paloalto TECHDOCS

Prisma Access Browser アクティベーションとオンボーディング

Contact Information

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

About the Documentation

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

Copyright

Last Revised

July 15, 2024

Table of Contents

Prisma Accessエンタープライズ バンドル ライセンスによる新規Prisma Access Browserのアクティベート

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager • Panorama	• 製品のアクティベーション リンク • アクティベーションにはSLS（Strata Logging Service）が必要 • CIE(Cloud Identity Engine)が付属しており、アクティベーション時にスピンアップ • カスタマー サポート ポータル アカウント

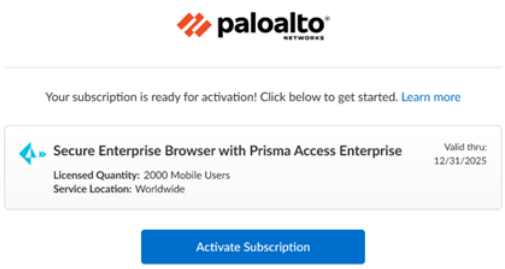
このタスクを開始する前に、前提条件を参照してください。

- クラウド
- Panorama

クラウド マネージドPrisma Access Browserバンドル ライセンス

Palo Alto Networks から、アクティベーションするライセンスを記載したメールが届いたら、アクティベーション リンクを使用してアクティベーション プロセスを開始します。

STEP 1 | メールの**[Activate Subscription (サブスクリプションをアクティベート)]**を選択します。



STEP 2 | Prisma Accessライセンスのアクティベーション、Prisma Access ライセンスの割り当て、およびサービス接続の計画に関する指示に従ってください。

STEP 3 | 引き続きPrisma Access Secure Enterprise Browserライセンスとアドオンを割り当ててください。**[Products (製品)]**または**[Add-ons (アドオン)]**は、契約に基づいてデフォルトで有効になっています。

STEP 4 | **Prisma Access**エンタープライズ対応のセキュア エンタープライズ ブラウザを選択します。

これは、PAモバイル ユーザー ライセンスの割り当てと似ています。Prisma Access Browser複数のPrisma Accessテナントにライセンスを部分的に割り当てて有効化することができます。以下に例を示します。

- 5,000ユニットのPrisma Access Browserエンタープライズ モバイル ユーザーを購入できます。
- 以下を割り当てることができます:
  - PoCテナントに1,000ユニット(これは最低限必要な数量)
  - 実稼働テナントに3,000ユニット
  - 後で使用できるように1,000ユニットを非アクティブのままにする

STEP 5 | Prisma Access Browser管理ガイドにアクセスしてPrisma Access Browserを管理してください。

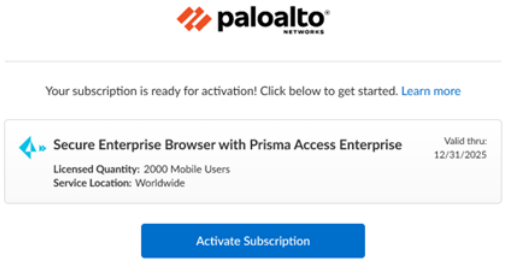
STEP 6 | (オプション) 管理者がPrisma Access Browserを管理できるようにロールを割り当てます。

Panorama管理Prisma Access Browserバンドル ライセンス

Palo Alto Networks からアクティベーションするライセンスを記載したメールが届いたら、アクティベーション リンクを使用してアクティベーション プロセスを開始します。

*Panorama*のマルチテナンシーでは利用できません。

STEP 1 | 電子メールで**[Activate Subscription (サブスクリプションをアクティベート)]**を選択します。



STEP 2 | Prisma Access（Panoramaで管理）ライセンスのアクティベーション手順に従います。

STEP 3 | 引き続き、使用可能なアドオンを有効にします。**[Products (製品)]**または**[Add-ons (アドオン)]**は、契約に基づいてデフォルトで有効になっています。

STEP 4 | **Prisma Access**エンタープライズ対応のセキュア エンタープライズ ブラウザを選択します。

STEP 5 | Panoramaで、**[Panorama]**タブ > **[Cloud Services Plugin (クラウド サービス プラグイン)]** > **Prisma Access Browser**タブに移動します。

これにより、Prisma Access Browser固有のビューのみを持つStrata Cloud Managerの必要最低限の機能を持つバージョンを含む新しいタブが起動します。

STEP 6 | Prisma Access Browser管理者ガイドにアクセスしてPrisma Access Browserを管理してください。

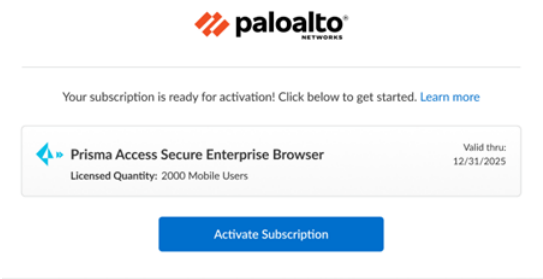
STEP 7 | （任意）管理者がPrisma Access Browserを管理できるようにロールを割り当てます。

スタンドアロンPrisma Access Browserライセンスのアクティベート

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	• 製品のアクティベーション リンク • CIE(Cloud Identity Engine)が付属しており、アクティベーション時にスピンアップ • カスタマー サポート ポータル アカウント

このタスクを開始する前に、前提条件を参照してください。

Palo Alto Networks から、アクティベーションするライセンスを記載したメールが届いたら、アクティベーション リンクを使用してアクティベーション プロセスを開始します。



STEP 1 | メール アドレスでログインします。

- Palo Alto Networksカスタマー サポートのアカウントをお持ちの場合は、アカウント登録時に使用したメール アドレスを入力し、**[Next (次へ)]**を選択してください。
- Palo Alto Networksカスタマー サポートのアカウントをお持ちでない場合は、**[Create a New Account (新規アカウントの作成)]** > **[Password (パスワード)]** > **[Next (次へ)]**を選択してください。

サービスでは、このライセンスに使用するテナントに割り当てられたユーザー アカウントに、このメール アドレスが使用されます。このテナント、およびこのメール アドレスによって作成されたその他のテナントには、スーパーユーザーのロールが付与されます。

STEP 2 | ユーザー名に関連付けられているカスタマー サポート ポータルのアカウントが1つだけの場合、カスタマー サポート アカウントはあらかじめ入力されています。

カスタマー サポート ポータルのアカウントが複数ある場合、他にも想定できる動作があります。

STEP 3 | 選択した受信者に製品を割り当てます。

記載されている名前は、お客様のカスタマー サポート ポータル アカウントと便宜上一致しています。提供された名前を使用することも、変更することもできます。

STEP 4 | 製品をデプロイするデータ取り込みリージョンを選択します。

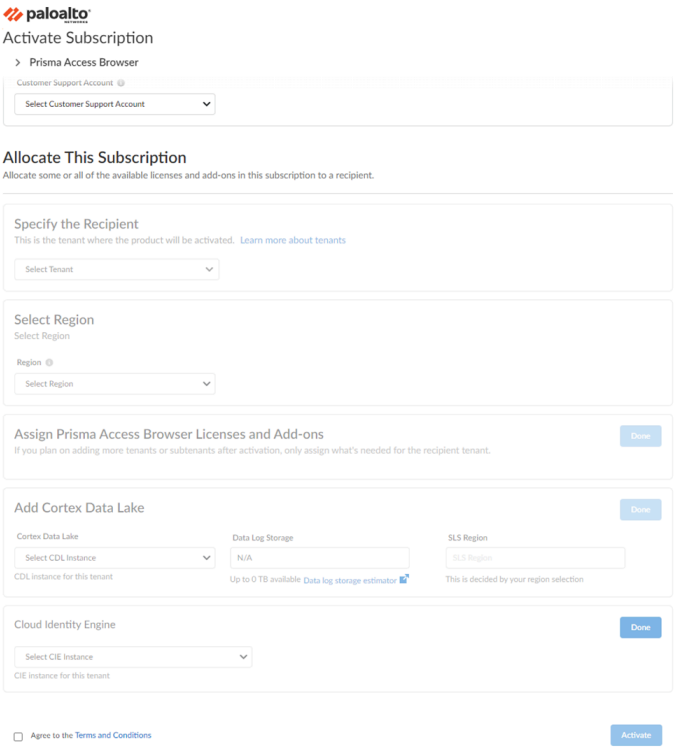
STEP 5 | Prisma Access Secure Enterprise Browserライセンスとアドオンの割り当て

1. **Prisma Access Secure Enterprise Browser**を選択します。
2. これは、PAモバイル ユーザー ライセンスの割り当てと似ています。複数のPrisma Accessテナント間でPrisma Access Browserライセンスを部分的に割り当ててアクティベートできるようになります。以下に例を示します。
   - 1,000ユニットのスタンドアロンPrisma Access Browserを購入できます
   - 以下を割り当てることができます:
     - PoCテナントに200ユニット(これは最低限必要な数量)
     - 実稼働テナントに600ユニット
     - 後で使用できるように200ユニットを非アクティブのままにする

STEP 6 | 設定、テレメトリ ログ、システム ログ、統計などのテナント データを格納するStrata Logging Service(旧称Cortex Data Lake)を追加します。既存のインスタンスを選択するか、新しいインスタンスを作成できます。

STEP 7 | [Cloud Identity Engine]を選択するか、新しいCIEインスタンスを作成して、インフラ全体のすべてのユーザーを識別および検証します。

STEP 8 | 利用規約に同意し、アクティベートします。



STEP 9 | Prisma Access Browser管理者ガイドにアクセスして、Prisma Access Browserを管理します。

STEP 10 | （任意）管理者がPrisma Access Browserを管理できるようにロールを割り当てます。

Strata Cloud Manager上へのPrisma Access Browserのオンボード

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	❑ Prisma Access Browserバンドル ライセンスのPrisma Access ❑ スーパーユーザーまたはPrisma Access Browserロール

このタスクを開始する前に、前提条件を参照してください。

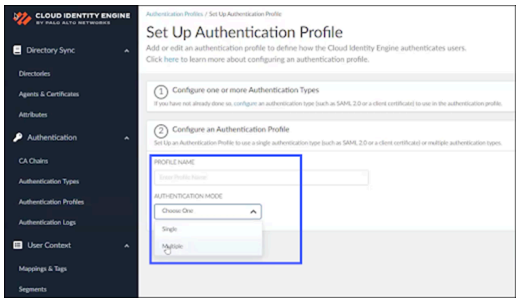
オンボーディング前のタスクの完了

Prisma Access Browserをオンボーディングする前に、いくつかのタスクを実行する必要があります。

STEP 1 | Cloud Identity Engineエンティティを定義します。これは、アクティベーション プロセスで選択したCloud Identity Engineを使用して設定できます。

STEP 2 | 認証プロファイルとオンボーディング プロセスの一部であるユーザー グループが必要です。これらはCloud Identity Engineで設定します。詳細については、認証プロファイルとユーザー グループを参照してください。

認証プロファイルは*1*つだけ持つことができます。複数のアイデンティティ プロバイダ（*IdP*）を使用する場合、プロファイルごとに複数の*IdP*を設定できます。これは、認証プロファイルを設定するときに複数の認証モードを選択することで実行できます。

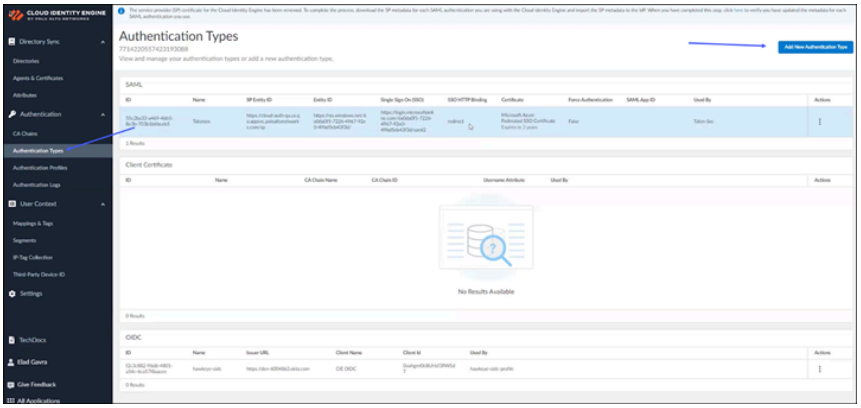


IdP設定の追加

現在のSAML IdPプロバイダを使用して、ネットワーク内の単一のログイン資格情報を管理できます。IdP設定はCloud Identity Engineのコンポーネントであり、そのツール内で管理できます。

STEP 1 | Cloud Identity Engineで、**[Authentication Type (認証タイプ)]**を選択します。

STEP 2 | **[Add New Authentication Type (新しい認証タイプの追加)]**をクリックします。



*IdP*プロバイダーの情報を使用してユーザー グループを作成する際は、有効なメール アドレスを正しく入力する必要があります。*UPN*では不十分です。

STEP 3 | [Set Up Authentication Type (認証の種類のセットアップ)]で、SAML 2.0の**[Set Up (セットアップ)]**をクリックします。

STEP 4 | SAML Authenticatorの設定を続行するには、Cloud Identity Engineの[Configure a SAML 2.0 Authentication Type (SAML 2.0認証タイプの設定)]を参照してください。

STEP 5 | （オプション）Google Workspace 統合を使用します。

Prisma Access Browserのオンボーディング

オンボーディング前の手順を実行したら、Strata Cloud ManagerでPrisma Access Browserをオンボーディングできます。

ユーザーを追加する前に、Strata Cloud ManagerでPrisma Access Browserをアクティベートして設定する必要があります。通常、これはアクティベーション後に1回だけ実行する必要がある1回限りの手順です。ただし、これらのタスクは、変更が必要になった時点でいつでも戻って実行できます。

このプロセスに使用できるウィザードがあり、いつでもグローバル設定を変更できます。ウィザードには、統合の各ステップを完了するための詳細な手順が記載されています。

表示されるコントロールはPrisma Access Browserライセンスによって異なります。Strata Cloud Managerのすべてのオンボーディング機能がすべてのライセンスで使用できるわけではありません。

Strata Cloud Managerから、**[Workflows (ワークフロー)]** > **[Prisma Access Setup (Prisma Accessセットアップ)]** > **[Prisma Access Browser (Prisma Accessブラウザ)]**

ステップ1 - ユーザー

ユーザ認証方式を定義し、ユーザー グループをオンボードします。

STEP 1 | ドロップダウン リストから、ユーザー認証に使用する**CIE**プロファイルを選択します。

STEP 2 | [User groups (ユーザー グループ)]ドロップダウ ンリストから、Prisma Access Browserにアクセスできるユーザー グループを選択します。

STEP 3 | **[Next (次へ):Prisma Access [Integration (統合)]**

ステップ2 - Prisma Accessの統合

STEP 1 | Prisma Accessへの外部接続を可能にします。

1. **[Go to Explicit Proxy settings (明示型プロキシ設定へ移動)]**を選択します。
2. こうすることで、**[Workflows (ワークフロー)]** > **Prisma Access[Setup (セットアップ)** > **[Explicit Proxy (明示型プロキシ])**に移動できます。
3. Prisma Access Browserを有効にします。
4. **Done**（完了）です。

STEP 2 | Prisma Accessセキュリティ ポリシーでPrisma Access Browserを許可します。

1. **[Manage (管理)]** > ［**Prisma Access**］ > ［**Security Policy (セキュリティ ポリシー)**］を選択します。
2. こうすることで、**[Manage (管理)]** > **Prisma Access** > **[Security Policy (セキュリティ ポリシー)]**
3. セキュリティ ポリシーにWebトラフィックを許可するルールを追加します。
4. 設定をプッシュしてルールを受け入れます。
5. **Done**（完了）です。

STEP 3 | サービス接続を作成します。

1. **[Create a service connection (サービス接続を作成)]**を選択します。
2. **[Workflow (ワークフロー)]** > **[Prisma Access Setup (Prisma Accessセットアップ)]** > **[Service Connections (サービス接続の設定]**、**[Add Service Connection (サービス接続の追加)]**に移動します。
3. **Done**（完了）です。
4. 次へ：**[Routing (ルーティング)]**

ステップ3 - ルーティング

ルーティング制御を使用すると、Prisma Access Browserがネットワーク トラフィックを処理する方法を管理できます。この機能は、Prisma Access Browserのデフォルト設定をセットアップします。特定のルールのコントロールの細かさを調整する必要がある場合は、トラフィック フローのブラウザのカスタマイズ制御を参照してください。

STEP 1 | 以下のいずれかのオプションを選択します。

- **Prisma Access**を介してプライベート アプリケーションのトラフィックをルーティングするだけです。
- すべてのトラフィックを**Prisma Access**を介してルーティングします。

STEP 2 | （オプション）ブラウザが内部ネットワーク内で実行されていることを検出したときに、Prisma Access Browserトラフィックが最適な方法で流れるようにします。この識別は、内部ネットワークの内部でのみ使用可能なホストとの接続の確立に基づいています。

- 解決するFQDNを入力します。
- 予想されるIPアドレスを入力します。

STEP 3 | **[Next (次へ):SSO**アプリケーションを適用します。

ステップ4 - SSOアプリケーションの適用

SSO対応アプリケーションでユーザーが認証できる唯一の方法は、Prisma Access Browserを使用する方法であることが重要です。これにより、外部のアクターがエンタープライズ アプリケーションにアクセスできなくなります。IdPを選択するには:

STEP 1 | ［Choose and configure your identity provider (アイデンティティ プロバイダの選択と設定)］で、使用可能なIdPを選択します。オプションは次のとおりです：

- Okta
- Microsoft Azure Active Directory
- PingID
- OneLogin
- VMware workspace ONE Access

STEP 2 | ローカル設定を行う場合は、出口IPアドレスをメモしておいてください。

STEP 3 | 次へ：ダウンロードして配布します。

ステップ5 - ダウンロードと配布

Prisma Access Browserのインストール ファイルをダウンロードして、ユーザーに送信する前に自分のデバイスでテストできます。テストの結果に満足したら、mobile device management (モバイルデバイス管理 - MDM)アプリケーションから配布される関連インストーラーをダウンロードすることができます。

また、ダウンロード リンクをユーザーに送信して、ユーザーが自分でPrisma Access Browserをダウンロードできるようにすることもできます。これはmacOSとWindowsのユーザー専用の単一リンクです。

STEP 1 | 使用可能なオプションから選択します。

- デスクトップ:
  - macOS
  - Windows
- モバイル:
  - iOS
  - Android

ダウンロード リンクをユーザーに送信して、ユーザーが自分でPrisma Access Browserをダウンロードできるようにすることもできます。これはmacOSとWindowsのユーザー専用の単一リンクです。

ダウンロード リンクをユーザーに送信する場合は、ユーザーがログインに使用できるのは*IdP*サービスで設定されている電子メールだけであることをユーザーに思い出させ通知してください。

STEP 2 | **[Next (次へ):Browser Policy (ブラウザ ポリシー)]**

ステップ6 - ブラウザ ポリシー

これで、Prisma Access Browserポリシー エンジンの探索と設定を開始して、安全でセキュアなユーザー環境を構築できます。

STEP 1 | **[Browser Policy (ブラウザ ポリシー)]**を選択します。

STEP 2 | **[Manage (管理)]** > **[Configuration (設定)]** > **Prisma Access[Browser (Prisma Accessブラウザ)]** > **[Policy (ポリシー)** > **[Rules (ルール)]**に移動します。

STEP 3 | Prisma Access Browserポリシー ルールを管理します。

新規ユーザーのオンボード

オンボーディング ワークフローは、新しいエンド ユーザーがブラウザの使用を開始したときに表示される、設定可能な一連のウィンドウです。

ITのニーズと要件に基づいて、エンド ユーザーが自分の写真やブックマークでブラウザをカスタマイズできる最大8つの個別のページを選択でき、ブラウザに関する基本的な情報を見つけることができる、一種の「クイックスタート」ガイドです。

オンボーディング ウィザードのカスタマイズ制御では、オンボーディング ワークフローを設定します。ネットワークに表示するウィンドウを選択できます。

これは、ブラウザ カスタマイズ > **[Onboarding Wizard (オンボーディング ウィザード)]**ときに、**[Manage (管理)]**、**[Configuration (設定)]**、**[Prisma Access Browser (Prisma Accessブラウザ)]**、**[Policy (ポリシー)]**、**[Profiles (プロファイル)]**で設定できます。設定の詳細については、[Onboarding Wizard (オンボーディング ウィザード)]のブラウザのカスタマイズ制御を参照してください。

Prisma Access Browserロールの割り当て

どこで使用できますか?	何が必要ですか?
• Strata Cloud Manager	❑ Prisma Access Browserバンドル ライセンスまたはPrisma Access Browserスタンドアロン ライセンスを持つPrisma Access ❑ ロール：カスタマー サポート ポータルにアクセスできるマルチテナント スーパーユーザーまたはスーパーユーザー

Prisma Access Browserのさまざまなタイプの管理者に対してロールベースのアクセス制御を作成および管理することができます。これにより、大規模な組織のメイン管理者は、可視性とアクセスを含めた特定のロールに関連する権限を持つ追加の管理者を任命できます。

ライセンス認証後、管理者ユーザー アクセスを管理し、Prisma Access Browser固有の以下のロールのいずれかを割り当てることができます:

エンタープライズ ロール	許可	サポートされるアプリケーション
PAブラウザへのアクセス権およびデータ管理者	アクセスとデータ ポリシーの設定と管理、カスタムまたはプライベート アプリケーションの定義、ポリシーに関連するエンド ユーザーの要求の処理、およびPrisma Access Browser管理セクション内のインベントリの側面ト(ユーザー、デバイス、拡張機能)と可視性の側面(ダッシュボード、エンドユーザー イベント)に対する読み取り専用アクセス	• Prisma Access Browser
PAブラウザのカスタマイズ管理者	ブラウザのカスタマイズ ポリシーを設定および管理するための読み取り/書き込みアクセス権と、Prisma Access Browser管理セクション内のインベントリの側面（ユーザー、デバイス、アプリケーション、拡張機能）および可視性の側面（ダッシュボード、エンドユーザー イベント）に対する読み取り専用アクセス。	• Prisma Access Browser

エンタープライズ ロール	許可	サポートされるアプリケーション
PAブラウザ権限要求管理者	ポリシーに関連するエンド ユーザーの要求を処理する読み取り/書き込みアクセス権と、Prisma Access Browserの管理セクション内の可視性の側面（ダッシュボード、エンドユーザー イベント）に対する読み取り専用アクセス。	• Prisma Access Browser
PAブラウザのセキュリティ管理者	ブラウザのセキュリティ ポリシーを設定および管理するための読み取り/書き込みアクセス権と、Prisma Access Browser管理セクション内のインベントリの側面（ユーザー、デバイス、アプリケーション、拡張機能）および可視性の側面（ダッシュボード、エンドユーザー イベント）に対する読み取り専用アクセス権。	• Prisma Access Browser
PAブラウザのセキュリティとデバイス ポスチャ管理者	ブラウザのセキュリティ ポリシーの設定と管理、デバイス ポスチャ グループの管理、サインイン ルールの設定を行う読み取り/書き込みアクセス。また、インベントリの側面（ユーザー、アプリケーション、拡張機能）と、Prisma Access Browserの管理セクション内の可視性の側面（ダッシュボード、エンドユーザー イベント）に対する読み取り専用の権限も提供します。	• Prisma Access Browser
PAブラウザ ビューのみの分析	Prisma Access Browserの管理セクション内の可視性の側面（ダッシュボード、詳細なエンド ユーザー イベント、インベントリの側面（ユーザー、デバイス、アプリケーション、拡張機能）など）への読み取りアクセス。	• Prisma Access Browser