paloalto
TECHDOCS

AI Access Security Activation et intégration

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

April 16, 2026

Table of Contents

Licences AI Access Security

Passez en revue les licences AI Access Security disponibles pour commencer à adopter et contrôler en toute sécurité les applications d'IA générative (GenAI) sur votre réseau.

- **Licence AI Access Security**

  La licence AI Access Security est une licence autonome. Elle comprend les trois types de licence suivants :

  - **AI Access Security EVAL** : licence d'évaluation pour AI Access Security. Si vous possédez une licence EVAL active, vous devez convertir la licence d'évaluation en licence de production après la fin de la période d'évaluation pour continuer à contrôler en toute sécurité l'accès aux applications GenAI et à les adopter.
  - **AI Access Security LAB** : licence AI Access Security spécifique à vos environnements de laboratoire. Cette licence n'est pas destinée à un environnement de production.
  - **AI Access Security** : licence de production pour AI Access Security.
- **CASB-PA et CASB-X**

  AI Access Security est inclus par défaut avec les licences CASB-PA et CASB-X. Aucune action supplémentaire n'est nécessaire pour activer AI Access Security. Vous pouvez commencer à utiliser AI Access Security pour adopter en toute sécurité les applications GenAI après avoir activé l'une de ces licences.
- **Prisma Access Browser** **Licence autonome**

  AI Access Security est inclus par défaut avec la licence Prisma Access Browser autonome. Aucune action supplémentaire n'est nécessaire pour activer AI Access Security. Vous pouvez commencer à utiliser AI Access Security pour adopter en toute sécurité les applications GenAI après avoir activé cette licence.

Qu’est-ce qui est inclus avec une licence AI Access Security ?

Les éléments inclus avec AI Access Security dépendent de la présence d’autres licences actives sur le locataire.

La fonctionnalité de AI Access Security incluse dépend de la version de PAN-OS ou du plan de données actuellement exécutée sur le locataire NGFW ou Prisma Access. Reportez-vous aux Prérequis pour la configuration pour plus d’informations sur les fonctionnalités incluses.

- **AI Access Security uniquement**

  Cela s’applique aux NGFW ou à Prisma Access gérés par Panorama ou Strata Cloud Manager lorsque seule la licence AI Access Security est active.

Version PAN-OS ou du plan de données	NGFW et Prisma Access (gérés par Panorama ou Strata Cloud Manager)
11.2.2-h1 et versions ultérieures Prisma Access 5.1 Innovation et versions ultérieures	• Visibilité sur plus de 2 250 applications GenAI fournies par les mises à jour du contenu dynamique et App-ID Cloud Engine (ACE). • Définissez des règles de politique pour contrôler l’accès aux applications GenAI et aux applications non GenAI. • Inspection Enterprise DLP et rendu des verdicts pour les applications GenAI prises en charge uniquement. Les correspondances de trafic contenant des données sensibles ne sont pas transmises à Enterprise DLP pour inspection et rendu du verdict pour les applications non GenAI. • Accédez à Strata Cloud Manager Command Center pour obtenir une visibilité GenAI. • Accédez au tableau de bord AI Access Security Activity Insights (Informations sur l’activité) pour afficher des données détaillées sur l’utilisation de l’application GenAI, les utilisateurs et les cas d’utilisation courants de GenAI survenant sur votre réseau. • Étiquetez les applications GenAI sur Strata Cloud Manager pour indiquer si l’application est approuvée au sein de votre organisation et pour l’application de politiques basées sur les étiquettes. AI Access Security ne synchronise pas les étiquettes des applications GenAI avec Panorama. • Générez des rapports uniquement pour les applications GenAI découvertes. • Affichez les applications GenAI dans le Dictionnaire des applications pour en savoir plus sur les applications GenAI spécifiques, les fournisseurs, la conformité et les caractéristiques de risque qui sous-tendent ces applications SaaS.

Version PAN-OS ou du plan de données	NGFW et Prisma Access (gérés par Panorama ou Strata Cloud Manager)
	• Affichez les applications GenAI installées en tant qu'applications/plug-ins tiers connectés dans 7 applications SaaS Marketplace. • Visibilité et contrôle des données au repos résidant dans l'application ChatGPT Enterprise.

- **Licences AI Access Security et Enterprise DLP**

  S'applique aux NGFW ou à Prisma Access gérés par Panorama ou Strata Cloud Manager lorsque les licences AI Access Security et Enterprise DLP sont actives.

Version PAN-OS ou du plan de données	NGFW et Prisma Access (gérés par Panorama ou Strata Cloud Manager)
11.2.2-h1 et versions ultérieures Prisma Access 5.1 Innovation et versions ultérieures	• Visibilité sur plus de 2 250 applications GenAI fournies par les mises à jour du contenu dynamique et App-ID Cloud Engine (ACE). • Définissez des règles de politique pour contrôler l'accès aux applications GenAI et aux applications non GenAI. • Inspection d'Enterprise DLP et rendu des verdicts pour les applications GenAI et non GenAI prises en charge. • Accédez à Strata Cloud Manager Command Center pour obtenir une visibilité GenAI. • Accédez au tableau de bord AI Access Security Activity Insights (Informations sur l'activité) pour afficher des données détaillées sur l'utilisation de l'application GenAI, les utilisateurs et les cas d'utilisation courants de GenAI survenant sur votre réseau. • Étiquetez les applications GenAI sur Strata Cloud Manager pour indiquer si l'application est approuvée au sein de votre organisation et pour l'application de politiques basées sur les étiquettes. AI Access Security ne synchronise pas les étiquettes des applications GenAI avec Panorama. • Générez des rapports uniquement pour les applications GenAI découvertes. • Affichez les applications GenAI dans le Dictionnaire des applications pour en savoir plus sur les applications GenAI spécifiques, les fournisseurs, la conformité et les caractéristiques de risque qui sous-tendent ces applications SaaS. • Affichez les applications GenAI installées en tant qu'applications/plug-ins tiers connectés dans 7 applications SaaS Marketplace.

Version PAN-OS ou du plan de données	NGFW et Prisma Access (gérés par Panorama ou Strata Cloud Manager)
	• Visibilité et contrôle des données au repos résidant dans l'application ChatGPT Enterprise.

- **Licences CASB-PA et CASB-X**

  S'applique aux NGFW ou à Prisma Access gérés par Strata Cloud Manager lorsque les licences CASB-PA ou CASB-X sont actives.

Version PAN-OS ou du plan de données	CASB-PA et CASB-X

10.2
11.1
Prisma Access 5.0 Preferred et Innovation et versions ultérieures
Prisma Access 5.1 Preferred et versions ultérieures
	• Visibilité sur plus de 2 250 applications GenAI fournies par les mises à jour du contenu dynamique et App-ID Cloud Engine (ACE).
	• Définissez des règles de politique pour contrôler l'accès aux applications GenAI et aux applications non GenAI.
	• Inspection d'Enterprise DLP et rendu des verdicts pour les applications GenAI et non GenAI prises en charge.
	• Accédez à Strata Cloud Manager Command Center pour obtenir une visibilité GenAI.
	• Accédez au tableau de bord AI Access Security Activity Insights (Informations sur l'activité) pour afficher des données détaillées sur l'utilisation de l'application GenAI, les utilisateurs et les cas d'utilisation courants de GenAI survenant sur votre réseau.
	• Consultez les informations suivantes pour toutes les applications SaaS Inline, y compris les applications GenAI :
	  • Tableaux de bord
	  • Utilisateurs
	  • Dictionnaire des applications
	  • Applications
	  • Rapports
	  • Recommandations en matière de politique
	• Affichez tous les plug-ins tiers (SSPM), y compris les plug-ins GenAI.
	• Affichez les détails des ressources de toutes les applications SaaS approuvées (data-at-rest) y compris les applications GenAI.

11.2.2-h1 et versions ultérieures Prisma Access 5.1 Innovation et versions ultérieures	• Visibilité sur plus de 2 250 applications GenAI fournies par les mises à jour du contenu dynamique et App-ID Cloud Engine (ACE). • Définissez des règles de politique pour contrôler l'accès aux applications GenAI et aux applications non GenAI.

Version PAN-OS ou du plan de données	CASB-PA et CASB-X

	• Inspection d'Enterprise DLP et rendu des verdicts pour les applications GenAI et non GenAI prises en charge.
	• Accédez à Strata Cloud Manager Command Center pour obtenir une visibilité GenAI.
	• Accédez au tableau de bord AI Access Security Activity Insights (Informations sur l'activité) pour afficher des données détaillées sur l'utilisation de l'application GenAI, les utilisateurs et les cas d'utilisation courants de GenAI survenant sur votre réseau.
	• Étiquetez les applications GenAI sur Strata Cloud Manager pour indiquer si l'application est approuvée au sein de votre organisation et pour l'application de politiques basées sur les étiquettes.
	AI Access Security ne synchronise pas les étiquettes des applications GenAI avec Panorama.
	• Consultez les informations suivantes pour toutes les applications SaaS Inline, y compris les applications GenAI :
	  • Tableaux de bord
	  • Utilisateurs
	  • Dictionnaire des applications
	  • Applications
	  • Rapports
	  • Recommandations en matière de politique
	• Affichez tous les plug-ins tiers (SSPM), y compris les plug-ins GenAI.
	• Affichez les détails des ressources de toutes les applications SaaS approuvées (data-at-rest) y compris les applications GenAI.

Prérequis pour la configuration AI Access Security

Examinez les prérequis d'utilisation de AI Access Security. Les prérequis décrivent les versions minimales du plan de données PAN-OS et Prisma Access ainsi que tous les services supplémentaires nécessaires pour utiliser AI Access Security.

Examinez les différentes combinaisons de licences AI Access Security et de versions PAN-OS pour en savoir plus sur les fonctionnalités prises en charge par AI Access Security.

- **NGFW et Prisma Access (géré par Panorama)**

  Référez-vous aux prérequis de la **licence AI Access Security** lors de la gestion de votre configuration AI Access Security depuis Panorama et n'activez que la licence AI Access Security.

  Référez-vous aux prérequis des **Licences CASB-PA et CASB-X** lors de la gestion de votre configuration AI Access Security depuis Panorama et activez une licence CASB-PA ou CASB-X.

Prérequis	Licence AI Access Security	Licences CASB-PA et CASB-X
PAN-OS ou plan de données	PAN-OS 11.2.2-h1	• PAN-OS 10.2.3 et Prisma Access 5.0 Preferred et Innovation • PAN-OS 11.1.0 et Prisma Access 5.1 Preferred • PAN-OS 11.2.2-h1 et Prisma Access 5.1 Innovation Examinez les Notes de version Prisma Access pour obtenir des détails sur la version minimum requise de Prisma Access.
Filtrage des données	Plug-in Enterprise DLP 5.0.4 ou version ultérieure	Examinez la Matrice de compatibilité pour la version du plug-in Enterprise DLP prise en charge sur votre version de PAN-OS.
	AI Access Security inclut Enterprise DLP lorsque vous activez les licences AI Access Security, CASB-PA et CASB-X.	

Prérequis	Licence AI Access Security	Licences CASB-PA et CASB-X
Gestion	Strata Cloud Manager Essentials ou Strata Cloud Manager Pro En savoir plus sur ce que chaque licence inclut.	S. O.
Plugin Cloud Services	Plug-in Cloud Services 5.1	
de journalisation	Strata Logging Service	

- **NGFW et Prisma Access (géré par Strata Cloud Manager)**

  Référez-vous aux prérequis de la **licence AI Access Security** lors de la gestion de votre configuration AI Access Security depuis Strata Cloud Manager et n'activez que la licence AI Access Security.

  Référez-vous aux prérequis des **licences CASB-PA et CASB-X** lors de la gestion de votre configuration AI Access Security depuis Strata Cloud Manager et activez une licence CASB-PA ou CASB-X.

Prérequis	Licence AI Access Security	Licences CASB-PA et CASB-X
PAN-OS ou plan de données	PAN-OS 11.2.2-h1	• PAN-OS 10.2.3 et Prisma Access 5.0 Preferred et Innovation • PAN-OS 11.1.0 et Prisma Access 5.1 Preferred • PAN-OS 11.2.2-h1 et Prisma Access 5.1 Innovation Examinez les Notes de version Prisma Access pour obtenir des détails sur la version minimum requise de Prisma Access.
Filtrage des données	AI Access Security inclut Enterprise DLP lorsque vous activez les licences AI Access Security, CASB-PA et CASB-X.	
Gestion	Strata Cloud Manager Essentials ou Strata Cloud Manager Pro En savoir plus sur ce que chaque licence inclut.	S. O.

Prérequis	Licence AI Access Security	Licences CASB-PA et CASB-X
de journalisation	Strata Logging Service	

Activer la licence AI Access Security

Activez votre licence AI Access Security pour permettre l'adoption en toute sécurité des applications d'IA générative (GenAI) par vos employés dans votre organisation. L'activation de AI Access Security est effectuée à l'aide d'un lien magique fourni par Palo Alto Networks après l'achat de la licence AI Access Security. Ces procédures supposent que vous disposez déjà de tous les codes d'autorisation de licence et liens magiques requis pour l'activation.

Après avoir acheté votre licence AI Access Security, vous devez l'activer à l'aide d'un lien magique qui vous a été envoyé par Palo Alto Networks. AI Access Security est inclus lorsque vous activez une licence CASB-PA ou CASB-X. Aucune autre action n'est requise pour activer AI Access Security après l'activation d'une licence CASB-PA ou CASB-X.

- Nouveaux déploiements
- Déploiements existants

Activer la licence AI Access Security (Nouveaux déploiements)

STEP 1 | Installez et effectuez la configuration initiale pour votre NGFW.

Cela inclut l'activation de toutes les licences de support requises.

STEP 2 | Configurez la gestion pour votre locataire NGFW ou Prisma Access.

- **NGFW (Managed by Panorama)**
  1. Configurez Panorama (
     - **Appareil M-Series** : configurez l'appareil M-Series en Gestion uniquement ou en mode Panorama.
     - **Panorama Appareil Virtuel** : Installez l'appareil virtuel Panorama sur l'hyperviseur de votre choix en Gestion uniquement ou en mode Panorama
  2. Déployez Strata Logging Service.
  3. Enregistrez Panorama.
  4. Activez la licence d'assistance Panorama.
  5. Activez la licence de gestion de périphérique Panorama (Appareil M-Series ou Panorama Appareil virtuel).
  6. Ajoutez vos pare-feux gérés à la gestion Panorama.
  7. Effectuez la mise à niveau de Panorama vers la version minimale de PAN-OS prise en charge pour AI Access Security.
  8. Effectuez la mise à niveau de votre NGFW vers la version minimale de PAN-OS prise en charge pour AI Access Security.
- **NGFW (Managed by Strata Cloud Manager)**
  1. Déployez Strata Logging Service.

     Strata Cloud Manager nécessite Strata Logging Service pour la journalisation.
  2. Activez la licence Strata Cloud Manager Essentials ou Strata Cloud Manager Pro.
  3. Intégrez votre NGFW à Strata Cloud Manager.
  4. Installez les dernières mises à jour du contenu dynamique et effectuez la mise à niveau de votre NGFW vers la version minimale de PAN-OS prise en charge pour AI Access Security.
- **Prisma Access (Managed by Panorama)**
  1. Configurez Panorama (
     - **Appareil M-Series** : configurez l'appareil M-Series en Gestion uniquement ou en mode Panorama.
     - **Panorama Appareil Virtuel** : Installez l'appareil virtuel Panorama sur l'hyperviseur de votre choix en Gestion uniquement ou en mode Panorama
  2. Déployez Strata Logging Service.
  3. Enregistrez Panorama.
  4. Activez la licence d'assistance Panorama.
  5. Activez la licence de gestion de périphérique Panorama (Appareil M-Series ou Panorama Appareil virtuel).
  6. Effectuez la mise à niveau de Panorama vers la version minimale de PAN-OS prise en charge pour AI Access Security.
  7. Installez le plug-in Cloud Services sur Panorama.
  8. Configurez Panorama Managed Prisma Access.

- **Prisma Access (Managed by Strata Cloud Manager)**
  1. Déployez Strata Logging Service.

     Strata Cloud Manager nécessite Strata Logging Service pour la journalisation.
  2. Activez la licence Prisma Access sur Strata Cloud Manager.
  3. Configurez Prisma Access.

STEP 3 | Configurez Enterprise Data Loss Prevention (E-DLP).

- **NGFW (Managed by Panorama)**
  1. Installez le plug-in Enterprise DLP sur Panorama.
  2. Activez Enterprise DLP pour NGFW.
  3. Modifiez le contenu cloud Enterprise DLP, le filtrage de données et les paramètres d'extrait selon les besoins.
- **NGFW (Managed by Strata Cloud Manager)**
  1. Activez Enterprise DLP pour NGFW.
  2. Modifiez le filtrage de données Enterprise DLP et les paramètres d'extrait selon les besoins.
- **Prisma Access (Managed by Panorama)**
  1. Installez le plug-in Enterprise DLP sur Panorama.
  2. Activez Enterprise DLP pour Prisma Access.
  3. Modifiez le contenu cloud Enterprise DLP, le filtrage de données et les paramètres d'extrait selon les besoins.
- **Prisma Access (Managed by Strata Cloud Manager)**
  1. Activez Enterprise DLP pour NGFW.
  2. Modifiez le filtrage de données Enterprise DLP et les paramètres d'extrait selon les besoins.

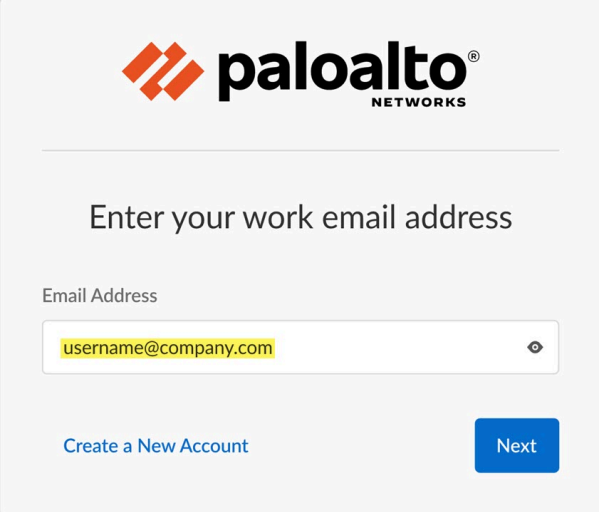
STEP 4 | Cliquez sur le lien magique fourni par Palo Alto Networks lorsque vous avez acheté l'abonnement AI Access Security.

STEP 5 | Cliquez sur **Activate Subscription (Activer l'abonnement)** pour commencer à activer AI Access Security.

STEP 6 | Entrez l'**Email Address (Adresse e-mail)** de votre Portail du support client (CSP) Palo Alto Networks. Cette adresse e-mail doit correspondre à l'adresse e-mail à laquelle le lien magique d'activation de AI Access Security a été envoyé.

Create a New Account (Créez un compte) si l'adresse e-mail qui a reçu le lien d'activation AI Access Security n'a pas déjà de compte CSP valide. Le compte nouvellement créé est

automatiquement associé au même locataire que celui pour lequel vous activez AI Access Security et se voit attribuer un rôle de super utilisateur multilocataire.



STEP 7 | (Multitlocataires uniquement) Dans la section **Customer Support Account (Compte de support client)**, sélectionnez le Compte de support client Palo Alto Networks associé au locataire pour lequel vous activez la licence AI Access Security.

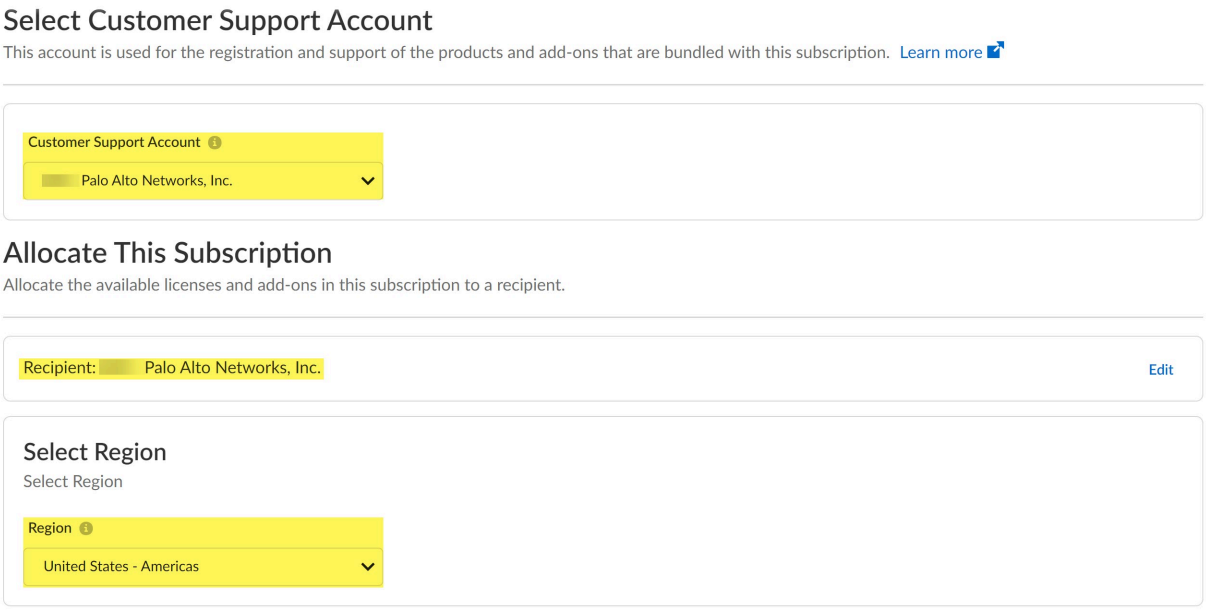
Ignorez cette étape si vous avez un compte locataire unique sur le Portail de Support Client. Votre Compte de support client est sélectionné par défaut.

STEP 8 | (Multilocataires uniquement) Dans la section **Allocate This Subscription (Allouer cet abonnement)**, sélectionnez le groupe de services de locataire (TSG) pour lequel vous souhaitez activer AI Access Security. Vous pouvez sélectionner le locataire parent ou un locataire enfant.

AI Access Security est activé uniquement pour le locataire sélectionné. Si vous sélectionnez un locataire parent, AI Access Security n'est activé pour aucun locataire enfant.

Ignorez cette étape si vous n'avez qu'un compte locataire unique sur le Portail de Support Client Il est sélectionné par défaut.

STEP 9 | Examinez la **Region (Région)** du locataire. Cette région est préremplie en fonction de la région du locataire NGFW ou Prisma Access déployé et ne peut pas être modifiée.

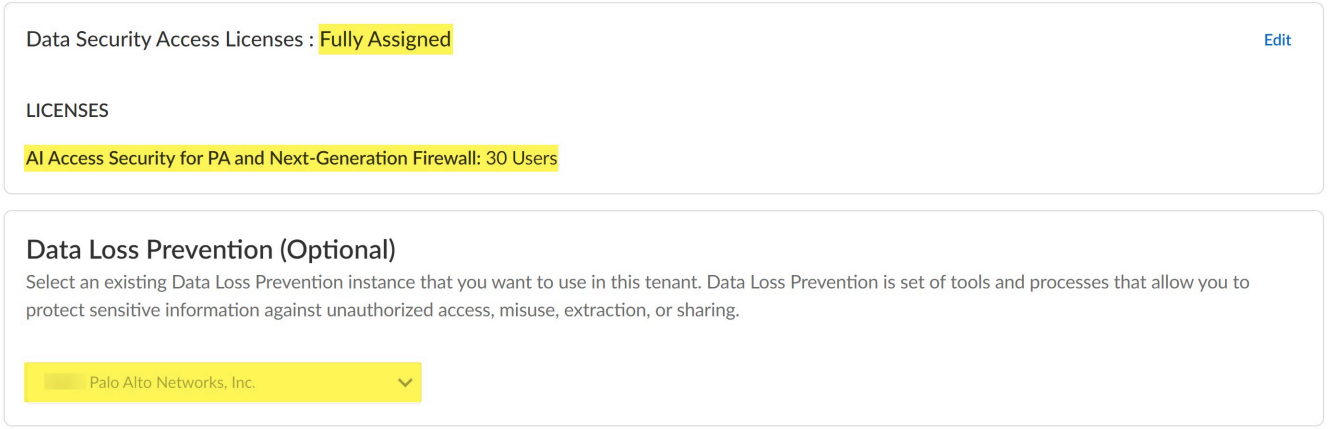


STEP 10 | Dans la section **Assign Licenses (Attribuer des licences)**, cliquez sur **Done (Terminé)** pour attribuer toutes vos licences AI Access Security. Vérifiez que votre **AI Access Security License (Licence de sécurité d'accès à l'IA)** est `Fully Assigned (Entièrement attribuée)`.

STEP 11 | Vérifiez que votre instance **Data Loss Prevention (Prévention des pertes de données)** est sélectionnée si Enterprise Data Loss Prevention (E-DLP) est active sur votre locataire.

Votre instance Enterprise DLP est sélectionnée par défaut si elle est déjà active sur votre locataire.

Ignorez cette étape si vous n'avez pas d'instance Enterprise DLP déjà active. Enterprise DLP n'est pas nécessaire pour activer AI Access Security. Si l'instance Enterprise DLP n'est pas déjà active, une instance est créée dans le cadre de l'activation de la licence. Passez en revue ce qui arrive à Enterprise DLP si vous ne renouvelez pas votre licence AI Access Security.

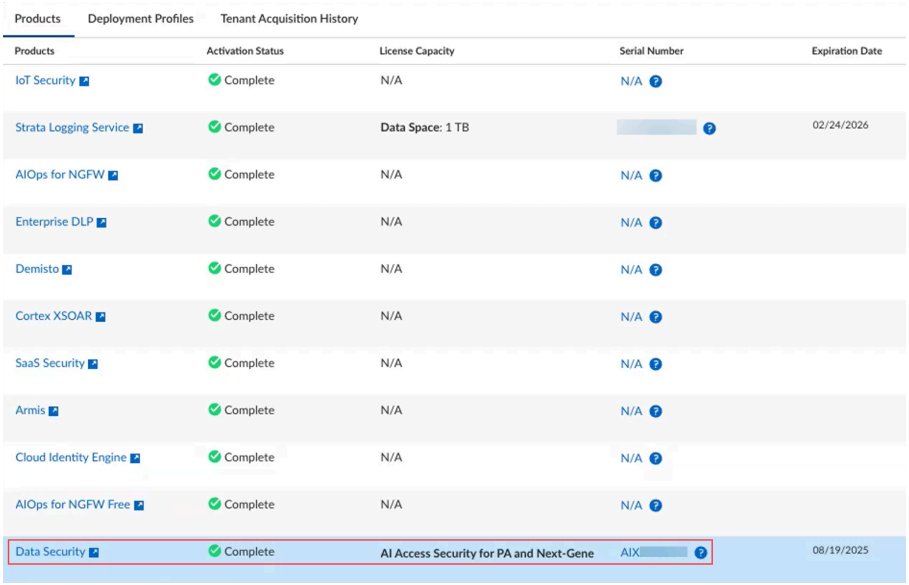


STEP 12 | Cliquez sur **Agree to the Terms and Conditions (Accepter les termes et conditions)** et sur

STEP 13 | **Activate (Activer).**

Vous êtes redirigé vers la page Tenant Management (Gestion des locataires) où le **Activation Status (État de l'activation)** de AI Access Security commence la phase `Initializing (Initialisation)`.

La licence AI Access Security s'affiche comme **Data Security (Sécurité des données)** et a un numéro de série qui commence par `AIX`. Passez à l'étape suivante après que le **Activation Status (État d'activation)** arrive à `Complete (Terminé)`.



STEP 14 | (NGFW uniquement) Associez la licence AI Access Security avec votre NGFW.

L'association de la licence AI Access Security est requise pour activer la licence pour votre NGFW.

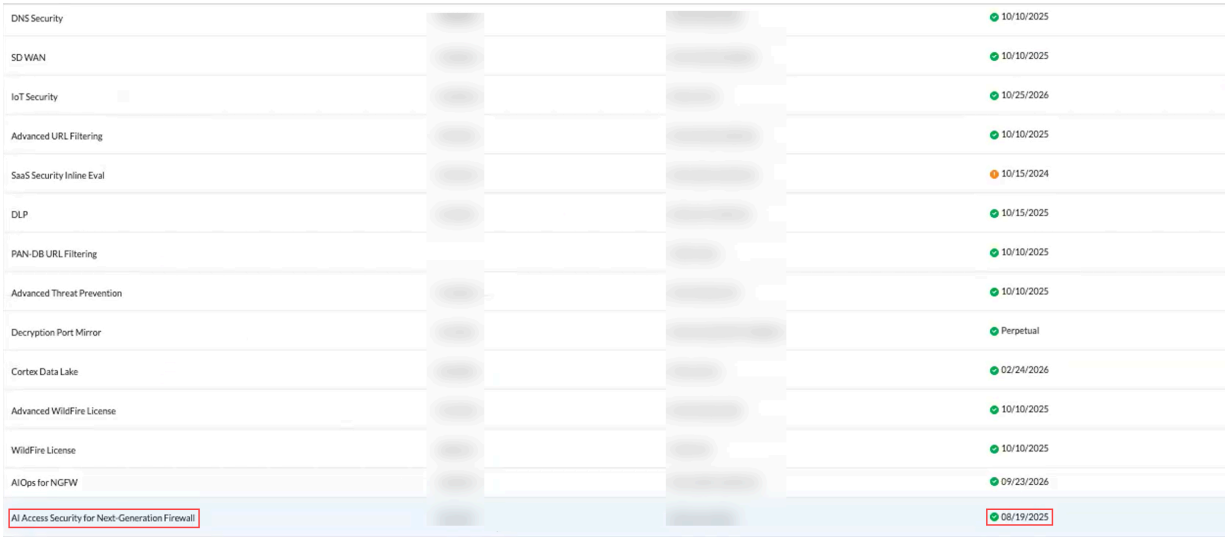
1. Dans le menu Strata Cloud Manager, sélectionnez **Settings (Paramètres)** > **Device Associations (Associations de périphériques)**.

   Le menu Strata Cloud Manager se trouve dans le coin inférieur gauche de Strata Cloud Manager.
2. Dans le menu Strata Cloud Manager, sélectionnez **System Settings (Paramètres système)** > **Device Associations (Associations de périphériques)**.

   Le menu Strata Cloud Manager se trouve dans le coin inférieur gauche de Strata Cloud Manager.
3. **Associate Apps (Associer des applications)**.
4. Dans les produits sous licence, sélectionnez **Data Security (Sécurité des données)**.
5. Sélectionnez le NGFW pour lequel vous souhaitez activer AI Access Security.
6. **Save (Enregistrer)**.

STEP 15 | Vérifiez que vous avez bien activé AI Access Security.

1. Palo Alto NetworksConnectez-vous au portail de support client (CSP).
2. Sélectionnez **Products (Produits)** > **Assets (Actifs)**.
3. Sélectionnez le locataire **NGFW** ou **Prisma Access** en fonction du point d'application pour lequel vous avez activé AI Access Security.
4. Utilisez les filtres pour localiser votre locataire NGFW ou Prisma Access.
5. Développez la liste des licences actives ou cliquez sur **Licenses & Subscriptions (Licences et abonnements)**.
6. Vérifiez que la licence AI Access Security est active.



STEP 16 | Prise en main de AI Access Security.

Activer la licence AI Access Security (Déploiements existants)

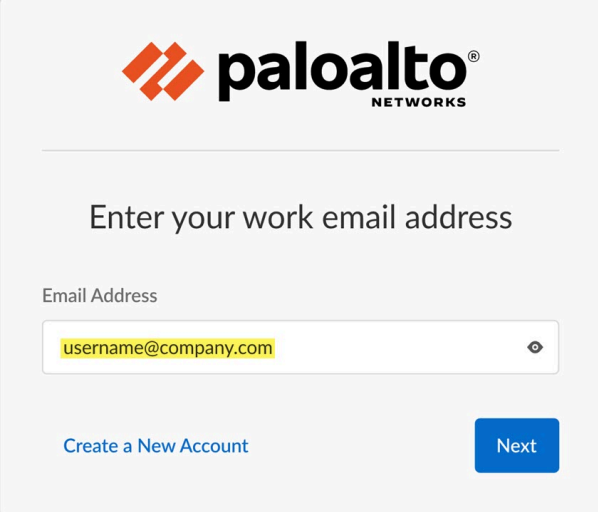
Cette procédure suppose que vous devez uniquement activer la licence AI Access Security, que toutes les licences préalables sont activées et que votre NGFW, Prisma Access, Panorama™ management server et Strata Cloud Manager sont configurés avec succès selon les besoins.

STEP 1 | Cliquez sur le lien magique fourni par Palo Alto Networks lorsque vous avez acheté l'abonnement AI Access Security.

STEP 2 | Cliquez sur **Activate Subscription (Activer l'abonnement)** pour commencer à activer AI Access Security.

STEP 3 | Entrez l'**Email Address (Adresse e-mail)** de votre Portail du support client (CSP) Palo Alto Networks. Cette adresse e-mail doit correspondre à l'adresse e-mail à laquelle le lien magique d'activation de AI Access Security a été envoyé.

Create a New Account (Créez un compte) si l'adresse e-mail qui a reçu le lien d'activation AI Access Security n'a pas déjà de compte CSP valide. Le compte nouvellement créé est automatiquement associé au même locataire que celui pour lequel vous activez AI Access Security et se voit attribuer un rôle de super utilisateur multilocataire.



STEP 4 | (Multitlocataires uniquement) Dans la section **Customer Support Account (Compte de support client)**, sélectionnez le Compte de support client Palo Alto Networks associé au locataire pour lequel vous activez la licence AI Access Security.

Ignorez cette étape si vous avez un compte locataire unique sur le Portail de Support Client. Votre Compte de support client est sélectionné par défaut.

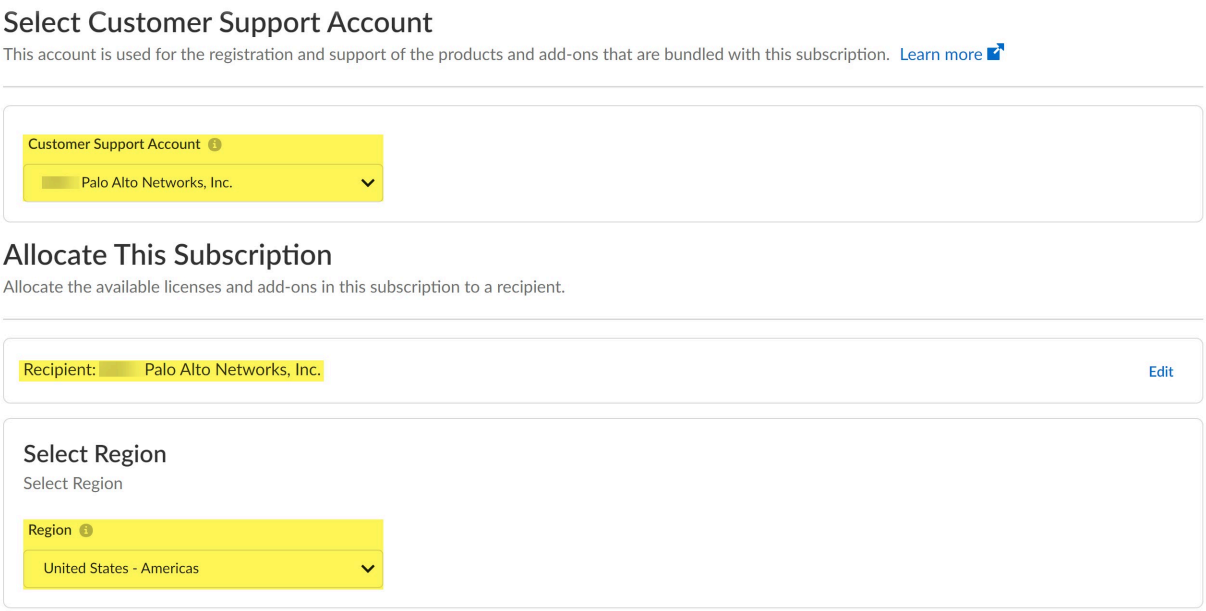
STEP 5 | (Multilocataires uniquement) Dans la section **Allocate This Subscription (Allouer cet abonnement)**, sélectionnez le groupe de services de locataire (TSG) pour lequel vous

souhaitez activer AI Access Security. Vous pouvez sélectionner le locataire parent ou un locataire enfant.

AI Access Security est activé uniquement pour le locataire sélectionné. Si vous sélectionnez un locataire parent, AI Access Security n'est activé pour aucun locataire enfant.

Ignorez cette étape si vous n'avez qu'un compte locataire unique sur le Portail de Support Client Il est sélectionné par défaut.

STEP 6 | Examinez la **Region (Région)** du locataire. Cette région est préremplie en fonction de la région du locataire NGFW ou Prisma Access déployé et ne peut pas être modifiée.



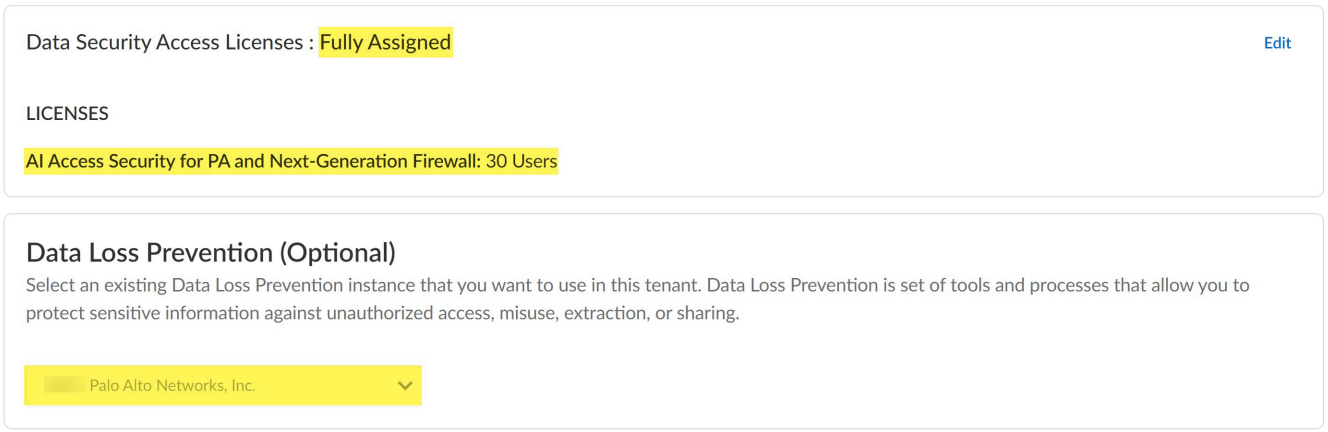
STEP 7 | Dans la section **Assign Licenses (Attribuer des licences)**, cliquez sur **Done (Terminé)** pour attribuer toutes vos licences AI Access Security. Vérifiez que la **AI Access Security Licence (Licence de sécurité d'accès à l'IA)** est `Fully Assigned (Entièrement attribuée)`.

STEP 8 | Vérifiez que votre instance **Data Loss Prevention (Prévention des pertes de données)** est sélectionnée si Enterprise Data Loss Prevention (E-DLP) est active sur votre locataire.

Votre instance Enterprise DLP est sélectionnée par défaut si elle est déjà active sur votre locataire.

Ignorez cette étape si vous n'avez pas d'instance Enterprise DLP déjà active. Enterprise DLP n'est pas nécessaire pour activer AI Access Security. Si l'instance Enterprise DLP n'est pas déjà

active, une instance est créée dans le cadre de l'activation de la licence. Passez en revue ce qui arrive à Enterprise DLP si vous ne renouvelez pas votre licence AI Access Security.

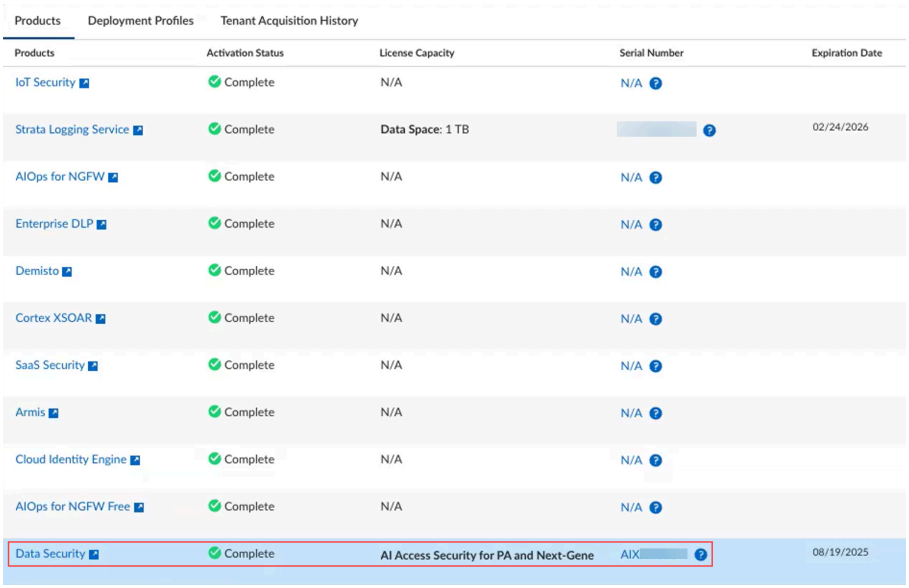


STEP 9 | Cliquez sur **Agree to the Terms and Conditions (Accepter les termes et conditions)** et sur

STEP 10 | **Activate (Activer)**.

Vous êtes redirigé vers la page Tenant Management (Gestion des locataires) où le **Activation Status (État de l'activation)** de AI Access Security commence la phase `Initializing (Initialisation)`.

La licence AI Access Security s'affiche comme **Data Security (Sécurité des données)** et a un numéro de série qui commence par `AIX`. Passez à l'étape suivante après que le **Activation Status (État d'activation)** arrive à `Complete (Terminé)`.



STEP 11 | (NGFW uniquement) Associez la licence AI Access Security avec votre NGFW.

L'association de la licence AI Access Security est requise pour activer la licence pour votre NGFW.

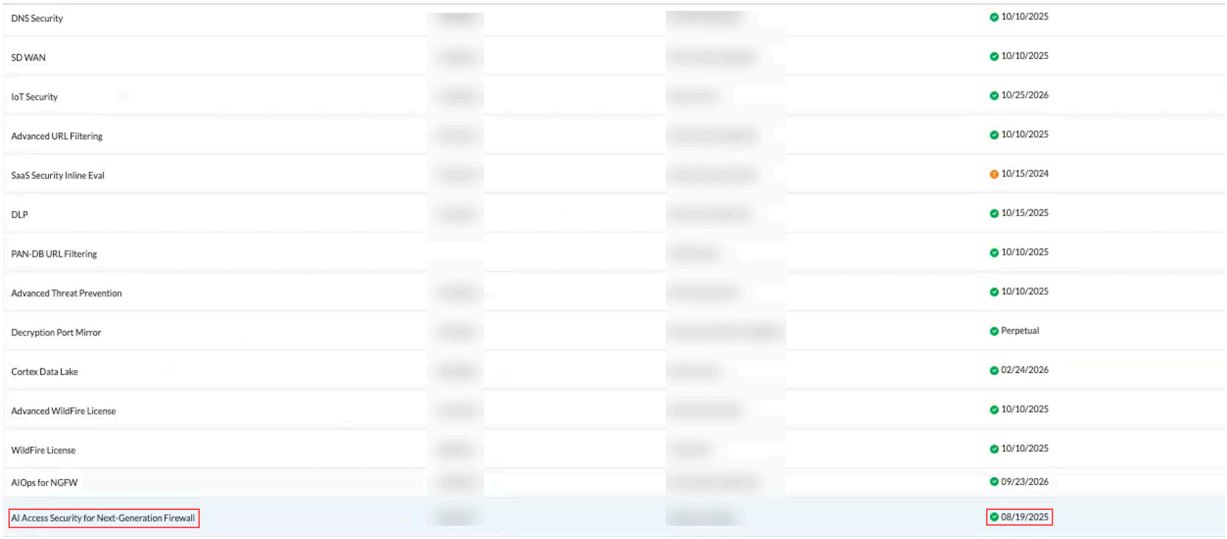
1. Dans le menu Strata Cloud Manager, sélectionnez **Settings (Paramètres)** > **Device Associations (Associations de périphériques)**.

   Le menu Strata Cloud Manager se trouve dans le coin inférieur gauche de Strata Cloud Manager.
2. Dans le menu Strata Cloud Manager, sélectionnez **System Settings (Paramètres système)** > **Device Associations (Associations de périphériques)**.

   Le menu Strata Cloud Manager se trouve dans le coin inférieur gauche de Strata Cloud Manager.
3. **Associate Apps (Associer des applications)**.
4. Dans les produits sous licence, sélectionnez **Data Security (Sécurité des données)**.
5. Sélectionnez le NGFW pour lequel vous souhaitez activer AI Access Security.
6. **Save (Enregistrer)**.

STEP 12 | Vérifiez que vous avez bien activé AI Access Security.

1. Palo Alto NetworksConnectez-vous au portail de support client (CSP).
2. Sélectionnez **Products (Produits)** > **Assets (Actifs)**.
3. Sélectionnez le locataire **NGFW** ou **Prisma Access** en fonction du point d'application pour lequel vous avez activé AI Access Security.
4. Utilisez les filtres pour localiser votre locataire NGFW ou Prisma Access.
5. Développez la liste des licences actives ou cliquez sur **Licenses & Subscriptions (Licences et abonnements)**.
6. Vérifiez que la licence AI Access Security est active.



STEP 13 | Prise en main de AI Access Security.

Convertir une licence d'évaluation AI Access Security en licence de production

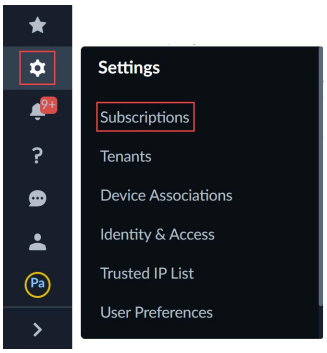
Si vous possédez une licence EVAL licence AI Access Security active, vous devez convertir la licence d'évaluation en une licence de production pour continuer à contrôler l'accès et à adopter les applications GenAI en toute sécurité une fois la période d'évaluation terminée. Si vous ne convertissez pas la licence d'évaluation en une licence de production :

- Le trafic contenant des données sensibles n'est plus transféré à Enterprise Data Loss Prevention (E-DLP) pour inspection et rendu de verdict.
- Enterprise DLP n'est plus accessible.
  - **Panorama™ management server** : **Objects (Objets)** > **DLP (DLP)**
  - **Strata Cloud Manager** : **Manage (Gérer)** > **Configuration (Configuration)** > **Data Loss Prevention (Prévention des pertes de données)**
- Les règles de sécurité Web et de politique de sécurité créées pour AI Access Security sont préservées.

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Dans le menu Strata Cloud Manager, sélectionnez **Settings (Paramètres)** > **Subscriptions (Abonnements)**.

Le menu Strata Cloud Manager se trouve dans le coin inférieur gauche de Strata Cloud Manager.



STEP 3 | Sélectionnez **System Settings (Paramètres système)** > **Subscriptions (Abonnements)**.

STEP 4 | Trouvez la licence d'évaluation AI Access Security et sélectionnez **Actions (Actions)** > **Eval to Prod Request (Demande de passage à la licence de production)**.

STEP 5 | Spécifiez les conditions de la licence de production que vous souhaitez pour votre locataire. La demande est examinée par votre représentant de compte Palo Alto Networks pour créer un devis.

Précisez les informations suivantes dans votre demande de licence de production.

- **Quantité de licences** : nombre de personnes pouvant utiliser AI Access Security.
- **Durée** : durée de votre abonnement AI Access Security.

STEP 6 | **Send Request (Envoyez la demande)**.

Renouveler une licence AI Access Security

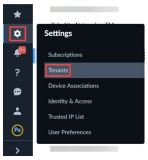
Vous pouvez renouveler votre licence AI Access Security arrivant à expiration pour continuer à adopter les applications GenAI en toute sécurité. Une licence AI Access Security arrivant à expiration ne se renouvelle pas automatiquement et nécessite un renouvellement manuel. Si la licence AI Access Security expire :

- Le trafic contenant des données sensibles n'est plus transféré à Enterprise Data Loss Prevention (E-DLP) pour inspection et rendu de verdict.
- Enterprise DLP n'est plus accessible.
  - **Panorama™ management server** : **Objects (Objets)** > **DLP (DLP)**
  - **Strata Cloud Manager** : **Manage (Gérer)** > **Configuration (Configuration)** > **Data Loss Prevention (Prévention des pertes de données)**
- Les règles de sécurité Web et de politique de sécurité créées pour AI Access Security sont préservées.

STEP 1 | Contactez votre représentant commercial Palo Alto Networks et demandez un renouvellement de votre licence AI Access Security.

STEP 2 | Connectez-vous à Strata Cloud Manager.

STEP 3 | Dans le menu en bas à gauche, sélectionnez **Settings (Paramètres)** > **Tenants (Locataires)**.



STEP 4 | Sélectionnez **System Settings (Paramètres système)** > **Tenants (Locataires)**.

STEP 5 | Sélectionnez le locataire pour lequel vous renouvelez la licence AI Access Security.

Vous pouvez sélectionner un locataire parent ou un locataire enfant. Un locataire avec une licence nécessitant une action immédiate pour renouveler la licence est marqué d'un cercle bleu.

STEP 6 | **Edit (Modifiez)** les licences des locataires.

STEP 7 | Cliquez sur **Agree to the terms and conditions (Accepter les termes et conditions)** et **Activate Now (Activer maintenant)**.