paloalto TECHDOCS

AI Access Security 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

April 16, 2026

Table of Contents

AI Access Securityライセンス

利用可能なAI Access Securityライセンスを確認して、ネットワーク上の生成AIアプリケーションへの安全な導入とアクセス制御を開始します。

- **AI Access Security**ライセンス

  AI Access Securityライセンスはスタンドアロン ライセンスです。これには、以下の3種類のライセンスが含まれます。

  - **AI Access Security EVAL**—AI Access Securityの評価版ライセンス。EVALライセンスを有効にしている場合は、生成AIアプリケーションへのアクセスを安全に制御し、安全に採用し続けるために、評価期間終了後に評価版ライセンスを本番ライセンスに変換する必要があります。
  - **AI Access Security LAB**—ラボ環境固有のAI Access Securityライセンス。このライセンスは実稼働環境向けではありません。
  - **AI Access Security**—AI Access Securityの本番ライセンス。
- **CASB-PA**および**CASB-X**

  AI Access Securityは、CASB-PAライセンスとCASB-Xライセンスの両方にデフォルトで含まれています。AI Access Securityをアクティベートするための追加アクションは必要ありません。これらのライセンスのいずれかをアクティブ化した後、AI Access Securityを使用して生成AIアプリケーションを安全に導入することができます。
- **Prisma Access Browser** スタンドアロン ライセンス

  AI Access Securityは、デフォルトでPrisma Access Browserスタンドアロン ライセンスに含まれています。AI Access Securityをアクティベーションするための追加アクションは必要ありません。このライセンスをアクティベートした後、AI Access Securityを使用して生成AIアプリケーションの安全な導入を開始することができます。

AI Access Securityライセンスには何が含まれますか?

AI Access Securityに含まれるものは、テナントで他のライセンスがアクティブかどうかによって異なります。

含まれているAI Access Security機能は、NGFWまたはPrisma Accessテナントで現在実行されているPAN-OSまたはデータプレーンのバージョンによって異なります。含まれている機能の詳細については、セットアップの前提条件を参照してください。

- **AI Access Security**のみ

  これは、AI Access Securityライセンスのみがアクティブな場合に、PanoramaまたはStrata Cloud Managerによって管理されるNGFWまたはPrisma Accessに適用されます。

PAN-OSまたはデータプレーンのバージョン	NGFWおよびPrisma Access(PanoramaまたはStrata Cloud Managerにより管理)
11.2.2-h1以降 Prisma Access5.1 Innovation以降	• 動的コンテンツ更新とApp-IDクラウドエンジン(ACE)を通じて提供される2,250を超える生成AI)アプリケーションの可視性。 • 生成AIアプリケーションと生成AI以外のアプリケーションへのアクセスを制御するポリシー ルールを定義します。 • サポートされている生成AIアプリケーションのみのEnterprise DLP検査と判定レンダリング。 機密データを含むトラフィックの一致は、非生成AIアプリケーションの検査と判定レンダリングのためにEnterprise DLPに転送されません。 • 生成AIの可視性のためにStrata Cloud Manager Command Centerにアクセスします。 • AI Access Securityアクティビティに関するインサイト ダッシュボードにアクセスして、詳細な生成AIアプリケーションの使用状況データ、ユーザー、およびネットワークで発生した一般的な生成AIユースケースを表示します。 • Strata Cloud Manager上の生成AIアプリケーションにタグを付けて、アプリケーションが組織内で承認されているかどうか、およびタグベースのポリシー適用を反映します。 AI Access Securityは生成AIアプリケーションのタグをPanoramaと同期しません。 • 検出された生成AIアプリケーションのみのレポートを生成します。 • アプリケーション ディクショナリで生成AIアプリケーションを表示して、SaaSアプリケーションの基盤となる特定の生成AIアプリケーション、ベンダー、コンプライアンス、およびリスク特性の詳細を確認してください。

PAN-OSまたはデータプレーンのバージョン	NGFWおよびPrisma Access(PanoramaまたはStrata Cloud Managerにより管理)
	• 7つのSaaSマーケットプレース アプリケーションにサードパーティ接続アプリケーション/プラグインとしてインストールされた生成AIアプリケーションを表示します。 • ChatGPTエンタープライズ アプリケーションに存在する保存データの可視性と制御。

- **AI Access Security**および**Enterprise DLP**ライセンス

  これは、AI Access SecurityライセンスとEnterprise DLPライセンスの両方がアクティブな場合に、PanoramaまたはStrata Cloud Managerによって管理されるNGFWまたはPrisma Accessに適用されます。

PAN-OSまたはデータプレーンのバージョン	NGFWおよびPrisma Access(PanoramaまたはStrata Cloud Managerにより管理)
11.2.2-h1以降 Prisma Access5.1 Innovation以降	• 動的コンテンツ更新とApp-IDクラウドエンジン(ACE)を通じて提供される2,250を超える生成AI)アプリケーションの可視性。 • 生成AIアプリケーションと生成AI以外のアプリケーションへのアクセスを制御するポリシー ルールを定義します。 • サポートされている生成AIおよび非生成AIアプリケーションのEnterprise DLP検査と判定レンダリング。 • 生成AIの可視性のためにStrata Cloud Manager Command Centerにアクセスします。 • AI Access Securityアクティビティに関するインサイト ダッシュボードにアクセスして、詳細な生成AIアプリケーションの使用状況データ、ユーザー、およびネットワークで発生した一般的な生成AIユースケースを表示します。 • Strata Cloud Manager上の生成AIアプリケーションにタグを付けて、アプリケーションが組織内で承認されているかどうか、およびタグベースのポリシー適用を反映します。 AI Access Securityは生成AIアプリケーションのタグをPanoramaと同期しません。 • 検出された生成AIアプリケーションのみのレポートを生成します。 • アプリケーション ディクショナリで生成AIアプリケーションを表示して、SaaSアプリケーションの基盤となる特定の生成AIアプリケーション、ベンダー、コンプライアンス、およびリスク特性の詳細を確認してください。

PAN-OSまたはデータプレーンのバージョン	NGFWおよびPrisma Access(PanoramaまたはStrata Cloud Managerにより管理)
	• 7つのSaaSマーケットプレース アプリケーションにサードパーティ接続アプリケーション/プラグインとしてインストールされた生成AIアプリケーションを表示します。 • ChatGPTエンタープライズ アプリケーションに存在する保存データの可視性と制御。

- **CASB-PA**および**CASB-X**ライセンス

  これは、CASB-PAまたはCASB-Xライセンスがアクティブなときに Strata Cloud Managerによって管理されるNGFWまたはPrisma Accessに適用されます。

PAN-OSまたはデータプレーンのバージョン	CASB-PAおよびCASB-X

10.2
11.1
Prisma Access 5.0 PreferredおよびInnovation以降
Prisma Access 5.1 Preferred以降
	• 動的コンテンツ更新とApp-IDクラウドエンジン(ACE)を通じて提供される2,250を超える生成AI)アプリケーションの可視性。
	• 生成AIアプリケーションと生成AI以外のアプリケーションへのアクセスを制御するポリシー ルールを定義します。
	• サポートされている生成AIおよび非生成AIアプリケーションのEnterprise DLP検査と判定レンダリング。
	• 生成AIの可視性のためにStrata Cloud Manager Command Centerにアクセスします。
	• AI Access Securityアクティビティに関するインサイト ダッシュボードにアクセスして、詳細な生成AIアプリケーションの使用状況データ、ユーザー、およびネットワークで発生した一般的な生成AIユースケースを表示します。
	• 生成AIアプリを含むすべてのSaaSインライン アプリについては、以下を参照してください。
	  • ダッシュボード
	  • ユーザー
	  • アプリケーション ディクショナリ
	  • アプリケーション
	  • レポート
	  • ポリシー推奨
	• 生成AIプラグインを含むすべてのサードパーティ プラグイン(SSPM)を表示します。

PAN-OSまたはデータプレーンのバージョン	CASB-PAおよびCASB-X
	• 生成AIアプリケーションを含む、許可されたすべてのSaaSアプリケーション(保存データ)のアセットの詳細を表示します。

11.2.2-h1以降
Prisma Access 5.1 Innovation以降
	• 動的コンテンツ更新とApp-IDクラウドエンジン(ACE)を通じて提供される2,250を超える生成AI)アプリケーションの可視性。
	• 生成AIアプリケーションと生成AI以外のアプリケーションへのアクセスを制御するポリシー ルールを定義します。
	• サポートされている生成AIおよび非生成AIアプリケーションのEnterprise DLP検査と判定レンダリング。
	• 生成AIの可視性のためにStrata Cloud Manager Command Centerにアクセスします。
	• AI Access Securityアクティビティに関するインサイト ダッシュボードにアクセスして、詳細な生成AIアプリケーションの使用状況データ、ユーザー、およびネットワークで発生した一般的な生成AIユースケースを表示します。
	• Strata Cloud Manager上の生成AIアプリケーションにタグを付けて、アプリケーションが組織内で承認されているかどうか、およびタグベースのポリシー適用を反映します。
	AI Access Securityは生成AIアプリケーションのタグをPanoramaと同期しません。
	• 生成AIアプリを含むすべてのSaaSインライン アプリについては、以下を参照してください。
	  • ダッシュボード
	  • ユーザー
	  • アプリケーション ディクショナリ
	  • アプリケーション
	  • レポート
	  • ポリシー推奨
	• 生成AIプラグインを含むすべてのサードパーティ プラグイン(SSPM)を表示します。
	• 生成AIアプリケーションを含む、許可されたすべてのSaaSアプリケーション(保存データ)のアセットの詳細を表示します。

AI Access Securityセットアップの前提条件

AI Access Securityを使用するための前提条件を確認します。前提条件は、PAN-OSとPrisma Accessデータプレーンの最小バージョン、およびAI Access Securityを使用するために必要な追加サービスについて説明しています。

AI Access Securityがサポートする機能の詳細については、さまざまなAI Access Securityライセンスと PAN-OSバージョンの組み合わせを確認してください。

- **NGFW**および**Prisma Access(Panorama**により管理)

  PanoramaからAI Access Security設定を管理する場合は、**AI Access Security**ライセンスの前提条件を参照し、AI Access Securityライセンスのみをアクティブにしてください。

  PanoramaからAI Access Security設定を管理する場合は、**CASB-PA**およびライセンス**CASB-X**の前提条件を参照し、CASB-PAまたはCASB-Xライセンスがアクティブであることを確認してください。

前提条件	AI Access Securityライセンス	CASB-PAおよびCASB-Xライセンス
PAN-OSまたはデータプレーン	PAN-OS11.2.2-h1	• PAN-OS10.2.3およびPrisma Access5.0のPreferredおよびInnovation • PAN-OS11.1.0およびPrisma Access5.1 Preferred • PAN-OS11.2.2-h1およびPrisma Access5.1のInnovation Prisma Accessリリース ノートで、最低限必要なPrisma Accessバージョンの詳細を確認します。
データのフィルタリング	Enterprise DLPプラグイン5.0.4以降	お使いのPAN-OSバージョンでサポートされているEnterprise DLPプラグインのバージョンについては、互換性マトリックスを参照してください。

前提条件	AI Access Securityライセンス	CASB-PAおよびCASB-Xライセンス
	AI Access Securityには、AI Access Security、CASB-PA、およびCASB-Xライセンスをアクティベートしたときのライセンスが含まれます。	
管理	Strata Cloud Manager Essentials または Strata Cloud Manager Pro 各ライセンスの内容についての詳細を読む。	該当なし
クラウドサービスプラグイン	クラウド サービス プラグイン5.1	
ロギング	Strata Logging Service	

- **NGFWおよびPrisma Access(Strata Cloud Managerにより管理)**

  Strata Cloud ManagerからAI Access Security設定を管理する場合は、**AI Access Security**ライセンスの前提条件を参照し、AI Access Securityライセンスのみをアクティブにしてください。

  Strata Cloud ManagerからAI Access Security設定を管理する場合は、**CASB-PA**およびライセンス**CASB-X**の前提条件を参照し、CASB-PAまたはCASB-Xライセンスがアクティブであることを確認してください。

前提条件	AI Access Securityライセンス	CASB-PAおよびCASB-Xライセンス
PAN-OSまたはデータプレーン	PAN-OS11.2.2-h1	• PAN-OS10.2.3およびPrisma Access5.0のPreferredおよびInnovation • PAN-OS11.1.0およびPrisma Access5.1 Preferred • PAN-OS11.2.2-h1およびPrisma Access5.1のInnovation Prisma Accessリリース ノートで、最低限必要なPrisma Accessバージョンの詳細を確認します。

前提条件	AI Access Securityライセンス	CASB-PAおよびCASB-Xライセンス
データのフィルタリング	AI Access Securityには、AI Access Security、CASB-PA、およびCASB-Xライセンスをアクティベートしたときの Enterprise DLPが含まれます。	
管理	Strata Cloud Manager Essentials または Strata Cloud Manager Pro 各ライセンスの内容についての詳細を読む。	該当なし
ロギング	Strata Logging Service	

AI Access Securityライセンスのアクティベーション

AI Access Securityライセンスをアクティベートして、あなたの組織が従業員が有効化する生成AIアプリケーションを安全に採用できるようにします。AI Access Securityのアクティベーションは、AI Access Securityライセンスの購入後、Palo Alto Networksが提供するマジックリンクを使用して行われます。これらの手順は、アクティベーションに必要なすべてのライセンス認証コードとマジックリンクをすでに持っていることを前提としています。

AI Access Securityライセンスを購入した後、Palo Alto Networksから送信されたマジックリンクを使用してライセンスをアクティベートする必要があります。AI Access Securityは、CASB-PAまたはCASB-Xライセンスをアクティベートする際に含まれています。CASB-PAまたはCASB-Xライセンスを有効にした後、AI Access Securityを有効にするために追加のアクションは必要ありません。

- 新しいデプロイメント
- 既存のデプロイメント

AI Access Securityライセンスをアクティブ化する(新しいデプロイメント)

STEP 1 | NGFW用に初期設定をインストールして実行します。

これには、必要なすべてのサポート ライセンスのアクティブ化が含まれます。

STEP 2 | NGFWまたはPrisma Accessテナントの管理をセットアップします。

- **NGFW (Managed by Panorama)**
  1. Panoramaをセットアップします。
     - **M-Series**アプライアンス—管理のみまたはPanoramaモードでM-Seriesアプライアンスをセットアップします。
     - **Panorama**仮想アプライアンス—Panorama仮想アプライアンスをお好みのハイパーバイザーに管理のみまたはパノラマモードで

       インストールします。
  2. Strata Logging Serviceをデプロイします。
  3. Panoramaを登録します。
  4. サポート ライセンスをアクティベートしますPanorama。
  5. Panoramaデバイス管理ライセンスをアクティベートします(M-Seruesアプライアンスまたはパノラマバーチャル アプライアンス)。
  6. マネージドファイアウォールをPanorama管理に追加します。
  7. PanoramaをAI Access Securityに対応した最小PAN-OSバージョンにアップグレードします 。
  8. NGFWをAI Access Securityに対応した最小PAN-OSバージョンにアップグレードします。
- **NGFW (Managed by Strata Cloud Manager)**
  1. Strata Logging Serviceをデプロイします。

     Strata Cloud Managerはロギングに Strata Logging Serviceを必要とします。
  2. Strata Cloud Manager EssentialsまたはStrata Cloud Manager Proライセンスをアクティベートします。
  3. NGFWをStrata Cloud Managerにオンボードします。
  4. 最新の動的コンテンツ更新をインストールし、NGFWをAI Access Securityに対応した最小PAN-OSバージョンにアップグレードします。
- **Prisma Access (Managed by Panorama)**
  1. Panoramaをセットアップします。
     - **M-Series**アプライアンス—管理のみまたはPanoramaモードでM-Seriesアプライアンスをセットアップします。
     - **Panorama**仮想アプライアンス—Panorama仮想アプライアンスをお好みのハイパーバイザーに管理のみまたはパノラマモードで

       インストールします。
  2. Strata Logging Serviceをデプロイします。
  3. Panoramaを登録します。
  4. Panoramaサポートライセンスをアクティベートします。

5. Panoramaデバイス管理ライセンスをアクティベートします(M-Seruesアプライアンスまたはは Panoramaバーチャル アプライアンス)。
6. PanoramaをAI Access Securityに対応した最小PAN-OSバージョンにアップグレードします 。
7. Cloud ServicesプラグインをPanoramaにインストールします。
8. Panorama Managed Prisma Accessをセットアップします。

- **Prisma Access (Managed by Strata Cloud Manager)**

1. Strata Logging Serviceをデプロイします。

   Strata Cloud ManagerはロギングにStrata Logging Serviceを必要とします。
2. Prisma Accessライセンスを Strata Cloud Managerでアクティベートします。
3. Prisma Accessをセットアップします。

STEP 3 | Enterprise Data Loss Prevention (E-DLP)をセットアップします。

- **NGFW (Managed by Panorama)**

1. Enterprise DLPプラグインをPanoramaにインストールします。
2. Enterprise DLPをNGFW用に有効化します。
3. 必要に応じてEnterprise DLPクラウドコンテンツ、データ フィルタリング、およびスニペット設定を編集します。

- **NGFW (Managed by Strata Cloud Manager)**

1. Enterprise DLPをNGFW用に有効化します。
2. 必要に応じてEnterprise DLPデータ フィルタリングおよびスニペット設定を編集します。

- **Prisma Access (Managed by Panorama)**

1. Enterprise DLPプラグインをPanoramaにインストールします。
2. Enterprise DLPをPrisma Access用に有効化します。
3. 必要に応じてEnterprise DLPクラウドコンテンツ、データ フィルタリング、およびスニペット設定を編集します。

- **Prisma Access (Managed by Strata Cloud Manager)**

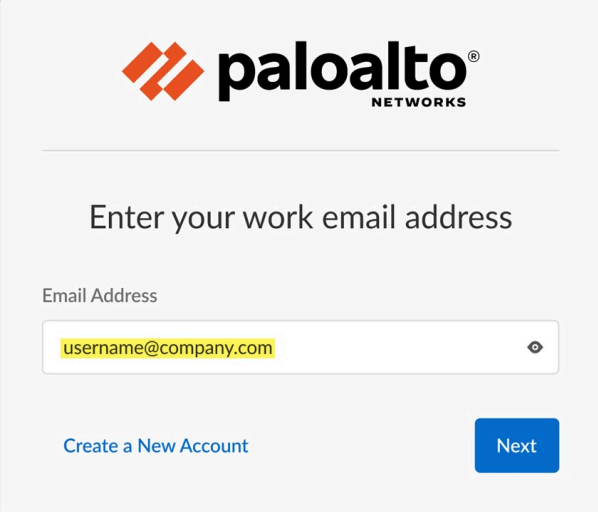
1. Enterprise DLPをNGFW用に有効化します。
2. 必要に応じてEnterprise DLPデータ フィルタリングおよびスニペット設定を編集します。

STEP 4 | AI Access Securityサブスクリプションの購入時にPalo Alto Networksから提供されたマジックリンクをクリックしてください。

STEP 5 | **[Activate Subscription(サブスクリプションをアクティベート)]**をクリックして、AI Access Securityのアクティベートを開始します。

STEP 6 | お使いのPalo Alto Networksカスタマーサポートポータル(CSP)メールアドレスを入力してください。このメールアドレスは、AI Access Securityをアクティベートするためのマジックリンクを受け取ったメールアドレスと一致する必要があります。

AI Access Securityのアクティベーション リンクを受け取ったメールアドレスが有効なCSPアカウントを持っていない場合、新しいアカウントを作成してください。新しく作成されたアカウントは、自動的にAI Access Securityをアクティベートするための同じテナントに関連付けられ、マルチテナントスーパーユーザーのロールが割り当てられます。



STEP 7 | (マルチテナンシーのみ)カスタマー サポート アカウント セクションで、AI Access Securityライセンスをアクティベートするテナントに関連付けられたPalo Alto Networksカスタマー サポート アカウントを選択します。

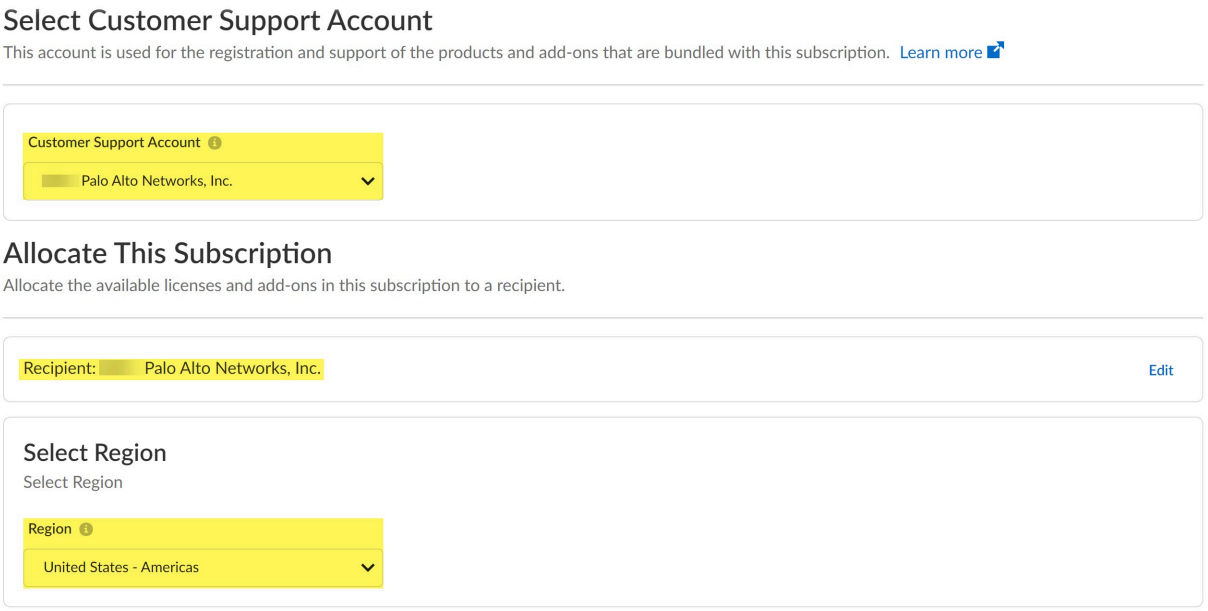
単一テナントのカスタマー サポート ポータル アカウントがある場合は、このステップをスキップしてください。あなたのカスタマー サポート アカウントはデフォルトで選択されています。

STEP 8 | (マルチテナンシーのみ) **[Allocate This Subscription(**このサブスクリプションを割り当てる**)]**セクションで、AI Access Securityをアクティベートしたいテナント サービス グループ(TSG)を選択します。親テナントまたは子テナントを選択できます。

AI Access Securityは選択されたテナントのみに対してアクティベートされます。親テナントを選択した場合、AI Access Securityは子テナントにはアクティベートされません。

単一テナントのカスタマー サポート ポータル アカウントしかない場合は、このステップをスキップしてください。デフォルトで選択されています。

STEP 9 | テナントリージョンを確認してください。このリージョンは、展開されたNGFWまたはPrisma Accessテナントリージョンに基づいて事前に入力されており、変更できません。

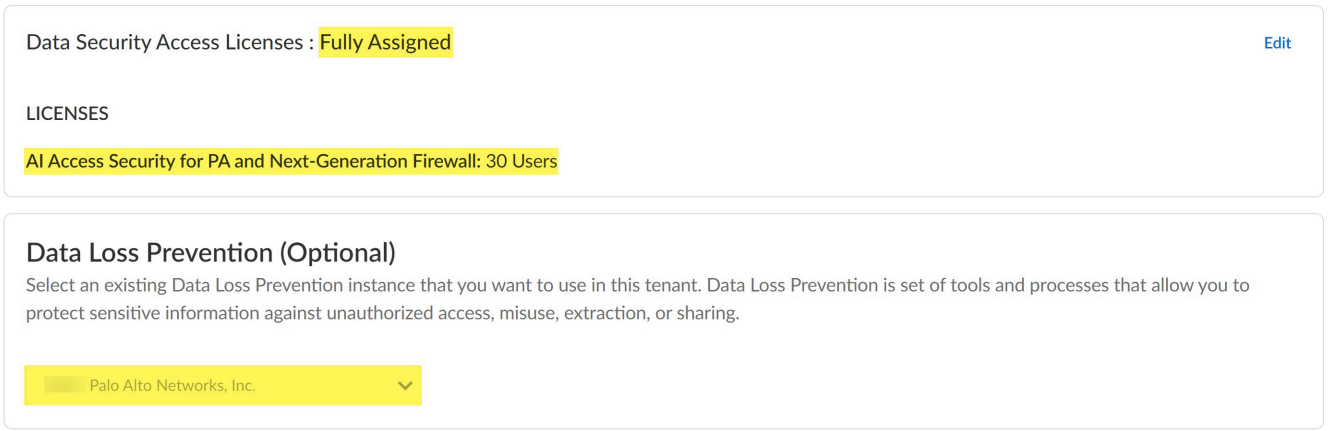


STEP 10 | **[Assign Licenses (**ライセンスを割り当てる**)]**セクションで、[完了]をクリックして、すべてのAI Access Securityライセンスを割り当てます。お使いの**AI**アクセス セキュリティ ライセンスが完全に割り当てられていることを確認してください。

STEP 11 | テナントでEnterprise Data Loss Prevention (E-DLP)がアクティブな場合、データ損失防止**(DLP)**インスタンスが選択されていることを確認してください。

Enterprise DLPインスタンスは、すでにテナントでアクティブな場合、デフォルトで選択されます。

Enterprise DLPがすでにアクティブでない場合は、このステップをスキップしてください。Enterprise DLPはAI Access Securityを有効にするために必要ありません。Enterprise DLPインスタンスがすでにアクティブでない場合、ライセンスのアクティベーションの一部として1つが作成されます。AI Access Securityライセンスを更新しない場合、Enterprise DLPに何が起こるかを確認してください。

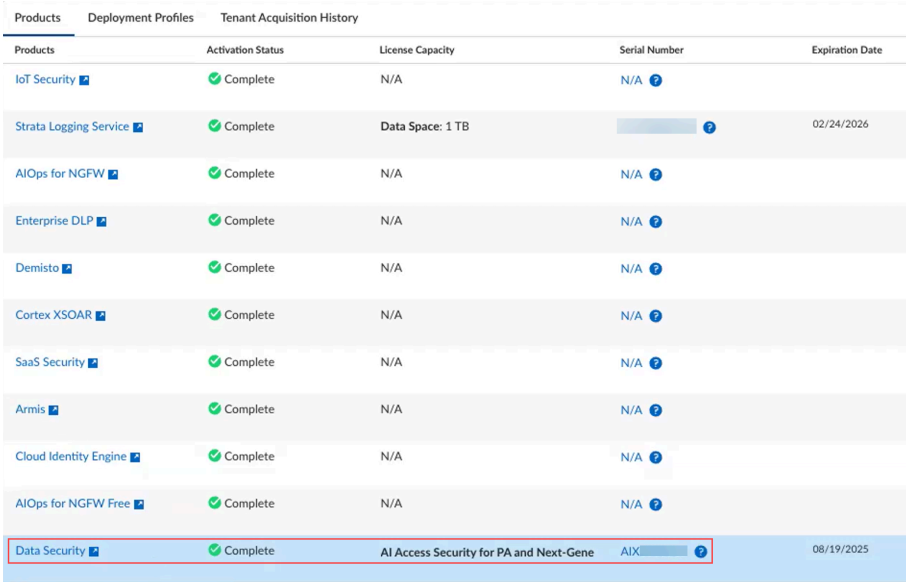


STEP 12 | 利用規約に同意します。

STEP 13 | アクティベートします。

[Tenant Maangement(テナント管理)]ページにリダイレクトされ、AI Access Security [アクティベーション状態]が初期設定中になります。

AI Access Securityライセンスはデータセキュリティとして表示され、シリアル番号はAIXで始まります。アクティベーション状態が完了になった後、次のステップに進んでください。



STEP 14 | (NGFWのみ) AI Access SecurityライセンスをNGFWに関連付けます。

AI Access Securityライセンスの関連付け、お使いのNGFWのライセンスをアクティベートするために必要です。

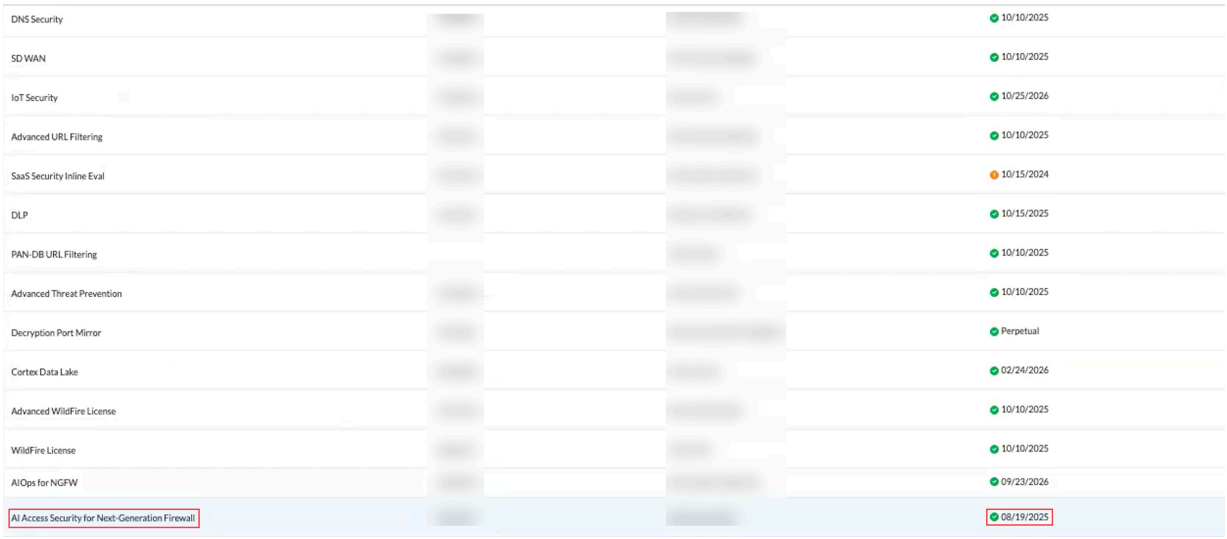
1. Strata Cloud Managerメニューで、[設定] > [デバイス アソシエーション]を選択します。

   Strata Cloud ManagerメニューはStrata Cloud Managerの左下隅にあります。
2. Strata Cloud Managerメニューで、[システム設定] > [デバイス アソシエーション]を選択します。

   Strata Cloud ManagerメニューはStrata Cloud Managerの左下隅にあります。
3. アプリを関連付けます。
4. [Licensed Products(ライセンス製品)]で、[データセキュリティ]を選択します。
5. AI Access Securityをアクティベートしたいを選択します。
6. **Save**（保存）を選択します。

STEP 15 | AI Access Securityを正常にアクティベートしたことを確認してください。

1. Palo Alto Networksカスタマー サポート ポータル(CSP)にログインします。
2. [製品] > [アセット]を選択します。
3. AI Access Securityをアクティベートした適用ポイントに基づいて**NGFW**または**Prisma Access**テナントを選択します。
4. フィルターを使用して、お使いのNGFWまたはPrisma Accessテナントを見つけます。
5. アクティブなライセンスのリストを展開するか、**[Licenses & Subscriptions(**ライセンスとサブスクリプション**)]**をクリックします。
6. AI Access Securityライセンスがアクティブであることを確認します。



STEP 16 | AI Access Securityを開始する

AI Access Securityライセンスのアクティベーション(既存のデプロイメント)

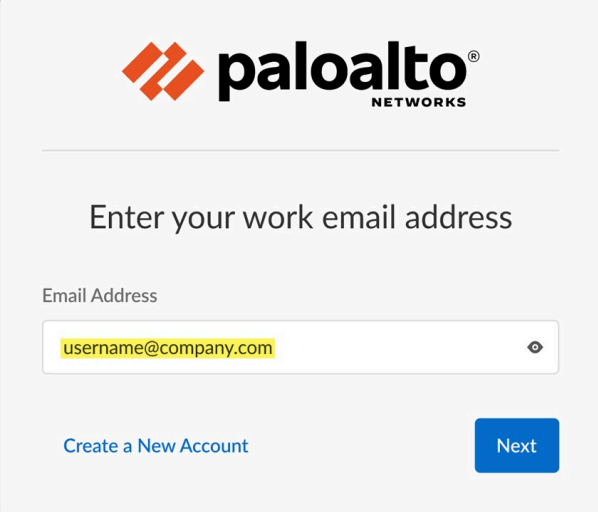
この手順では、AI Access Securityライセンスをアクティベートするだけで、前提条件となるすべてのライセンスがアクティベートされ、必要に応じてNGFW、Prisma Access、Panorama™ management server、およびStrata Cloud Managerが正常にセットアップされていることを前提としています。

STEP 1 | AI Access Securityサブスクリプションの購入時にPalo Alto Networksから提供されたマジックリンクをクリックしてください。

STEP 2 | **[Activate Subscription(サブスクリプションをアクティベート)]**をクリックして、AI Access Securityのアクティベートを開始します。

STEP 3 | お使いのPalo Alto Networksカスタマーサポートポータル(CSP)メールアドレスを入力してください。このメールアドレスは、AI Access Securityをアクティベートするためのマジックリンクを受け取ったメールアドレスと一致する必要があります。

AI Access Securityのアクティベーション リンクを受け取ったメールアドレスが有効なCSPアカウントを持っていない場合、新しいアカウントを作成してください。新しく作成されたアカウントは、自動的にAI Access Securityをアクティベートするための同じテナントに関連付けられ、マルチテナントスーパーユーザーのロールが割り当てられます。



STEP 4 | (マルチテナンシーのみ)カスタマー サポート アカウント セクションで、AI Access Securityライセンスをアクティベートするテナントに関連付けられたPalo Alto Networksカスタマー サポート アカウントを選択します。

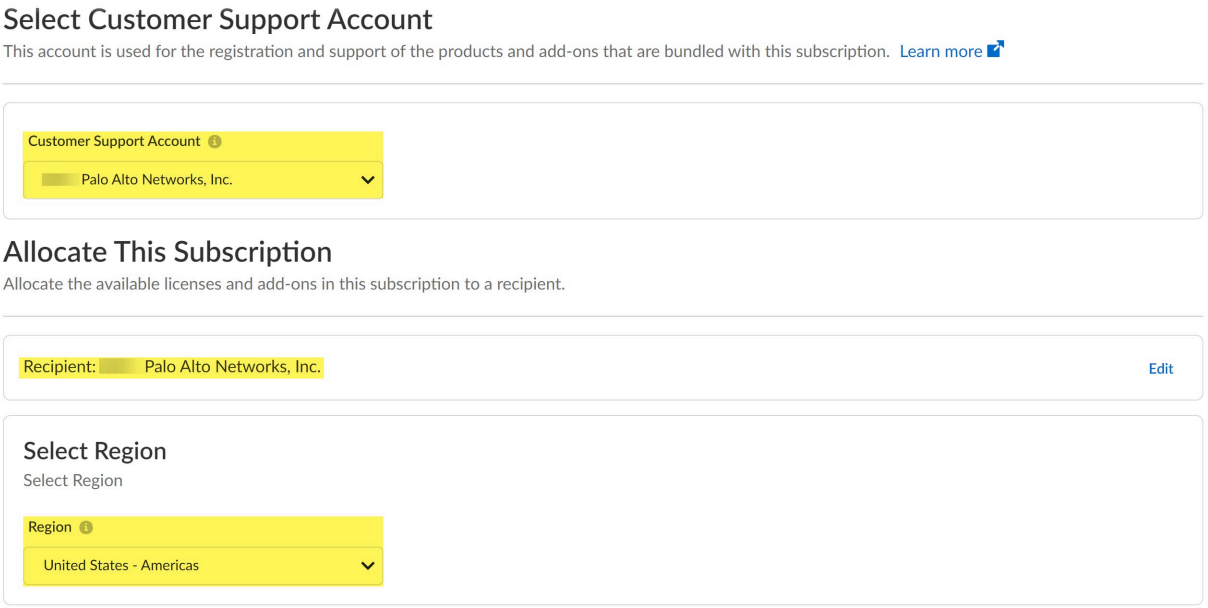
単一テナントのカスタマー サポート ポータル アカウントがある場合は、このステップをスキップしてください。あなたのカスタマー サポート アカウントはデフォルトで選択されています。

STEP 5 | (マルチテナンシーのみ) **[Allocate This Subscription(**このサブスクリプションを割り当てる**)]**セクションで、AI Access Securityをアクティベートしたいテナント サービス グループ(TSG)を選択します。親テナントまたは子テナントを選択できます。

AI Access Securityは選択されたテナントのみに対してアクティベートされます。親テナントを選択した場合、AI Access Securityは子テナントにはアクティベートされません。

単一テナントのカスタマー サポート ポータル アカウントしかない場合は、このステップをスキップしてください。デフォルトで選択されています。

STEP 6 | テナントリージョンを確認してください。このリージョンは、展開されたNGFWまたはPrisma Accessテナントリージョンに基づいて事前に入力されており、変更できません。



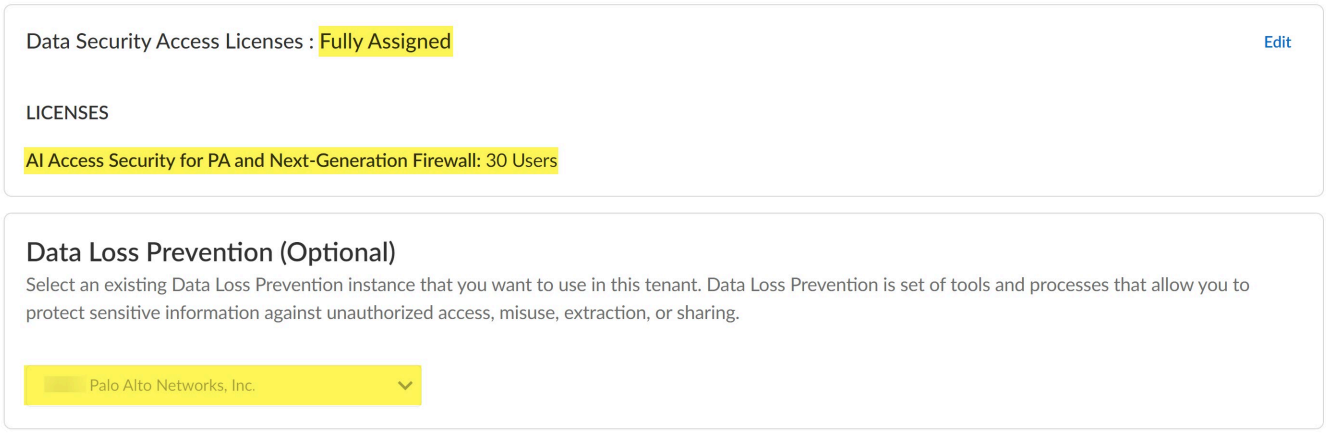
STEP 7 | **[Assign Licenses (**ライセンスを割り当てる**)]**セクションで、[完了]をクリックして、すべてのAI Access Securityライセンスを割り当てます。**AI**アクセス セキュリティ ライセンスが完全に割り当て済みであることを確認する

STEP 8 | テナントでEnterprise Data Loss Prevention (E-DLP)がアクティブな場合、データ損失防止**(DLP)**インスタンスが選択されていることを確認してください。

Enterprise DLPインスタンスは、すでにテナントでアクティブな場合、デフォルトで選択されます。

Enterprise DLPがすでにアクティブでない場合は、このステップをスキップしてください。Enterprise DLPはAI Access Securityを有効にするために必要ありません。Enterprise DLPインスタンスがすでにアクティブでない場合、ライセンスのアクティベーションの一

部として1つが作成されます。AI Access Securityライセンスを更新しない場合、Enterprise DLPに何が起こるかを確認してください。

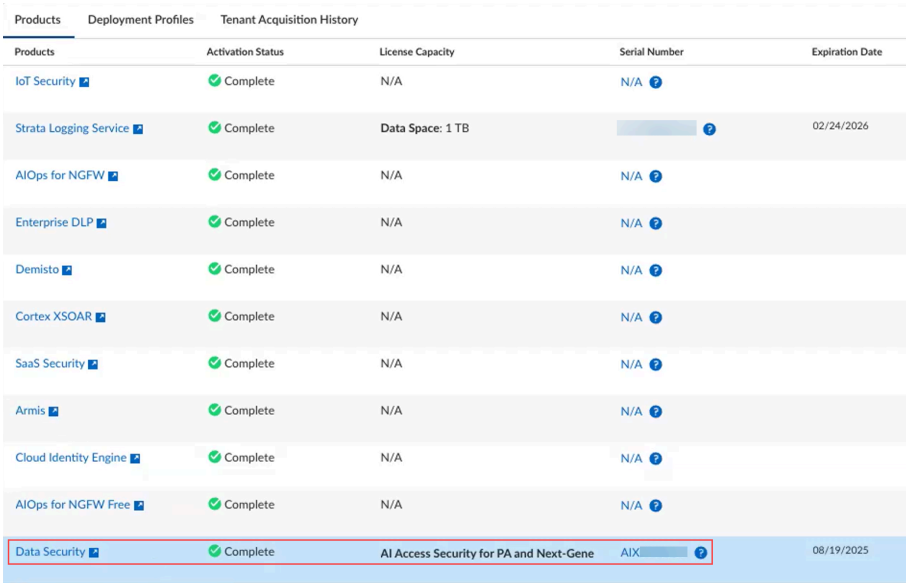


STEP 9 | 利用規約に同意します。

STEP 10 | アクティベートします。

[Tenant Maangement(テナント管理)]ページにリダイレクトされ、AI Access Security [アクティベーション状態]が初期設定中になります。

AI Access Securityライセンスはデータセキュリティとして表示され、シリアル番号はAIXで始まります。アクティベーション状態が完了になった後、次のステップに進んでください。



STEP 11 | (NGFWのみ) AI Access SecurityライセンスをNGFWに関連付けます。

AI Access Securityライセンスの関連付け、お使いのNGFWのライセンスをアクティベートするために必要です。

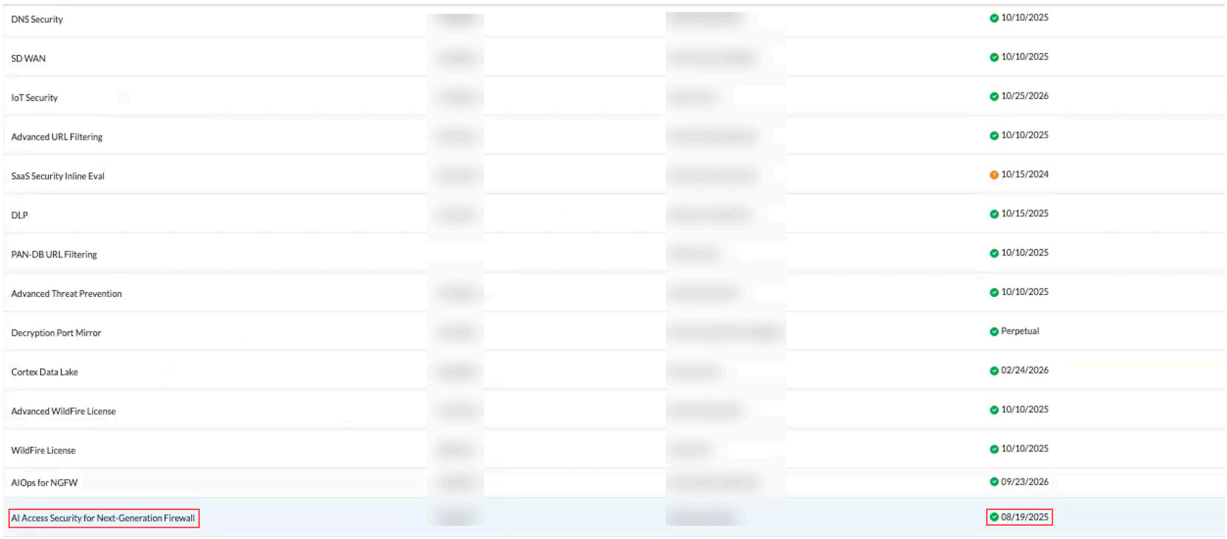
1. Strata Cloud Managerメニューで、[設定] > [デバイス アソシエーション]を選択します。

   Strata Cloud ManagerメニューはStrata Cloud Managerの左下隅にあります。
2. Strata Cloud Managerメニューで、[システム設定] > [デバイス アソシエーション]を選択します。

   Strata Cloud ManagerメニューはStrata Cloud Managerの左下隅にあります。
3. アプリを関連付けます。
4. [Licensed Products(ライセンス製品)]で、[データセキュリティ]を選択します。
5. AI Access SecurityをアクティベートしたいNGFWを選択します。
6. **Save**（保存）を選択します。

STEP 12 | AI Access Securityを正常にアクティベートしたことを確認してください。

1. Palo Alto Networksカスタマー サポート ポータル(CSP)にログインします。
2. [製品] > [アセット]を選択します。
3. AI Access Securityをアクティベートした適用ポイントに基づいて**NGFW**または**Prisma Access**テナントを選択します。
4. フィルターを使用して、お使いのNGFWまたはPrisma Accessテナントを見つけます。
5. アクティブなライセンスのリストを展開するか、**[Licenses & Subscriptions(**ライセンスとサブスクリプション**)]**をクリックします。
6. AI Access Securityライセンスがアクティブであることを確認します。



STEP 13 | AI Access Securityを開始する

評価版ライセンスを製品ライセンスに変換する

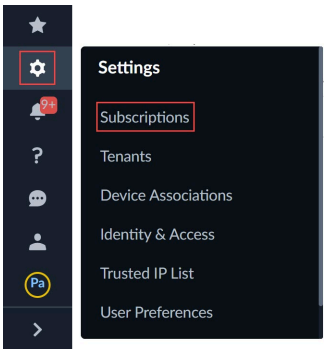
AI Access SecurityEVALライセンスが有効な場合、評価期間終了後も生成AIアプリへのアクセスと採用を安全に制御し続けるには、評価版ライセンスを製品ライセンスに変換する必要があります。評価版ライセンスを製品ライセンスに変換しない場合:

- 機密データを含むトラフィックは、検査および判定レンダリングのためにEnterprise Data Loss Prevention (E-DLP)に転送されなくなります。
- Enterprise DLPにアクセスできなくなりました。
  - **Panorama™ management server**—オブジェクト > **DLP**
  - **Strata Cloud Manager**—管理設定データ損失防止**(DLP)**
- AI Access Security用に作成されたWebセキュリティおよびセキュリティ ポリシー ルールは保持されます。

STEP 1 | Strata Cloud Managerにログインします。

STEP 2 | Strata Cloud Managerメニューで、[設定] > [サブスクリプション]を選択します。

Strata Cloud ManagerメニューはStrata Cloud Managerの左下隅にあります。



STEP 3 | [システム設定] > [サブスクリプション]を選択します。

STEP 4 | AI Access Security評価版ライセンスを見つけ、[アクション] > **[Eval to Prod Request(**評価版から製品版へのリクエスト**)]**を選択します。

STEP 5 | テナントに使用する製品ライセンス条件を指定します。要求は、Palo Alto Networksアカウント担当者によって確認され、見積もりが作成されます。

製品ライセンス要求に次の情報を指定します。

- ライセンス数—AI Access Securityを使用できる個人の数。
- 期間—AI Access Securityサブスクリプションの長さ。

STEP 6 | 要求を送信します。

AI Access Securityライセンスの更新

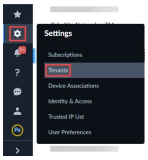
生成AIアプリを安全に採用し続けるために、有効期限が切れるAI Access Securityライセンスを更新できます。有効期限が切れるAI Access Securityは自動更新されず、手動で更新する必要があります。AI Access Securityの有効期限が切れた場合:

- 機密データを含むトラフィックは、検査および判定レンダリングのためにEnterprise Data Loss Prevention (E-DLP)に転送されなくなります。
- Enterprise DLPにアクセスできなくなりました。
  - **Panorama™ management server**—オブジェクト > **DLP**
  - **Strata Cloud Manager**—管理設定データ損失防止**(DLP)**
- AI Access Security用に作成されたWebセキュリティおよびセキュリティ ポリシー ルールは保持されます。

STEP 1 | Palo Alto Networksの販売担当者に連絡し、AI Access Securityライセンスの更新をリクエストしてください。

STEP 2 | Strata Cloud Managerにログインします。

STEP 3 | 左下のメニューから、[設定] > [テナント]を選択します。



STEP 4 | [システム設定] > [テナント]を選択します。

STEP 5 | AI Access Securityライセンスを更新するテナントを選択します。

親テナントまたは子テナントを選択できます。ライセンス更新に即時対応が必要な許可を受けたテナントは、青丸で示されます。

STEP 6 | テナントライセンスを編集します。

STEP 7 | 利用規約に同意し、今すぐアクティベートします。