント**)**のユーザー名を入力するか、追加（**+**）ボタンをクリックして、サポートされている挿入可能なルックアップ値を見ます。
6. （任意）**Disconnect on idle (**アイドリング時に接続解除**)**フィールドで、アプリケーションがトラフィックを VPN トンネル経由でルーティングするのを停止した後、エンドポイントが GlobalProtect アプリケーションからログアウトするまでの時間（秒）を指定します。
7. Authentication (認証) 領域でユーザーの**Authentication (**認証**)**方式を**Certificate (**証明書**)**に設定します。

   iOS エンドポイント用のリモート アクセス *VPN* 設定では必ず証明書ベースの認証が求められます。

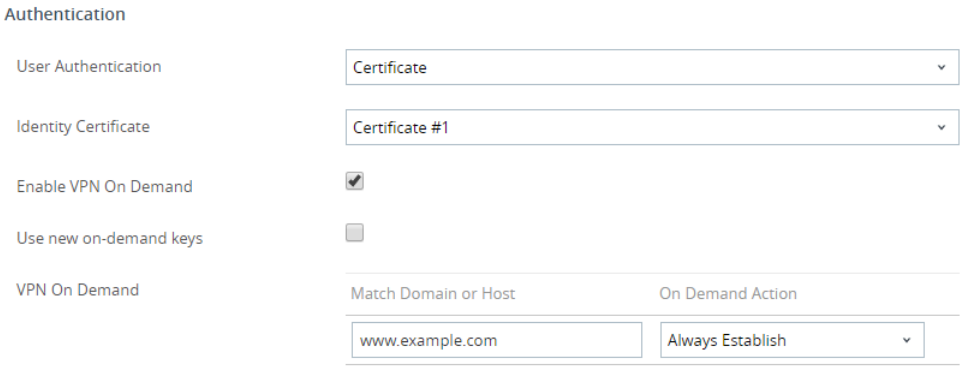
8. 指示されたら、GlobalProtect でユーザー認証に使用する**Identity Certificate** （アイデンティティ証明書）を選択します。**Identity Certificate (**アイデンティティ証明書**)**は、**Credentials (**認証情報**)**で設定した証明書と同じものです。
9. **Enable VPN On Demand (**オンデマンド **VPN** の有効化**)**オプションが有効（デフォルト設定）であることを確認します。

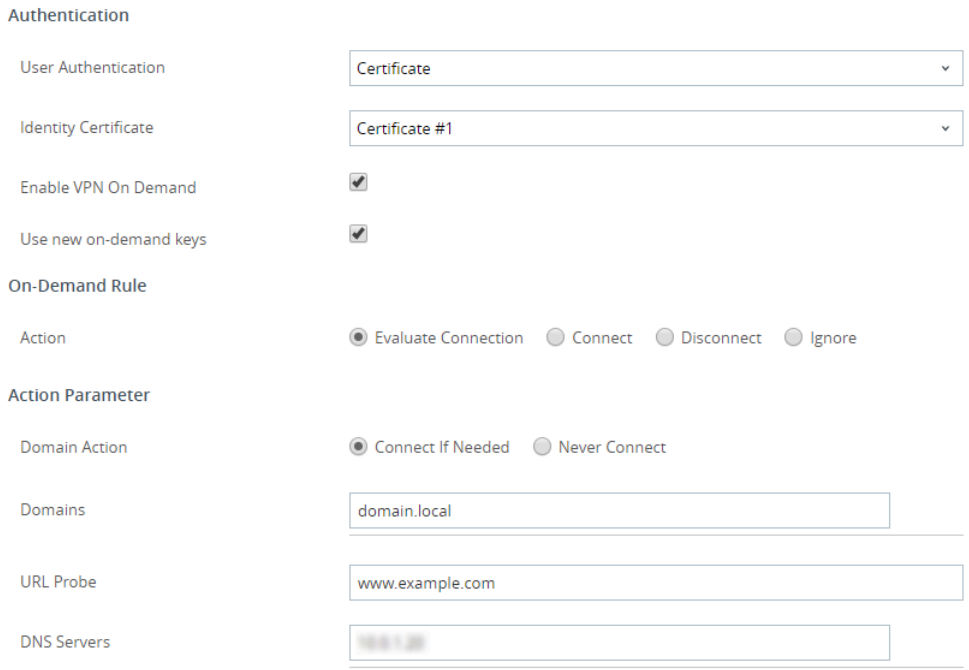
10. （任意）レガシー**VPN On-Demand (**オンデマンド **VPN)**接続ルールを設定します：

- **Match Domain or Host (**ドメインまたはホストにマッチ**)**—ユーザーのアクセス時に確立される GlobalProtect 接続を開始するドメインまたはホスト名を入力します。
- **On Demand Action (**オンデマンド アクション**)**—**On Demand Action (**オンデマンド アクション**)**を**Establish if Needed (**必要な場合に確立**)**あるいは**Always Establish (**必ず確立**)**に設定し、ユーザーが指定されたドメインやホスト名に直接到達できない場合にのみ、GlobalProtect 接続を確立します。**On Demand Action (**オンデマンド アクション**)**を**Never Establish (**確立しない**)**に設定し、ユーザーが指定されたドメインやホスト名

にアクセスする際に GlobalProtect 接続を確立しないようにします。接続がすでに確立されている場合は、継続して使用できます。

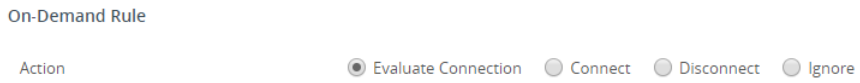


11. （任意）GlobalProtect アプリケーションが**Use new on-demand keys (**新しいオンデマンドキーを使用**)**できるようにして、より詳細なオンデマンド接続ルールを設定します。**ADD RULE (**ルールの追加**)**をクリックすれば複数のルールを追加できます。



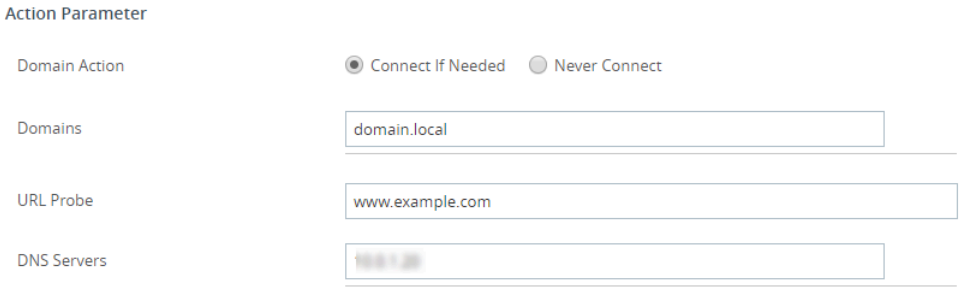
- On-Demand Rule (オンデマンド ルール) 領域で、Criteria (条件)の定義に基づいて GlobalProtect 接続に割り当てる**Action (**アクション**)**を選択します：
  - **Evaluate Connection (**接続を評価**)**—ネットワークおよび接続設定に基づいて自動的に GlobalProtect 接続を確立します。この評価は、ユーザーがドメインに接続しようと試みる度に行われます。
  - **Connect (**接続**)**—GlobalProtect 接続を自動的に確立します。
  - **Disconnect (**接続解除**)**—自動的に GlobalProtectを無効化し、GlobalProtect が再接続できないようにします。

- **Ignore (無視)**—既存の GlobalProtect 接続をそのまま維持し、接続が解除された際に GlobalProtect が再接続できないようにします。



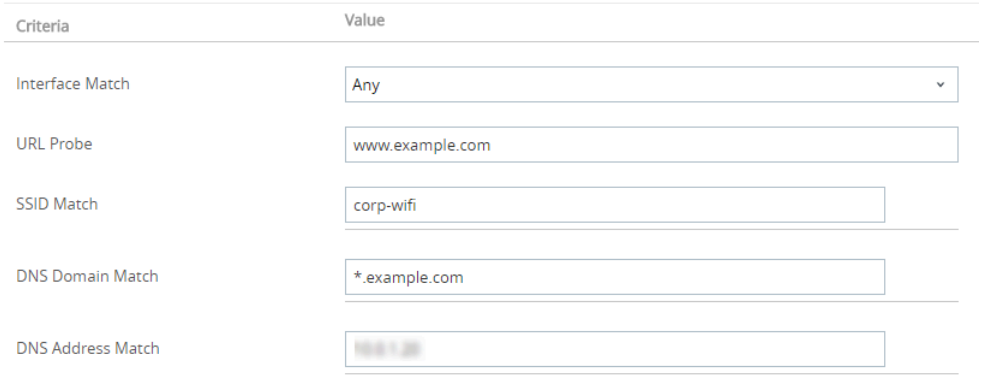
- （任意）オンデマンド接続用の**Action (アクション)**を**Evaluate Connection (接続を評価)**に設定する場合、接続を評価する際にドメイン名の解決が失敗した場合（例えば、タイムアウトが原因となって DNS サーバーが応答できない場合）に、GlobalProtect が再接続を試行できるかどうかを指定するために、Action Parameter (アクション パラメーター) も設定する必要があります。**ADD ACTION PARAMETERS (アクション パラメーターの追加)**をクリックすれば複数のパラメーターを追加できます。
  - **Domain Action (ドメイン アクション)**を**Connect if Needed (必要な場合に接続)**に設定して GlobalProtect が再接続できるようにするか、**Never Connect (接続しない)**に設定して GlobalProtect が再接続できないようにします。
  - この**Action Parameter (アクション パラメーター)**を割り当てる**Domains (ドメイン)**を入力します。
  - （任意）**Domain Action (ドメイン アクション)**を**Connect if Needed (必要な場合に接続)**に設定する場合、プローブを行う HTTP あるいは HTTPS の URL を**URL Probe (URL プローブ)**フィールドに入力します。URL のホスト名を解決できない、サーバーに到達できない、あるいはサーバーが 200 の HTTP ステータスコードを返さない場合、GlobalProtect が接続を確立します。
  - （任意）**Domain Action (ドメイン アクション)**を**Connect if Needed (必要な場合に接続)**に設定する場合、特定の**Domains (ドメイン)**を解決するために使用する**DNS**

Servers (DNS サーバー**)**（内部あるいは信頼できる外部）の IP アドレスを入力します。DNS サーバーに接続できない場合、GlobalProtect 接続が確立されます。



- オンデマンド接続ルールにマッチさせる次の条件を設定します。指定された条件すべてにエンドポイントがマッチする場合、そのエンドポイントにオンデマンド接続ルールが適用されます。
  - **Interface Match (**インターフェイス マッチ**)**—エンドポイントのネットワークアダプタにマッチさせる接続タイプを指定します：**Any (**すべて**)**、**Ethernet (**イーサネット**)**、**Wi-Fi**、**Cellular (**携帯**)**。
  - **URL Probe (URL** プローブ**)**—マッチさせる HTTP あるいは HTTPS の URL を入力します。マッチした場合は 200 の HTTP ステータスコードが返されます。
  - **SSID Match (SSID** マッチ**)**—マッチさせるネットワーク SSID を入力します。追加（**+**）ボタンをクリックすれば複数のネットワーク SSID を追加できます。指定されたネットワーク SSID にエンドポイントが一つ以上一致しなければ、マッチしたとみなされません。
  - **DNS Domain Match (DNS** ドメイン マッチ**)**—マッチさせる DNS 検索ドメインを入力します。また、ワイルドカードのレコード（**`*.example.com`**など）を使ってすべてのサブドメインにマッチさせることもできます。
  - **DNS Address Match (DNS** アドレス マッチ**)**—マッチさせる DNS サーバーの IP アドレスを入力します。追加（**+**）ボタンをクリックすれば複数の DNS サーバーの IP アドレスを追加できます。また、単一のワイルドカードのレコード（**`17.*`**など）を使用し、IP アドレスを持たないすべての DNS サーバーにマッチさせることもできます。エンドポイントでリストアップされているすべての DNS サーバーの IP アドレ

スが、指定された DNS サーバーの IP アドレスに一致しなければ、マッチしたとみなされません。

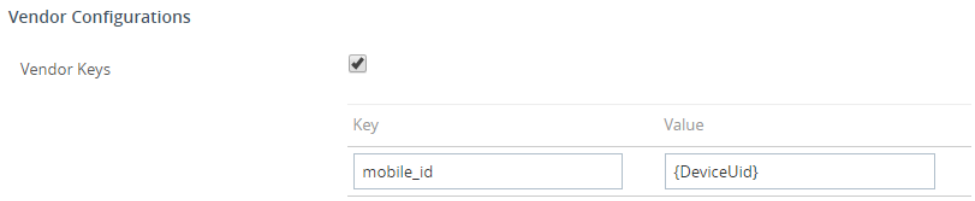


12. （任意）**Proxy (プロキシ)**タイプを選択し、関連する設定を行います。

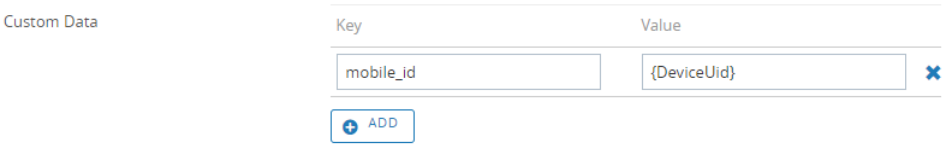
STEP 6 | （任意）（GlobalProtect アプリケーション 5.0 から）GlobalProtect のデプロイ環境で MDM と HIP の統合が必要な場合、一意のデバイス識別子（UDID）属性を指定します。

HIP ベースのポリシーを施行するのに使用するモバイル デバイス属性を MDM サーバーから取得するために、GlobalProtect に MDM を統合できるようになっています。GlobalProtect アプリケーションがエンドポイントの UDID を GlobalProtect ゲートウェイに提示しなければ、MDM の統合が機能しません。UDID 属性により、GlobalProtect アプリケーションが MDM ベースのデプロイ環境で UDID 情報を取得・使用できるようになります。プロファイルから UDID 属性を削除すると、MDM の統合を利用できなくなります。GlobalProtect アプリケーションは新しい UDID を生成しますが、それを統合のために使用することはできません。

- **Palo Alto Networks GlobalProtect**ネットワーク**Connection Type (**接続タイプ**)**を使用している場合、**VPN**設定に移動して Vendor Configuration (ベンダー設定) 領域で **Vendor Keys (**ベンダーキー**)**を有効化してください。**Key (**キー**)**を**`mobile_id`**に、**Value (**値**)**を**`{DeviceUid}`**に設定します。



- **Custom (**カスタム**)**ネットワーク**Connection Type (**接続タイプ**)**を使用している場合、**VPN**設定に移動して Connection Info (接続情報) 領域で**Custom Data (**カスタム データ**)**を**ADD (**追加**)**してください。**Key (**キー**)**を**`mobile_id`**に、**Value (**値**)**を**`{DeviceUid}`**に設定します。



STEP 7 | 変更を**SAVE & PUBLISH (**保存して公開**)**します。

AirWatch を使用してユーザーが開始するリモート アクセス *VPN* を *Windows 10 UWP* エンドポイント用に設定

リモート アクセス（オンデマンド）による VPN の構成では、ユーザーが手動でアプリを起動して安全な GlobalProtect の接続を確立する必要があります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、ユーザーが接続を開始・確立した後にのみ、必ず VPN トンネル経由でルーティングされます。

> ***Windows*** エンドポイントについては ***AirWatch*** でまだ ***GlobalProtect*** が公式の接続プロバイダとしてリストされていないため、代わりとなる ***VPN*** プロバイダを選択し、***GlobalProtect*** アプリケーションの設定を編集して、以下の手順に従って設定を ***VPN*** プロファイルにインポートし直す必要があります。

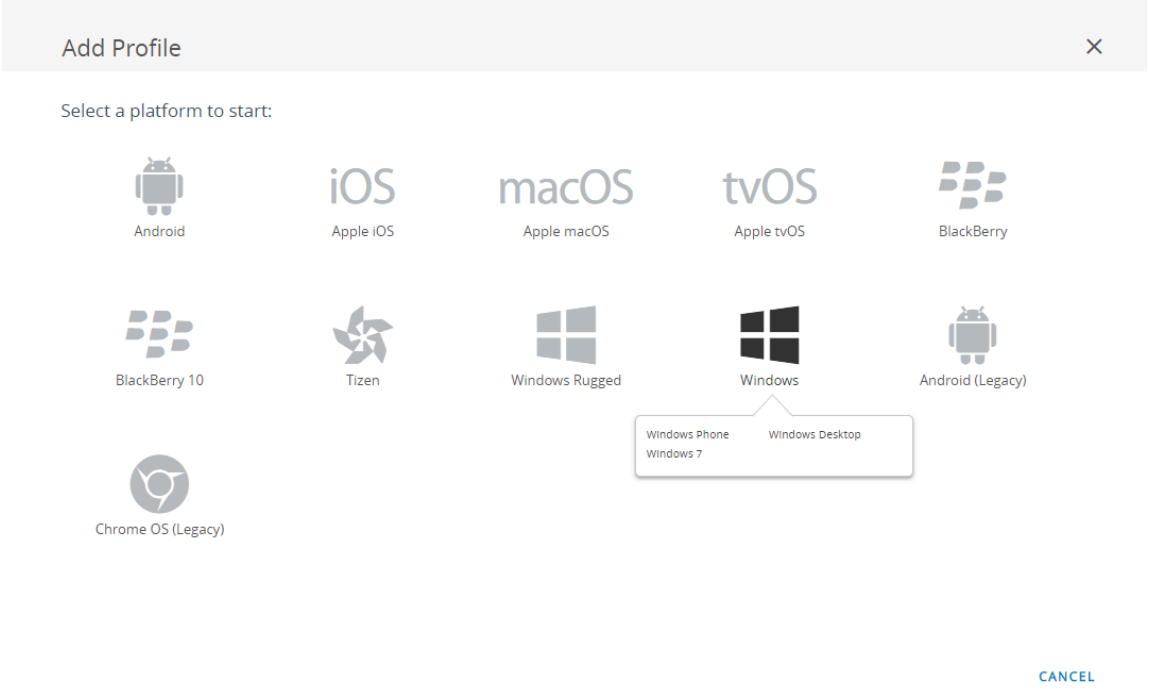
次の各作業により、AirWatch を使用して Windows 10 UWP エンドポイント用にユーザーが開始するリモート アクセス VPN 設定を構成することができます：

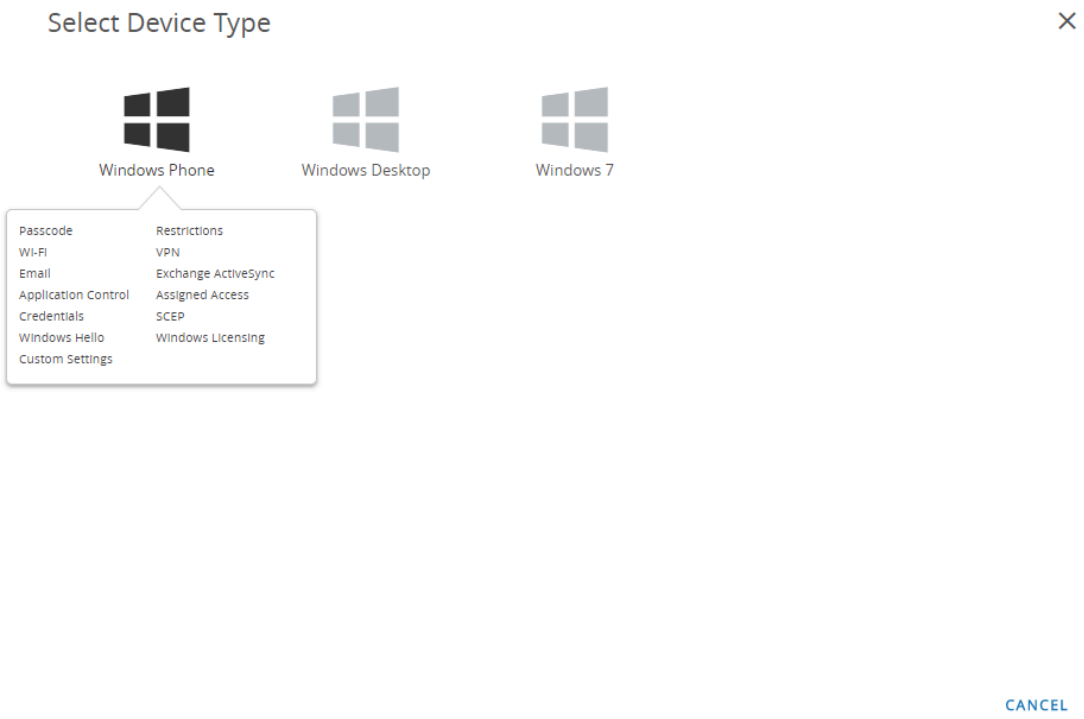
STEP 1 | Windows 10 UWP 用 の GlobalProtect アプリケーションをダウンロードします。

- AirWatch を使用して GlobalProtect モバイル アプリケーションをデプロイします。
- Microsoft ストアから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | AirWatch コンソールから、既存の Windows 10 UWP プロファイルを編集するか、新しいプロファイルを追加します。

1. **Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles (プロファイル)**を選択して新しいプロファイルを**ADD (追加)**します。
2. プラットフォームとして **Windows** を、デバイスタイプとして **Windows Phone**（**Windows** フォン）を選択します。





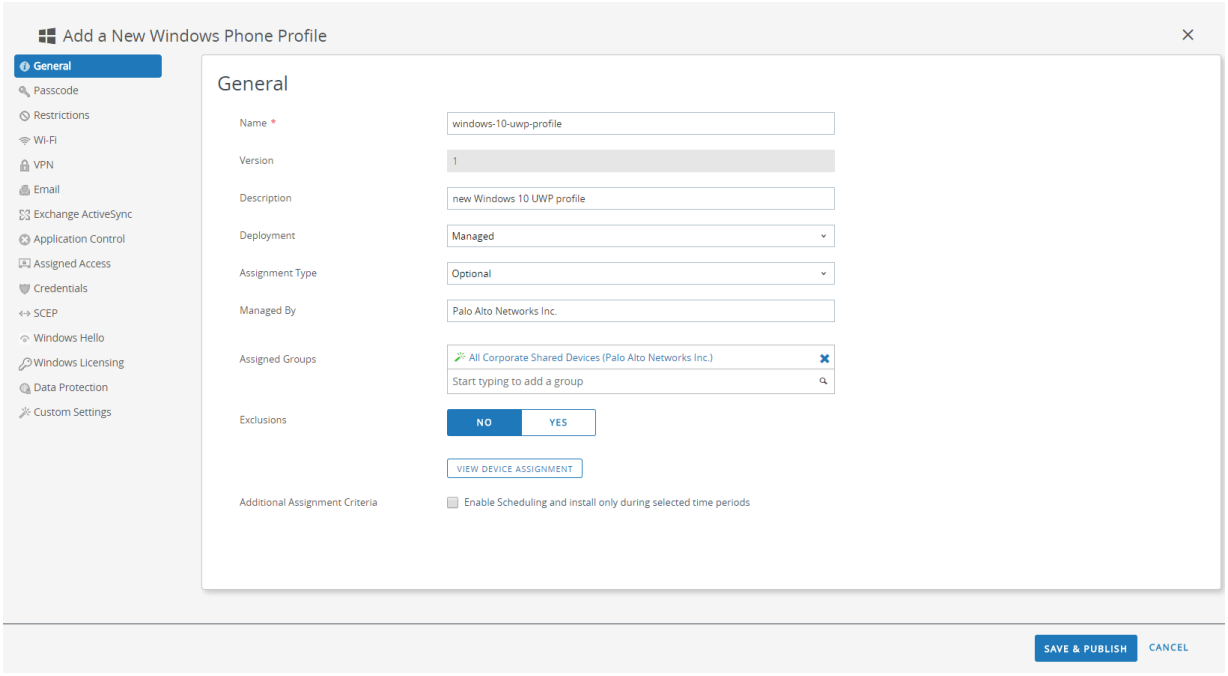
STEP 3 | **General (**一般**)**設定の設定を行います。

1. プロファイルの**Name**（名前）を入力します。
2. （任意）その目的を示すプロファイルの簡単な**Description (**説明**)**を入力します。
3. （任意）**Deployment (**デプロイ**)**方法を**Managed (**管理対象**)**に設定し、登録解除時にプロファイルを自動的に削除できるようにします
4. （任意）プロファイルをエンドポイントにデプロイする方法として、**Assignment Type (**割り当てタイプ**)**を選択します。プロファイルをすべてのエンドポイントに自動的にデプロイするには、**Auto**（自動）を選択します。エンド ユーザーがプロファイルをセルフサービス ポータル（SSP）からインストールしたり、プロファイルを個別のエンドポイントに手

動でデプロイできるようにするには、**Optional**（任意）を選択します。エンド ユーザーがエンドポイントに適用されるコンプライアンス ポリシーに違反した場合にプロファイルをデプロイするには、**Compliance**（コンプライアンス）を選択します。

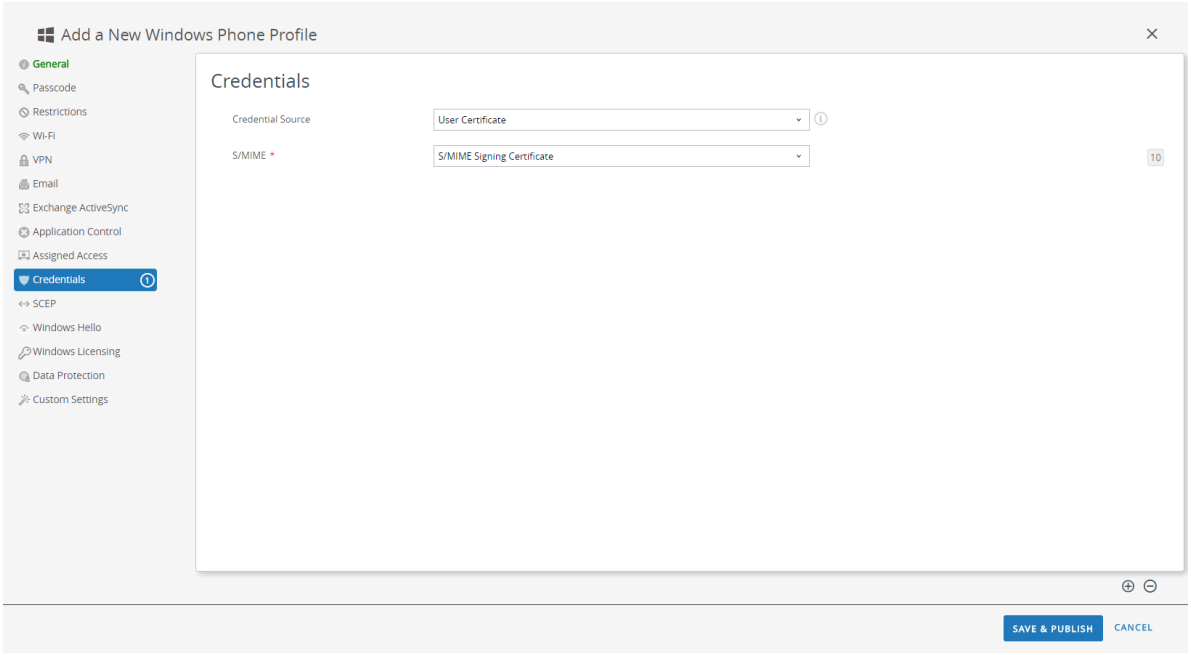
5. （任意）**Managed By (**管理者**)**フィールドに、プロファイルへの管理アクセスを持つ組織グループを入力します。
6. （任意）**Assigned Groups (**割り当てられたグループ**)**フィールドに、プロファイルの追加先となるスマート グループを追加します。このフィールドには、最低限の OS、デバイス モデル、所有者カテゴリ、組織グループなどの仕様で設定できる新規スマート グループを作成するオプションが含まれます。
7. （任意）このプロファイルの割り当てに**Exclusions (**除外**)**を含めるかどうか指定します。**Yes (**はい**)**を選択すると**Excluded Groups (**除外されたグループ**)**フィールドが表示され、プロファイルの割り当てから除外するスマート グループを選択できるようになります。
8. （任意）**Enable Scheduling and install only during selected time periods (**スケジュールを有効化し、選択した期間中にのみインストール**)**する場合、プロファイルのインストレーションにタイム スケジュール（**Devices (**デバイス**)** > **Profiles & Resources (**プロファイルおよびリソース**)** > **Profiles Settings (**プロファイル設定**)** > **Time Schedules (**タイム スケジュール**)**）を適用し、プロファイルをエンドポイントにインストールできる期間を制限すること

ができます。指示されたら、**Assigned Schedules (**割り当てられたスケジュール**)**フィールドにスケジュール名を入力します。



STEP 4 | （任意）GlobalProtect のデプロイメントでクライアント証明書認証が必要な場合、**Credentials (**認証情報**)**の設定を行います：

- AirWatch ユーザーからクライアント証明書を取得する方法：
  1. **Credential Source (**認証情報ソース**)**を**User Certificate (**ユーザー証明書**)**に設定します。
  2. **S/MIME Signing Certificate (S/MIME** 署名証明書**)**（デフォルト）を選択します。

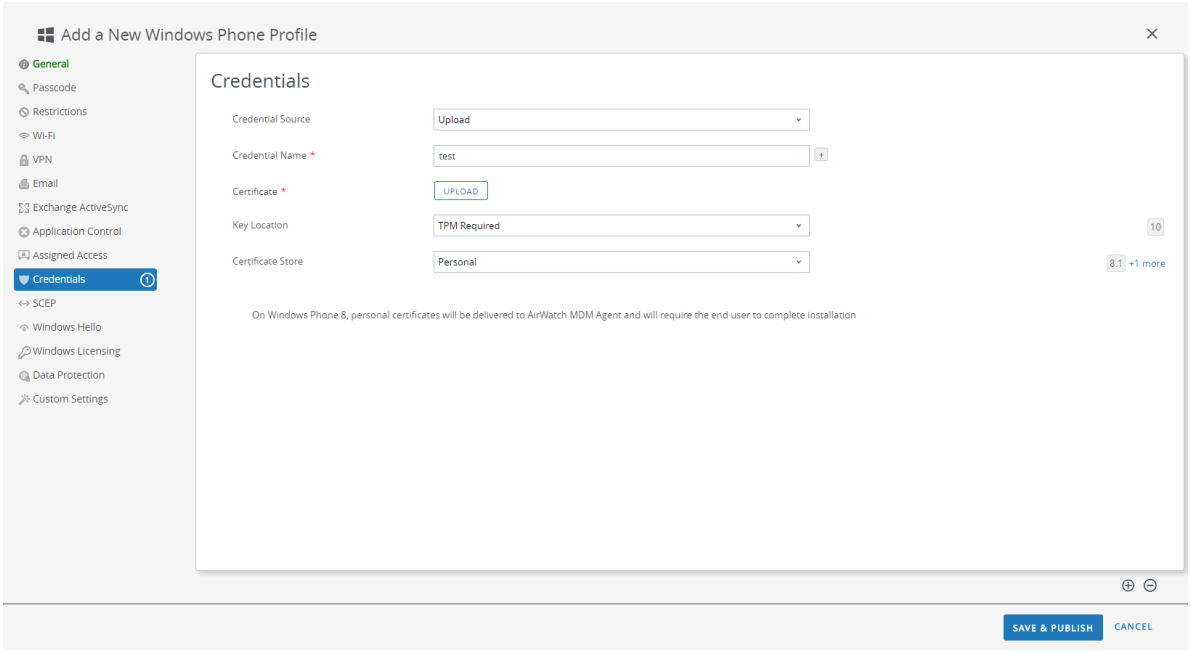


- 手動でクライアント証明書をアップロードする方法：
  1. **Credential Source (**認証情報ソース**)**を **(**アップロード**)**に設定します。
  2. **Credential Name (**認証情報名**)**を入力します。
  3. **UPLOAD (**アップロード**)**をクリックし、アップロードする証明書を参照して選択します。
  4. 証明書を選択したら**SAVE (**保存**)**をクリックします。
  5. 証明書の秘密鍵を保存する**Key Location (**キーの場所**)**を選択します：
     - **TPM Required (TPM** が必要**)**—Trusted Platform Module（信頼されたプラットフォーム モジュール）に秘密鍵を保存します。エンドポイントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵をインストールできません。
     - **TPM If Present (**存在する場合は **TPM)**—信頼されたプラットフォーム モジュールがエンドポイントに存在する場合、秘密鍵をそのモジュールに保存します。エンドポ

イントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵はエンドポイントのソフトウェアに保存されます。

- **Software (ソフトウェア)**—秘密鍵をエンドポイントのソフトウェアに保存します。
- **Passport (パスポート)**—秘密鍵を Microsoft Passport に保存します。このオプションを使用する場合、AirWatch 保護エージェントをエンドポイントにインストールしなければなりません。

6. **Certificate Store**（証明書ストア）を **Personal**（個人）に設定します。

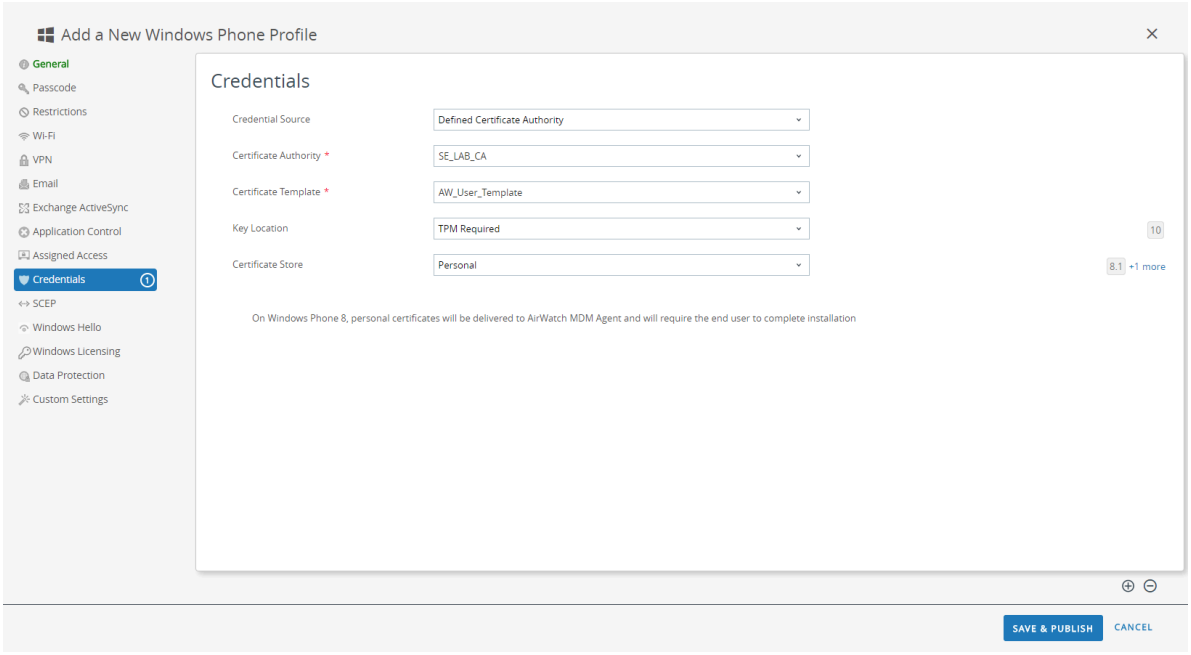


- 事前定義済みの認証局およびテンプレートを使用する方法：
  1. **Credential Source (**認証情報ソース**)**を**Defined Certificate Authority (**定義済みの認証局**)**に設定します。
  2. 証明書の取得元にする**Certificate Authority (**認証局**)**を選択します。
  3. その認証局で使用する**Certificate Template (**証明書テンプレート**)**を選択します。
  4. 証明書の秘密鍵を保存する**Key Location (**キーの場所**)**を選択します：
     - **TPM Required (TPM** が必要**)**—Trusted Platform Module（信頼されたプラットフォーム モジュール）に秘密鍵を保存します。エンドポイントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵をインストールできません。
     - **TPM If Present (**存在する場合は **TPM)**—信頼されたプラットフォーム モジュールがエンドポイントに存在する場合、秘密鍵をそのモジュールに保存します。エンドポ

イントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵はエンドポイントのソフトウェアに保存されます。

- **Software (ソフトウェア)**—秘密鍵をエンドポイントのソフトウェアに保存します。
- **Passport (パスポート)**—秘密鍵を Microsoft Passport に保存します。このオプションを使用する場合、AirWatch 保護エージェントをエンドポイントにインストールしなければなりません。

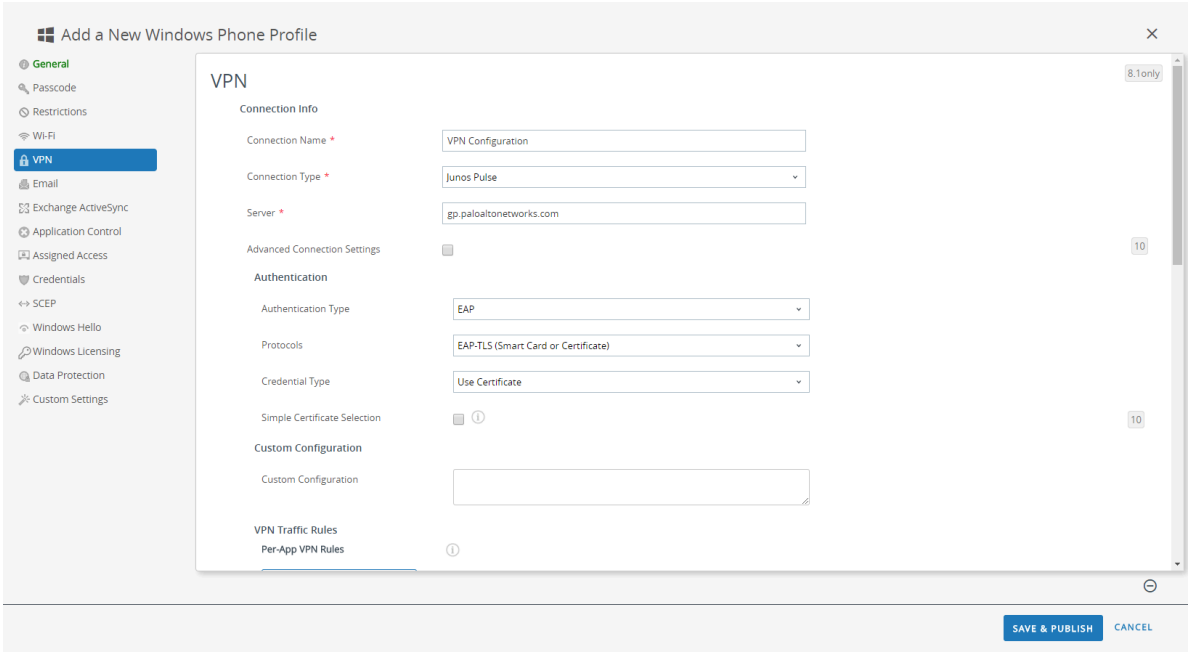
5. **Certificate Store**（証明書ストア）を **Personal**（個人）に設定します。



STEP 5 | **VPN** の設定を行います。

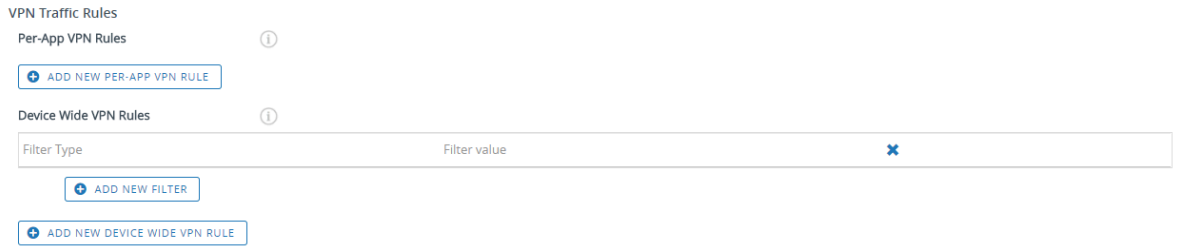
1. エンドポイントが表示する**Connection Name (**接続名**)**を入力します。
2. 別の**Connection Type (**接続タイプ**)**のプロバイダーを選択します（GlobalProtect VPN プロファイルに必要な関連するベンダー設定が含まれていないため、**IKEv2**、**L2TP**、**PPTP**、**Automatic**（自動）は選択しないでください）。

   Windows エンドポイントについては *AirWatch* がまだ *GlobalProtect* を公式の接続プロバイダとしてリストしていないため、代わりとなる *VPN* プロバイダを選択する必要があります。
3. ユーザーが接続する GlobalProtect ポータルのホスト名または IP アドレスを**Server (**サーバー**)**フィールドに入力します。
4. Authentication（認証）領域で**Authentication Type (**認証タイプ**)**を選択し、エンドユーザーを認証する方式を指定します。



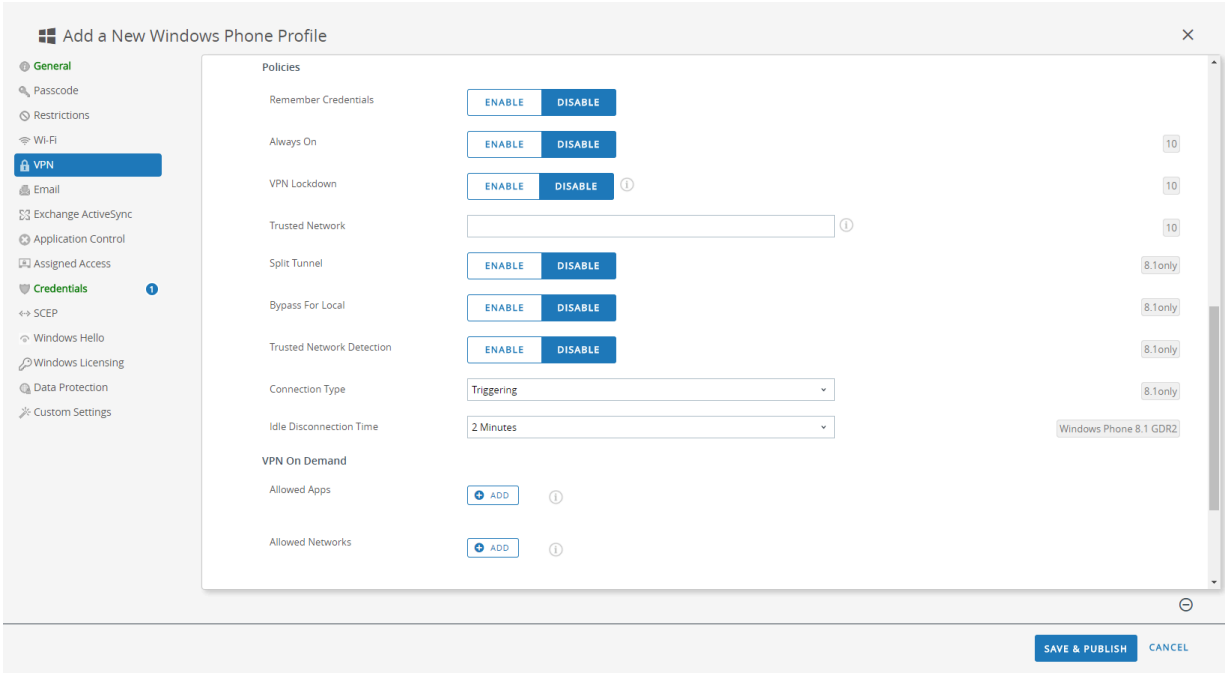
5. （任意）GlobalProtect がユーザーの認証情報を保存するのを許可するには、Policies（ポリシー）エリアにある **Remember Credentials**（認証情報の記憶）オプションを **ENABLE (**有効**)** にします。
6. （任意）VPN Traffic Rules (VPN トラフィック ルール) 領域で**ADD NEW DEVICE WIDE VPN RULE (**全デバイス対象の新しい **VPN** ルールを追加**)**して、特定のルートにマッチするトラフィックを VPN トンネル経由で送信します。このルールはアプリケーション単位に束縛されませんが、エンドポイント全体で評価されます。特定の一致条件にマッチするトラフィックは VPN トンネル経由でルーティングされます。

   ADD NEW FILTER (新規フィルターの追加**)**をクリックして一致条件を追加します。指示されたら、**FilterType (**フィルターのタイプ**)**および**Filter Value (**フィルターの値**)**を入力します。



7. このプロファイルに必ずオンデマンド接続方式を使用させるために、Policies (ポリシー) 領域で次の設定を行います：
   - **Always On (**常時オン**)**を**DISABLE (**無効化**)**します。このフィールドが**ENABLED (**有効**)**である場合、安全な接続が常にオンになります。
   - **VPN Lockdown (VPN** ロックダウン**)**を**DISABLE (**無効化**)**します。このフィールドが**ENABLED (**有効**)**である場合、安全な接続が常にオンで接続された状態になり、アプリが接続されていない時はネットワーク アクセスが無効化されます。AirWatch の **VPN Lockdown**（**VPN** ロックダウン）オプションは、GlobalProtect ポータル設定で指

定する **Enforce GlobalProtect for Network Access**（ネットワーク アクセスの際に必ず **GlobalProtect** を利用する）オプションと同じです。



STEP 6 | 変更を**SAVE & PUBLISH (**保存して公開**)**します。

STEP 7 | GlobalProtect を接続タイプのプロバイダーとして設定する場合、XML 内の VPN プロファイルを編集します。

XML で直接行う追加の編集を最小限にするために、*VPN* プロファイルの設定をエクスポートする前に設定をレビューします。*VPN* プロファイルをエクスポートした後で設定を変更する必要が生じた場合、*XML* に直接変更を加えるか、*VPN* プロファイルの設定を更新して再度このステップを実施することができます。

1. **Devices** > **Profiles**（プロファイル） > **List View**（リスト ビュー） で、前述のステップで追加した新しいプロファイルの隣にあるラジオ ボタンを選択し、次に表の上部にある **</>XML** を選択します。AirWatch でプロファイルの XML ビューが開きます。
2. プロファイルを **Export**（エクスポート）した後、任意のテキスト エディタで開きます。
3. GlobalProtect の以下の設定を編集します。

- `PluginPackageFamilyName` を指定する `LoclURI` エレメントで、エレメントを次のように変更します:

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

- 続く `Data` エレメントで、値を次のように変更します：

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. エクスポートしたプロファイルに加えた変更を保存します。
2. AirWatch に戻り、**Devices**（デバイス） > **Profiles**（プロファイル） > **List View**（リストビュー） を選択します。
3. 新しいプロファイルを作成（**Add** > **Add Profile** > **Windows** > **Windows Phone** (追加 > プロファイルの追加 > Windows > Windowsフォン)）して名前を付けます。
4. **Custom Settings** > **Configure** (カスタム設定 > 設定)を選択し、編集した設定をコピーアンドペーストします。
5. 変更を**Save & Publish** (保存して公開)します。

STEP 8 | **Devices**（デバイス） > **Profiles**（プロファイル） > **List View**（リスト ビュー）からオリジナルのプロファイルを選択することでオリジナルのプロファイルを消去して、**More Actions**（他の操作） > **Deactivate**（無効化）を選択します。AirWatch により、プロファイルが Inactive（無効）のリストに移動されます。

STEP 9 | 設定のテストを行います。

Microsoft Intune を使用してユーザーが開始するリモート アクセス VPN を設定

Microsoft Intune とは、中央から一元的にモバイル エンドポイントを管理できるようにする、クラウド ベースのエンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより、デバイス レベルあるいはアプリケーション レベルで、Microsoft

Intune が管理するモバイル エンドポイントおよびファイアウォール間で安全に接続を行えるようになります。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

Microsoft Intune を使ってユーザーが開始するリモート アクセス VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- Microsoft Intune を使用してユーザーが開始するリモート アクセス VPN を iOS エンドポイント用に設定

Microsoft Intune を使用してユーザーが開始するリモート アクセス *VPN* を *iOS* エンドポイント用に設定

リモート アクセス（オンデマンド）による VPN の構成では、ユーザーが手動でアプリを起動して安全な GlobalProtect の接続を確立する必要があります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、ユーザーが接続を開始・確立した後にのみ、必ず VPN トンネル経由でルーティングされます。

次の各作業により、Microsoft Intune を使用して iOS エンドポイント用にユーザーが開始するリモート アクセス VPN 設定を構成することができます：

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

- Microsoft Intune を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | （任意）証明書ベースの認証が必要なデプロイ環境の場合、証明書プロファイルの設定を行います。

STEP 3 | 新しい iOS VPN プロファイルを作成します。

- **Platform (プラットフォーム)**を**iOS**に設定します。

STEP 4 | iOS エンドポイント用にオンデマンド（リモート アクセス）の VPN 設定を行います。

- **Connection type (接続タイプ)**を**Palo Alto Networks GlobalProtect** に設定します。
- Automatic VPN settings (自動 VPN 設定)領域で**On-demand VPN (オンデマンド VPN)**を有効化し、VPN 接続を開始するタイミングを制御する条件ルールを設定します。

MobileIron を使用してユーザーが開始するリモート アクセス **VPN** を設定

MobileIron とは、中央のコンソールから一元的にモバイル エンドポイントを管理できるようにする、エンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより、デバイス レベルあるいはアプリケーション レベルで、MobileIron が管理するモバイル エンドポイントおよびファイアウォール間で安全に接続を行えるようになります。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

MobileIron を使ってユーザーが開始するリモート アクセス VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- MobileIron を使用してユーザーが開始するリモート アクセス VPN を iOS エンドポイント用に設定

MobileIron を使用してユーザーが開始するリモート アクセス *VPN* を *iOS* エンドポイント用に設定

リモート アクセス（オンデマンド）による VPN の構成では、ユーザーが手動でアプリを起動して安全な GlobalProtect の接続を確立する必要があります。GlobalProtect ゲートウェイで設定されている特定のフィルター（ポートや IP アドレスなど）にマッチするトラフィックは、ユーザーが接続を開始・確立した後にのみ、必ず VPN トンネル経由でルーティングされます。

次の各作業により、MobileIron を使用して iOS エンドポイント用にユーザーが開始するリモート アクセス VPN 設定を構成することができます：

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

- MobileIron を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | 証明書設定の追加を行ってから証明書設定を行います。

オンデマンドの *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。

STEP 3 | オンデマンド（リモート アクセス）の VPN 設定を追加します。

- 設定タイプを**VPN On Demand (**オンデマンド **VPN)**に設定します。

STEP 4 | iOS 用にオンデマンド VPN の設定を行います。

- **Connection Type (**接続タイプ**)**を**Palo Alto Networks GlobalProtect**に設定してから、関連する設定を行います。

アプリ単位の **VPN** 設定

アプリ単位の VPN 設定において、どの管理アプリケーションが GlobalProtect VPN トンネル経由でトラフィックを送信できるかを指定できます。管理していないアプリケーションは GlobalProtect VPN トンネルを解する代わりにインターネットに直接接続を続けようとします。

サポートされているモバイルデバイス管理システムを使ってアプリ単位の VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- AirWatchを使用したアプリ単位の VPN 設定
- Microsoft Intune を使用したアプリ単位の VPN 設定
- MobileIron を使用したアプリ単位の VPN 設定

AirWatchを使用したアプリ単位の **VPN** 設定

AirWatch とは、中央のコンソールから一元的にモバイル エンドポイントを管理できるようにする、エンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより AirWatch 管理モバイル エンドポイントとファイアウォール間の、デバイスまたはアプリケーションレベルでの保護された接続が実現します。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

AirWatch を使ってアプリ単位の VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- AirWatch を使用した iOS エンドポイントのアプリ単位の VPN 設定
- AirWatch を使用した Android エンドポイントのアプリ単位の VPN 設定
- AirWatch を使用した Windows 10 UWP エンドポイント用のアプリ単位の VPN 設定

AirWatch を使用した *iOS* エンドポイントのアプリ単位の *VPN* 設定

AirWatch を使用して GlobalProtect VPN アクセスを設定することで管理下のモバイル エンドポイントから内部リソースにアクセスできるようになります。アプリ単位の VPN 設定において、どの管理アプリケーションが VPN トンネル経由でトラフィックをルーティングできるかを指定できます。管理していないアプリケーションは VPN トンネルを解する代わりにインターネットに直接接続を続けようとします。

次の各作業により、AirWatch を使用して iOS エンドポイント用にアプリ単位の VPN 設定を構成することができます：

STEP 1 | iOS 用 GlobalProtect アプリをダウンロードします。

- AirWatch を使用して GlobalProtect モバイル アプリケーションをデプロイします。
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

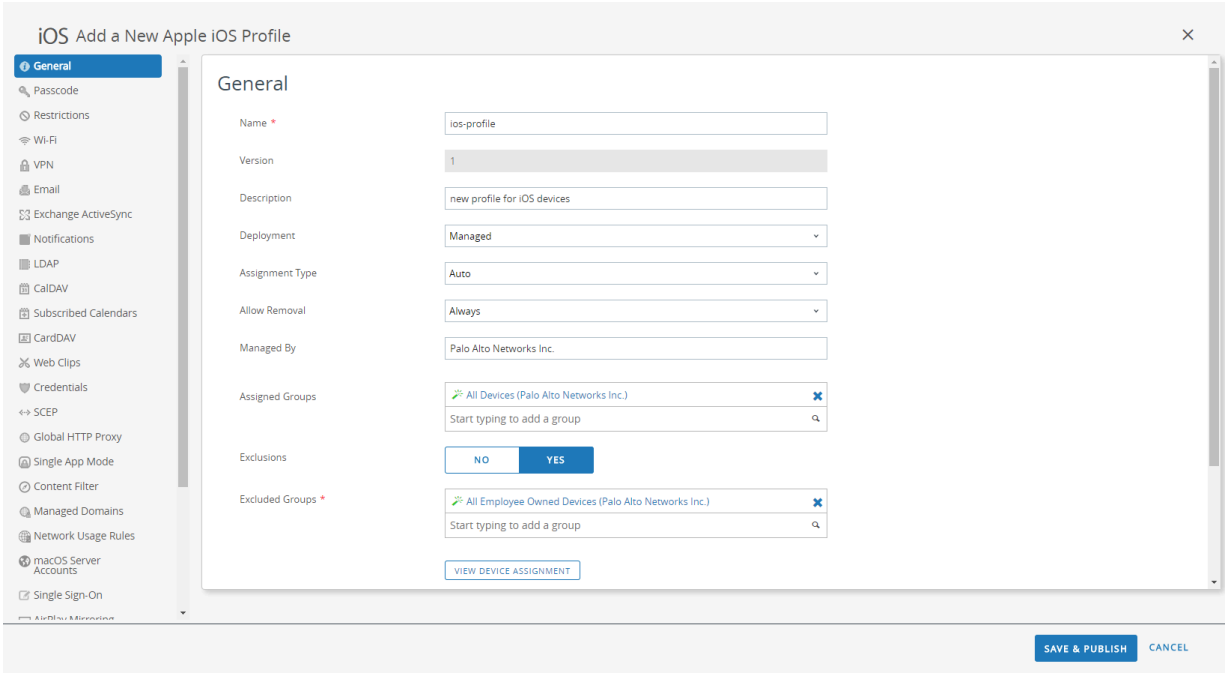
STEP 2 | AirWatch コンソールから、既存の Apple iOS プロファイルを編集するか、新しいプロファイルを追加します。

1. **Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles (プロファイル)**を選択して新しいプロファイルを**ADD (追加)**します。
2. プラットフォームのリストで**iOS**を選択します。

STEP 3 | **General (一般)設定の設定を行います。**

1. プロファイルの**Name**（名前）を入力します。
2. （任意）その目的を示すプロファイルの簡単な**Description (説明)**を入力します。
3. （任意）登録解除時にプロファイルを自動的に削除するかどうかを指定する**Deployment (デプロイメント)**方式として、**Managed**（管理対象）（プロファイルは削除されます）あるいは**Manual**（手動）（プロファイルはエンドユーザーが削除するまでインストールされたままになります）のいずれかを選択します。
4. （任意）プロファイルをエンドポイントにデプロイする方法として、**Assignment Type (割り当てタイプ)**を選択します。プロファイルをすべてのエンドポイントに自動的にデプロイするには、**Auto**（自動）を選択します。エンド ユーザーがプロファイルをセルフサービス ポータル（SSP）からインストールしたり、プロファイルを個別のエンドポイントに手動でデプロイできるようにするには、**Optional**（任意）を選択します。エンド ユーザーがエンドポイントに適用されるコンプライアンス ポリシーに違反した場合にプロファイルをデプロイするには、**Compliance**（コンプライアンス）を選択します。
5. （任意）エンドユーザーに対してプロファイルの**Allow Removal (削除を許可)**するかどうかを選択します。エンド ユーザーがいつでもプロファイルを手動で削除できるようにするには、**Always**（常に許可）を選択します。エンド ユーザーがプロファイルを削除できないようにするには、**Never**（拒否）を選択します。エンド ユーザーがプロファイルを削除するのに管理者の許可が必要になるようにするには、**With Authorization**（認証あり）を選択します。**With Authorization**（認証あり）を選択すると、必要なパスワードが追加されます。
6. （任意）**Managed By (管理者)**フィールドに、プロファイルへの管理アクセスを持つ組織グループを入力します。
7. （任意）**Assigned Groups (割り当てられたグループ)**フィールドに、プロファイルの追加先となるスマート グループを追加します。このフィールドには、最低限の OS、デバイス モデル、所有者カテゴリ、組織グループなどの仕様で設定できる新規スマート グループを作成するオプションが含まれます。
8. （任意）このプロファイルの割り当てに**Exclusions (除外)**を含めるかどうか指定します。**Yes (はい)**を選択すると**Excluded Groups (除外されたグループ)**フィールドが表示さ

れ、プロファイルの割り当てから除外するスマート グループを選択できるようになります。

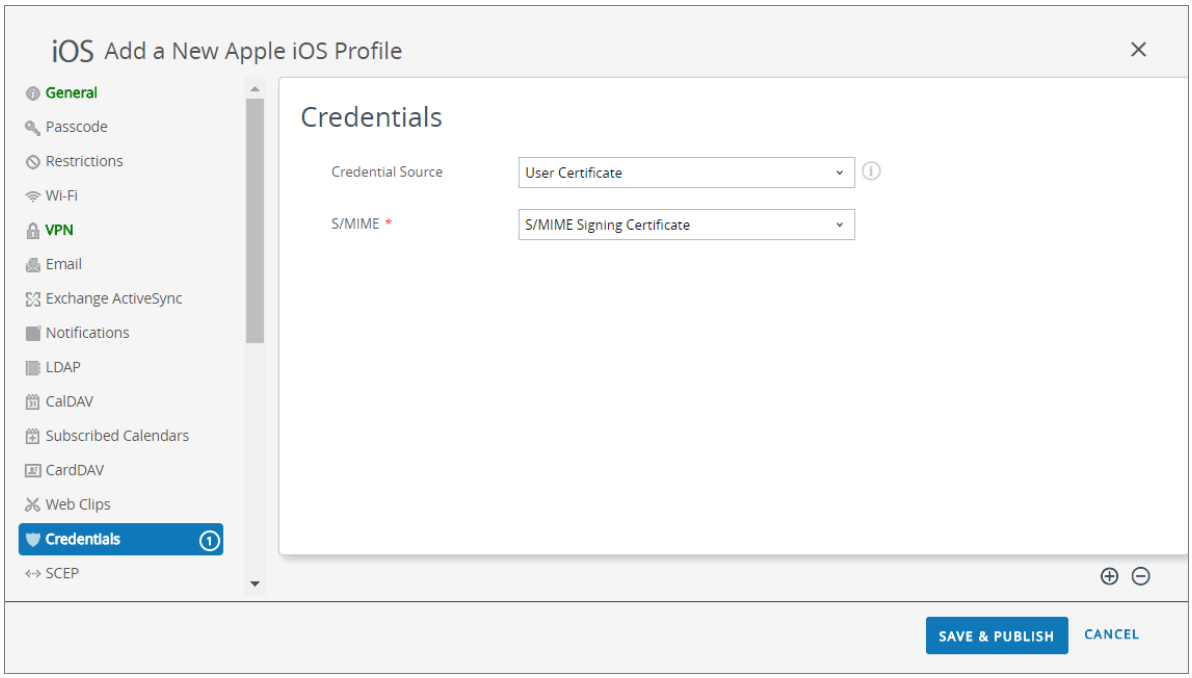


STEP 4 | **Credentials (認証情報)**の設定を行います：

アプリ単位の *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。

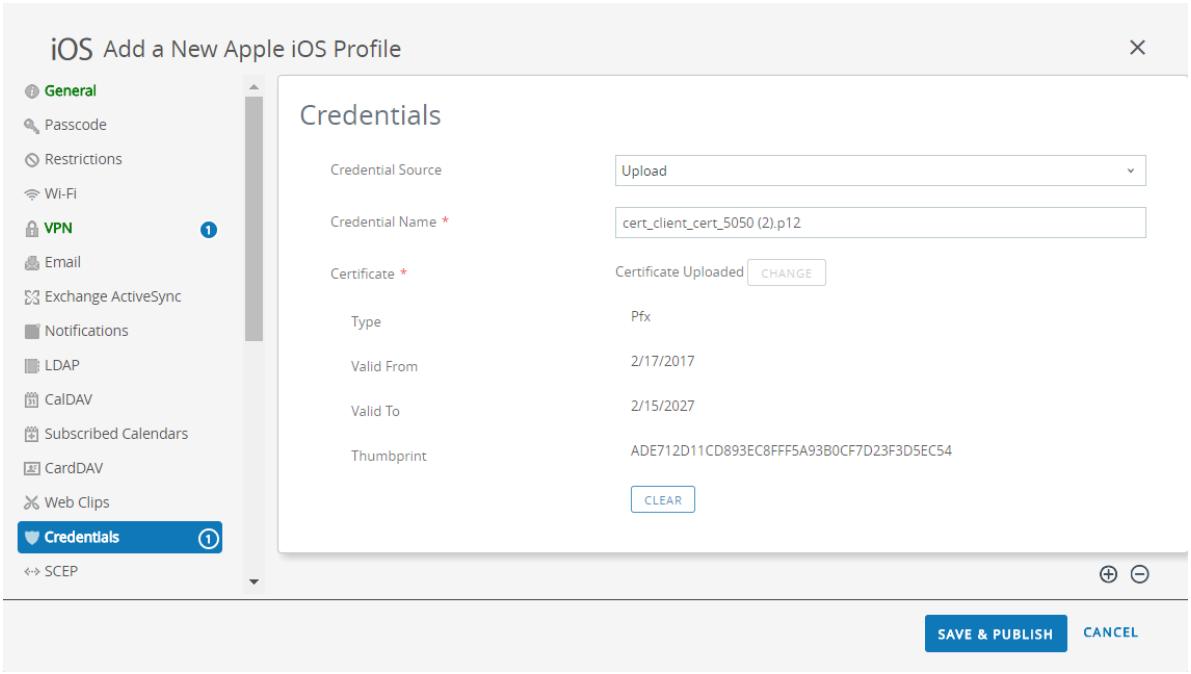
iOS 12 から、*GlobalProtect* クライアント認証用にクライアント証明書を使用する場合、*MDM* サーバーからプッシュされる *VPN* プロファイルの一部としてクライアント証明書をデプロイしなければならなくなります。その他の方式を使って *MDM* サーバーからクライアント証明書をデプロイする場合、*GlobalProtect* アプリケーションで証明書を使用することはできません。

- AirWatch ユーザーからクライアント証明書を取得する方法：
  1. **Credential Source (認証情報ソース)**を**User Certificate (ユーザー証明書)**に設定します。
  2. **S/MIME Signing Certificate (S/MIME 署名証明書)**（デフォルト）を選択します。

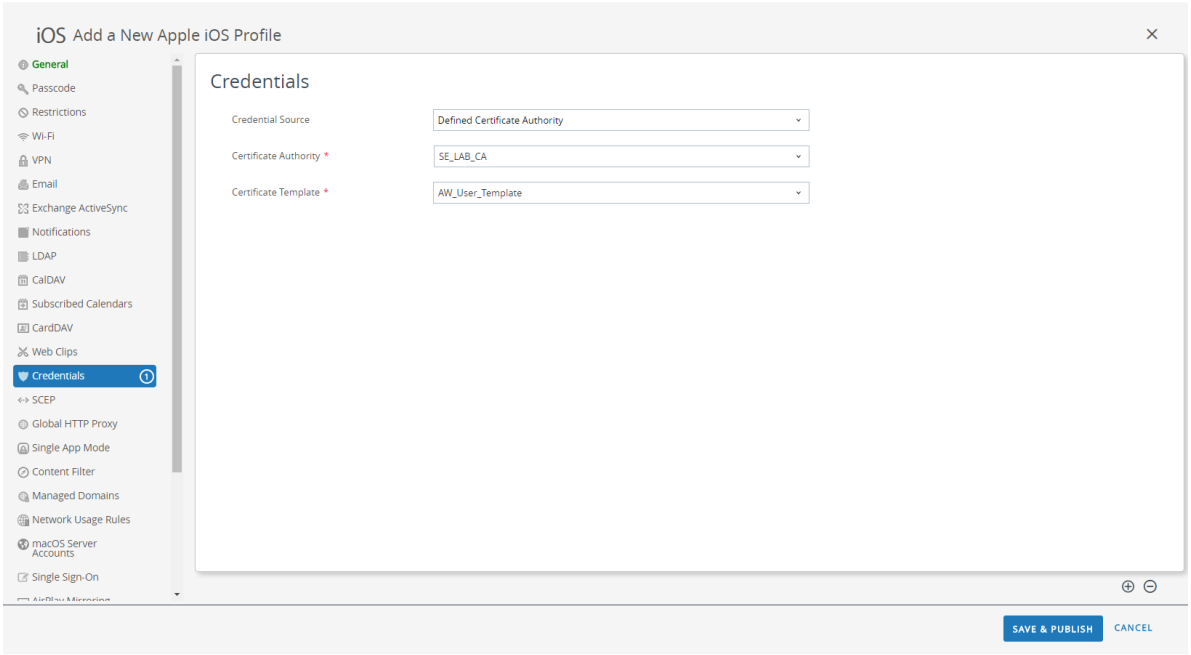


- 手動でクライアント証明書をアップロードする方法：
  1. **Credential Source (認証情報ソース)**を **(アップロード)**に設定します。
  2. **Credential Name (認証情報名)**を入力します。

3. **UPLOAD** (アップロード)をクリックし、アップロードする証明書を参照して選択します。
4. 証明書を選択したら**SAVE** (保存)をクリックします。



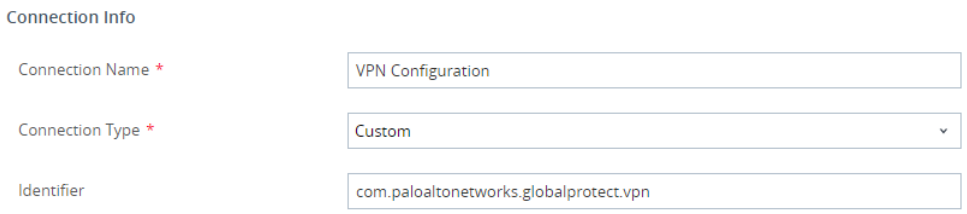
- 事前定義済みの認証局およびテンプレートを使用する方法：
  1. **Credential Source** (認証情報ソース)を**Defined Certificate Authority** (定義済みの認証局)に設定します。
  2. 証明書の取得元にする**Certificate Authority** (認証局)を選択します。
  3. その認証局で使用する**Certificate Template** (証明書テンプレート)を選択します。



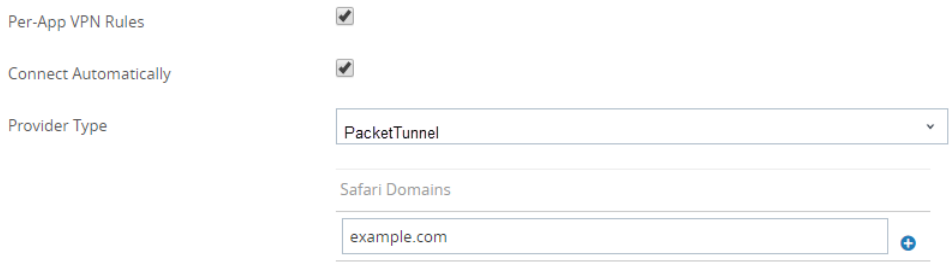
STEP 5 | **VPN** の設定を行います。

1. エンドポイントが表示する**Connection Name (**接続名**)**を入力します。
2. ネットワーク**Connection Type (**接続タイプ**)**を選択します：
   - GlobalProtect アプリケーション 4.1.x 以前のリリースの場合、**Palo Alto Networks GlobalProtect**を選択します。
   - GlobalProtect アプリケーション 5.0 以降の場合は**Custom (**カスタム**)**を選択します。
3. （任意）**Connection Type (**接続タイプ**)**を**Custom (**カスタム**)**にセットする場合、GlobalProtect アプリケーションを識別する次のバンドル ID を**Identifier (**識別子**)**フィールドに入力します：

   com.paloaltonetworks.globalprotect.vpn

4. ユーザーが接続する GlobalProtect ポータルのホスト名または IP アドレスを**Server (**サーバー**)**フィールドに入力します。
5. （任意）VPN **Account (**アカウント**)**のユーザー名を入力するか、追加（**+**）ボタンをクリックして、サポートされている挿入可能なルックアップ値を見ます。
6. （任意）**Disconnect on idle (**アイドリング時に接続解除**)**フィールドで、アプリケーションがトラフィックを VPN トンネル経由でルーティングするのを停止した後、エンドポイントが GlobalProtect アプリケーションからログアウトするまでの時間（秒）を指定します。
7. **Per App VPN Rules** （アプリ単位の **VPN** ルール）を有効化して、管理対象のアプリケーションのトラフィックをすべて GlobalProtect VPN トンネル経由でルーティングします。
   - GlobalProtect が特定の**Safari Domains (Safari** ドメイン**)**に**Connect Automatically (**自動接続**)**できるようにします。追加（**+**）ボタンをクリックすれば複数の**Safari Domains (Safari** ドメイン**)**を追加できます。
   - **Provider Type (**プロバイダータイプ**)**を選択し、トラフィックをトンネリングする方法（アプリケーション層あるいは IP 層のどちらで行うか）を指定します。

8. Authentication (認証) 領域でユーザーの**Authentication (**認証**)**方式を**Certificate (**証明書**)**に設定します。

アプリ単位の *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。

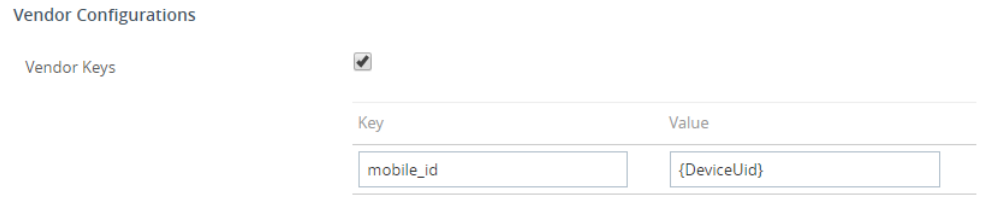
9. 指示されたら、GlobalProtect でユーザー認証に使用する**Identity Certificate** （アイデンティティ証明書）を選択します。**Identity Certificate (**アイデンティティ証明書**)**は、**Credentials (**認証情報**)**で設定した証明書と同じものです。

10. （任意）**Proxy (**プロキシ**)**タイプを選択し、関連する設定を行います。

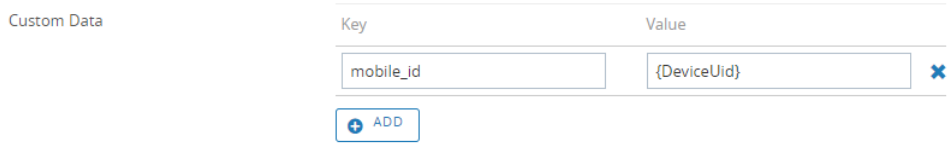
STEP 6 | （任意）（GlobalProtect アプリケーション 5.0 から）GlobalProtect のデプロイ環境で MDM と HIP の統合が必要な場合、一意のデバイス識別子（UDID）属性を指定します。

HIP ベースのポリシーを施行するのに使用するモバイル デバイス属性を MDM サーバーから取得するために、GlobalProtect に MDM を統合できるようになっています。GlobalProtect アプリケーションがエンドポイントの UDID を GlobalProtect ゲートウェイに提示しなければ、MDM の統合が機能しません。UDID 属性により、GlobalProtect アプリケーションが MDM ベースのデプロイ環境で UDID 情報を取得・使用できるようになります。プロファイルから UDID 属性を削除すると、MDM の統合を利用できなくなります。GlobalProtect アプリケーションは新しい UDID を生成しますが、それを統合のために使用することはできません。

- **Palo Alto Networks GlobalProtect**ネットワーク**Connection Type (**接続タイプ**)**を使用している場合、**VPN**設定に移動して Vendor Configuration (ベンダー設定) 領域で **Vendor Keys (**ベンダーキー**)**を有効化してください。**Key (**キー**)**を**`mobile_id`**に、**Value (**値**)**を**`{DeviceUid}`**に設定します。



- **Custom (**カスタム**)**ネットワーク**Connection Type (**接続タイプ**)**を使用している場合、**VPN**設定に移動して Connection Info (接続情報) 領域で**Custom Data (**カスタム データ**)**を**ADD (**追加**)**してください。**Key (**キー**)**を**`mobile_id`**に、**Value (**値**)**を**`{DeviceUid}`**に設定します。



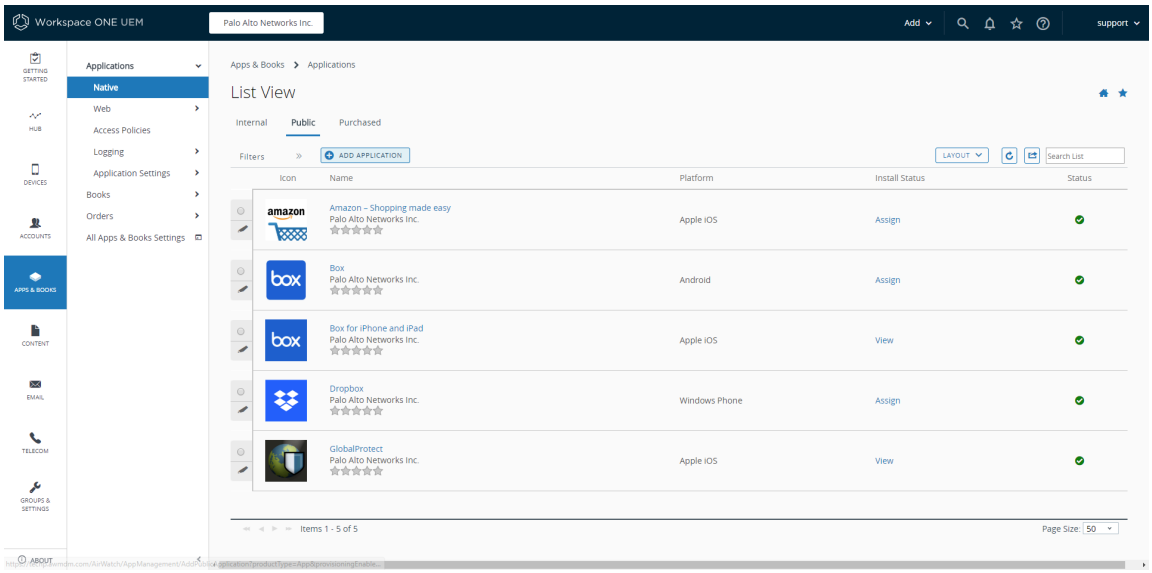
STEP 7 | 変更を**SAVE & PUBLISH (**保存して公開**)**します。

STEP 8 | アプリ単位の VPN 設定を新しい管理対象アプリケーション用に設定するか、既存の管理対象アプリケーションの設定を変更します。

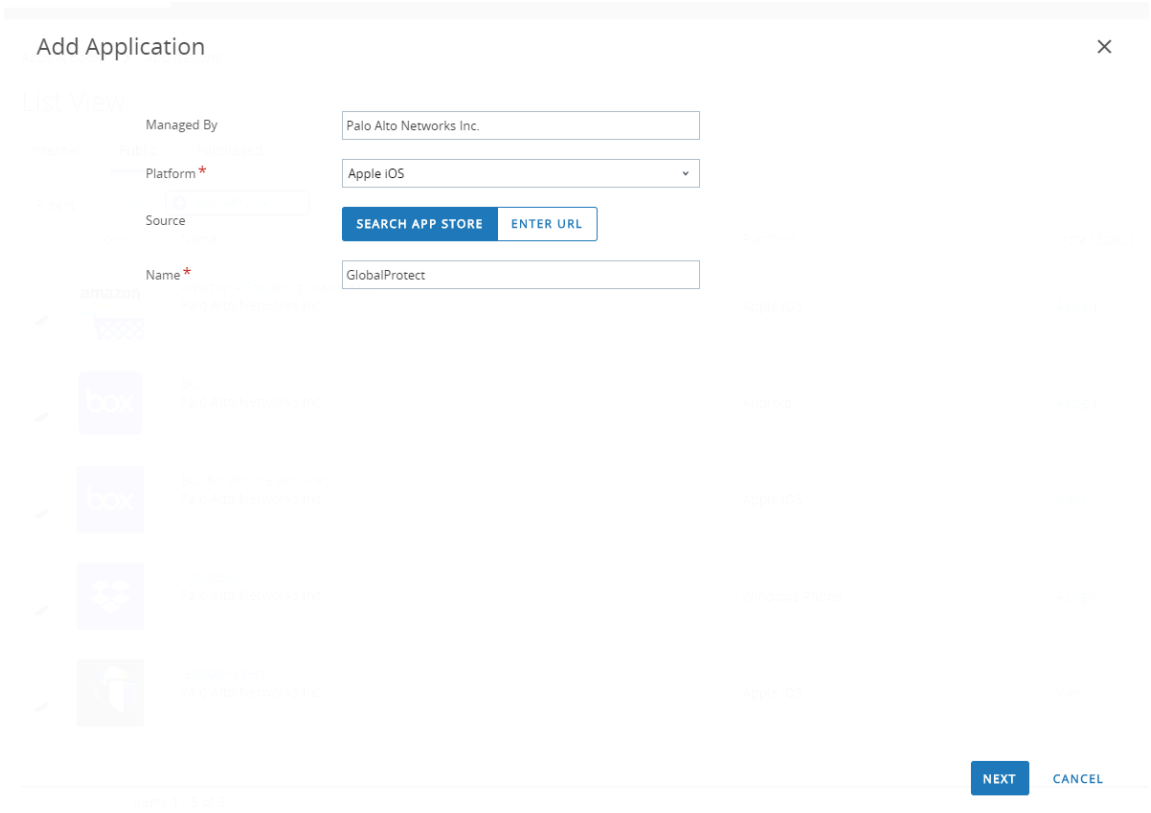
アプリケーション設定を構成し、アプリ単位の VPN を有効にしたら、ユーザーのグループにアプリケーションを公開します。これで、アプリケーションが GlobalProtect VPN トンネル経由でトラフィックを送信できるようになります。

1. **APPS & BOOKS (**アプリおよび本**)** > **Applications (**アプリケーション**)** > **Native (**ネイティブ**)** > **Public (**パブリック**)**を選択します。
2. 新しいアプリケーションを追加するには、**ADD APPLICATION**（アプリケーションの追加）を選択します。既存のアプリケーションの設定を変更するには、Public アプリ

ケーション（リストビュー）リストからアプリケーションを探して、行の隣のアクションメニューにある編集（）アイコンを選択します。

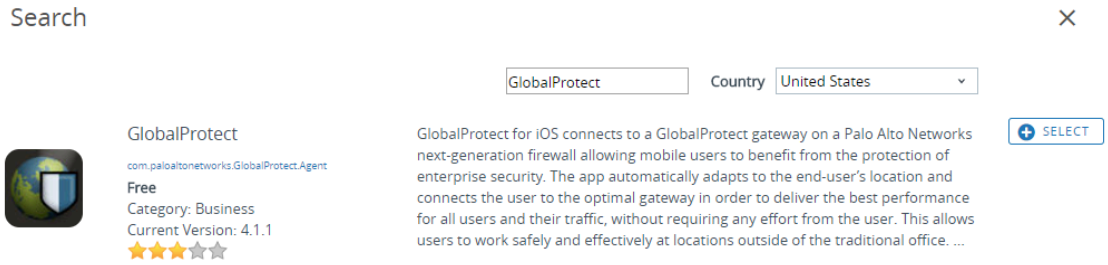


3. **Managed By (**管理者**)**フィールドで、このアプリを管理する組織グループを選択します。
4. **Platform (**プラットフォーム**)**を**Apple iOS**に設定します。
5. アプリを優先的に探す**Source (**ソース**)**を選択します：
   - **SEARCH APP STORE (APP STORE** を検索**)**—アプリの**Name (**名前**)**を入力します。
   - **ENTER URL (URL** を入力**)**—アプリケーションが持つ App Store の URL を入力します（たとえば、Box アプリを追加するには、https://itunes.apple.com/us/app/box-for-iphone-and-ipad/id290853822?mt=8&uo=4を入力します）。

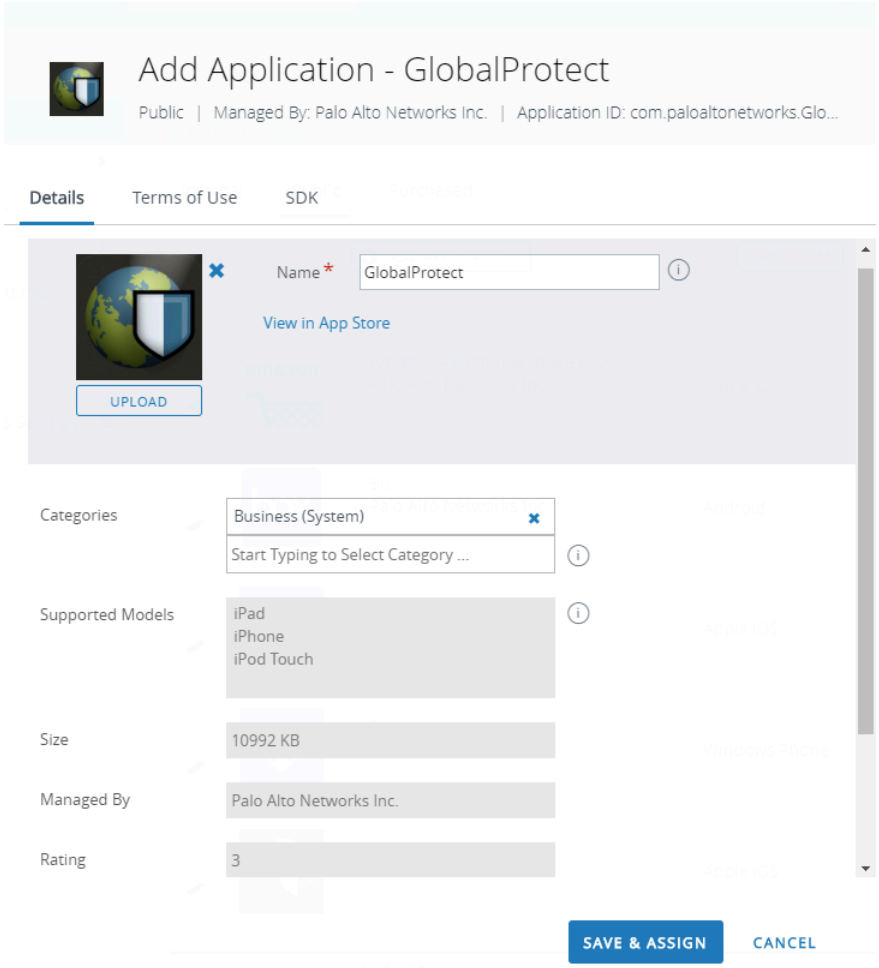


6. **NEXT (次へ)** をクリックします。

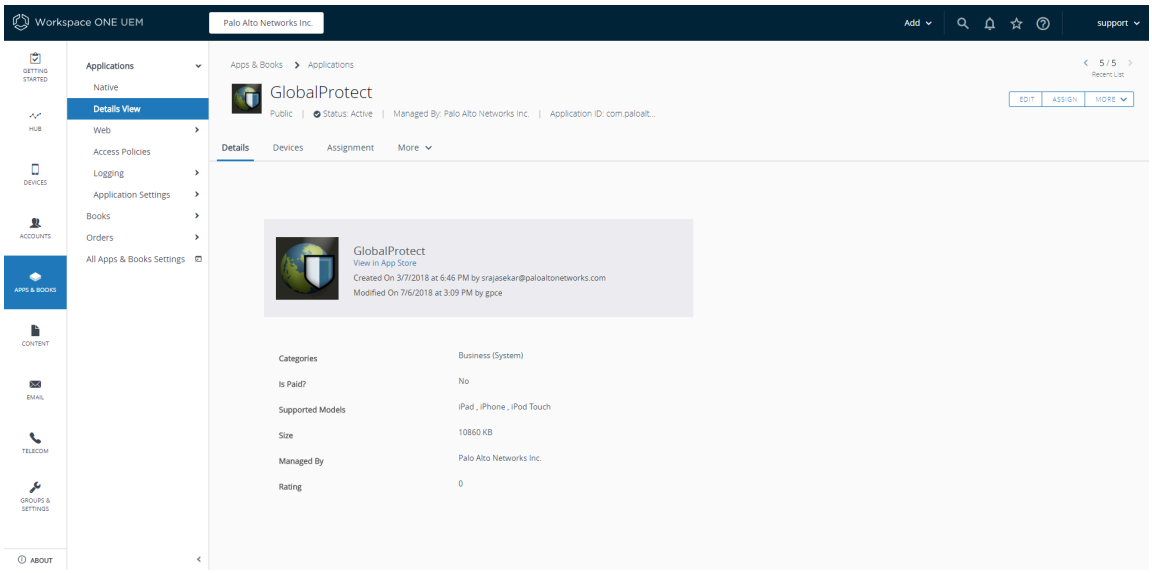
   App Store で検索することにした場合は、検索結果のリストからアプリを **SELECT**（選択）する必要もあります。



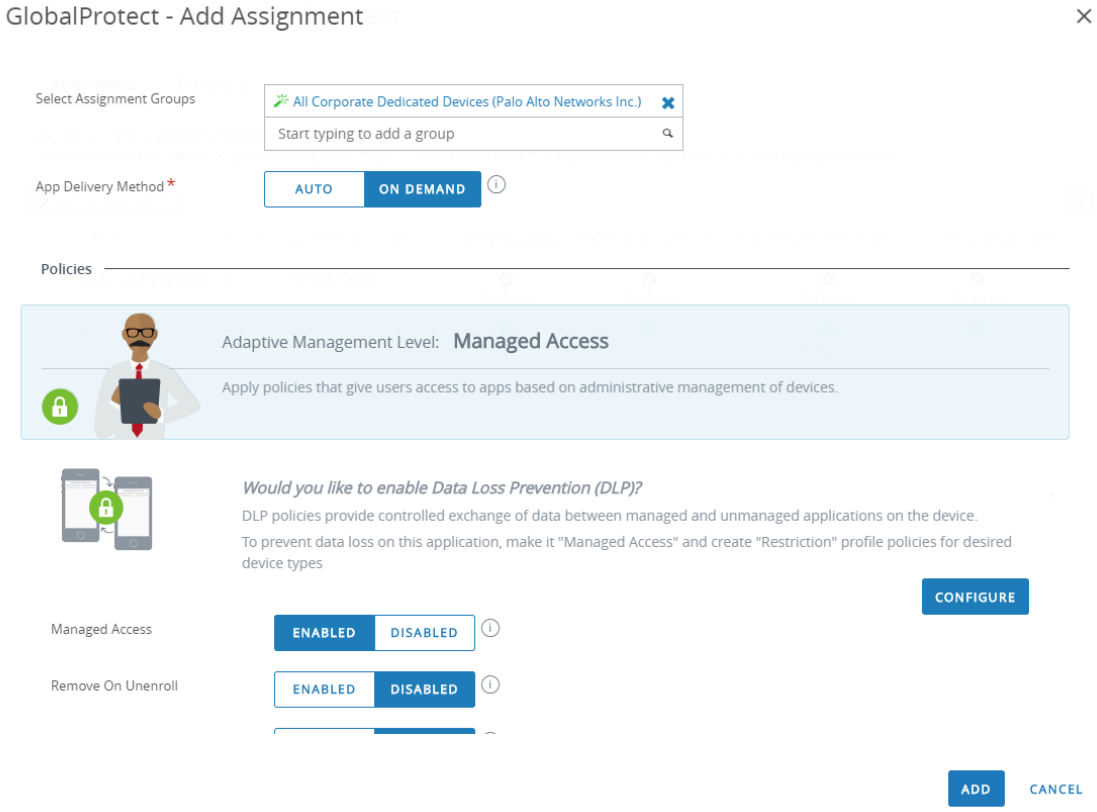
7. Add Application (アプリケーションの追加) ダイアログでアプリの**Name (名前)**が正しいことを確認します。この名前が AirWatch アプリ カタログに表示されます。
8. （任意）AirWatch アプリ カタログでアクセスしやすくなるよう、アプリを事前定義済みあるいはカスタム**Categories (カテゴリ)**に割り当てます。



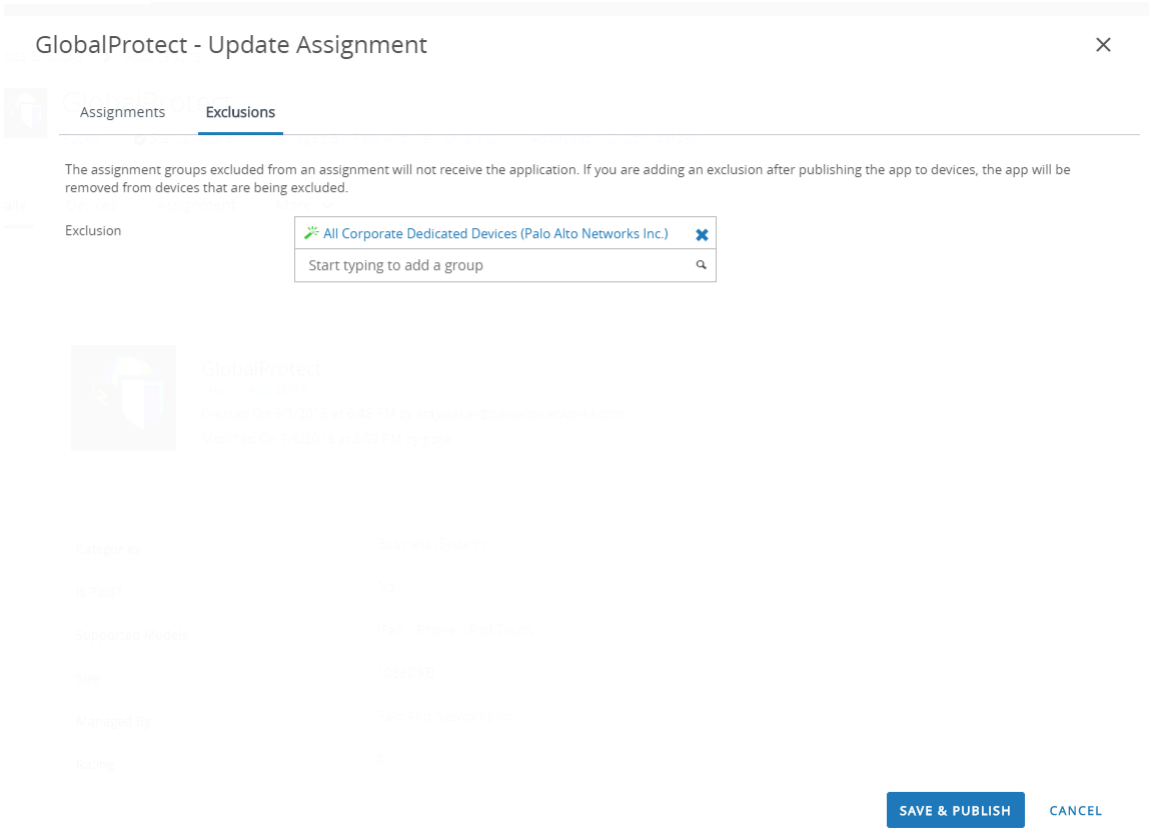
9. 新しいアプリを**SAVE & ASSIGN (**保存して割り当て**)**ます。
10. 新たに追加されたアプリを公開アプリの一覧から選択します（リストビュー）。
11. **Applications (**アプリケーション**)** > **Details View (**詳細ビュー**)**の画面右上にある**ASSIGN (**割り当て**)**をクリックします。



12. **Assignments** (割り当て)を選択してから**ADD ASSIGNMENT** (割り当ての追加)をクリックし、このアプリにアクセスするスマート グループを追加します。
    1. **Select Assignment Groups** (割り当てグループの選択)フィールドで、このアプリへのアクセスを許可するスマート グループを選択します。
    2. **App Delivery Method** (アプリの配信方法)を選択します。**AUTO** (自動)を選択すると、特定のスマート グループにアプリが自動的にデプロイされます。**ON DEMAND** (オンデマンド)を選択する場合は手動でアプリをデプロイする必要があります。
    3. **Managed Access** (管理対象アクセス)オプションを**ENABLED** (有効)に設定します。このオプションにより、適用する管理ポリシーに応じてユーザーがアプリにアクセスできるようになります。
    4. 必要に応じて、残りの設定を行います。
    5. 新しい割り当てを**ADD** （追加）します。



13. （任意）特定のスマート グループがアプリにアクセスできないようにするには、**Exclusions (除外)**を選択してから、除外したいスマート グループを**Exclusion (除外)**フィールドから選択します。



14. 割り当てられたスマート グループに設定を **SAVE & PUBLISH**（保存して公開）します。

AirWatch を使用した *Android* エンドポイントのアプリ単位の *VPN* 設定

AirWatch を使用して GlobalProtect VPN アクセスを設定することで管理下のモバイル エンドポイントから内部リソースにアクセスできるようになります。アプリ単位の VPN 設定において、どの管理アプリケーションが GlobalProtect VPN トンネル経由でトラフィックを送信できるかを指定できます。管理していないアプリケーションは GlobalProtect VPN トンネルを解する代わりにインターネットに直接接続を続けようとします。

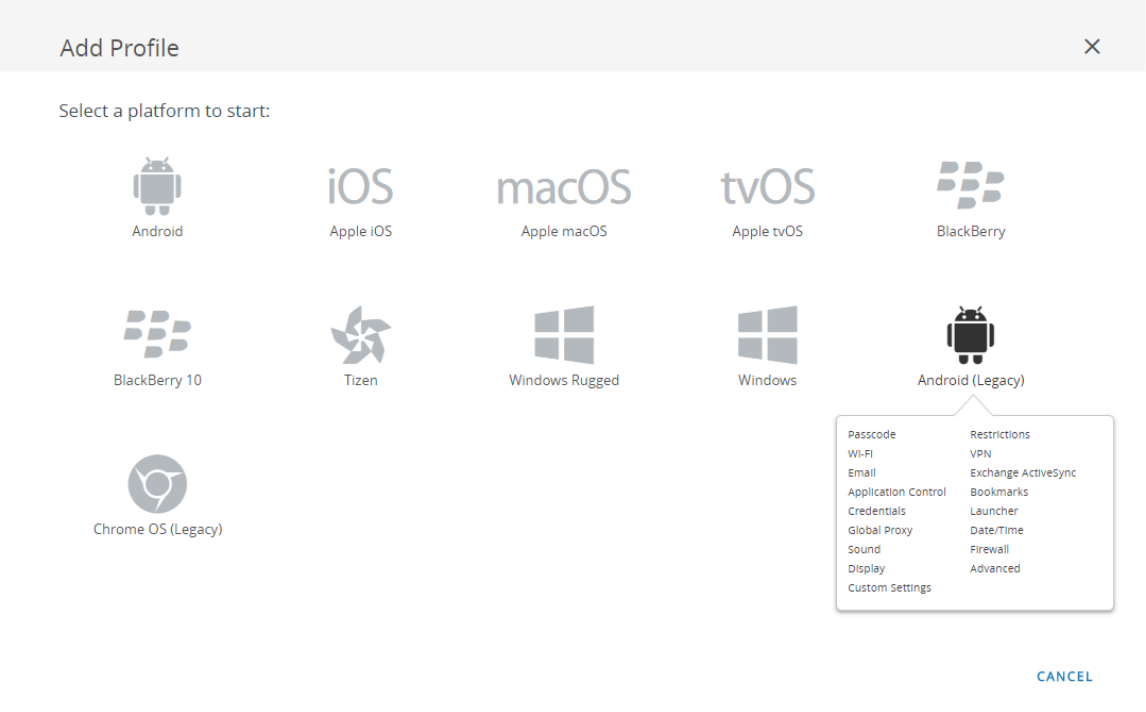
次の各作業により、AirWatch を使用して Android エンドポイント用にアプリ単位の VPN 設定を構成することができます：

STEP 1 | Android 用 GlobalProtect アプリをダウンロードします。

- AirWatch を使用して GlobalProtect モバイル アプリケーションをデプロイします。
- Google Playから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | AirWatch コンソールから、既存の Android プロファイルを編集するか、新しいプロファイルを追加します。

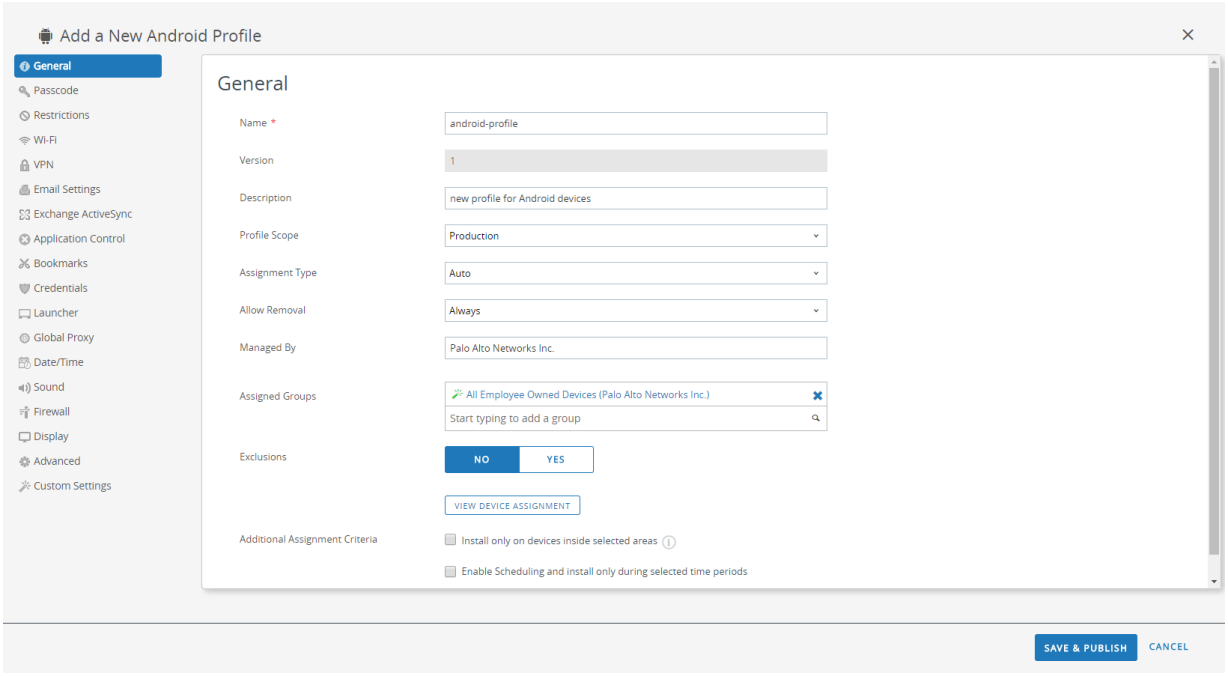
1. **Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles (プロファイル)**を選択して新しいプロファイルを**ADD (追加)**します。
2. プラットフォームのリストで**Android (Legacy) (アンドロイド（レガシー）)**を選択します。



STEP 3 | **General (**一般**)**設定の設定を行います。

1. プロファイルの**Name**（名前）を入力します。
2. （任意）その目的を示すプロファイルの簡単な**Description (**説明**)**を入力します。
3. （任意）**Profile Scope (**プロファイルのスコープ**)**で、**Production (**プロダクション**)**、**Staging (**ステージング**)**、**Both (**両方**)**のいずれかを選択します。
4. （任意）プロファイルをエンドポイントにデプロイする方法として、**Assignment Type (**割り当てタイプ**)**を選択します。プロファイルをすべてのエンドポイントに自動的にデプロイするには、**Auto**（自動）を選択します。エンド ユーザーがプロファイルをセルフサービス ポータル（SSP）からインストールしたり、プロファイルを個別のエンドポイントに手動でデプロイできるようにするには、**Optional**（任意）を選択します。エンド ユーザーがエンドポイントに適用されるコンプライアンス ポリシーに違反した場合にプロファイルをデプロイするには、**Compliance**（コンプライアンス）を選択します。
5. （任意）エンドユーザーに対してプロファイルの**Allow Removal (**削除を許可**)**するかどうかを選択します。エンド ユーザーがいつでもプロファイルを手動で削除できるようにするには、**Always**（常に許可）を選択します。エンド ユーザーがプロファイルを削除できないようにするには、**Never**（拒否）を選択します。エンド ユーザーがプロファイルを削除するのに管理者の許可が必要になるようにするには、**With Authorization**（認証あり）を選択します。**With Authorization**（認証あり）を選択すると、必要なパスワードが追加されます。
6. （任意）**Managed By (**管理者**)**フィールドに、プロファイルへの管理アクセスを持つ組織グループを入力します。
7. （任意）**Assigned Groups (**割り当てられたグループ**)**フィールドに、プロファイルの追加先となるスマート グループを追加します。このフィールドには、最低限の OS、デバイス モデル、所有者カテゴリ、組織グループなどの仕様で設定できる新規スマート グループを作成するオプションが含まれます。
8. （任意）このプロファイルの割り当てに**Exclusions (**除外**)**を含めるかどうか指定します。**Yes (**はい**)**を選択すると**Excluded Groups (**除外されたグループ**)**フィールドが表示さ

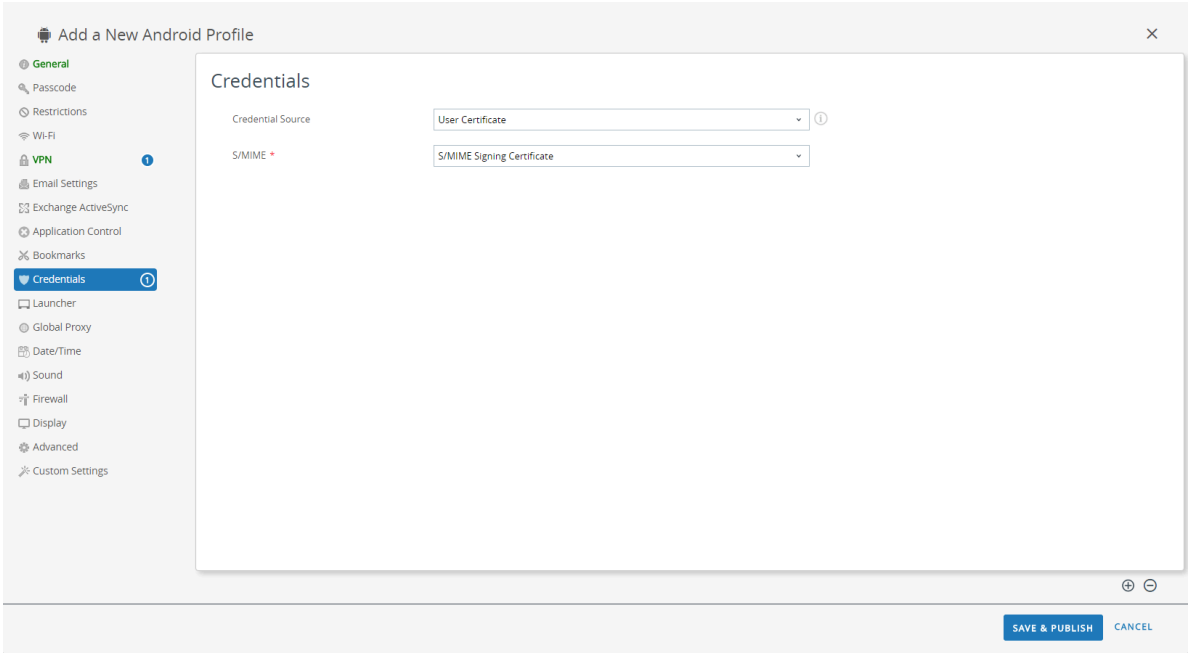
れ、プロファイルの割り当てから除外するスマート グループを選択できるようになります。



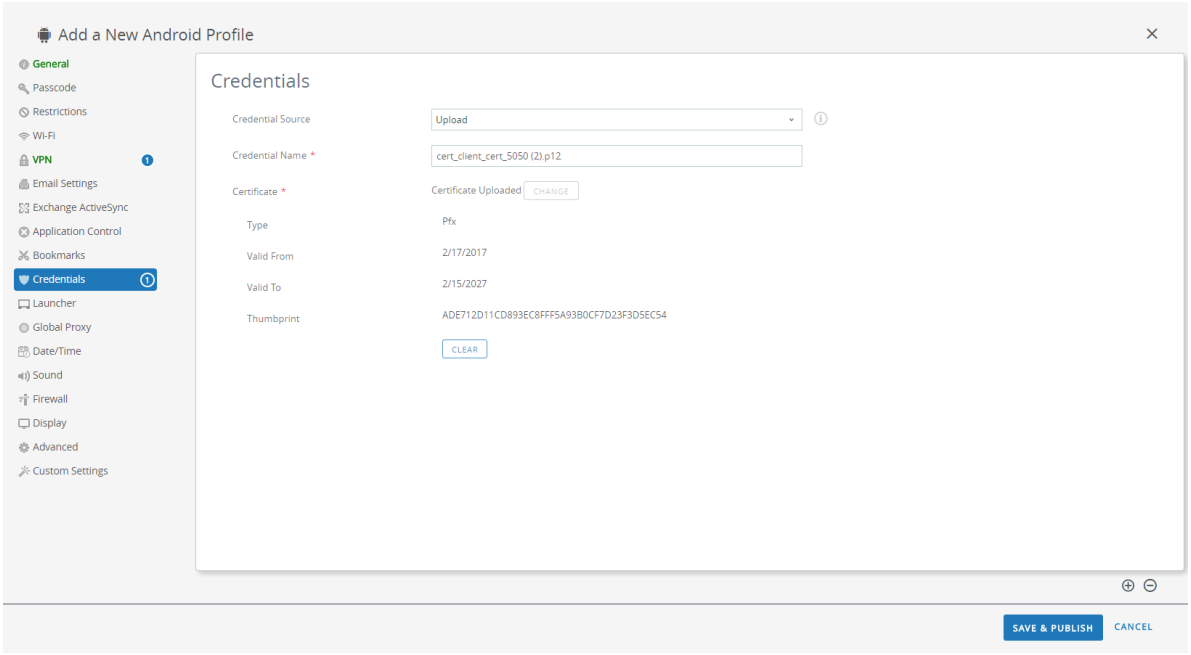
STEP 4 | **Credentials (**認証情報**)**の設定を行います：

アプリ単位の *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。

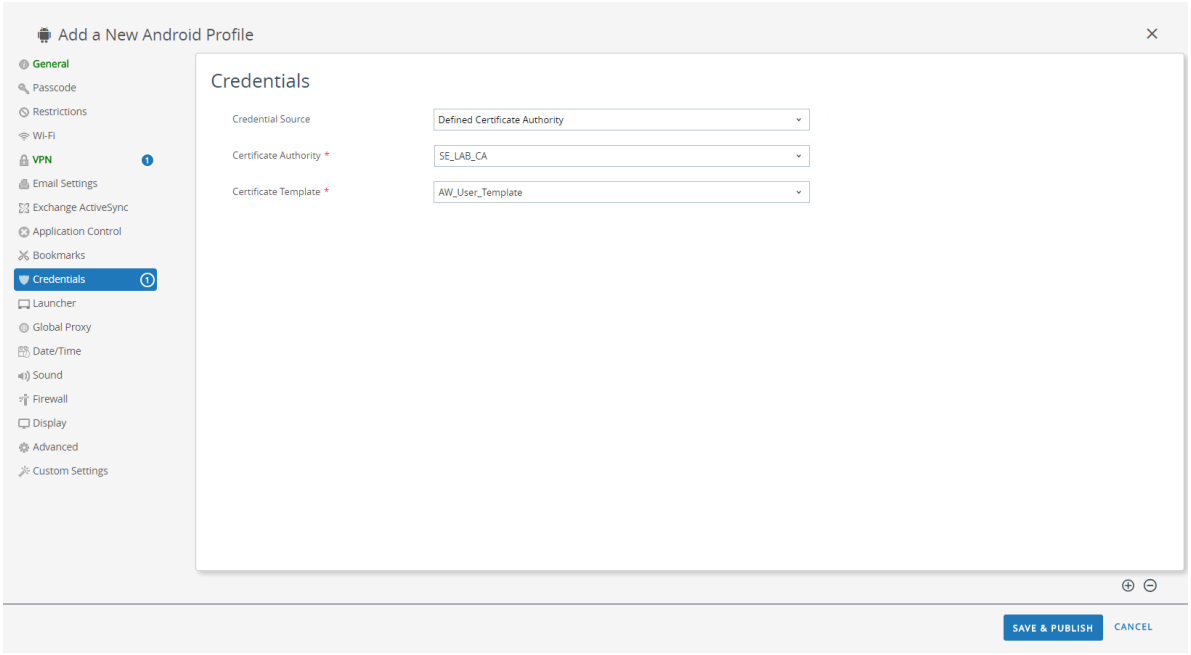
- AirWatch ユーザーからクライアント証明書を取得する方法：
  1. **Credential Source (**認証情報ソース**)**を**User Certificate (**ユーザー証明書**)**に設定します。
  2. **S/MIME Signing Certificate (S/MIME** 署名証明書**)**（デフォルト）を選択します。



- 手動でクライアント証明書をアップロードする方法：
  1. **Credential Source (**認証情報ソース**)**を **(**アップロード**)**に設定します。
  2. **Credential Name (**認証情報名**)**を入力します。
  3. **UPLOAD (**アップロード**)**をクリックし、アップロードする証明書を参照して選択します。
  4. 証明書を選択したら**SAVE (**保存**)**をクリックします。



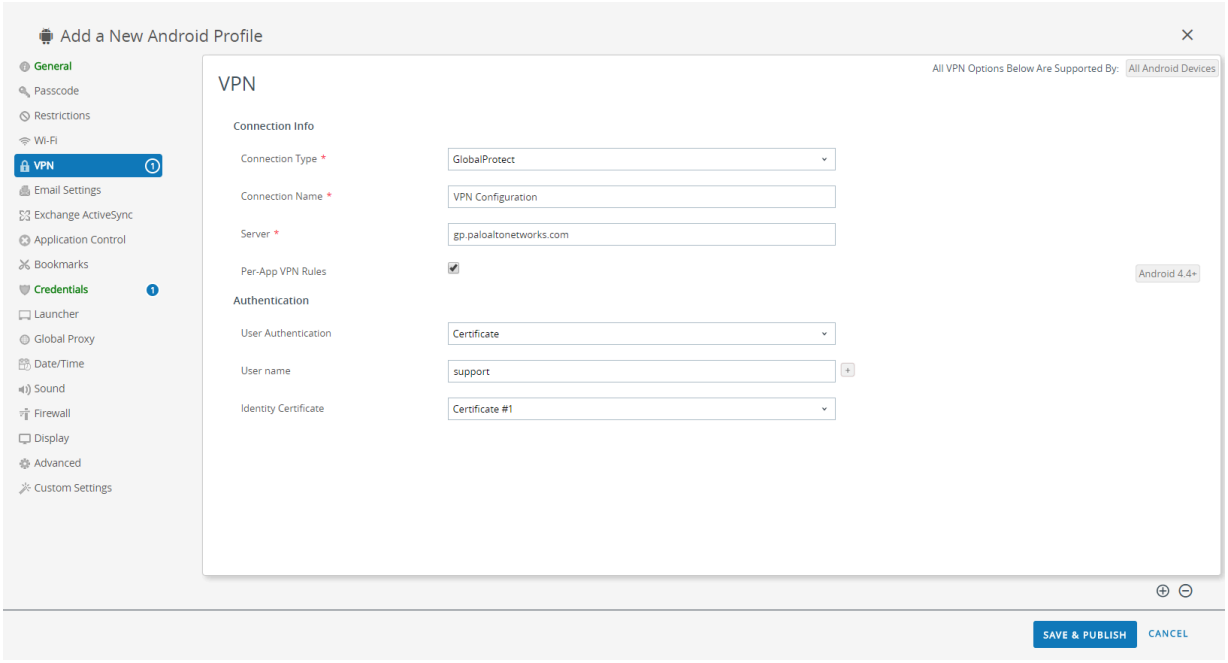
- 事前定義済みの認証局およびテンプレートを使用する方法：
  1. **Credential Source (**認証情報ソース**)**を**Defined Certificate Authority (**定義済みの認証局**)**に設定します。
  2. 証明書の取得元にする**Certificate Authority (**認証局**)**を選択します。
  3. その認証局で使用する**Certificate Template (**証明書テンプレート**)**を選択します。



STEP 5 | **VPN** の設定を行います。

1. ネットワーク**Connection Type (**接続タイプ**)**を**GlobalProtect**に設定します。
2. エンドポイントが表示する**Connection Name (**接続名**)**を入力します。
3. ユーザーが接続する GlobalProtect ポータルのホスト名または IP アドレスを**Server (**サーバー**)**フィールドに入力します。
4. **Per-App VPN Rules** （アプリ単位の **VPN** ルール）を有効化して、管理対象のアプリケーションのトラフィックをすべて GlobalProtect VPN トンネル経由でルーティングします。
5. Authentication（認証）領域で**User Authentication (**ユーザー認証**)**方式を**Certificate (**証明書**)**に設定します。

   アプリ単位の *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。
6. VPN アカウント用の**User name** （ユーザー名）を入力するか、追加（**+**）ボタンをクリックして、サポートされている挿入可能なルックアップ値を表示します。
7. 指示されたら、GlobalProtect でユーザー認証に使用する**Identity Certificate** （アイデンティティ証明書）を選択します。**Identity Certificate (**アイデンティティ証明書**)**は、**Credentials (**認証情報**)**で設定した証明書と同じものです。



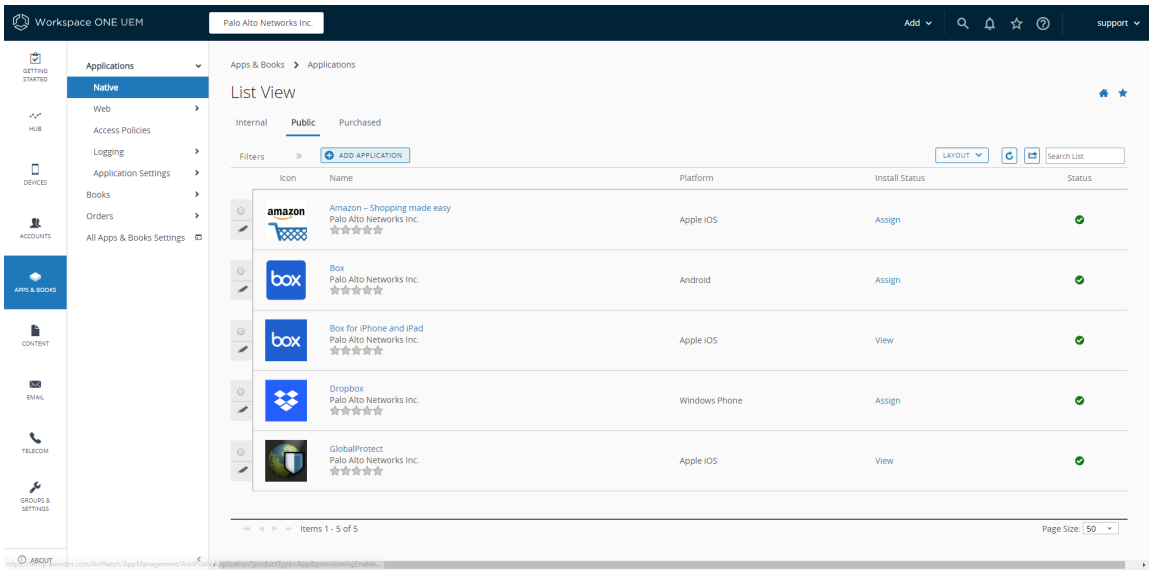
STEP 6 | 変更を**SAVE & PUBLISH (**保存して公開**)**します。

STEP 7 | アプリ単位の VPN 設定を新しい管理対象アプリケーション用に設定するか、既存の管理対象アプリケーションの設定を変更します。

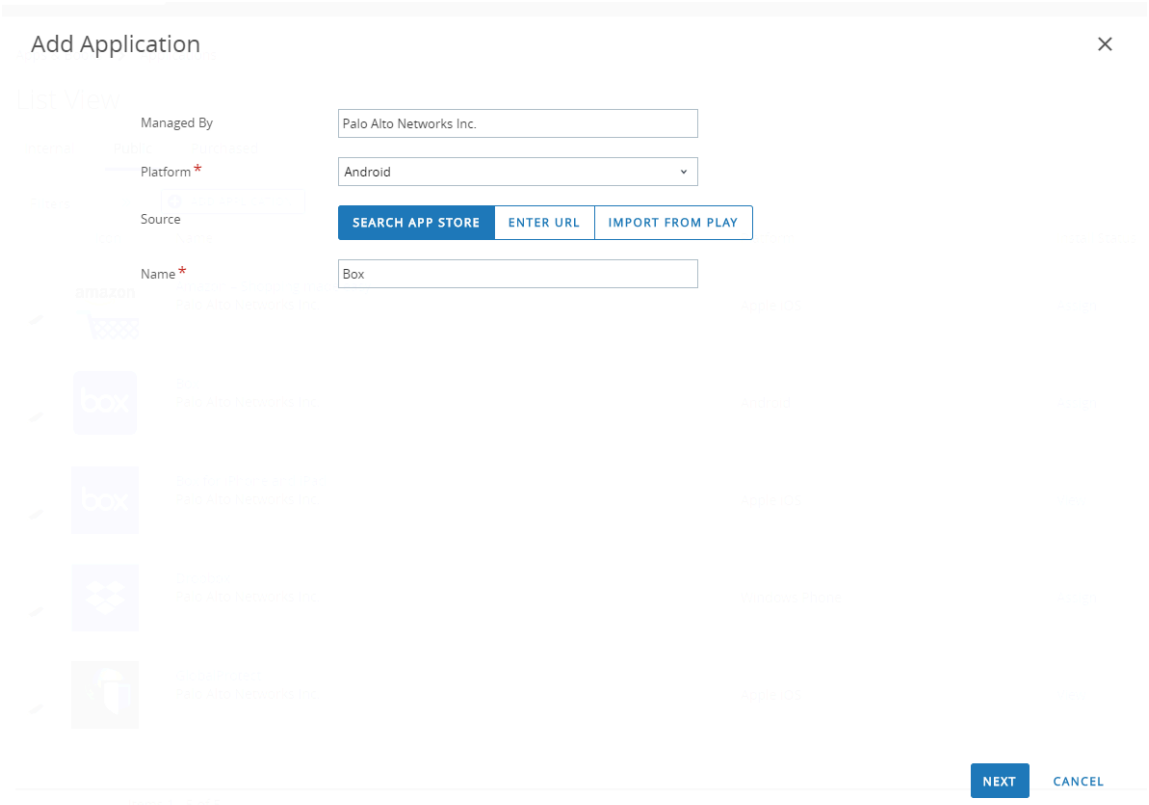
アプリケーション設定を構成し、アプリ単位の VPN を有効にしたら、ユーザーのグループにアプリケーションを公開します。これで、アプリケーションが GlobalProtect VPN トンネル経由でトラフィックを送信できるようになります。

1. **APPS & BOOKS (**アプリおよび本**)** > **Applications (**アプリケーション**)** > **Native (**ネイティブ**)** > **Public (**パブリック**)**を選択します。
2. 新しいアプリケーションを追加するには、**ADD APPLICATION**（アプリケーションの追加）を選択します。既存のアプリケーションの設定を変更するには、Public アプリ

ケーション（リストビュー）リストからアプリケーションを探して、行の隣のアクションメニューにある編集（）アイコンを選択します。

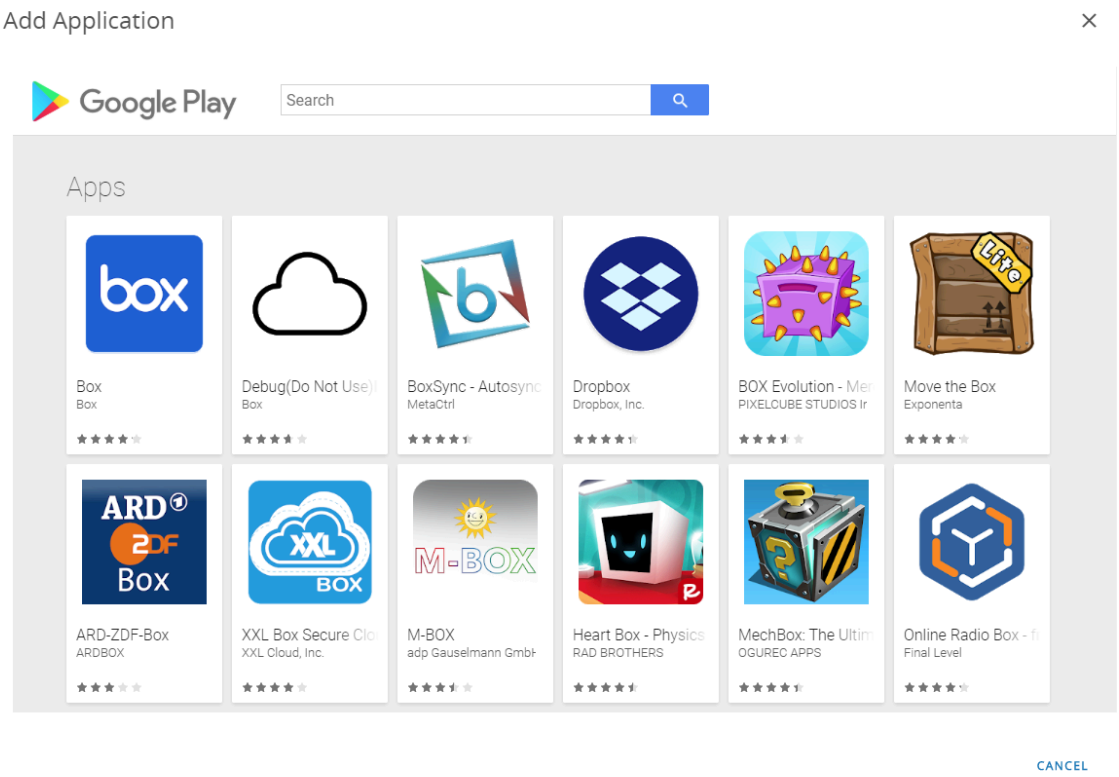


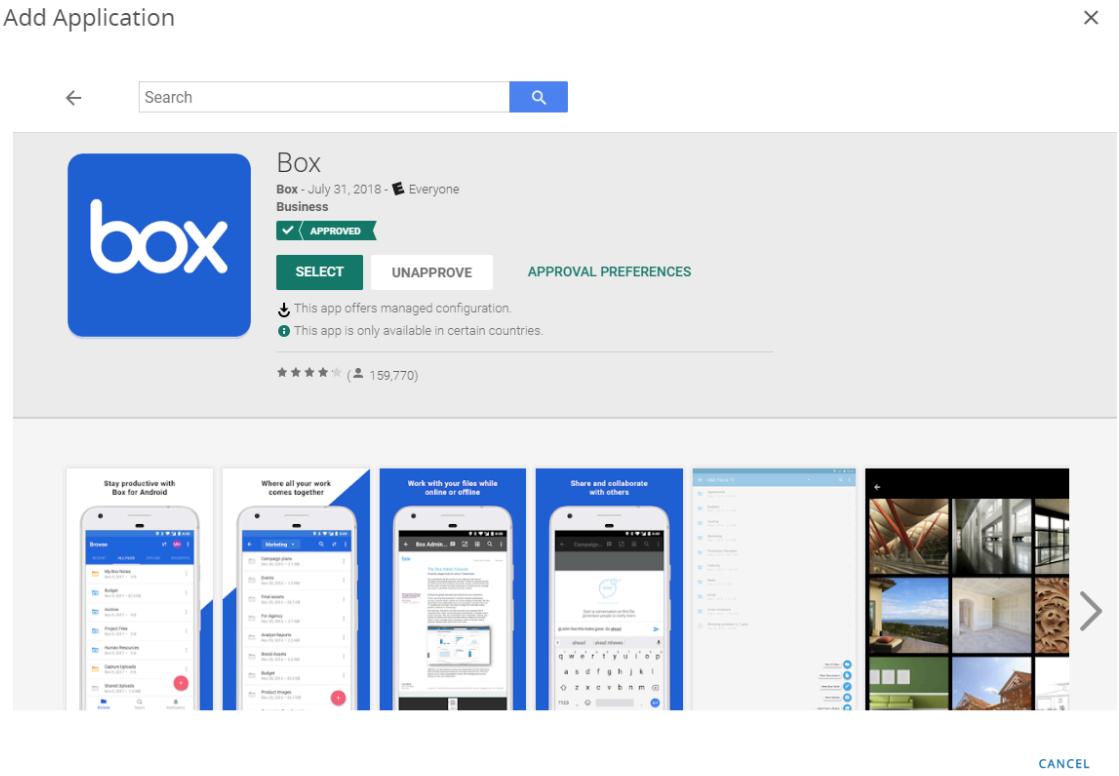
3. **Managed By (**管理者**)**フィールドで、このアプリを管理する組織グループを選択します。
4. **Platform (**プラットフォーム**)**を**Android**に設定します。
5. アプリを優先的に探す**Source (**ソース**)**を選択します：
   - **SEARCH APP STORE (APP STORE** を検索**)**—アプリの**Name (**名前**)**を入力します。
   - **ENTER URL (URL** を入力**)**—アプリケーションの Google Play URL を入力します（たとえば、URL を使って Box アプリを検索するには、https://play.google.com/store/apps/details?id=com.box.androidを入力します）。
   - **IMPORT FROM PLAY (PLAY** からインポート**)**—企業が承認したアプリを Google Play からインポートします。



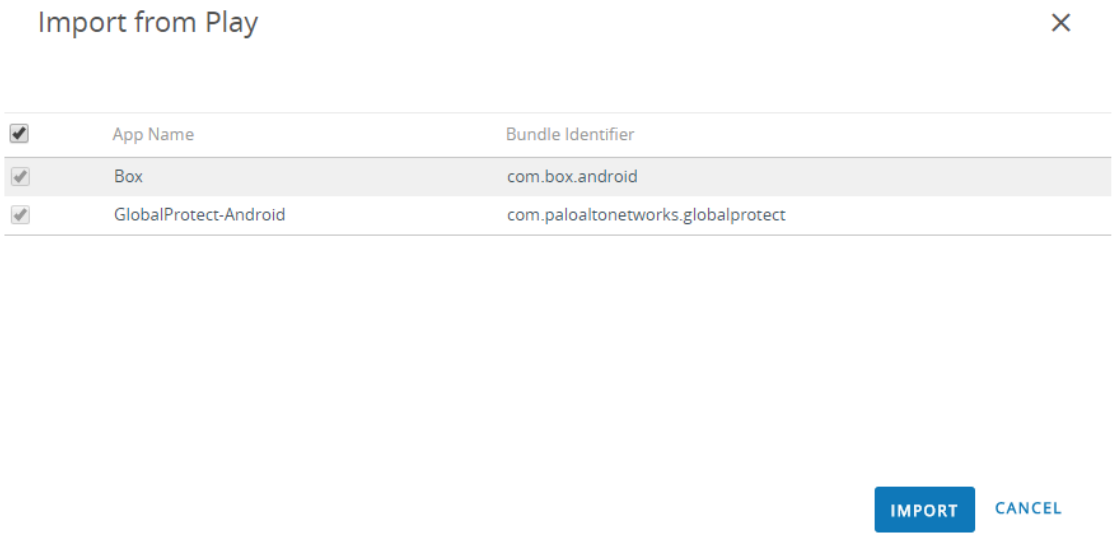
6. **NEXT (次へ)** をクリックします。

   Google Play を検索する場合、検索結果の一覧にあるアプリのアイコンをクリックします。アプリを企業が承認していない場合、アプリを**APPROVE (承認)**する必要があります。アプリが承認されたら、アプリを**SELECT (選択)**します。

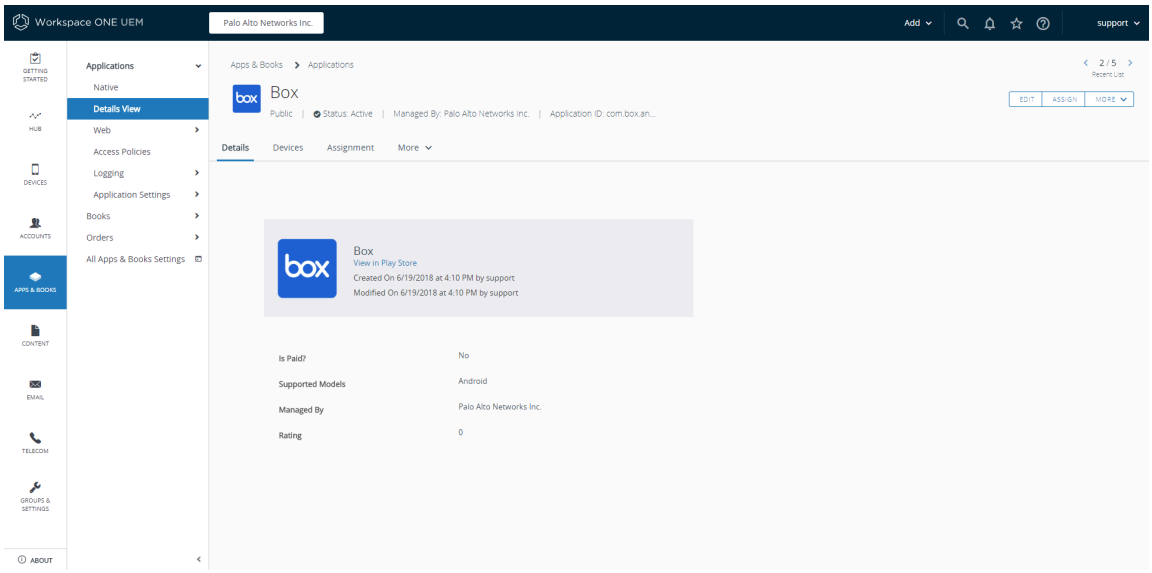




Google Play からアプリをインポートする場合、企業が承認したアプリの一覧からアプリを選択し、**IMPORT (インポート)**をクリックします。リスト内にアプリケーションがない場合、 Android for Work 管理者に連絡してアプリケーションの承認を取ります。

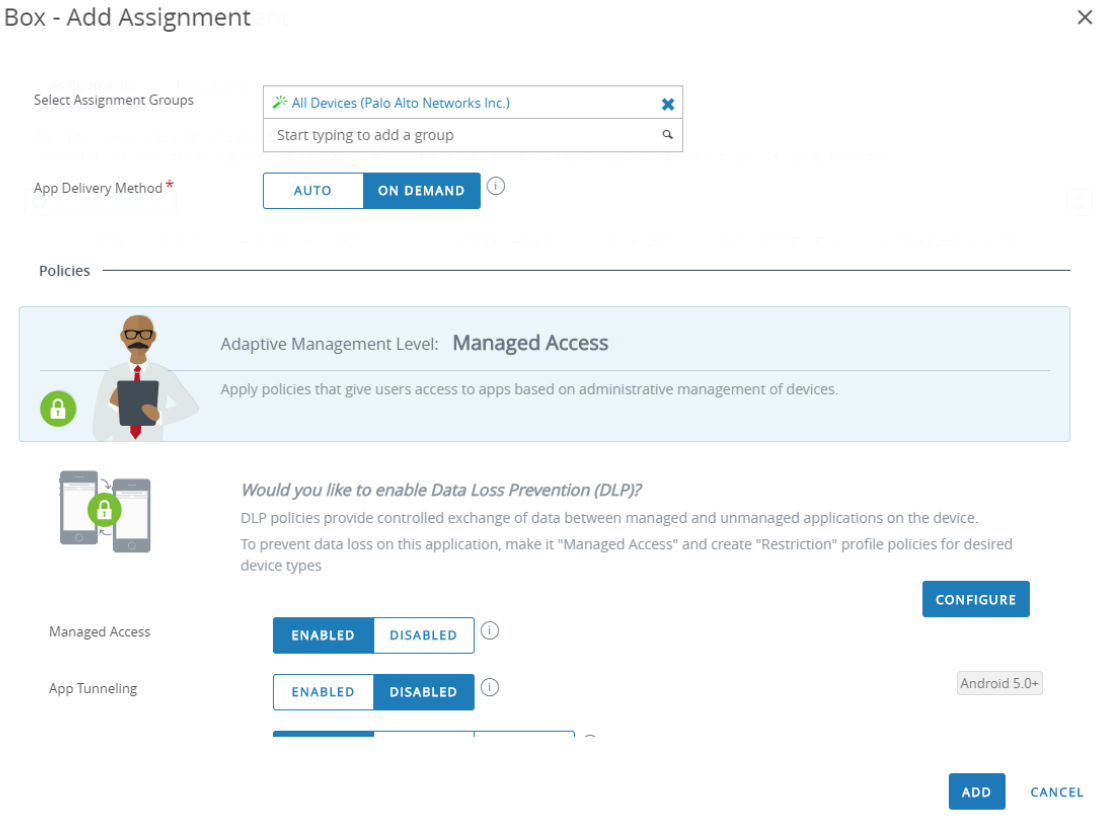


7. 新たに追加されたアプリを公開アプリの一覧から選択します（リストビュー）。
8. **Applications (アプリケーション)** > **Details View (詳細ビュー)**の画面右上にある**ASSIGN (割り当て)**をクリックします。

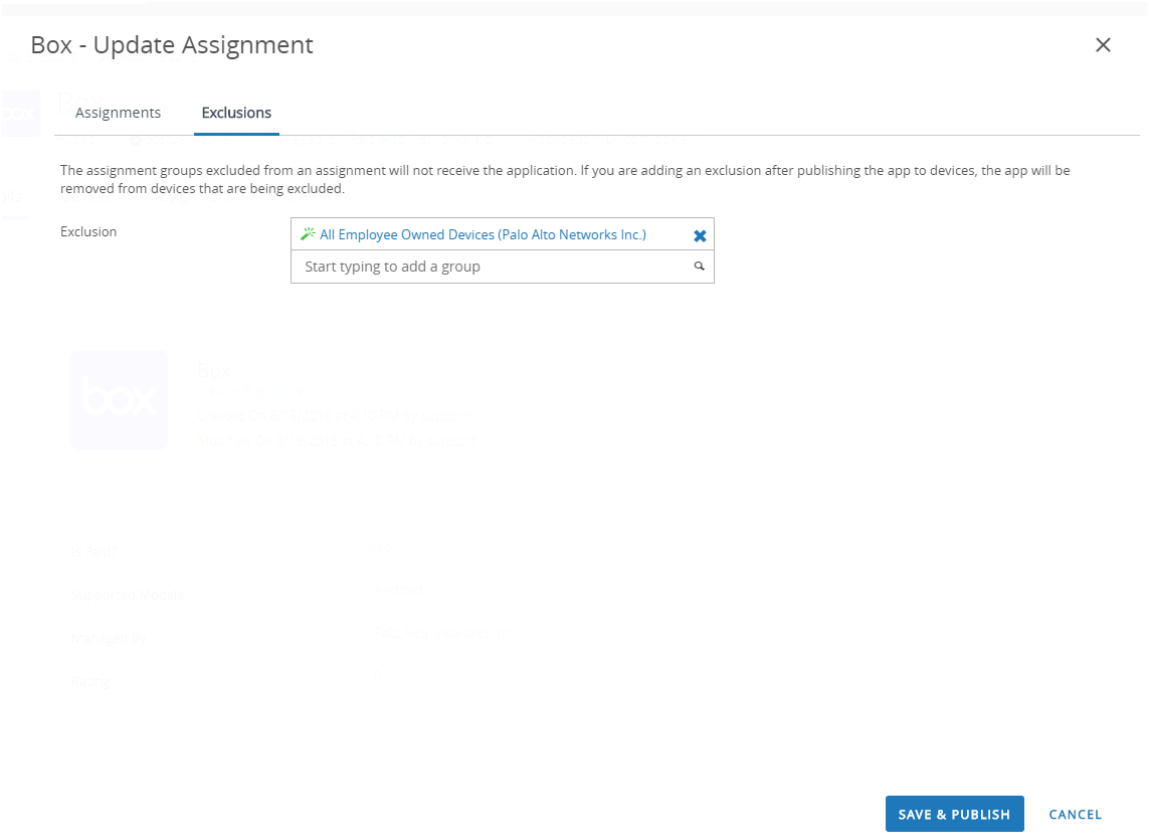


9. **Assignments** (割り当て)を選択してから**ADD ASSIGNMENT** (割り当ての追加)をクリックし、このアプリにアクセスするスマート グループを追加します。

   1. **Select Assignment Groups** (割り当てグループの選択)フィールドで、このアプリへのアクセスを許可するスマート グループを選択します。
   2. **App Delivery Method** (アプリの配信方法)を選択します。**AUTO** (自動)を選択すると、特定のスマート グループにアプリが自動的にデプロイされます。**ON DEMAND** (オンデマンド)を選択する場合は手動でアプリをデプロイする必要があります。
   3. **Managed Access** (管理対象アクセス)オプションを**ENABLED** (有効)に設定します。このオプションにより、適用する管理ポリシーに応じてユーザーがアプリにアクセスできるようになります。
   4. 必要に応じて、残りの設定を行います。
   5. 新しい割り当てを**ADD** （追加）します。



10. （任意）特定のスマート グループがアプリにアクセスできないようにするには、**Exclusions (除外)**を選択してから、除外したいスマート グループを**Exclusion (除外)**フィールドから選択します。



11. 割り当てられたスマート グループに設定を **SAVE & PUBLISH**（保存して公開）します。

AirWatch を使用した *Windows 10 UWP* エンドポイント用のアプリ単位の *VPN* 設定

AirWatch を使用して GlobalProtect VPN アクセスを設定することで管理下のモバイル エンドポイントから内部リソースにアクセスできるようになります。アプリ単位の VPN 設定において、どの管理アプリケーションが GlobalProtect VPN トンネル経由でトラフィックを送信できるかを指定できます。管理していないアプリケーションは GlobalProtect VPN トンネルを解する代わりにインターネットに直接接続を続けようとします。

Windows エンドポイントについては *AirWatch* でまだ *GlobalProtect* が公式の接続プロバイダとしてリストされていないため、代わりとなる *VPN* プロバイダを選択し、*GlobalProtect* アプリケーションの設定を編集して、以下の手順に従って設定を *VPN* プロファイルにインポートし直す必要があります。

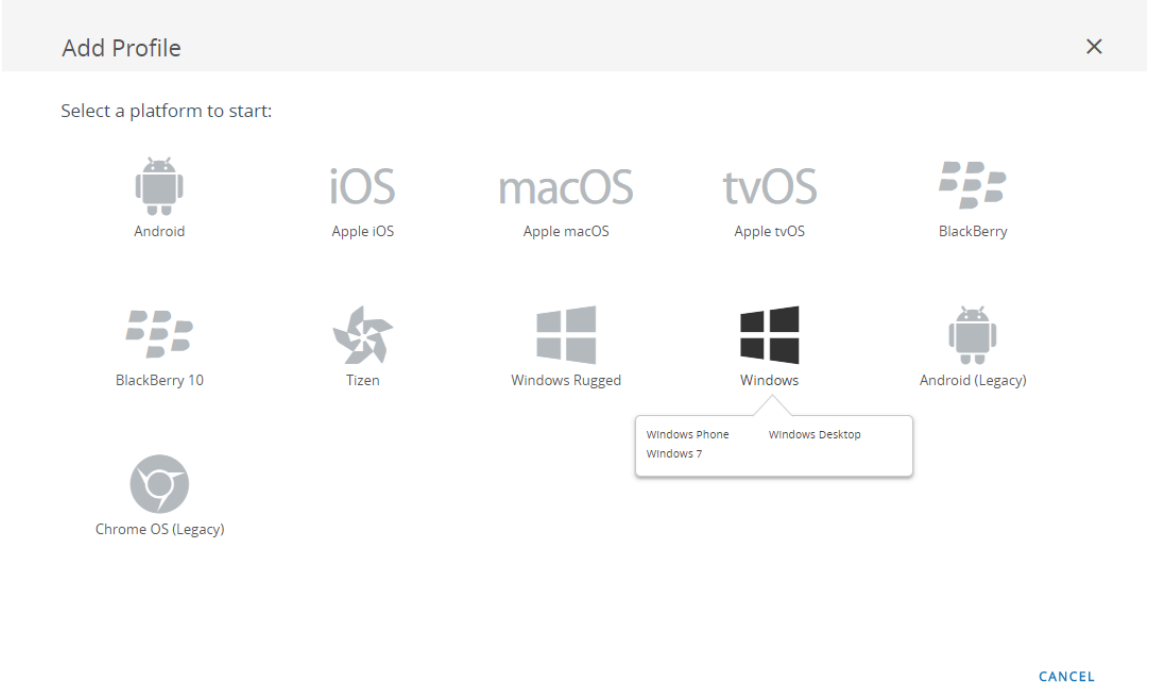
次の各作業により、AirWatch を使用して Windows 10 UWP エンドポイント用にアプリ単位の VPN 設定を構成することができます：

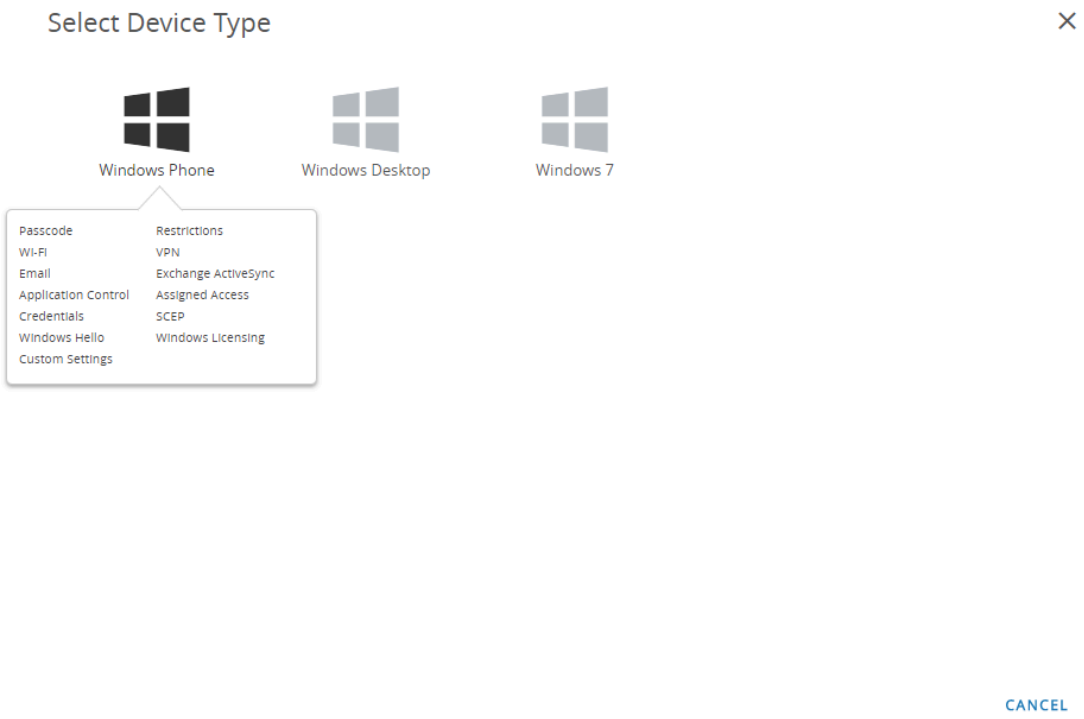
STEP 1 | Windows 10 UWP 用 の GlobalProtect アプリケーションをダウンロードします。

- AirWatch を使用して GlobalProtect モバイル アプリケーションをデプロイします。
- Microsoft ストアから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | AirWatch コンソールから、既存の Windows 10 UWP プロファイルを編集するか、新しいプロファイルを追加します。

1. **Devices (デバイス)** > **Profiles & Resources (プロファイルおよびリソース)** > **Profiles (プロファイル)**を選択して新しいプロファイルを**ADD (追加)**します。
2. プラットフォームとして **Windows** を、デバイスタイプとして **Windows Phone**（**Windows** フォン）を選択します。





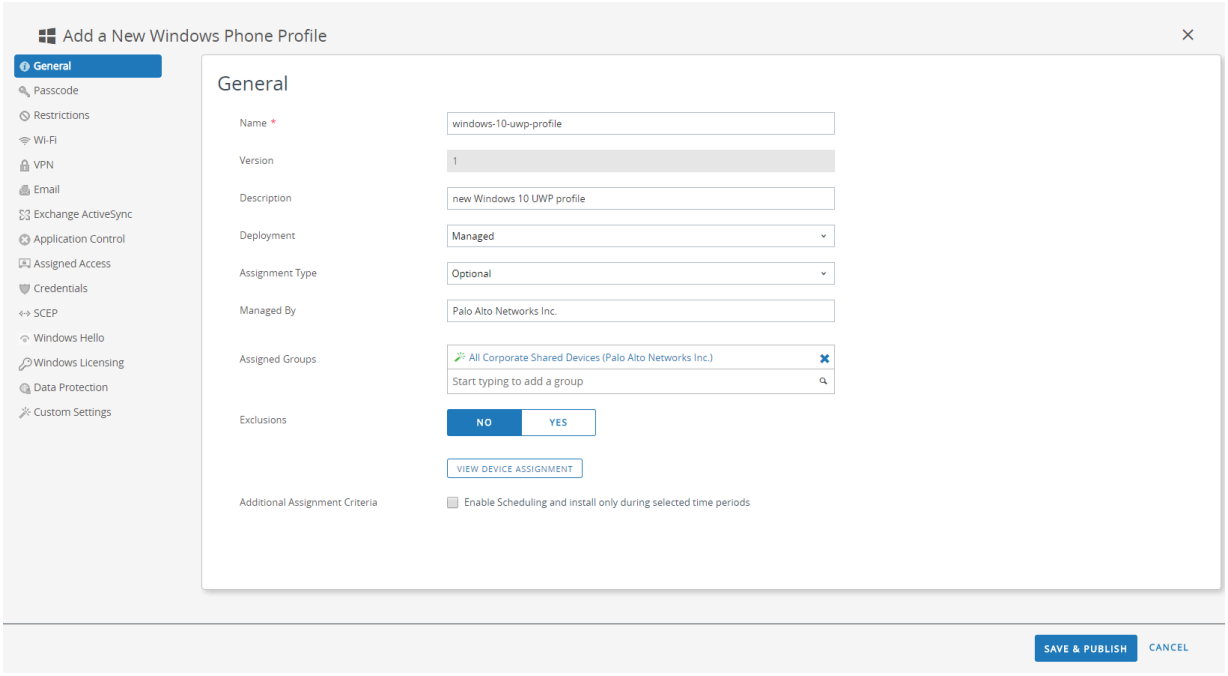
STEP 3 | **General (**一般**)**設定の設定を行います。

- プロファイルの**Name**（名前）を入力します。
- （任意）その目的を示すプロファイルの簡単な**Description (**説明**)**を入力します。
- （任意）**Deployment (**デプロイ**)**方法を**Managed (**管理対象**)**に設定し、登録解除時にプロファイルを自動的に削除できるようにします
- （任意）プロファイルをエンドポイントにデプロイする方法として、**Assignment Type (**割り当てタイプ**)**を選択します。プロファイルをすべてのエンドポイントに自動的にデプロイするには、**Auto**（自動）を選択します。エンド ユーザーがプロファイルをセルフサービ

ス ポータル（SSP）からインストールしたり、プロファイルを個別のエンドポイントに手動でデプロイできるようにするには、**Optional**（任意）を選択します。エンド ユーザーがエンドポイントに適用されるコンプライアンス ポリシーに違反した場合にプロファイルをデプロイするには、**Compliance**（コンプライアンス）を選択します。

- （任意）**Managed By (**管理者**)**フィールドに、プロファイルへの管理アクセスを持つ組織グループを入力します。
- （任意）**Assigned Groups (**割り当てられたグループ**)**フィールドに、プロファイルの追加先となるスマート グループを追加します。このフィールドには、最低限の OS、デバイス モデル、所有者カテゴリ、組織グループなどの仕様で設定できる新規スマート グループを作成するオプションが含まれます。
- （任意）このプロファイルの割り当てに**Exclusions (**除外**)**を含めるかどうか指定します。**Yes (**はい**)**を選択すると**Excluded Groups (**除外されたグループ**)**フィールドが表示さ

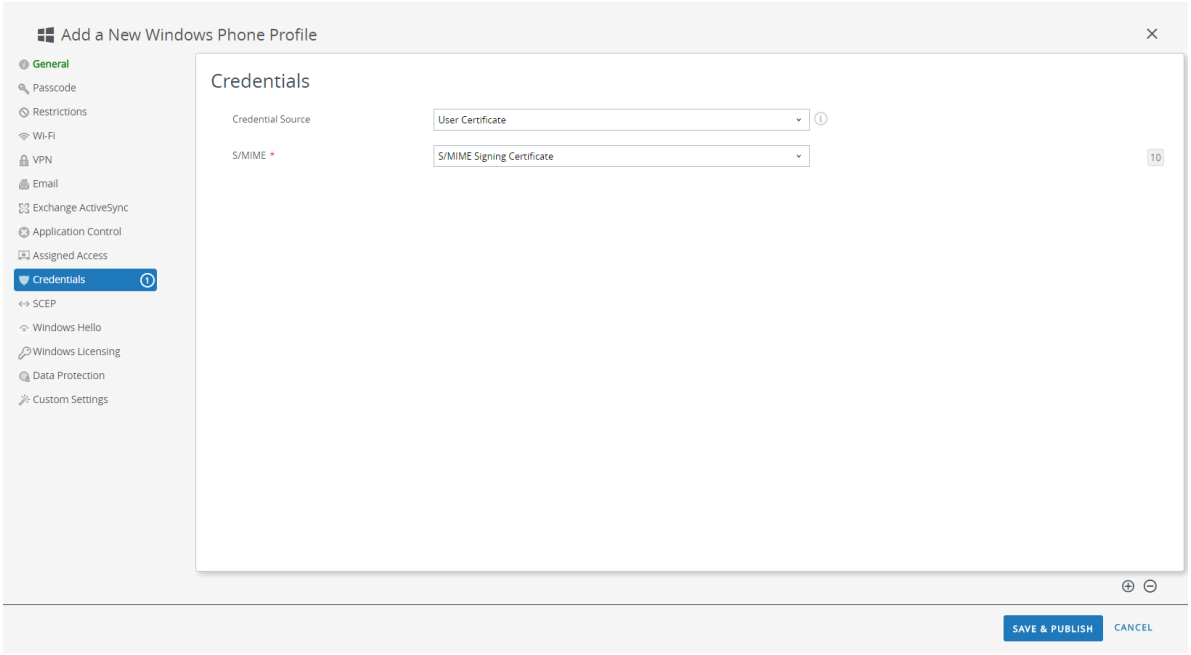
れ、プロファイルの割り当てから除外するスマート グループを選択できるようになります。



STEP 4 | **Credentials (**認証情報**)**の設定を行います：

アプリ単位の *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。

- AirWatch ユーザーからクライアント証明書を取得する方法：
  1. **Credential Source (**認証情報ソース**)**を**User Certificate (**ユーザー証明書**)**に設定します。
  2. **S/MIME Signing Certificate (S/MIME** 署名証明書**)**（デフォルト）を選択します。

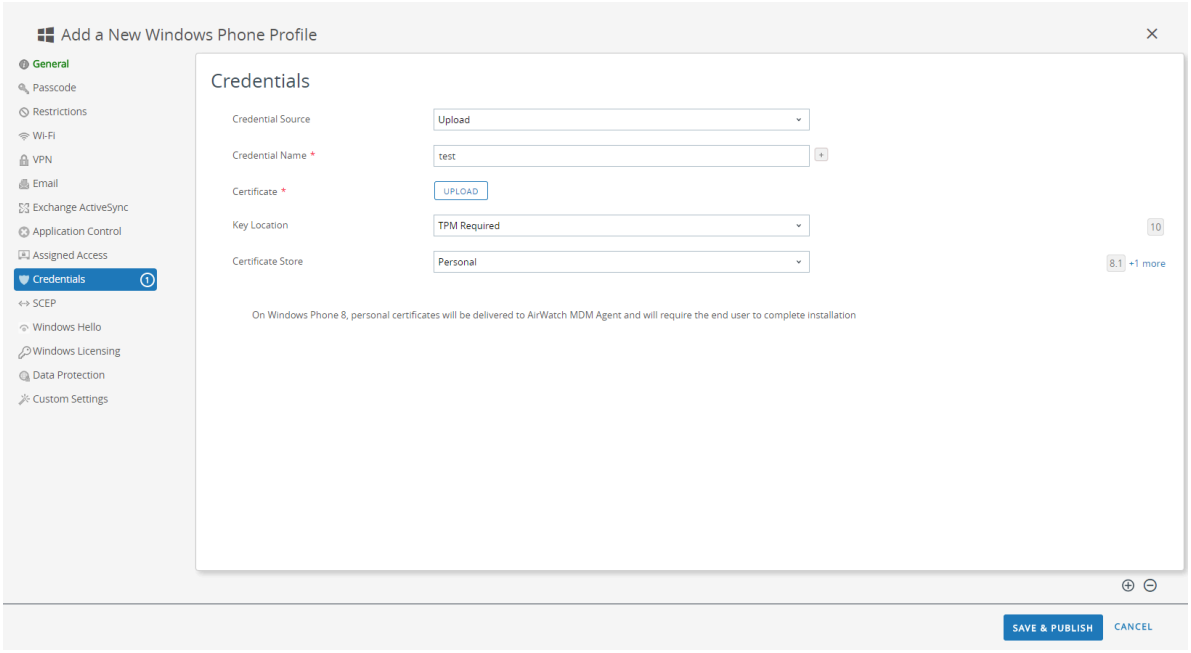


- 手動でクライアント証明書をアップロードする方法：
  1. **Credential Source (**認証情報ソース**)**を **(**アップロード**)**に設定します。
  2. **Credential Name (**認証情報名**)**を入力します。
  3. **UPLOAD (**アップロード**)**をクリックし、アップロードする証明書を参照して選択します。
  4. 証明書を選択したら**SAVE (**保存**)**をクリックします。
  5. 証明書の秘密鍵を保存する**Key Location (**キーの場所**)**を選択します：
     - **TPM Required (TPM** が必要**)**—Trusted Platform Module（信頼されたプラットフォーム モジュール）に秘密鍵を保存します。エンドポイントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵をインストールできません。
     - **TPM If Present (**存在する場合は **TPM)**—信頼されたプラットフォーム モジュールがエンドポイントに存在する場合、秘密鍵をそのモジュールに保存します。エンドポ

イントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵はエンドポイントのソフトウェアに保存されます。

- **Software (ソフトウェア)**—秘密鍵をエンドポイントのソフトウェアに保存します。
- **Passport (パスポート)**—秘密鍵を Microsoft Passport に保存します。このオプションを使用する場合、AirWatch 保護エージェントをエンドポイントにインストールしなければなりません。

6. **Certificate Store**（証明書ストア）を **Personal**（個人）に設定します。

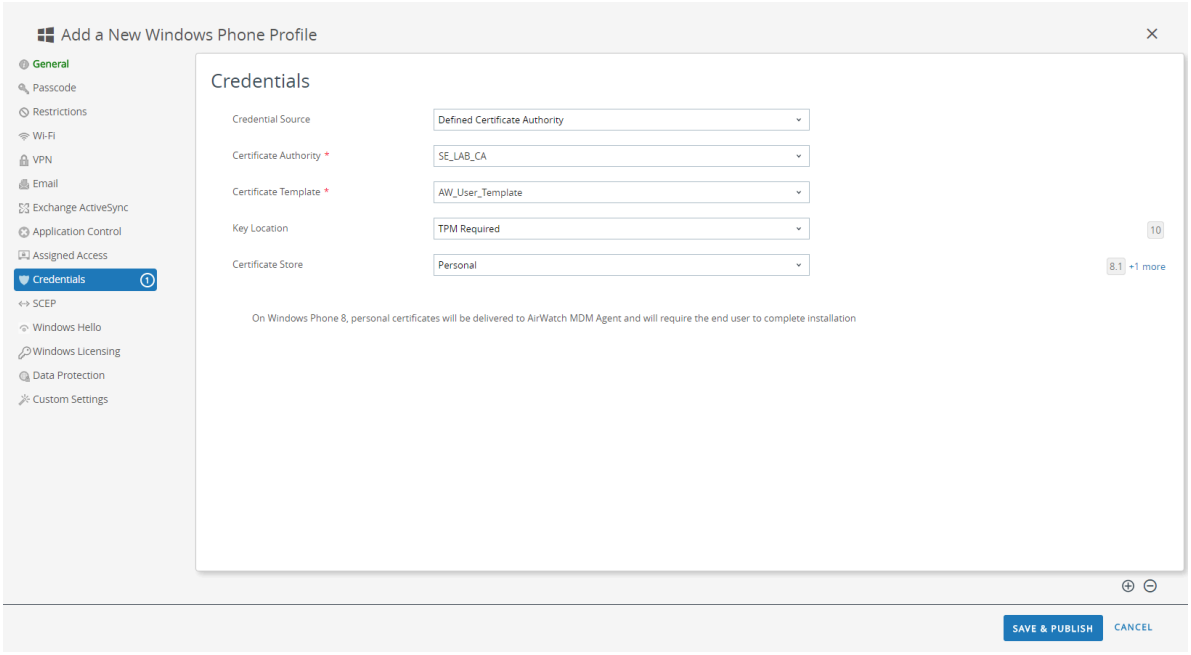


- 事前定義済みの認証局およびテンプレートを使用する方法：
  1. **Credential Source (**認証情報ソース**)**を**Defined Certificate Authority (**定義済みの認証局**)**に設定します。
  2. 証明書の取得元にする**Certificate Authority (**認証局**)**を選択します。
  3. その認証局で使用する**Certificate Template (**証明書テンプレート**)**を選択します。
  4. 証明書の秘密鍵を保存する**Key Location (**キーの場所**)**を選択します：
     - **TPM Required (TPM** が必要**)**—Trusted Platform Module（信頼されたプラットフォーム モジュール）に秘密鍵を保存します。エンドポイントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵をインストールできません。
     - **TPM If Present (**存在する場合は **TPM)**—信頼されたプラットフォーム モジュールがエンドポイントに存在する場合、秘密鍵をそのモジュールに保存します。エンドポ

イントで信頼されたプラットフォーム モジュールを利用できない場合、秘密鍵はエンドポイントのソフトウェアに保存されます。

- **Software (ソフトウェア)**—秘密鍵をエンドポイントのソフトウェアに保存します。
- **Passport (パスポート)**—秘密鍵を Microsoft Passport に保存します。このオプションを使用する場合、AirWatch 保護エージェントをエンドポイントにインストールしなければなりません。

5. **Certificate Store**（証明書ストア）を **Personal**（個人）に設定します。

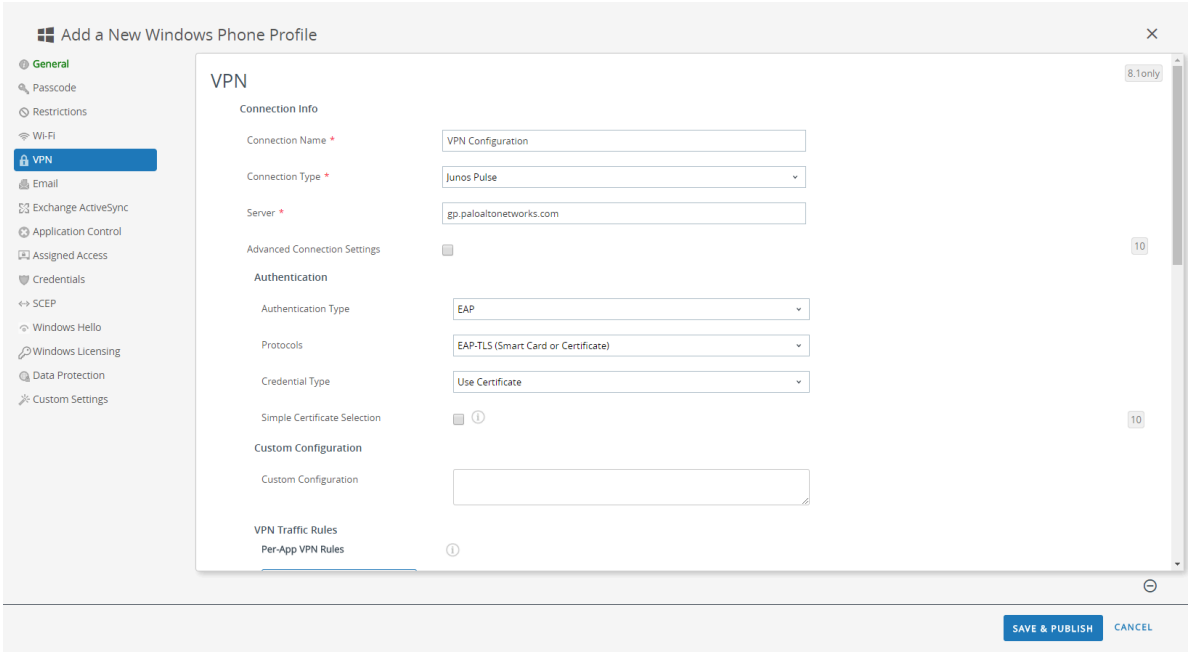


STEP 5 | **VPN** の設定を行います。

1. エンドポイントが表示する**Connection Name (**接続名**)**を入力します。
2. 別の**Connection Type (**接続タイプ**)**のプロバイダーを選択します（GlobalProtect VPN プロファイルに必要な関連するベンダー設定が含まれていないため、**IKEv2**、**L2TP**、**PPTP**、**Automatic**（自動）は選択しないでください）。

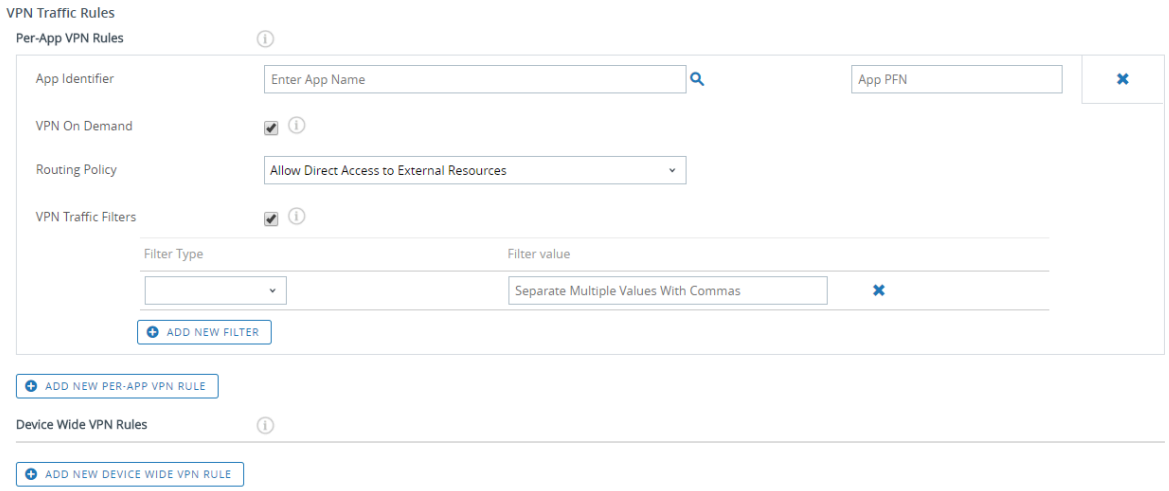
   Windows エンドポイントについては *AirWatch* がまだ *GlobalProtect* を公式の接続プロバイダとしてリストしていないため、代わりとなる *VPN* プロバイダを選択する必要があります。
3. ユーザーが接続する GlobalProtect ポータルのホスト名または IP アドレスを**Server (**サーバー**)**フィールドに入力します。
4. Authentication (認証) 領域で証明書ベースの**Authentication Type (**認証タイプ**)**を選択し、エンドユーザーを認証する方式を指定します。

   アプリ単位の *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。



5. （任意）GlobalProtect がユーザーの認証情報を保存するのを許可するには、Policies（ポリシー）エリアにある **Remember Credentials**（認証情報の記憶）オプションを **ENABLE (**有効**)** にします。
6. VPN Traffic Rules (VPN トラフィック ルール) 領域で**ADD NEW PER-APP VPN RULE (**新しいアプリ単位の **VPN** ルールを追加**)**し、特定の古いアプリ（通常は .exe ファイル）や新しいアプリ（通常は Microsoft ストアからダウンロード）に使用するルールを指定します。
   1. （任意）**VPN On Demand (**オンデマンド **VPN)**を有効化し、アプリが起動する際に GlobalProtect が自動的に接続を確立できるようにします。
   2. **Routing Policy (**ルーティング ポリシー**)**を選択し、アプリのトラフィックを VPN トンネル経由で送るかどうかを指定します。
   3. （任意）特定の**VPN Traffic Filters (VPN** トラフィック フィルター**)**を構成し、IP アドレスやポートといった特定の一致条件にマッチするアプリケーションのトラフィックのみを VPN 経由でルーティングします。

      ADD NEW FILTER (新規フィルターの追加**)**をクリックして一致条件を追加します。指示されたら、**Filter Name (**フィルター名**)**およびそれに対応する**Filter Value (**フィルターの値**)**を入力します。



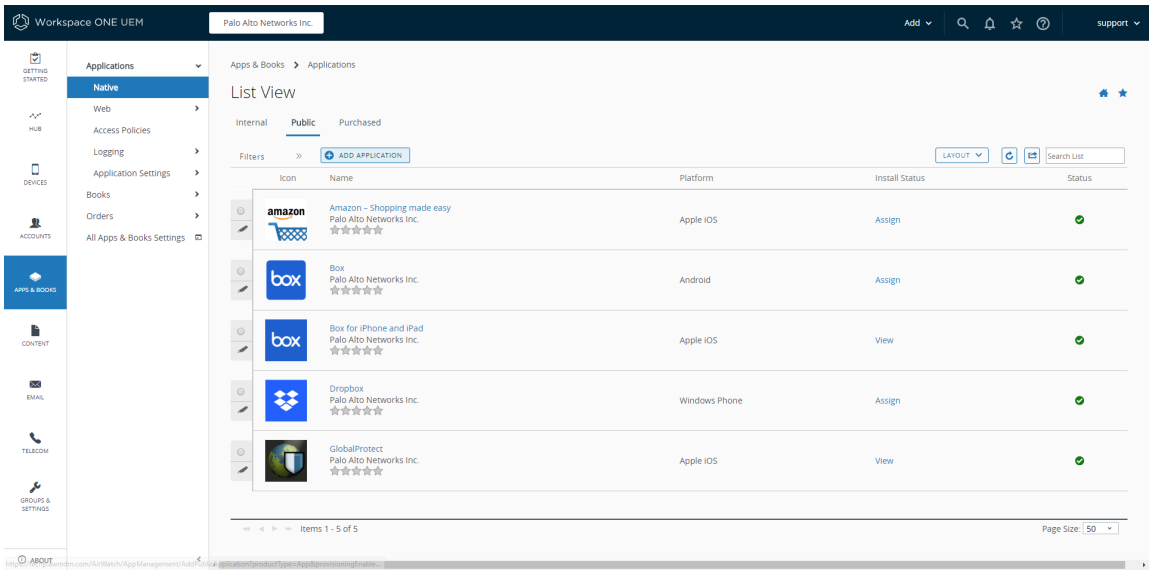
STEP 6 | 変更を**SAVE & PUBLISH (**保存して公開**)**します。

STEP 7 | アプリ単位の VPN 設定を新しい管理対象アプリケーション用に設定するか、既存の管理対象アプリケーションの設定を変更します。

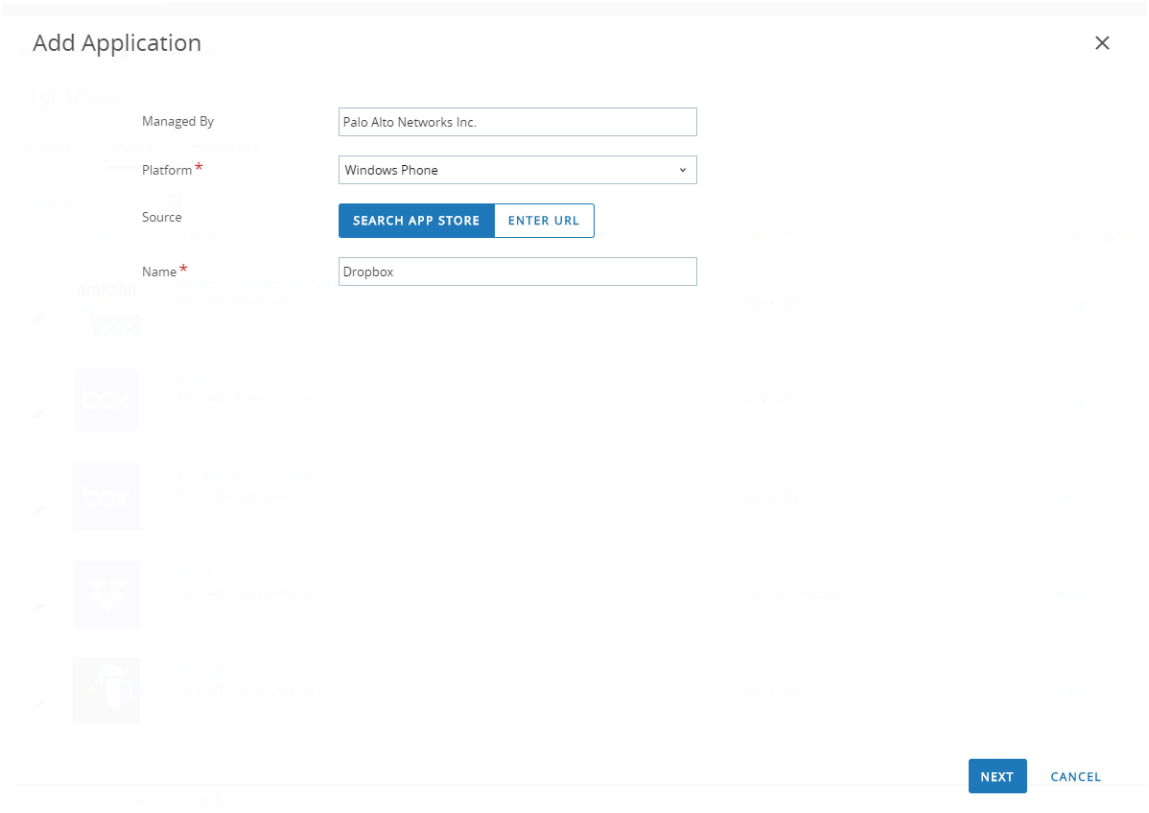
アプリケーション設定を構成し、アプリ単位の VPN を有効にしたら、ユーザーのグループにアプリケーションを公開します。これで、アプリケーションが GlobalProtect VPN トンネル経由でトラフィックを送信できるようになります。

1. **APPS & BOOKS (**アプリおよび本**)** > **Applications (**アプリケーション**)** > **Native (**ネイティブ**)** > **Public (**パブリック**)**を選択します。
2. 新しいアプリケーションを追加するには、**ADD APPLICATION**（アプリケーションの追加）を選択します。既存のアプリケーションの設定を変更するには、Public アプリ

ケーションリストからアプリケーションを探して、行の隣のアクションメニューにある編集（  ）アイコンを選択します。

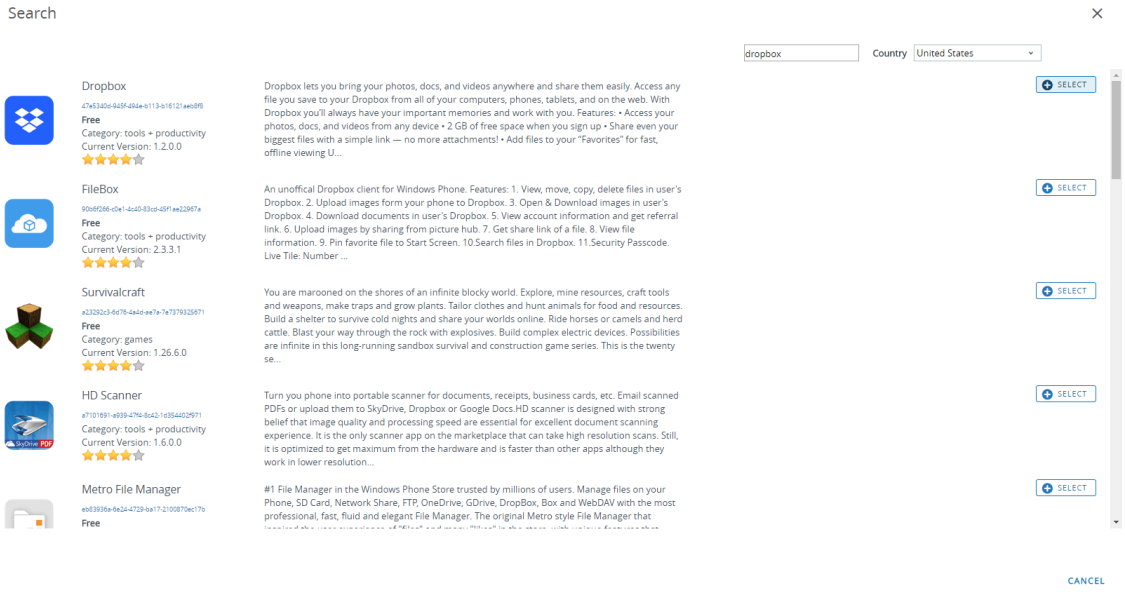


3. **Managed By (**管理者**)**フィールドで、このアプリを管理する組織グループを選択します。
4. **Platform (**プラットフォーム**)**を**Windows Phone**に設定します。
5. アプリを優先的に探す**Source (**ソース**)**を選択します：
   - **SEARCH APP STORE (APP STORE** を検索**)**—アプリの**Name (**名前**)**を入力します。
   - **ENTER URL (URL** を入力**)**—アプリケーションの Microsoft ストア用 URL を入力します（たとえば、URL を使って Dropbox のモバイル アプリを検索するには、https://www.microsoft.com/en-us/p/dropbox-mobile/9wzdncrfj0pkを入力します）。

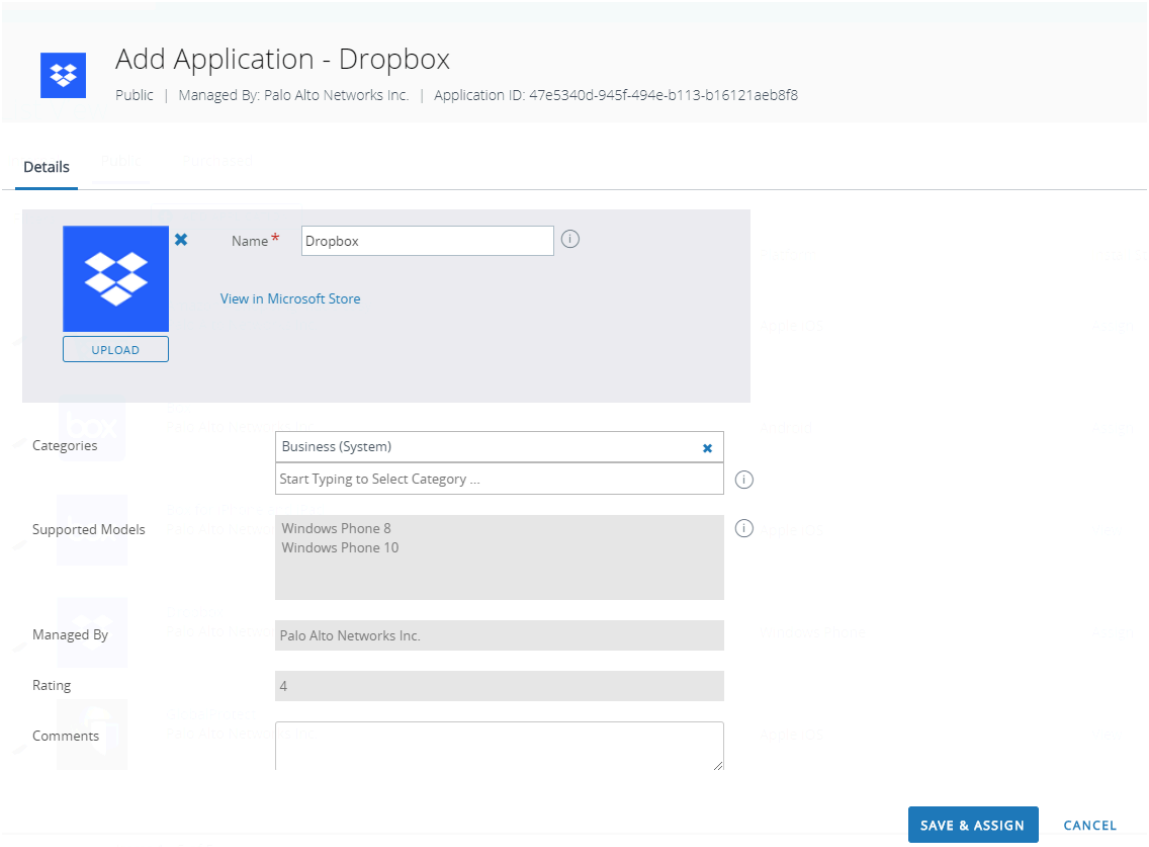


6. **NEXT (次へ)** をクリックします。

   Microsoft ストアで検索する場合は、検索結果のリストからアプリを **SELECT** （選択）する必要があります。

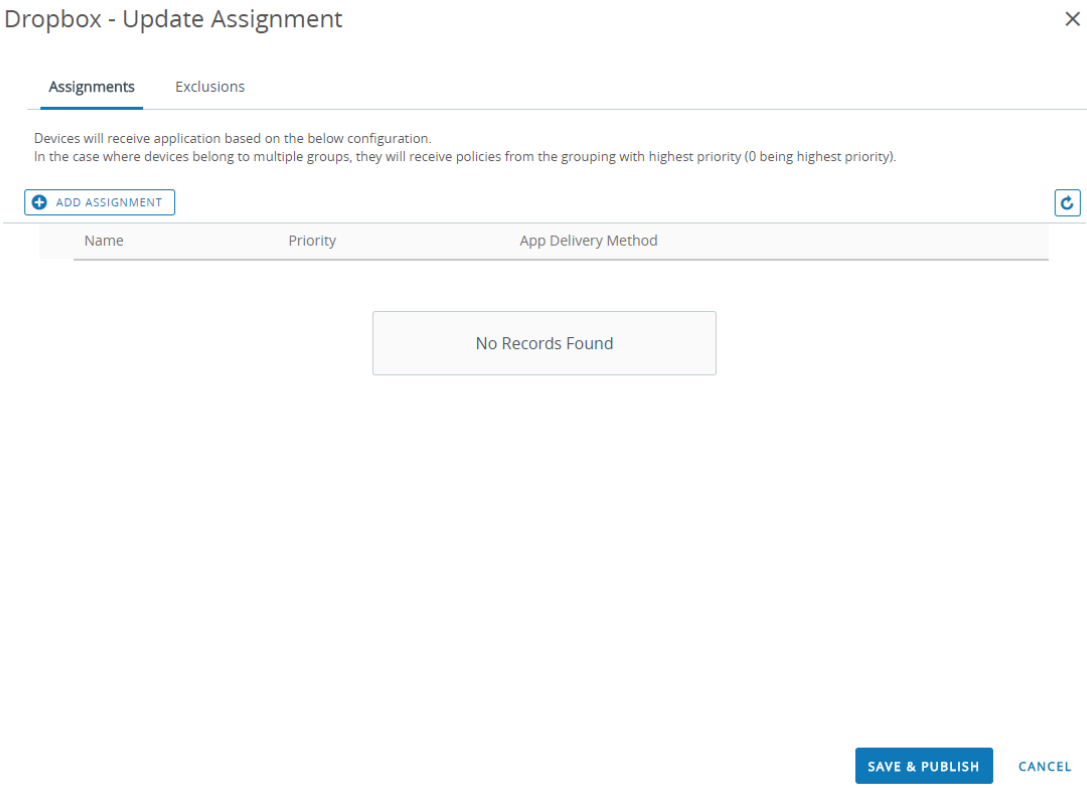


7. Add Application (アプリケーションの追加) ダイアログでアプリの**Name (名前)**が正しいことを確認します。この名前が AirWatch アプリ カタログに表示されます。
8. （任意）AirWatch アプリ カタログでアクセスしやすくなるよう、アプリを事前定義済みあるいはカスタム**Categories (カテゴリ)**に割り当てます。



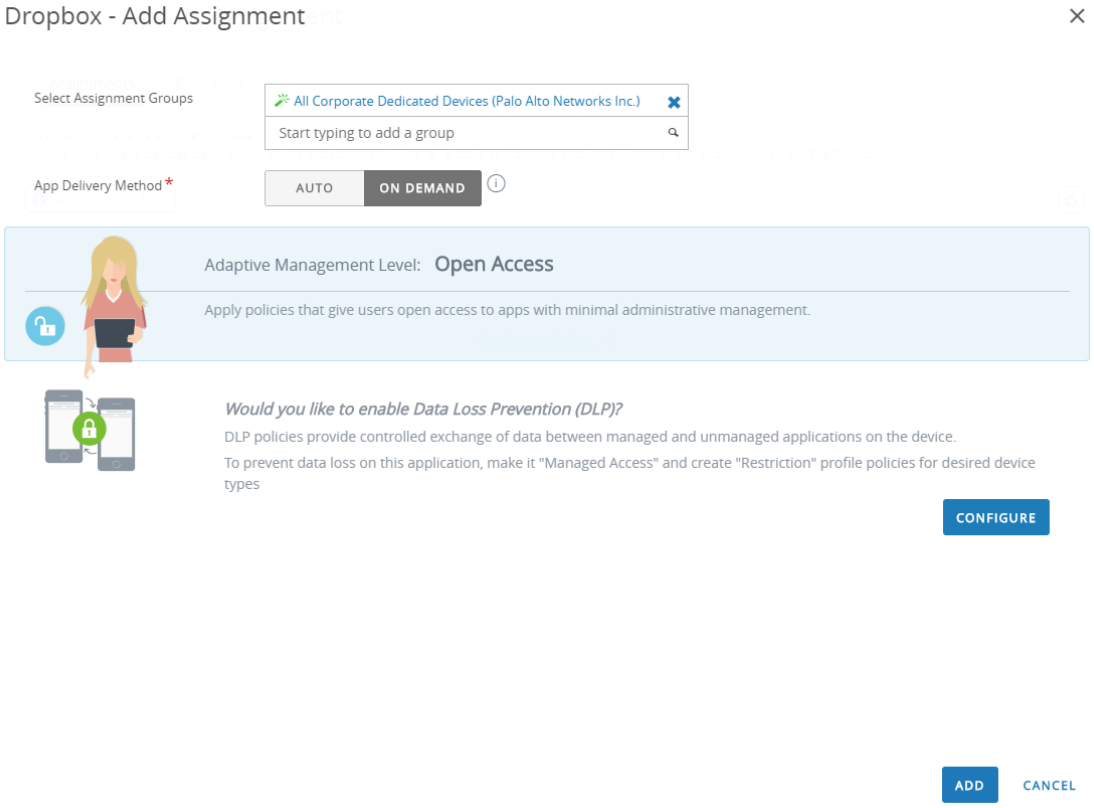
9. 新しいアプリを**SAVE & ASSIGN (**保存して割り当て**)**ます。

10. Update Assignment (割り当ての更新) ダイアログで、**Assignments (**割り当て**)**を選択してから**ADD ASSIGNMENT (**割り当ての追加**)**をクリックし、このアプリにアクセスするスマート グループを追加します。

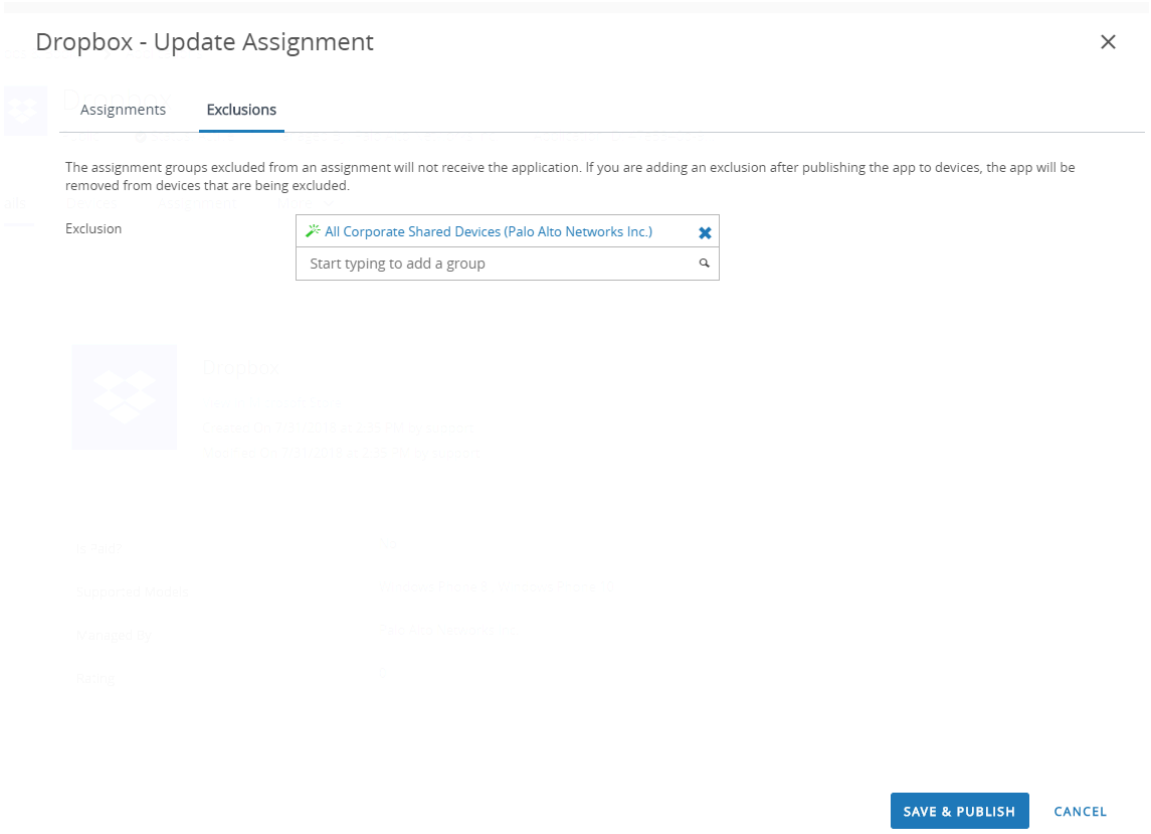


1. **Select Assignment Groups** (割り当てグループの選択)フィールドで、このアプリへのアクセスを許可するスマート グループを選択します。

2. **App Delivery Method** (アプリの配信方法)を選択します。**AUTO** (自動)を選択すると、特定のスマート グループにアプリが自動的にデプロイされます。**ON DEMAND** (オンデマンド)を選択する場合は手動でアプリをデプロイする必要があります。
3. 新しい割り当てを**ADD** （追加）します。



11. （任意）特定のスマート グループがアプリにアクセスできないようにするには、**Exclusions (除外)**を選択してから、除外したいスマート グループを**Exclusion (除外)**フィールドから選択します。



12. 割り当てられたスマート グループに設定を **SAVE & PUBLISH**（保存して公開）します。

STEP 8 | GlobalProtect を接続タイプのプロバイダーとして設定する場合、XML 内の VPN プロファイルを編集します。

XML で直接行う追加の編集を最小限にするために、*VPN* プロファイルの設定をエクスポートする前に設定をレビューします。*VPN* プロファイルをエクスポートした後で設定を変更する必要が生じた場合、*XML* に直接変更を加えるか、*VPN* プロファイルの設定を更新して再度このステップを実施することができます。

1. **Devices** > **Profiles**（プロファイル） > **List View**（リスト ビュー） で、前述のステップで追加した新しいプロファイルの隣にあるラジオ ボタンを選択し、次に表の上部にある **</>XML** を選択します。AirWatch でプロファイルの XML ビューが開きます。
2. プロファイルを **Export**（エクスポート）した後、任意のテキスト エディタで開きます。
3. GlobalProtect の以下の設定を編集します。

- `PluginPackageFamilyName` を指定する `LoclURI` エレメントで、エレメントを次のように変更します:

  `<LocURI>./Vendor/MSFT/VPNv2/PaloAltoNetworks/PluginProfile/PluginPackageFamilyName</LocURI>`

- 続く `Data` エレメントで、値を次のように変更します：

  `<Data>PaloAltoNetworks.GlobalProtect_rn9aeerfb38dg</Data>`

1. エクスポートしたプロファイルに加えた変更を保存します。
2. AirWatch に戻り、**Devices**（デバイス） > **Profiles**（プロファイル） > **List View**（リストビュー） を選択します。
3. 新しいプロファイルを作成（**Add** > **Add Profile** > **Windows** > **Windows Phone** (追加 > プロファイルの追加 > Windows > Windowsフォン)）して名前を付けます。
4. **Custom Settings** > **Configure** (カスタム設定 > 設定)を選択し、編集した設定をコピーアンドペーストします。
5. 変更を**Save & Publish** (保存して公開)します。

STEP 9 | **Devices**（デバイス） > **Profiles**（プロファイル） > **List View**（リスト ビュー）からオリジナルのプロファイルを選択することでオリジナルのプロファイルを消去して、**More Actions**（他の操作） > **Deactivate**（無効化）を選択します。AirWatch により、プロファイルが Inactive（無効）のリストに移動されます。

STEP 10 | 設定のテストを行います。

Microsoft Intune を使用したアプリ単位の VPN 設定

Microsoft Intune とは、中央から一元的にモバイル エンドポイントを管理できるようにする、クラウド ベースのエンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect

アプリケーションにより、デバイス レベルあるいはアプリケーション レベルで、Microsoft Intune が管理するモバイル エンドポイントおよびファイアウォール間で安全に接続を行えるようになります。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

Microsoft Intune を使ってアプリ単位の VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- Microsoft Intune を使用した iOS エンドポイントのアプリ単位の VPN 設定
- Microsoft Intune を使用した Windows 10 UWP エンドポイント用のアプリ単位の VPN 設定

Microsoft Intune を使用した *iOS* エンドポイントのアプリ単位の *VPN* 設定

Microsoft Intune を使用して GlobalProtect VPN アクセスを設定することで管理下のモバイル エンドポイントから内部リソースに簡単にアクセスできるようになります。アプリ単位の VPN 設定において、どの管理アプリケーションが VPN トンネル経由でトラフィックをルーティングできるかを指定できます。管理していないアプリケーションは VPN トンネルを解する代わりにインターネットに直接接続を続けようとします。

次の各作業により、Microsoft Intune を使用して iOS エンドポイント用にアプリ単位の VPN 設定を構成することができます：

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

- Microsoft Intune を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | Microsoft Intune にアプリを追加します。

アプリを監視・設定・保護する前に、アプリを Microsoft Intune に追加しておく必要があります。

- **App type (アプリ タイプ)を iOS**に設定します。
- Microsoft Intune に iOS ストアのアプリを追加します。

STEP 3 | iOS 用にアプリ単位の VPN を設定します。

- アプリ単位の VPN を作成する際、**Platform (プラットフォーム)を iOS**に、**Connection type (接続タイプ)を Palo Alto Networks GlobalProtect**に設定する必要があります。
- アプリを VPN プロファイルに関連付ける際、**VPNS**のドロップダウンリストからアプリ単位の VPN プロファイルを選択します。

Microsoft Intune を使用した *Windows 10 UWP* エンドポイント用のアプリ単位の *VPN* 設定

Microsoft Intune を使用して GlobalProtect VPN アクセスを設定することで管理下のモバイル エンドポイントから内部リソースに簡単にアクセスできるようになります。アプリ単位の VPN 設定において、どの管理アプリケーションが VPN トンネル経由でトラフィックをルーティングできるかを指定できます。管理していないアプリケーションは VPN トンネルを解する代わりにインターネットに直接接続を続けようとします。

次の各作業により、Microsoft Intune を使用して Windows 10 UWP エンドポイント用にアプリ単位の VPN 設定を構成することができます：

STEP 1 | Windows 10 UWP 用 の GlobalProtect アプリケーションをダウンロードします。

- Microsoft Intune を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- Microsoft ストアから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | 証明書プロファイルの設定を行います。

アプリ単位の *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。

STEP 3 | 新しい Windows 10 UWP の VPN プロファイルを作成します。

- **Platform (プラットフォーム)**を**Windows 10 and later (Windows 10 以降)**に設定します。

STEP 4 | Windows 10 UWP エンドポイント用にアプリ単位の VPN 設定を行います。

- **Connection type (接続タイプ)**を**Palo Alto Networks GlobalProtect** に設定します。
- Apps and Traffic rules (アプリおよびトラフィック ルール)領域で、**Associate WIP or apps with this VPN (WIP** またはアプリを **VPN** に関連付ける)オプションを**Associate apps with this connection (**アプリをこの接続に関連付ける)に設定します。**Restrict VPN connection to these apps (**これらのアプリへの **VPN** 接続を制限する)オプションを**Enable (**有効化)してから、VPN 接続を使用させたい関連するアプリを**Add (**追加)します。

MobileIron を使用したアプリ単位の **VPN** 設定

MobileIron とは、中央のコンソールから一元的にモバイル エンドポイントを管理できるようにする、エンタープライズ モビリティ管理プラットフォームのことです。GlobalProtect アプリケーションにより、デバイス レベルあるいはアプリケーション レベルで、MobileIron が管理するモバイル エンドポイントおよびファイアウォール間で安全に接続を行えるようになります。GlobalProtect を保護された接続として使用することで、モバイル エンドポイント上のトラフィックの確認と脅威防止のためのネットワーク安全ポリシーの強制が行われます。

MobileIron を使ってアプリ単位の VPN 設定を構成する方法については、次の各セクションの情報を参照してください：

- MobileIron を使用した iOS エンドポイントのアプリ単位の VPN 設定

MobileIron を使用した *iOS* エンドポイントのアプリ単位の *VPN* 設定

MobileIron を使用して GlobalProtect VPN アクセスを設定することで管理下のモバイル エンドポイントから内部リソースに簡単にアクセスできるようになります。アプリ単位の VPN 設定において、どの管理アプリケーションが VPN トンネル経由でトラフィックをルーティングできるかを指定できます。管理していないアプリケーションは VPN トンネルを解する代わりにインターネットに直接接続を続けようとします。

次の各作業により、MobileIron を使用して iOS エンドポイント用にアプリ単位の VPN 設定を構成することができます：

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

- MobileIron を使用した GlobalProtect モバイル アプリケーションのデプロイ.
- App Storeから直接 GlobalProtect アプリケーションをダウンロードします。

STEP 2 | 証明書設定の追加を行ってから証明書設定を行います。

> アプリ単位の *VPN* 構成では必ず、証明書ベースの認証を使用する必要があります。

STEP 3 | アプリ単位の VPN 設定を追加します。

- 設定タイプを**Per-app VPN (**アプリ単位の **VPN)**に設定します。

STEP 4 | iOS 用にアプリ単位の VPN 設定を行います。

- **Connection Type (**接続タイプ**)**を**Palo Alto Networks GlobalProtect**に設定してから、関連する設定を行います。

WildFire と App Scan の統合の有効化

AirWatch で App Scan を有効化することで、アプリケーションに関する WildFire の脅威インテリジェンスを活用し、Android エンドポイント上のマルウェアを検出することが可能になります。これが有効な場合、AirWatch エージェントは Android エンドポイントにインストールされているアプリのリストを AirWatch に送信します。これは、登録時、その後はあらゆるエンドポイントがチェックアウトする際に実行されます。その後、AirWatch は定期的にクエリを送信して WildFire に判定を求め、その判定に基づいてエンドポイント上でコンプライアンスを確保するためのアクションを実施できるようになります。

STEP 1 | 作業を始める前に、WildFire の API キーを取得します。API キーをまだお持ち出ない場合は、サポートにお問い合わせください。

STEP 2 | AirWatchで**Groups & Settings** > **All Settings** > **Apps** > **App Scan** > **Third Party Integration** (グループおよび設定 > すべての設定 > アプリ > App Scan > サードパーティの統合)を選択します。

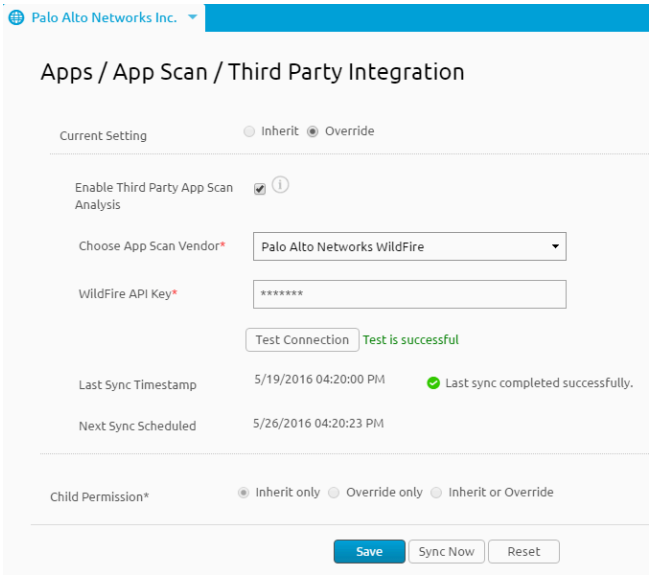
STEP 3 | **Current Setting:**（現在の設定：）を選択します。**Override**（オーバーライド）します。

STEP 4 | **Enable Third Party App Scan Analysis**（サードパーティ **App Scan** 分析を有効化）を選択し、AirWatch と WildFire が通信できるようにします。

STEP 5 | **Choose App Scan Vendor**（**App Scan** のベンダー）のドロップダウンリストから **Palo Alto Networks WildFire** を選択します。

STEP 6 | WildFire の API キーを入力します。

STEP 7 | **Test Connection**（テスト接続）をクリックし、AirWatch が WildFire と通信できることを確認します。テストが成功したらインターネットに接続していることを確認し、API キーを再び入力してもう一度実行します。



STEP 8 | 変更を**Save**（保存）します。AirWatch は、WildFire と通信してアプリケーション ハッシュに対する最新の判定を得るための同期タスクのスケジューリングを行い、定期的にそのタスクを実行します。**Sync Now**（今すぐ同期）をクリックし、WildFire との手動同期を開始します。

macOSエンドポイントのGlobalProtectアプリケーションの通知を抑制する

macOS の GlobalProtect アプリケーションは、kernel（macOS Catalina 10.15.3以前を実行している macOS デバイス）とシステム（macOS Catalina 10.15.4以降と GlobalProtect アプリケーション 5.1.4以降を実行している macOS デバイス）の2種類の拡張機能をサポートしています。GlobalProtect gateway（GlobalProtect ゲートウェイ）で split tunnel（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 接続を適用した場合（GlobalProtect App Customization（GlobalProtect アプリケーションのカスタマイズ）を参照）、 notification message（通知メッセージ）が GlobalProtect アプリケーションに表示されます。このメッセージは、これらの機能が有効になっている GlobalProtect アプリケーションにアクセスするとロードがブロックされていた macOS の kernel 拡張機能またはシステム拡張機能を有効にするようにユーザーに求めます。

GlobalProtect アプリケーション ユーザーが kernel 拡張またはシステム拡張のいずれかを通知を受信すること無しに自動的にロードできるようにするには、サポートされているmobile device management (モバイルデバイス管理 - MDM) を使用して、Airwatch などのその拡張に対するポリシーを作成できます。

macOS エンドポイントの GlobalProtect アプリケーションで通知を抑制する方法については、以下のセクションを参照してください:

- macOSエンドポイントのGlobalProtectアプリケーション内の、Kernel拡張機能を有効化する
- macOSエンドポイントのGlobalProtectアプリケーション内の、システム拡張機能を有効化する

macOSエンドポイントのGlobalProtectアプリケーション内の、Kernel拡張機能を有効化する

macOS 10.13 以降、Apple は、kernel 拡張機能を実行する前にその承認をユーザーに要求するソフトウェア変更を導入しました。

ユーザーは macOS 上の kernel 拡張機能を手動で有効にできますが (**System Preferences**（システム設定） > **Security & Privacy**（セキュリティとプライバシー）に移動して、 kernel 拡張機能の **Allow**（許可）を選択する）、Qualified MDM vendor（認定 MDM ベンダー） を使用してポリシーを作成し、 kernel 拡張機能を自動承認できます。このプロセスは Apple Technical Note TN2450 で説明されています。

以下のワークフローは、Airwatch を使用してテストされています。

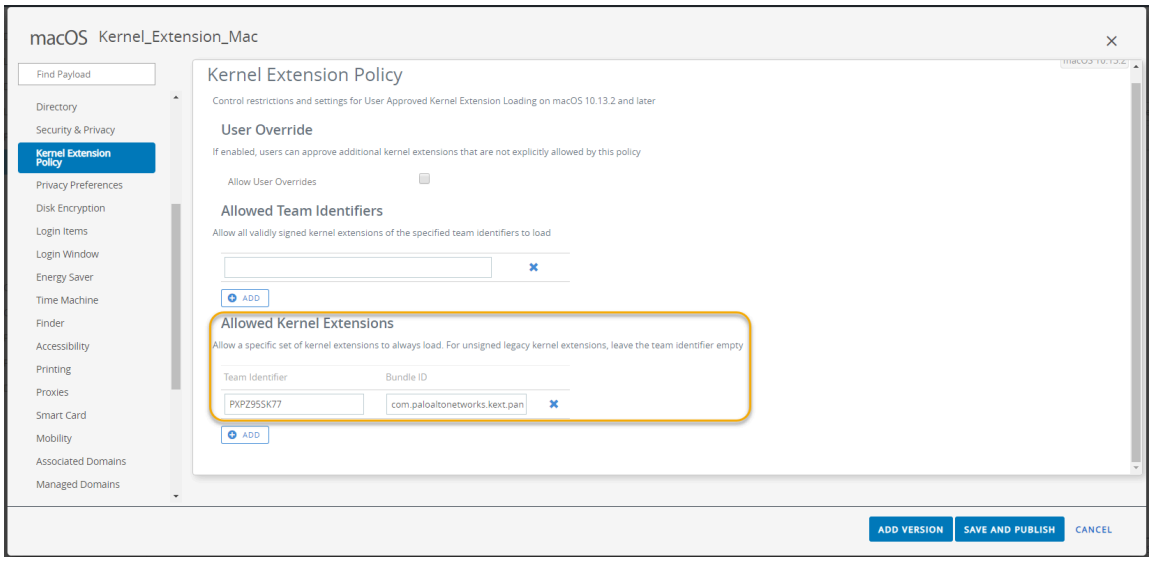
STEP 1 | kernel 拡張機能ポリシーを作成します。

1. AirWatch に管理者としてログインします。
2. **Devices**（デバイス） > **Profiles & Resources**（プロファイルとリソース） > **Profiles**（プロファイル）の順に選択し、ドロップダウンメニューから **Add**（追加） > **Add Profile**（プロファイルの追加） を選択します。
3. **Add Profile**（プロファイルの追加）領域で、 **Apple macOS** をクリックしてから、**Device Profile**（デバイスプロファイル） アイコンをクリックします。
4. **General**（一般） 領域で、プロファイル名を入力します。

   リスト内では、既存の kernel 拡張機能プロファイル（**Devices**（デバイス） > **Profiles & Resources**（プロファイルとリソース） > **Profiles**（プロファイル））を選択することもできます。

STEP 2 | kernel 拡張機能を追加し、関連するポリシーを macOS デバイスに配布します。

1. **Kernel Extension Policy**（**Kernel** 拡張機能ポリシー）を選択します。
2. GlobalProtect アプリケーションで使用される **Team Identifier**（チーム識別子）を入力します (**PXPZ95SK77**)。
3. **Bundle ID**（バンドル **ID**）を入力します (**com.paloaltonetworks.kext.pangpd**)。



4. **Save and Publish**（保存して公開）をクリックして変更内容を保存します。

macOSエンドポイントのGlobalProtectアプリケーション内の、システム拡張機能を有効化する

macOS 10.15.4 以降、Apple は kernel 拡張機能のサポートを制限しました。GlobalProtect アプリケーションは kernel 拡張機能の代わりにシステム拡張機能を使用します。ユーザーは、システム拡張機能を使用する前にそれを承認する必要があります。

AirWatch を使用してシステム拡張を自動的に承認するようにプロファイルを設定するには、以下の手順を使用します。この設定は AirWatch でテストされていますが、任意の Qualified MDM vendor（認定 MDM ベンダー）を使用してこのプロファイルの作成と実装を行うことができます。

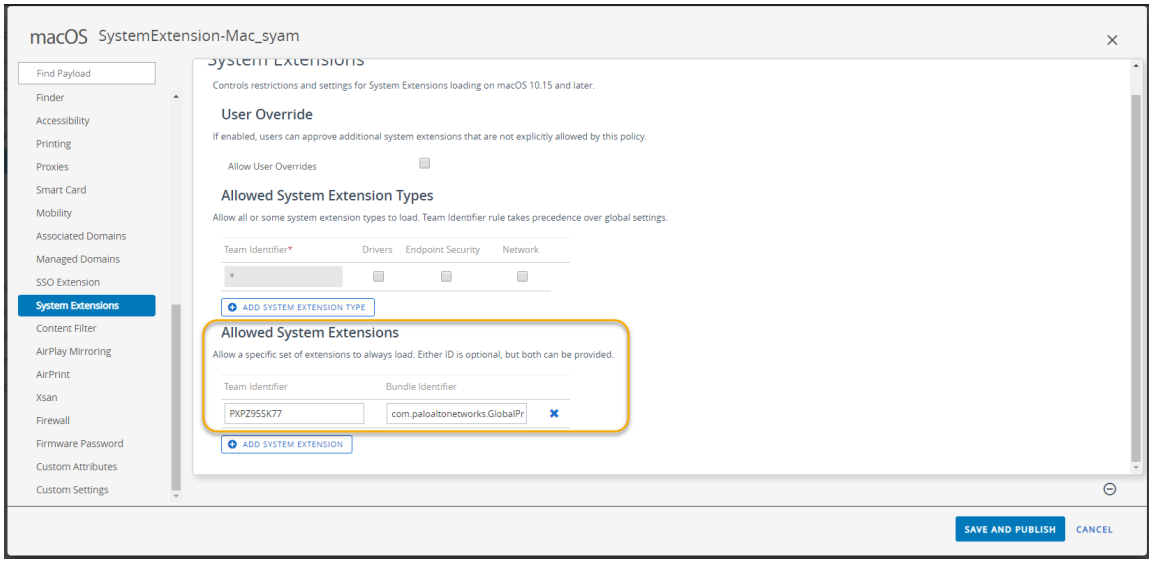
STEP 1 | システム拡張機能のプロファイルを作成します。

1. AirWatch に管理者としてログインします。
2. **Devices**（デバイス） > **Profiles & Resources**（プロファイルとリソース） > **Profiles**（プロファイル）の順に選択し、ドロップダウンメニューから **Add**（追加） > **Add Profile**（プロファイルの追加） を選択します。
3. **Add Profile**（プロファイルの追加）領域で、 **Apple macOS** をクリックしてから、**Device Profile**（デバイスプロファイル） アイコンをクリックします。
4. **General**（一般） 領域で、プロファイル名を入力します。

   リスト内では、既存のシステム拡張機能プロファイル（**Devices**（デバイス） > **Profiles & Resources**（プロファイルとリソース） > **Profiles**（プロファイル））を選択することもできます。

STEP 2 | システム拡張機能を追加します。

1. **System Extensions**（システム拡張機能）を選択します。
2. GlobalProtect アプリケーションで使用される **Team Identifier**（チーム識別子）を入力します (**PXPZ95SK77**)。
3. **Bundle Identifier**（バンドル識別子）を入力します(**com.paloaltonetworks.GlobalProtect.client.extension**)



4. **Save and Publish**（保存して公開）をクリックして変更内容を保存します。

他のサードパーティ製の MDM を使用した GlobalProtect アプリケーションの管理

サポートされているサードパーティの MDM ベンダーを使用していない場合、他のサードパーティ製の MDM システムを使って GlobalProtect アプリケーションをデプロイ・管理することができます：

- iOS 用 GlobalProtect アプリケーションの設定
  - (例:GlobalProtect iOS アプリケーションのデバイスレベルの VPN の設定
  - (例:GlobalProtect iOS アプリケーションのレベルの VPN の設定
- Android 用 GlobalProtect アプリケーションの設定
  - (例:VPN の設定
  - (例:VPN 設定の削除

iOS 用 GlobalProtect アプリケーションの設定

サードパーティーのMDMシステムは企業リソースへのアクセスを許可する設定をプッシュ可能で、エンドポイントの制限を適用するメカニズムを提供しますが、モバイル エンドポイントとサービス間の接続は保護しません。アプリが安全な接続を確立できるようにするには、エンドポイントで VPN サポートを有効にする必要があります。

以下の表は、サードパーティーの MDM システムを使用して設定可能な一般的な設定です。

設定	説明	Value（値）
接続タイプ	接続タイプがポリシーによって有効になっています。	**Custom SSL**
識別子	リバース DNS 書式のカスタム SSL VPN の識別子。	**com.paloaltonetworks.globalprotect.vp**
サーバー	GlobalProtect ポータルのホスト名または IP アドレス。	**<hostname or IP address>** 以下に例を示します：gp.paloaltonetworks.com
アカウント	接続認証のためのユーザーアカウント。	**<username>**ユーザー名
User Authentication ユーザー認証	接続の認証タイプ。	**Certificate | Password**
認証情報	（証明書ユーザー認証のみ）接続を認証する認証情報。	**<credential>** 以下に例を示します: **clientcredial.p12**

設定	説明	Value（値）
VPN オンデマンド有効化	（任意）接続およびオンデマンドアクションを確立するドメインとホスト名： • 常に接続を確立 • 接続を確立しない • 必要に応じて接続を確立	**<domain and hostname and the on-demand action>** 以下に例を示します。 gp.acme.com; Never establish

例:**GlobalProtect iOS** アプリケーションのデバイスレベルの **VPN** の設定

以下の例は iOS 用 GlobalProtect アプリケーションのデバイスレベル VPN 設定を検証するために使用できる VPN ペイロードを含む XML 設定を示します。

```
<?xml version="1.0"
encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample Device Level VPN)</string>
<key>PayloadIdentifier</key>
<string>Sample Device Level VPN.vpn</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadType</key>
<string>com.apple.vpn.managed</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011d</string>
<key>UserDefinedName</key>
<string>Sample Device Level VPN</string>
<key>Proxies</key>
<dict/>
<key>VPNType</key>
<string>VPN</string>
<key>VPNSubType</key>
<string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
<key>IPv4</key>
<dict>
<key>OverridePrimary</key>
<integer>0</integer>
</dict>
<key>VPN</key>
```

```
<dict>
<key>RemoteAddress</key>
<string>cademogp.paloaltonetworks.com</string>
<key>AuthName</key>
<string></string>
<key>DisconnectOnIdle</key>
<integer>0</integer>
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>OnDemandRules</key>
<array>
<dict>
<key>Action</key>
<string>Connect</string>
</dict>
</array>
<key>AuthenticationMethod</key>
<string>Password</string>
</dict>
<key>VendorConfig</key>
<dict>
<key>AllowPortalProfile</key>
<integer>0</integer>
<key>FromAspen</key>
<integer>1</integer>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Sample Device Level VPN</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadDescription</key>
<string>Profile Description</string>
<key>PayloadIdentifier</key>
<string>Sample Device Level VPN</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011c</string>
<key>PayloadRemovalDisallowed</key>
<false/>
</dict>
</plist>
```

例:**GlobalProtect iOS** アプリケーションのレベルの **VPN** の設定

以下の例は iOS 用 GlobalProtect アプリケーションのアプリケーション レベル VPN 設定を検証するために使用できる VPN ペイロードを含む XML 設定を示します。

```
<?xml version="1.0"
encoding="UTF-8"?>
```

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://
www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Configures VPN settings, including authentication.</string>
<key>PayloadDisplayName</key>
<string>VPN (Sample App Level VPN)</string>
<key>PayloadIdentifier</key>
<string>Sample App Level VPN.vpn</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadType</key>
<string>com.apple.vpn.managed.applayer</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>VPNUUID</key>
<string>cGFuU2FtcGxlIEFwcCBMZXZlbCBWUE52cG5TYW1wbGUgQXBwIExldmVsIFZQTg==</
string>
<key>SafariDomains</key>
<array>
<string>*.paloaltonetworks.com</string>
</array>
<key>PayloadUUID</key>
<string>54370008-205f-7c59-0000-01a1</string>
<key>UserDefinedName</key>
<string>Sample App Level VPN</string>
<key>Proxies</key>
<dict/>
<key>VPNType</key>
<string>VPN</string>
<key>VPNSubType</key>
<string>com.paloaltonetworks.GlobalProtect.vpnplugin</string>
<key>IPv4</key>
<dict>
<key>OverridePrimary</key>
<integer>0</integer>
</dict>
<key>VPN</key>
<dict>
<key>RemoteAddress</key>
<string>cademogp.paloaltonetworks.com</string>
<key>AuthName</key>
<string></string>
<key>OnDemandMatchAppEnabled</key>
<integer>1</integer>
<key>OnDemandEnabled</key>
<integer>1</integer>
<key>DisconnectOnIdle</key>
<integer>0</integer>
<key>AuthenticationMethod</key>
<string>Password</string>
</dict>
```

```
<key>VendorConfig</key>
<dict>
<key>OnlyAppLevel</key>
<integer>1</integer>
<key>AllowPortalProfile</key>
<integer>0</integer>
<key>FromAspen</key>
<integer>1</integer>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Sample App Level VPN</string>
<key>PayloadOrganization</key>
<string>Palo Alto Networks</string>
<key>PayloadDescription</key>
<string>Profile Description</string>
<key>PayloadIdentifier</key>
<string>Sample App Level VPN</string>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadUUID</key>
<string>5436fc94-205f-7c59-0000-011c</string>
<key>PayloadRemovalDisallowed</key>
<false/>
</dict>
</plist>
```

Android 用 GlobalProtect アプリケーションの設定

Android For Work データ制限対応のどのサードパーティーのモバイル デバイス管理（MDM）システムからでも Android For Work エンドポイント上で GlobalProtect アプリケーションをデプロイおよび設定できます。

Android エンドポイント上で、GlobalProtect ゲートウェイで設定したアクセスルートに基づきトラフィックは VPN トンネル経由でルーティングされます。Android For Work を管理するサードパーティーのモバイル エンドポイント マネージャーから、VPN トンネル経由でルーティングされるトラフィックを再建策できます。

エンドポイントが企業所有の環境では、エンドポイント所有者はエンドポイントにインストールされたすべてのアプリケーションを含むエンドポイント全体を管理します。デフォルトでは、すべてのインストール済みアプリケーションがゲートウェイで設定したアクセスルートに基づきトラフィックを送信できます。

自分所有のデバイスを持ち込む（BYOD）環境では、エンドポイントは企業所有ではなく仕事と個人のアプリケーションを分けるために Work Profile を使います。デフォルトでは、Work Profile で管理されたアプリのみがゲートウェイで設定したアクセスルートに基づきトラフィックを送信できます。個人のエンドポイントにインストール済みのアプリは Work Profile にインストールされた管理 GlobalProtect アプリに設定された VPN トンネル経由でトラフィックを送信できません。

さらに小さなアプリケーションからトラフィックをルーティングするには、Per-App VPN をオンにすれば、 GlobalProtect のみで特定管理アプリケーションからトラフィックをルーティングできます。Per-App VPN については、VPN トンネル経由でトラフィックをルーティングすることから特定の管理対象アプリケーションの許可リスト化およびブロックリスト化ができます。

VPN 設定の一環として、ユーザーが VPN に接続する方法を指定することもできます。接続方法を **user-logon**（ユーザー ログオン）に設定すると、 GlobalProtect アプリは自動で接続を確立します。接続方法を **on-demand**（オンデマンド）に設定すると、自動で接続を確立します。

MDM で定義されている *VPN*　接続方式は、*GlobalProtect* ポータル クライアント設定で定義されている接続方式よりも優先されます。

VPN 設定を削除することで自動的に GlobalProtect アプリケーションを元の構成設定に戻します。

Android 用に GlobalProtect アプリケーションを設定するには、以下の Android App 制限を設定します。

鍵	値タイプ	説明	例
Portal（ポータル）	文字列	ポータルの IP アドレスまたは完全修飾ドメイン名（FQDN）。	**10.1.8.190**
ユーザー名	文字列	ユーザーのユーザー名。	**john**
パスワード	文字列	ユーザーのパスワード。	**Passwd!234**
mobile_id	文字列	モバイルデバイスを一意に識別するためにサードパーティの MDM サービスで設定されたモバイル ID。GlobalProtect はこのモバイルIDを使用してデバイス情報を取得します。	**5188a8193be43f42d332dde5cb2c941e**
証明書	文字列（Base64）	エージェントとポータルの認証に使用されるクライアント証明書（証明書）。	**DAFDSaweEWQ23wDSAFD….**
client_certificate_passphrase	文字列	クライアント証明書に関連付けられたキー。	**PA$$W0RD$123**
app_list	文字列	Per-App VPN の特定の設定を指定します。許可リストまたはブロックリストのいずれかの文字列を始め、セミコロンで分けたアプリケーション名の配列に	**allow list | block list: com.google.calendar;**

鍵	値タイプ	説明	例
		従います。許可リストはネットワーク通信に VPN トンネル を使うアプリケーションを指定します。許可リストにない、またはブロックリストにあるその他のアプリケーションのネットワークトラフィックは VPN トンネル を通りません。	**com.android.email; com.android.chrome**
connect_method	文字列	ユーザーログオンは、Windows 証明書を使用してユーザーを GlobalProtect ポータルに自動的に接続するか、オンデマンドでユーザーをゲートウェイに手動で接続します。	**user-logon | on-demand**
remove_vpn_config_via_restriction	ブール値	すべての GlobalProtect VPN 設定情報を恒久的に削除します。	**true | false**

例:**VPN** の設定

```
private static String RESTRICTION_PORTAL
= "portal";
private static String RESTRICTION_USERNAME = "username";
private static String RESTRICTION_PASSWORD = "password";
private static String RESTRICTION_CONNECT_METHOD = "connect_method";
private static String RESTRICTION_CLIENT_CERTIFICATE
= "client_certificate";
private static String RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE
= "client_certificate_passphrase";
private static String RESTRICTION_APP_LIST = "app_list";
private static String RESTRICTION_REMOVE_CONFIG =
 "remove_vpn_config_via_restriction";

Bundle config = new Bundle();
config.putString(RESTRICTION_PORTAL, "192.168.1.1");
config.putString(RESTRICTION_USERNAME, "john");
config.putString(RESTRICTION_PASSWORD, "Passwd!234");
config.putString(RESTRICTION_CONNECT_METHOD, "user-logon");
config.putString(RESTRICTION_CLIENT_CERTIFICATE,
 "DAFDSaweEWQ23wDSAFD….");
config.putString(RESTRICTION_CLIENT_CERTIFICATE_PASSPHRASE,
"PA$$W0RD$123");
config.putString(RESTRICTION_APP_LIST, "allow
 list:com.android.chrome;com.android.calendar");
```

```
DevicePolicyManager dpm = (DevicePolicyManager)
getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.getComponentName(thi
"com.paloaltonetworks.globalprotect", config);
```

例:**VPN** 設定の削除

```
Bundle config = new Bundle();
config.putBoolean(RESTRICTION_REMOVE_CONFIG, true );
DevicePolicyManager dpm = (DevicePolicyManager)
getSystemService(Context.DEVICE_POLICY_SERVICE);
dpm.setApplicationRestrictions(EnforcerDeviceAdminReceiver.
getComponentName(this),"com.paloaltonetworks.globalprotect",
config);
```

IoTデバイス向けGlobalProtect

GlobalProtect for IoT では、IoT デバイスからのトラフィックを保護し、セキュリティポリシーの施行を IoT デバイスに拡張できます。GlobalProtect for IoT のセットアップ後、GlobalProtect アプリケーションは、クライアント認証ならびにユーザー名とパスワード（オプション）を使用して GlobalProtect ポータルまたはゲートウェイを認証します。認証に成功すると、GlobalProtect アプリケーションは IPSec トンネルを確立します。IPSec を使用する接続に失敗する場合、GlobalProtect アプリケーションを設定して SSL トンネルをフォールバックすることができます。features supported by OS for IoT devices（IoT デバイスの OS 上の対応機能）の一覧を確認したい場合は、Palo Alto Networks Compatibility Matrix（Palo Alto Networks 互換性マトリクス）を参照してください。

IoT用GlobalProtect の要件

GlobalProtect for IoT の要件は以下の通りです:

- Prisma Access または GlobalProtect サブスクリプションのいずれか
- PAN-OS 9.1 を実行しているファイアウォール (今すぐアップグレード)
- 以下のオペレーティング システムの内の1つ:
  - Android
  - Raspbian
  - Ubuntu
  - Windows IoT Enterprise
- 128MB の RAM
- 4GB のストレージ
- x86 および ARMv7 または ARMv5 プロセッサ
- CLI または WebDM からのスナップ アプリケーション パッケージを使用したインストール

GlobalProtectポータルとIoTデバイス用ゲートウェイを設定する

STEP 1 | 次をレビュー IoT用GlobalProtect の要件。

STEP 2 | IoT用のアプリをサポートするように GlobalProtect ゲートウェイを設定します。

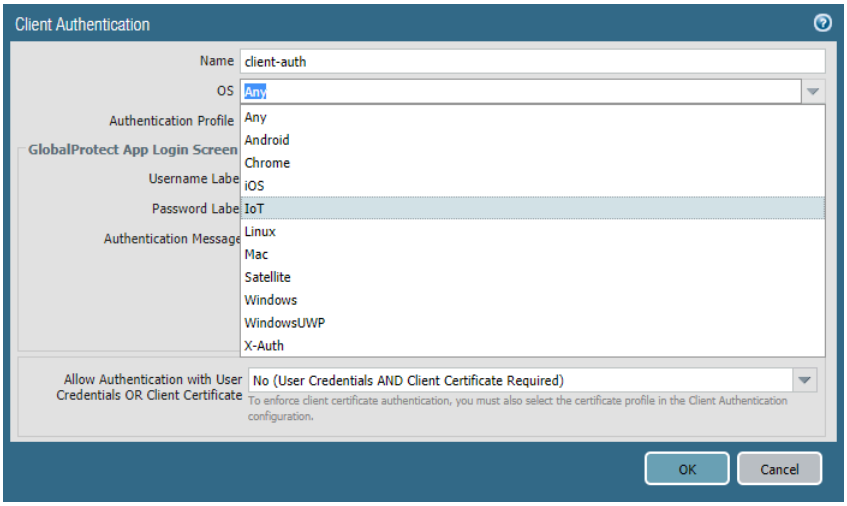
1. GlobalProtect ゲートウェイをセットアップするための前提条件タスクを完了します。
2. IoT用の GlobalProtect アプリケーションをサポートする各ゲートウェイに GlobalProtect サブスクリプションをインストールします。Prisma Access を使用する場合、GlobalProtectサブスクプションは不要です。
3. お使いのIoTデバイスのゲートウェイ設定をカスタマイズします:

   ゲートウェイを設定するときに、特に IoT に適用されるクライアント認証設定を指定できます。たとえば、2要素認証を使用するようにWindows および macOS エンドポイントを構成し、証明書ベースの認証を使用するように IoT デバイスを要求できます。

   また、特定の IP プール、アクセスルート、スプリット トンネリングなど、サポートされているネットワークとクライアントの設定を IoT デバイス用に構成することもできます。

   1. **Network**（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ）の順に選択し、ゲートウェイ設定を選択するか **Add**（追加）します。
   2. IoT デバイスのクライアント認証設定を追加します:
      1. **Authentication**（認証）を選択し、新しいクライアント認証設定を**Add**（追加）します。
      2. クライアント認証設定を識別するための**Name**（名前）を入力し、**OS** を **IoT** に設定し、このゲートウェイで認証ユーザーに使用する**Authentication Profile**（認証

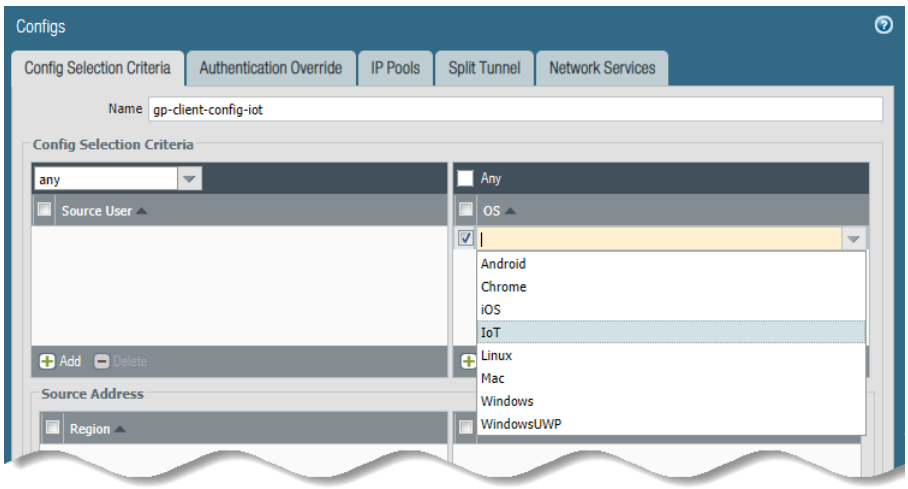
プロファイル）を指定します。クライアント証明書認証を有効にするプロファイルを選択します。



3. **OK** をクリックします。

3. IoT エンドポイントのみに適用する、特定のクライアント設定を構成するには、新しい Client Settings（クライアント設定）を構成します:

   1. **Agent**（エージェント）を選択して、新しいクライアント設定構成を **Add**（追加）します。
   2. 必要な場合は、クライアント認証設定を構成します。
   3. **User/User Group**（ユーザー/ユーザーグループ）を選択してから、OS を **Add**（追加）し、**IoT** を選択します。



   4. **OK** をクリックします。

4. **OK** をクリックします。
5. 設定を **Commit**（コミット）します。

STEP 3 | IoT デバイス用の GlobalProtect アプリケーションをサポートするために、ポータルを設定します。

IoT デバイスをサポートするには、GlobalProtect アプリケーションが接続できる1つ以上のゲートウェイを設定してから、ポータルとアプリケーションの設定を構成する必要があります。ポータルは、設定情報と使用可能なゲートウェイに関する情報をアプリケーションに送信します。GlobalProtect ポータルから設定を受信した後、アプリケーションはクライアント設定にリストされているゲートウェイを検出し、最適なゲートウェイを選択します。以下のワークフローを使用して、IoT デバイス用のGlobalProtect アプリケーションをサポートするように GlobalProtect ポータルを設定します。

1. すでに設定が済んでいる場合は、GlobalProtect ポータルをセットアップするための前提条件タスクを完了します。
2. ポータルに対して認証する IoT デバイスのクライアント設定を定義します。
   1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） の順に選択し、ポータルの設定を選択します。
   2. ユーザーがポータルにアクセスするときに IoT デバイスに適用されるクライアント認証設定を構成します:
      1. **Authentication**（認証）を選択し、新しいクライアント認証設定を**Add**（追加）します。
      2. **Name**（名前）を入力してクライアント認証設定を識別し、**OS** を **IoT** に設定し、このポータルで認証ユーザーに使用する Authentication Profile（認証プロファイル）を指定します。クライアント証明書認証を有効にするプロファイルを選択します。
3. IoT デバイスのエージェント設定をカスタマイズします。

   環境に応じて、既存の設定を変更するか、新しい設定を作成して下さい。たとえば、OS 固有のゲートウェイを使用する場合、または IoT デバイスに固有のホスト情報を収集する場合は、新しいエージェント設定を作成することを検討してください。

   サポートされている機能の詳細については、Palo Alto Networks 互換性マトリックスの IoT デバイス用OSがサポートしている機能一覧を参照してください。

   1. GlobalProtect エージェント設定を定義する：
   2. **Agent (**エージェント**)** を選択し、既存のエージェント設定を選択するか、新しい設定を **Add (**追加**)** します。
   3. IoT デバイスの認証設定を構成します。
   4. **User/User Group**（ユーザー/ユーザーグループ）を選択してから、**OS** を Add（追加）し、**IoT** を選択します。
   5. この設定が行われたユーザーが接続できる外部ゲートウェイを指定します。
   6. （オプション） **App**（アプリケーション）を選択し、該当の IoT 用 GlobalProtect アプリケーションのポータル設定をカスタマイズします。GlobalProtect アプリケーションによって、IoT に適用されない設定は破棄されます。オペレーティングシステ

ムがサポートする機能の一覧については、Palo Alto Networks 互換性マトリックスの IoT デバイス用OS がサポートしている機能一覧を参照してください。

7. **OK** を 2 回クリックします。
8. 設定を **Commit**（コミット）します。

4. IoT デバイス上で、Enforce Policies（ポリシーの強制）を実行します(**Objects** > **GlobalProtect** > **HIP Objects**)。

   IoT デバイスに固有のホスト情報を使用して HIP オブジェクトを作成し、それを任意の HIP プロファイルの一致条件に使用できるようになりました。これでHIP プロファイルをポリシールールの一致条件として使用して、対応するセキュリティポリシーを適用できます。

   1. **General**（一般） > **Host Info**（ホスト情報） > **OS** を選択します。
   2. **Contains** > **IoT**（IoT を追加）を選択します。
   3. **OK** をクリックします。
   4. 必要に応じて HIP オブジェクトを追加します。
   5. HIP ベースのポリシー適用の設定。

STEP 4 | IoT 用 GlobalProtect アプリケーションをインストールしてセットアップします。

お使いのIoT デバイスのオペレーティングシステム用に提供されている手順を使用します。

- AndroidでのIoT用GlobalProtectのインストール
- RaspbianでのIoT用GlobalProtectのインストール
- UbuntuでのIoT用GlobalProtectのインストール
- WindowsでのIoTデバイス用GlobalProtectのインストール

AndroidでのIoT用GlobalProtectのインストール

Android デバイスで GlobalProtect for IoT を使用するには、アプリケーションと GlobalProtect 設定をシステム アプリケーションとして Android オペレーティング システム イメージにビルドする必要があります。GlobalProtect をヘッドレス モードで動作させるには、GlobalProtect アプリケーション パッケージを使用して事前設定ファイルをデプロイする必要があります。

STEP 1 | GlobalProtect.apk をビルド済みのシステム アプリケーションとして Android OS イメージに追加します。

1. Support Siteで、**Updates**（更新） > **Software Updates**（ソフトウェア更新）を選択して、GlobalProtect APK をダウンロードします。
2. `android_src_tree_root/packages/app/` ディレクトリ内で、APK ファイルをデコードします。

   デコーダーがアプリケーションを GlobalProtect フォルダに展開します。
3. GlobalProtect フォルダで、 `Android.mk` ファイルを作成します。このファイルは、エンコーダがビルド システムに使用するソースと共有ライブラリを定義します。

   ファイルを編集して以下を含めます:

   ```
   LOCAL_PATH := $(call my-dir)
   include $(CLEAR_VARS)
   LOCAL_MODULE_TAGS := optional
   LOCAL_MODULE := GlobalProtect
   LOCAL_SRC_FILES := $(LOCAL_MODULE).apk
   LOCAL_MODULE_CLASS := APPS
   LOCAL_MODULE_SUFFIX := $(COMMON_ANDROID_PACKAGE_SUFFIX)
   LOCAL_CERTIFICATE := PRESIGNED
   include $(BUILD_PREBUILT)
   ```
4. `android_src_tree_root/vendor/` 内の追加の MK ファイルについては、以下の行を追加します:

   ```
   PRODUCT_PACKAGES += GlobalProtect
   ```
5. IoT デバイスをサポートする CPU アーキテクチャに応じて、libgpjni.so を `/system/lib` または `/system/lib64` のいずれかに追加します。libgpjni.so ファイルは、GlobalProtect.apk が apktool によってデコードされた後に lib ディレクトリから取得可能です。

STEP 2 | VPN 接続の権限リクエスト ポップアップを事前承認するために、Android Framework ソース コードを修正します。

`android_src_tree_root/frameworks/base/services/core/java/com/android/server/connectivity/Vpn.java` ファイルを編集して、以下のコード セグメントを追加します:

```
private boolean isVpnUserPreConsented(String packageName) {
```

```
    if (“com.paloaltonetworks.globalprotect”.equals(packageName)){
        Log.v(TAG, "IoT, isVpnUserPreConsented always true");
    return true;
    }
    AppOpsManager appOps =
        (AppOpsManager)
 mContext.getSystemService(Context.APP_OPS_SERVICE);

    // Verify that the caller matches the given package and has
 permission to activate VPNs.
    return
 appOps.noteOpNoThrow(AppOpsManager.OP_ACTIVATE_VPN,Binder.getCallingUid(),
        packageName) == AppOpsManager.MODE_ALLOWED;
    }
}
```

STEP 3 | Android 8.0 以降のリリースでは、Android の動作をカスタマイズして、通知バーの GlobalProtect アイコンを抑制します。

`android_src_tree_root/frameworks/base/services/core/java/com/android/server/am/ActiveServices.java` ファイルを編集して、以下のコード セグメントを追加します。

```
if ( r.packageName.equals("com.paloaltonetworks.globalprotect") ) {
    Slog.d(TAG, "not to show the foreground service running
 notification for IoT");
} else {
    r.postNotification();
}
```

STEP 4 | Android IoT デバイスの事前デプロイしたい VPN 設定を設定します。

1. 以下のフォーマットで設定ファイル (`globalprotect.conf`) を作成し、GlobalProtect ポータルの IP アドレスを編集します。認証設定は次のいずれかです: ユーザー名とパスワード、またはクライアント証明書パス (client-cert-path) と pass-phrase ファイル (client-cert-passphrase)。

   Username-password ベースの認証

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
    <PanSetup>
                <Portal>192.168.1.23</Portal>
    </PanSetup>
        <Settings>
                <head-less>yes</head-less>
                <os-type>IoT</os-type>
                <username>user1</username>
                <password>mypassw0rd</password>
                <log-path-service>/home/gptest/Desktop/data/
gps</log-path-service>
```



```
                <log-path-agent>/home/gptest/Desktop/data/
gpadata</log-path-agent>
        </Settings>
</GlobalProtect>
```

クライアント証明書ベースの認証

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
    <PanSetup>
                <Portal>192.168.1.23</Portal>
    </PanSetup>
        <Settings>
                <head-less>yes</head-less>
                <os-type>IoT</os-type>
                <client-cert-path>/home/gptest/Desktop/data/
pan_client_cert.pfx</client-cert-path>
                <client-cert-passphrase>/home/gptest/Desktop/
data/pan_client_cert_passcode.dat</client-cert-passphrase>
                <username>user1</username>
                <password>paloalto</password>
                <log-path-service>/home/gptest/Desktop/data/
gps</log-path-service>
                <log-path-agent>/home/gptest/Desktop/data/
gpadata</log-path-agent>
        </Settings>
</GlobalProtect>
```

2. `globalprotect.conf` ファイルを Base64 フォーマットでエンコードし、`android_src_tree_root/system/config/` ディレクトリに保存します。

   ファイルを別の場所に保存することもできます。ただし、`android_src_tree_root/assets/gp_conf_location.txt` ファイル内のこの設定箇所を変更する必要があります。

STEP 5 | GlobalProtect APK ファイルをビルドします。

STEP 6 | GlobalProtect APK ファイルに署名します。

STEP 7 | 新しい OS をシステムイメージの一部として Android デバイスにプッシュしてから、新しい OS を Android デバイスにプッシュします。

RaspbianでのIoT用GlobalProtectのインストール

RaspbianデバイスでのGlobalProtect for IoTのインストールを実行するには、以下の手順を完了してください。

Raspbian と *Ubuntu* 用の *GlobalProtect for IoT* は、*Arm* ベースのアーキテクチャのみをサポートします。

STEP 1 | Support Siteで、**Updates**（更新） > **Software Updates**（ソフトウェア更新）を選択して、ご利用の OS のGlobalProtect パッケージをダウンロードします。

STEP 2 | IoT 用 GlobalProtect アプリケーションをインストールします。

ソフトウェアをインストールするには、該当の IoT デバイスで、 **sudo dpkg -i GlobalProtect_deb_arm<*version*>.deb** コマンドを使用します。

```
sudo dpkg -i GlobalProtect_deb_arm-5.1.0.0-84.deb
```

ソフトウェアを後でアンインストールするには、***sudo dpkg -P globalprotect*** コマンドを使用します。

STEP 3 | Raspbian IoT デバイスの事前デプロイしたい VPN 設定を行います。

1. `client-cert` パスで、証明書を pcks12 形式でインポートして、 .pfx 拡張子で保存します（ 例、**pan_client_cert.pfx**）。
2. `client-cert-passphrase` パス内で、.dat 拡張子でパスコードを保存します（例、**pan_client_cert_passcode.dat**）
3. `log-path-service` パスで、PanGPS のデフォルトのパスを使用していない場合 (例、`/opt/paloaltonetworks/globalprotect`)、 `log-setting` パス フォルダが `opt/paloaltonetworks` と同じ権限を有していることを確認します。
4. 以下の形式で `/opt/paloaltonetworks/globalprotect/pangps.xml` 事前デプロイ設定ファイルを次のフォーマットで作成し、GlobalProtect ポータルの IP アドレスと認証設定を編集します。次のいずれか: ユーザー名とパスワード、またはクライアント証明書パス (**client-cert-path**) とパスフレーズファイル (**client-cert-passphrase**)。GlobalProtect サービス（ **log-path-service** ）およびエージェント（ **log-path-agent** ）のログを保存するフォルダをオプションで指定することもできます。

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
 <PanSetup>
          <Portal>192.168.1.160</Portal>       //pre-deployed
 portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
```

```
 <Settings>
        <portal-timeout>5</portal-timeout>
        <connect-timeout>5</connect-timeout>
        <receive-timeout>30</receive-timeout>
        <os-type>IoT</os-type>             //pre-deployed OS type
 for IoT. If this tag does not present, GP will automatic detect
 the OS type.
        <head-less>yes</head-less>       //pre-deployed head-less
 mode
        <username>abc</username>    //optional pre-deployed
 username
        <password>xyz</password>       //optional pre-deployed
 password
        <client-cert-path>cli_cert_path</client-cert-path>
  //optional pre-deployed client certificate file(p12) path
        <client-cert-passphrase>cli_cert_passphrase_path< /client-
cert-passphrase>       //optional pre-deployed client certificate
 passphrase file path
        <log-path-service>/tmp/gps</log-path-service>  //optional
 pre-deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional
 pre-deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | 事前デプロイ設定を反映させるために、GlobalProtect プロセスを再起動します。

STEP 5 | IoT デバイスのデプロイ後、必要に応じて **globalprotect collect-log** コマンドを使用してログを収集することができます。

```
user@raspbianhost:~/Desktop/data$ globalprotect collect-log
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 6 | (オプション) 認証方法がユーザー名/パスワードとクライアント証明書の組み合わせである場合は、クライアント証明書の **CommonName** がユーザー名と一致することを確認してください。

UbuntuでのIoT用GlobalProtectのインストール

Ubuntu で GlobalProtect for IoT をインストールをするには、次の手順を完了させてください。

Raspbian と *Ubuntu* 用の *GlobalProtect for IoT* は、*Arm* ベースのアーキテクチャのみをサポートします。

STEP 1 | Support Siteで、**Updates**（更新） > **Software Updates**（ソフトウェア更新）を選択して、ご利用の OS のGlobalProtect パッケージをダウンロードします。

STEP 2 | IoT 用 GlobalProtect アプリケーションをインストールします。

ソフトウェアをインストールするには、該当の IoT デバイスで、 **sudo dpkg -i GlobalProtect_deb-<*version*>.deb**コマンドを使用します。

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

ソフトウェアを後でアンインストールするには、***sudo dpkg -P globalprotect*** コマンドを使用します。

STEP 3 | Ubuntu の IoT デバイスに事前デプロイしたい VPN 設定を実施します。

1. `client-cert` パスで、証明書を pcks12 形式でインポートして、 .pfx 拡張子で保存します（ 例、**pan_client_cert.pfx**）。
2. `client-cert-passphrase` パス内で、.dat 拡張子でパスコードを保存します（例、**pan_client_cert_passcode.dat**）
3. `log-path-service` パスで、PanGPS のデフォルトのパスを使用していない場合 (例、`/opt/paloaltonetworks/globalprotect`)、 `log-setting` パス フォルダが `opt/paloaltonetworks` と同じ権限を有していることを確認します。
4. 以下の形式で `/opt/paloaltonetworks/globalprotect/pangps.xml` 事前デプロイ設定ファイルを次のフォーマットで作成し、GlobalProtect ポータルの IP アドレスと認証設定を編集します。次のいずれか: ユーザー名とパスワード、またはクライアント証明書パス (**client-cert-path**) とパスフレーズファイル (**client-cert-passphrase**)。GlobalProtect サービス（ **log-path-service** ）およびエージェント（ **log-path-agent** ）のログを保存するフォルダをオプションで指定することもできます。

```
<?xml version="1.0" encoding="UTF-8"?>

<GlobalProtect>
 <PanSetup>
          <Portal>192.168.1.160</Portal>       //pre-deployed
 portal address
</PanSetup>
 <PanGPS>
 </PanGPS>
 <Settings>
```

```
        <portal-timeout>5</portal-timeout>
        <connect-timeout>5</connect-timeout>
        <receive-timeout>30</receive-timeout>
        <os-type>IoT</os-type>              //pre-deployed OS type
 for IoT. If this tag does not present, GP will automatic detect
 the OS type.
        <head-less>yes</head-less>       //pre-deployed head-less
 mode
        <username>abc</username>    //optional pre-deployed
 username
        <password>xyz</password>       //optional pre-deployed
 password
        <client-cert-path>cli_cert_path</client-cert-path>
  //optional pre-deployed client certificate file(p12) path
        <client-cert-passphrase>cli_cert_passphrase_path< /client-
cert-passphrase>       //optional pre-deployed client certificate
 passphrase file path
        <log-path-service>/tmp/gps</log-path-service>  //optional
 pre-deployed log folder for PanGPS
        <log-path-agent>/tmp/gpa</log-path-agent>      //optional
 pre-deployed log folder for PanGPA and globalprotect CLI
 </Settings>
</GlobalProtect>
```

STEP 4 | 事前デプロイ設定を反映させるために、GlobalProtect プロセスを再起動します。

STEP 5 | IoT デバイスのデプロイ後、必要に応じて **globalprotect collect-log** コマンドを使用してログを収集することができます。

```
user@linuxhost:~$ globalprotect collect-log
The support file is saved to /home/gptest/.GlobalProtect/
GlobalProtectLogs.tgz
```

STEP 6 | (オプション) 認証方法がユーザー名/パスワードとクライアント証明書の組み合わせである場合は、クライアント証明書の **CommonName** がユーザー名と一致することを確認してください。

WindowsでのIoTデバイス用GlobalProtectのインストール

Windows 10 IoT で稼働しているデバイスは、GlobalProtect アプリケーションを使用できます。Microsoft System Center Configuration Manager (SCCM) などの、ご所属の組織の配布方法を使用して、Windows 10 IoT Enterprise を実効する IoT デバイス上で GlobalProtect アプリケーションのデプロイとインストールを行います

GlobalProtect Windows IoT のデプロイは、証明書ベースの認証をサポートします。各 IoT デバイスのローカル マシン ストアに、認証に使用される証明書をインストールする必要があります。IoT デバイスに同じ Root CA を持つ複数の証明書がある場合、GlobalProtect は IoT デバイスのローカル マシン ストアの最初の証明書を使用して認証します。証明書がデバイスで正しい順序になっていることを確認してください。

次のセクションでは、Windows IoT を実行しているデバイスに GlobalProtect アプリケーションをインストールする方法について説明します:

- IoT デバイス上での MSIEXEC ファイルのダウンロードとインストール
- IoT デバイスのレジストリ キーを変更します（On-Demand（オンデマンド）またはAlways On（常時オン））
- IoT デバイスのレジストリ キーを変更する（Always On with Pre-logon（プレ ログオンで常時オン））

IoT デバイス上での MSIEXEC ファイルのダウンロードとインストール

`msiexec.exe` ファイルをお使いの IoT デバイスにダウンロードしてインストールし、**On-Demand**（オンデマンド） 接続方法または **Always On**（常時オン） 接続方法用に GlobalProtect アプリケーションをインストールします。IoT 以外のデバイスで行う場合と同じ方法を使用して、deploy the msiexec.exe file（msiexec.exe ファイルのデプロイ）を実行します。

IoT デバイスのレジストリ キーを変更します（On-Demand（オンデマンド）またはAlways On（常時オン））

OS の種類を IoT、デバイス タイプをヘッドレス、及びポータル アドレスを指定する必要があります。オプションで、ユーザー名とパスワードを指定できます。ユーザー名とパスワードを指定しない場合、GlobalProtect は証明書ベースの認証を使用します。

On-Demand（オンデマンド）接続方法または **Always On**（常時オン）接続方法には、以下のインストール方法を使用できます。

- OS の種類を指定します (必須):

  レジストリ サブキー: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名前）: os-type

  Type（タイプ）：REG_SZ

  Data（データ）:IoT
- ヘッドレス IoT デバイスを指定する (必須):

  レジストリ サブキー: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名前）: head-less

  Type（タイプ）：REG_SZ

  Data（データ）: yes
- ポータルのアドレスを指定する (必須):

  レジストリ サブキー: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Name(名前)：ポータル

  Type（タイプ）：REG_SZ

  Data（データ）:GlobalProtect ポータルの IP アドレスまたは FQDN を入力します。
- ユーザー名を指定する (オプション):

  レジストリ サブキー: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名前）: username

  Type（タイプ）：REG_SZ

  Data（データ）:IoT デバイスで使用するユーザー名を入力します。
- パスワードを入力する (オプション):

  レジストリ サブキー: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名前）: password

  Type（タイプ）：REG_SZ

  Data（データ）:IoT デバイスで使用するパスワードを入力します。

IoT デバイスのレジストリ キーを変更する（Always On with Pre-logon（プレ ログオンで常時オン））

ポータルアドレス、プレ ログオンのタイムアウト値、およびサービスのみの値を指定する必要があります。システムの再起動時に IoT デバイスがアプリ インターフェースを自動的に起動しな

いようにするには、GlobalProtect 値を削除する必要があります。ユーザーがログインしていないため、ログオン前の VPN トンネルはユーザー名を関連付けません。

Pre-logon (Always On)（プレ ログオン（常時オン））の接続方法には、次のインストール方法を使用できます。

- ポータルのアドレスを指定する (必須):

  レジストリ サブキー: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Name(名前)：ポータル

  Type（タイプ）：REG_SZ

  Data（データ）:GlobalProtect ポータルの IP アドレスまたは FQDN を入力します。
- プレ ログオン値を入力 (必須):

  レジストリ サブキー: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`

  Name(名前)：Prelogon（プレ ログオン）

  Type（タイプ）：REG_SZ

  Data（データ）:1
- サービス専用の値を指定する (必須):

  レジストリ サブキー: `\HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\Settings`

  Name（名前）: service-only（サービス専用）

  Type（タイプ）：REG_SZ

  Data（データ）: yes
- GlobalProtect 値を削除する (必須):

  Registry subkey（レジストリのサブキー）: `\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`

  Name(名前)：GlobalProtect

  Type（タイプ）：REG_SZ

ホスト情報

企業のネットワークの境界に厳重なセキュリティを実装していたとしても、実際にはアクセスするエンドポイントと同じ程度の安全性しか保たれません。モバイルの浸透が進む最近の仕事環境では、空港、カフェ、ホテルなどのさまざまな場所から、企業が支給するエンドポイントや個人用などの多様なデバイスを使用して企業のリソースにアクセスできることが当然とみなされつつあります。必然的に、エンドポイントに対するネットワークのセキュリティを拡張し、包括的で一貫性のあるセキュリティを確実に適用することが求められます。GlobalProtect™ ホスト情報プロファイル（HIP）の機能によって、最新のセキュリティ パッチおよびウイルス対策の定義がインストールされているか、ディスク暗号化が有効になっているか、デバイスが脱獄または root 化されていないか（モバイル デバイスのみ）、カスタム アプリケーションを含む組織内で必要な特定のソフトウェアが実行されているかなどの、エンドポイントのセキュリティ状態に関する情報を収集し、定義したホスト ポリシーを準拠していることを基準に、特定のホストへのアクセスを許可する判断材料にすることができます。

以下のセクションでは、ポリシー適用でホスト情報を使用する方法について説明します。

ホスト情報について

GlobalProtect アプリの役割のひとつに、このアプリが実行されているホストに関する情報の収集があります。アプリは GlobalProtect ゲートウェイに正常に接続されると、ゲートウェイにこのホスト情報を送信します。ゲートウェイは、アプリが送信したこの生ホスト情報を、定義されている HIP オブジェクトおよび HIP プロファイルと照合します。一致していると認められた場合、HIP マッチ ログにエントリが生成されます。さらに、ポリシー ルールで HIP プロファイルの一致が認められると、対応するセキュリティ ポリシーが適用されます。

ポリシーの適用にホスト情報を使用することで、重要なリソースにアクセスするリモート ホストが適切に整備された、セキュリティ標準に準拠した粒度の細かいセキュリティを実現でき、その後に、ネットワーク リソースへのアクセスを許可できます。たとえば、機密データ システムへのアクセスを許可する前に、データにアクセスするホストのハード ドライブの暗号化を確実に有効にすることが必要になる場合があります。エンドポイント システムで暗号化が有効になっている場合のみアプリケーションへのアクセスを許可するセキュリティ ルールを作成して、このポリシーを適用できます。さらに、このルールに準拠していないエンドポイントに対して、アクセスが拒否された理由をユーザーに警告し、欠落している暗号化ソフトウェアのインストール プログラムにアクセスできるファイル共有にリンクする通知メッセージを作成できます（当然、ユーザーにそのファイル共有へのアクセスを許可するために、特定の HIP プロファイルと一致するホストの特定の共有へのアクセスを許可する、対応するセキュリティ ルールを作成する必要があります）。

- GlobalProtect アプリが収集するデータ
- ゲートウェイがポリシー適用でホスト情報を使用する方法
- システムの準拠を確認する方法
- エンドポイントの状態の表示方法

GlobalProtect アプリが収集するデータ

デフォルトでは、GlobalProtect アプリは、エンドポイントで実行されているエンド ユーザー セキュリティ パッケージに関するベンダー固有のデータを収集し（OPSWAT グローバル パートナーシップ プログラムがまとめるように）、ポリシー適用のためにこのデータを GlobalProtect ゲートウェイにレポートします。

セキュリティ ソフトウェアは、エンド ユーザー保護の徹底のために進化を継続する必要がありますが、GlobalProtect ゲートウェイ ライセンスにより、各パッケージに利用できる最新のパッチおよびソフトウェア バージョンを GlobalProtect データ ファイルのダイナミック更新によって受信できるようにもなります。

アプリは、デフォルトで、ホストのセキュリティ状態の特定に役立つ以下の情報のカテゴリに関するデータを収集します。

表 **8 :** 表：データ収集 カテゴリ

カテゴリ	収集されるデータ
一般	ホスト名、ログオン ドメイン、オペレーティング システム、アプリのバージョン、Windows システムの場合はマシンが属するドメインなどの、ホスト自体に関する情報。 *Windows* エンドポイントのドメインの場合、*GlobalProtect* アプリは、*ComputerNameDnsDomain* について定義されているドメインの情報を収集します。このドメインは、ローカル コンピュータまたはローカル コンピュータに関連付けられているクラスタに割り当てられる *DNS* ドメインです。このデータは、*HIP* マッチ ログ詳細 (**Monitor** (モニタ) > **Logs** (ログ) > **HIP Match**(**HIP** マッチ)) の *Windows* エンドポイントの **Domain** (ドメイン) に表示されます。
モバイル デバイス	デバイス名、ログオン ドメイン、オペレーティング システム、アプリ バージョン、デバイスが接続されているモバイル デバイス ネットワークについての情報など、モバイル デバイスに関する情報。さらに、GlobalProtect はデバイスが root 化または脱獄されているかどうかに関する情報も収集します。 モバイル デバイスの属性を収集し、*HIP* 実施ポリシーで使用するには、*GlobalProtect* に *MDM* サーバーが必要です。*GlobalProtect* は現在、*AirWatch MDM* サーバーとの *HIP* 統合をサポートしています。 AirWatch が管理するデバイスの場合、GlobalProtect アプリが収集するホスト情報の他に、AirWatch サービスから収集される追加情報もあります。AirWatch で取得できる属性一覧は、ホスト情報を収集するための Windows User-ID エージェントの設定を参照してください。
パッチ管理	ホストで有効化またはインストールされているパッチ管理ソフトウェアと、パッチが欠落しているかどうかに関する情報。

カテゴリ	収集されるデータ
	欠落しているパッチの ***Severity*** **(**重大度**)** 値を *HIP* オブジェクト（***Objects*** **(**オブジェクト**)** > ***GlobalProtect*** > ***HIP Objects*** **(***HIP* オブジェクト**)** > ***<hip-object>*** > ***Patch Management*** **(**パッチ管理**)** > ***Criteria*** **(**条件**)**）の一致条件として構成する場合は、*GlobalProtect* 重大度値と *OPSWAT* 重大度格付けの間で次のマッピングを使用します。 • ***0***–低 • ***1***–中 • ***2***–重要 • ***3***–極めて重大
ファイアウォール	ホストにインストールまたは有効化されているファイアウォールに関する情報。
マルウェア対策	エンドポイントで有効化またはインストールされているアンチウイルスまたはアンチスパイウェア ソフトウェア、リアルタイム保護が有効かどうか、ウイルス定義バージョン、最終スキャン時間、ベンダー名と製品名に関する情報。 GlobalProtect は OPSWAT 技術を利用し、エンドポイント上にあるサードパーティ製のセキュリティ アプリケーションの検知・評価を行います。OPSWAT OESIS フレームワークを統合することで、エンドポイントのコンプライアンス状況を GlobalProtect によって評価できるようになります。例えば、特定のベンダーが提供する特定のバージョンのアンチウイルス ソフトウェアがエンドポイント上に存在することを確認するために HIP プロファイルや HIP オブジェクトを定義したり、そのウイルス定義ファイルが最新のものであることを確認したりできます。

カテゴリ	収集されるデータ
	OPSWAT は、*macOS*エンドポイント上のゲートキーパーセキュリティ機能に関する次のマルウェア対策情報を検出できません。 • エンジン バージョン • 定義バージョン • 日付 • 最終スキャン日時
ディスク バックアップ	ディスク バックアップ ソフトウェアがインストールされているかどうか、最終バックアップ時間、ソフトウェアのベンダー名と製品名に関する情報。
ディスク暗号化	ディスク暗号化ソフトウェアがインストールされているかどうか、どのドライブやパスに暗号化が設定されているか、ソフトウェアのベンダー名と製品名に関する情報。
データ損失防止(DLP)	企業の機密情報が企業のネットワークから持ち出されたり、安全でない可能性があるデバイスに保存されたりすることを防ぐための、データ損失防止（DLP）ソフトウェアがインストールまたは有効化されているかどうかに関する情報。この情報は、Windows エンドポイントからのみ収集されます。
Certificate（証明書）	エンドポイントにインストールされたマシン証明書についての情報です。
カスタム チェック	特定のレジストリキー (Windows のみ)、プロパティ リスト (plist) (macOS のみ)、OR 演算子システムのプロセスおよびユーザー空間アプリケーションのプロセスが存在するかどうかについての情報です。

特定のカテゴリの情報を除外して特定のホストで収集されないようにすることができ、これにより、CPU サイクルを節約し、応答時間を改善することができます。これを実行するには、ポータル上でエージェント設定を作成してから、(**Network (ネットワーク)** > **GlobalProtect** > **Portals (ポータル)** > ***<portal-config>*** > **Agent (エージェント)** > ***<agent-config>*** > **Data Collection (データ収集)**) で興味のないカテゴリを除外します。たとえば、エンドポイントでディスク バックアップ ソフトウェアが動作しているかどうかに基づいてポリシーを作成しない場合に、そのカテゴリを除外すると、アプリでディスク バックアップに関する情報を収集しなくなります。

ユーザーのプライバシーを提供するために、個人エンドポイントで収集される情報を除外することもできます。たとえば、サードパーティーのモバイルデバイスマネージャー によって管理されない、エンドポイントにインストールされているアプリケーションのリストを除外できます。

ゲートウェイがポリシー適用でホスト情報を使用する方法

アプリが、収集する情報に関する情報を、ポータルからダウンロードされたクライアントの設定から取得する一方で、ゲートウェイには HIP オブジェクトおよび HIP プロファイルを作成し、モニタリングやポリシー適用の対象となるホストの属性を定義しておきます。

- **HIP** オブジェクト – 関心のあるアプリ情報のみを抽出し、ポリシーを適用するために使用される一致条件です。たとえば、生ホスト データに、エンドポイントにインストールされている複数のアンチウイルス パッケージに関する情報が含まれていて、関心のあるのは、組織内で必要とする特定の 1 つのアプリケーションである場合があります。この場合は、適用において関心のある特定のアプリケーションに一致する HIP オブジェクトを作成します。

  必要な HIP オブジェクトを判別する最良の方法は、収集したホスト情報をどのように使用してポリシーを適用するかを判別することです。HIP オブジェクト自体は、セキュリティ ポリシーで使用される HIP プロファイルを作成できるようにする構成要素にすぎません。そのため、オブジェクトをシンプルにし、たとえば、特定のタイプの必須ソフトウェアがあるか、特定のドメインのメンバーか、特定のエンドポイント OS があるかなど、1 つの条件にのみ一致させることが必要になる場合があります。こうすることで、非常に粒度の細かい（そして非常に強力な）HIP で補完されたポリシーを柔軟に作成することができます。
- **HIP** プロファイル – HIP オブジェクトのコレクション。モニタリングまたはセキュリティ ポリシー適用のために、まとめて評価されます。HIP プロファイルを作成すると、Boolean ロジックを使用して、以前に作成した HIP オブジェクト（および他の HIP プロファイル）を組み合わせることができます。たとえば、作成した HIP プロファイルに対してトラフィック フローを評価し、一致か不一致かを判定することができます。一致がある場合、対応するポリシー ルールが適用されます。一致がなければ、他のポリシー照合条件と同様に、フローは次のルールと照合して評価されます。

トラフィック ログが、ポリシーに一致する場合のみログ エントリを作成するのと異なり、HIP マッチ ログは、アプリによって送信された生データが、定義した HIP オブジェクトや HIP プロファイルに一致する場合に常にエントリを作成します。このため、HIP マッチ ログは、HIP プロファイルをセキュリティ ポリシーに関連付ける前に時間をかけてネットワークのエンドポイントの状態をモニターするための優れたリソースとなり、関連付ける必要があるポリシーを厳密に判断するときに役立ちます。HIP オブジェクトと HIP プロファイルを作成し、ポリシー一致条件として使用する方法の詳細は、HIP ベースのポリシー適用の設定を参照してください。

システムの準拠を確認する方法

デフォルトでは、HIP が有効なセキュリティ ルールが適用された結果として行われるポリシーの決定に関する情報は、エンド ユーザーに提供されません。ただし、特定の HIP プロファイルが一致するときまたは一致しないときに HIP 通知メッセージが表示されるように設定して、この機能を実現できます。

メッセージが表示されるタイミング（すなわち、ユーザーの設定がポリシーの HIP プロファイルに一致するときに表示されるのか、一致しないときに表示されるのか）に関する決定は、ポリシーおよび HIP の一致（または不一致）の意味に大いに依存します。つまり、一致することは、

ネットワーク リソースへのフル アクセス権限が付与されていることを意味するのでしょうか。それとも、遵守していないことが原因で、アクセスが制限されたことを意味するのでしょうか。

たとえば、以下のシナリオを検討します。

- 会社の必須のアンチウイルスおよびアンチスパイウェア ソフトウェア パッケージがインストールされていない場合に一致する HIP プロファイルを作成します。この場合、HIP プロファイルに一致するユーザーに対して、ソフトウェアをインストールする必要があること（必要に応じて、対応するソフトウェアのインストーラにアクセスするためのファイル共有へのリンクを提供する）を伝える HIP 通知メッセージを作成することになります。
- それらの同じアプリケーションがインストールされている場合に一致する *HIP* プロファイルを作成します。この場合、プロファイルと一致しないユーザーのメッセージを作成して、インストール パッケージの場所に転送することができます。

HIP オブジェクトと HIP プロファイルの作成方法と HIP 通知メッセージの定義に使用する方法の詳細については、HIP ベースのポリシー適用の設定を参照してください。

エンドポイントの状態の表示方法

エンドポイントが GlobalProtect に接続するときは常に、アプリにより HIP データがゲートウェイに提示されます。ゲートウェイでは、このデータに基づいて、ホストが照合する HIP オブジェクトまたは HIP プロファイルを判別します。一致が検出されるごとに、HIP マッチ ログ エントリが生成されます。トラフィック ログが、ポリシーに一致する場合のみログ エントリを作成するのと異なり、HIP マッチ ログは、アプリによって送信された生データが、定義した HIP オブジェクトや HIP プロファイルに一致する場合に常にエントリを作成します。このため、HIP マッチ ログは、HIP プロファイルをセキュリティ ポリシーに関連付ける前に時間をかけてネットワークのエンドポイントの状態をモニターするための優れたリソースとなり、関連付ける必要があるポリシーを厳密に判断するときに役立ちます。

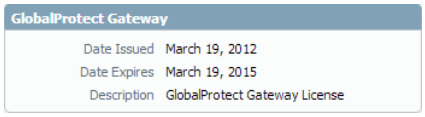
HIP マッチ ログは、エンドポイントの状態が作成した HIP オブジェクトに一致する場合にのみ生成されるため、ホストの状態を完全に可視化するには、特定の状態に適合するエンドポイント（セキュリティ ポリシー用）に加えて、その状態に適合しないエンドポイント（可視化用）を対象とする複数の HIP オブジェクトを作成して、HIP マッチをログに記録する必要があります。たとえば、アンチウィルス ソフトウェアまたはアンチスパイウェア ソフトウェアがインストールされていないエンドポイントはネットワークに接続できないようにするとします。この場合、特定のアンチウィルス ソフトウェアまたはアンチスパイウェア ソフトウェアがインストールされているホストに一致する HIP オブジェクトを作成します。このオブジェクトを HIP プロファイルに含め、VPN ゾーンからのアクセスを許可するセキュリティ ポリシー ルールに関連付けることにより、アンチウィルス ソフトウェアまたはアンチスパイウェア ソフトウェアによって保護されているホストのみが接続できるようにします。

この例では、この要件に準拠していないエンドポイントを HIP Match ログで表示することはできません。アンチウィルス ソフトウェアまたはアンチスパイウェア ソフトウェアがインストールされていないエンドポイントのログを確認して、そのユーザーを追跡できるようにするには、アンチウィルス ソフトウェアがインストールされていないという条件に一致する HIP オブジェクトも作成します。このオブジェクトはロギング目的でのみ使用するため、HIP プロファイルに追加したり、セキュリティ プロファイル ルールに関連付けたりする必要はありません。

HIP ベースのポリシー適用の設定

ポリシー適用でホスト情報を使用できるようにするには、以下のステップを実行する必要があります。HIP 機能の詳細は、ホスト情報についてを参照してください。

STEP 1 | HIP チェックのための正規のライセンスを取得していることを確認します。



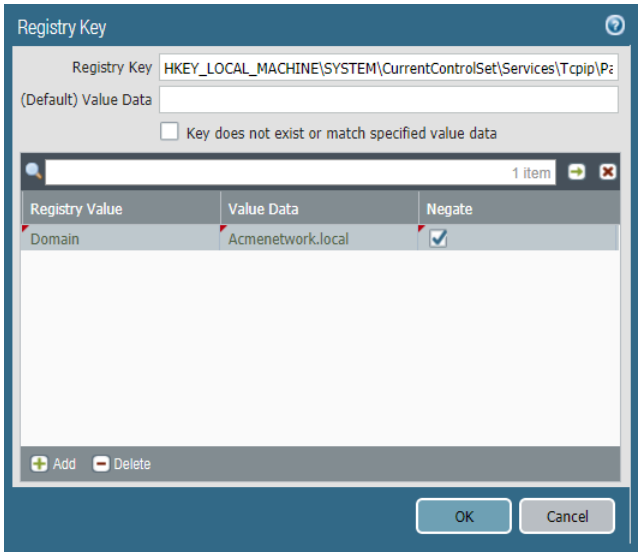
HIP 機能を使用するには、HIP チェックを実行する各ゲートウェイに GlobalProtect サブスクリプション ライセンスを購入し、インストールしておく必要があります。各ポータルおよびゲートウェイの状態を確認するには、**Device** > **Licenses**（ライセンス）の順に選択します。

必要なライセンスがない場合は、Palo Alto Networks のセールス エンジニアまたはリセラーにお問い合わせください。ライセンスの詳細は、GlobalProtect ライセンスについてを参照してください。

STEP 2 | （任意）アプリで収集するカスタム ホスト情報を定義します。たとえば、HIP オブジェクト作成対象の（ベンダー）リストや（製品）リストに含まれていない必須アプリケーションがある場合、カスタム チェックを作成して、アプリケーションがインストールされてい

るか（対応するレジストリ キーまたは plist キーがある）、実行中か（対応する実行中プロセスがある）を判定できます。

ステップ *2* およびステップ *3* で、*GlobalProtect* ポータル設定が済んでいるとします。ポータルをまだ設定していない場合は、GlobalProtect ポータルへのアクセスのセットアップで手順を参照してください。



1. GlobalProtect ポータルをホストしているファイアウォールで、**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択します。
2. 変更するポータル設定を選択します。
3. **Agent**（エージェント） タブで、カスタム HIP チェックを追加するクライアントの設定を選択するか、新しいクライアントの設定を **Add**（追加）します。
4. **Data Collection**（データ収集）を選択し、**Collect HIP Data**（**HIP** データの収集）オプションを有効にします。
5. **Custom Checks**（カスタム チェック）で、このエージェント設定を実行するホストから収集するデータを以下のように定義します。
   - 特定のレジストリ情報を収集するには：**Windows** タブで、データを収集する **Registry Key**（レジストリ キー）の名前を **Registry Key**（レジストリ キー）領域に **Add**（追加）します。データ収集を特定の **Registry Value**（レジストリ値）に制限するには、特定のレジストリ値を **Add**（追加）して定義します。**OK** をクリックして設定を保存します。
   - 実行中のプロセスに関する情報を収集するには：適切なタブ（**Windows** または **Mac**）を選択してプロセスを **Process List**（プロセス リスト）に **Add**（追加）します。アプリで情報を収集するプロセスの名前を入力します。

- 特定のプロパティリストを収集するには：**Mac** タブで、データを収集する **Plist** を **Add**（追加）します。特定のキー値に対するデータ収集を制限するには、**Key**（キー）値を**Add**（追加）します。**OK** をクリックして設定を保存します。

6. 新しいエージェントの設定の場合は、必要に応じてGlobalProtect ポータルのエージェント設定の定義を行います。
7. **OK** をクリックして設定を保存します。
8. 変更を **Commit**（コミット）します。

STEP 3 | （任意）コレクションからカテゴリを除外します。

1. GlobalProtect ポータルがホストされているファイアウォールで、**[Network]** > **[GlobalProtect]** > **[ポータル]** の順に選択します。
2. 変更するポータル設定を選択します。
3. **Agent**（エージェント）タブで、カテゴリを除外するクライアント設定を選択するか、新しい設定を **Add**（追加）します。
4. **Data Collection**（データ収集） を選択し、**Collect (HIP Data)**（収集（**HIP** データ））が有効になっていることを確認します。
5. **Exclude Categories**（カテゴリの除外）で、新しいカテゴリの除外を **Add**（追加） します。
6. ドロップダウンから、除外する **Category**（カテゴリ）を選択します。
7. （任意）カテゴリ全体を除外するのではなく、選択したカテゴリ内から特定のベンダーや製品を除外する場合は、**Add**（追加）をクリックします。ベンダーの編集ダイアログで、除外する**Vendor**（ベンダー）を選択し、**Add**（追加）をクリックして、そのベンダーから特定の製品を除外します。ベンダーの定義が完了したら、**OK** をクリックします。除外リストに複数のベンダーおよび製品を追加できます。
8. 除外する各カテゴリについてステップ 5～7 を繰り返します。
9. 新しいエージェントの設定の場合は、必要に応じてGlobalProtect ポータルのエージェント設定の定義を行います。
10. **OK** をクリックして設定を保存します。
11. 変更を **Commit**（コミット）します。

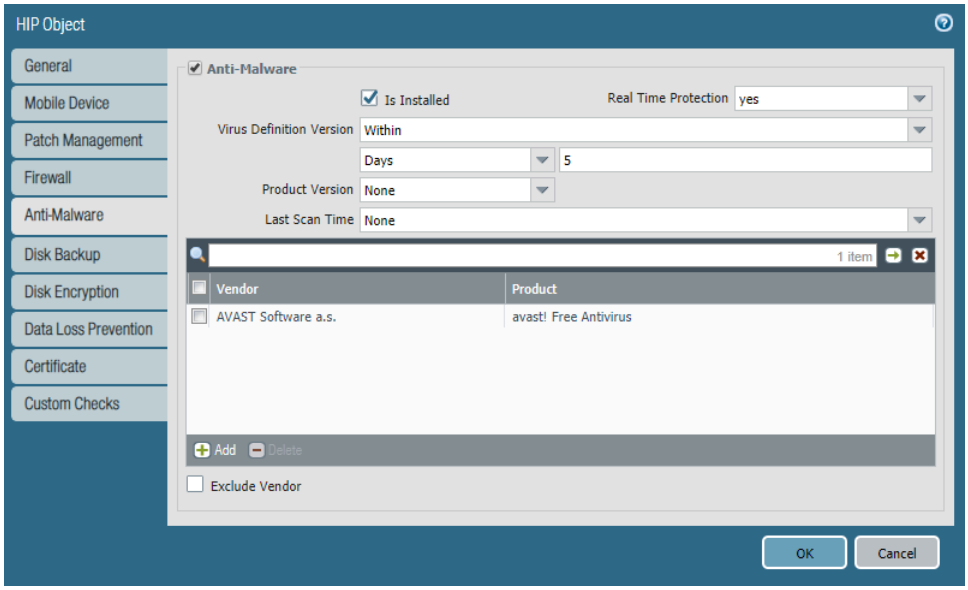
STEP 4 | アプリが収集した生ホスト データにフィルタをかける HIP オブジェクトを作成します。

必要な HIP オブジェクトを判別する最良の方法は、収集したホスト情報をどのように使用してポリシーを適用するかを判別することです。HIP オブジェクト自体は、セキュリティ ポリシーで使用される HIP プロファイルを作成できるようにする構成要素にすぎません。そのため、オブジェクトをシンプルにし、たとえば、特定のタイプの必須ソフトウェアがあるか、特定のドメインのメンバーか、特定の OS があるかなど、1 つのアイテムにのみ一致させる

ことが必要になる場合があります。こうすることで、非常に粒度の細かい（そして非常に強力な）HIP で補完されたポリシーを柔軟に作成することができます。

特定の *HIP* カテゴリやフィールドの詳細は、オンライン ヘルプを参照してください。

1. GlobalProtect ゲートウェイをホストするファイアウォールで（複数のゲートウェイの間で HIP オブジェクトを共有する場合は Panorama で）、**Objects**（オブジェクト） > **GlobalProtect** > **HIP Objects**（**HIP** オブジェクト）の順に選択し、HIP オブジェクトを **Add**（追加）します。
2. オブジェクトの **Name** [名前] を入力します。
3. 照合するホスト情報のカテゴリに対応するタブを選択し、チェック ボックスをオンにして、このカテゴリに対して照合するオブジェクトを有効にします。たとえば、アンチウイルスまたはアンチスパイウェア ソフトウェアに関する情報を検索するオブジェクトを作成するには、**Anti-Malware**（アンチマルウェア） タブを選択し、次に **Anti-Malware**（アンチマルウェア） チェック ボックスをオンにして、対応するフィールドを利用できるようにします。フィールドに入力して、目的の一致条件を定義します。たとえば、次の図は、エンドポイントに AVAST Free Antivirus ソフトウェア アプリケーションがインストールされていて、**Real Time Protection**（リアルタイム保護）が有効であり、過去 5 日間に更新されたウィルス定義がある場合に一致する HIP オブジェクトを作成する方法を示しています。



HIP オブジェクト内で、照合するカテゴリごとにこの手順を繰り返します。詳細は、表:データ収集カテゴリを参照してください。

4. （任意） エンドポイントの所有権カテゴリまたはコンプライアンス ステータスと一致するようにタグを設定します。

   たとえば、従業員が所有するエンドポイントと一致するタグを作成し、ユーザーが個人のエンドポイント上の機密ネットワーク リソースにアクセスするのを防ぐことができます。

   Windows 用 User-ID エージェントは、MDM サーバーに次の情報を問い合わせます。

   - モバイルデバイスのコンプライアンス ステータス。
   - モバイルデバイスが属するスマート グループ（所有カテゴリ）。

   ユーザー ID エージェントは、この情報を HIP レポートに組み込まれたタグに変換します。これらのタグ値に基づいて HIP オブジェクトを作成して、ネットワーク内のエンドポイントに HIP ベースのセキュリティポリシーを適用することができます。詳細情報

は、ホスト情報を収集するための Windows User-ID エージェントの設定を参照してください。

1. **Mobile Device**（モバイル デバイス）チェックボックスを選択して、**Mobile Device**（モバイル デバイス）設定の構成を有効にします。
2. **Device**（デバイス）タブで、**Tag**（タグ）ドロップダウンメニューから一致演算子を選択します（**Contains**（含む） または **Is Not**（含まない））。
3. （任意）プロンプトが表示されたら、次の所有権カテゴリ値のいずれかを入力します。

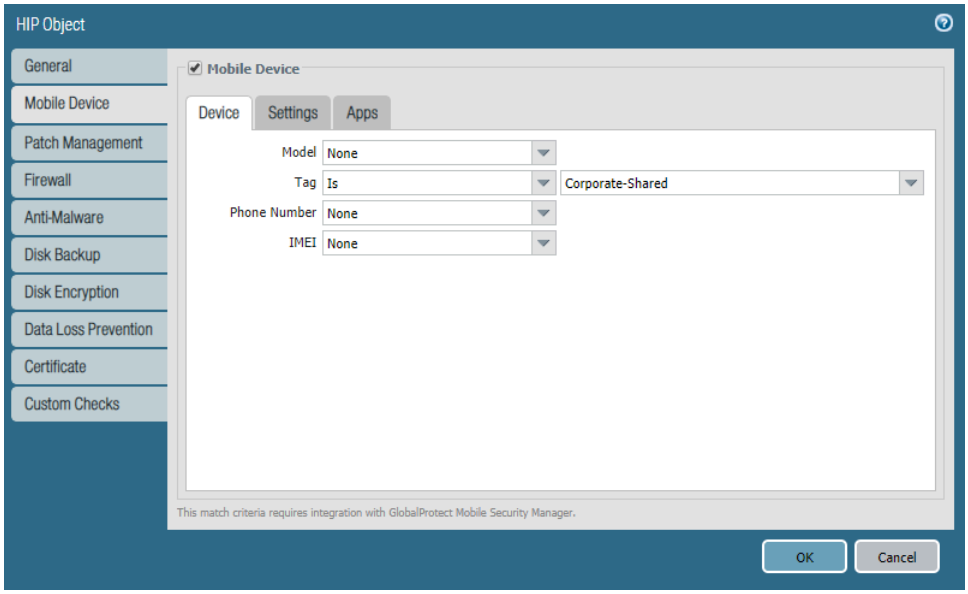
   所有権カテゴリは、誰がエンドポイントを所有しているかを示します。

   - 従業員の所有
   - 法人専用
   - 法人の共有

4. （任意）プロンプトが表示されたら、次のコンプライアンス ステータス値のいずれかを入力します。

   コンプライアンスステータスは、エンドポイントが定義したセキュリティ ポリシーに準拠しているかどうかを示します。

   - **`Compliant`**
   - **`NonCompliant`**
   - **`NotAvailable`**

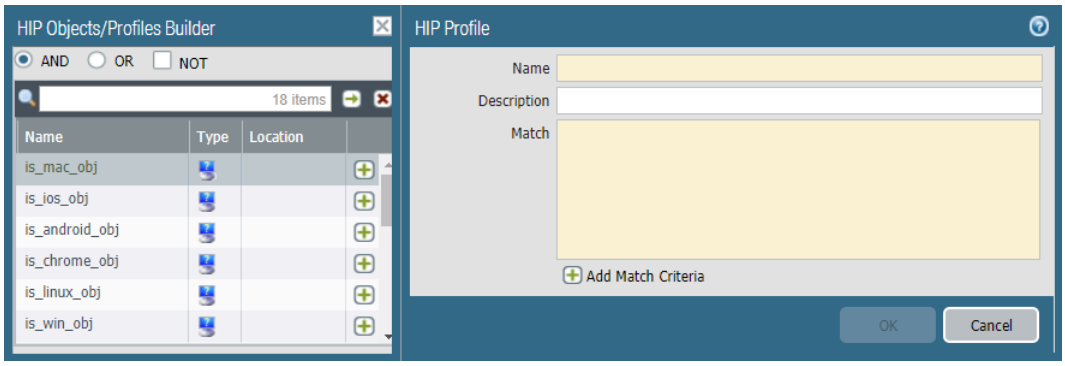


5. **OK** をクリックして HIP オブジェクトを保存します。
6. 以上の手順を繰り返して、必要な HIP オブジェクトをそれぞれ追加します。
7. 変更を **Commit**（コミット）します。

STEP 5 | ポリシーで使用する HIP プロファイルを作成します。

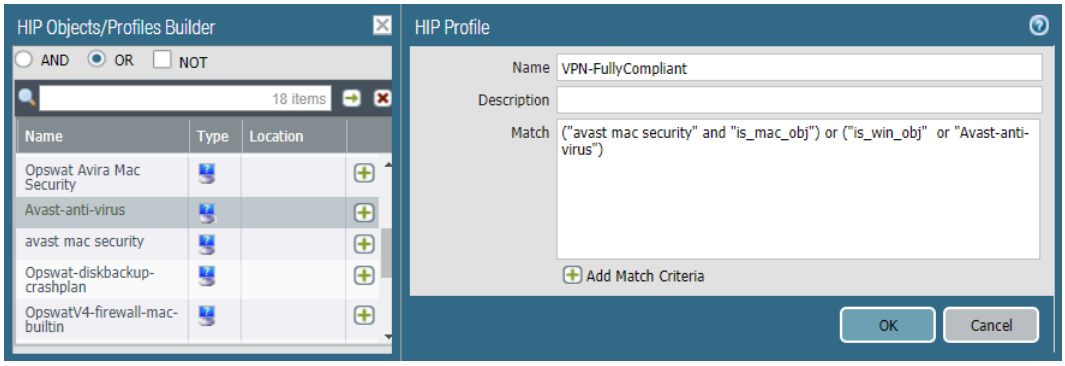
HIP プロファイルを作成すると、Boolean ロジックを使用して、以前に作成した HIP オブジェクト（および他の HIP プロファイル）を組み合わせることができます。たとえば、作成した HIP プロファイルに対してトラフィック フローを評価し、一致か不一致かを判定することができます。一致があれば、対応するポリシー ルールが適用されます。一致がなければ、他のポリシー照合条件と同様に、フローは次のルールに対して評価されます。

1. GlobalProtect ゲートウェイをホストするファイアウォールで（複数のゲートウェイの間で HIP プロファイルを共有する場合は Panorama で）、**Objects**（オブジェクト） > **GlobalProtect** > **HIP Profiles**（**HIP** プロファイル）の順に選択し、HIP プロファイルを **Add**（追加）します。
2. **Name**（名前）および**Description**（説明）を入力してプロファイルを識別します。
3. **Add Match Criteria**（一致条件の追加）をクリックして、HIP Objects/Profiles Builder（HIP オブジェクト/プロファイル ビルダー）を開きます。
4. 一致条件として使用する HIP オブジェクトまたはプロファイルを選択し、次に Add（追加）アイコン（⊕）をクリックして、HIP Profile（HIP プロファイル）ダイアログの **Match**（一致）テキスト ボックスに移動させます。オブジェクトの条件がフローに当てはまらない場合にのみ HIP プロファイルでオブジェクトを一致として評価する場合、オブジェクトを追加する前に、**NOT** チェック ボックスをオンにします。



5. 続けて、作成するプロファイルに必要なだけ一致条件を追加して、追加した条件の間に Boolean 演算子ラジオ ボタン（**AND** または **OR**）を選択します）ここでも必要に応じて **NOT** チェック ボックスを使用します）。
6. 複雑な Boolean 式を作成する場合は、**Match**（一致）テキスト ボックス内の適切な位置に手動でかっこを追加して、HIP プロファイルが意図したロジックを使用して評価されるようにします。たとえば、以下の HIP プロファイルは、FileVault ディスク暗号化（macOS システム）または TrueCrypt ディスク暗号化（Windows システム）が設定

されていて、必要なドメインに属し、Symantec アンチウイルス クライアントがインストールされているホストから発生するトラフィックを照合します。



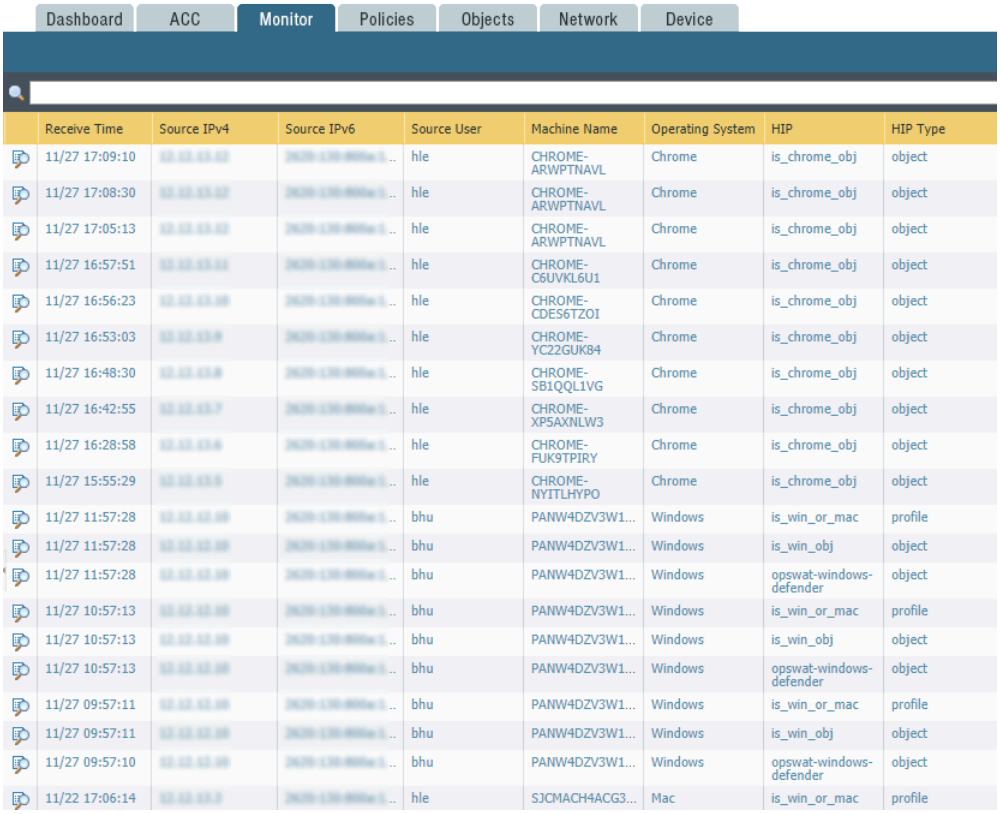
7. すべての一致条件の追加が完了したら、**OK** をクリックしてプロファイルを保存します。
8. 以上の手順を繰り返して、必要な HIP プロファイルをそれぞれ追加します。
9. 変更を **Commit**（コミット）します。

STEP 6 | 作成した HIP オブジェクトおよび HIP プロファイルが GlobalProtect トラフィックと予想通りに照合されることを確認します。

ホスト エンドポイントのセキュリティの状態およびアクティビティをモニターする手段として *HIP* オブジェクトおよび *HIP* プロファイルをモニターすることを検討します。時間経過と共にホスト情報を監視していくことで、セキュリティとコンプライアンスの問題がどこにあるのかを理解しやすくなり、有用なポリシーを作成するのに役立ちます。詳細については、エンドポイントの状態の表示方法を参照してください。

GlobalProtect ユーザーが接続しているゲートウェイで、**Monitor**（監視） > **Logs**（ログ） > **HIP Match**（**HIP** マッチ）の順に選択します。このログは、定義した HIP オブジェクトおよび HIP プロファイルに対して、アプリによってレポートされた生 HIP データを評価したと

きにゲートウェイで識別されたすべての一致を示します。他のログと異なり、HIP マッチでは、セキュリティ ポリシーが一致しなくてもログを記録することができます。



STEP 7 | HIP ベースのアクセス制御を必要とする、リクエストを送信する GlobalProtect ユーザーが含まれる送信元ゾーンの User-ID を有効にします。たとえユーザー識別機能を使用する予定がなくても、User-ID を有効にする必要があります。有効にしないと、ファイアウォールで HIP マッチ ログ エントリが生成できなくなります。

1. **[Network]** > **[ゾーン]** の順に選択します。
2. User-ID を有効にするゾーンの **Name**（名前）をクリックします。
3. **Enable User Identification (ユーザー ID の有効化)** を行って **OK** をクリックします。

STEP 8 | HIP が有効なセキュリティ ルールをゲートウェイに作成します。

セキュリティ ルールを作成し、送信元および宛先の基準に基づくフローに適合することをテストしてから、HIP プロファイルに追加することをお勧めします。こうすることで、HIP が有効なルールのポリシー内での配置を効果的に判断できます。

1. **[Policies]** > **[セキュリティ]** の順に選択し、HIP プロファイルを追加するルールを選択します。
2. **Source**（送信元） タブで、**Source Zone**（送信元ゾーン） がで User-ID を有効にしたゾーンであることを確認します。
3. **User**（ユーザー）タブで、ユーザーの識別に使用する **HIP Profiles**（**HIP** プロファイル）を **Add**（追加）します。
4. **OK** をクリックしてルールを保存します。
5. 変更を **Commit**（コミット）します。

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

STEP 9 | HIP プロファイルを使用しているセキュリティ ルールが適用されるときにエンド ユーザーに表示される通知メッセージを定義します。

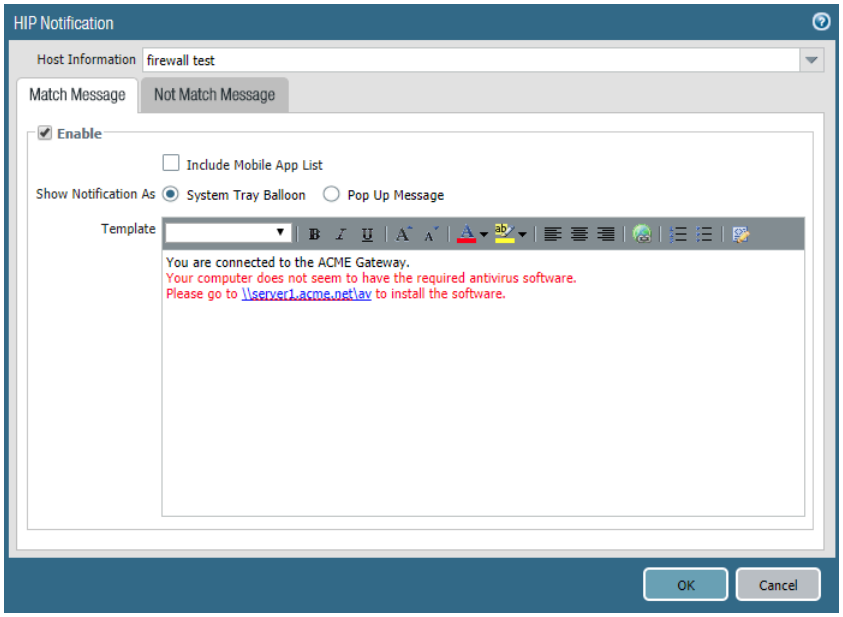
通知メッセージが表示されるタイミング（すなわち、ユーザーの設定がポリシーの HIP プロファイルに一致するときに表示されるのか、一致しないときに表示されるのか）に関する決定は、ポリシーおよび HIP の一致（または不一致）の意味に大いに依存します。つまり、一致することは、ネットワーク リソースへのフル アクセス権限が付与されていることを意味するのでしょうか。それとも、遵守していないことが原因で、アクセスが制限されたことを意味するのでしょうか。

たとえば、会社の必須のアンチウイルスおよびアンチスパイウェア ソフトウェア パッケージがインストールされていない場合に一致する HIP プロファイルを作成するとします。この場合、HIP プロファイルに一致するユーザーに対して、ソフトウェアをインストールする必要があることを伝える HIP 通知メッセージを作成することが必要になる場合があります。または、これらと同じアプリケーションがインストールされている場合に HIP プロファイルが一致するなら、プロファイルに一致しないユーザーに対してメッセージを作成することが必要になる場合があります。

1. GlobalProtect ゲートウェイをホストしているファイアウォールで、**Network**（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ）の順に選択します。
2. HIP 通知メッセージを追加するゲートウェイ構成を選択します。
3. **Agent**（エージェント） > **HIP Notification**（**HIP** 通知）の順に選択し、**Add**（追加）をクリックします。
4. **Host Information**（ホスト情報）ドロップダウンから、このメッセージが適用される HIP プロファイルを選択します。
5. 対応する HIP プロファイルが一致または不一致のときにメッセージを表示するかどうかによって、**Match Message**（メッセージの一致）または**Not Match Message**（一致しないメッセージ）を選択します。場合によっては、照合するオブジェクトおよびポリ

シーの対象に応じて、一致する場合と一致しない場合の両方でメッセージの作成が必要になることがあります。

6. **Match Message**（メッセージの一致）または **Not Match Message**（一致しないメッセージ）を **Enable**（有効）にして、**Pop Up Message**（ポップアップメッセージ）または **System Tray Balloon**（システムトレイのバルーン）としてメッセージを表示するかどうかを選択します。
7. **Template**（テンプレート）テキスト ボックスにメッセージのテキストを入力し、次に **OK** をクリックします。テキスト ボックスにはテキストの WYSIWYG ビューおよび HTML ソースビューの両方が表示されます。これらは、**Source Edit**（ソース編集）アイコン を使用して切り替えることができます。ツールバーには、テキストを書式設定したり、外部ドキュメントへのハイパーリンク を作成したり（必要なソフトウェア プログラムのダウンロード URL にユーザーを直接リンクさせる場合など）する、様々なオプションが用意されています。



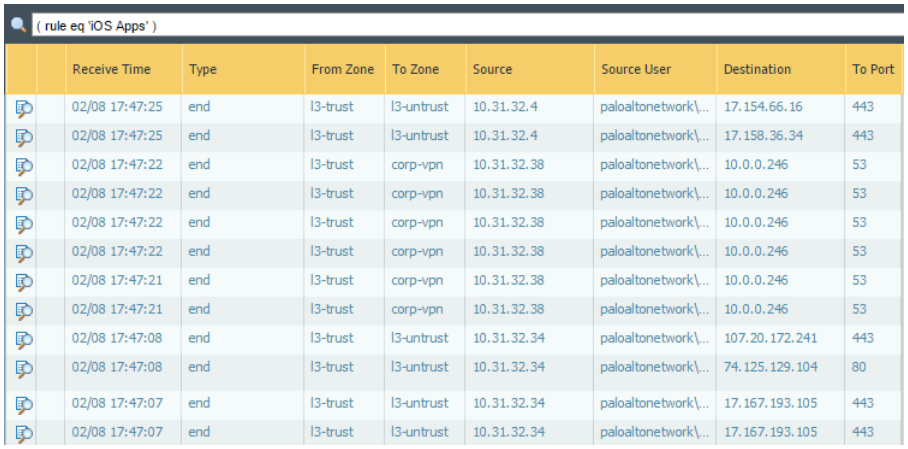
8. 定義するメッセージごとにこの手順を繰り返します。
9. 変更を **Commit**（コミット）します。

STEP 10 | HIP プロファイルが正常に動作していることを確認します。

以下のように、トラフィック ログを使用して、どのトラフィックが HIP が有効なポリシーに到達しているかをモニターできます。

1. ゲートウェイをホストしているファイアウォールで、**Monitor**（監視） > **GlobalProtect** > **Traffic**（トラフィック）の順に選択します。
2. ログをフィルタリングして、監視対象の HIP プロファイルとルールに一致するトラフィックのみを表示します。たとえば、「iOS Apps」という名前のセキュリティ ルー

ルに一致するトラフィックを検索するには、以下のようにフィルタ テキスト ボックスに「（**rule eq 'iOS Apps'** ）」と入力します。



エンドポイントからのアプリケーションおよびプロセス データの収集

Windows レジストリと macOS plist を使用して、それぞれ Windows および macOSオペレーティング システムでの設定項目を設定し、保存することができます。カスタム チェックを作成し、Windows および macOS エンドポイントで、アプリケーションがインストールされている（対応するレジストリ キーまたは plist キーがある）かどうか、または実行中（対応する実行中のプロセスがある）かどうかを判定することができます。カスタム チェックを有効にすると、GlobalProtect アプリにより、特定のレジストリ情報（Windows エンドポイントのレジストリ キーとレジストリ キーの値）および設定リスト（plist）情報（macOS エンドポイントの plist と plist キー）が収集されます。カスタム チェックで収集されるように定義したデータは、GlobalProtect アプリによって収集されるホスト情報の生データに含められ、アプリが接続するときに GlobalProtect ゲートウェイに送信されます。

カスタム チェックで収集されるデータをモニターするには、HIP オブジェクトを作成します。次に、その HIP オブジェクトを HIP プロファイルに追加し、収集したデータとエンドポイント トラフィックを照合して、セキュリティ ルールを適用します。ゲートウェイでは、（カスタム チェックで定義されているデータと照合される）HIP オブジェクトを使用して、アプリによって送信された生のホスト情報をフィルタにかけます。ゲートウェイがエンドポイント データを HIP オブジェクトと照合すると、そのデータについての HIP マッチ ログ エントリが生成されます。ゲートウェイで HIP プロファイルを使用して、収集したデータをセキュリティ ルールと照合することもできます。HIP プロファイルをセキュリティ ポリシー ルールの条件として使用する場合、ゲートウェイは、一致するトラフィックでそのセキュリティ ルールを適用します。

以下のステップを実行してカスタム チェックを有効にし、Windows および macOS エンドポイントからデータを収集します。このワークフローには、セキュリティ ポリシーの一致条件としてエンドポイント データを使用して、トラフィックを監視、識別、および処理するためのカスタムチェック用の HIP オブジェクトと HIP プロファイルを作成するオプションの手順も含まれています。

Windows レジストリまたはグローバル *macOS plist* から直接にアプリの設定を定義する方法の詳細は、アプリの設定の透過的なデプロイを参照してください。

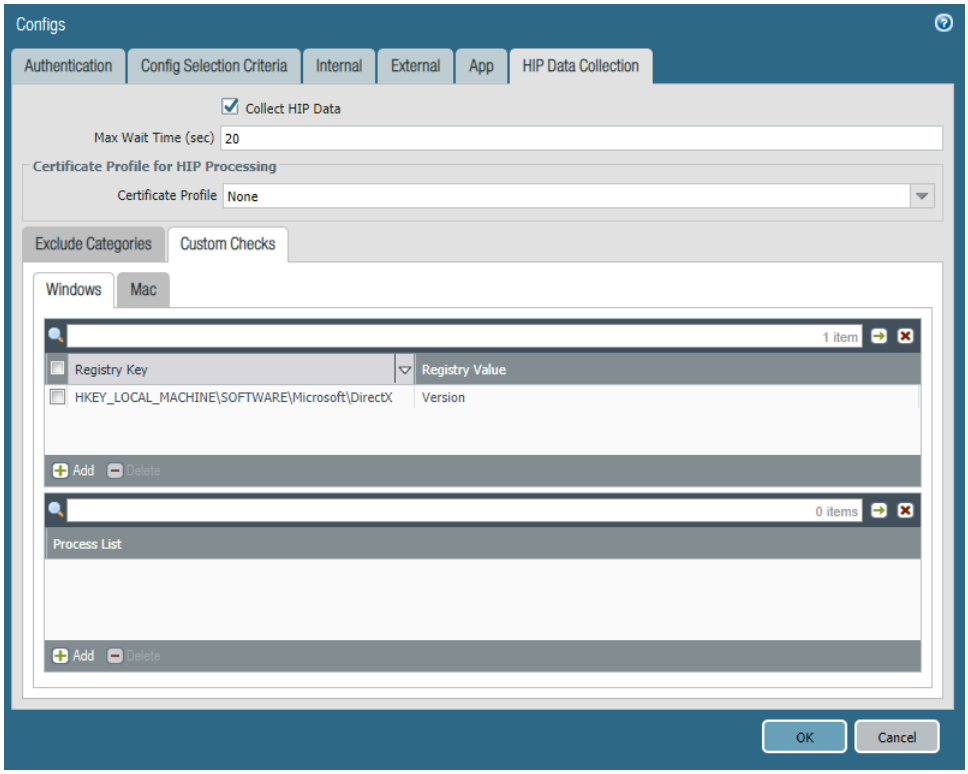
STEP 1 | GlobalProtect アプリを有効にして、Windows エンドポイントから Windows レジストリ情報を収集するか、macOS エンドポイントから plist 情報を収集します。収集される情報に

は、エンドポイントに特定のアプリケーションがインストールされているかどうかや、アプリケーションの特定の属性またはプロパティを含めることができます。

Windows エンドポイントからのデータの収集：

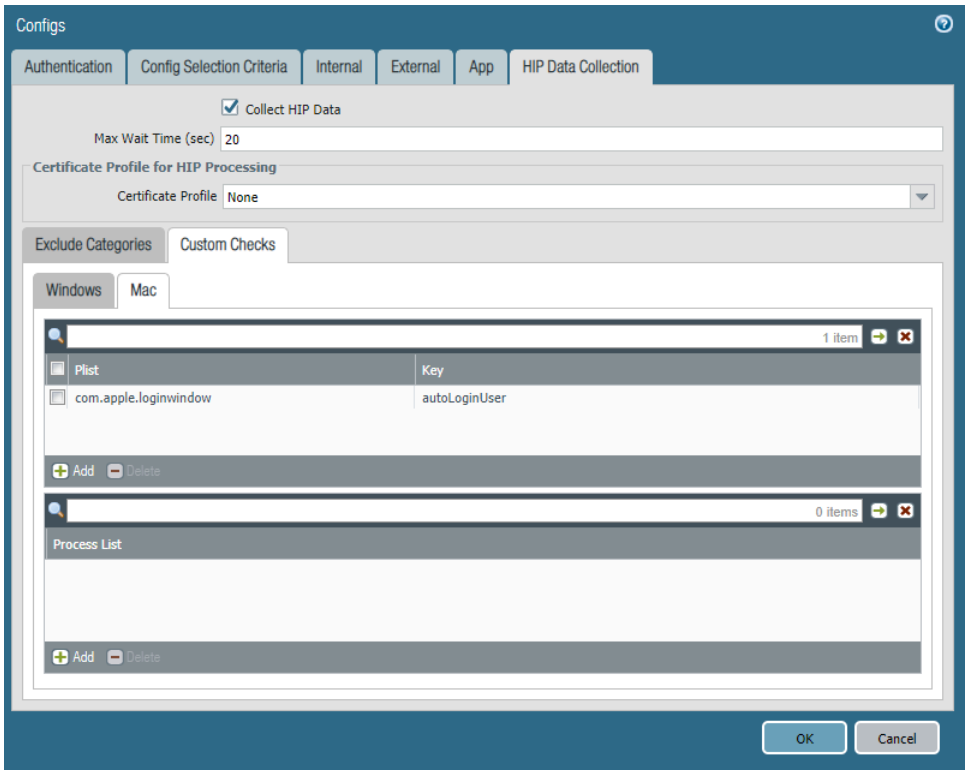
1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します
2. 既存のポータル設定を選択するか、新しく **Add**（追加）します。
3. **Agent**（エージェント）タブで、変更するクライアントの設定を選択します。または、新しい設定を **Add**（追加）します）。
4. **HIP Data Collection (HIP** データ収集**)** を選択します。
5. GlobalProtect アプリケーションを有効化して **Collect HIP Data (HIP** データを収集**)** します。
6. **Custom Checks**（カスタム チェック） > **Windows**を選択して、情報を収集する **Registry Key**（レジストリ キー）を **Add**（追加）します。データ収集の対象をレジスト

リ キーに含まれている値に限定する場合は、対応する **Registry Value**（レジストリ値）を追加します。

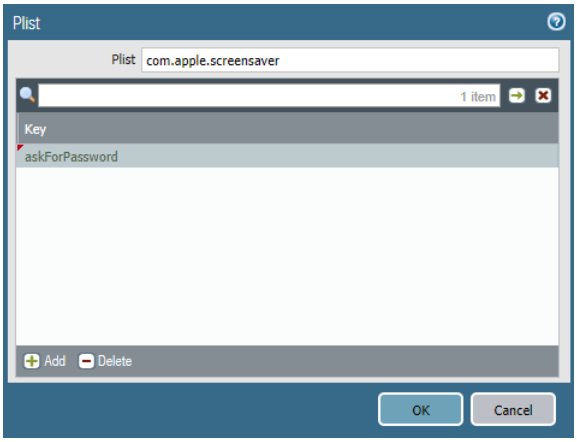


macOS エンドポイントからのデータの収集：

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します
2. 既存のポータル設定を選択するか、新しく **Add**（追加）します。
3. **Agent**（エージェント）タブで、変更するクライアントの設定を選択します。または、新しい設定を **Add**（追加）します）。
4. **HIP Data Collection (HIP** データ収集**)** を選択します。
5. GlobalProtect アプリケーションを有効化して **Collect HIP Data (HIP** データを収集**)** します
6. **Custom Checks**（カスタム チェック） > **Mac**を選択して、情報を収集する **Plist** と対応する plist **Key**（キー）を **Add**（追加）して、アプリケーションがインストールされているかどうかを判断します。



たとえば、スクリーン セーバーの起動後に macOS エンドポイントを呼び戻すためにパスワードが必要かどうかについての情報を収集するには、**Plist** **`com.apple.screensaver`** とその **Key**（キー） **`askForPassword`** を **Add**（追加）します。



STEP 2 | （任意）エンドポイントで特定のプロセスが実行されているかどうかを確認します。

1. **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）を選択します
2. 既存のポータル設定を選択するか、新しく **Add**（追加）します。
3. **Agent**（エージェント）タブで、変更するクライアントの設定を選択します。または、新しい設定を **Add**（追加）します）。
4. **HIP Data Collection (HIP** データ収集**)** を選択します。
5. GlobalProtect アプリケーションを有効化して **Collect HIP Data (HIP** データを収集**)** します
6. **Custom Checks (**カスタムチェック**)** > **Windows** あるいは **Mac** を選択します。
7. 情報を収集する対象のプロセスの名前を、**Process List**（プロセス リスト） に **Add**（追加） します。

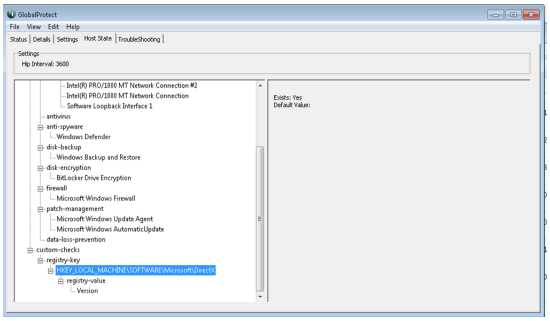
STEP 3 | カスタム チェックを保存します。

OK をクリックし、変更を **Commit**（コミット**)** します。 します。

STEP 4 | GlobalProtect アプリが、カスタム チェックで定義されているデータをエンドポイントから収集することを確認します。

Windows エンドポイントの場合：

1. システム トレイのアイコンをクリックして Windows エンドポイント用 GlobalProtect アプリを起動します。GlobalProtect ステータス パネルが開きます。
2. 設定（ ）アイコンをクリックして、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. **Host Profile**（ホスト プロファイル）タブを選択すると、GlobalProtect アプリがエンドポイントから収集している情報が表示されます。**custom-checks**（カスタムチェック）ドロップダウンに、収集のために定義したデータが表示されていることを確認します。



macOS エンドポイントの場合：

1. システム トレイのアイコンをクリックして macOS エンドポイント用 GlobalProtect アプリを起動します。GlobalProtect ステータス パネルが開きます。
2. 設定（ ）アイコンをクリックして、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. **Host Profile**（ホスト プロファイル）タブを選択すると、GlobalProtect アプリがエンドポイントから収集している情報が表示されます。**custom-checks**（カスタムチェック）ドロップダウンに、収集のために定義したデータが表示されていることを確認します。

STEP 5 | （任意）レジストリ キー（Windows）または plist（macOS）に一致する HIP オブジェクトを作成します。これにより、GlobalProtect アプリから収集された生のホスト情報をフィルタリングして、カスタムチェックのデータを監視できます。

カスタム チェック データとして HIP オブジェクトが定義されている場合には、ゲートウェイでアプリから送信された生データが HIP オブジェクトと照合され、そのデータの HIP マッチ ログ エントリが生成されます（**Monitor** > **HIP Match**（**HIP** マッチ））。

Windows および macOS エンドポイントの場合：

1. **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP** オブジェクト**)** の順に選択します。
2. 既存の HIP オブジェクトを選択するか、新しく **Add (追加)** します。
3. **Custom Checks**（カスタム チェック）タブで、チェックボックスを選択し、**Custom Checks**（カスタム チェック）を有効にします。

Windows エンドポイントのみの場合：

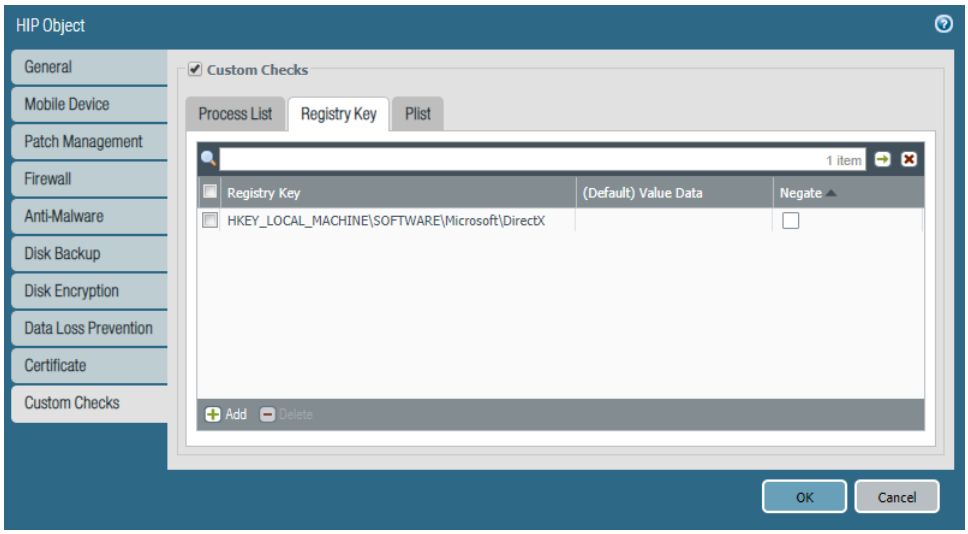
1. 指定のレジストリキーの Windows エンドポイントを検査するには、**Custom Checks (**カスタム チェック**)** > **Registry Key (**レジストリ キー**)** を選択してから、マッチさせるレジストリキーを **Add (追加)** します。入力を求められたら **Registry Key (**レジストリキー**)** を入力し、次のいずれかのオプションを設定します：
   - レジストリキーのデフォルトの値にマッチさせる場合は、**(Default) Value Data ((**デフォルトの**)** 値データ**)** を入力します。
   - 指定したレジストリ キーが存在しないクライアントのみを識別するには、**[**キーが存在しないか、指定した値データと一致しない**]** をオンにします。

   > ***(Default) Value Data ((***デフォルトの***)***値データ***)*** と ***Key does not exist or match the specified value data (***キーが存在しないか指定した値データにマッチ***)*** オプションを両方同時に設定することはできません。
2. レジストリキー内の特定の値にマッチさせる場合は、**Custom Checks (**カスタム チェック**)** > **Registry Key (**レジストリ キー**)** を選択してから、マッチさせるレジストリキーを **Add (追加)** します。入力を求められたら **Registry Key (**レジストリキー**)** を入力します。**Add (追加)** をクリックしてから次のいずれかのオプションを設定します：
   - レジストリキー内の特定の値にマッチさせる場合は、**Registry Value (**レジストリ値**)** および対応する **Value Data (**値データ**)** を入力します。

- 指定したレジストリ値を持たないエンドポイントにマッチさせる場合は、**Registry Value (**レジストリ値**)** を入力してから **Negate (**反転**)** チェックボックスを選択します。

  このオプションを使用する場合は、***Registry Key (***レジストリキー***)*** の ***Value Data (***値データ***)*** を入力しないでください。

  レジストリキーに複数のレジストリ値を追加すると、*GlobalProtect* ゲートウェイはエンドポイントに対して、指定したすべてのレジストリ値をチェックします。

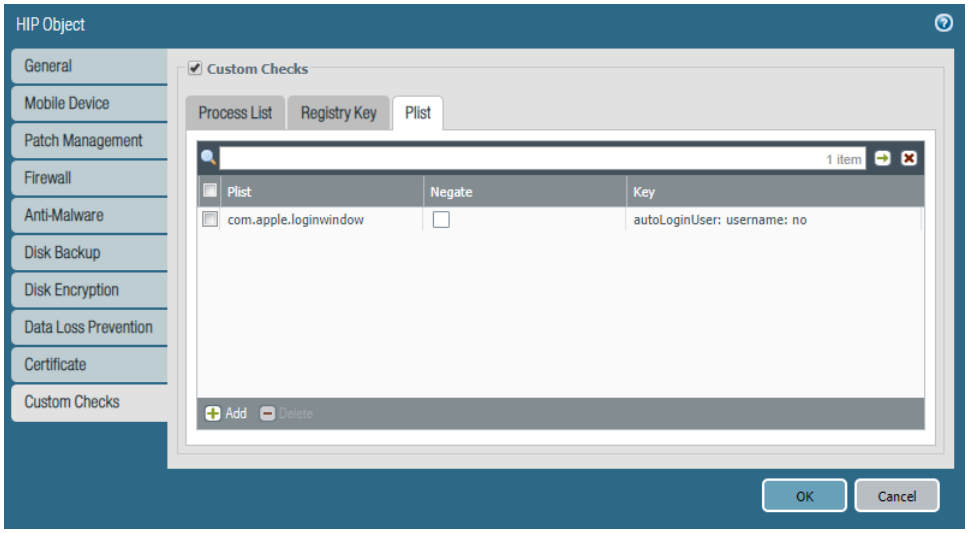


3. **OK** をクリックして HIP オブジェクトを保存します。変更を **Commit**（コミット）して、次のデバイス チェックインで **HIP Match**（**HIP** マッチ）ログのデータを表示するか、またはステップ 6 に進みます。

macOS エンドポイントのみの場合：

1. 特定の plist について macOS エンドポイントをチェックするには、**Plist** を選択してから、チェックしたい plist を **Add (**追加**)** します。入力を求められたら **Plist** の名前を入力します。指定した plist を持たない macOS エンドポイントと一致させる場合は、**Plist does not exist**（**Plist** がありません）オプションを有効にします。
2. plist 内の特定のキーと値のペアにマッチさせる場合は、**Plist** を選択してから、チェックしたい plist を **Add (**追加**)** します。入力を求められたら **Plist** の名前を入力し、マッチさせる **Key (**キー**)** および対応する **Value (**値**)** を **Add (**追加**)** します。（または、特定の

キーと値が設定されていないエンドポイントを識別する場合は、**Key**（キー） および **Value**（値）に値を追加した後に **Negate**（反転）を選択します）。



3. **OK** をクリックして HIP オブジェクトを保存します。変更を **Commit**（コミット）して、次のデバイス チェックインで **HIP Match**（**HIP** マッチ）ログのデータを表示するか、またはステップ 6 に進みます。

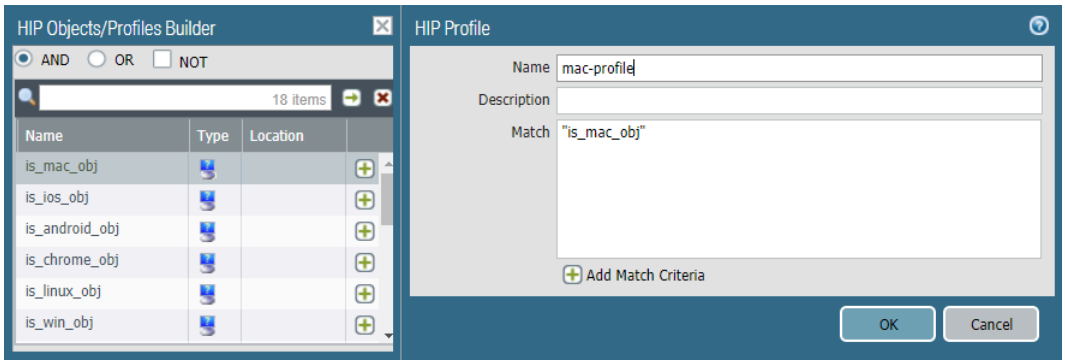
STEP 6 | （任意）HIP プロファイルを作成して、HIP オブジェクトがトラフィックに対して評価されるようにすることができます。

HIP プロファイルは、セキュリティ ポリシーに適合するトラフィックがあるかどうかをチェックするための追加条件として、そのポリシーに追加することができます。トラフィッ

クが HIP プロファイルに一致する場合は、そのトラフィックにセキュリティ ポリシー ルールが適用されます。

HIP プロファイルの作成についての詳細は、HIP ベースのポリシー適用の設定を参照してください。

1. **Objects (オブジェクト)** > **GlobalProtect** > **HIP Objects (HIP オブジェクト)** の順に選択します。
2. 既存の HIP プロファイルを選択するか、新しく **Add**（追加）します。
3. **Add Match Criteria**（一致条件の追加）をクリックして、HIP Objects/Profiles Builder（HIP オブジェクト/プロファイル ビルダー）を開きます。
4. 一致条件として使用する **HIP** オブジェクトまたはプロファイルを選択し、次に Add（追加）アイコン（  ）をクリックして、HIP Profile（HIP プロファイル）ダイアログの **Match**（一致）テキスト ボックスに移動させます。
5. 新しい HIP プロファイルにオブジェクトを追加したら、**OK** をクリックして変更を **Commit**（コミット）します。



STEP 7 | HIP プロファイルをセキュリティ ポリシーに追加し、カスタム チェックで収集されたデータを使用して、トラフィックと照合して処理することができます。

Policies（ポリシー） > **Security**（セキュリティ）を選択してから、既存のセキュリティ ポリシーを選択するか新しいセキュリティ ポリシーを **Add**（追加）します。**User**（ユーザー）タブで、 **HIP Profiles**（**HIP** プロファイル）をポリシーに **Add**（追加）します。セキュリティ ポリシーのコンポーネントの詳細、およびセキュリティ ポリシーを使用してトラフィックと照合して処理する方法の詳細は、セキュリティ ポリシーを参照してください。

HIP レポートの再配信

ホスト情報プロファイル (HIP) ポリシーを一貫した形で適用し、ポリシー管理を簡略化するために、GlobalProtect アプリケーションから受信 (そして内部あるいは外部の GlobalProtect ゲートウェイに送信する) した HIP レポートをエンタープライズ内の他のゲートウェイ、ファイアウォール、専用ログコレクタ (DLC)、Panorama アプライアンスに再配信することができます。次のユースケースで HIP レポートの再配信が役立ちます：

- 内部および外部の GlobalProtect ゲートウェイの両方に一貫したポリシーを適用したい場合。
- 複数のファイアウォールを経由する特定のユーザーのトラフィックに一貫した HIP ポリシーを適用したい場合。

HIP レポートを再配信するために、User-ID 情報の再配信 で使用したのと同じデプロイの推奨事項とベストプラクティスを採用します。

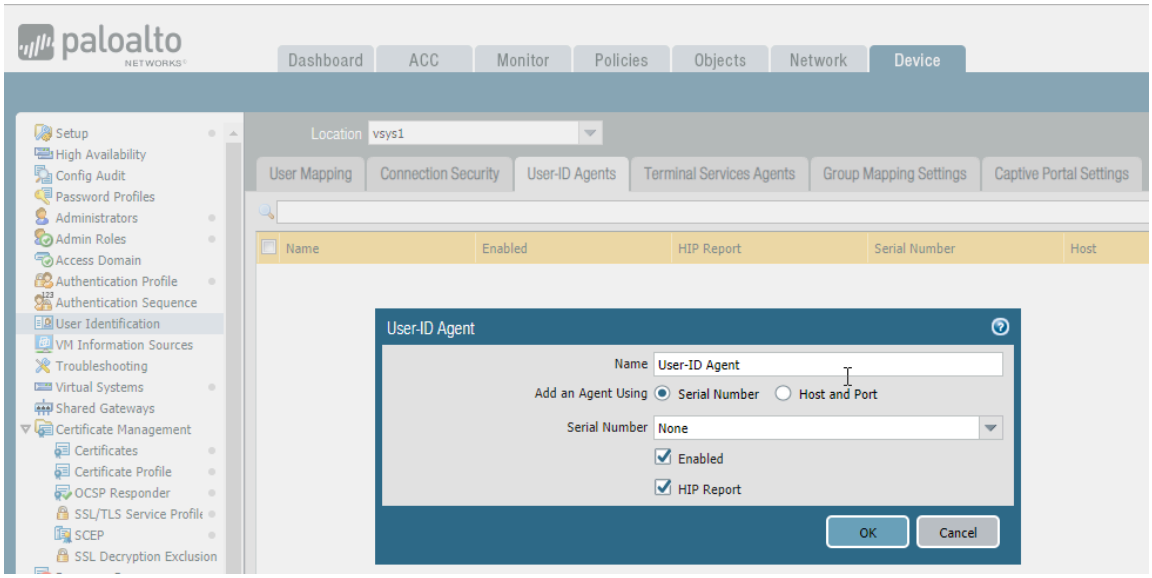
次のステップに従い、HIP レポートの再配信を設定します。

STEP 1 | HIP ベースのポリシー適用の設定 ゲートウェイおよびファイアウォールについて。

STEP 2 | HIP レポートの再配信を設定します。

1. **Device (デバイス)** > **User Identification (ユーザー ID)** > **User-ID Agents (User-ID エージェント)** の順に選択します。
2. 既存の User-ID エージェントを選択するか、新しく **Add (追加)** します。

   エージェントは *Palo Alto Networks* 次世代ファイアウォール、*GlobalProtect* ゲートウェイ、*DLC*、あるいは *Panorama* アプライアンスでなければなりません。
3. **HIP Report (HIP レポート)** を選択します。



4. <239>OK</239> をクリックします。

STEP 3 | GlobalProtect ファイアウォールあるいはゲートウェイを使用して HIP レポートを配信する場合は、必ず HIP レポートの再配信に使用するファイアウォールあるいはゲートウェイ上

のグループ マッピング設定を、User-ID を設定したファイアウォールあるいはゲートウェイの次の属性と一致させてください。

Panorama アプライアンスあるいは *DLC* を使用して *HIP* レポートを配信する場合は、このステップをスキップします。

- HIP レポートの再配信用ファイアウォールあるいはゲートウェイのユーザー属性を、User-ID ファイアウォールあるいはゲートウェイのユーザー属性と一致させる設定を行います。

  例えば、HIP レポートの再配信に使用するファイアウォールあるいはゲートウェイが、**Primary attribute (プライマリ属性)** という sAMAccountName、**Alternate Username 1 (代替ユーザー名 1)** という User Principal Name (UPN) (ユーザー プリンシパル名) を持つ場合は、必ず User-ID を設定したファイアウォールあるいはゲートウェイ上で同じ値を設定します。

  属性を同じ順序にする必要はありません。例えば、*HIP* レポートの再配信用のファイアウォールが ***Primary attribute (***プライマリ属性***)*** という *sAMAccountName* および ***Alternate Username 1 (***代替ユーザー名 ***1)*** という *UPN* を持つ場合、***Alternate Username (***代替ユーザー名***)*** という *sAMAccountName* および ***Primary attribute 1 (***代替ユーザー名 ***1)*** という *UPN* を使って *User-ID* ファイアウォールを設定できます。
- グループ マッピングでユーザードメインを設定してデプロイを行う場合、HIP レポートの再配信用ファイアウォールあるいはゲートウェイのユーザードメイン属性を、User-ID ファイアウォールあるいはゲートウェイのユーザードメイン属性と一致させるよう設定します。ユーザードメイン属性は、すべてのファイアウォールおよびゲートウェイにかけて一貫したものでなければなりません。
- HIP レポートの再配信用ファイアウォールあるいはゲートウェイ上で共通ユーザーグループ (同じ認証サーバーに接続して同じユーザーグループを取得するファイアウォールおよびゲートウェイ上のユーザーグループ) を設定し、User-ID ファイアウォールあるいはゲートウェイのユーザーグループと一致させます。

STEP 4 | ユーザー ID 情報を管理対象ファイアウォールに再配信するために使用したのと同じワークフローで、管理対象の Panorama アプライアンス、ゲートウェイ、ファイアウォール、仮想システムに HIP レポートを再配信します。

エンドポイントのアクセスをブロック

ネットワークへの GlobalProtect アクセスが可能なエンドポイントをユーザーが無くした、盗まれた場合、またはユーザーが組織を離れた場合、エンドポイントをブロックリストに入れることで、そのエンドポイントからネットワークにアクセスできなくすることが可能です。

ブロックリストは論理的なネットワークの位置（例：vsys、1）のローカルにあり、ロケーション毎に最大 1,000 のエンドポイントを含めることができます。そのため、GlobalProtect のデプロイ環境をホストしているロケーションごとに別々のブロック リストを作成することが可能です。

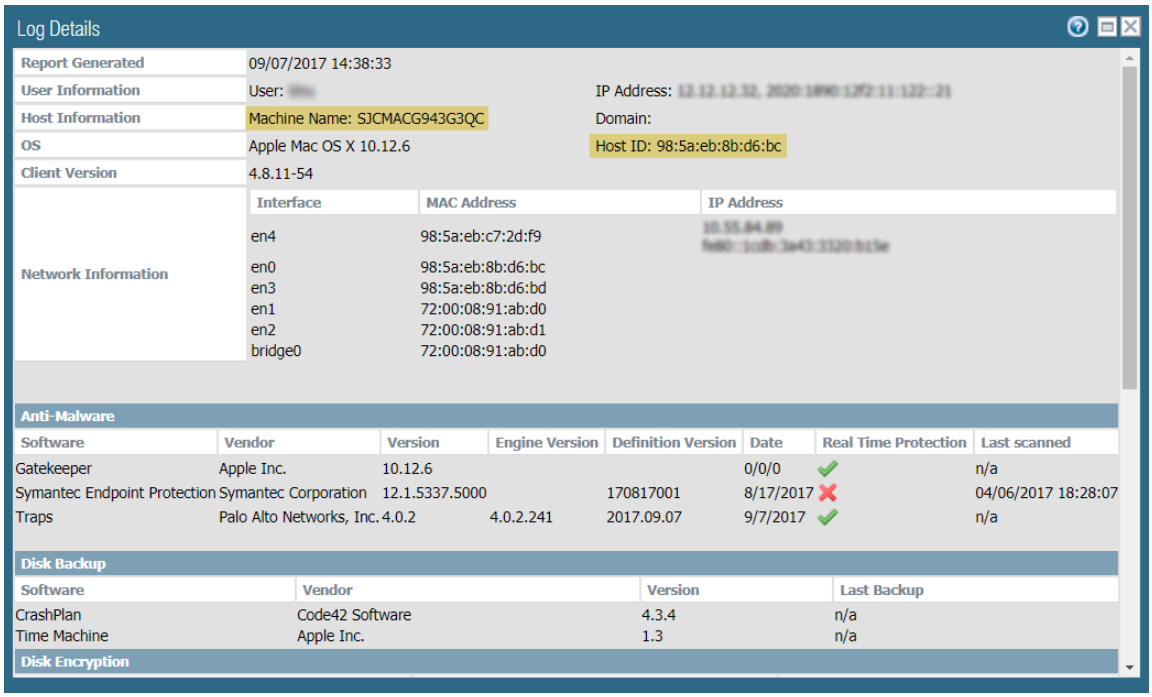
STEP 1 | ブロックするエンドポイントのホスト ID を識別します。

ホスト ID は、GlobalProtect がホストの識別のために割り当てる、一意の ID です。ホスト ID の値は、エンドポイント タイプによって異なります。

- Windows — Windows レジストリ（HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid）に保存されているマシン GUID
- macOS — 最初の組み込み物理ネットワーク インターフェイスの MAC アドレス
- Android — Android ID
- iOS — UDID
- Chrome — GlobalProtect によって割り当てられた、長さが 32 文字の一意の英数字

ホスト ID が不明な場合、HIP マッチ ログで User-ID をホスト ID に相関できます。

1. **[Monitor]**監視する > **[ログ]** > **[HIP マッチ]** の順に選択します。
2. エンドポイントに関連付けられた送信元ユーザーで、HIP マッチ ログをフィルタリングします。
3. HIP マッチ ログを開き、**OS** > **Host Id**（ホスト **ID**）でホスト ID を識別し、必要に応じて **Host Information**（ホスト情報） > **Machine Name**（マシン名）を識別します。

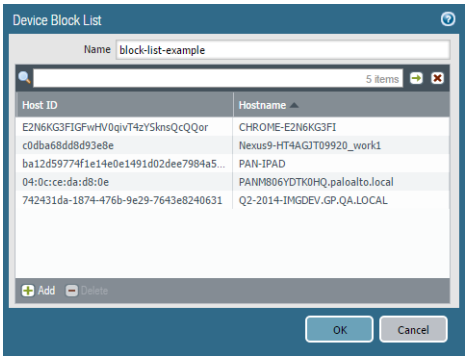


STEP 2 | デバイス ブロック リストを作成します。

Panorama テンプレートを使用してデバイス ブロック リストをファイアウォールにプッシュ送信することはできません。

1. **Network** > **GlobalProtect** > **Device Block List** (ネットワーク > GlobalProtect > デバイス ブロックリスト)を選択し、デバイス ブロックリストを**Add** (追加)します。
2. **Name**（名前）フィールドに分かりやすいリスト名を入力します。
3. ファイアウォールに仮想システム（vsys）が複数ある場合は、プロファイルの使用が可能な **Location**（場所）（vsys または **Shared**（共有）を選択します。

STEP 3 | デバイスをブロック リストに追加します。



1. エンドポイントを **Add**（追加）します。ブロックする必要があるエンドポイントのホスト ID（必須）およびホスト名（任意）を入力します。
2. 必要に応じて、他のエンドポイントを**Add**（追加）します。
3. **OK** をクリックし、ブロック リストを保存して有効化します。

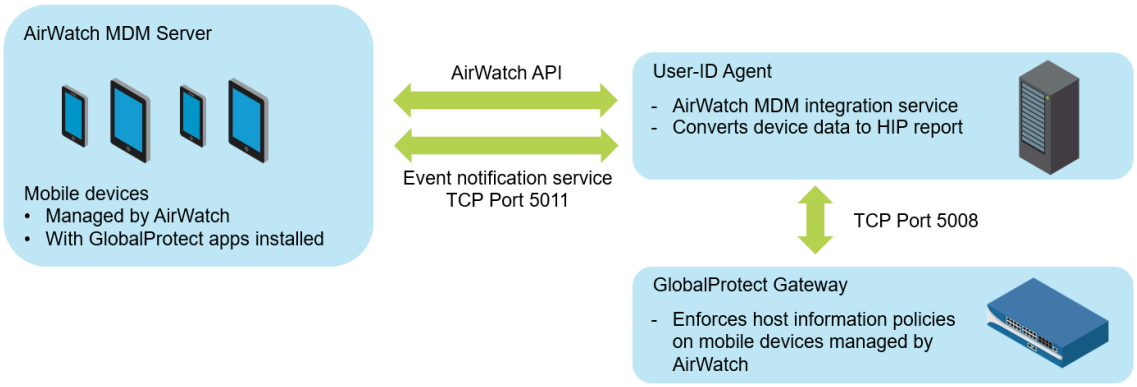
デバイス ブロック リストに対してはコミットは不要で、ただちに有効になります。

ホスト情報を収集するための Windows User-ID エージェントの設定

Windows ベースの User-ID エージェントは新しい AirWatch MDM 統合サービスをサポートするように拡張されています。このサービスにより、GlobalProtect はサービスによって収集されたホスト情報を使用して、AirWatch が管理するデバイスで HIP ベースのポリシーを実施できます。AirWatch MDM 統合サービスは Windows ベースの User-ID エージェントの一部として実行され、AirWatch API を使用して VMware AirWatch が管理するモバイル エンドポイントから情報を収集し、このデータをホスト情報に変換します。

AirWatch が管理する *Android* エンドポイントの場合、この機能は *Android for Work* エンドポイントでは使用できますが、その他のタイプの *Android* エンドポイントでは使用できません。

- MDM 統合の概要
- 収集される情報
- システム要件
- ホスト情報を取得するための GlobalProtect の設定
- MDM 統合サービスのトラブルシューティング



MDM 統合の概要

Windows ベースの User-ID エージェントに付属している MDM 統合サービスは、モバイル デバイスのホスト情報を完全に取得するために、AirWatch MDM サーバーに対する完全な HIP クエリを実行します。モバイル デバイスの GlobalProtect アプリからも HIP 情報がゲートウェイに送信され、GlobalProtect アプリと MDM 統合サービスから送信された HIP 情報をマージします。GlobalProtect アプリを実行しているモバイル デバイスが GlobalProtect ゲートウェイに接続されたときに、GlobalProtect はホスト情報プロファイルを含むセキュリティ ポリシーを適用できます。

AirWatch デバイス情報を定期的に取得するように MDM 統合サービスを設定し、この情報を GlobalProtect ゲートウェイにプッシュできます。さらに、このサービスは、AirWatch イベント

（コンプライアンス変更など）が発生したときに、AirWatch イベント通知を監視し、更新されたデバイス情報を取得できます。

収集される情報

AirWatch が管理するエンドポイントから収集された情報が HIP レポート属性に変換される方法は、以下の表の通りです。マッピングは自動的に実行されます。

AirWatch 属性	HIP レポート属性
デバイス情報	
SerialNumber	serial-number
MacAddress	wifimac
Imei	IMEI
OperatingSystem	version
Model	model
DeviceFriendlyName	devname
IsSupervised	supervised
Udid (Unique Device Identifier)	udid
UserName	user
LastEnrolledOn	enroll-time
プラットフォーム	os
EnrollmentStatus	managed-by-mdm
LastSeen	last-checkin-time
ComplianceStatus (User-ID エージェント 8.0.3 以降)	Compliant NonCompliant NotAvailable
Ownership (User-ID エージェント 8.0.3 以降)	従業員の所有 法人専用 法人の共有

AirWatch 属性	HIP レポート属性
Security Information	
DataProtectionEnabled	disk-encrypted
IsPasscodePresent	passcode-set
IsPasscodeCompliant	passcode-compliant
ネットワーク情報	
DataRoamingEnabled	data-roaming
GPS Coordinates	
latitude	latitude
longitude	longitude
SampleTime	last-location-time
アプリケーションの詳細情報	
ApplicationName	appname
Version（バージョン）	version
ApplicationIndentifier	package

システム要件

AirWatch MDM 統合サービスには、以下のソフトウェアが必要です。

ソフトウェア	最小サポート バージョン
User-IDエージェント	8.0.1
PAN-OS	7.1.0
Android 用 GlobalProtect アプリ	4.0.0
iOS 用 GlobalProtect アプリ	4.0.1
AirWatch Server	8.4.7.0

ソフトウェア	最小サポート バージョン
Windows Server	2008、2012 2016（User-ID エージェント 8.0.4 および PAN-OS 8.0.4 の場合）

ホスト情報を取得するための GlobalProtect の設定

以下の手順実行し、AirWatch が管理するデバイスからホスト情報を取得するように GlobalProtect を設定します。

STEP 1 | User-ID エージェントをインストールします。User-ID エージェントは、VMware AirWatch モバイル デバイス管理（MDM）システムへの安全な接続が可能な場所にある必要があります。

AirWatch MDM 統合サービスは、PAN-OS Windows ベースの User-ID エージェントに付属しています。

STEP 2 | Windows ベースの User-ID エージェントと GlobalProtect ゲートウェイ間の SSL 認証を設定します。

SSL 認証を設定する際には、以下の点に注意してください。

- Windows ベースの User-ID エージェントが User-ID エージェント ホストのホスト名/IP アドレスと同じ共通名（CN）を持っていること。
- サーバー証明書はファイアウォールから信頼されます（ファイアウォールの MDM 設定の信頼される CA リストに含まれる）。
- ファイアウォールで設定された MDM クライアント証明書のルート認証局（CA）証明書を Windows サーバーの Windows トラスト ストアにインポートする必要があります。
  1. Windows ベースの User-ID エージェントと GlobalProtect ゲートウェイ間の認証用にサーバー証明書と秘密鍵を取得します。証明書バンドルは、PEM 証明書、完全な証明書チェーン、秘密鍵が含まれる PEM フォーマットである必要があります。
  2. Windows ベースの User-ID エージェントを開き、**Server Certificate**（サーバー証明書）を選択します。
  3. サーバー証明書を **Add**（追加）します。
- 証明書ファイルを **Browse**（参照）してファイルを **Open**（開く）操作を行い、証明書を Windows ベースの User-ID エージェントにアップロードします。
- 証明書の **Private Key Password**（秘密鍵パスワード）を入力します。
- **[OK]** をクリックします。

エージェントは証明書が有効であることを確認し、秘密鍵の暗号化パスワードをホスト マシンの Windows 認証ストアに保存します。

インストールに成功すると、証明書に関する詳細情報（共通名、有効期限、発行者など）が **Server Certificate**（サーバー証明書）タブに表示されます。

1. Windows ベースの User-ID エージェントを再起動します。

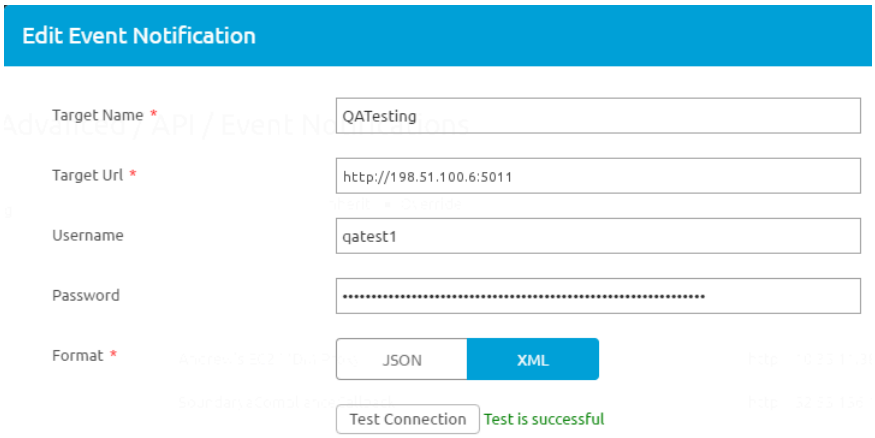
STEP 3 | Windows ベースの User-ID エージェントで MDM 統合サービスを設定します。

1. Windows ベースの User-ID エージェントで **MDM Integration**（**MDM** 統合）を選択します。
2. TCP 通信用に **Gateway Connection TCP Port**（ゲートウェイ接続 **TCP** ポート）を指定します。Windows ベースの User-ID エージェントはこのポートですべての MDM 関連のメッセージをリッスンします。デフォルト ポートは 5008 です。ポートを変更するには、1 ～ 65535 の数値を指定します。
3. **Setup**（セットアップ）タブで **Edit**（編集）をクリックします。
4. **MDM Vendor**（**MDM** ベンダー）に **AirWatch** を選択します。

STEP 4 | AirWatch イベントを監視して収集する **MDM Event Notification**（**MDM** イベント通知）設定を指定します（たとえば、デバイスの登録、デバイスでのワイプ、コンプライアンスの変更など）。イベントが発生すると、MDM 統合サービスは AirWatch API から更新された

デバイス情報を取得し、この情報をすべての設定済み GlobalProtect ゲートウェイにプッシュします。

MDM Event Notification（***MDM*** イベント通知）に関しては、必ずここで入力した値を *AirWatch* コンソールの ***Groups & Settings***（グループおよび設定） > ***All Settings***（すべての設定） > ***System***（システム） > ***Advanced***（詳細） > ***API*** > ***Event Notifications***（イベント通知）でも設定する必要があります。

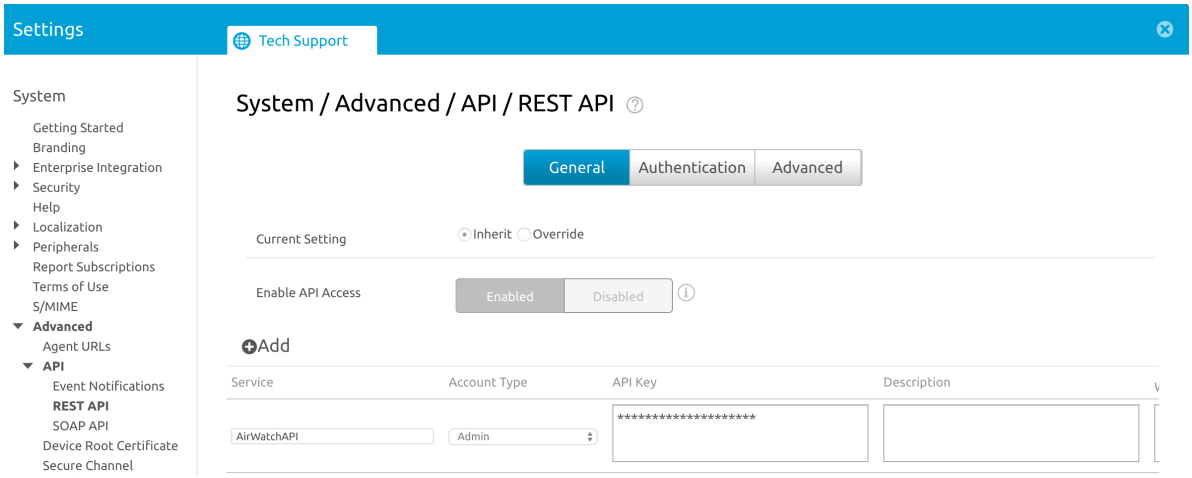


- イベント通知サービスと通信するための **TCP Port**（**TCP** ポート）を設定します。**`http://<external_hostname>/<ip_address>:<port>`**。ここで、 **`<ip-address>`** は MDM 統合サービスの IP アドレスです。デフォルト ポートは 5011 です。ポートを変更するには、1 ～ 65535 の数値を指定します。
- イベント通知について、受信した要求を認証するために必要な認証情報である **Username**（ユーザー名）と **Password**（パスワード）を入力します。
- MDM イベントにアクセスするための **Permitted IP**（アクセス許可 **IP**）アドレスを入力します。これは、MDM イベントがポストされる IP アドレスのコンマ区切りリストです。たとえば、AirWatch サーバーの IP アドレスです。指定する IP アドレスの指針については、AirWatch サポート チームにお問い合わせください。

STEP 5 | AirWatch API と接続するための **MDM API Authentication**（**MDM API** 認証） 設定を追加します。

- Windows ベースの User-ID エージェントを接続する AirWatch MDM サーバーの **Server Address**（サーバー アドレス）を入力します。たとえば、**`api.awmdm.com`** のように入力します。
- AirWatch MDM API にアクセスするために必要な認証情報である **Username**（ユーザー名）と **Password**（パスワード）を入力します。
- **Tenant Code**（テナント コード）を入力します。これは、AirWatch MDM API にアクセスするために必要な一意の 16 進数のコード番号です。AirWatch コンソールで、テナン

ト コードは **System**（システム） > **Advanced**（詳細） > **API** > **REST API** > **API Key**（API キー）で確認できます。



- **Mobile Device State Retrieval Interval**（モバイル デバイスの状態取得間隔）を入力します。この設定により、AirWatch が管理するデバイスからホスト情報を取得する頻度が制御されます。デフォルトの間隔は 30 分です。間隔を変更するには、1 ～ 600 の数値を指定します。

STEP 6 | 変更を **Commit (コミット)** します。

STEP 7 | **Test Connection**（接続のテスト）をクリックして、Windows ベースの User-ID エージェントが AirWatch API に接続できることを確認します。

STEP 8 | MDM 統合サービスと通信して、AirWatch が管理するデバイスの HIP レポートを取得するように GlobalProtect ゲートウェイを設定します。

1. PAN-OS Web インターフェイスで、**Network**（ネットワーク） > **GlobalProtect** > **MDM** の順に選択します。
2. MDM 統合サービスに関する以下の情報を **Add**（追加）します。

- **Name**（名前） – MDM 統合サービスの名前を入力します（最大 31 文字）。名前の大文字と小文字は区別されます。また、一意の名前にする必要があります。文字、数字、スペース、ハイフン、およびアンダースコアのみを使用してください。
- （任意）ゲートウェイが属している仮想システムを選択します。
- **Server**（サーバー） – ゲートウェイが HIP レポートを取得するために接続する、Airwatch MDM 統合サービスのインターフェイスの IP アドレスまたは FQDN を入力します。このインターフェイスへのサービス ルートがあることを確認します。
- **Connection Port**（接続ポート） – MDM 統合サービスが HIP レポート要求をリッスンする接続ポートを入力します。デフォルト ポートは 5008 です。ポートを変更するには、1 ～ 65535 の数値を指定します。
- **Client Certificate**（クライアント証明書） – HTTPS 接続を確立する際にゲートウェイが MDM 統合サービスに提示するクライアント証明書を選択します。ドロップ ダウンからクライアント証明書を選択することも、新しいクライアント証明書をインポートすることもできます。**Certificate Purpose**（証明書の目的）では、クライアント認証証明書であることを示す必要があります。

クライアント証明書のルート認証局（*CA*）証明書を、*User-ID* エージェントがインストールされている *Windows* サーバーの *Windows* トラスト ストアにインポートする必要があります。

1. MDM 統合サービス ホストにインストールされているサーバー証明書に関連付けられたルート CA 証明書を **Add**（追加）します。ゲートウェイと MDM 統合サービス間で安全な接続を確立するには、ルート CA 証明書とサーバー証明書の両方が必要です。ドロップ ダウンからルート CA 証明書を選択することも、新しい証明書を インポートすることもできます。
2. <239>OK</239> をクリックします。
3. 変更を **Commit (コミット)** します。

STEP 9 | AirWatch デバイスのデータが GlobalProtect に転送されるかどうか、接続を確認してください。

1. Windows ベースの User-ID エージェントを開き、**MDM Integration**（**MDM** 統合） > **Mobile Devices**（モバイル デバイス）を選択します。AirWatch が管理するすべてのデバイスの一意のデバイス ID とユーザー名のリストが表示されます。
2. （任意）リストで **Filter**（フィルタ）を設定すれば、特定の **Mobile Device**（モバイル デバイス）を検索することができます。
3. （任意）。デバイス ID のリストからデバイスを選択し、**Retrieve Device State**（デバイスの状態の取得）をクリックしてデバイスに関する最新情報を抽出し、GlobalProtect

ゲートウェイでホスト情報プロファイルがどのようにマッピングされているか確認します。

MDM 統合サービスのトラブルシューティング

イベント通知に問題があるか、AirWatch REST API への認証中に問題が発生した場合には、以下の手順に従ってください。

AirWatch MDM サーバーからのイベント通知を MDM 統合サービスが受信しない。

1. **Debug**（デバッグ）オプション（**File**（ファイル）メニュー）を **Debug**（デバッグ）または **Verbose**（冗長）に設定します。
2. Windows サーバーの User-ID エージェント インストール フォルダに移動し、`MaDebug` ファイルを開きます。以下のようなメッセージを探します。

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

3. この IP アドレスを **Permitted IP**（アクセス許可 **IP**）アドレス（**MDM Integration**（**MDM** 統合） > **Setup**（セットアップ） > **Permitted IP**（アクセス許可 **IP**））として追加します。

Airwatch REST API への認証に失敗する。

以下を確認してください。

- MDM 統合サービスが AirWatch MDM サービスに認証するために使用する認証情報が有効であること。
- Airwatch REST API にアクセスするために使用するユーザー アカウントに API アクセス許可があり、（最低でも）AirWatch が管理するモバイル デバイスおよびユーザーのデータに対する読み取り専用のアクセス許可があること。
- **Tenant Code**（テナント コード）（API キー）が正しくユーザー アカウントと関連付けられていること。使用していないすべての API キーを削除します。

Certifications 証明書

FIPS-CC モードを有効化した Windows および macOS エンドポイント用の GlobalProtect™ アプリケーションは、Federal Information Processing Standard (連邦情報処理標準-FIPS 140-2) およびコモンクライテリア (CC) の要件を満たしています。これらのセキュリティ証明書は標準的なセキュリティや一連の機能があることを証明するものであり、米国政府機関や他の規制された国内外の業界でよく採用されています。製品証明書およびサードパーティの検証に関する詳細については、Palo Alto Networks の証明書ページを参照してください。

FIPS-CC モードで Windows および macOS エンドポイント用の GlobalProtect アプリケーションを設定したりトラブルシューティングしたりする方法については、次のセクションを参照してください：

- FIPS-CC モードの有効化および検証
- FIPS-CCセキュリティ機能
- FIPS-CC モードのトラブルシューティング

FIPS-CC モードの有効化および検証

次の方法により、GlobalProtect アプリケーションの FIPS-CC モードを有効化・検証できます：

- Windows レジストリを使用して FIPS-CC モードを有効化・検証
- macOS のプロパティ リストを使用して FIPS-CC モードを有効化・検証

Windows レジストリあるいは *macOS* の *plist* を変更する場合、*Windows* あるいは *macOS* の管理者アカウントが必要になります。

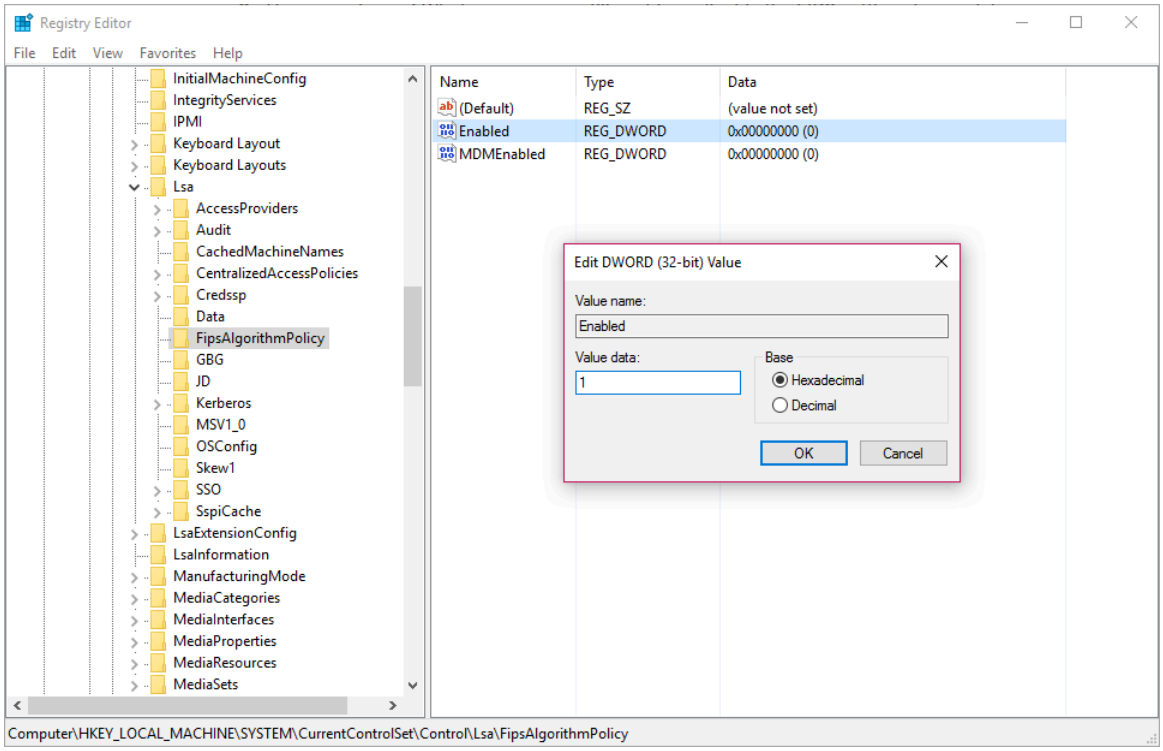
Windows レジストリを使用して FIPS-CC モードを有効化・検証

Windows エンドポイント上で次のステップに従い、Windows レジストリを使用して GlobalProtect™ の FIPS-CC モードを有効化して検証します：

STEP 1 | Windows オペレーティングシステム用に FIPS モードを有効化します。

GlobalProtect の FIPS-CC モードを有効化するには、まず Windows オペレーティングシステム用の FIPS モードを有効化し、Windows エンドポイントが FIPS 140-2 に対応していることを確認する必要があります。

1. コマンドプロンプトを起動します。
2. **regedit** と入力して Windows レジストリを開きます。
3. Window レジストリで次に移動します：**HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy**.
4. **Enabled (有効)** なレジストリ値を右クリックし、それを **Modify (編集)** します。
5. FIPS モードを有効化するために、**Value Data (値データ)** を **1** に設定します。デフォルトの値である **0** は、FIPS モードが無効であることを示します。

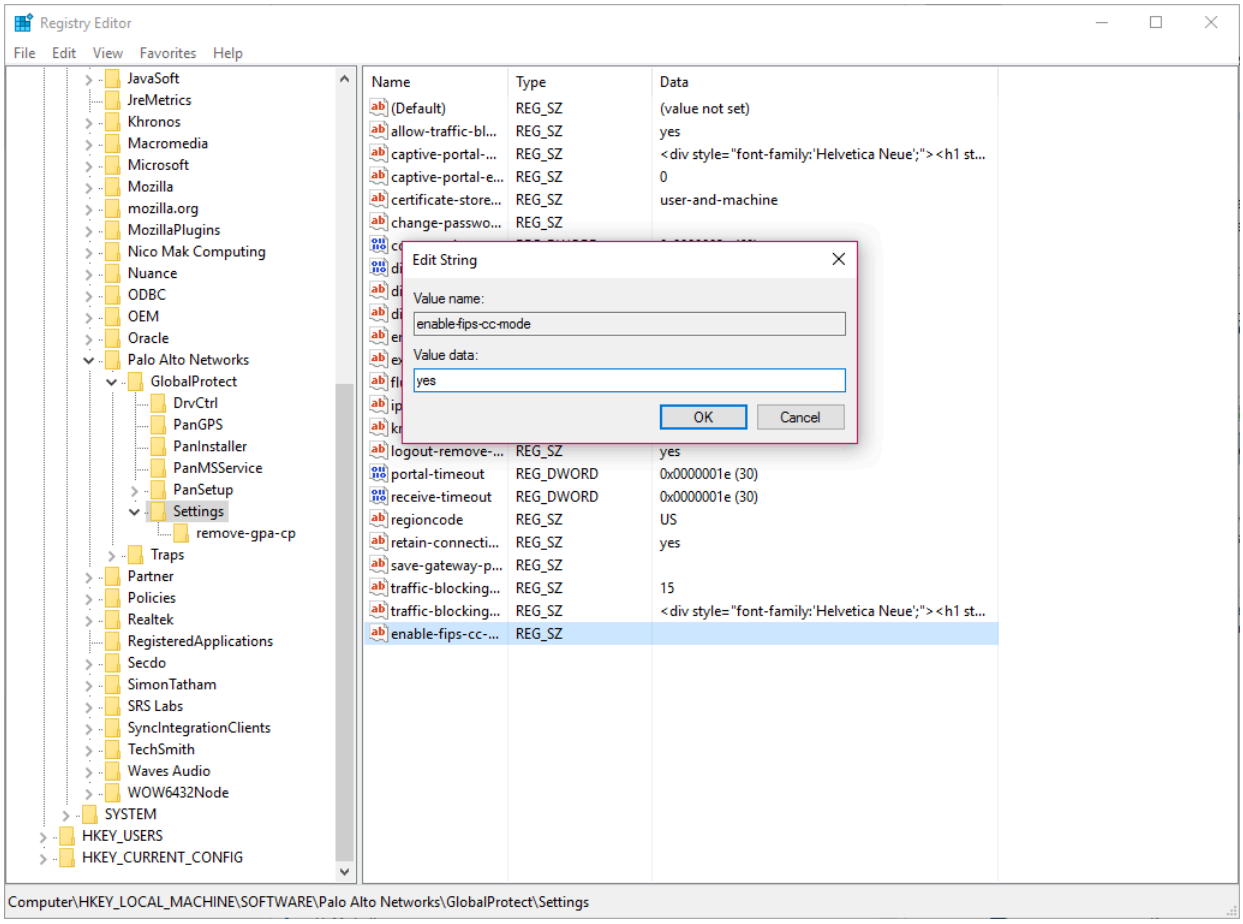


6. <239>OK</239> をクリックします。
7. エンドポイントを再起動します。

STEP 2 | GlobalProtect の FIPS-CC モードを有効化します。

FIPS-CC モードを有効化した後、無効化することはできません。*GlobalProtect* を非 *FIPS-CC* モードで実行するためには、エンドユーザーが *GlobalProtect* アプリケーションをアンインストールしてインストールし直す必要があります。これにより、*Windows* レジストリからすべての *FIPS-CC* モードの設定が削除されます。

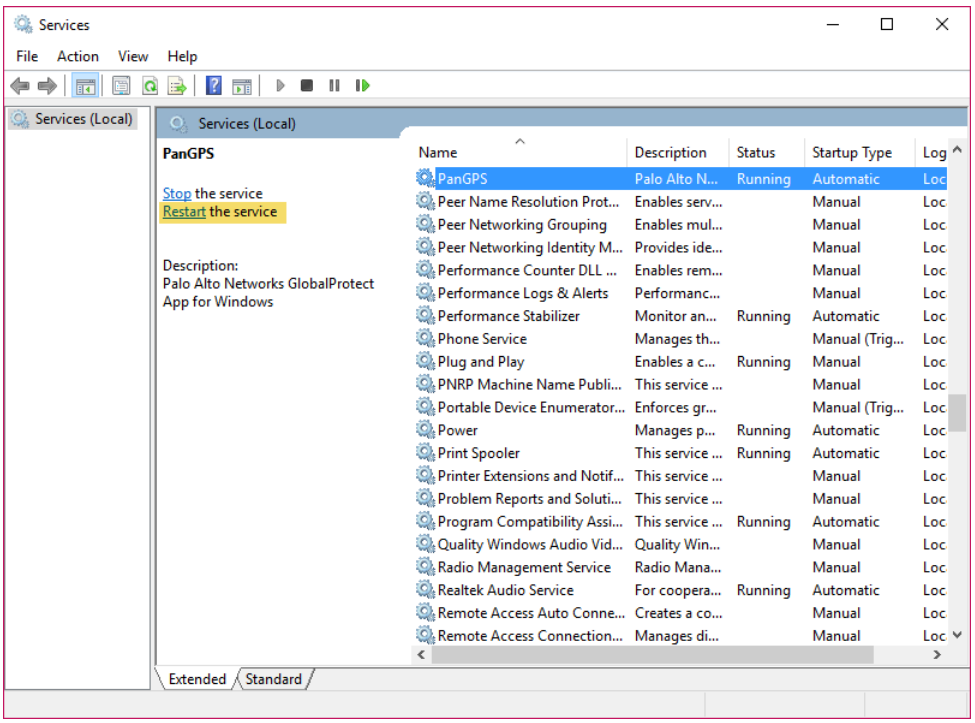
1. コマンドプロンプトを起動します。
2. **regedit** と入力して Windows レジストリを開きます。
3. Window レジストリで次に移動します：`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\ GlobalProtect\Settings`:
4. **Edit (編集)** をクリックしてから **New (新規)** > **String Value (文字列値)** を選択します。
5. 指示に従って新しいレジストリ値の **Name (名前)** として **enable-fips-cc-mode** を指定します。
6. 新しいレジストリ値を右クリックし、それを **Modify (編集)** します。
7. FIPS-CC モードを有効化するために、**Value Data (値データ)** を **yes （はい）** に設定します。
8. <239>OK</239> をクリックします。



STEP 3 | GlobalProtect を再起動します。

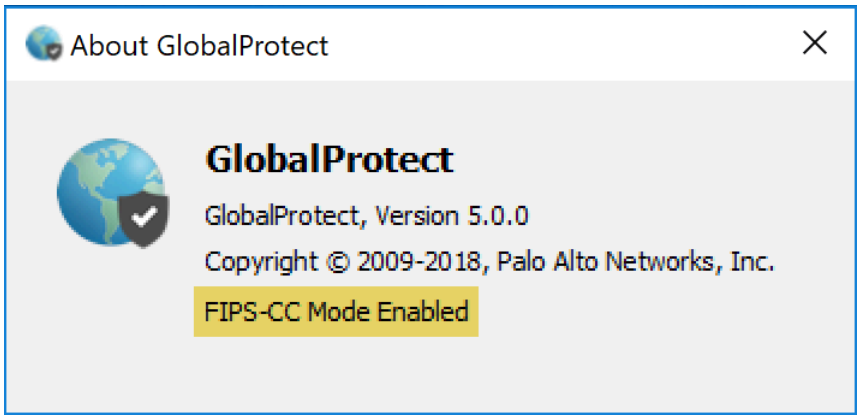
GlobalProtect アプリケーションが FIPS-CC モードで起動できるようにするには、次のいずれかの方法で GlobalProtect を再起動する必要があります。

- エンドポイントを再起動します。
- GlobalProtect アプリケーションおよび GlobalProtect サービス (PanGPS) を再起動します：
  1. コマンドプロンプトを起動します。
  2. **`services.msc`** と入力して Windows サービス マネージャを開きます。
  3. サービス リストから **PanGPS** を選択します。
  4. サービスを **Restart (再起動)** します。



STEP 4 | GlobalProtect アプリケーション上で FIPS-CC モードが有効になっていることを確認します。

1. GlobalProtect アプリの使用
2. ステータスパネルから設定ダイアログを開きます (⚙)。
3. **About**（バージョン情報）を選択します。
4. FIPS-CC モードが有効になっていることを確認します。FIPS-CC モードが有効な場合、About (情報) ダイアログに `FIPS-CC Mode Enabled` という状態が表示されます。



macOS のプロパティ リストを使用して FIPS-CC モードを有効化・検証

macOS エンドポイント上で次のステップに従い、macOS の plist (プロパティ リスト) を使用して GlobalProtect™ の FIPS-CC モードを有効化して検証します：

GlobalProtect の FIPS-CC モードを有効化するには、macOS エンドポイントが FIPS 140-2 に対応していなければなりません。デフォルト設定では、macOS 10.8 以降のリリースを実行しているエンドポイントで、Mac オペレーティングシステムの FIPS モードが自動的に有効化されます。

STEP 1 | GlobalProtect plist ファイルを開いて、GlobalProtect アプリのカスタマイズ設定を見つけます。

1. Xcode などの plist エディタを起動します。
2. Mac グローバル plist ファイルの場所（`/Library/Preferences/com.paloaltonetworks.GlobalProtect.settings.plist`）に移動します。
3. GlobalProtect Settings (設定) ディクショナリを探します：`/Palo Alto Networks/GlobalProtect/Settings`。

   Settings ディクショナリが存在しない場合は、作成します。各キーを文字列として Settings ディクショナリに追加します。

STEP 2 | GlobalProtect の FIPS-CC モードを有効化します。

FIPS-CC を有効化した後、無効化することはできません。*GlobalProtect* を非 *FIPS-CC* モードで実行するためには、エンドユーザーが *GlobalProtect* アプリケーションをアンインストールしてインストールし直す必要があります。これにより、*macOS* の *plist* からすべての *FIPS-CC* モードの設定が削除されます。

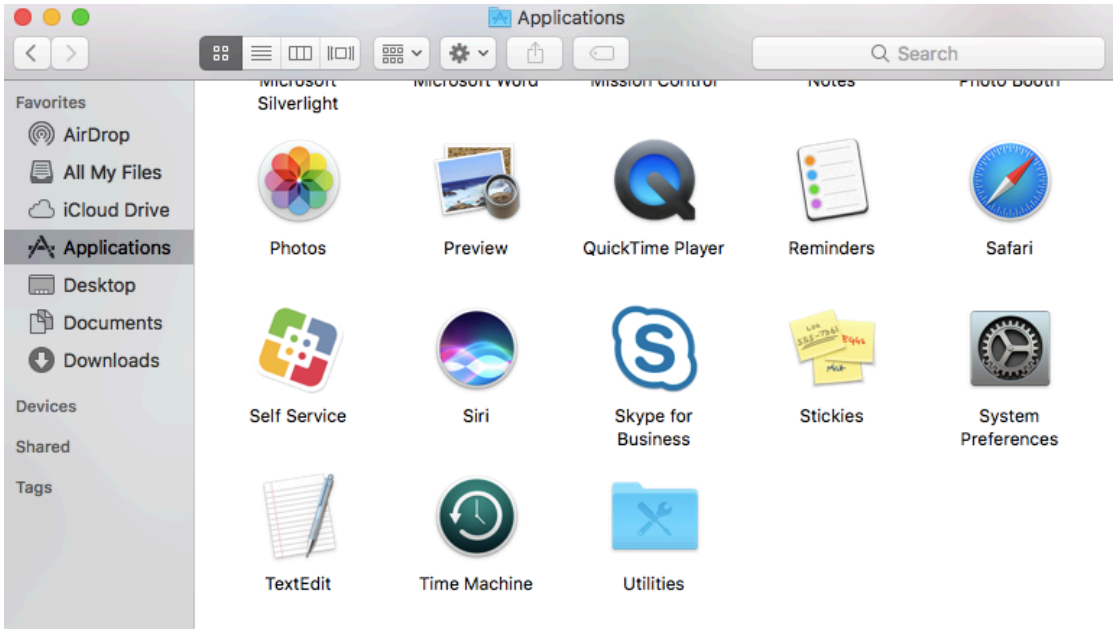
Settings (設定) ディクショナリで、次のキーと値のペアを追加して FIPS-CC モードを有効化します：

```
<key>enable-fips-cc-mode</key>
<string>yes</string>
```

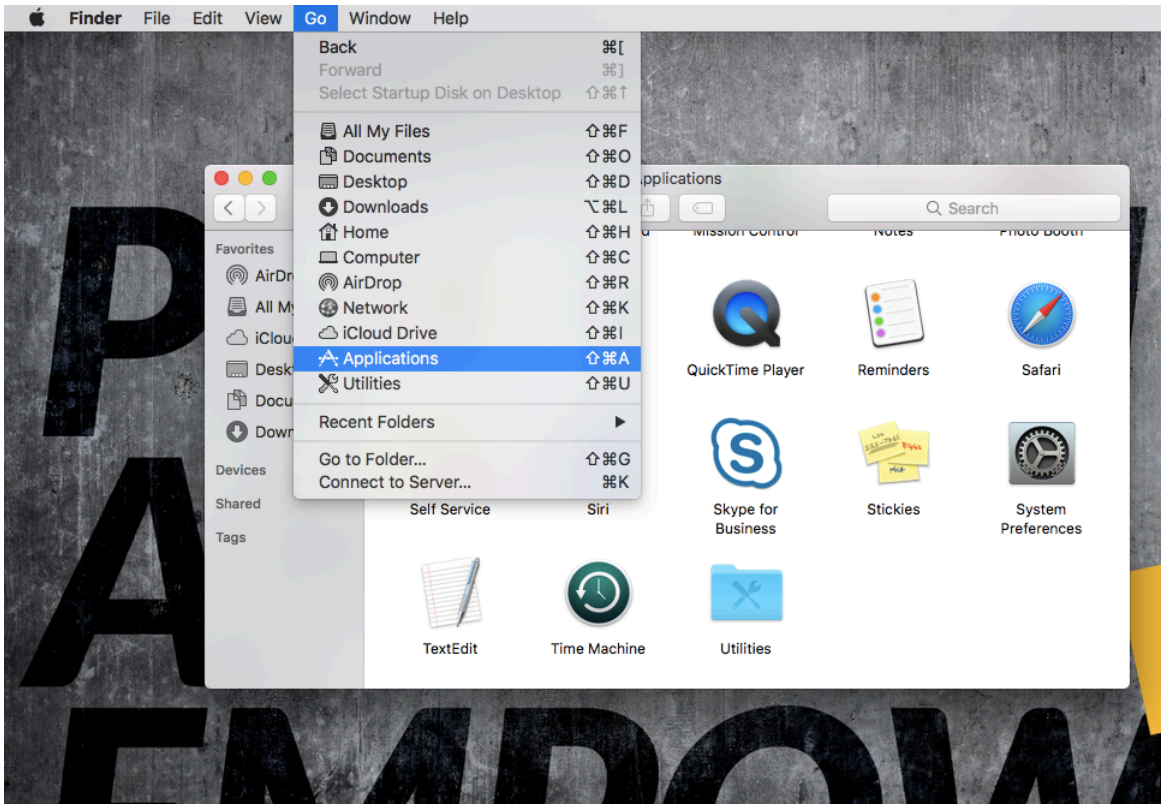
STEP 3 | GlobalProtect を再起動します。

GlobalProtect アプリケーションが FIPS-CC モードで起動できるようにするには、次のいずれかの方法で GlobalProtect を再起動する必要があります。

- エンドポイントを再起動します。
- GlobalProtect アプリケーションおよび GlobalProtect サービス (PanGPS) を再起動します：
  1. ファインダーを起動します。
  2. Applications (アプリケーション) フォルダを開きます：
     - ファインダーのサイドバーで **Applications (アプリケーション)** を選択します。



     - ファインダーのサイドバーに **Applications (アプリケーション)** が表示されない場合は、ファインダーのメニューバーで **Go (移動)** > **Applications (アプリケーション)** を選択します。



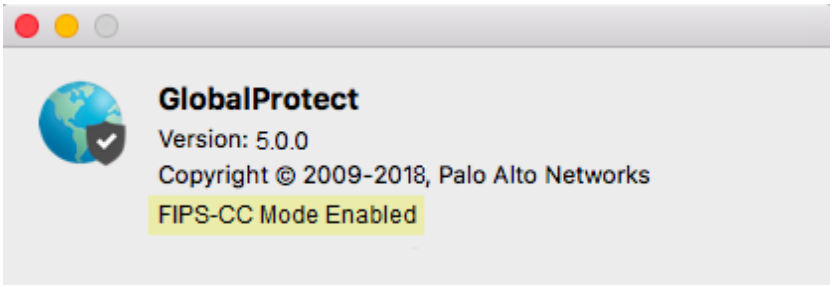
ファインダーのサイドバーに ***Applications*** (アプリケーション) を表示するには、ファインダーのメニューバーで ***Finder*** (ファインダー) > ***Preferences*** (設定) を選択します。ファインダーの設定で ***Sidebar*** (サイドバー) を選択してからオプションを有効化し、***Applications*** (アプリケーション) を表示します。

3. Utilities (ユーティリティ) フォルダを開きます。
4. ターミナルを起動します。
5. 以下のコマンドを実行します。

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

STEP 4 | GlobalProtect アプリケーション上で FIPS-CC モードが有効になっていることを確認します。

1. GlobalProtect アプリの使用
2. ステータスパネルから設定ダイアログを開きます ( )。
3. **About**（バージョン情報）を選択します。
4. FIPS-CC モードが有効になっていることを確認します。FIPS-CC モードが有効な場合、About (情報) ダイアログに `FIPS-CC Mode Enabled` という状態が表示されます。



FIPS-CCセキュリティ機能

GlobalProtect の FIPS-CC モードを有効化すると、Windows および macOS エンドポイント上のすべての GlobalProtect アプリケーションに次のセキュリティ機能が適用されます。

- TLS あるいは IPSec を使用して GlobalProtect アプリケーションおよびゲートウェイ間の VPN トンネルをすべて暗号化する必要があります。
- IPSec VPN トンネルを設定する場合、IPSec のセットアップ時に表示される暗号スイート オプションを選択する必要があります。
- IPSec VPN トンネルを設定する場合、次のいずれかの暗号化アルゴリズムを指定できます：
  - AES-CBC-128 (SHA1 認証アルゴリズムを使用)
  - AES-GCM-128
  - AES-GCM-256
- サーバーおよびクライアント証明書の両方が次のいずれかのシグネチャ アルゴリズムを使用する必要があります：
  - RSA 2048 bit (あるいはそれ以上)
  - ECDSA P-256
  - ECDSA P-384
  - ECDSA P-521

  さらに、SHA256、SHA384、あるいは SHA512 のシグネチャ ハッシュ アルゴリズムを使用する必要があります。

FIPS-CC モードのトラブルシューティング

FIPS-CC モードを有効化した後に問題が発生した場合は、次のセクションを参照して問題のトラブルシューティングを進めてください：

- GlobalProtect ログの表示および収集
- FIPS-CC モードの問題を解決

GlobalProtect ログの表示および収集

GlobalProtect™ ログで、FIPS-CC の問題についての詳細情報をさらに確認できます。

次のステップで GlobalProtect ログを表示あるいは収集できます：

STEP 1 | GlobalProtect アプリの使用

STEP 2 | ステータスパネルから設定ダイアログを開きます (⚙)。

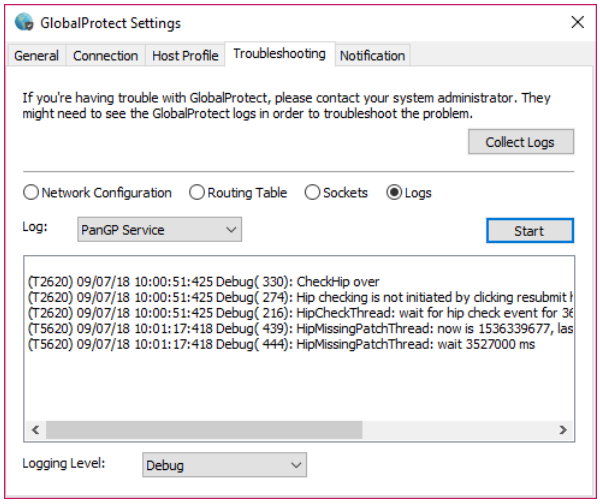
STEP 3 | **Settings**[設定]を選択します。

STEP 4 | GlobalProtect Settings (設定) パネルで **Troubleshooting (トラブルシューティング)** を選択します。

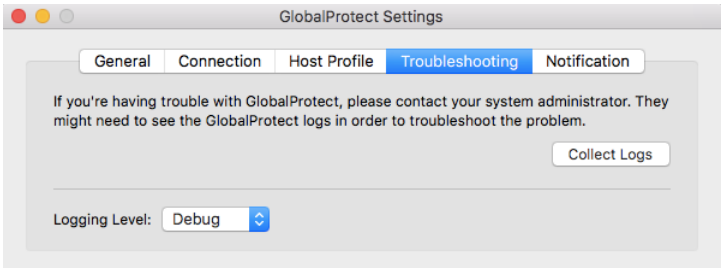
STEP 5 | **Logging Level (ロギング レベル)** を選択します。

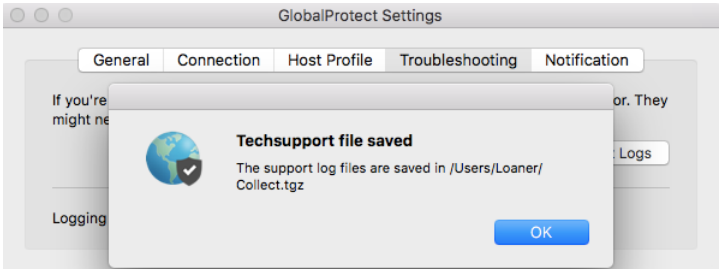
STEP 6 | (任意—Windows のみ) GlobalProtect ログを表示します：

1. **Logs (ログ)** を選択します。
2. **Log (ログ)** タイプを選択します。
3. ログの収集を **Start (開始)** します。



STEP 7 | (任意)**Collect Logs (**ログを収集**)** して GlobalProtect 管理者に送信し、トラブルシューティングを行います。

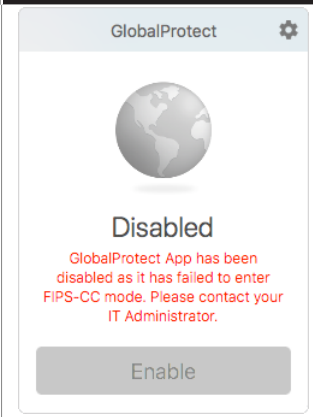
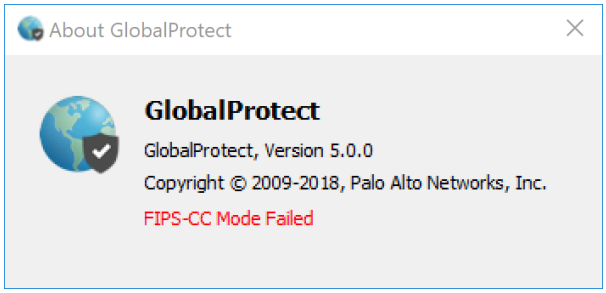




FIPS-CC モードの問題を解決

次の表は、FIPS-CC モードで生じ得る問題およびその解決策を示しています。以下に記載されていない問題が発生した場合は、GlobalProtect™ の管理者に問い合わせてトラブルシューティングをサポートしてもらってください。

問題	説明	ソリューション
FIPS パワーオンの自己テストあるいは整合性テストのエラーが原因で、GlobalProtect アプリケーションが FIPS-CC モードで初期化されません。	FIPS-CC モードを有効化した後、GlobalProtect アプリケーションが FIPS パワーオンの自己テストおよび整合性テストをアプリの初期化時およびシステムあるいはアプリの再起動時に実行します。このいずれかのテストが失敗すると、GlobalProtect アプリケーションが無効化され、About (情報) ウィンドウに `FIPS-CC Mode Failed (FIPS-CC モード失敗)` というエラーメッセージが表示されます。	アプリケーションを再起動してエラー状態を快勝してください。問題が発生し続ける場合は、アプリケーションをアンインストールしてからインストールし直します。

問題	説明	ソリューション
	 	
FIPS 条件付き自己テストの失敗により、GlobalProtect アプリケーションが FIPS-CC モードで接続を確立できません。	FIPS-CC モードで初期化された後、GlobalProtect アプリケーションは FIPS 条件付き自己テストを実行します。自己テストが失敗すると、GlobalProtect アプリケーションはセッションを終了して未接続の状態になります。	GlobalProtect 接続を確立するには、GlobalProtect ポータルに認証し直す必要があります。

GlobalProtect が初期化されない、あるいは *FIPS-CC* モードで接続されない場合は、*GlobalProtect* の *Settings* (設定) パネルにある ***Troubleshooting*** (トラブルシューティング) タブにアクセスし、ログを表示・収集してトラブルシューティングを行うことができます。他のタブはすべて、*GlobalProtect* が正常に接続されるまで使用できません。

GlobalProtect クイック設定

以下のセクションでは、いくつかの一般的な GlobalProtect™ デプロイメントの設定手順について説明します。

- リモート アクセス VPN（認証プロファイル）
- リモート アクセス VPN（証明書プロファイル）
- 2 要素認証を使用したリモート アクセス VPN
- 常時オンの VPN 設定
- Pre-Logon を使用したリモート アクセス VPN
- GlobalProtect 複数ゲートウェイ設定
- GlobalProtect による内部 HIP チェックとユーザーベースのアクセス
- 内部ゲートウェイと外部ゲートウェイの混合設定
- ネットワーク アクセス用に GlobalProtect を適用およびキャプティブポータル
- 公開中の KB:Active Directory のパスワード変更

リモート アクセス VPN（認証プロファイル）

リモート アクセス用 GlobalProtect VPNでは GlobalProtect ポータルとゲートウェイが ethernet1/2 に設定されているため、**ethernet1/2** は GlobalProtect ユーザーが接続する物理インターフェイスになっています。ユーザーがポータルおよびゲートウェイに接続されて認証されたら、エンドポイントがその仮想アダプタからトンネルを確立します。仮想アダプタには、ゲートウェイ tunnel.2 の設定に関連付けられた IP アドレス プール内のアドレス（この例では 10.31.32.3 ～ 10.31.32.118）が割り当てられています。GlobalProtect VPN トンネルは個別の **corp-vpn** ゾーンが終点となるため、トラフィックへの可視性を得られるだけでなく、リモートユーザーに合わせてセキュリティ ポリシーをカスタマイズできます。

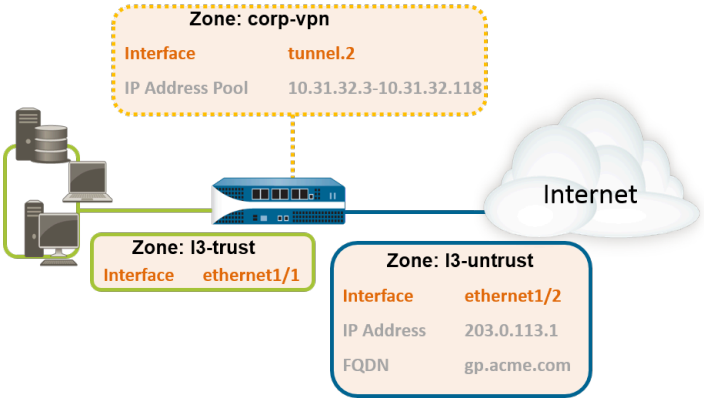


図 **5 :** リモート アクセス用 **GlobalProtect VPN**

STEP 1 | GlobalProtect のインターフェイスおよびゾーンの作成を行います。

すべてのインターフェイス設定に ***default***（デフォルト）仮想ルーターを使用し、ゾーン間ルーティングの作成を回避します。

- **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)**を選択します。**ethernet1/2** を、IP アドレス 203.0.113.1 を含む Layer3 Ethernet インターフェイスとして設定し、それを **l3-untrust Security Zone (セキュリティ ゾーン)** およびデフォルトの **Virtual Router (仮想ルーター)** に割り当てます。
- IP アドレス **203.0.113.1** を **gp.acme.com** にマッピングする DNS「A」レコードを作成します。
- **Network**（ネットワーク） > **Interfaces (インターフェイス)** > **Tunnel**（トンネル） を選択して **tunnel.2** インターフェイスを**Add**（追加） します。トンネル インターフェイスを **corp-vpn** と呼ばれる新しい **Security Zone (セキュリティ ゾーン)** に **Add (追加)** してから、それを **Virtual Router (仮想ルーター)** に割り当てます。
- **corp-vpn** ゾーンの [User-ID の有効化] をオンにします。

STEP 2 | セキュリティ ポリシーを作成し、**corp-vpn** ゾーンと **l3-trust** ゾーン間のトラフィック フローを有効にして、内部リソースへのアクセスを可能にします。

1. **Policies** > **Security**（セキュリティ）の順に選択し、新しいルールを **Add**（追加）します。
2. この例では、以下の設定を使用してルールを定義します。
   - **Name**（名前）（**General**（全般）タブ）—VPN アクセス
   - **Source Zone**（送信元ゾーン）（**Source**（送信元）タブ）—corp-vpn
   - **Destination Zone**（宛先ゾーン）（**Destination**（宛先）タブ）—l3-trust

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

STEP 3 | 以下のいずれかの方法を使用して、GlobalProtect ポータルおよびゲートウェイをホストするインターフェイスのサーバー証明書を取得します。

- （推奨）一般的なサードパーティ CA からサーバー証明書をインポートします。
- ポータルでルート CA を使用して自己署名サーバー証明書を生成します。

[Device] > **[証明書の管理]** > **[証明書]** の順に選択し、証明書を以下のように管理します。

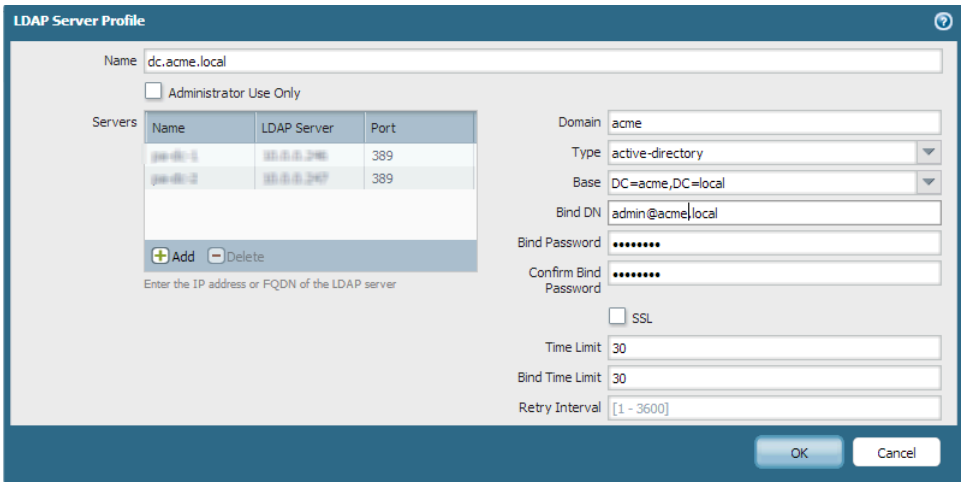
- サーバー証明書を取得します。ポータルとゲートウェイは同じインターフェイス上にあるため、両方のコンポーネントに同じサーバー証明書を使用できます。
- 証明書の CN は FQDN、gp.acme.com と一致する必要があります。
- ユーザーが証明書エラーなしでポータルに接続できるようにするには、パブリック CA からのサーバー証明書を使用します。

STEP 4 | サーバー プロファイルを作成します。

サーバー プロファイルによって、認証サービスへの接続方法がファイアウォールに指示されます。ローカル、RADIUS、Kerberos、SAML、および LDAP 認証メソッドがサポートされて

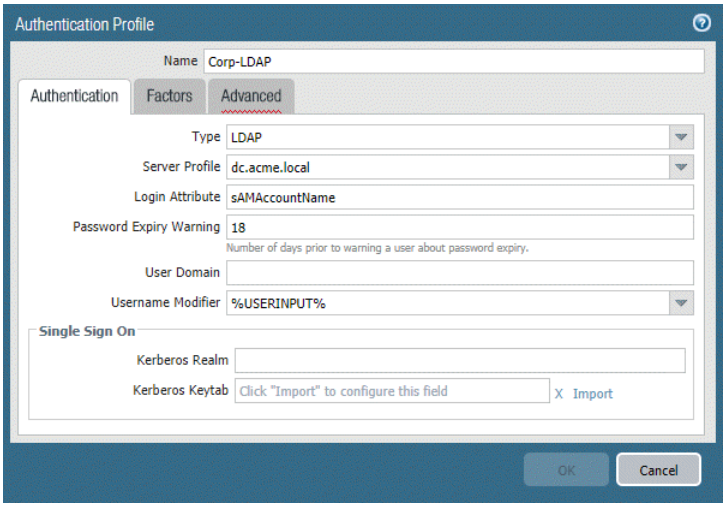
います。この例では、Active Directory に対してユーザーを認証する LDAP 認証プロファイルを使用しています。

LDAP サーバーに接続するサーバー プロファイルを作成します（**Device** > **Server Profiles**（サーバープロファイル） > **LDAP**）。



STEP 5 | （任意）認証プロファイルを作成します。

サーバー プロファイルを認証プロファイルに関連付けます（**Device** > **Authentication Profile**（認証プロファイル））。



STEP 6 | GlobalProtect ゲートウェイの設定を行います。

Network（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ）の順に選択し、以下の設定を **Add**（追加）します。

Interface（インターフェイス）—**ethernet1/2**

IP Address (IP アドレス)—**203.0.113.1**

Server Certificate（サーバー証明書）—**GoDaddy** によって発行された **GP-server-cert.pem**

Authentication Profile（認証プロファイル）—**Corp-LDAP**

Tunnel Interface（トンネル インターフェイス）—**tunnel.2**

IP Pool (IP プール)—**10.31.32.3 - 10.31.32.118**

STEP 7 | GlobalProtect ポータルを設定します。

Network（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択し、以下の設定を **Add**（追加）します。

1. GlobalProtect ポータルへのアクセスのセットアップ：

   Interface（インターフェイス）—**ethernet1/2**

   IP Address (IP アドレス)—**203.0.113.1**

   Server Certificate（サーバー証明書）—**GoDaddy** によって発行された **GP-server-cert.pem**

   Authentication Profile（認証プロファイル）—**Corp-LDAP**
2. GlobalProtect クライアント認証設定の定義：

   Connect Method（接続方式）—オンデマンド（ユーザー操作による手動接続）

   External Gateway Address（外部ゲートウェイ アドレス）—**gp.acme.com**

STEP 8 | GlobalProtect アプリ ソフトウェアのデプロイを行います。

Device > **GlobalProtect Client**（**GlobalProtect** クライアント）の順に選択します。エージェント更新をポータルでホストするの手順に従ってください。

STEP 9 | （任意）GlobalProtect モバイル アプリケーションを使用できるようにします。

GlobalProtect ゲートウェイ サブスクリプションを購入してインストールし（**Device** > **Licenses**（ライセンス））、アプリを使用できるようにします。

STEP 10 | GlobalProtect の設定を保存します。

Commit（コミット）をクリックします。

リモート アクセス VPN（証明書プロファイル）

証明書認証では、ユーザーを識別できる有効なクライアント証明書をユーザーが GlobalProtect ポータルまたはゲートウェイに提示する必要があります。ポータルあるいはゲートウェイは証明書自体に加えて証明書プロファイルを使用することでも、証明書を送信したユーザーが実際にその証明書の発行対象であるかどうかを判断できます。

クライアント証明書が唯一の認証手段である場合は、証明書のいずれかのフィールドにユーザー名が含まれている必要があります。通常、ユーザー名は証明書の Subject フィールド内の共有名（CN）に対応します。

認証に成功したら、GlobalProtect アプリはゲートウェイを使用してトンネルを確立し、ゲートウェイのトンネル設定内の IP プールから IP アドレスが割り当てられます。**corp-vpn** ゾーンからのセッションでユーザー ベースのポリシー適用をサポートするため、証明書内のユーザー名はゲートウェイによって割り当てられた IP アドレスにマッピングされます。セキュリティポリシーがドメイン名に加えてユーザー名を必要とする場合、証明書プロファイルで指定されたドメイン値がユーザー名に付加されます。

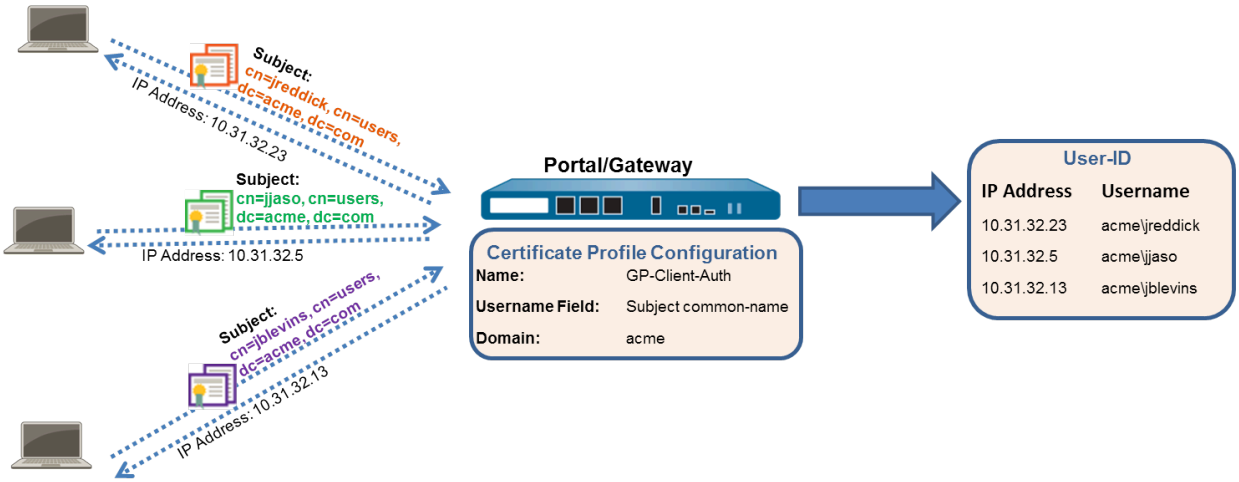


図 **6 : GlobalProtect** クライアント証明書の認証設定

このクイック設定では、リモート アクセス用 GlobalProtect VPN と同じトポロジを使用します。唯一の設定の違いは、外部認証サーバーに対してユーザーを認証する代わりに、この設定ではクライアント証明書の認証のみを使用する点です。

STEP 1 | GlobalProtect のインターフェイスおよびゾーンの作成を行います。

すべてのインターフェイス設定に ***default***（デフォルト）仮想ルーターを使用し、ゾーン間ルーティングの作成を回避します。

- **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)**を選択します。**ethernet1/2** を、IP アドレス **203.0.113.1** を含む Layer3 Ethernet インターフェイスとして設定し、それを **l3-untrust Security Zone**（セキュリティ ゾーン） およびデフォルトの **Virtual Router**（仮想ルーター）に割り当てます。
- IP アドレス **203.0.113.1** を **gp.acme.com** にマッピングする DNS「A」レコードを作成します。
- **Network**（ネットワーク） > **Interfaces (インターフェイス)** > **Tunnel**（トンネル） を選択して **tunnel.2** インターフェイスを**Add**（追加） します。トンネル インターフェイスを corp-vpn と呼ばれる新しい **Security Zone**（セキュリティ ゾーン）に追加してから、それを**Virtual Router**（仮想ルーター）に割り当てます。
- **corp-vpn** ゾーンの [User-ID の有効化] をオンにします。

STEP 2 | セキュリティ ポリシーを作成し、**corp-vpn** ゾーンと **l3-trust** ゾーン間のトラフィック フローを有効にして、内部リソースへのアクセスを可能にします。

1. **Policies** > **Security**（セキュリティ）の順に選択し、新しいルールを **Add**（追加）します。
2. この例では、以下の設定を使用してルールを定義します。
   - **Name**（名前）（**General**（全般） タブ）—**VPN Access**
   - **Source Zone**（送信元ゾーン）（**Source**（送信元）タブ）—**corp-vpn**
   - **Destination Zone**（宛先ゾーン）（**Destination**（宛先）タブ）—**l3-trust**

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

STEP 3 | 以下のいずれかの方法を使用して、GlobalProtect ポータルおよびゲートウェイをホストするインターフェイスのサーバー証明書を取得します。

- （推奨）一般的なサードパーティ CA からサーバー証明書をインポートします。
- ポータルでルート CA を使用して自己署名サーバー証明書を生成します。

[Device] > **[証明書の管理]** > **[証明書]** の順に選択し、証明書を以下のように管理します。

- サーバー証明書を取得します。ポータルとゲートウェイは同じインターフェイス上にあるため、両方のコンポーネントに同じサーバー証明書を使用できます。
- 証明書の CN は FQDN、gp.acme.com と一致する必要があります。
- ユーザーが証明書エラーなしでポータルに接続できるようにするには、パブリック CA からのサーバー証明書を使用します。

STEP 4 | GlobalProtect クライアントおよびエンドポイントに対してクライアント証明書を発行します。

1. エンタープライズ PKI またはパブリック CA を使用して、一意のクライアント証明書を各 GlobalProtect ユーザーに発行します。
2. エンドポイントの個人用証明書ストアに証明書をインストールします。

STEP 5 | クライアント証明書プロファイルを作成します。

1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificate Profile (証明書プロファイル)** を選択します。新しい証明書プロファイルを**Add**（追加）してから、**GP-client-cert** などのプロファイルの**Name**（名前）を入力します。
2. **Username Field**（ユーザー名フィールド）ドロップダウン リストから **Subject**（サブジェクト）を選択します。
3. **CA Certificates**（**CA** 証明書）エリアで、クライアント証明書が発行した CA 証明書を**Add**（追加）します。**OK** を 2 回クリックします。

STEP 6 | GlobalProtect ゲートウェイの設定を行います。

リモート アクセス用 GlobalProtect VPN に示されたトポロジ図を参照してください。

Network（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ）の順に選択し、以下の設定を **Add**（追加）します。

Interface（インターフェイス）—**ethernet1/2**

IP Address (IP アドレス)—**203.0.113.1**

Server Certificate（サーバー証明書）—**GoDaddy** によって発行された **GP-server-cert.pem**

Certificate Profile（証明書プロファイル）—**GP-client-cert**

Tunnel Interface（トンネル インターフェイス）—**tunnel.2**

IP Pool (IP プール)—**10.31.32.3 - 10.31.32.118**

STEP 7 | GlobalProtect ポータルを設定します。

Network（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択し、以下の設定を **Add**（追加）します。

1. GlobalProtect ポータルへのアクセスのセットアップ：

   Interface（インターフェイス）—`ethernet1/2`

   IP Address (IP アドレス)—`203.0.113.1`

   Server Certificate（サーバー証明書）—`GoDaddy` によって発行された `GP-server-cert.pem`

   Certificate Profile（証明書プロファイル）—`GP-client-cert`

2. GlobalProtect エージェント設定の定義：

   Connect Method（接続方式）—オンデマンド（ユーザー操作による手動接続）

   External Gateway Address（外部ゲートウェイ アドレス）—`gp.acme.com`

STEP 8 | GlobalProtect アプリ ソフトウェアのデプロイを行います。

Device > **GlobalProtect Client**（**GlobalProtect** クライアント）の順に選択します。エージェント更新をポータルでホストするの手順に従ってください。

STEP 9 | （任意）GlobalProtect モバイル アプリケーションを使用できるようにします。

GlobalProtect ゲートウェイ サブスクリプションを購入してインストールし（**Device** > **Licenses**（ライセンス））、アプリを使用できるようにします。

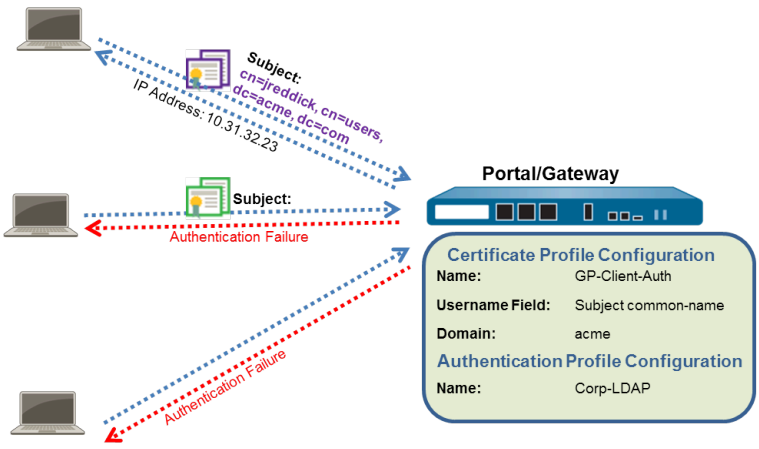
STEP 10 | GlobalProtect の設定を保存します。

Commit（コミット）をクリックします。

2 要素認証を使用したリモート アクセス VPN

認証プロファイルおよび証明書プロファイル（両者を併せて 2 要素認証が可能）を伴う GlobalProtect ポータルまたはゲートウェイを設定する場合、エンドユーザーはアクセス権を得る前に両方のプロファイルを通じて認証を成功させる必要があります。ポータル認証の場合、最初のポータル接続が行われる前に、証明書がエンド エンドポイントに事前にデプロイされている必要があります。さらに、ユーザーが提示するクライアント証明書は、証明書プロファイルで定義された内容と一致する必要があります。

- 証明書プロファイルでユーザー名フィールドが指定されていない場合（**Username Field**（ユーザー名フィールド）が **None**（なし）に設定されている場合）、クライアント証明書にユーザー名は必要ありません。この場合、ユーザーは認証プロファイルに対する認証時にユーザー名を提供する必要があります。
- 証明書プロファイルでユーザー名フィールドが指定されている場合、ユーザーが提示する証明書には、対応するフィールドにユーザー名が含まれている必要があります。たとえば、証明書プロファイルで **Subject**（サブジェクト）がユーザー名フィールドであると指定されている場合、ユーザーが提示する証明書には共通名フィールドに値が含まれている必要があります。含まれていない場合は認証に失敗します。さらに、ユーザー名フィールドが必須の場合、ユーザーが認証プロファイルに対する認証で認証情報を入力しようとするときに、証明書のユーザー名フィールド内の値が自動的にユーザー名として入力されます。ユーザーに証明書内のユーザー名での認証を強制しない場合、証明書プロファイルのユーザー名フィールドは指定しないでください。



このクイック設定では、リモート アクセス用 GlobalProtect VPN と同じトポロジを使用します。ただし、この設定では、ユーザーが証明書プロファイルと認証プロファイルに対して認証する必要があります。2 要素認証の特定のタイプに関する詳細は、以下のトピックを参照してください。

- 証明書および認証プロファイルを使用した 2 要素認証の有効化
- 1 回限りのパスワード（OTP）を使用した 2 要素認証の有効化
- スマート カードを使用した 2 要素認証の有効化
- ソフトウェアトークンアプリケーションを使用して2要素認証を有効にする

次の作業を行って、2 要素認証を使用するリモート VPN アクセスを設定します。

STEP 1 | GlobalProtect のインターフェイスおよびゾーンの作成を行います。

すべてのインターフェイス設定に ***default***（デフォルト）仮想ルーターを使用し、ゾーン間ルーティングの作成を回避します。

- **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)**を選択します。**ethernet1/2** を、IP アドレス **203.0.113.1** を含む **Layer3** Ethernet インターフェイスとして設定し、それを **l3-untrust Security Zone**（セキュリティ ゾーン） およびデフォルトの **Virtual Router**（仮想ルーター）に割り当てます。
- IP アドレス **203.0.113.1** を **gp.acme.com** にマッピングする DNS「A」レコードを作成します。
- **Network**（ネットワーク） > **Interfaces (インターフェイス)** > **Tunnel**（トンネル） を選択して **tunnel.2** インターフェイスを**Add**（追加） します。トンネル インターフェイスを **corp-vpn** と呼ばれる新しい **Security Zone**（セキュリティ ゾーン）に追加してから、それを**Virtual Router**（仮想ルーター）に割り当てます。
- **corp-vpn** ゾーンの [User-ID の有効化] をオンにします。

STEP 2 | セキュリティ ポリシーを作成し、**corp-vpn** ゾーンと **l3-trust** ゾーン間のトラフィック フローを有効にして、内部リソースへのアクセスを可能にします。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択し、**Add**（追加）をクリックして新しいルールを作成します。
2. この例では、以下の設定を使用してルールを定義します。
   - **Name**（名前）（**General**（全般） タブ）—**VPN Access**
   - **Source Zone**（送信元ゾーン）（**Source**（送信元）タブ）—**corp-vpn**
   - **Destination Zone**（宛先ゾーン）（**Destination**（宛先）タブ）—**l3-trust**

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

STEP 3 | 以下のいずれかの方法を使用して、GlobalProtect ポータルおよびゲートウェイをホストするインターフェイスのサーバー証明書を取得します。

- （推奨）一般的なサードパーティ CA からサーバー証明書をインポートします。
- ポータルでルート CA を使用して自己署名サーバー証明書を生成します。

[Device] > **[証明書の管理]** > **[証明書]** の順に選択し、証明書を以下のように管理します。

- サーバー証明書を取得します。ポータルとゲートウェイは同じインターフェイス上にあるため、両方のコンポーネントに同じサーバー証明書を使用できます。
- 証明書の CN は FQDN、gp.acme.com と一致する必要があります。
- ユーザーが証明書エラーなしでポータルに接続できるようにするには、パブリック CA からのサーバー証明書を使用します。

STEP 4 | GlobalProtect クライアントおよびエンドポイントに対してクライアント証明書を発行します。

1. エンタープライズ PKI またはパブリック CA を使用して、一意のクライアント証明書を各 GlobalProtect ユーザーに発行します。
2. エンドポイントの個人用証明書ストアに証明書をインストールします。

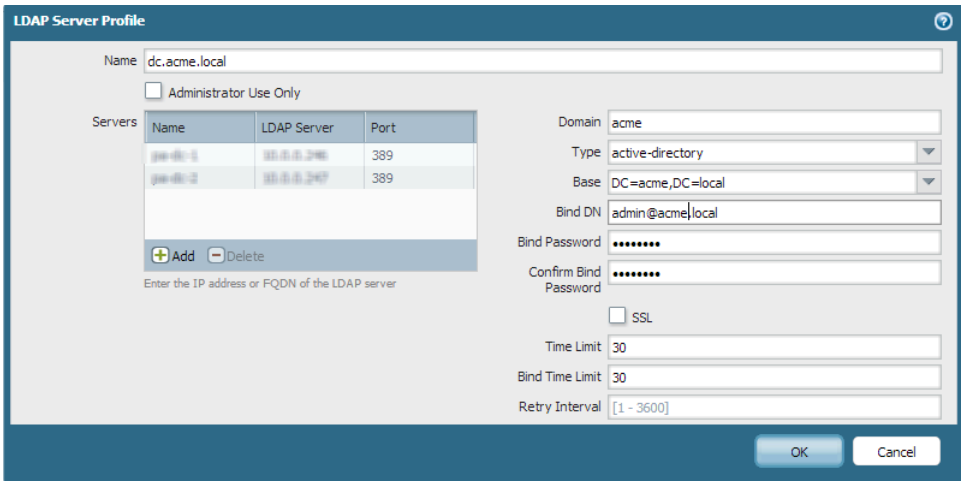
STEP 5 | クライアント証明書プロファイルを作成します。

1. **Device (デバイス)** > **Certificate Management (証明書管理)** > **Certificate Profile (証明書プロファイル)** を選択します。新しい証明書プロファイルを**Add**（追加）してから、**`GP-client-cert`** などのプロファイルの**Name**（名前）を入力します。
2. エンド ユーザーの認証に使用されるユーザー名の取得元を指定します。
   - **From user**（ユーザーから取得）– 認証プロファイルで指定したサービスに対して認証するときにエンド ユーザーがユーザー名を入力するように設定するには、**Username Field**（ユーザー名フィールド）で **None**（なし）を選択します。
   - **From certificate**（証明書から取得）– 証明書からユーザー名を抽出するには、**Username Field**（ユーザー名フィールド）で **Subject**（サブジェクト）を選択します。このオプションを使用する場合、ユーザーがポータル/ゲートウェイへのログインを求められたときに証明書に含まれる CN によってユーザー名フィールドが自動的に入力されます。ユーザーはそのユーザー名を使用してログインすることを要求されます。
3. **CA Certificates**（**CA** 証明書）エリアで、クライアント証明書が発行した CA 証明書を**Add**（追加）します。**OK** を 2 回クリックします。

STEP 6 | サーバー プロファイルを作成します。

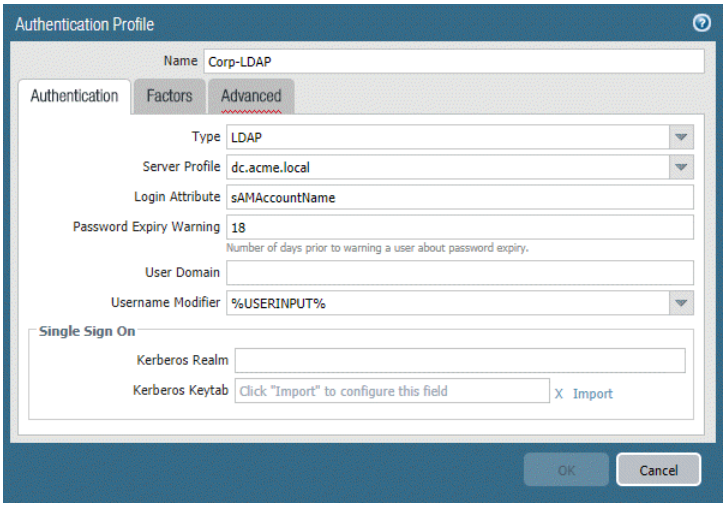
サーバー プロファイルによって、認証サービスへの接続方法がファイアウォールに指示されます。ローカル、RADIUS、Kerberos、SAML、および LDAP 認証メソッドがサポートされています。この例では、Active Directory に対してユーザーを認証する LDAP 認証プロファイルを使用しています。

LDAP サーバーに接続するサーバー プロファイルを作成します。 **[Device]** > **[サーバー プロファイル]** > **[LDAP]**



STEP 7 | （任意）認証プロファイルを作成します。

サーバー プロファイルを認証プロファイルに関連付けます（**Device > Authentication Profile**（認証プロファイル））。



STEP 8 | GlobalProtect ゲートウェイの設定を行います。

リモート アクセス用 GlobalProtect VPN に示されたトポロジ図を参照してください。

Network（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ）の順に選択し、以下の設定を **Add**（追加）します。

Interface（インターフェイス）—**ethernet1/2**

IP Address (IP アドレス)—**203.0.113.1**

Server Certificate（サーバー証明書）—**GoDaddy** によって発行された **GP-server-cert.pem**

Certificate Profile（証明書プロファイル）—**GP-client-cert**

Authentication Profile（認証プロファイル）—**Corp-LDAP**

Tunnel Interface（トンネル インターフェイス）—**tunnel.2**

IP Pool (IP プール)—**10.31.32.3 - 10.31.32.118**

STEP 9 | GlobalProtect ポータルを設定します。

Network（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択し、以下の設定を **Add**（追加）します。

1. GlobalProtect ポータルへのアクセスのセットアップ：

   Interface（インターフェイス）—**ethernet1/2**

   IP Address (IP アドレス)—**203.0.113.1**

   Server Certificate（サーバー証明書）—**GoDaddy** によって発行された **GP-server-cert.pem**

   Certificate Profile（証明書プロファイル）—**GP-client-cert**

   Authentication Profile（認証プロファイル）—**Corp-LDAP**
2. GlobalProtect エージェント設定の定義：

   Connect Method（接続方式）—オンデマンド（ユーザー操作による手動接続）

   External Gateway Address（外部ゲートウェイ アドレス）—**gp.acme.com**

STEP 10 | GlobalProtect アプリ ソフトウェアのデプロイを行います。

Device（デバイス） > **GlobalProtect Client**（**GlobalProtect** クライアント）の順に選択します。エージェント更新をポータルでホストするの手順に従ってください。

STEP 11 | （オプション）アプリの設定の透過的なデプロイをします。

ポータルの設定からアプリの設定をデプロイする代わりに、Windows レジストリやグローバル macOS plist から、エージェントの設定を直接定義することができます。デプロイできる設定例には、ポータル IP アドレスを指定することやユーザーがエンドポイントにログインして GlobalProtect ポータルに接続する前に GlobalProtect が VPN トンネルを開始できるようにすることを含みます。Windows エンドポイント上でのみ、MSIEXEC インストーラーを使っても構成設定ができます。詳しい情報については、カスタマイズ可能なアプリの設定を参照してください。

STEP 12 | （任意）GlobalProtect モバイル アプリケーションを使用できるようにします。

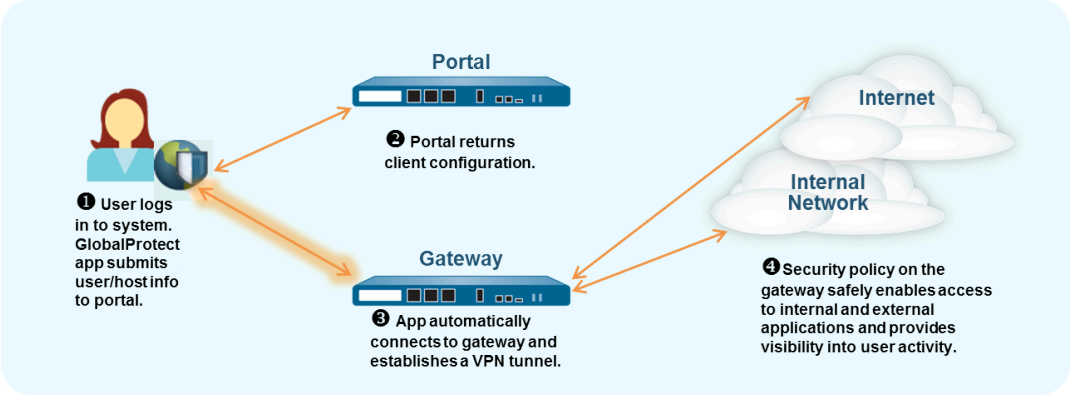
GlobalProtect ゲートウェイ サブスクリプションを購入してインストールし（**Device** > **Licenses**（ライセンス））、アプリを使用できるようにします。

STEP 13 | GlobalProtect の設定を保存します。

Commit（コミット）をクリックします。

常時オンの VPN 設定

「常時オン」の GlobalProtect 設定では、ユーザーのログイン時にアプリが GlobalProtect ポータルに接続し、ユーザーおよびホスト情報を送信してクライアント設定を受信します。次に、下の図に示すように、ポータルによって提供されるクライアント設定で指定されたゲートウェイへの VPN トンネルが自動的に接続され、確立されます。



次のいずれかのリモート アクセス VPN 設定を常時オン設定に切り替えるために、接続方式を変更できます。

- リモート アクセス VPN（認証プロファイル）
- リモート アクセス VPN（証明書プロファイル）
- 2 要素認証を使用したリモート アクセス VPN

リモートアクセス VPN 設定を常時オン設定に切り替えるには、次のステップを実行します。

STEP 1 | **Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） の順に選択し、ポータルの設定を選択します。

STEP 2 | **Agent**（エージェント）タブで、変更するエージェント設定を選択します。

STEP 3 | **App**（アプリ）を選択してから、**Connect Method**（接続手法）を **User-logon (Always On)**（ユーザー ログオン（常時オン））に設定します。

STEP 4 | **OK** をクリックして、エージェント設定を保存します。

STEP 5 | 変更するエージェント設定ごとにステップ 2～4 を繰り返します。

STEP 6 | **OK** をクリックしてポータル設定を保存し、変更を **Commit**（コミット）します。

Pre-Logon を使用したリモート アクセス VPN

Pre-logon とは、ユーザーがログインする前に VPN トンネルを確立する接続方式のことです。このログオン前の目的は、エンドポイントの電源が入ったらできるだけ早くエンドポイント（ユーザーではなく）を認証し、ドメイン スクリプトや他のタスクを実行することです。マシン証明書により、エンドポイントが GlobalProtect ゲートウェイとの VPN トンネルを確立できるようになります。IT 管理者は一般的に、ユーザーのためにエンドポイントを準備しながらマシン証明書をインストールします。

ユーザーがログインする前の状態であるため、ログオン前の VPN トンネルは関連付けのためにユーザー名を使用しません。トラスト ゾーン内のリソースにエンドポイントがアクセスできるようにするためには、ログオン前のユーザーとマッチするセキュリティポリシーを作成する必要があります。これらのポリシーは、DHCP、DNS、Active Directory（有効期限の切れたパスワードを変更する場合など）、アンチウイルス、オペレーティング システム更新サービスなど、システムの起動に必要な基本サービスへのアクセスのみを許可しなければなりません。ユーザーがゲートウェイを認証したら、GlobalProtect アプリは VPN トンネルをそのユーザーに再割り当てします（ファイアウォールの IP アドレスマッピングはログオン前のエンドポイントから認証されたユーザーに変更されます）。

Windows 7 および Windows 10 エンドポイント用の GlobalProtect Credential Provider ログオン画面には、ログイン前に事前ログオン接続ステータスも表示されます。これにより、エンドユーザーはログイン時にネットワークリソースにアクセスできるかどうかを判断できます。GlobalProtect アプリがエンドポイントを内部として検出すると、ログオン画面に内部プレログオン接続ステータスが表示されます。GlobalProtect アプリがエンドポイントを外部として検出すると、ログオン画面に接続済みまたは未接続 プレログオン接続ステータスが表示されます。

Windows エンドポイントは、プレログオンのある *macOS* エンドポイントとは動作が異なります。*macOS* エンドポイントの場合、プレログオン トンネルはユーザーがログインする際に破棄され、新しいトンネルが作成されます。

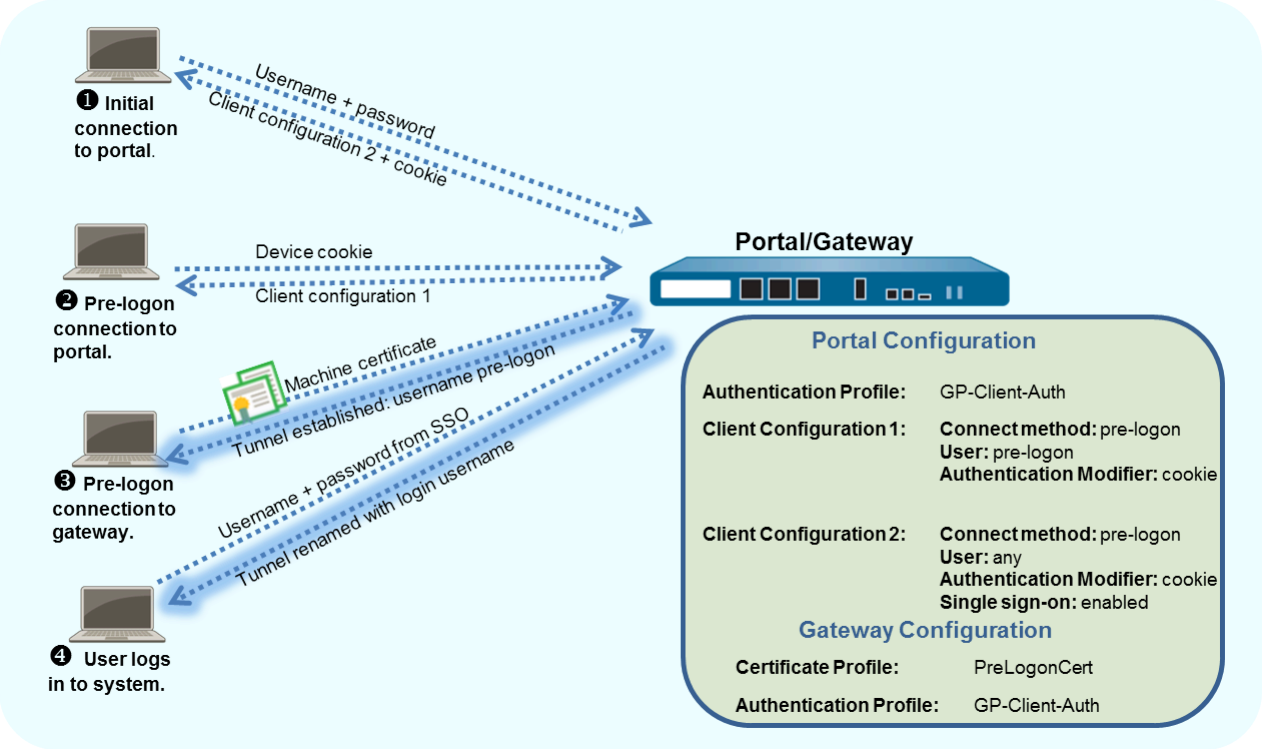
ユーザーが新しい接続をリクエストすると、ポータルが認証プロファイルを使用してユーザーを認証します。またポータルは、クライアント証明書を検証する証明書プロファイルを任意で使用することもできます（クライアント証明書が構成に含まれている場合）。この場合、ユーザー証明書がユーザーを識別する必要があります。認証後、エンドポイントの GlobalProtect 構成が最新のものであるかどうかをポータルが判断します。使用するポータルの構成が変更されると、ポータルは更新後の構成をエンドポイントにプッシュ送信します。

Cookie ベースの認証がポータルまたはゲートウェイ上の構成に含まれている場合、ポータルまたはゲートウェイは暗号化された Cookie をクライアント上にインストールします。それ以降、ポータルまたはゲートウェイがユーザー認証やエージェント側の構成を更新する際は、その Cookie を使用するようになります。Cookie 認証と共にプレ ログオンの接続方式がエージェント設定プロファイルに含まれている場合、GlobalProtect コンポーネントはプレ ログオンに Cookie を使用できます。

ユーザーが決してエンドポイントにログインしない場合（例えば、ヘッドレス エンドポイント）や、ユーザーが初めてログインするシステムでプレ ログオン接続が必要な場合、ポータルに接続してプレ ログオン設定をダウンロードさせる手続きを省いて、エンドポイントがプレ ログオン トンネルを確立できるようにすることが可能です。こうするためには、 Windows レジス

トリまたは macOS plist 内でントリを作成してデフォルトの動作をオーバーライドする必要があります。

次に、GlobalProtect エンドポイントが設定で指定されたポータルに接続し、そのマシン証明書（ゲートウェイで設定された証明書プロファイル内で指定）を使用してエンドポイントの認証を行い、GlobalProtect 接続を確立します。その後、エンドユーザーがマシンにログインし、エージェント設定でシングルサインオン（SSO）が有効になっている場合は、ユーザのログイン時にユーザー名とパスワードが取得されます。エージェント設定で SSO が有効になっていない場合、 または SSO がエンドポイントでサポートされていない場合（macOS システムなど）、Save User Credentials（ユーザー認証情報の保存）をアプリに保存する必要があります（ ユーザー認証情報の保存オプションを**Yes**（はい）に設定する必要があります）。ゲートウェイに対する認証に成功したら、トンネルの名前変更（macOS）または再構築が行われ、ユーザーベースおよびグループベースのポリシーを適用できます。



この例では、リモート アクセス用 GlobalProtect VPN に示された GlobalProtect トポロジを使用します。

STEP 1 | GlobalProtect のインターフェイスおよびゾーンの作成を行います。

すべてのインターフェイス設定に ***default***（デフォルト）仮想ルーターを使用し、ゾーン間ルーティングの作成を回避します。

- この例を挙げると、**Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）タブを選択し、次の構成を設定します。
  1. **Ethernet1/2**（イーサネット **1/2**）を選択します。
  2. **Interface Type**（インターフェイス タイプ）ドロップダウン リストから **Layer3**（レイヤー **3**）を選択します。
  3. **Config**（設定）タブで、**Assign Interface To**（インターフェイスの割り当て対象）を**Virtual Router**（仮想ルーター）および**l3-untrust Security Zone**（セキュリティ ゾーン）にデフォルト設定します。
  4. **IPv4** タブで、**Add**（追加）をクリックして **203.0.113.1** IP アドレス（または **203.0.113.1** をマップするオブジェクト）を選択するか、**New Address**（新規アドレス）を追加して新しいオブジェクトとアドレス マッピング（アドレス タイプは**Static**（静的）のまま）を作成します。たとえば、IP アドレス **203.0.113.1** を **gp.acme.com** にマッピングする DNS「A」レコードを作成します。
- **Network**（ネットワーク） > **Interfaces (**インターフェイス**)** > **Tunnel**（トンネル） を選択して新しいトンネル インターフェイスを**Add**（追加） します。
  1. **Interface Name**（インターフェイス名）の場合は、**tunnel.2** を選択します。
  2. **Config**（設定）タブで、 **corp-vpn** と呼ばれる新しい **Security Zone**（セキュリティ ゾーン）とデフォルトの **Virtual Router**（仮想ルーター）を**Assign Interface To**（インターフェイスの割り当て対象）にします。
- **corp-vpn** ゾーンの [User-ID の有効化] をオンにします。

STEP 2 | セキュリティ ポリシー ルールを作成します。

この設定では、以下のポリシーが必要になります（**Policies** > **Security**（セキュリティ））。

1. 認証サービス、DNS、DHCP、Microsoft Updates など、エンドポイントの起動に必要な基本サービスへのログオン前のユーザー アクセスを可能にするルールを **Add**（追加）します。
2. その他のすべての宛先およびアプリケーションへのログオン前のユーザー アクセスを拒否するルールを **Add**（追加） します。
3. さまざまなユーザーまたはユーザーグループが特定の送信先とアプリケーションにアクセスできるように、その他のルールを **Add**（追加） します。インターネット ゲートウェイのセキュリティポリシーの推奨設定に従ってこれらのルールを作成してください。

STEP 3 | 以下のいずれかの方法を使用して、GlobalProtect ポータルおよびゲートウェイをホストするインターフェイスのサーバー証明書を取得します。

- （推奨）一般的なサードパーティ CA からサーバー証明書をインポートします。
- ポータルでルート CA を使用して自己署名サーバー証明書を生成します。

Device > **Certificate Management** > **Certificates**(デバイス > 証明書の管理 > 証明書) の順に選択し、証明書を次の基準に基づいて管理します。

- サーバー証明書を取得します。ポータルとゲートウェイは同じインターフェイス上にあるため、両方のコンポーネントに同じサーバー証明書を使用できます。
- 証明書の CN は FQDN、gp.acme.com と一致する必要があります。
- エンドポイントが証明書エラーなしでポータルに接続できるようにするには、パブリック CA からのサーバー証明書を使用します。

STEP 4 | GlobalProtect に接続する各エンドポイント用のマシン証明書を生成し、証明書を各マシンの個人用証明書ストアにインポートします。

各エンドポイントに対して自己署名証明書を生成することもできますが、ベスト プラクティスとして独自の公開鍵インフラストラクチャ（PKI）を使用して、エンドポイントに証明書を発行および配布します。

1. GlobalProtect クライアントおよびエンドポイントに対してクライアント証明書を発行します。
2. エンドポイントの個人用証明書ストアに証明書をインストールします。（Windows エンドポイントのローカル コンピュータ ストアまたは macOS エンドポイントのシステム キーチェーン）

STEP 5 | マシン証明書を発行した CA からの信頼されたルート CA 証明書をポータルとゲートウェイにインポートします。

秘密鍵をインポートする必要はありません。

1. Base64 形式で CA 証明書をダウンロードします。
2. 次のステップに従って、ポータルまたはゲートウェイをホストする各ファイアウォールに、以下の手順で証明書をインポートします。
   1. **Device**（デバイス） > **Certificate Management**（証明書の管理） > **Certificates**（証明書） > **Device Certificates**（デバイス証明書）の順に選択してから **Import**（インポート）をクリックします。
   2. **Certificate Name**（証明書名）フィールドに、クライアント CA 証明書であることを識別できる名前を入力します。
   3. **Browse**（参照）をクリックして、CA からダウンロードした **Certificate File**（証明書ファイル）を選択します。
   4. **File Format**（ファイル フォーマット）を **Base64 Encoded Certificate (PEM)**（**Base64** エンコード済み証明書 **(PEM)**）に設定します。
   5. **OK** をクリックして、証明書を保存します。
   6. **Device Certificates**（デバイス証明書）タブで、先ほどインポートした証明書を選択します。
   7. **Trusted Root CA**（信頼されたルート **CA**）のチェックボックスを選択して、**OK** をクリックします。

STEP 6 | GlobalProtect ゲートウェイをホストする各ファイアウォールで、クライアント マシン証明書の検証に使用する CA 証明書を決定する証明書プロファイルを作成します。

システムへのログイン時のユーザー認証にクライアント証明書の認証を使用する場合、マシン証明書を発行した CA 証明書に加えて、クライアント証明書を発行した CA 証明書が異なる場合はその CA 証明書も証明書プロファイル内で参照されていることを確認します。

1. **Device**（デバイス） > **Certificates**（証明書） > **Certificate Management**（証明書の管理） > **Certificate Profile**（証明書プロファイル）の順に選択し、新しい証明書プロファイルを **Add(追加)**します。
2. **`PreLogonCert`** などの、サーバー プロファイルを識別する **Name**（名前）を入力します。
3. **Username Field**（ユーザー名欄）を **None**（なし）に設定します。
4. （任意）ログイン時のユーザー認証にクライアント証明書の認証も使用する場合、クライアント証明書を発行した CA 証明書がマシン証明書を発行した CA 証明書と異なる場合はその CA 証明書を追加します。
5. **CA Certificates**（**CA** 証明書）欄で、CA 証明書を**Add**（追加）します。
6. ステップ 5 でインポートした **Trusted Root CA**（信頼されたルート **CA**）を選択してから、**OK** をクリックします。
7. **OK** をクリックしてプロファイルを保存します。

STEP 7 | GlobalProtect ゲートウェイの設定を行います。

リモート アクセス用 GlobalProtect VPN に示されたトポロジ図を参照してください。

ゲートウェイへのログオン前のアクセス用に証明書プロファイルを作成する必要がありますが、ログイン ユーザーにはクライアント証明書の認証か認証プロファイル ベースの認証のいずれかを使用できます。この例では、ポータルに対するユーザー認証に使用されるものと同じ LDAP プロファイルが使用されています。

1. **Network**（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ）の順に選択し、以下のゲートウェイ設定を **Add**（追加）します。

   Interface（インターフェイス）—**ethernet1/2**

   IP Address (IP アドレス)—**203.0.113.1**

   Server Certificate（サーバー証明書）—**GoDaddy** によって発行された **GP-server-cert.pem**

   Certificate Profile(証明書プロファイル)—**PreLogonCert**

   Authentication Profile（認証プロファイル）—**Corp-LDAP**

   Tunnel Interface（トンネル インターフェイス）—**tunnel.2**

   IP Pool (IP プール)—**10.31.32.3 - 10.31.32.118**
2. ゲートウェイ設定を **Commit**（コミット）します。

STEP 8 | GlobalProtect ポータルを設定します。

Device（デバイス） の詳細設定（ネットワーク パラメータ、認証サービス プロファイル、認証サーバー用の証明書）を行います。

Network（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択し、以下のポータル設定を **Add**（追加）します。

GlobalProtect ポータルへのアクセスのセットアップ：

Interface（インターフェイス）—**ethernet1/2**

IP Address (IP アドレス)—**203.0.113.1**

Server Certificate（サーバー証明書）—**GoDaddy** によって発行された **GP-server-cert.pem**

Certificate Profile (証明書プロファイル)—**None （なし）**

Authentication Profile（認証プロファイル）—Corp-LDAP

STEP 9 | ログオン前のユーザーおよびログイン済みユーザー用にGlobalProtect エージェント設定の定義を行います。

ログオン前のユーザーがログインする前後で同じゲートウェイにアクセスしてほしい場合は、単一の設定を使用します。

ログオン前のユーザーをログイン前後で別のゲートウェイにリダイレクトする場合は、設定プロファイルを 2 つ作成します。この最初の設定の**User/User Group**（ユーザー/ユーザーグ

ループ）で、**pre-logon**（ログオン前）フィルターを選択します。ログオン前では、（ログオン前のパラメータがユーザーと関連付けられている場合でも）ポータルはまずユーザーでは

なくエンドポイントを認証し、接続のセットアップを行います。それ以降、ポータルはユーザーがログインする際に認証を行います。

ポータルはユーザーを認証した後、2 つ目の設定をデプロイします。この場合、**User/User Group**（ユーザー/ユーザーグループ）は **any**（いずれか）です。

ベスト プラクティスとして、*2* 番目の設定で *SSO* を有効にし、ユーザーがエンドポイントにログインする際に即座に正しいユーザー名がゲートウェイに報告されるようにします。*SSO* が有効になっていない場合、*GlobalProtect* エージェントの設定パネルにある保存済みのユーザー名が使用されます。

GlobalProtect Portal Configuration（**GlobalProtect** ポータル設定）ウィンドウ（**Network**（ネットワーク） > **GlobalProtect** > **Portals**（ポータル） > **<portal-config>**）の **Agent**（エージェント）タブを選択し、次の設定のいずれか一つを**Add**（追加）します：

- ログオン前のユーザーがログインする前後で同じゲートウェイを使用する場合：

Use single sign-on（シングル サインオンの使用）–**enabled**

Connect Method(接続方式)–**pre-logon**(プレ ログオン)

External Gateway Address(外部ゲートウェイ アドレス)–**gp1.acme.com**

User/User Group（ユーザー/ユーザー グループ）–**any**

Authentication Override（認証のオーバーライド）–透明性を確保しながらユーザー認証および構成の更新を行う Cookie 認証

- ログオン前のユーザーがログインする前後で別のゲートウェイを使用する場合：

最初のエージェント設定：

Connect Method(接続方式)–**pre-logon**(プレ ログオン)

External Gateway Address(外部ゲートウェイ アドレス)–**gp1.acme.com**

User/User Group(ユーザー/ユーザー グループ)–**pre-logon**(プレ ログオン)

Authentication Override（認証のオーバーライド）–透明性を確保しながらユーザー認証および構成の更新を行う Cookie 認証

2 つ目のエージェント設定：

Use single sign-on（シングル サインオンの使用）–**enabled**

Connect Method(接続方式)–**pre-logon**(プレ ログオン)

External Gateway Address（外部ゲートウェイ アドレス）–**gp2.acme.com**

User/User Group（ユーザー/ユーザー グループ）–**any**

Authentication Override（認証のオーバーライド）–透明性を確保しながらユーザー認証および構成の更新を行う Cookie 認証

ログオン前設定が設定リストの先頭であることを確認します。先頭でない場合は選択して **Move Up**（上へ）をクリックします。

STEP 10 | GlobalProtect の設定を保存します。

Commit（コミット）をクリックします。

STEP 11 | （任意） ユーザーが決してデバイスにログインしない場合（例えば、ヘッドレスデバイス）やユーザーが初めてログインするエンドポイントでプレ ログオン 接続が必要な場合、`Prelogon` レジストリエントリをエンドポイント上に作成します。

また、デフォルトのポータル *IP* アドレスを事前にデプロイする必要もあります。

レジストリ設定の詳細については、アプリの設定の透過的なデプロイを参照してください。

1. GlobalProtect の設定の一覧を表示するには、次の Windows レジストリの場所に移動します：

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

2. **Edit (編集)** > **New (新規)** > **String Value (文字列値)** を選択して次のレジストリのエントリを作成します：

   - **`Prelogon`** という名前で値が **1** の **String Value (文字列)** を作成します。この設定によりユーザーがエンドポイントにログインする前に GlobalProtect が接続を開始できます。
   - **`Portal`** と名付けて **String Value**（文字列値）を作成します。この文字列値は IP アドレスまたは GlobalProtect エンドポイントのデフォルト ポータルのホスト名を特定します。

GlobalProtect 複数ゲートウェイ設定

以下の GlobalProtect 複数ゲートウェイ トポロジでは、2 番目の外部ゲートウェイが設定に追加されています。このトポロジでは、2 番目の GlobalProtect ゲートウェイをホストするためにファイアウォールを追加構成する必要があります。ポータルによってデプロイされるクライアント構成を追加するときに、クライアント構成ごとに異なるゲートウェイを指定したり、すべてのゲートウェイへのアクセスを許可することもできます。

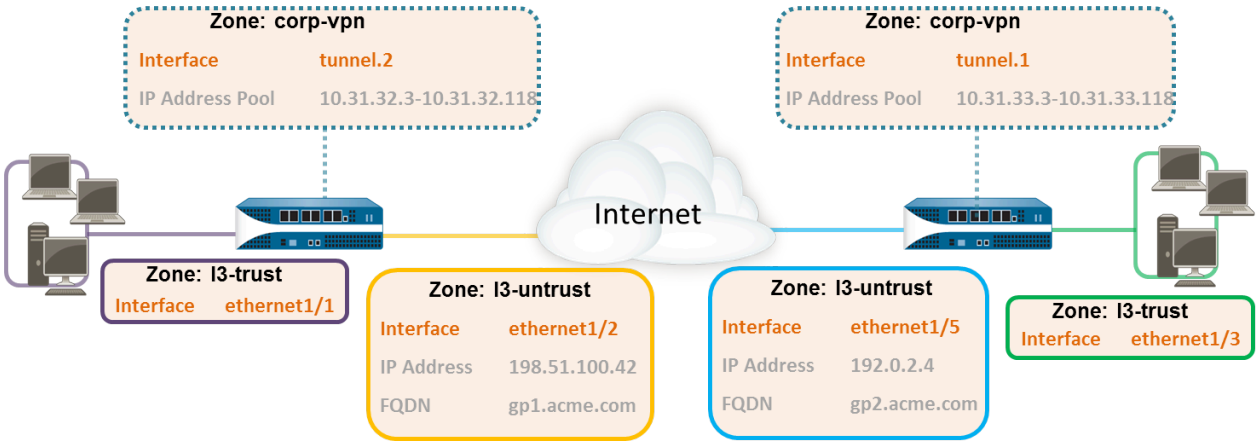


図 **7 : GlobalProtect** 複数ゲートウェイ トポロジ

クライアント設定に複数のゲートウェイが含まれている場合、アプリはクライアント設定に含まれるすべてのゲートウェイへの接続を試みます。次に、アプリは優先順位と応答時間を使用して、接続するゲートウェイを決定します。アプリは、優先順位が高いゲートウェイの応答時間が全ゲートウェイの応答時間の平均よりも長い場合にのみ、優先順位が低いゲートウェイに接続します。詳細については、複数ゲートウェイ構成時のゲートウェイの優先順位を参照してください。

STEP 1 | GlobalProtect のインターフェイスおよびゾーンの作成を行います。

この設定では、ゲートウェイをホストする各ファイアウォールでインターフェイスをセットアップする必要があります。

すべてのインターフェイス設定に ***default***（デフォルト）仮想ルーターを使用し、ゾーン間ルーティングの作成を回避します。

ポータル/ゲートウェイ（gw1）をホストするファイアウォールで、以下を実行します。

- **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** を選択し、さらに **ethernet1/2** を選択します。
- **ethernet1/5** を、IP アドレス **192.0.2.4** を含む Layer3 インターフェイスとして設定し、それを **l3-untrust** Security Zone（セキュリティ ゾーン） および **Virtual Router**（仮想ルーター）に割り当てます。
- IP アドレス **198.51.100.42** を **gp1.acme.com** にマッピングする DNS「A」レコードを作成します。
- **Network**（ネットワーク） > **Interfaces (インターフェイス)** > **Tunnel**（トンネル） を選択して **tunnel.2** インターフェイスを**Add**（追加） します。インターフェイスを **corp-vpn** と呼ばれる新しい **Security ZoneSecurity Zone**（セキュリティ ゾーン） に追加します。このインターフェイスを **default** Virtual Router (仮想ルーター) に割り当てます。
- **corp-vpn** ゾーンの [User-ID の有効化] をオンにします。

2 番目のゲートウェイ（gw2）をホストするファイアウォールで、以下を実行します。

- **Network (ネットワーク)** > **Interfaces (インターフェイス)** > **Ethernet (イーサネット)** を選択し、さらに **ethernet1/5** を選択します。
- **ethernet1/5** を、IP アドレス **192.0.2.4** を含む Layer3 インターフェイスとして設定し、それを **l3-untrust** Security Zone（セキュリティ ゾーン） および **Virtual Router**（仮想ルーター）に割り当てます。
- IP アドレス **192.0.2.4** を **gp2.acme.com** にマッピングする DNS「A」レコードを作成します。
- **Network**（ネットワーク） > **Interfaces (インターフェイス)** > **Tunnel**（トンネル） を選択して **tunnel.1** インターフェイスを**Add**（追加） します。インターフェイスを **corp-vpn** と呼ばれる新しい **Security ZoneSecurity Zone**（セキュリティ ゾーン） に追加します。このインターフェイスをデフォルトの **Virtual Router**（仮想ルーター）に割り当てます。
- **corp-vpn** ゾーンの [User-ID の有効化] をオンにします。

STEP 2 | モバイル エンドポイントで GlobalProtect アプリケーションを使用するエンドユーザーがいる場合、または HIP 対応のセキュリティ ポリシーを使用する場合、各ゲートウェイの GlobalProtect サブスクリプションを購入してインストールします。

GlobalProtect サブスクリプションを購入してアクティベーション コードを受け取ったら、以下の手順に従ってポータルをホストするファイアウォールにライセンスをインストールします。

1. **Device** > **Licenses (**デバイス **>** ライセンス**)**を選択します。
2. **Activate feature using authorization code**（認証コードを使用した機能のアクティベーション）を選択します。
3. **Authorization Code**（認証コード）の入力を促されたら、認証コードを入力して **OK** をクリックします。
4. ライセンスが正常にアクティベーションされたことを確認します：

STEP 3 | GlobalProtect ゲートウェイをホストしている各ファイアウォールで、セキュリティ ポリシーを作成します。

この設定では、**corp-vpn** ゾーンと **l3-trust** ゾーン間のトラフィック フローを有効にして内部リソースへのアクセスを可能にするポリシー ルールが必要です（**Policies**（ポリシー） > **Security**（セキュリティ）

STEP 4 | GlobalProtect ポータルおよび GlobalProtect ゲートウェイをホストする各インターフェイスのサーバー証明書を取得するには、次の推奨事項を使用してください。

- （ポータルまたはポータル/ゲートウェイをホストしているファイアウォール上で）一般的なサードパーティ CA からサーバー証明書をインポートします。
- （ゲートウェイのみをホストしているファイアウォール上で）ポータルでルート CA を使用して自己署名サーバー証明書を生成します。

ポータル/ゲートウェイまたはゲートウェイをホストする各ファイアウォールで、**Device** > **Certificate Management** > **Certificates**(デバイス > 証明書の管理 > 証明書) の順に選択し、以下のように証明書を管理します。

- ポータル/gw1 をホストするインターフェイスのサーバー証明書を取得します。ポータルとゲートウェイは同じインターフェイス上にあるため、同じサーバー証明書を使用する必要があります。証明書の CN は FQDN、`gp1.acme.com` と一致する必要があります。エンドポイントが証明書エラーなしでポータルに接続できるようにするには、パブリック CA からのサーバー証明書を使用します。
- gw2 をホストするインターフェイスのサーバー証明書を取得します。このインターフェイスはゲートウェイのみをホストするため、自己署名証明書を使用できます。証明書の CN は FQDN、`gp2.acme.com` と一致する必要があります。

STEP 5 | ポータルおよびゲートウェイに対するユーザーの認証方法を定義します。

必要に応じて、証明書プロファイルと認証プロファイルの任意の組み合わせを使用し、ポータルおよびゲートウェイのセキュリティを確保できます。ポータルおよび個々のゲートウェイには、異なる認証スキームを使用することもできます。この手順は、以下のセクションを参照してください。

- 外部認証のセットアップ（認証プロファイル）
- クライアント証明書認証のセットアップ（証明書プロファイル）
- 2 要素認証のセットアップ（トークンまたは OTP ベース）

次に、ポータルおよびゲートウェイ設定の証明書プロファイルや認証プロファイルを参照する必要があります。

STEP 6 | GlobalProtect ゲートウェイの設定を行います。

次の例では、GlobalProtect 複数ゲートウェイ トポロジに示された gp1 と gp2 の設定を使用しています。

ファイアウォール ホスティング gp1 で、**Network**（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ） の順に選択します。ゲートウェイ設定を次の通りに構成します：

Interface（インターフェイス）—**ethernet1/2**

IP Address (IP アドレス)—**198.51.100.42**

Server Certificate（サーバー証明書）—**GP1-server-cert.pem issued by GoDaddy**

Tunnel Interface（トンネル インターフェイス）—**tunnel.2**

IP Pool (IP プール)—**10.31.32.3 - 10.31.32.118**

ファイアウォール ホスティング gp1 で、**Network**（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ） の順に選択します。ゲートウェイ設定を次の通りに構成します：

Interface（インターフェイス）—**ethernet1/2**

IP Address (IP アドレス)—**198.51.100.42**

Server Certificate(サーバー証明書)—**self-signed certificate, GP2-server-cert.pem**

トンネル インターフェイス：**tunnel.1**

IP Pool (IP プール)—**10.31.33.3 - 10.31.33.118**

STEP 7 | GlobalProtect ポータルを設定します。

Network (ネットワーク) > GlobalProtect > Portalsポータル.を選択します。ポータル設定を次の通りに構成します：

1. GlobalProtect ポータルへのアクセスのセットアップ：

   Interface（インターフェイス）—ethernet1/2

   IP Address (IP アドレス)—198.51.100.42

   Server Certificate（サーバー証明書）—GP1-server-cert.pem issued by GoDaddy

2. GlobalProtect エージェント設定の定義：

   作成するクライアント設定数は、ユーザー/グループ ベースのポリシーや HIP 対応のポリシーの適用が必要かどうかを含む、特定のアクセス要件によって異なります。

STEP 8 | GlobalProtect エージェント ソフトウェアのデプロイを行います。

Device > GlobalProtect Client（GlobalProtect クライアント）の順に選択します。

この例では、アプリ更新をポータルでホストする手順に従います。

STEP 9 | GlobalProtect の設定を保存します。

ポータルおよびゲートウェイをホストするファイアウォールで設定を **Commit（コミット）**します。

GlobalProtect による内部 HIP チェックとユーザーベースのアクセス

User-ID や HIP チェックと併用した場合、内部ゲートウェイはユーザーやデバイス状態別にトラフィックを安全かつ正確に識別して制御する方法を提供するため、その他のネットワーク アクセス制御（NAC）サービスの代わりに使用できます。内部ゲートウェイは、重要なリソースへの認証済みアクセスが必要な機密環境で役立ちます。

内部ゲートウェイのみの設定では、すべてのエンドポイントがユーザー ログオン モード（常時オン）で設定されている必要があります。オンデマンド モードはサポートされていません。さらに、すべてのクライアント設定でシングル サインオン（SSO）を使用することをお勧めします。また、内部ホストはゲートウェイとのトンネル接続を確立する必要はないため、エンドポイントの物理ネットワーク アダプタの IP アドレスが使用されます。

このクイック設定では、Engineering グループのユーザーに内部ソース管理とバグ データベースへのアクセスを許可し、Finance グループのユーザーに CRM アプリケーションへのアクセスを許可するグループ ベースのポリシーの適用に内部ゲートウェイが使用されています。認証されたすべてのユーザーは内部 Web リソースにアクセスできます。さらに、ゲートウェイで設定された HIP プロファイルでは、最新のセキュリティ パッチがインストールされているかどうか、ディスク暗号化が有効になっているかどうか、必須ソフトウェアがインストールされているかどうかなどの内部メンテナンス要件に各ホストが従っていることを確認します。

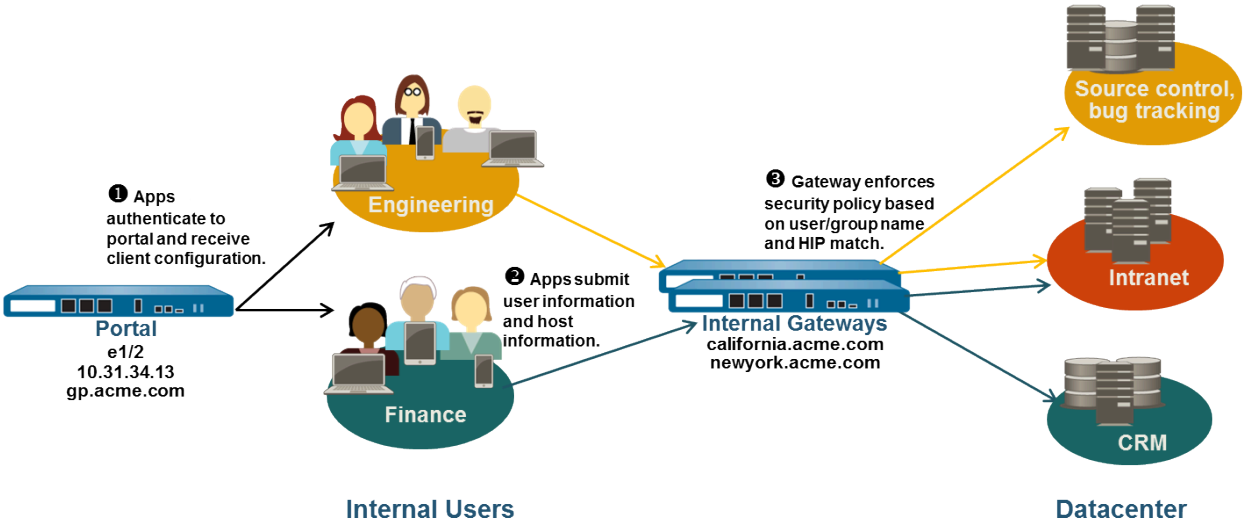


図 **8 : GlobalProtect** 内部ゲートウェイ設定

次のステップに従い、GlobalProtect の内部ゲートウェイを構成します。

STEP 1 | GlobalProtect のインターフェイスおよびゾーンの作成を行います。

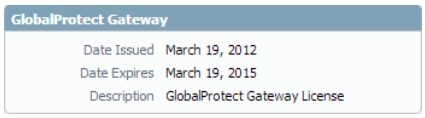
この設定では、ポータルやゲートウェイをホストする各ファイアウォールでインターフェイスをセットアップする必要があります。この設定では内部ゲートウェイのみを使用するため、内部ネットワークのインターフェイスでポータルおよびゲートウェイを設定する必要があります。

すべてのインターフェイス設定に ***default***（デフォルト）仮想ルーターを使用し、ゾーン間ルーティングの作成を回避します。

ポータル/ゲートウェイをホストする各ファイアウォールで、以下を実行します。

1. ポータル/ゲートウェイをホストする Ethernet ポートを選択し、**`l3-trust` Security Zone**（セキュリティ ゾーン）（**Network**（ネットワーク） > **Interfaces** > **Ethernet**（イーサネット））に IP アドレス付きのレイヤー 3 インターフェイスを設定します。
2. **`l3-trust`** ゾーンの **[User-ID** の有効化] チェック ボックスをオンにします。

STEP 2 | エンドユーザーのいずれかがモバイル デバイス上の GlobalProtect アプリにアクセスする場合、または HIP 対応セキュリティ ポリシーを使用する予定の場合は、内部ゲートウェイをホストするファイアウォールごとに GlobalProtect サブスクリプションを購入してインストールします。



GlobalProtect サブスクリプションを購入してアクティベーション コードを受け取ったら、以下の手順に従い、ゲートウェイをホストするファイアウォールに GlobalProtect サブスクリプションをインストールします：

1. **Device** > **Licenses (**デバイス **>** ライセンス**)**を選択します。
2. **Activate feature using authorization code**（認証コードを使用した機能のアクティベーション）を選択します。
3. **Authorization Code**（認証コード）の入力を促されたら、認証コードを入力して **OK** をクリックします。
4. ライセンスが正常にアクティベーションされたことを確認します。

必要なライセンスがない場合は、Palo Alto Networks のセールス エンジニアまたはリセラーにお問い合わせください。ライセンスの詳細は、GlobalProtect ライセンスについてを参照してください。

STEP 3 | GlobalProtect ポータルおよび各 GlobalProtect ゲートウェイのサーバー証明書を取得します。

エンドポイントがポータルに初めて接続する場合、ポータル サーバー証明書の発行に使用されたルート CA 証明書を信頼する必要があります。最初のポータル接続前にポータルで自己

署名証明書を使用してルート CA 証明書をエンドポイントにデプロイするか、信頼された CA からポータル用のサーバー証明書を取得することができます。

ゲートウェイでは自己署名証明書を使用できます。

推奨されるワークフローは以下のとおりです。

1. ポータルをホストするファイアウォールで、以下を実行します。
   1. 一般的なサードパーティ CA からサーバー証明書をインポートします。
   2. GlobalProtect コンポーネントの自己署名証明書を発行するためのルート CA 証明書を作成します。
   3. ポータルでルート CA を使用して自己署名サーバー証明書を生成します。各ゲートウェイでこの手順を繰り返します。
2. 内部ゲートウェイをホストする各ファイアウォールで、自己署名入りサーバー証明書をデプロイします。

STEP 4 | ポータルおよびゲートウェイに対するユーザーの認証方法を定義します。

必要に応じて、証明書プロファイルと認証プロファイルの任意の組み合わせを使用し、ポータルおよびゲートウェイのセキュリティを確保できます。ポータルおよび個々のゲートウェイには、異なる認証スキームを使用することもできます。この手順は、以下のセクションを参照してください。

- 外部認証のセットアップ（認証プロファイル）
- クライアント証明書認証のセットアップ（証明書プロファイル）
- 2 要素認証のセットアップ（トークンまたは OTP ベース）

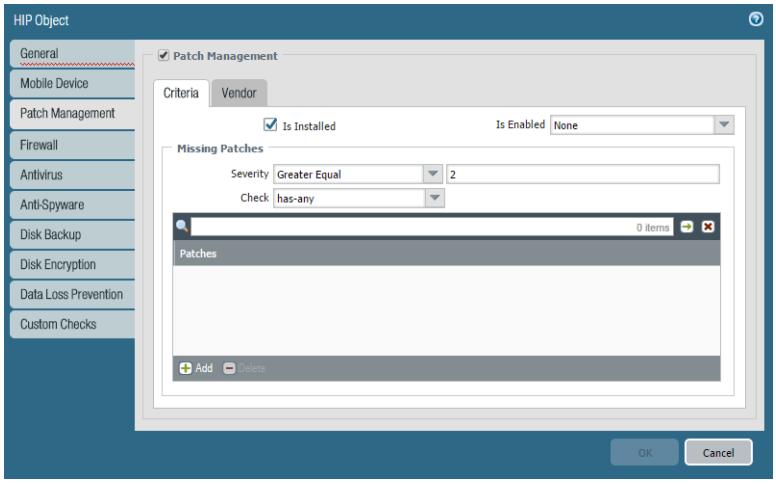
次に、ポータルおよびゲートウェイ設定の証明書プロファイルや認証プロファイルを参照する必要があります。

STEP 5 | ゲートウェイへのアクセスにセキュリティ ポリシーを適用する必要がある HIP プロファイルを作成します。

HIP 照合の詳細は、ホスト情報を参照してください。

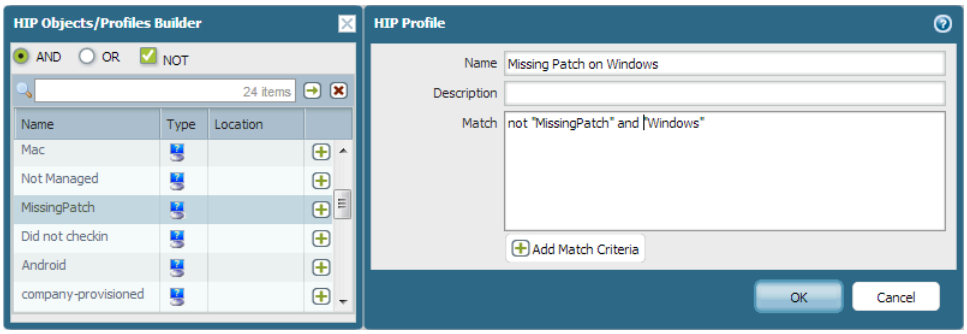
1. アプリが収集した生ホスト データにフィルタをかける HIP オブジェクトを作成します。たとえば、最新の必須パッチが適用されていないユーザーによるアクセスを禁止する場合、パッチ管理ソフトウェアがインストール済みかどうか、および指定された重

大度のすべてのパッチが最新であるかどうかを照合する HIP オブジェクトを作成します。



2. ポリシーで使用する HIP プロファイルを作成します。

   たとえば、最新のパッチが適用された Windows ユーザーのみが内部アプリケーションにアクセスできるようにするには、欠落しているパッチが存在しないホストを照合する以下の HIP プロファイルを関連付けます。



STEP 6 | 内部ゲートウェイを設定します。

Network (ネットワーク) > **GlobalProtect** > **Gateways**（ゲートウェイ） の順に選択し、既存のポータル設定を選択するか、新しいゲートウェイを **Add (追加)** します。以下のゲートウェイ設定を構成します：

- **interface** インターフェイス
- **IP** アドレス
- サーバー証明書
- **Authentication Profile**（認証プロファイル）/**Configuration Profile**（設定プロファイル）

ゲートウェイ設定ではトンネル接続は不要なため、（HIP 通知をセットアップしない限り）クライアント設定は必要ありません。ゲートウェイ設定の作成手順は、GlobalProtect ゲートウェイの設定を参照してください。

STEP 7 | GlobalProtect ポータルを設定します。

これまでのすべての設定では ***Connect Method***（接続方式）に *User-logon (Always On)*（ユーザーログオン（常にオン））または ***On-demand (Manual user initiated connection)***（オンデマンド（ユーザーが手動で接続を開始））を使用できますが、内部ゲートウェイ設定は常時オンである必要があるため、***Connect Method***（接続方式）には *User-logon (Always On)*（ユーザーログオン（常にオン））を使用する必要があります。

Network (ネットワーク) > **GlobalProtect** > **Portals (ポータル)** の順に選択し、既存のポータルを選択するか、新しいポータルを **Add (追加)** します。ポータルを次の通りに構成します：

1. GlobalProtect ポータルへのアクセスのセットアップ：

   Interface（インターフェイス）—**ethernet1/2**

   IP Address（IP アドレス）—**10.31.34.13**

   Server Certificate（サーバー証明書）—**GP-server-cert.pem issued by GoDaddy** で **CN=gp.acme.com**
2. GlobalProtect クライアント認証設定の定義：

   Use single sign-on（シングル サインオンの使用）—**enabled**

   Connect Method（接続方式）—**User-logon (Always On)**

   Internal Gateway Address（内部ゲートウェイ アドレス）—**california.acme.com, newyork.acme.com**

   User/User Group（ユーザー/ユーザー グループ）—**any**
3. ポータル設定を **Commit**（コミット）します。

STEP 8 | GlobalProtect アプリ ソフトウェアのデプロイを行います。

Device > **GlobalProtect Client**（**GlobalProtect** クライアント）の順に選択します。

この例では、アプリ更新をポータルでホストする作業を行います。

STEP 9 | ゲートウェイの HIP 対応セキュリティ ルールやユーザー/グループ ベースのセキュリティ ルールを作成します。

この例では、以下のセキュリティ ルールを追加します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択し、**Add**（追加）をクリックします。
2. **Source**（送信元）タブで **Source Zone**（送信元ゾーン）を **l3-trust** に設定します。
3. **User**（ユーザー）タブで、照合する HIP プロファイルとユーザー/グループを追加します。
   - **HIP Profiles**（**HIP** プロファイル）エリアで **Add**（追加）をクリックし、**MissingPatch** という HIP プロファイルを選択します。
   - **Source User**（送信元ユーザー）を **Add**（追加）し、「Finance」または「Engineering」というグループを作成して選択します。
4. **OK** をクリックしてルールを保存します。
5. ゲートウェイ設定を **Commit**（コミット）します。

			Source				Destination				
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	CRM access	none	l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	✓
2	Eng access	none	l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	✓

内部ゲートウェイと外部ゲートウェイの混合設定

GlobalProtect の内部ゲートウェイと外部ゲートウェイの混合設定では、VPN アクセス用のゲートウェイと機密内部リソースへのアクセス用のゲートウェイを個別に設定できます。この設定では、GlobalProtect アプリが内部ホスト検出を実行し、内部ネットワークと外部ネットワークのどちらに属しているかを特定します。アプリが外部ネットワークにあると判断された場合、クライアント設定に含まれる外部ゲートウェイへの接続を試み、優先順位が最も高く、応答時間が最も短いゲートウェイで接続を確立します。

すべての外部を手動専用のゲートウェイとして設定する一方で *GlobalProtect* 接続方法を ***User-Logon (Always On)***（ユーザー ログオン（常時オン）） または ***Pre-Logon (Always On)***（ログオン前（常時オン））に設定する場合は、*GlobalProtect* アプリはどの外部ゲートウェイにも自動接続しません。外部ユーザーが手動でゲートウェイ接続を確立しない限り、*GlobalProtect* は ***Not Connected***（未接続）状態のままです。この動作により、外部ユーザーの ***On-Demand***（オンデマンド） *VPN* 動作をサポートしながら、内部ユーザーのユーザー*ID*を取得するために *GlobalProtect* をデプロイできます。

セキュリティ ポリシーはゲートウェイごとに個別に定義されるため、外部ユーザーと内部ユーザーがアクセスできるリソースを詳細に制御できます。さらに、ユーザー/グループ メンバーシップまたは HIP プロファイル照合に基づいて異なるクライアント設定をデプロイするようにポータルを設定することで、ユーザーがアクセスできるゲートウェイも詳細に制御できます。

この例では、ポータルおよび 3 つすべてのゲートウェイ（1 つが外部で 2 つが内部）が個別のファイアウォールにデプロイされています。gpvpn.acme.com の外部ゲートウェイは企業ネットワークへのリモート VPN アクセスを提供し、内部ゲートウェイはグループ メンバーシップに基づく機密データセンター リソースへの詳細なアクセス制御を提供します。さらに、データセンターにアクセスするホストのセキュリティ パッチが常に最新になるように、HIP チェックが使用されています。

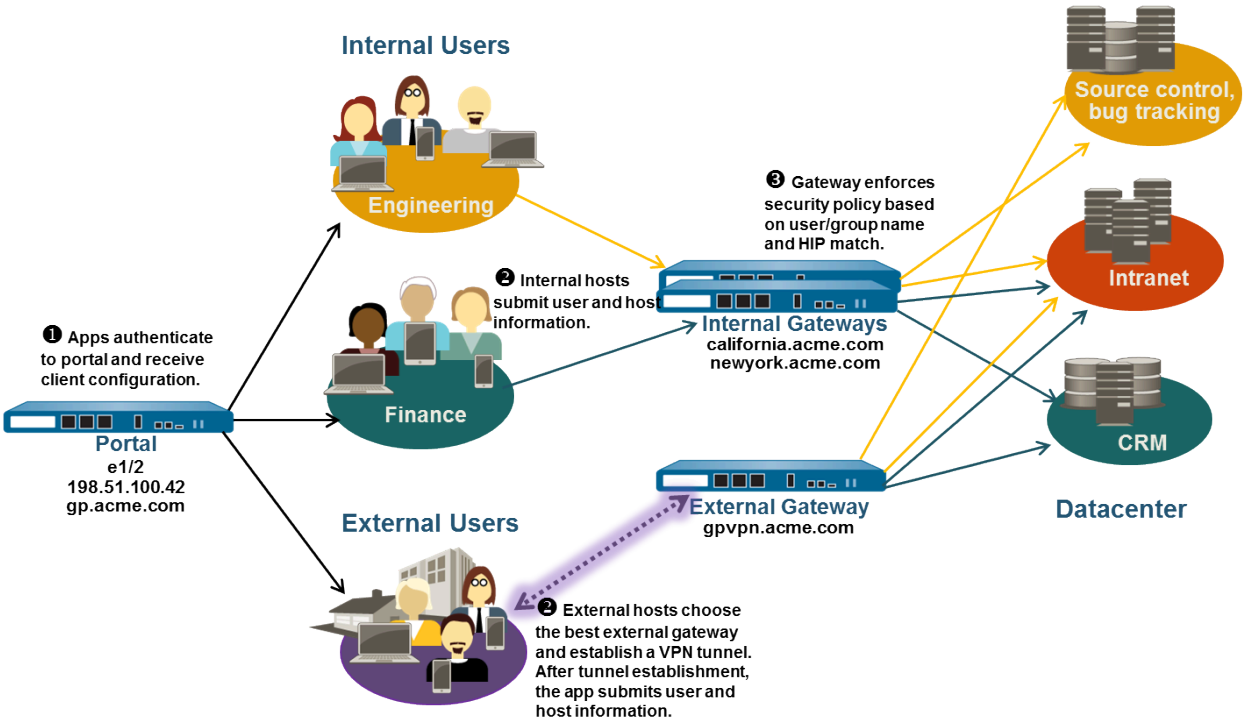


図 **9 :** 内部ゲートウェイと外部ゲートウェイを使用した **GlobalProtect** デプロイメント

次のステップを実行することにより、内部・外部の GlobalProtect ゲートウェイをまとめて構成できます。

STEP 1 | GlobalProtect のインターフェイスおよびゾーンの作成を行います。

この設定では、ポータルをホストするファイアウォールおよびゲートウェイをホストする各ファイアウォールでインターフェイスをセットアップする必要があります。

GlobalProtect ポータルまたはゲートウェイを設定したインターフェイスで *HTTP*、*HTTPS*、*Telnet*、または *SSH* を許可するインターフェイス管理プロファイルを追加すると、インターネットからの管理インターフェイスへのアクセスを許可することになるため、追加しないでください。管理アクセスの保護のベストプラクティスに従い、攻撃を阻止するようにファイアウォールへの管理アクセスを保護してください。

すべてのインターフェイス設定に ***default***（デフォルト）仮想ルーターを使用し、ゾーン間ルーティングの作成を回避します。

ポータル ゲートウェイ（gp.acme.com）をホストするファイアウォールで、以下を実行します。

- **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）の順に選択して、**ethernet1/2** を IP アドレス **198.51.100.42** を含む Layer 3 Ethernet インターフェイスに設定します。これを **l3-untrust Security Zone**（セキュリティ ゾーン）およびデフォルトの **Virtual Router**（仮想ルーター）に割り当てます。
- IP アドレス 198.51.100.42 を gp.acme.com にマッピングする DNS「A」レコードを作成します。
- **Network**（ネットワーク） > **Interfaces (インターフェイス)** > **Tunnel**（トンネル） を選択して **tunnel.2** インターフェイスを**Add**（追加） します。これを corp-vpn と呼ばれる新しい **Security Zone**（セキュリティ ゾーン）とデフォルトの **Virtual Router**（仮想ルーター）に割り当てます。
- corp-vpn ゾーンの [ユーザー ID の有効化] をオンにします。

外部ゲートウェイ（gpvpn.acme.com）をホストするファイアウォールで、以下を実行します。

- **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）の順に選択して、**ethernet1/2** を IP アドレス **198.51.100.42** を含む Layer 3 Ethernet インターフェイスに設定します。これを **l3-untrust Security Zone**（セキュリティ ゾーン）およびデフォルトの **Virtual Router**（仮想ルーター）に割り当てます。
- IP アドレス 192.0.2.4 を gpvpn.acme.com にマッピングする DNS「A」レコードを作成します。
- **Network**（ネットワーク） > **Interfaces (インターフェイス)** > **Tunnel**（トンネル） を選択して **tunnel.3** インターフェイスを**Add**（追加） します。これを corp-vpn と呼ばれる

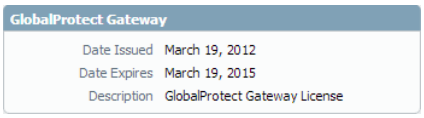
新しい **Security Zone**（セキュリティ ゾーン）とデフォルトの **Virtual Router**（仮想ルーター）に割り当てます。

- corp-vpn ゾーンの [ユーザー ID の有効化] をオンにします。

内部ゲートウェイ（california.acme.com および newyork.acme.com）をホストするファイアウォールで、以下を実行します。

- **Network**（ネットワーク） > **Interfaces**（インターフェイス） > **Ethernet**（イーサネット）の順に選択して、内部ネットワーク上で IP アドレスを含む Layer 3 Ethernet インターフェイスを設定します。これらを **l3-trust Security Zone**（セキュリティ ゾーン）およびデフォルトの **Virtual Router**（仮想ルーター）に割り当てます。
- 内部 IP アドレス california.acme.com と newyork.acme.com をマッピングする DNS「A」レコードを作成します。
- l3-trust ゾーンのユーザー ID の有効化チェック ボックスをオンにします。

STEP 2 | モバイル エンドポイントで GlobalProtect アプリを使用するエンドユーザーがいる場合、または HIP 対応のセキュリティ ポリシーを使用する場合、ゲートウェイ（内部および外部）をホストする各ファイアウォールの GlobalProtect サブスクリプションを購入してインストールします。



GlobalProtect サブスクリプションを購入してアクティベーション コードを受け取ったら、ゲートウェイをホストするファイアウォールに GlobalProtect サブスクリプションをインストールします：

1. **Device** > **Licenses (**デバイス **>** ライセンス**)**を選択します。
2. **Activate feature using authorization code**（認証コードを使用した機能のアクティベーション）を選択します。
3. **Authorization Code**（認証コード）の入力を促されたら、認証コードを入力して **OK** をクリックします。
4. ライセンスとサブスクリプションが正常にアクティベーションされたことを確認します。

必要なライセンスがない場合は、Palo Alto Networks のセールス エンジニアまたはリセラーにお問い合わせください。ライセンスの詳細は、GlobalProtect ライセンスについてを参照してください。

STEP 3 | GlobalProtect ポータルおよび各 GlobalProtect ゲートウェイのサーバー証明書を取得します。

エンドポイントがポータルに初めて接続する場合、ポータル サーバー証明書の発行に使用されたルート CA 証明書を信頼する必要があります。

ゲートウェイで自己署名証明書を使用し、クライアント設定内のアプリにルート CA 証明書をデプロイします。ベスト プラクティスとして、ポータルをホストするファイアウォールですべての証明書を生成し、ゲートウェイにデプロイします。

推奨されるワークフローは以下のとおりです。

1. ポータルをホストするファイアウォールで、以下を実行します。
   1. 一般的なサードパーティ CA からサーバー証明書をインポートします。
   2. GlobalProtect コンポーネントの自己署名証明書を発行するためのルート CA 証明書を作成します。
   3. ポータルでルート CA を使用して自己署名サーバー証明書を生成します。各ゲートウェイでこの手順を繰り返します。
2. 内部ゲートウェイをホストする各ファイアウォールで、以下を実行します。
   - 自己署名サーバー証明書をデプロイします。

STEP 4 | ポータルおよびゲートウェイに対するユーザーの認証方法を定義します。

証明書プロファイルと認証プロファイルの任意の組み合わせを使用し、ポータルおよびゲートウェイのセキュリティを確保できます。ポータルおよび個々のゲートウェイには、異なる認証スキームを使用することもできます。この手順は、以下のセクションを参照してください。

- 外部認証のセットアップ（認証プロファイル）
- クライアント証明書認証のセットアップ（証明書プロファイル）
- 2 要素認証のセットアップ（トークンまたは OTP ベース）

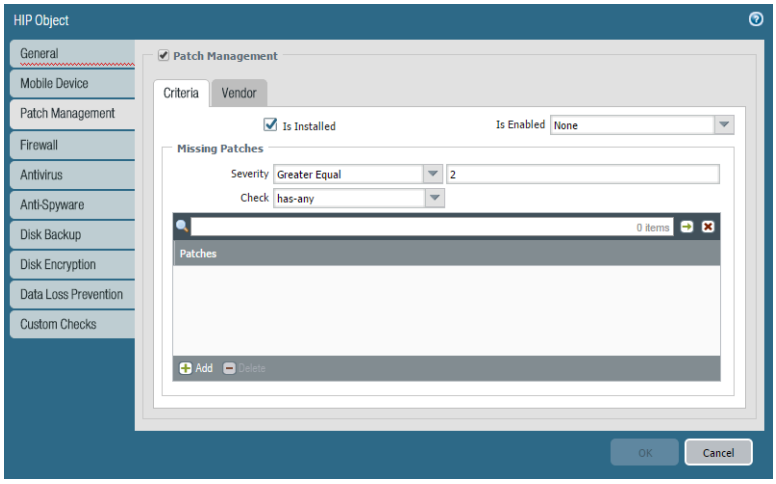
次に、ポータルおよびゲートウェイ設定の証明書プロファイルや認証プロファイルを参照する必要があります。

STEP 5 | ゲートウェイへのアクセスにセキュリティ ポリシーを適用する必要がある HIP プロファイルを作成します。

HIP 照合の詳細は、ホスト情報を参照してください。

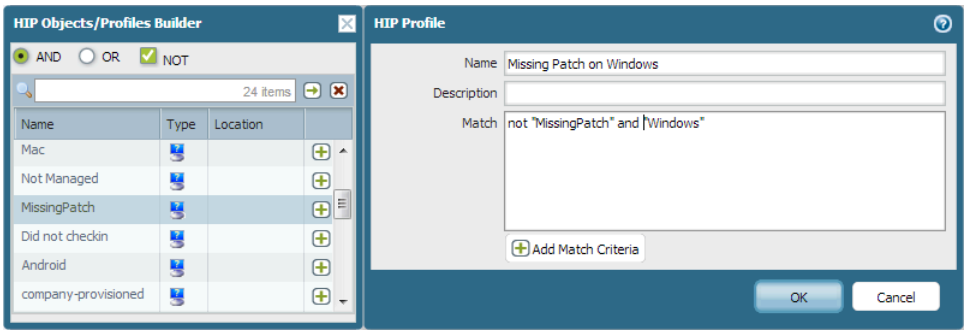
1. アプリが収集した生ホスト データにフィルタをかける HIP オブジェクトを作成します。たとえば、最新の必須パッチが適用されていないユーザーによるアクセスを禁止する場合、パッチ管理ソフトウェアがインストール済みかどうか、および指定された重

大度のすべてのパッチが最新であるかどうかを照合する HIP オブジェクトを作成します。



2. ポリシーで使用する HIP プロファイルを作成します。

   たとえば、最新のパッチが適用された Windows エンドポイントのみが内部アプリケーションにアクセスできるようにするには、欠落しているパッチが存在しないホストを照合する以下の HIP プロファイルを関連付けます。



STEP 6 | 内部ゲートウェイを設定します。

Network（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ）の順に選択し、以下の設定を含むゲートウェイ設定を **Add**（追加）します。

- **interface** インターフェイス
- **IP** アドレス
- サーバー証明書
- **Authentication Profile**（認証プロファイル）/**Configuration Profile**（設定プロファイル）

ゲートウェイ設定ではトンネル接続は不要なため、（HIP 通知をセットアップしない限り）クライアント設定は必要ありません。ゲートウェイ設定の作成手順は、GlobalProtect ゲートウェイの設定を参照してください。

STEP 7 | GlobalProtect ポータルを設定します。

この例では、すべてのアプリケーションにデプロイする単一のクライアント設定を作成する方法を示していますが、さまざまな用途に合わせて別々の設定を作成し、ユーザ/グループ名

やアプリケーションが動作しているエンドポイント オペレーティングシステムをデプロイできます。

Network（ネットワーク） > **GlobalProtect** > **Portals**（ポータル）の順に選択し、以下のポータル設定を **Add**（追加）します。

1. GlobalProtect ポータルへのアクセスのセットアップ：

   Interface（インターフェイス）—**ethernet1/2**

   IP Address（IP アドレス）—**198.51.100.42**

   Server Certificate（サーバー証明書）—**GP-server-cert.pem issued by GoDaddy** で **CN=gp.acme.com**

2. GlobalProtect クライアント認証設定の定義：

   Internal Host Detection（内部ホスト検出）—**enabled**

   Use single sign-on（シングル サインオンの使用）—**enabled**

   Connect Method（接続方式）—**User-logon (Always On)**

   External Gateway Address（外部ゲートウェイ アドレス）—**gpvpn.acme.com**

   Internal Gateway Address（内部ゲートウェイ アドレス）—**california.acme.com, newyork.acme.com**

   User/User Group（ユーザー/ユーザー グループ） — any

3. ポータル設定を **Commit**（コミット）します。

STEP 8 | GlobalProtect アプリ ソフトウェアのデプロイを行います。

Device > **GlobalProtect Client**（**GlobalProtect** クライアント）の順に選択します。

この例では、アプリ更新をポータルでホストする作業を行います。

STEP 9 | 各ゲートウェイでセキュリティ ポリシー ルールを作成し、VPN ユーザーのアプリケーションへのアクセスを安全に有効にします。

- セキュリティ ポリシーを作成し（**Policies**（ポリシー） > **Security**（セキュリティ））、corp-vpn ゾーンと l3-trust ゾーン間のトラフィック フローを有効にします。
- HIP 対応およびユーザー/グループベースのポリシー ルールを作成し、内部データセンター リソースへの詳細なアクセスを有効にします。
- 可視化を実現するため、既知の脅威から保護するデフォルトのセキュリティ プロファイルを使用して、l3-untrust ゾーンへの web-browsing アクセスをすべてのユーザーに許可します。

			Source				Destination					
	Name	Tags	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile
1	CRM access	none	corp-vpn l3-trust	any	Finance	Missing Patch ...	l3-trust	any	sap	application-default	✓	none
2	Eng access	none	corp-vpn l3-trust	any	Engineering	Missing Patch ...	l3-trust	any	bugzilla perforce	application-default	✓	none
3	GP access	none	corp-vpn l3-trust	any	any	any	l3-untrust	any	web-browsing	application-default	✓	

STEP 10 | GlobalProtect の設定を保存します。

ポータルおよびゲートウェイの設定を **Commit**（コミット）します。

ネットワーク アクセス用に GlobalProtect を適用およびキャプティブポータル

大抵の場合、モバイルユーザーは喫茶店、空港、ホテルなどでキャプティブポータルが有効化された Wi-Fi ネットワークに接続します。ユーザーがキャプティブポータルにログインして初めて、インターネットにアクセスできるようになります。ユーザーは、名前およびメールアドレスなどの識別子を使用してブラウザベースのキャプティブポータル ログインページあるいは OS ベースのキャプティブポータル割り当てを介してログインできます。この設定により、ユーザーがキャプティブポータルにログインできる時間を制限することができます。ユーザーが正常にログインしてインターネットを利用できるようになると、GlobalProtect アプリケーションは自動的に接続を確立します。ユーザーが指定された期間内にログインできなければ、すべてのトラフィックがブロックされます。

ネットワークをセキュリティ関連の脅威にさらすリスクをさらに減らすには、ネットワーク アクセスのために GlobalProtect を適用できます。このオプションを有効化すると、アプリが GlobalProtect ゲートウェイに接続されるまでの間、GlobalProtect はすべてのネットワーク トラフィックをブロックします。すべてのトラフィックが VPN トンネルを通じて検査され、ポリシーが適用されるため、ユーザーのトラフィックに対する完全な可視性と制御を確保できます。

キャプティブポータルの存在、およびネットワーク アクセスのために GlobalProtect 接続を求めるかどうかに応じて、ユーザーは特定のワークフローに従ってネットワークにアクセスする必要があります：

キャプティブポータル	ネットワーク アクセスのために **GlobalProtect** を適用	ワークフロー
有り。	有り。	ネットワーク アクセスに GlobalProtect 接続を求め、エンドユーザーがインターネットにアクセスする際にキャプティブポータルへのログインも求める場合、ユーザーは次のステップでネットワークにアクセスする必要があります： **1.** Wi-Fi ネットワークに接続します。 Wi-Fi ネットワークに接続した後、GlobalProtect は自動的にキャプティブポータルを検出します。管理者がキャプティブポータル検出メッセージを設定している場合、ネットワークにアクセスするためにキャプティブポータルにログインする必要があるというメッセージを

キャプティブポータル	ネットワーク アクセスのために **GlobalProtect** を適用	ワークフロー
		GlobalProtect アプリケーションがユーザーに通知します。 管理者はまた、キャプティブポータル検出メッセージを表示するまでの時間を設定することもできます。 **2.** 次のいずれかのオプションを使用してキャプティブポータルにログインします： • ウェブ ブラウザを開いてキャプティブポータル ログインページ経由でログインします。 • エンドポイントのオペレーティングシステム (OS) に組み込まれたネイティブのキャプティブポータル割り当てを使用してログインします。 キャプティブポータルのログインに成功するとインターネットを利用できるようになり、GlobalProtect アプリケーションが自動的に接続されます。アプリが即座に接続されず、管理者がネットワーク アクセスを利用するために GlobalProtect に接続しなければならないことを示すトラフィック ブロックの通知メッセージを設定している場合、接続が確立されるまでの間このメッセージが表示されます。 管理者はまた、トラフィック ブロックの通知を表示するまでの時間を設定することもできます。 キャプティブポータルのログインが失敗し、キャプティブポータルのログインページがタイムアウトする、あるいは GlobalProtect が接続を確立できない場合、ネットワークを使用できなくなります。ポータルのログインを初期化し直し、それによってキャプティブポータルのログイン期間をやり直すためには、GlobalProtect アプリケーションを起動してからアプリの設定 ( ) メニューで **Refresh Connection (接続を更新)** する必要があります。
有り。	無し	エンドユーザーがインターネットを使用するためにキャプティブポータルにログインしなければなないが、ネット

キャプティブポータル	ネットワーク アクセスのために **GlobalProtect** を適用	ワークフロー
		ワーク アクセスで GlobalProtect 接続が不要な場合、ユーザーは次のステップでネットワークにアクセスする必要があります： **1.** Wi-Fi ネットワークに接続します。 Wi-Fi ネットワークに接続した後、GlobalProtect は自動的にキャプティブポータルを検出します。 **2.** 次のいずれかのオプションを使用してキャプティブポータルにログインします： • ウェブ ブラウザを開いてキャプティブポータル ログインページ経由でログインします。 • エンドポイントのオペレーティングシステム (OS) に組み込まれたネイティブのキャプティブポータル割り当てを使用してログインします。 ログインが成功してインターネットを利用できるようになったら、GlobalProtect アプリケーションが自動的に接続されます。
無し	有り。	ネットワーク アクセスに GlobalProtect 接続を求めるものの、エンドユーザーがインターネットにアクセスする際にキャプティブポータルにログインする必要がない場合、ユーザーは Wi-Fi ネットワークに接続する必要があります。Wi-Fi に接続してインターネットを利用できるようになると、GlobalProtect アプリケーションが自動的に接続されます。 アプリが即座に接続されず、管理者がネットワーク アクセスを利用するために GlobalProtect に接続しなければならないことを示すトラフィック ブロックの通知メッセージを設定している場合、接続が確立されるまでの間このメッセージが表示されます。GlobalProtect が接続を確立できない場合、ユーザーがネットワークからブロックされます。接続を解除してから Wi-Fi ネットワークに接続し直し、エンドポイントを再起動するか、GlobalProtect 接続を更新することでネットワークを検出し直す必要があります。

次のステップでキャプティブポータル設定をカスタマイズし、ネットワーク アクセスで GlobalProtect 接続を求めるかどうかを指定します：

常時オンの接続方式とともに *GlobalProtect* を設定する場合のみ、***Enforce GlobalProtect for Network Access*** **(**ネットワーク アクセスのために ***GlobalProtect*** を適用**)** オプションを設定します。

STEP 1 | GlobalProtect ポータルへのアクセスのセットアップ.

STEP 2 | GlobalProtect エージェント設定の定義.

STEP 3 | GlobalProtect アプリのカスタマイズを定義する.

- GlobalProtect 接続を常にオンにするために、**Connect Method (**接続方式**)** を **User-logon (Always On) (**ユーザーログオン (常にオン)**)** に設定します。
- ユーザーがインターネットにアクセスするためにキャプティブポータルにログインする必要がある場合、次のオプションを設定することでキャプティブポータル設定をカスタマイズできます：
  - **Captive Portal Exception Timeout (sec) (**キャプティブポータルの例外タイムアウト **(**秒**))** フィールドに、ユーザーがキャプティブポータルにログインできる時間 (秒単位) を入力します (範囲は 0～3600 秒、デフォルトは 0 秒)。この期間中にユーザーがログインしない場合、キャプティブポータルのログインページがタイムアウトし、ユーザーがネットワークを使用できなくなります。
  - GlobalProtect アプリケーションがキャプティブポータルを検出した場合にユーザーに通知するためには、**Display Captive Portal Detection Message (**キャプティブポータルの検知メッセージの表示**)** を **Yes (**はい**)** に設定します。
    - **Captive Portal Notification Delay (sec) (**キャプティブポータルの通知遅延 **(**秒**))** フィールドに、GlobalProtect アプリケーションがキャプティブポータル検出メッセージを表示するまでの時間 (秒単位) を入力します (範囲は 1～120 秒、デフォルトは 5 秒)。キャプティブポータルが検出された後、しかしインターネットに到達可能になるまでに、GlobalProtect はこのタイマーを開始します。
    - GlobalProtect がキャプティブポータルを検出した際に表示する **Captive Portal Detection Message (**キャプティブポータル検出メッセージ**)** をカスタマイズします。
- すべてのネットワーク トラフィックに GlobalProtect VPN トンネルを経由させるには、次のオプションを設定します：
  - **Enforce GlobalProtect for Network Access (**ネットワーク アクセスのために **GlobalProtect** を適用**)** オプションを **Yes (**はい**)** に設定します。
  - ネットワークにアクセスするために GlobalProtect 接続が必要であることを GlobalProtect アプリケーションがユーザーに通知できるようにするには、**Display Traffic Blocking Notification Message (**トラフィックブロックの通知メッセージの表示**)** を **Yes (**はい**)** に設定します。インターネットに到達可能になった後、GlobalProtect アプリケーションは GlobalProtect 接続が確立される前にこのメッセージを表示します。
    - **Traffic Blocking Notification Delay (sec) (**トラフィック ブロックの通知遅延 **(**秒**))** フィールドに、GlobalProtect アプリケーションがトラフィック ブロックの通知メッセージを表示するまでの時間 (秒単位) を入力します (範囲は 5～120 秒、デフォルトは 15 秒)。インターネットに到達可能になると、GlobalProtect がこのタイマーを開始します。

- ネットワーク アクセスのために GlobalProtect 接続が必要であることを示す **Traffic Blocking Notification Message (**トラフィックブロックの通知メッセージ**)** をカスタマイズします。このメッセージは 512 文字以内でなければなりません。

STEP 4 | 変更を **Commit**（コミット）します。

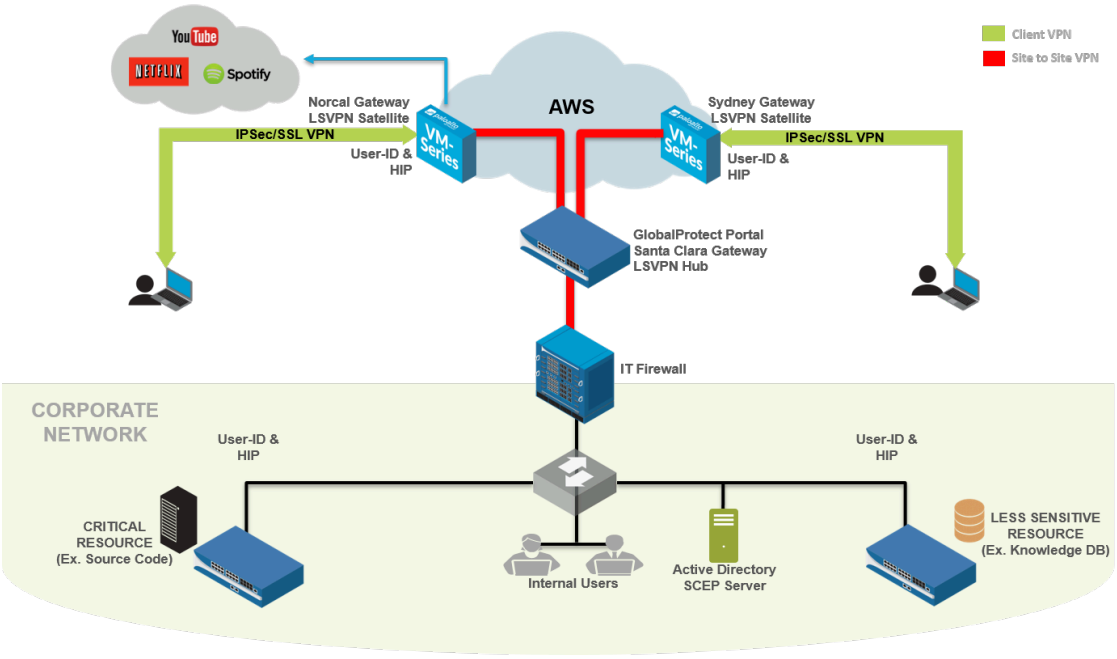
GlobalProtect アーキテクチャ

このセクションでは、インターネット トラフィックや企業リソースへのアクセスを保護する GlobalProtect™ をデプロイする際に役立つ、参照アーキテクチャの例を大まかにご紹介します。

このセクションでご紹介する参照アーキテクチャやガイドラインは、一般的な導入シナリオを想定したものです。このアーキテクチャを応用する前に、企業のセキュリティ、インフラストラクチャの保守性、エンドユーザー体験に係る要件などを決定してから、それらの要件に基づいて GlobalProtect をデプロイしてください。

企業毎に異なる要件もあるでしょうが、このドキュメントとベストプラクティスの設定ガイドラインで大まかにご紹介する一般的な原則や、よくある設計上の留意事項を役立てれば、企業のセキュリティ要件を満たすことができるようになります。

GlobalProtect 参照アーキテクチャのトポロジ



- GlobalProtect Portal（GlobalProtect ポータル）
- GlobalProtect ゲートウェイ

GlobalProtect Portal（GlobalProtect ポータル）

このトポロジでは、コロケーション空間にある PA-3020 が GlobalProtect ポータルとして機能します。

従業員や契約業者は、Active Directory（AD）認証情報およびワンタイムパスワード（OTP）から成る 2 要素認証（2FA）を使用してポータルへの認証を行うことができます。ポータルはユーザーやグループのメンバーシップ、およびオペレーティングシステムに応じて、GlobalProtect クライアントの設定をデプロイします。

小さなグループあるいは試験用のチームに適用されるポータルのクライアント設定を別途設定しておくことで、より多くのユーザーに公開する前に各機能を試験することができます。新しい機能（PAN-OS 7.1 およびその後のコンテンツ更新のもとで利用できる SCEP（Simple Certificate Enrollment Protocol）や Enforce GlobalProtect（GlobalProtect 強制）機能など）を含むクライアント設定は必ず、他のユーザーに提供する前にまずは試験用の構成のもとで有効化され、試験用のユーザーによって確認が行われます。

さらに、GlobalProtect ポータルは設定を GlobalProtect サテライトにプッシュ送信します。この設定には、サテライトが接続してサイト間トンネルを確立できる GlobalProtect ゲートウェイが含まれています。

GlobalProtect ゲートウェイ

コロケーション空間内の PA-3020（前述のもの）は、GlobalProtect ゲートウェイ（Santa Clara Gateway）としても機能します。Amazon Web Services（AWS）および Microsoft Azure パブリック クラウドに、さらに 10 個のゲートウェイがデプロイされています。これらの AWS および Azure ゲートウェイがデプロイされる地域または POP ロケーションは、世界各地の従業員の立地によって異なります。

- **Santa Clara Gateway**—従業員や契約業者は 2FA を使用して Santa Clara Gateway（コロケーション空間内の PA-3020）への認証を行うことができます。ユーザーはこのゲートウェイに対して自身の Active Directory 認証情報および OTP を提供する必要があります。このゲートウェイはセンシティブなリソースを保護しているため、手動専用のゲートウェイとして構成されています。つまり、ユーザーはこのゲートウェイに自動接続されず、手動でこのゲートウェイに接続するよう選択する必要があります。例えば、手動専用のゲートウェイではない AWS-Norcal に接続したユーザーは、機密性の高い内部リソースの一部を利用できません。ユーザーがこれらのリソースにアクセスするためには、後から手動で Santa Clara Gateway に切り替え、認証を行う必要があります。

  また、Santa Clara Gateway は AWS および Azure 内のゲートウェイから行うあらゆるサテライト接続について、Large Scale VPN（LSVPN）トンネルの終端点として構成されています。さらに、Santa Clara Gateway は企業本部にある IT ファイアウォールに向かうインターネット プロトコル セキュリティ（IPSec）トンネルをセットアップするようにも構成されています。これは、企業本部内のリソースにアクセスするために使用するトンネルです。
- **Amazon Web Services** および **Microsoft Azure** 内のゲートウェイ—このゲートウェイは 2Fa（クライアント証明書および Active Directory 認証情報）を求めます。GlobalProtect ポータルは GlobalProtect SCEP 機能を使用し、これらのゲートウェイに認証する際に必要となるクライアント証明書を配布します。

  また、パブリック クラウド内のこれらのゲートウェイは GlobalProtect サテライトとしても機能します。これらは GlobalProtect ポータルと通信を行い、サテライト設定をダウンロードし、Santa Clara Gateway とサイト間トンネルを確立します。GlobalProtect サテライトは、初回はシリアル番号を使って、以降は証明書を使用して認証を行います。
- 企業本部内のゲートウェイ—企業本部内では、3 つのファイアウォールが GlobalProtect ゲートウェイとして機能します。これらは内部的なゲートウェイであり、エンドポイントにトンネルの確立を求めることはありません。ユーザーは Active Directory 認証情報を使用してこれらのゲートウェイへの認証を行います。この内部的なゲートウェイは GlobalProtect を使用して、User-ID を識別し、エンドポイントからホスト情報プロファイル（HIP）を収集します。

これらの内部的なゲートウェイが *SCEP* によって提供される証明書、または *Kerberos* のサービス チケットを使用して認証を行うように設定することで、エンドユーザーにできるだけシームレスな体験を提供できるようになります。

GlobalProtect 参照アーキテクチャの機能

エンド ユーザー体験

エンドユーザーはリモート（企業ネットワーク外）から、AWS または Azure 内のいずれかのゲートウェイに接続します。GlobalProtect ポータルのクライアント設定を構成する際、ゲートウェイに同じ優先度を割り当ててください。この設定では、トンネルのセットアップにエンドポイントで測定された各ゲートウェイの SSL 応答時間によって、ユーザーがどのゲートウェイに接続するかが決まります。

例えば、オーストラリアのユーザーは通常、AWS-Sydney ゲートウェイに接続します。このユーザーが AWS-Sydney に接続されると、GlobalProtect アプリはエンドポイントから AWS-Sydney のファイアウォールに向かうすべてのトラフィックをトンネル内で検査するようになります。GlobalProtect は、インターネットで公開されたサイトに向かうトラフィックについては直接 AWS-Sydney ゲートウェイを通し、企業のリソースに向かうトラフィックについては、AWS-Sydney ゲートウェイと Santa Clara ゲートウェイ間のサイト間トンネルを、次に企業本部への IPsec サイト間トンネルを通してトラフィックを送ります。これは、インターネットにアクセスするユーザーが体験する可能性がある、あらゆる遅延を減らすことを目的としたアーキテクチャです。AWS-Sydney ゲートウェイ（またはシドニー付近のいずれかのゲートウェイ）に到達できない場合、GlobalProtect アプリがインターネット トラフィックを企業本部内のファイアウォールに戻すことで、遅延が生じる場合があります。

Active Directory サーバーは企業ネットワーク内に存在します。リモート ユーザーが認証を行う際、GlobalProtect アプリは AWS/Azure 内から Santa Clara ゲートウェイに向かうサイト間トンネルを通して認証リクエストを送信します。次にこのゲートウェイは、IPsec サイト間トンネルを通して企業本部内の Active Directory サーバーへとリクエストを転送します。

リモートユーザーの認証およびトンネルのセットアップにかかる時間を減らすために、*Active Directory* サーバーを複製し、*AWS* 内で利用できるようにすることを考慮してください。

企業ネットワーク内のエンドユーザーは、ログイン後すぐに 3 つの内部的なゲートウェイへの認証を行います。そして GlobalProtect アプリは、これらの内部的なゲートウェイに HIP レポートを送信します。。そして GlobalProtect アプリは、これらの内部的なゲートウェイに HIP レポートを送信します。企業ネットワーク上のオフィスにいるユーザーは、業務用のリソースにアクセスする際は必ず User-ID および HIP の要件を満たす必要があります。

管理およびロギング

このデプロイ環境では、コロケーション空間に導入されている Panorama からすべてのファイアウォールを管理・構成することができます。

セキュリティの一貫性を保つために、AWS および Azure 内のすべてのファイアウォールが同じセキュリティポリシーと設定を使用する必要があります。ゲートウェイの設定を簡素化するために、Panorama はデバイスグループとテンプレートも 1 つずつ使用します。このデプロイ環境では、すべてのゲートウェイがあらゆるログを Panorama に転送します。これにより、各ファイアウォールにログインする手間を省いて一元的にネットワーク トラフィックの監視や問題のトラブルシューティングを行えるようになります。

ソフトウェア更新が必要になれば、Panorama を使用してソフトウェア更新をすべてのファイアウォールにデプロイすることができます。Panorama はまずファイアウォールを 1 つ、または 2 つアップグレードし、アップグレードが成功したことを確認してから他のファイアウォールを更新します。

監視および高可用性

このデプロイ環境でファイアウォールを監視する際は、サーバー、ネットワーク、およびログを監視するオープンソースのソフトウェアである Nagios を使用できます。定期的にポータルおよびゲートウェイのプレ ログオン ページからの応答を検証し、応答が予期したものでなければアラートを送信するよう、Nagios を設定します。また、GlobalProtect Simple Network Management Protocol（SNMP）の Management Information Base（MIB）オブジェクトを構成してゲートウェイの使用状況を監視することもできます。

このデプロイ環境に存在する GlobalProtect ポータルのインスタンスは 1 つだけです。ポータルが利用できなくなれば、新しいユーザー（ポータルに接続するのが初めてのユーザー）が GlobalProtect に接続することは不可能になります。しかし、既存のユーザーはキャッシュされたポータルのクライアント設定を使用してゲートウェイのいずれかに接続できます。

AWS 内で GlobalProtect ゲートウェイとして構成された仮想マシン（VM）ファイアウォールを複数使用することで、ゲートウェイを冗長化することができます。そのため、ゲートウェイを高可用性（HA）ペアとして構成する必要はありません。

GlobalProtect 参照アーキテクチャの構成

参照アーキテクチャに即したデプロイ環境を構築するために、次の設定のチェックリストを確認してください。

- ゲートウェイ設定
- ポータル設定
- ポリシー設定

ゲートウェイ設定

- スプリット トンネルを無効にします。そのために、**Agent**（エージェント） > **Client Settings**（クライアント設定） > **Split Tunnel**（トンネルの分割）で Access Routes（アクセスルート）が指定されていないことを確認します。「GlobalProtect ゲートウェイの設定」を参照してください。
- **Agent**（エージェント） > **Client Settings**（クライアント設定） > **Split Tunnel**（スプリットトンネル）で **No direct access to local network**（ローカルネットワークへの直接アクセスなし）を有効にします。「GlobalProtect ゲートウェイの設定」を参照してください。
- ゲートウェイが **Accept cookie for authentication override**（**Cookie** による認証オーバーライドを許可）できるようにします。「GlobalProtect ゲートウェイの設定」を参照してください。

ポータル設定

- **Connect Method**（接続方式）を **Always-on (User logon)**（常にオン（ユーザーログオン））に設定します。GlobalProtect アプリのカスタマイズを参照してください。
- **Use Single Sign-On**（シングル サインオンの使用）（Windows のみ）を **Yes**（はい）に設定します。GlobalProtect アプリのカスタマイズを参照してください。
- ポータルが **Save User Credentials**（ユーザー認証情報を保存）するように設定します（値を **Yes**（はい）に設定します）。GlobalProtect エージェント設定の定義を参照してください。
- ポータルが **Accept cookie for authentication override**（**Cookie** による認証オーバーライドを許可）できるようにします。GlobalProtect エージェント設定の定義を参照してください。
- **Cookie Lifetime**（**Cookie** の有効期限）を 20 時間に設定します。GlobalProtect エージェント設定の定義を参照してください。
- ネットワーク アクセスの際に **Enforce GlobalProtect**（必ず **GlobalProtect** を利用）します。GlobalProtect アプリのカスタマイズを参照してください。
- **Enforce GlobalProtect for Network Access**（ネットワーク アクセスの際に必ず **GlobalProtect** を利用する）を有効にする場合は、パスコードを使用して GlobalProtect アプリを無効にすることをユーザーに許可します。GlobalProtect アプリのカスタマイズを参照してください。
- **Internal Host Detection**（内部ホスト検出）を設定します。GlobalProtect エージェント設定の定義を参照してください。

- Data Collection（データ収集）にて**Collect HIP Data**（**HIP** データの収集）オプションを有効にします。GlobalProtect エージェント設定の定義を参照してください。
- SSL 復号化に使用する SSL 転送プロキシ CA 証明書を配布・インストールします。GlobalProtect エージェント設定の定義を参照してください。

ポリシー設定

- すべてのファイアウォールがインターネット ゲートウェイのセキュリティポリシーの推奨設定に基づいてセキュリティポリシーおよびプロファイルを使用するように設定します。この参考用のデプロイ環境の場合、コロケーション空間内の Santa Clara Gateway および AWS/Azure パブリック クラウド内のゲートウェイがこれに含まれます。
- AWS および Azure 内のすべてのゲートウェイのSSL Decryption（SSL 復号化）を有効にします。
- AWS 内のすべてのゲートウェイ用にポリシーベースの転送ルールを設定し、特定のウェブサイトに向かうトラフィックを Santa Clara Gateway を介して転送します。これにより、ユーザーが AWS 内のゲートウェイに接続する際、www.stubhub.com や www.lowes.com など、AWS の IP アドレス範囲からのトラフィックをブロックするサイトであっても確実にアクセスできるようになります。

paloalto TECHDOCS

GlobalProtect 暗号化

GlobalProtect の暗号選択について

GlobalProtect は IPsec と SSL の両方のトンネル モードをサポートしています。GlobalProtect は、GlobalProtect アプリが必ず代替として SSL トンネルに切り替える前に、まず IPsec トンネルのセットアップを試みる機能もサポートしています。IPsec トンネルを使用する場合、GlobalProtect アプリは SSL/TLS を使用して暗号化および認証のアルゴリズムとキーを交換します。GlobalProtect が SSL/TLS トンネルを保護するために使用する暗号スイートは、以下によって選択されます。

- ゲートウェイが受け入れる **SSL/TLS** バージョン—GlobalProtect ポータルおよびゲートウェイは、SSL/TLS プロファイルを使用するアプリで使用できる暗号スイートのリストを制限できます。ファイアウォールで、証明書および許可されるプロトコルのバージョンを指定して SSL/TLS プロファイルを作成し、それを GlobalProtect ポータルおよびゲートウェイに関連付けます。
- ゲートウェイのサーバー証明書のアルゴリズム—エンドポイントのオペレーティング システムによって、GlobalProtect アプリが Client Hello メッセージに含める暗号スイートが決まります。ゲートウェイが優先的に使用する暗号スイートが GlobalProtect アプリに含まれている場合、ゲートウェイは SSL セッションにその暗号スイートを選択します。Client Hello メッセージ内の暗号スイートの順序によって、暗号スイートの選択が変わることはありません。ゲートウェイは、SSL/TLS サービス プロファイル、ゲートウェイ サービス証明書のアルゴリズム、および優先リストに基づいて暗号スイートを選択します。サービス プロファイルは、GlobalProtect ゲートウェイ認証設定から選択します。

GlobalProtect アプリとゲートウェイ間の暗号交換

以下の図は、VPN トンネルを作成するときの GlobalProtect ゲートウェイと GlobalProtect アプリ間の暗号の交換を示しています。

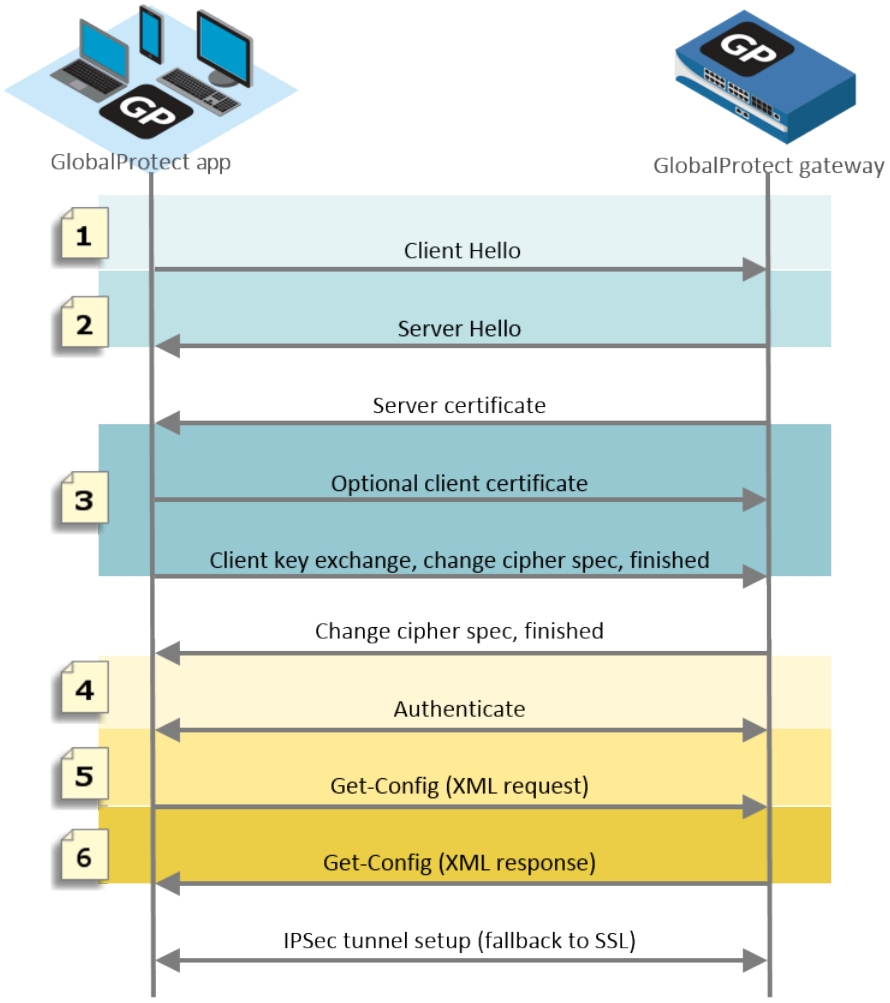


図 **10 :** アプリとゲートウェイ間の暗号交換

各ステージの詳細な説明は、以下の表でご確認いただけます。

表 **9 :** アプリとゲートウェイ間の暗号交換

通信ステージ	説明
1。Client Hello	アプリがエンドポイントの OS に基づいて暗号スイートのリストを提案します。
2.Server Hello	ゲートウェイがアプリから提案された暗号スイートを選択します。トンネルを設定するための暗号を選択する際、ゲートウェイはアプリ

通信ステージ	説明
	から提案された暗号スイートの数や順序を無視し、代わりに、SSL/TLS バージョン、ゲートウェイ サーバーのアルゴリズム、優先リスト（GlobalProtect の暗号選択についてを参照）に基づきます。
3.任意のクライアント証明書	ゲートウェイは必要に応じてユーザーまたはエンドポイントの ID を信頼するためにアプリからのクライアント証明書を要求することもできます。
4.SSL セッション	SSL/TLS セッションを設定した後で、アプリはゲートウェイに認証を行い、ゲートウェイの設定を要求します（Get-Config-Request）。設定を要求するために、アプリは暗号や認証アルゴリズム、さらにトンネル インターフェイスの優先される IP アドレスなどの設定を提案します。ゲートウェイは要求に応答し、GlobalProtect の IPSec 暗号化プロファイルの設定に基づいて、暗号化および認証のアルゴリズムを選択します （Get-Config-Response）。

以下の表に、macOS エンドポイントのアプリとゲートウェイ間の暗号交換の例を示します。

表 **10 :** 例**:macOS** エンドポイントの暗号交換

通信ステージ	例**: macOS** エンドポイント
1。Client Hello	TLS 1.2 37 個の暗号スイート（リファレンス:macOS エンドポイントの GlobalProtect アプリがサポートする TLS 暗号）
2.Server Hello	• GlobalProtect が ECDSA 証明書を使用し、TLS 1.2 が受け入れられる場合、SSL セッションは ECDSA-AES256-CBC-SHA を使用します。 • GlobalProtect が RSA 証明書を使用し、TLS 1.2 が受け入れられる場合、SSL セッションは RSA-AES256-CBC-SHA256 を使用します。
3.任意のクライアント証明書	ECDSA または RSA で署名され、SHA1、SHA256、または SHA384 を使用するクライアント証明書

4.SSL セッション	• SSL セッションは ECDSA-AES256-CBC-SHA または RSA-AES256-CBC-SHA256 を使用します
	• Get-Config-Request
	  • 暗号化—AES-256-GCM、AES-128-GCM、AES-128-CBC
	  • 認証—SHA1 および OS タイプ、優先される IP アドレスなど

通信ステージ	例: **macOS** エンドポイント

	• Get-Config-Response
	  • クライアントからサーバー、およびサーバーからクライアントの SPI、暗号化鍵、認証鍵
	  • トンネル タイプ、ポート、スプリット トンネル モード、IP、DNS など

GlobalProtect 暗号化に関するリファレンス

リファレンス：GlobalProtect アプリの暗号化機能

GlobalProtect アプリは、OpenSSL ライブラリ 1.0.1h を使用して、GlobalProtect ポータルと GlobalProtect ゲートウェイ間の安全な通信を確立します。以下の表に、暗号化機能を必要とする各 GlobalProtect アプリの機能と、GlobalProtect アプリが使用する暗号化キーを示します。

暗号化機能	鍵	使用率
Winhttp（Windows）および NSURLConnection（macOS） aes256-sha	HTTPS 接続を確立するために GlobalProtect アプリと GlobalProtect ポータル/ゲートウェイ間でネゴシエートされるダイナミック キー。	GlobalProtect アプリと GlobalProtect ポータルおよび GlobalProtect ゲートウェイ間で認証用の HTTPS 接続を確立するために使用されます。
OpenSSL aes256-sha	SSL ハンドシェーク中に GlobalProtect アプリと GlobalProtect ゲートウェイ間でネゴシエートされるダイナミック キー。	GlobalProtect アプリと GlobalProtect ゲートウェイ間で HIP レポート送信、SSL トンネル ネゴシエーション、ネットワーク検出用の SSL 接続を確立するために使用されます。
IPSec 暗号化および認証 Aes-128-sha1、aes-128-cbc、aes-128-gcm、および aes-256-gcm	GlobalProtect ゲートウェイから送信されるセッション キー。	GlobalProtect アプリと GlobalProtect ゲートウェイ間で IPSec トンネルを確立するために使用されます。ネットワークでサポートしているもののうち、最も強固なアルゴリズムを使用してください（AES-GCM を推奨）。 データの整合性を確保し、なりすましを防止するためには、SHA1 認証アルゴリズムが aes-128-cbc 暗号化に必要です。AES-GCM 暗号化アルゴリズム（aes-128-gcm および aes-256-gcm）にはネイティブの ESP 整合性保護機能が備わっているため、SHA1 認証アルゴ

暗号化機能	鍵	使用率
		リズムは構成時に必要であっても、暗号に対しては使用されません。

GlobalProtect アプリがサポートする TLS 暗号スイート

さまざまなエンドポイント オペレーティング システムにインストールされた GlobalProtect アプリでサポートされる TLS 暗号の例は、以下のセクションの通りです。これらのリストは、サポートされるすべてのオペレーティングシステムについて網羅されているわけではありません。

- リファレンス：macOS エンドポイントの GlobalProtect エージェントがサポートする TLS 暗号
- リファレンス：Windows 7 エンドポイントの GlobalProtect エージェントがサポートする TLS 暗号
- リファレンス：Android 6.0.1 エンドポイントの GlobalProtect エージェントがサポートする TLS 暗号
- リファレンス：iOS 10.2.1 エンドポイントの GlobalProtect エージェントがサポートする TLS 暗号
- リファレンス：Chromebook の GlobalProtect エージェントがサポートする TLS 暗号

リファレンス：**macOS** エンドポイントの **GlobalProtect** アプリがサポートする **TLS** 暗号

macOS エンドポイントの **GlobalProtect** アプリがサポートする **TLS** 暗号	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)

macOS エンドポイントの GlobalProtect アプリがサポートする TLS 暗号	
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
	TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
	TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)
	TLS_RSA_WITH_RC4_128_MD5 (0x0004)

リファレンス：Windows 7 エンドポイントの GlobalProtect アプリがサポートする TLS 暗号

Windows 7 エンドポイントの GlobalProtect アプリがサポートする TLS 暗号	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Windows 7 エンドポイントの GlobalProtect アプリがサポートする TLS 暗号	
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

リファレンス：Android 6.0.1 エンドポイントの GlobalProtect アプリがサポートする TLS 暗号

Android 6.0.1 向け GlobalProtect アプリは 20 個の暗号スイートをサポートしています。

Android 6.0.1 エンドポイントの GlobalProtect アプリがサポートする TLS 暗号	
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_RC4_128_SHA (0x0005)

Android 6.0.1 エンドポイントの GlobalProtect アプリがサポートする TLS 暗号	
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

リファレンス：iOS 10.2.1 エンドポイントの GlobalProtect アプリがサポートする TLS 暗号

iOS 10.2.1 向け GlobalProtect アプリは 19 個の暗号スイートをサポートしています。

iOS 10.2.1 エンドポイントの GlobalProtect アプリがサポートする TLS 暗号	
TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

リファレンス：Chromebook の GlobalProtect アプリがサポートする TLS 暗号

Chrome OS 55.0.2883 向け GlobalProtect アプリは 91 個の暗号スイートをサポートしています。

Chromebook の GlobalProtect アプリがサポートする TLS 暗号（Chrome OS 55.0.2883）	
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0085)

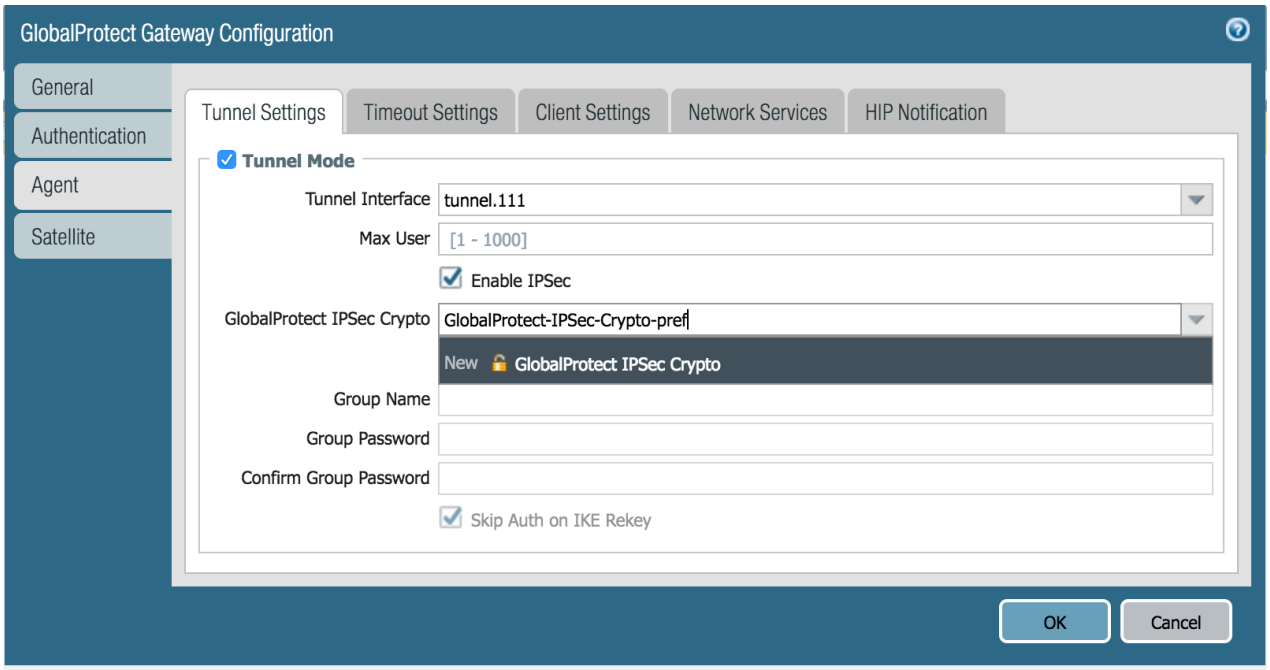
Chromebook の GlobalProtect アプリがサポートする TLS 暗号（Chrome OS 55.0.2883）	
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)	TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
TLS_DH_DSS_WITH_AES_256_GCM_SHA384 (0x00a5)	TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)	TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
TLS_DH_RSA_WITH_AES_256_GCM_SHA384 (0x00a1)	TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0084)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
TLS_DH_RSA_WITH_AES_256_CBC_SHA256 (0x0069)	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
TLS_DH_DSS_WITH_AES_256_CBC_SHA256 (0x0068)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
TLS_DH_RSA_WITH_AES_256_CBC_SHA (0x0037)	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
TLS_DH_DSS_WITH_AES_256_CBC_SHA (0x0036)	TLS_DH_DSS_WITH_AES_128_GCM_SHA256 (0x00a4)
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0088)	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA (0x0087)	TLS_DH_RSA_WITH_AES_128_GCM_SHA256 (0x00a0)

Chromebook の GlobalProtect アプリがサポートする TLS 暗号（Chrome OS 55.0.2883）	
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA (0x0086)	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)	TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)	TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
TLS_DH_RSA_WITH_AES_128_CBC_SHA256 (0x003f)	TLS_RSA_WITH_SEED_CBC_SHA (0x0096)
TLS_DH_DSS_WITH_AES_128_CBC_SHA256 (0x003e)	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0041)
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)	TLS_RSA_WITH_IDEA_CBC_SHA (0x0007)
TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)	TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
TLS_DH_RSA_WITH_AES_128_CBC_SHA (0x0031)	TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (0xc007)
TLS_DH_DSS_WITH_AES_128_CBC_SHA (0x0030)	TLS_ECDH_RSA_WITH_RC4_128_SHA (0xc00c)
TLS_DHE_RSA_WITH_SEED_CBC_SHA (0x009a)	TLS_ECDH_ECDSA_WITH_RC4_128_SHA (0xc002)
TLS_DHE_DSS_WITH_SEED_CBC_SHA (0x0099)	TLS_RSA_WITH_RC4_128_SHA (0x0005)
TLS_DH_RSA_WITH_SEED_CBC_SHA (0x0098)	TLS_RSA_WITH_RC4_128_MD5 (0x0004)
TLS_DH_DSS_WITH_SEED_CBC_SHA (0x0097)	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0045)	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc008)
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0044)	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x0016)
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA (0x0043)	TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA (0x0013)
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA (0x0042)	TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA (0x0010)
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)	TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA (0x000d)
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)	TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA (0xc00d)
	TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA (0xc003)
	TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Chromebook の GlobalProtect アプリがサポートする TLS 暗号（Chrome OS 55.0.2883）	
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)	TLS_DHE_RSA_WITH_DES_CBC_SHA (0x0015)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)	TLS_DHE_DSS_WITH_DES_CBC_SHA (0x0012)
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)	TLS_DH_RSA_WITH_DES_CBC_SHA (0x000f)
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)	TLS_DH_DSS_WITH_DES_CBC_SHA (0x000c)
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)	TLS_RSA_WITH_DES_CBC_SHA (0x0009)
	TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

IPsec トンネルをセットアップするために使用される暗号

GlobalProtect は、GlobalProtect アプリが IPsec トンネル用に使用できる暗号化および認証のアルゴリズムの優先順を制限または設定できます。このアルゴリズムと設定は、GlobalProtect ゲートウェイのトンネルを設定するときに設定する **GlobalProtect IPSec Crypto**（**GlobalProtect IPsec** 暗号化プロファイル）で定義されています**Network**（ネットワーク） > **GlobalProtect** > **Gateways**（ゲートウェイ） > **<gateway-config>** > **GlobalProtect Gateway Configuration**（**GlobalProtect** ゲートウェイ設定） > **Agent**（エージェント） > **Tunnel Settings**（トンネル設定））。



GlobalProtect アプリが GlobalProtect ゲートウェイとの SSL セッションを設定すると、この SSL セッションに使用される暗号スイートは、ゲートウェイで設定された SSL/TLS プロファイル、およびゲートウェイ証明書が使用するアルゴリズムのタイプによって決まります。SSL セッションを確立すると、GlobalProtect アプリは SSL 経由で設定を要求し、VPN トンネルのセットアップを開始します。

同じ SSL セッションを使用して、GlobalProtect ゲートウェイはアプリが IPsec トンネルのセットアップに使用する必要がある暗号化および認証のアルゴリズム、キー、SPI に応答します。

より高いセキュリティ要件がある場合は *AES-GCM* を推奨します。データの整合性を確保し、なりすましを防止するためには、*SHA1* 認証アルゴリズムが *aes-128-cbc* 暗号化に必要です。*AES-GCM* 暗号化アルゴリズム（*aes-128-gcm* および *aes-256-gcm*）にはネイティブの *ESP* 整合性保護機能が備わっているため、*SHA1* 認証アルゴリズムは構成時に必要であっても、暗号に対しては使用されません。

ゲートウェイで設定した **GlobalProtect IPSec Crypto**（**GlobalProtect IPsec** 暗号化プロファイル）によって、IPsec トンネルをセットアップするために使用される暗号化および認証のアルゴリズムが決まります。GlobalProtect ゲートウェイは、アプリの提案に一致するプロファイルに記載された暗号化アルゴリズムの中で最初に一致したアルゴリズムに応答します。

その後、GlobalProtect アプリはゲートウェイからの応答に基づいてトンネルのセットアップを試みます。

SSL API

GlobalProtect は SSL ハンドシェークを実行するために OpenSSL とネイティブ システム API の両方を使用します。GlobalProtect ゲートウェイの待機時間の測定 (GlobalProtect が最適なゲートウェイを選択するために使用)、ゲートウェイのログアウト、HIP チェック メッセージおよびレポートの送信などの操作は、すべて OpenSSL ライブラリを使用してセットアップされた SSL セッションを経由して実行されます。ゲートウェイの pre-login、login、get-config などの操作は、すべてネイティブ システム API を使用してセットアップされた SSL セッションを経由して実行されます。