paloalto
TECHDOCS

Activation et intégration de Strata Cloud Manager

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 17, 2026

Table of Contents

Activer vos licences Strata Cloud Manager

Pour commencer à utiliser Strata Cloud Manager, vous devez activer le niveau de licence approprié : Essentials ou Pro.

- Activer Strata Cloud Manager Essentials : le niveau gratuit qui offre la gestion de la configuration et la gestion du cycle de vie de la sécurité du réseau, et peut également apporter de la visibilité si vous disposez d'une licence payante du service de journalisation Strata.
- Activer Strata Cloud Manager Pro : outre les fonctionnalités de Strata Cloud Manager Essentials, ce niveau fournit des fonctionnalités avancées. Lorsque vous activez Strata Cloud Manager Pro, vous bénéficiez également d'un accès au service de journalisation Strata qui inclut une année de conservation des journaux et un stockage illimité.

Si vous utilisiez Strata Cloud Manager avant l'introduction de ces nouveaux niveaux de licence, vos licences existantes pour Prisma Access et AIOps pour NGFW Premium restent prises en charge. Vous pouvez continuer à modifier, prolonger ou renouveler ces licences. De plus, si vous utilisez AIOps pour NGFW Gratuit, vous avez la possibilité de passer à AIOps pour NGFW Premium.

- Activation d'AIOps pour NGFW Premium
- Activer le contrat ELA pour AIOps pour NGFW Premium
- Activer un contrat de licence de crédits NGFW logiciels
- Activer votre licence Prisma Access
- Licences ADEM

Activer Strata Cloud Manager Essentials

Strata Cloud Manager Essentials est le niveau gratuit qui offre des fonctionnalités de gestion de la configuration et de gestion du cycle de vie de la sécurité du réseau pour simplifier les opérations et fournir une sécurité essentielle. Pour plus de détails sur la prise en charge des modèles de périphériques, voir Compatibilité des modèles de périphériques.

Vous pouvez activer des pare-feu VM-Series financés par des crédits NGFW logiciels en utilisant le niveau de licence Strata Cloud Manager Essentials. Si vous ne sélectionnez pas d'abonnement au cloud dans le profil de déploiement, Strata Cloud Manager Essentials s'active automatiquement.

STEP 1 | Connectez-vous au hub.

STEP 2 | Accédez à l'URL d'activation de Strata Cloud Manager Essentials : https://apps.paloaltonetworks.com/activation/scm-essentials.

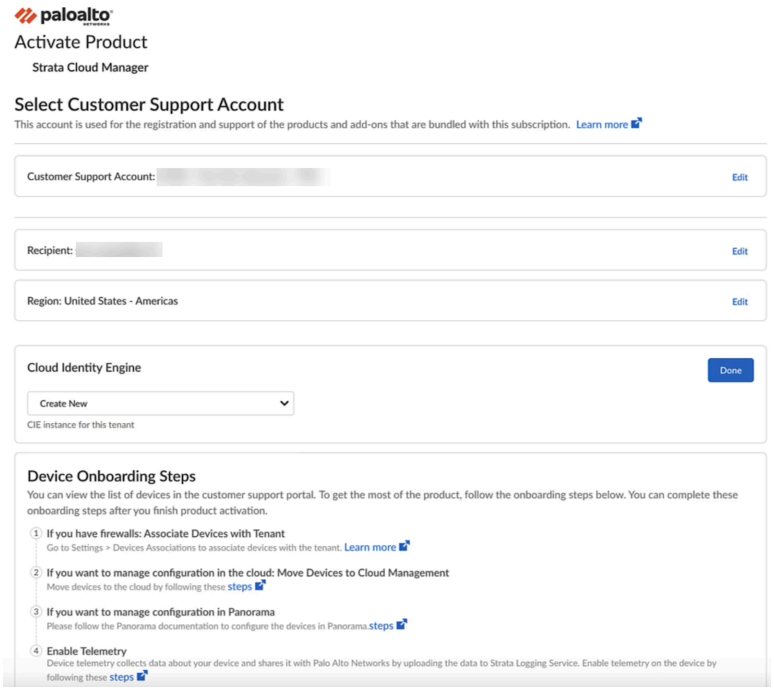
STEP 3 | Sélectionnez le compte de support client.

STEP 4 | Dans **Create New (Créer nouveau)**, choisissez le locataire où vous allez activer Strata Cloud Manager Pro.

STEP 5 | Sélectionnez la **région** où vous souhaitez déployer Strata Cloud Manager. Voir les régions prises en charge pour Strata Cloud Manager.

La prise en charge des régions varie selon que vous souhaitez gérer des NGFW, Prisma Access ou les deux simultanément. Pour gérer les deux, vous devez sélectionner une région qui prend en charge à la fois les NGFW et Prisma Access.

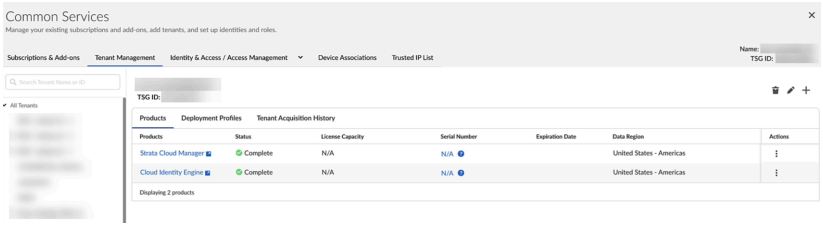
STEP 6 | Sélectionnez Cloud Identity Engine ou créez une nouvelle instance CIE pour identifier et vérifier tous les utilisateurs de votre infrastructure. Vous pouvez également ignorer cette étape en sélectionnant **None (Aucun)**.



STEP 7 | Cliquez sur **Agree to the Terms and Conditions (Accepter les conditions générales)**, puis sur **Activate (Activer)**.

STEP 8 | Attendez que Strata Cloud Manager s'initialise et que le statut indique Complete (Terminé).

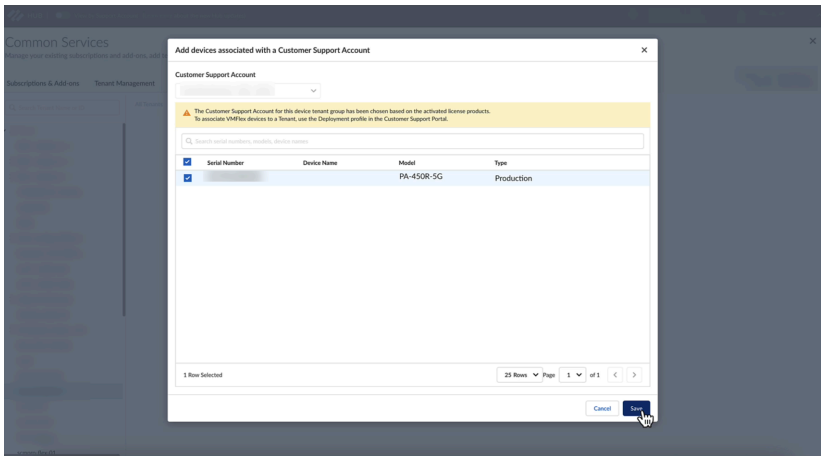
Si vous avez créé une nouvelle instance de Cloud Identity Engine, attendez que son statut indique Complete (Terminé).



STEP 9 | Associez des périphériques NGFW, Panorama ou les deux à un locataire contenant votre Strata Cloud Manager.

Assurez-vous d'associer tous les pare-feu gérés par Panorama individuellement au locataire.

1. Accédez à **Common Services (Services communs) > Device Associations (Associations de périphériques)**.
2. **Ajoutez des périphériques.**

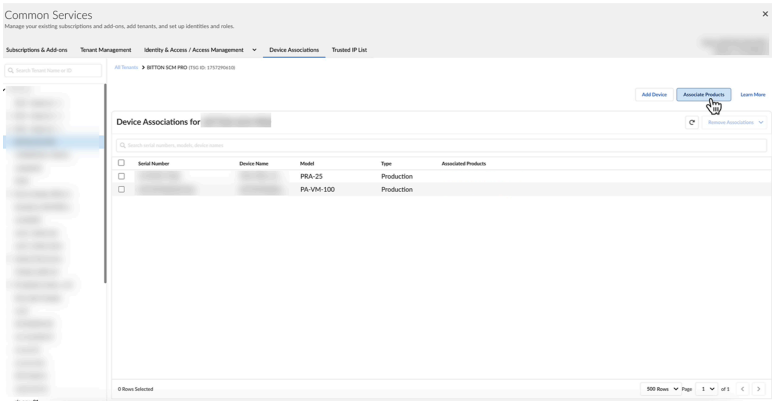


3. Sélectionnez un ou plusieurs pare-feu ou appareils Panorama, puis **Save (Enregistrer)**.

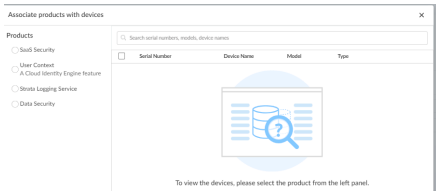
STEP 10 | Si vous disposez du service de journalisation Strata, vous pouvez l'associer à des périphériques. Sinon, vous pouvez l'ignorer.

Après avoir activé Strata Cloud Manager Essentials, vous pouvez spécifier les pare-feu ou appareils Panorama que vous souhaitez utiliser avec le service de journalisation Strata.

1. Sélectionnez **Common Services (Services communs) > Device Associations (Associations de périphériques)**.
2. **Associate Products (Associer des produits)**.



3. Dans la colonne de sélection des produits, sélectionnez **Strata Logging Service (Service de journalisation Strata)**.



4. Sélectionnez des périphériques et cliquez sur **Save (Enregistrer)**.

STEP 11 | Activez la télémétrie sur des périphériques. Strata Cloud Manager évalue la santé des périphériques de votre déploiement en analysant les données de télémétrie que vos périphériques PAN-OS envoient au service de journalisation Strata. Pour envoyer ces données, vous devez avoir activé la télémétrie de périphérique sur vos périphériques.

À partir de PAN-OS 12.1.2, 11.1.11, 11.2.8, 10.2.17 et des versions ultérieures, la fonctionnalité d'activation automatique de la télémétrie configure la télémétrie de sorte qu'elle soit activée par défaut sur vos périphériques. Lors de l'intégration d'un nouveau périphérique (Panorama ou pare-feu), la télémétrie est automatiquement activée avec des paramètres contrôlés de manière centralisée via Strata Cloud Manager ou le Hub.

STEP 12 | Connectez-vous à Strata Cloud Manager en cliquant sur son icône dans le hub.

Activer Strata Cloud Manager Pro

Strata Cloud Manager Pro fournit des fonctionnalités avancées en plus de celles de la licence Essentials. Contrairement à la version Essentials, cette licence inclut le service de journalisation Strata et offre une année de conservation des journaux. Pour plus de détails sur la prise en charge des modèles de périphériques, voir Compatibilité des modèles de périphériques.

Lorsque votre licence Strata Cloud Manager Pro expire, l'instance Strata Cloud Manager revient au niveau de licence Strata Cloud Manager Essentials. Lorsque la licence arrive à expiration pour d'autres abonnements, certains abonnements continuent de fonctionner de façon limitée, tandis que d'autres cessent complètement de fonctionner. Découvrez ce qui se passe à l'expiration de chaque abonnement.

- NGFW
- Prisma Access
- Pare-feu VM-Series financés par des crédits NGFW logiciels
- ELA
- ESA Pro

Activer Strata Cloud Manager Pro pour NGFW

Cette tâche montre comment activer Strata Cloud Manager Pro pour NGFW. Pour plus de détails sur la prise en charge des modèles de périphériques, voir Compatibilité des modèles de périphériques.

Voici les prérequis pour NGFW :

- **Prérequis pour l'intégration à la gestion cloud** : avant d'intégrer votre NGFW à Strata Cloud Manager, vérifiez que toutes les conditions de préparation du périphérique sont remplies. Cela inclut la configuration réseau, la compatibilité logicielle et les exigences de licence. Suivez ces étapes pour vous assurer que votre pare-feu est géré avec succès à l'aide de Strata Cloud Manager.
- **Ports TCP et FQDN pour la gestion cloud** : pour permettre une communication fluide entre le NGFW et Strata Cloud Manager, configurez des ports TCP spécifiques et des Fully Qualified Domain Name (nom de domaine complet - FQDN).

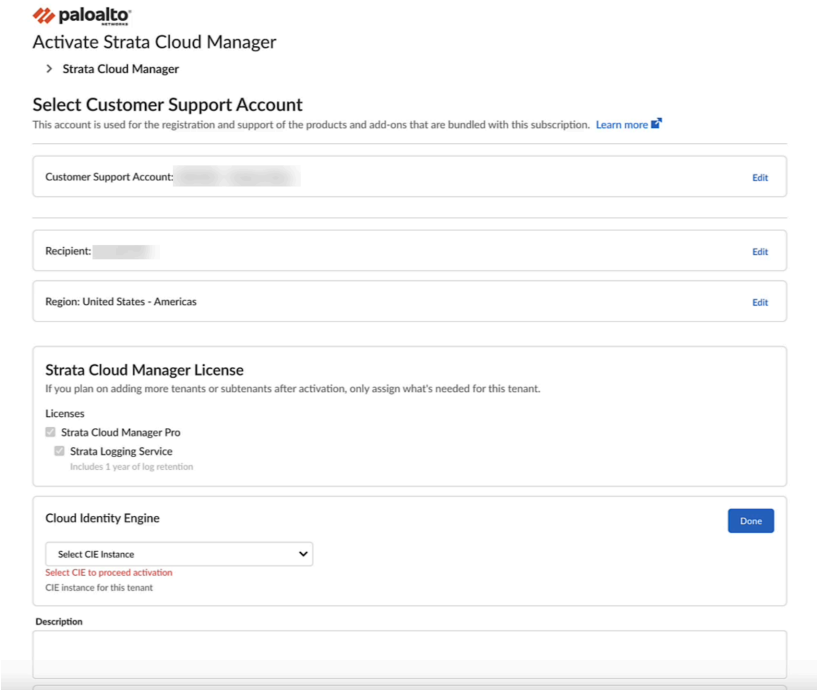
STEP 1 | Après avoir reçu un e-mail de Palo Alto Networks identifiant la licence Strata Cloud Manager Pro que vous activez, cliquez sur le lien contenu dans l'e-mail pour commencer le processus d'activation.

STEP 2 | Choisissez le compte de support client que vous souhaitez utiliser.

STEP 3 | Dans **Select Tenant (Sélectionner le locataire)**, choisissez le locataire où vous allez activer Strata Cloud Manager Pro. Si vous n'avez pas de locataire existant, sélectionnez **Create New (Créer nouveau)**.

STEP 4 | Sélectionnez la **région** où vous souhaitez déployer Strata Cloud Manager. Voir les régions prises en charge pour Strata Cloud Manager.

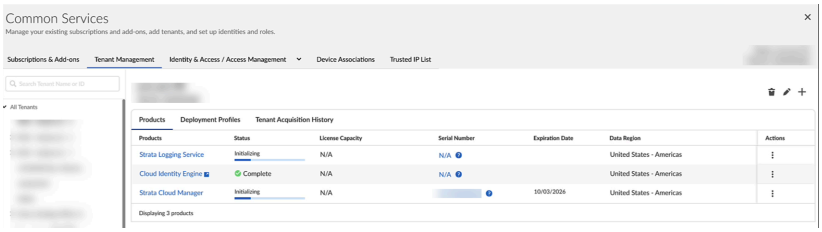
Strata Cloud Manager Pro inclut le service de journalisation Strata avec une durée de conservation des journaux d'un an.



STEP 5 | Sélectionnez Cloud Identity Engine ou créez une nouvelle instance CIE pour identifier et vérifier tous les utilisateurs de votre infrastructure.

STEP 6 | Cliquez sur **Agree to the Terms and Conditions (Accepter les conditions générales)**, puis sur **Activate (Activer)**.

STEP 7 | Attendez que Strata Cloud Manager, Cloud Identity Engine et le service de journalisation Strata s'initialisent et que leur état indique Complete (Terminé).



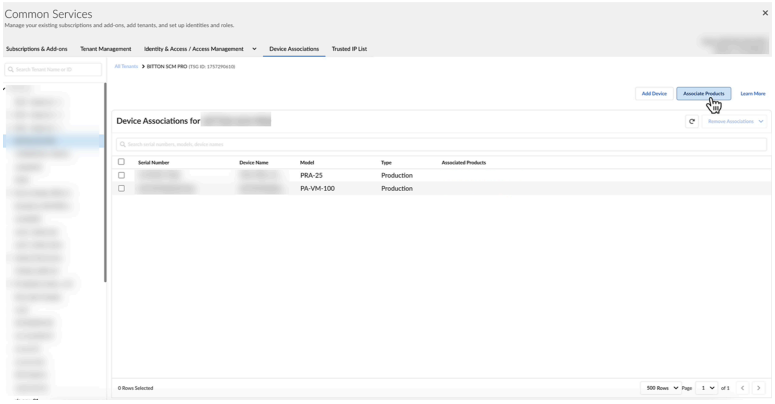
STEP 8 | Associez des périphériques NGFW, Panorama ou les deux à un locataire contenant votre Strata Cloud Manager.

Assurez-vous d'associer tous les pare-feu gérés par Panorama individuellement au locataire.

1. Accédez à **Common Services (Services communs) > Device Associations (Associations de périphériques)**.
2. **Ajoutez des périphériques.**
3. Sélectionnez un ou plusieurs pare-feu ou appareils Panorama, puis **Save (Enregistrer)**.

STEP 9 | Associez des produits aux périphériques. Après avoir activé Strata Cloud Manager Pro, vous devez spécifier les pare-feu ou appareils Panorama que vous souhaitez utiliser avec la solution.

1. Accédez à **Common Services (Services communs) > Device Associations (Associations de périphériques)**.
2. **Associate Products (Associer des produits)**.



3. Dans la colonne de sélection des produits, sélectionnez **Strata Cloud Manager**.
4. Sélectionnez des périphériques et cliquez sur **Save (Enregistrer)**.

STEP 10 | Activez la télémétrie sur des périphériques. Strata Cloud Manager évalue la santé des périphériques de votre déploiement en analysant les données de télémétrie que vos périphériques PAN-OS envoient au service de journalisation Strata. Pour envoyer ces données, vous devez avoir activé la télémétrie de périphérique sur vos périphériques.

À partir de PAN-OS 12.1.2, 11.1.11, 11.2.8, 10.2.17 et des versions ultérieures, la fonctionnalité d'activation automatique de la télémétrie configure la télémétrie de sorte qu'elle soit activée par défaut sur vos périphériques. Lors de l'intégration d'un nouveau périphérique (Panorama ou pare-feu), la télémétrie est automatiquement activée avec des paramètres contrôlés de manière centralisée via Strata Cloud Manager ou le Hub.

STEP 11 | Connectez-vous à Strata Cloud Manager en cliquant sur son icône dans le hub.

Activer Strata Cloud Manager Pro pour Prisma Access

Tous les types de licence Prisma Access incluent l'accès à Strata Cloud Manager, et tous les déploiements de Prisma Access peuvent tirer parti de Strata Cloud Manager pour des fonctionnalités de visibilité (par exemple, le centre de commande et les informations sur l'activité) et la surveillance du DEM autonome.

De plus, vous pouvez choisir d'utiliser Strata Cloud Manager pour votre gestion de la configuration Prisma Access ; vous pouvez également utiliser Panorama pour la gestion de la configuration. Dans les deux cas, vous serez guidé pour activer Strata Cloud Manager Pro lors de l'activation de votre licence Prisma Access :

- Activer Prisma Access, avec la gestion de la configuration Strata Cloud Manager
- Activer Prisma Access, avec la gestion de la configuration Panorama

Activer Strata Cloud Manager Pro pour des modèles VM-Series financés par des crédits NGFW logiciels

Vous pouvez gérer les pare-feu VM-Series financés par des crédits NGFW logiciels en utilisant Strata Cloud Manager et ainsi bénéficier d'un accès fluide aux fonctionnalités avancées de gestion et de surveillance grâce à l'activation de Strata Cloud Manager Pro.

Strata Cloud Manager prend en charge la gestion à la fois des pare-feu VM-Series autonomes et des déploiements VM-Series gérés par Panorama, offrant une solution complète pour superviser plusieurs environnements :

- Activer Strata Cloud Manager Pro pour les pare-feu VM-Series
- Activer Strata Cloud Manager Pro pour les pare-feu VM-Series gérés par Panorama

Activer Strata Cloud Manager Pro avec le contrat de licence d'entreprise

Cette tâche montre comment activer le contrat de licence d'entreprise (ELA) pour Strata Cloud Manager. Le module complémentaire pour l'ELA est un modèle de consommation pour les grandes entreprises permettant d'attribuer des abonnements en masse aux ressources achetées auprès de Palo Alto Networks.

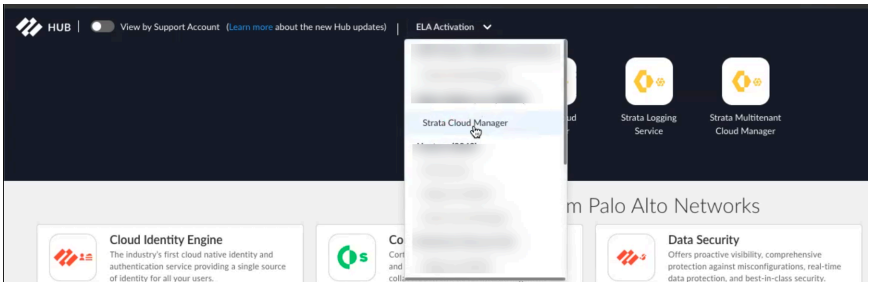
Voici les prérequis pour NGFW :

- **Prérequis pour l'intégration à la gestion cloud** : avant d'intégrer votre NGFW à Strata Cloud Manager, vérifiez que toutes les conditions de préparation du périphérique sont remplies. Cela inclut la configuration réseau, la compatibilité logicielle et les exigences de licence. Suivez ces étapes pour vous assurer que votre pare-feu est géré avec succès à l'aide de Strata Cloud Manager.
- **Ports TCP et FQDN pour la gestion cloud** : pour permettre une communication fluide entre le NGFW et Strata Cloud Manager, configurez des ports TCP spécifiques et des Fully Qualified Domain Name (nom de domaine complet - FQDN).

*Vous pouvez activer plusieurs locataires Strata Cloud Manager Pro en utilisant la même licence pour des périphériques appartenant aux mêmes comptes de support. Pour ce faire, accédez à la Gestion des locataires pour créer de nouveaux locataires. Accédez ensuite à **Subscriptions & Add-ons (Abonnements et modules complémentaires)** et recherchez votre abonnement, puis cliquez sur **Activate Cloud Tenant (Activer le locataire Cloud)** qui vous redirigera vers la page d'activation. Choisissez le même TSG sur la page d'activation que celui que vous avez utilisé initialement.*

STEP 1 | Utilisez l'une des méthodes d'activation suivantes.

- Connectez-vous au hub et sélectionnez **ELA Activation (Activation ELA)** > **Strata Cloud Manager**.



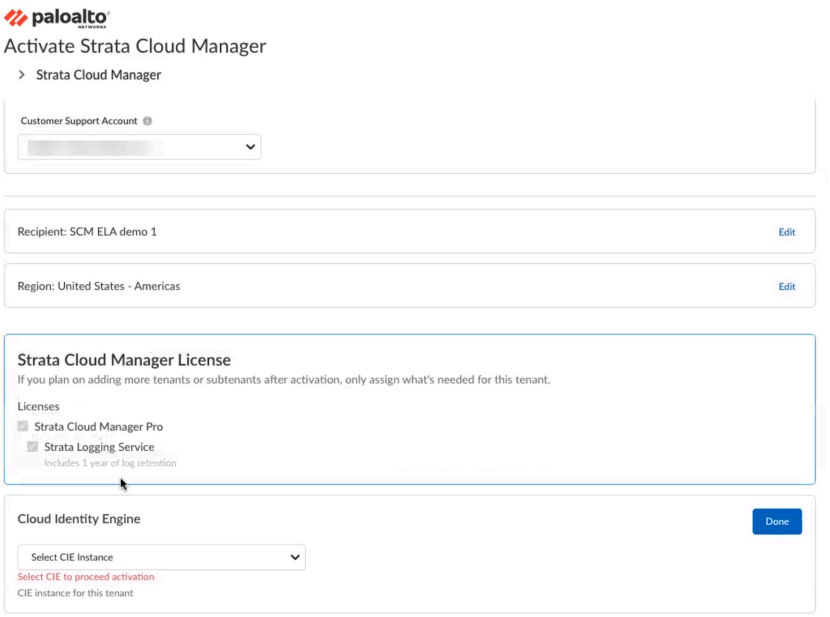
- Connectez-vous au portail de support client et procédez à l'activation en accédant à **License Management (Gestion des Licences)** > **Licenses (Licences)**, puis en cliquant sur **ELA-Ngfw Activation (Activation ELA-Ngfw)**.

STEP 2 | Choisissez le compte de support client que vous souhaitez utiliser.

STEP 3 | Dans **Select Tenant (Sélectionner le locataire)**, choisissez le locataire où vous allez activer Strata Cloud Manager Pro. Si vous n'avez pas de locataire existant, sélectionnez **Create New (Créer nouveau)**.

STEP 4 | Sélectionnez la **région** où vous souhaitez déployer Strata Cloud Manager. Voir les régions prises en charge pour Strata Cloud Manager.

Strata Cloud Manager Pro inclut le service de journalisation Strata avec une durée de conservation des journaux d'un an.



STEP 5 | Sélectionnez Cloud Identity Engine ou créez une nouvelle instance CIE pour identifier et vérifier tous les utilisateurs de votre infrastructure.

STEP 6 | Cliquez sur **Agree to the Terms and Conditions (Accepter les conditions générales)**, puis sur **Activate (Activer)**.

STEP 7 | Attendez que Strata Cloud Manager et le service de journalisation Strata s'initialisent et que l'état d'activation des deux affiche Complete (Terminé).

STEP 8 | Associez des périphériques NGFW, Panorama ou les deux à un locataire contenant votre Strata Cloud Manager.

Assurez-vous d'associer tous les pare-feu gérés par Panorama individuellement au locataire.

1. Accédez à **Common Services (Services communs) > Device Associations (Associations de périphériques)**.
2. **Ajoutez des périphériques.**
3. Sélectionnez un ou plusieurs pare-feu ou appareils Panorama, puis **Save (Enregistrer)**.

STEP 9 | Associez des produits aux périphériques. Après avoir activé Strata Cloud Manager Pro, vous devez spécifier les pare-feu ou appareils Panorama que vous souhaitez utiliser avec la solution.

1. Connectez-vous au hub et sélectionnez **Common Services (Services communs) > Device Associations (Associations de périphériques**.
2. **Associate Products (Associer des produits)**.
3. Dans la colonne de sélection des produits sous licence, sélectionnez **Strata Cloud Manager**.
4. Sélectionnez des périphériques et cliquez sur **Save (Enregistrer)**.

STEP 10 | Activez la télémétrie sur des périphériques. Strata Cloud Manager évalue la santé des périphériques de votre déploiement en analysant les données de télémétrie que vos périphériques PAN-OS envoient au service de journalisation Strata. Pour envoyer ces données, vous devez avoir activé la télémétrie de périphérique sur vos périphériques.

À partir de PAN-OS 12.1.2, 11.1.11, 11.2.8, 10.2.17 et des versions ultérieures, la fonctionnalité d'activation automatique de la télémétrie configure la télémétrie de sorte qu'elle soit activée par défaut sur vos périphériques. Lors de l'intégration d'un nouveau périphérique (Panorama ou pare-feu), la télémétrie est automatiquement activée avec des paramètres contrôlés de manière centralisée via Strata Cloud Manager ou le Hub.

STEP 11 | Connectez-vous à Strata Cloud Manager en cliquant sur son icône dans le hub.

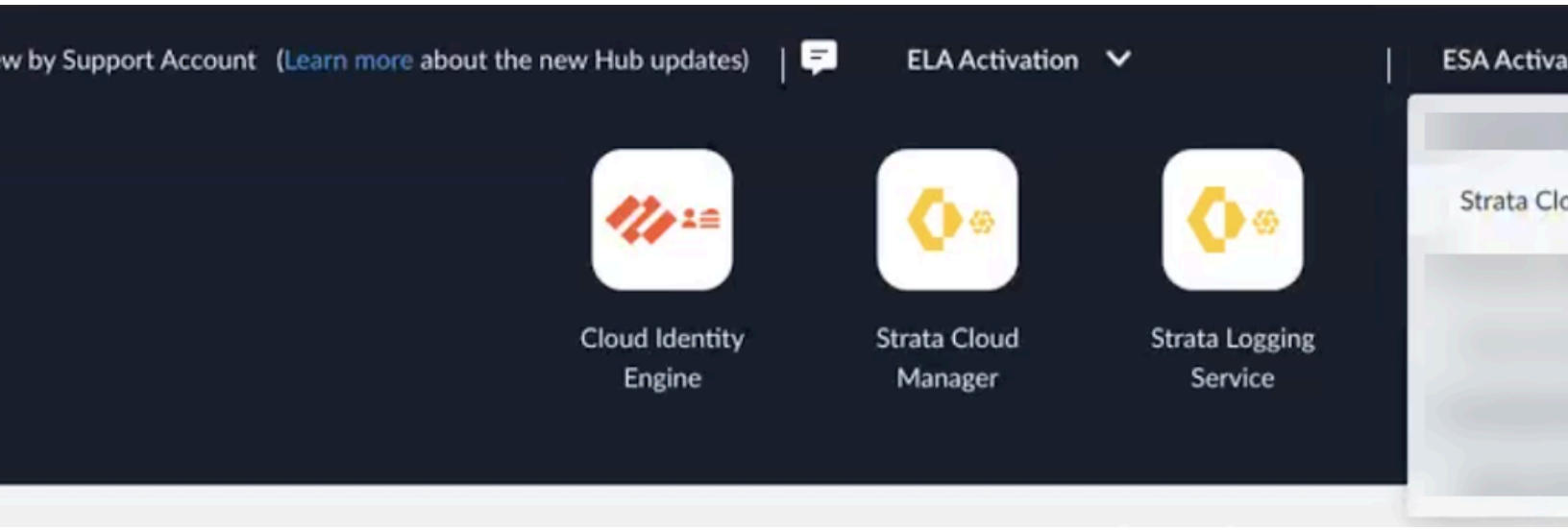
Activez Strata Cloud Manager Pro avec le contrat de licence d'entreprise

Le contrat de licence d'entreprise (ESA) Pro de Palo Alto Networks inclut Strata Cloud Manager Pro pour NGFW. Le contrat ESA Pro fournit une solution simplifiée pour une expérience de support cohérente à travers vos ressources existantes et vos achats prévus. Ce programme d'entreprise permet aux organisations de maximiser les économies et les avantages à mesure qu'elles se développent, ce qui en fait un choix idéal pour les clients disposant de grands déploiements de pare-feu en expansion.

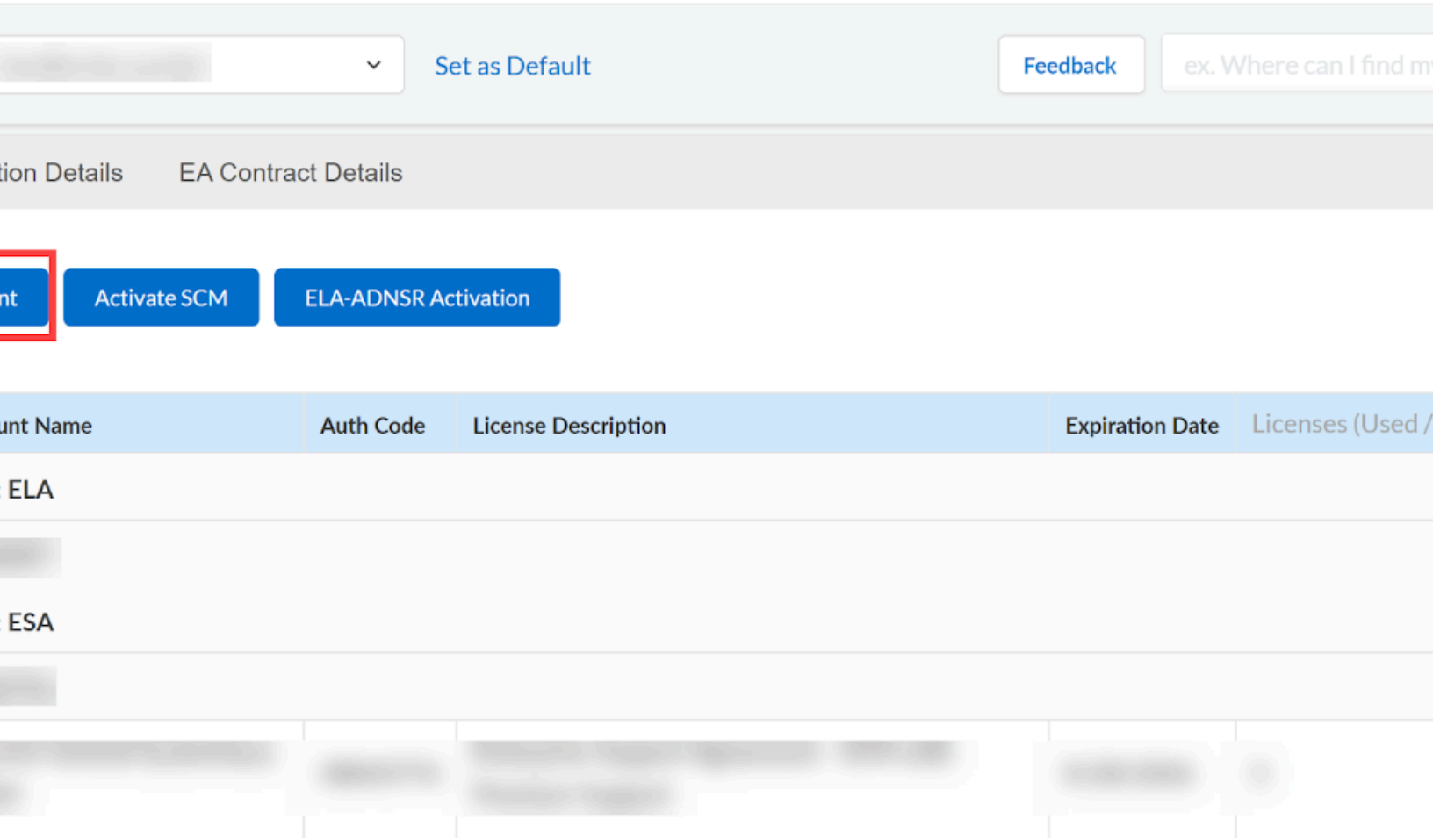
Cette tâche montre comment activer le contrat ESA Pro pour Strata Cloud Manager. Vous pouvez commencer le processus d'activation d'ESA Pro depuis le hub ou le portail de support client comme décrit ci-dessous.

STEP 1 | Utilisez l'une des méthodes d'activation suivantes :

- Connectez-vous au hub et sélectionnez **ESA Activation (Activation ESA)** > **Strata Cloud Manager**.

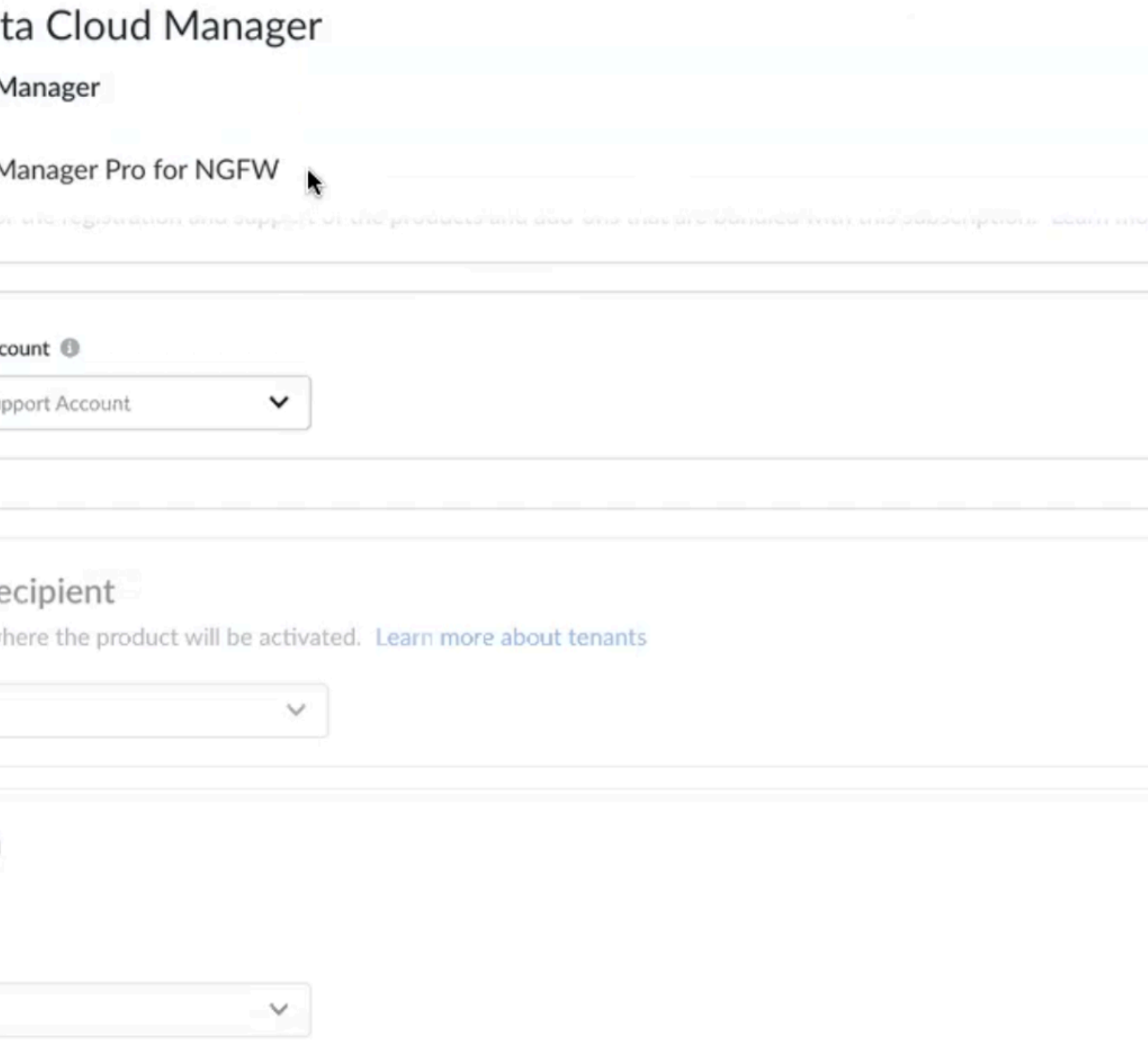


- Ouvrez une session dans le portail de support client. Dans le volet latéral gauche, accédez à **License Management (Gestion des Licences)**, puis sous **Licenses (Licences)**, sélectionnez **Activate Enterprise Agreement (Activer un contrat d'entreprise)**.



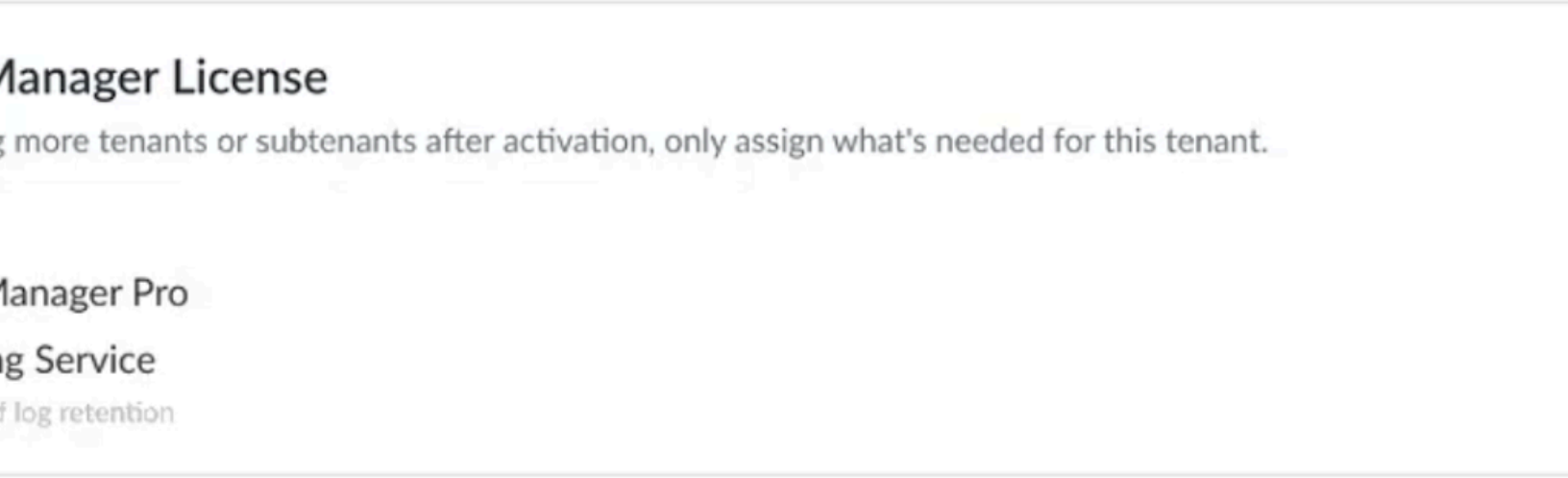
STEP 2 | Choisissez le compte de support client que vous souhaitez utiliser.

STEP 3 | Cliquez sur **New (Nouveau)** pour créer un nouveau locataire où vous activerez l'instance de Strata Cloud Manager.



STEP 4 | Sélectionnez la **région** où vous souhaitez déployer Strata Cloud Manager. Voir les régions prises en charge pour Strata Cloud Manager.

Une licence Strata Cloud Manager Pro inclut le service de journalisation Strata avec une durée de conservation des journaux d'un an.



STEP 5 | Sélectionnez Cloud Identity Engine ou créez une nouvelle instance CIE pour identifier et vérifier tous les utilisateurs de votre infrastructure.

STEP 6 | Cliquez sur **Agree to the Terms and Conditions (Accepter les conditions générales)**, puis sur **Activate (Activer)**.

STEP 7 | Attendez que Strata Cloud Manager et le service de journalisation Strata s'initialisent et que l'état d'activation des deux affiche Complete (Terminé).

STEP 8 | Associez des périphériques NGFW, Panorama ou les deux à un locataire contenant votre Strata Cloud Manager.

Assurez-vous d'associer tous les pare-feu gérés par Panorama individuellement au locataire.

1. Accédez à **Common Services (Services communs) > Device Associations (Associations de périphériques)**.
2. **Ajoutez des périphériques.**
3. Sélectionnez un ou plusieurs pare-feu ou appareils Panorama, puis **Save (Enregistrer)**.

STEP 9 | Associez des produits aux périphériques. Après avoir activé Strata Cloud Manager Pro, vous devez spécifier les pare-feu ou appareils Panorama que vous souhaitez utiliser avec la solution.

1. Connectez-vous au hub et sélectionnez **Common Services (Services communs) > Device Associations (Associations de périphériques**.
2. **Associate Products (Associer des produits)**.
3. Dans la colonne de sélection des produits sous licence, sélectionnez **Strata Cloud Manager**.
4. Sélectionnez des périphériques et cliquez sur **Save (Enregistrer)**.

STEP 10 | Activez la télémétrie sur les périphériques. Strata Cloud Manager évalue la santé des périphériques de votre déploiement en analysant les données de télémétrie que vos périphériques PAN-OS envoient au service de journalisation Strata. Pour envoyer ces données, vous devez avoir activé la télémétrie de périphérique sur vos périphériques.

À partir de PAN-OS 12.1.2, 11.1.11, 11.2.8, 10.2.17 et des versions ultérieures, la fonctionnalité d'activation automatique de la télémétrie configure la télémétrie de sorte qu'elle soit activée par défaut sur vos périphériques. Lors de l'intégration d'un nouveau périphérique (Panorama ou pare-feu), la télémétrie est automatiquement activée avec des paramètres contrôlés de manière centralisée via Strata Cloud Manager ou le Hub.

STEP 11 | Connectez-vous à Strata Cloud Manager en cliquant sur son icône dans le hub.

Migrer de Panorama vers Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (Managed by Panorama) • Prisma Access (Managed by Panorama)	Migration des NGFW : ☐ Licence Strata Cloud Manager Essentials ou Pro ☐ Assurez-vous que vos NGFW répondent aux prérequis pour la gestion cloud Migration de Prisma Access : ☐ Licence Prisma Access ☐ Pour commencer la migration de Prisma Access (géré par Panorama) vers Prisma Access (géré par Strata Cloud Manager), contactez l'équipe de compte Palo Alto Networks

La migration de Panorama vers Strata Cloud Manager est désormais disponible pour les déploiements Prisma Access et NGFW, vous permettant de bénéficier de la gestion cloud et de la gestion de configuration partagée dans l'environnement cloud. Le processus de migration prend en compte des considérations telles que la préservation de la configuration et la continuité des politiques.

Pour les déploiements NGFW, vous pouvez suivre ce flux de travail pour examiner la compatibilité de configuration, même si vous n'êtes pas encore prêt à procéder à la migration. Vous pouvez décider de rogner ou d'accepter les fonctionnalités qui ne sont pas prises en charge ou qui sont partiellement prises en charge pour la gestion de la configuration Strata Cloud Manager. Lors de la migration, Strata Cloud Manager convertit les hiérarchies de groupes d'appareils Panorama en structures de dossiers Strata Cloud Manager correspondantes et convertit les modèles et piles de modèles Panorama en extraits réutilisables.

Pour les déploiements Prisma Access, les migrations se concentrent sur la préservation de votre infrastructure d'accès à distance, des configurations d'utilisateurs mobiles et de la connectivité site à site tout en transférant la supervision de la gestion à Strata Cloud Manager.

- Migration des pare-feu nouvelle génération :
- Migration de Prisma Access

Migrer de Panorama vers Strata Cloud Manager (NGFW)

Vous pouvez migrer vos configurations NGFW existantes de Panorama vers Strata Cloud Manager pour une gestion de la configuration basée sur le cloud.

Pendant la migration, Strata Cloud Manager :

- Copie et traduit les politiques de sécurité, les configurations réseau et les objets pris en charge.
- Maintient la topologie réseau existante et les déploiements NGFW.
- Met en évidence les zones partiellement prises en charge ou non prises en charge.

Contactez l'équipe de compte Palo Alto Networks pour activer le flux de travail de migration.

Gérer vos NGFW en utilisant Strata Cloud Manager au lieu de Panorama peut vous offrir des avantages tels qu'une gestion unifiée pour Prisma Access et les NGFW, une évolutivité native du cloud de votre réseau, et une visibilité améliorée.

Strata Cloud Manager vous guide à travers la migration de vos configurations grâce à ces étapes clés :

- Chargez les configurations existantes : importez vos configurations Panorama actuelles.
- Exécutez une évaluation de compatibilité : identifiez les fonctionnalités ou configurations non prises en charge qui nécessitent une attention particulière.
- Effectuez une validation et préparez-vous au déploiement : terminez les vérifications finales avant la migration.
- Contrôle de la migration : les appareils et groupes d'appareils peuvent être migrés par phases, vous permettant de migrer des appareils non critiques ou de procéder site par site.

Examinez les résultats à chaque étape, apportez les ajustements nécessaires et vérifiez que vos configurations sont entièrement compatibles avec Strata Cloud Manager avant de terminer la migration.

Comment la gestion de la configuration change lorsque vous passez de Panorama à Strata Cloud Manager

La gestion de la configuration Panorama est basée sur les éléments suivants :

- Groupes d'appareils : organisez les pare-feu en groupes hiérarchiques pour la gestion des politiques de sécurité (règles de sécurité, politiques NAT, filtres d'application).
- Modèles et piles de modèles : définissez les paramètres du réseau et des périphériques (interfaces, zones, routage, paramètres système).
- Héritage : les groupes d'appareils héritent des politiques des groupes parents ; les piles de modèles superposent plusieurs modèles avec des capacités de remplacement.

La gestion de la configuration Strata Cloud Manager est basée sur :

- Dossiers : conteneurs hiérarchiques qui contiennent à la fois des politiques de sécurité ET des configurations réseau.
- Extraits : blocs de configuration réutilisables qui peuvent être attachés à des dossiers à n'importe quel niveau.

- Conteneurs : titulaires de configuration spécifiques aux appareils pour des exigences de pare-feu uniques.

Lors de la migration, Strata Cloud Manager convertit votre configuration basée sur Panorama et la décompose en dossiers et extraits :

Panorama	Strata Cloud Manager
Groupes de périphériques	Dossiers
Modèles et piles de modèles	Extraits
Groupes de périphériques partagés	Dossier All Firewalls (Tous les pare-feu)
Objets partagés	Dossier global sous forme d'extrait attaché
Politiques dans les groupes d'appareils	Politiques sous le(s) dossier(s) mappé(s)
Objets (adresses, EDL, etc.)	Objets sous le(s) dossier(s) mappé(s)

Principale différence entre Panorama et Strata Cloud Manager à garder à l'esprit :

- Les dossiers de Strata Cloud Manager contiennent à la fois des configurations réseau et de sécurité, tandis que Panorama les divise en modèles et groupes d'appareils
- Les dossiers de Strata Cloud Manager offrent un héritage plus flexible avec des remplacements basés sur des extraits par rapport aux remplacements de groupe de niveau inférieur observés dans Panorama
- Les extraits de Strata Cloud Manager offrent une approche plus « plug-and-play » pour les configurations par rapport aux modèles et aux piles de modèles de Panorama qui sont hérités du haut vers le bas de la pile.

Après la migration, vous gérez les configurations via le modèle de dossier et d'extrait. L'ordre d'attachement des extraits détermine la priorité de configuration, offrant un contrôle granulaire sur la façon dont plusieurs sources de configuration se combinent. Vous pouvez également créer des conteneurs spécifiques aux périphériques pour les NGFW nécessitant des configurations uniques en dehors du modèle d'héritage de dossier.

Ressources supplémentaires

En savoir plus sur les Groupes d'appareils et les Modèles.

En savoir plus sur les Extraits et les Dossiers

Préparez la migration de vos NGFW vers Strata Cloud Manager

Avant de commencer la migration, assurez-vous que les éléments suivants sont prêts :

- Configuration logicielle minimale : PAN-OS 10.2.3 ou version ultérieure
- Exporter le fichier de configuration Panorama : exportez la configuration complète en cours d'exécution de votre instance Panorama source au format XML

- Clé principale Panorama : obtenez la clé principale utilisée pour le chiffrement dans votre configuration Panorama (si vous n'utilisez pas la clé par défaut)
- Locataire Strata Cloud Manager : vérifiez que votre locataire Strata Cloud Manager est déployé, qu'il dispose de la licence appropriée et qu'il est opérationnel
- Configuration NGFW : collectez les derniers fichiers de configuration transmis (fichiers de support technique) des NGFW que vous prévoyez de valider après la migration
- Topologie réseau : examinez vos hiérarchies de groupes d'appareils actuelles, les relations de modèles et les attributions de NGFW
- Sauvegarde de configuration : créez des sauvegardes complètes de vos configurations Panorama et NGFW actuelles par mesure de sécurité
- Accès administrateur : assurez-vous d'avoir accès au rôle de super utilisateur à la fois dans Panorama et Strata Cloud Manager.
- Planification de la migration : identifiez quels groupes d'appareils, modèles et NGFW vous souhaitez migrer dans votre phase initiale
- Matrice de compatibilité : comprenez quelles fonctionnalités peuvent ne pas être prises en charge dans Strata Cloud Manager et planifiez les ajustements de configuration nécessaires

Migrer vos NGFW gérés par Panorama vers Strata Cloud Manager

Migrez vos configurations NGFW de Panorama vers Strata Cloud Manager :

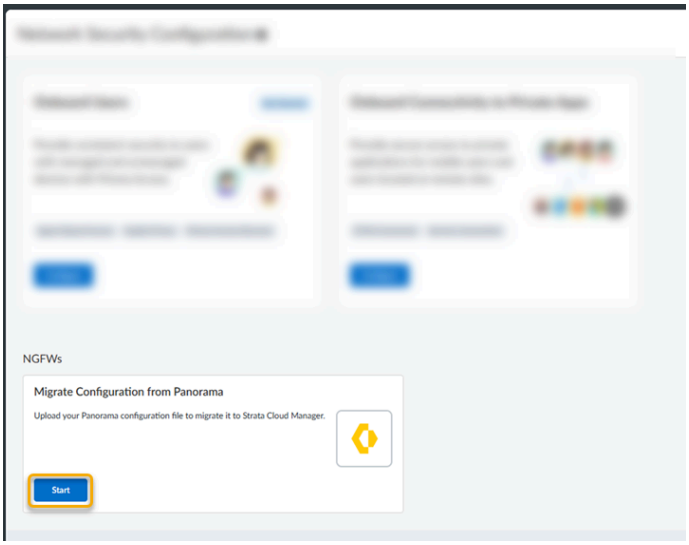
STEP 1 | Préparez votre Panorama pour la migration.

1. Connectez-vous au Panorama qui gère vos NGFW avec un compte d'administration auquel le rôle de super utilisateur est attribué.
2. **(Facultatif)** Si vous avez configuré une clé principale personnalisée pour Panorama, notez-la.

   Si votre déploiement utilise la clé principale par défaut, cette étape n'est pas requise.
3. Assurez-vous que la configuration actuelle de Panorama est à jour et que vous avez validé et transmis toutes les modifications actuelles à Panorama en accédant à **Commit (Valider)** > **Commit & Push (Valider et appliquer)** et sélectionnez **Preview Changes (Prévisualiser les modifications)**.
4. **(Facultatif)** Vérifiez les différences entre la configuration en cours d'exécution et la configuration candidate, puis décidez si vous souhaitez appliquer ces modifications. Pour valider et appliquer les modifications, sélectionnez **Edit Selections (Modifier les sélections)**, puis sélectionnez les NGFW que vous souhaitez appliquer dans **Push Scope (Étendue de la transmission)**.
5. **(Facultatif)** Sélectionnez **Commit and Push (Valider et appliquer)** pour valider et appliquer les modifications.
6. Accédez à **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et sélectionnez **Export the named Panorama configuration snapshot (Exporter l'instantané de configuration Panorama nommé)**.

   Le fichier .xml doit être chargé sur Strata Cloud Manager pendant le processus de migration. Chargez uniquement le fichier de configuration .xml ; ne chargez pas de fichiers de support technique ni aucun autre fichier.
7. Sélectionnez le fichier de configuration **running-config.xml**, puis cliquez sur **OK**.

STEP 2 | Connectez-vous à Strata Cloud Manager en tant qu'administrateur avec un rôle de super utilisateur et accédez à **Configuration (Configuration)** > **Onboarding (Intégration)**.

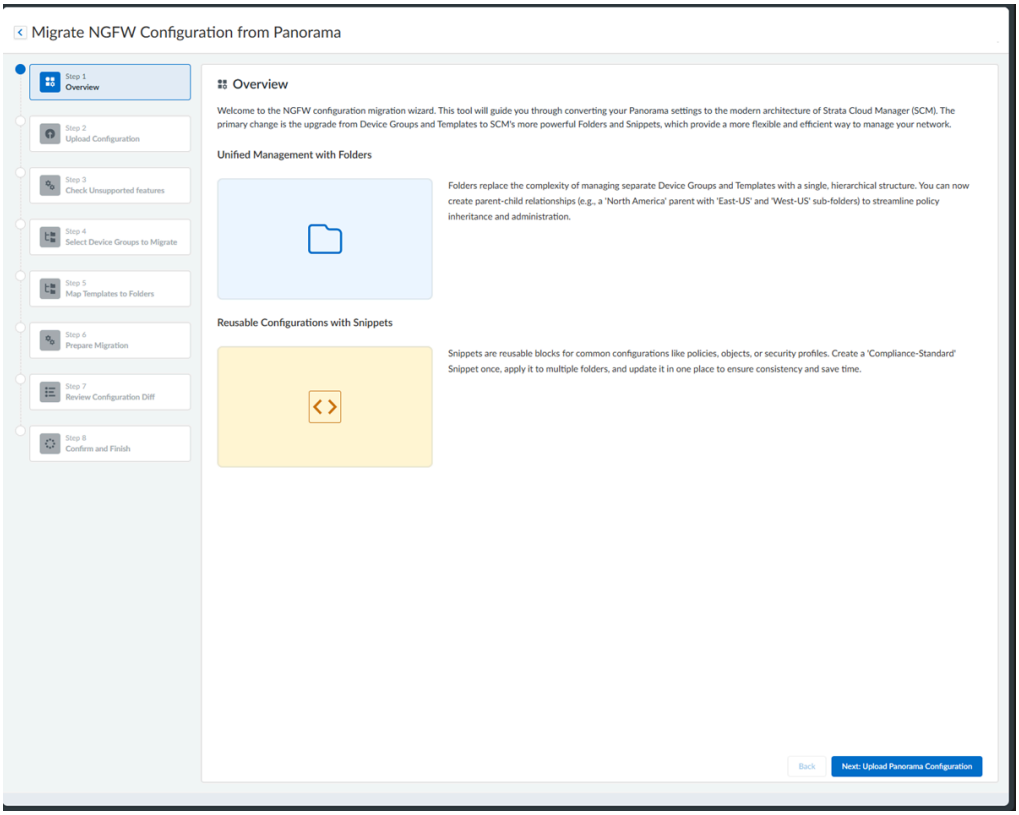


Le programme de migration détecte que vous disposez d'un déploiement géré par Panorama.

1. Confirmez que le locataire est correct.
2. (Facultatif) Créez un instantané nommé de votre configuration en cours au cas où une restauration serait nécessaire.

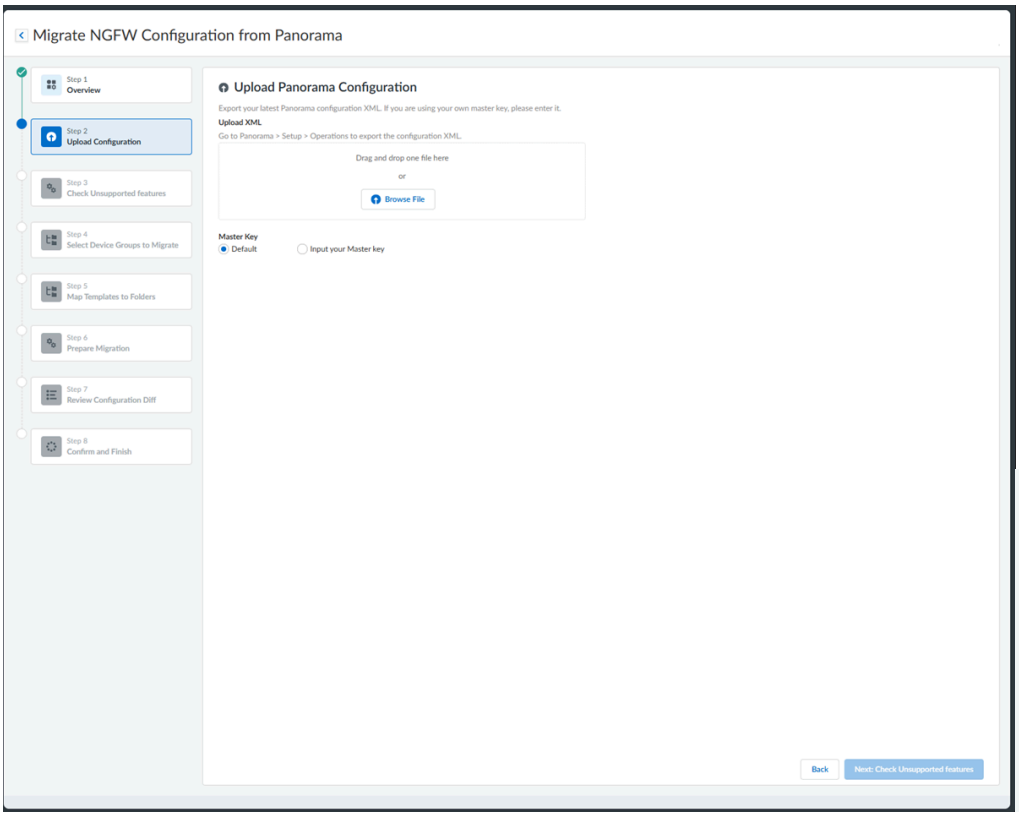
La migration ne doit pas être tentée pendant une fenêtre de mise à niveau de Strata Cloud Manager. Consultez votre calendrier de mise à niveau pour voir si une mise à niveau est prévue.

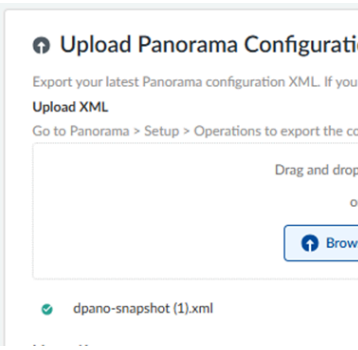
STEP 3 | Lisez la section **Overview (Vue d'ensemble)** de la migration.



1. Examinez les composants de base de la gestion de Strata Cloud Manager : les **Folders (Dossiers)** et les **Snippets (Extraits)**.
2. Cliquez sur **Next: Upload Panorama Configuration (Suivant : Télécharger la configuration Panorama)**.

STEP 4 | Téléchargez la configuration Panorama.

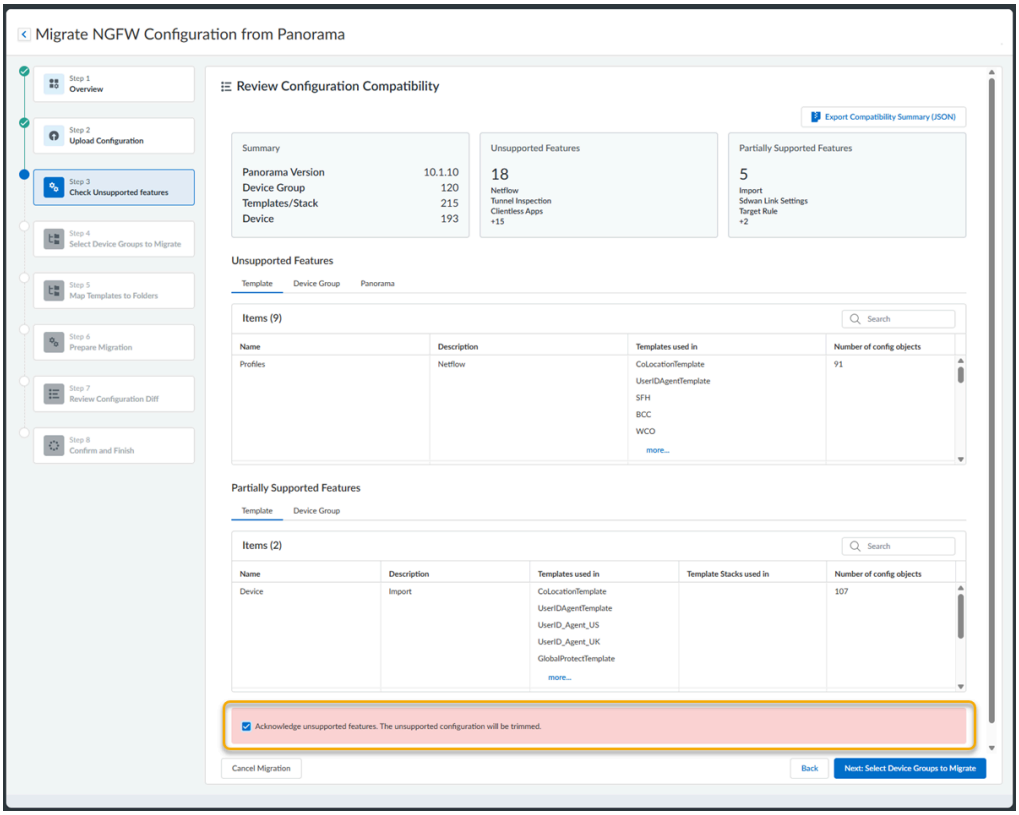




1. Sélectionnez le fichier *.xml* de configuration Panorama que vous avez téléchargé au cours d'une précédente étape en le faisant glisser et en le déposant depuis l'explorateur de fichiers ou en sélectionnant l'option **Choose File (Choisir un fichier)**.
2. **(Facultatif)** Saisissez votre **Master Key (Clé principale)** ou, si vous n'avez pas créé de clé principale personnalisée, utilisez la clé principale **Default (Par défaut)**.

3. Cliquez sur **Next: Review Migration Compatibility (Suivant : Examiner la compatibilité de migration)**.

STEP 5 | Examiner la compatibilité de configuration.



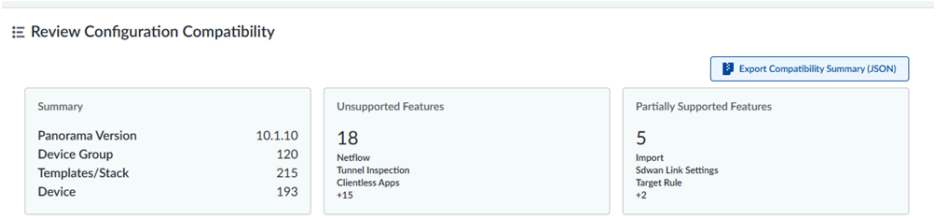
1. **(Facultatif)** Cliquez sur **Export Compatibility Summary (Exporter le résumé de compatibilité)** et examinez la compatibilité de configuration de votre organisation avant

de continuer et de permettre à Strata Cloud Manager de rogner toute configuration non prise en charge ou partiellement prise en charge.

Le rognage des fonctionnalités non prises en charge et partiellement prises en charge évite la migration des fonctionnalités qui ne peuvent pas être déployées en toute sécurité dans Strata Cloud Manager.

Ce processus n'impactera que la configuration organisée pour Strata Cloud Manager. Les configurations dans Panorama resteront inchangées.

Pour chaque zone signalée, vous devez prévoir de reconstruire, remplacer ou différer ces configurations.



2. Examinez les **Unsupported Features (Fonctionnalités non prises en charge)** qui seront rognées de votre configuration pendant la migration.

   Ces fonctionnalités seront rognées de vos configurations et ne seront pas organisées dans Strata Cloud Manager pendant le processus de migration de configuration.
3. Examinez la section **Partially Supported Features (Fonctionnalités partiellement prises en charge)** et déterminez un chemin de résolution.

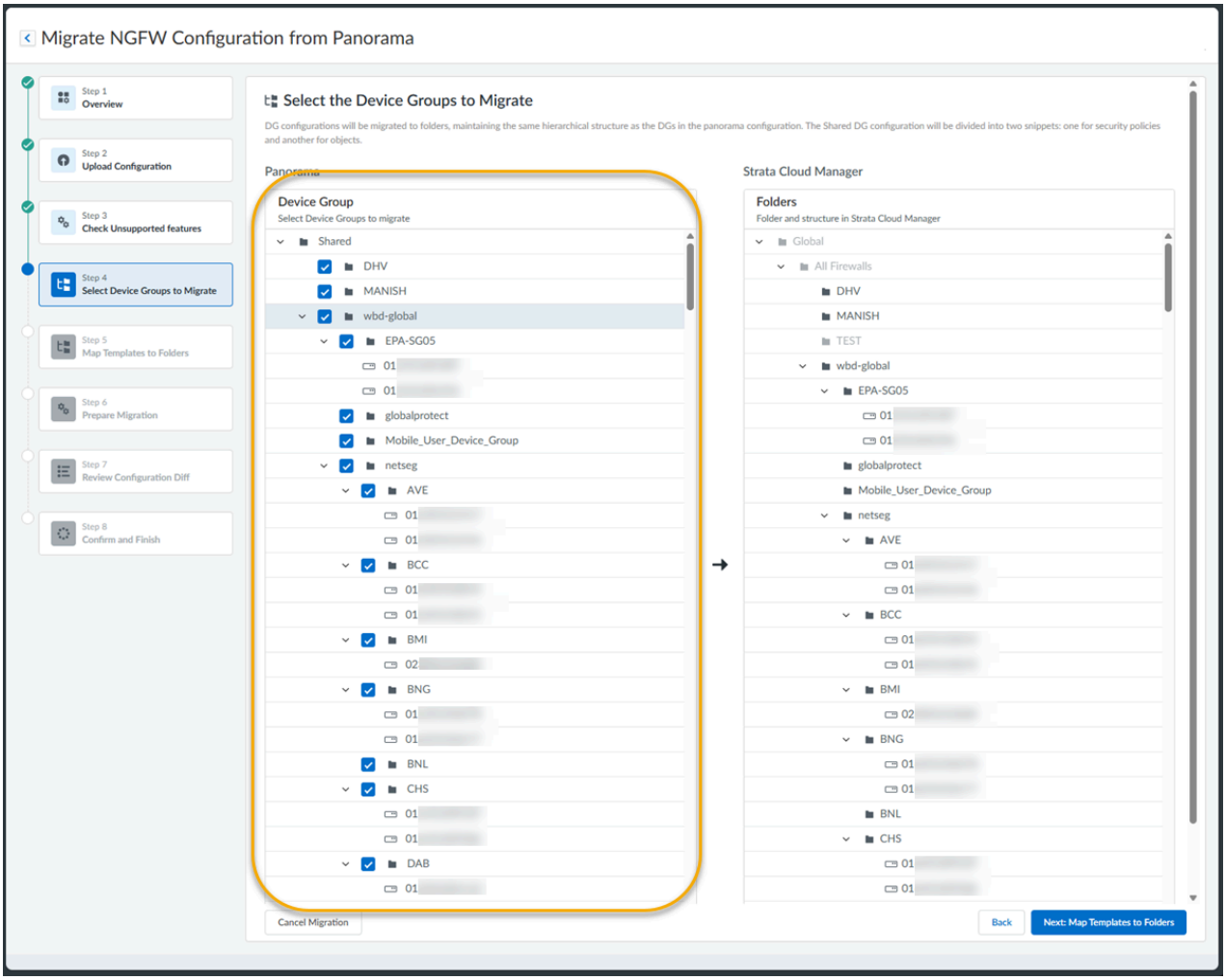
   Identifiez les éléments exacts qui seront absents de la configuration.

   Vous pouvez accepter les fonctionnalités partiellement prises en charge et élaborer un plan de correction après la migration ou revenir à votre configuration Panorama et nettoyer ces zones avant de recommencer le processus de migration.
4. Cliquez sur **Acknowledge (Accepter)** pour accepter les fonctionnalités non prises en charge et partiellement prises en charge.
5. Cliquez sur **Next: Select Device Groups to Migrate (Suivant : Sélectionner les groupes d'appareils à migrer)**.

Pour ceux qui cherchent simplement à comparer les configurations prises en charge ou s'il est décidé qu'une planification supplémentaire est nécessaire, vous pouvez mettre fin au processus de migration ici.

STEP 6 | Faites votre choix parmi **Devices (Périphériques)** ou **Device Groups (Groupes d'appareils)** pour sélectionner les appareils ou groupe d'appareils à migrer.

Si vous migrez des NGFW depuis Panorama pour la première fois, il est recommandé de migrer d'abord des périphériques ou groupes d'appareils non critiques pour voir comment vos configurations seront migrées vers Strata Cloud Manager.

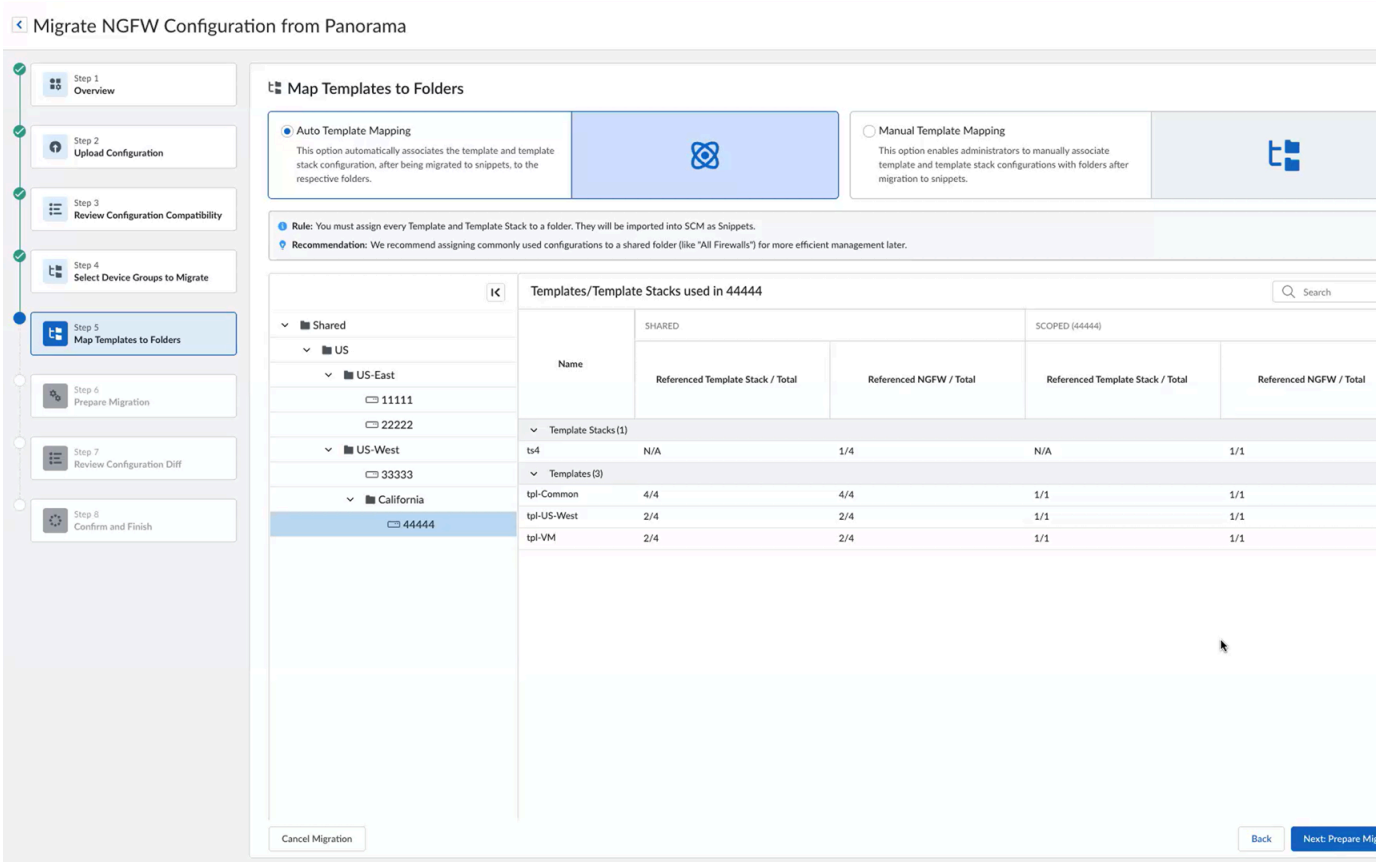


Pendant la migration :

- Les objets sont importés dans un extrait et attachés au dossier global.
- Les politiques sont importées sous le(s) dossier(s) migrés par le flux de travail.
- Les groupes d'appareils partagés sont automatiquement mappés au dossier All Firewalls (Tous les pare-feu).

1. Cliquez sur **Next: Map Templates to Folders (Suivant : Mapper les modèles aux dossiers)**.

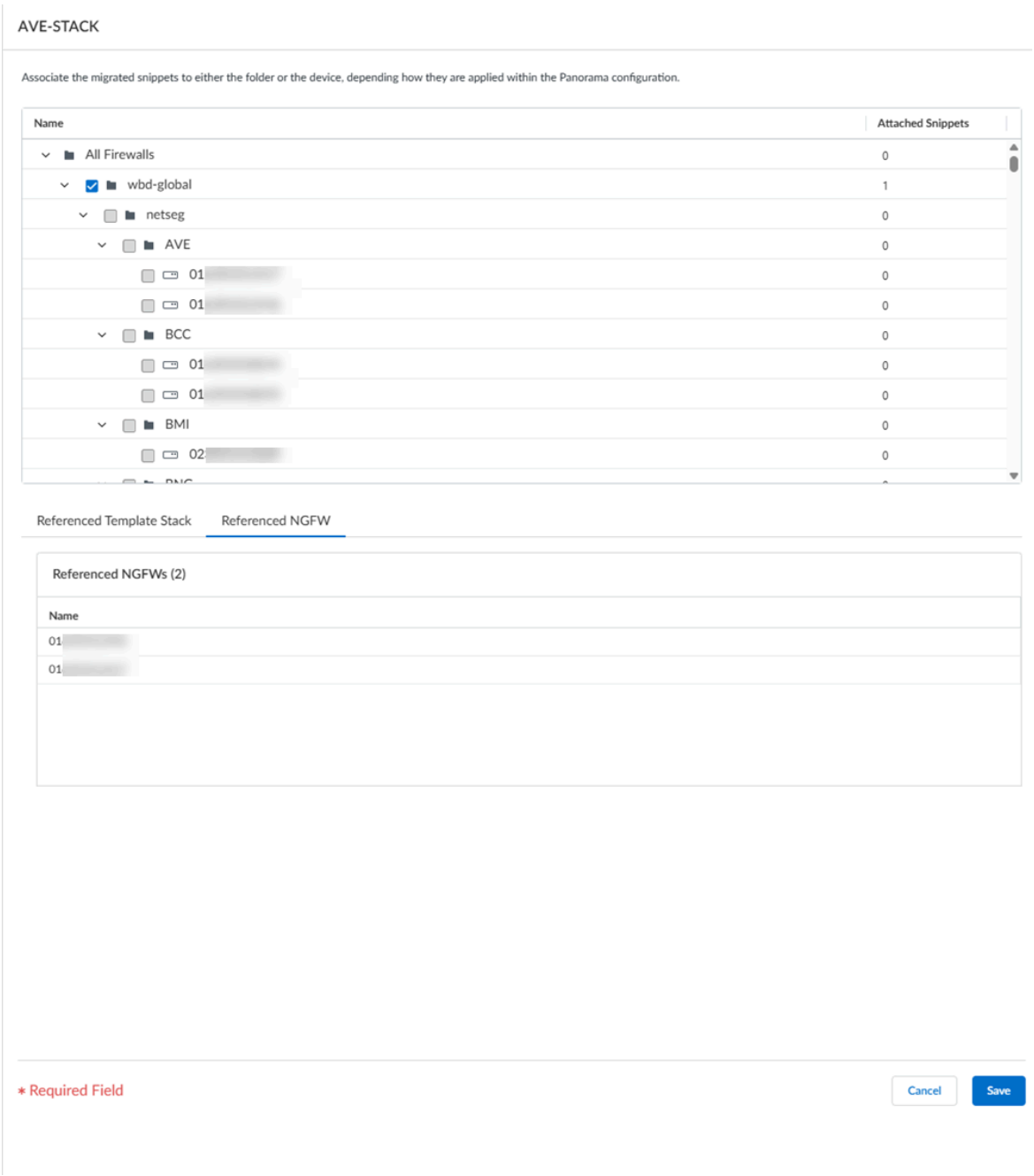
STEP 7 | Mappez des **Templates (Modèles)** à vos **Folders (Dossiers)** nouvellement configurés.



Pendant la migration, les **Templates (Modèles)** sont configurés en **Snippets (Extraits)** équivalents.

Si deux groupes d'appareils ou plus réutilisent le même modèle, élevez-le à un dossier supérieur. Si un seul site en a besoin, conservez-le au niveau du site.

1. Sélectionnez un **Device Group (Groupe d'appareils)** pour révéler les **Templates/ Template Stacks (Modèles / piles de modèles)** utilisés par ce groupe d'appareils.



2. Cliquez sur **Edit (Modifier)** pour modifier le mappage afin d'attribuer chaque **Template/ Template Stack (Modèle / pile de modèles** à un **Folder (Dossier)**.
3. Élevez les modèles référencés à plusieurs endroits vers des dossiers supérieurs.

   Par exemple, si vous avez défini des paramètres de modèle généraux, le fait de les mapper au dossier All Firewalls (Tous les pare-feu) établit ces paramètres comme la source de vérité pour tous les NGFW.
4. Après avoir attribué plusieurs extraits à un dossier, ajustez l'ordre.
5. Cliquez sur **Move Up (Déplacer vers le haut)** ou **Move Down (Déplacer vers le bas)** pour finaliser l'ordre.
6. Cliquez sur **Update (Mettre à jour)** pour mettre à jour l'ordre.

7. Cliquez sur **Save (Enregistrer)** pour enregistrer le nouvel ordre.

   Avant de passer à l'étape suivante, vérifiez ce qui suit :

   - Il ne reste aucun modèle ni aucune pile de modèles non attribués.
   - Tous les modèles référencés par plusieurs groupes d'appareils ont été élevés vers les dossiers appropriés.

8. Cliquez sur **Next: Prepare Migration (Suivant : Préparer la migration)**.

   Le processus de migration commence.

   Attendez que toutes les étapes soient terminées.

   Si vous rencontrez un problème lors de la migration, revenez aux étapes précédentes pour évaluer la situation et apporter des modifications. Si le problème persiste, veuillez contacter le support de Palo Alto Networks.

STEP 8 | Préparez la migration.

1. **Load Configuration to Strata Cloud Manager (Charger la configuration dans Strata Cloud Manager)** pour préparer la migration.

   1. Le flux de travail de migration :

      - Traduit les appareils et groupes d'appareils ainsi que les modèles et piles de modèles en dossiers et extraits en utilisant l'ordre que vous avez défini pour les mappages et extraits.
      - Crée un instantané de Strata Cloud Manager pour permettre la restauration des modifications organisées.
      - Vérifie l'absence de conflits dans les configurations Strata Cloud Manager existantes (collisions de noms, références manquantes, limites de 31 caractères, étendue du CABR).
      - Crée la configuration organisée qui figurera dans Strata Cloud Manager après le chargement.

2. Cliquez sur **Load Results (Télécharger les résultats)** pour examiner les objets, politiques ou extraits créés, mis à jour ou ignorés.
3. Cliquez sur **Validation Results (Résultats de validation)** pour consulter les résultats de validation et examiner les erreurs, avertissements et messages d'information après la migration.
4. Cliquez sur **Next: Review Config Diffs (Suivant : Examiner les différences de configuration)**.

   La configuration nouvellement générée est validée dans Strata Cloud Manager.

STEP 9 | Examinez les différences de configuration.

1. Dans l'arborescence des dossiers à gauche, développez le dossier et sélectionnez un numéro de série de NGFW à valider.
2. Cliquez sur **Browse File (Parcourir le fichier)** et choisissez le TSF pour le numéro de série sélectionné.

   En téléchargeant le TSF pour le NGFW choisi, vous pourrez valider correctement toutes les configurations prises en charge, partiellement prises en charge et non prises en charge.

   Veillez à rechercher tout ce qui a été créé, modifié ou supprimé. Les configurations rognées n'ont rien de surprenant.

   En raison des conventions de nommage dans Strata Cloud Manager, certains noms longs seront compressés si nécessaire.
3. Examinez les volets des différences de configuration.
   1. Volets verts : éléments créés ou ajoutés. Ils sont présents dans Strata Cloud Manager, mais pas sur le périphérique d'origine.
   2. Volets rouges : éléments supprimés ou rognés. Ils peuvent ne pas être pris en charge dans Strata Cloud Manager, mais se trouvent sur le périphérique.
   3. Volets jaunes : éléments modifiés.

   La vue des différences peut être étendue, limitée à un NGFW à la fois et calculée à partir du dernier XML transmis par le TSF.
4. Vérifiez les différences pour des périphériques représentatifs de chaque type de modèle ou de site.
5. (Facultatif) Cliquez sur **Export (Exporter)** pour exporter les résultats des différences.
6. (Facultatif) Cliquez sur **Regenerate Diffs (Régénérer les différences)** si des corrections ont été apportées.
7. Cliquez sur **Next: Confirm and Finish (Suivant : Confirmer et terminer)**.

STEP 10 | Cliquez sur **Confirm (Confirmer)** pour terminer les migrations de NGFW vers Strata Cloud Manager.

Maintenant que la migration est terminée, consultez la documentation disponible pour Strata Cloud Manager.

1. Assurez-vous que les résultats des étapes 8 et 9 sont acceptés.
2. Cliquez sur **Confirm (Confirmer)** pour confirmer la migration.

   La migration est officiellement marquée comme terminée.
3. (Facultatif) Pour rétablir la configuration à l'état précédant la migration, vous pouvez sélectionner **Revert (Rétablir)** à tout moment. Un flux de travail de restauration est alors lancé pour rétablir Strata Cloud Manager à un instantané pris avant le chargement de la migration.
4. (Facultatif) Pour annuler la migration à tout moment, sélectionnez **Cancel Migration (Annuler la migration)**. Le processus de migration est alors interrompu et les modifications temporaires annulées.

Migrer de Panorama vers Strata Cloud Manager (Prisma Access)

Si vous disposez d'un déploiement Prisma Access dont la configuration est gérée par Panorama et que vous souhaitez migrer vers Strata Cloud Manager pour la gestion de la configuration, Palo Alto Networks propose un flux de travail intégré au produit qui vous permet de migrer la configuration Prisma Access existante vers Strata Cloud Manager.

Pour activer le flux de travail de migration, vous devez contacter l'équipe de compte Palo Alto Networks.

La gestion de la configuration Prisma Access à l'aide de Strata Cloud Manager au lieu de Panorama offre certains avantages. En voici quelques exemples :

- Évaluations continues des meilleures pratiques
- Configurations par défaut sécurisées
- Optimisation de la configuration basée sur l'apprentissage automatique (ML)
- Flux de travail de sécurité web rationalisés
- Résumé visuel interactif (centre de commande) aidant à évaluer l'intégrité, la sécurité et l'efficacité du réseau
- Flux de travail intuitifs pour les tâches complexes
- API de gestion simples et sécurisés
- Architecture cloud native offrant évolutivité, résilience et portée mondiale
- Aucun matériel à gérer ou logiciel à maintenir

Préparer la migration vers Prisma Access (Managed by Strata Cloud Manager)

Avant de commencer la migration, vous devez connaître la configuration logicielle minimale requise et les types de déploiements Prisma Access (Managed by Panorama) que vous pouvez migrer.

- **Quand migrer** : n'effectuez pas la migration pendant une mise à niveau du plan de données ou de l'infrastructure. Vérifiez vos préférences de mise à niveau pour voir si une mise à niveau du plan de données est prévue.
- **Migration unidirectionnelle de Panorama vers Prisma Access (Managed by Strata Cloud Manager)** : la migration peut uniquement avoir lieu d'un déploiement Prisma Access (Managed by Panorama) vers un déploiement Prisma Access (Managed by Strata Cloud Manager). Après avoir migré vers Strata Cloud Manager, vous ne pourrez pas rétablir la gestion par Panorama du déploiement Prisma Access.
- **Version minimale de Panorama** : vous avez besoin de Panorama 10.0 ou version ultérieure.
- **Rôle administrateur requis** : vous devez être connecté en tant que super utilisateur dans Strata Cloud Manager pour commencer la migration.
- **Exigences en matière de licences** : vous avez besoin d'une licence Prisma Access.

- **Cloud Identity Engine** : vous devez avoir intégré le composant de synchronisation d'annuaire du Cloud Identity Engine à Prisma Access (Managed by Panorama) avant la migration.
- **Fonctionnalités non prises en charge** : le programme de migration ne prend pas en charge les fonctionnalités Prisma Access suivantes :
  - Filtrage des données (utilisez Enterprise DLP comme solution de rechange)
  - Déploiements FedRAMP
  - Sécurité IdO
  - Déploiements multi-locataires
  - Proxy SSH
  - Authentification distincte pour les portails et les passerelles GlobalProtect
- **Migrations Prisma SD-WAN et Prisma Access** : si vous migrez un déploiement Prisma Access et un déploiement Prisma SD-WAN, Prisma Access et Prisma SD-WAN doivent partager le même ID de groupe de services aux locataires (ID TSG).
- **Problèmes de différences de configuration** : lorsque vous exécutez config diff pendant la migration, ignorez les différences qui affichent les noms d'objet suivants, car elles n'affectent pas votre configuration :
  - Clientless-vpn crypto-settings
  - Hip-profiles rename
  - Mobile-user-redundancy
  - Exclude-video-traffic

Migrer le déploiement Prisma Access (Managed by Panorama) vers Strata Cloud Manager

Pour migrer le déploiement Prisma Access (Managed by Panorama) vers un déploiement Prisma Access (Managed by Strata Cloud Manager), procédez comme suit.

En résumé, vous devez :

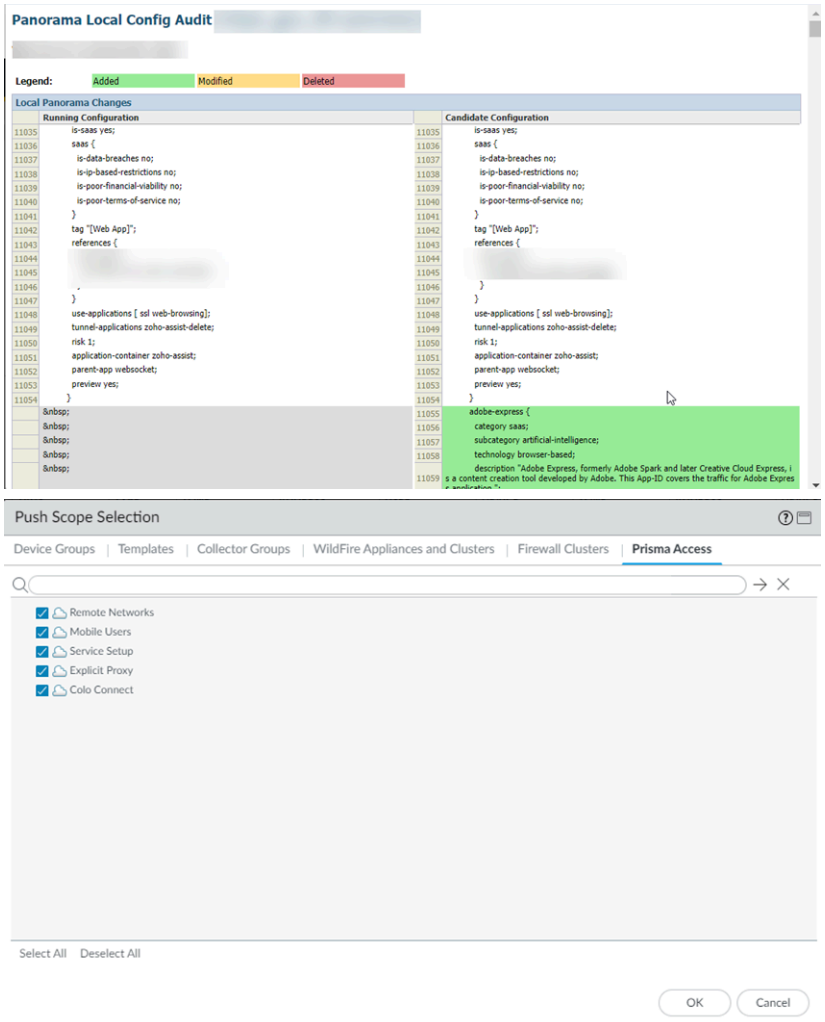
1. Vérifier que vous avez appliqué la dernière configuration sur Prisma Access, enregistré la dernière configuration et exporté un fichier de configuration .xml à partir du Panorama qui gère Prisma Access.
2. Démarrer le programme de migration à partir de Strata Cloud Manager.
3. Vérifier les différences de configuration (diffs) entre la configuration Panorama et la configuration Strata Cloud Manager migrée.
4. Résoudre les différences et terminer la migration.

STEP 1 | Préparez votre Panorama pour la migration.

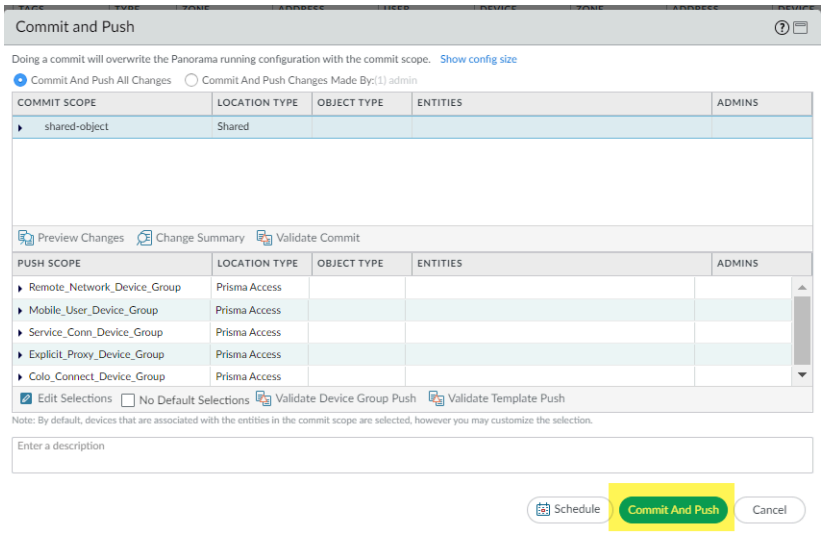
1. Connectez-vous au Panorama qui gère Prisma Access avec un compte d'administration auquel le rôle de super utilisateur est attribué.
2. (Facultatif) Si vous avez configuré une clé principale personnalisée pour votre Panorama et pour Prisma Access, notez-la.

   Si votre déploiement utilise la clé principale par défaut, cette étape n'est pas requise.
3. Assurez-vous que la configuration actuelle de Panorama est à jour, que vous avez validé toutes les modifications à Panorama et que vous avez appliqué ces modifications sur Prisma Access. Pour ce faire, accédez à **Commit (Valider)** > **Commit & Push (Valider et appliquer)** et sélectionnez **Preview Changes (Prévisualiser les modifications)**.
4. (Facultatif) Vérifiez les différences entre la configuration en cours d'exécution et la configuration candidate, puis décidez si vous souhaitez appliquer ces modifications. Si vous souhaitez valider et appliquer les modifications, sélectionnez **Edit Selections**

(Modifier les sélections), puis sélectionnez les composants Prisma Access que vous souhaitez appliquer dans **Push Scope (Étendue de la transmission)**.



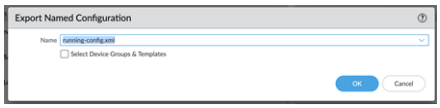
5. (Facultatif) Sélectionnez **Commit and Push (Valider et appliquer)** pour valider et appliquer les modifications.



6. Accédez à **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et sélectionnez **Export named Panorama configuration snapshot (Exporter l'instantané de configuration Panorama nommé)**.

   Ce fichier .xml doit être chargé sur Strata Cloud Manager pendant le processus de migration. **Chargez uniquement le fichier de configuration .xml ; ne chargez pas de fichiers de support technique ni aucun autre fichier.**

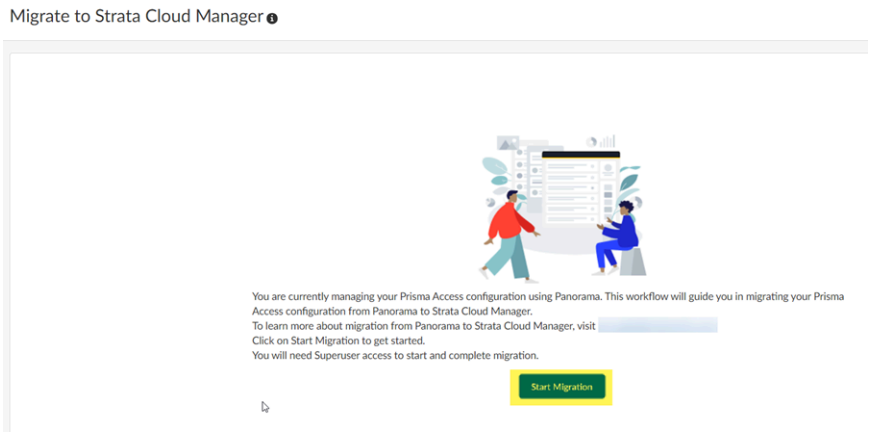
7. Sélectionnez le fichier de configuration **running-config.xml**, puis appuyez sur **OK**.



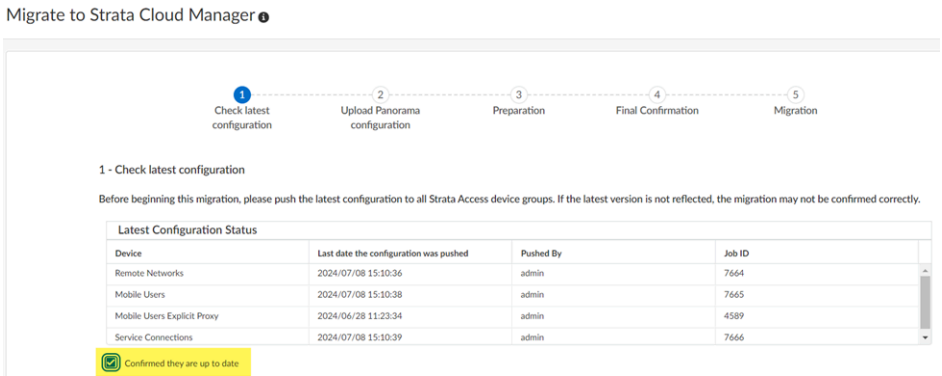
STEP 2 | Connectez-vous à Strata Cloud Manager en tant qu'administrateur avec un rôle de super utilisateur et accédez à **Manage (Gérer)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)**.

Le programme de migration détecte que vous disposez d'un déploiement géré par Panorama.

STEP 3 | Sélectionnez **Start Migration (Démarrer la migration)**.

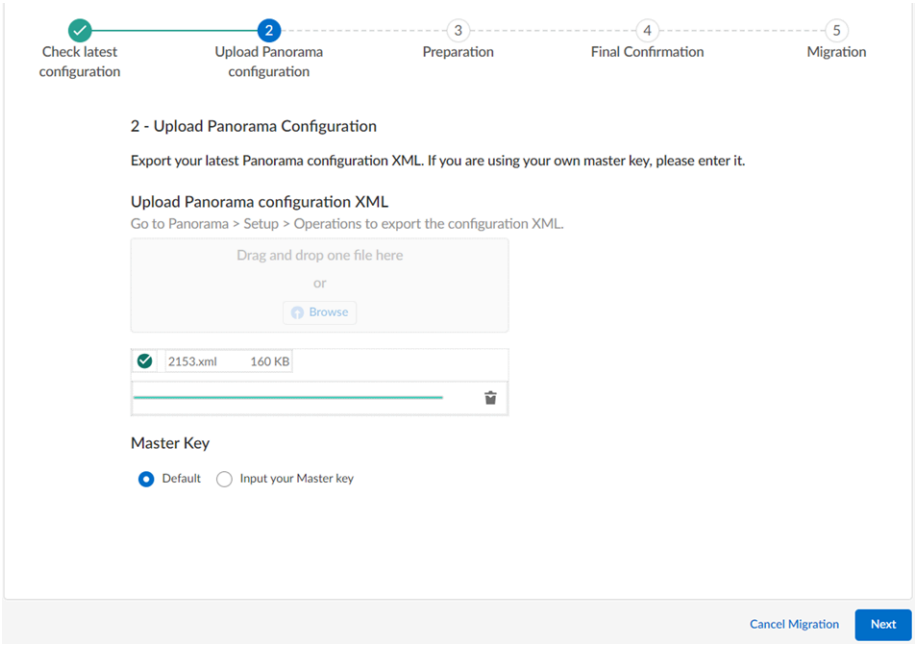


STEP 4 | Le programme de migration vous demande de vérifier si la configuration est à jour et vous indique le dernier utilisateur qui l'a mise à jour. Après avoir vérifié que cette configuration comporte les dernières modifications, sélectionnez **Confirmed they are up to date (Confirmation de leur mise à jour)** et cliquez sur **Next (Suivant)**.

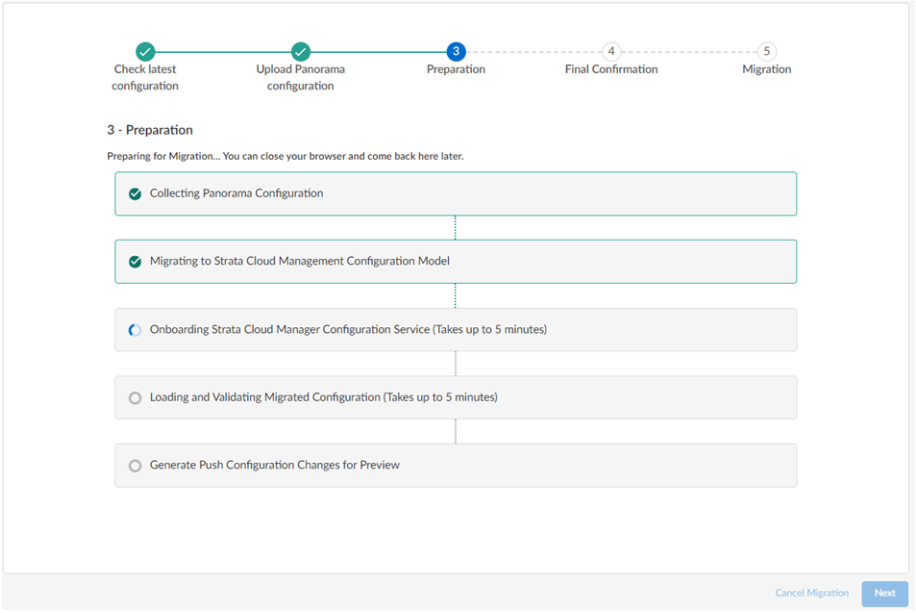


STEP 5 | Sélectionnez le fichier .xml de configuration Panorama que vous avez téléchargé au cours d'une précédente étape en le faisant glisser et en le déposant, ou en utilisant l'option **Choose File (Choisir un fichier)**.

STEP 6 | Saisissez votre **Master Key (Clé principale)**, ou si vous n'avez pas créé de clé principale personnalisée, demandez à Strata Cloud Manager d'utiliser la clé principale **Default (Par défaut)**, puis cliquez sur **Next (Suivant)**.

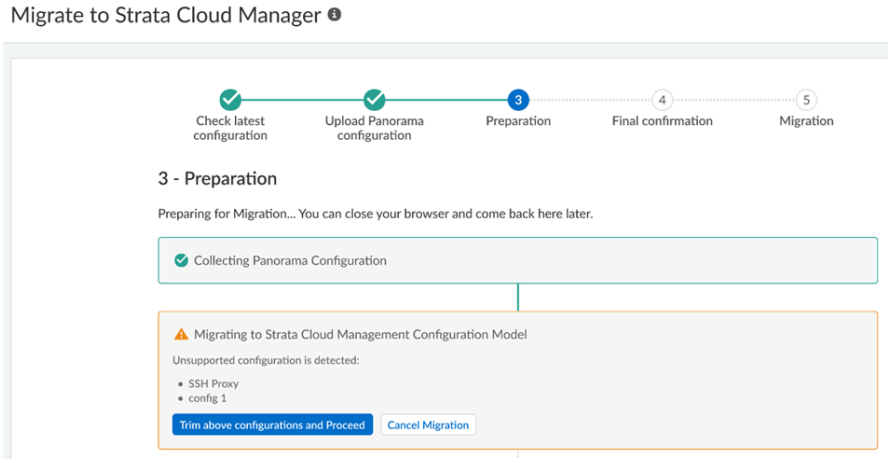


Le programme de migration commence.



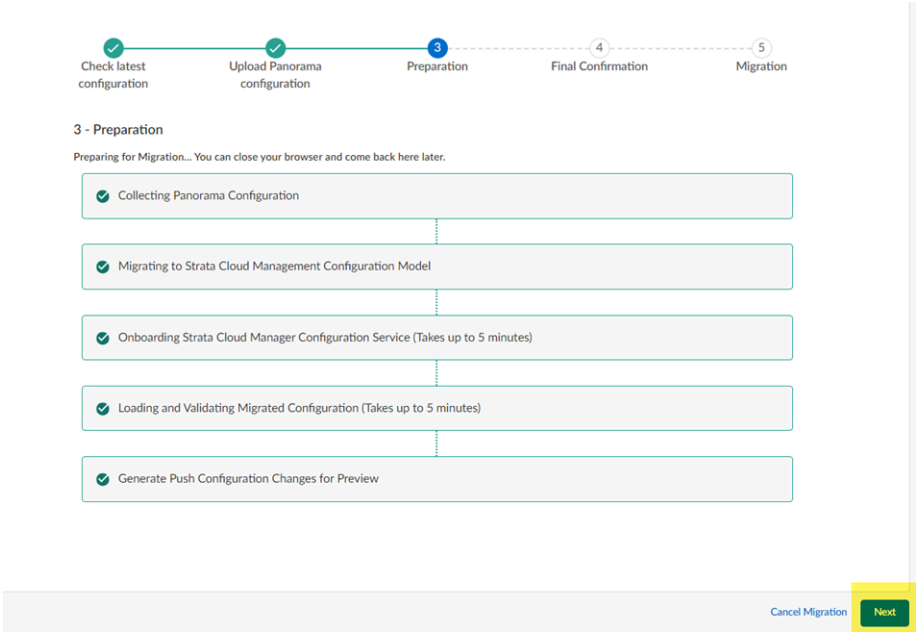
Attendez que toutes les étapes soient terminées.

STEP 7 | Si, lors de la migration, le programme indique qu'il a rencontré une configuration non prise en charge, vous pouvez sélectionner **Trim the above configurations and proceed (Couper les configurations ci-dessus et continuer)** ou **Cancel migration (Annuler la migration)**.



Certaines configurations non prises en charge (comme les configurations multilocataires) annulent la migration et le programme de migration ne peut pas résoudre le problème. Le cas échéant, sélectionnez **Cancel Migration (Annuler la migration)**.

STEP 8 | Une fois la migration terminée, cliquez sur **Next (Suivant)**.



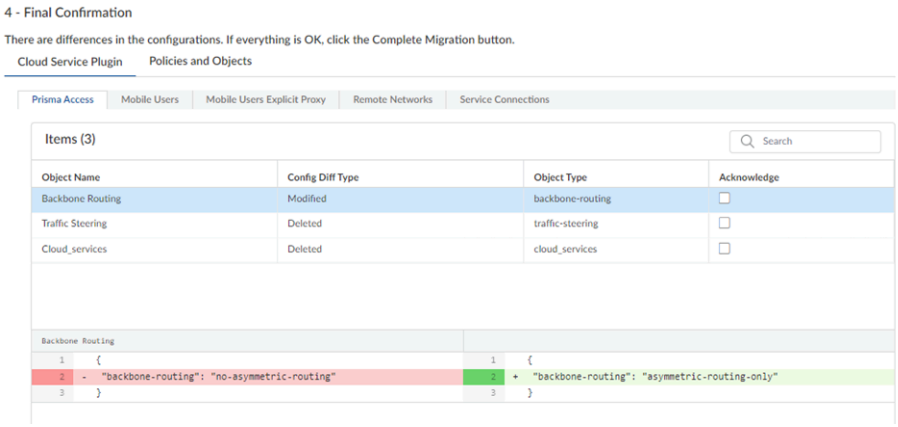
STEP 9 | Si le programme de migration a apporté des modifications, passez-les en revue sur l'écran de confirmation finale.

Le programme de migration peut apporter des modifications à la configuration pour tenir compte des différences entre la configuration Panorama et la configuration Strata Cloud Manager, ou pour corriger une fonctionnalité non prise en charge. Si des modifications

sont nécessaires, le programme de migration affiche ces modifications dans une vue des différences, avec les nouvelles lignes en vert et les lignes supprimées en rouge.

Ignorez les différences qui affichent les noms d'objets suivants, car elles n'affectent pas votre configuration :

- *Clientless-vpn crypto-settings*
- *Hip-profiles rename*
- *Mobile-user-redundancy*
- *Exclude-video-traffic*



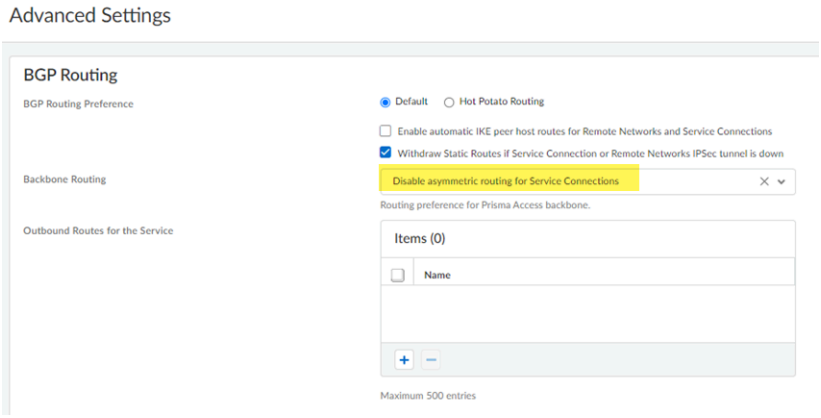
STEP 10 | (Facultatif) Modifiez les différences de configuration.

Les modifications que vous apportez ne sont pas validées sur la configuration tant que vous n'avez pas terminé la migration et appliqué les modifications sur Strata Cloud Manager.

1. Accédez à la zone dans la configuration Prisma Access où vous avez trouvé les différences, puis modifiez la configuration.

   Pour l'exemple donné à l'étape précédente, le programme de migration a apporté une modification au routage principal (en remplaçant **no-asymmetric-routing** par **asymmetric-routing-only**). Pour rétablir ce paramètre tel qu'il était défini dans la configuration d'origine, accédez à **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration Prisma Access)** > **Service Connections (Connexions aux services)** > **Advanced Settings (Paramètres avancés) Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Configuration Scope (Portée de la configuration)** > **Prisma Access (Prisma Access)** > **Service Connections (Connexions aux services)** > **Advanced Settings (Paramètres avancés)** et définissez la configuration

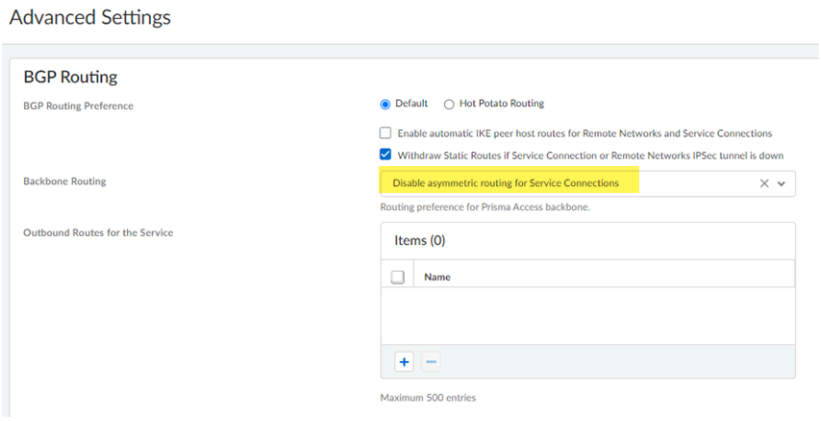
Backbone Routing (Routage principal) sur **Disable Asymmetric Routing for Service Connections (Désactiver le routage asymétrique pour les connexions aux services)**.



.

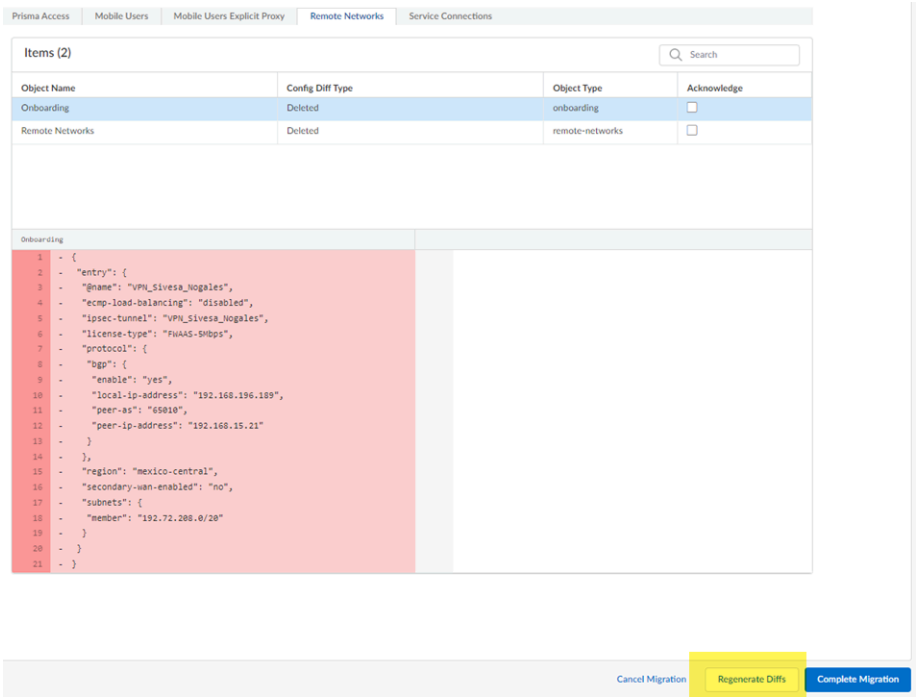
2. (Facultatif) Pour ne pas perdre le fil de vos modifications, sélectionnez **Acknowledge (Accepter)** au fur et à mesure que vous les réalisez.

   Bien que cela ne soit pas obligatoire, il peut être utile d'accepter les modifications au fur et à mesure que vous les réalisez afin de savoir où vous en êtes.



3. Continuez de passer en revue les changements, d'y apporter des modifications et de les accepter.

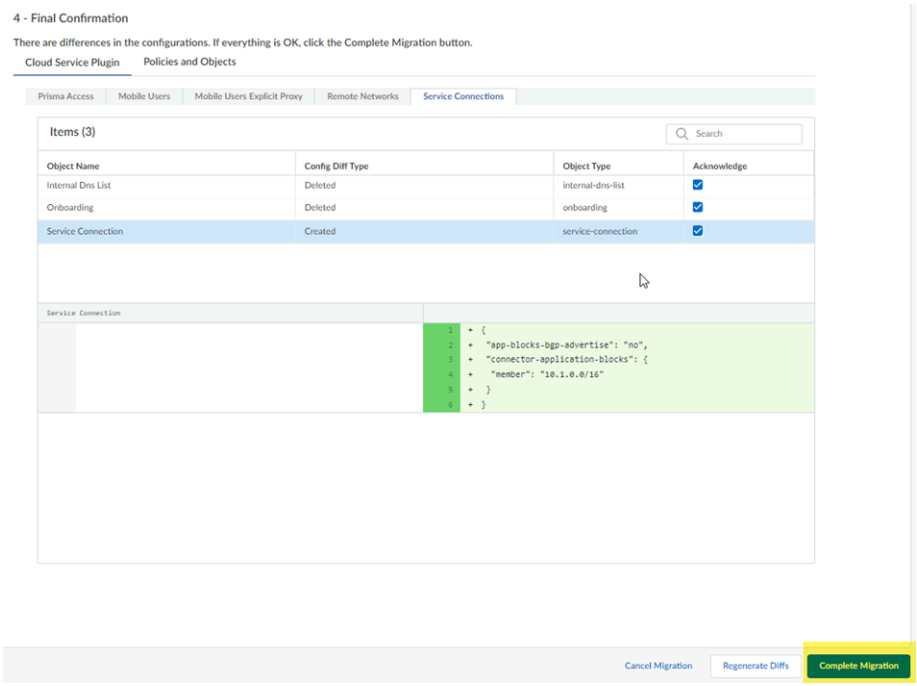
STEP 11 | (Facultatif) Si vous avez apporté des modifications à la configuration, sélectionnez **Regenerate Diffs (Régénérer les différences)** pour voir les différences mises à jour.



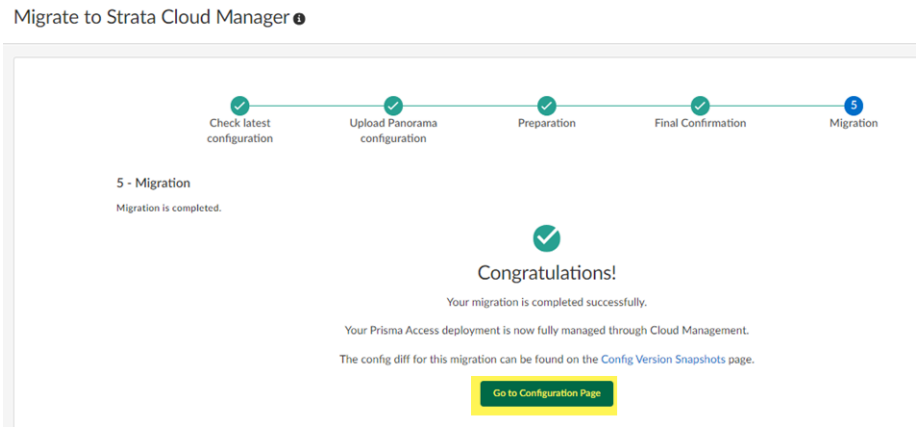
STEP 12 | Sélectionnez **Complete Migration (Terminer la migration)**.

Bien que cela ne soit pas obligatoire, vous pouvez également sélectionner **Acknowledge (Accepter)** pour accepter les modifications.

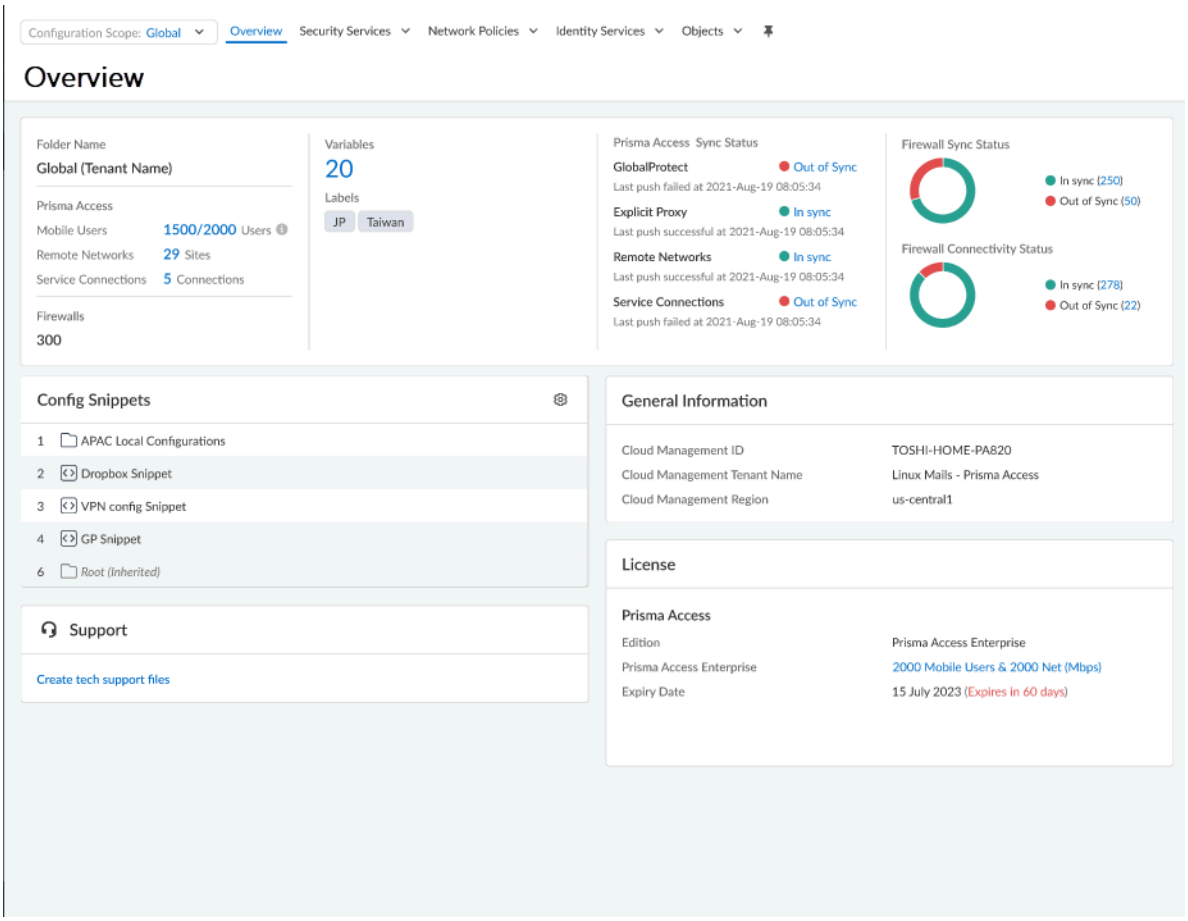
Après avoir sélectionné Complete Migration (Terminer la migration), vous ne pourrez pas revenir à un déploiement géré par Panorama. Votre déploiement utilisera définitivement Strata Cloud Manager pour sa gestion.



STEP 13 | (Facultatif) Sélectionnez **Go to Configuration Page (Aller à la page de configuration)** pour voir la configuration migrée.

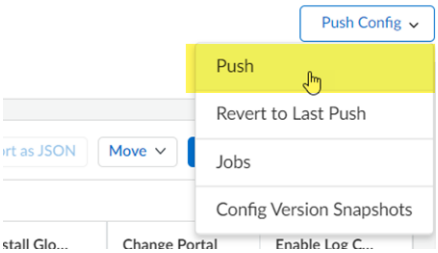


Le déploiement migré s'affiche.



STEP 14 | Sélectionnez **Push Config (Transmettre la configuration)** > **Push (Pousser)** pour appliquer les modifications de la configuration migrée.

Cette opération de transmission permet de s'assurer que la migration s'est terminée correctement et que Prisma Access a appliqué toutes les modifications à la configuration migrée.



STEP 15 | Notez tous les messages que vous avez reçus pendant l'opération de transmission et, si vous rencontrez des problèmes, apportez les modifications nécessaires à la configuration.

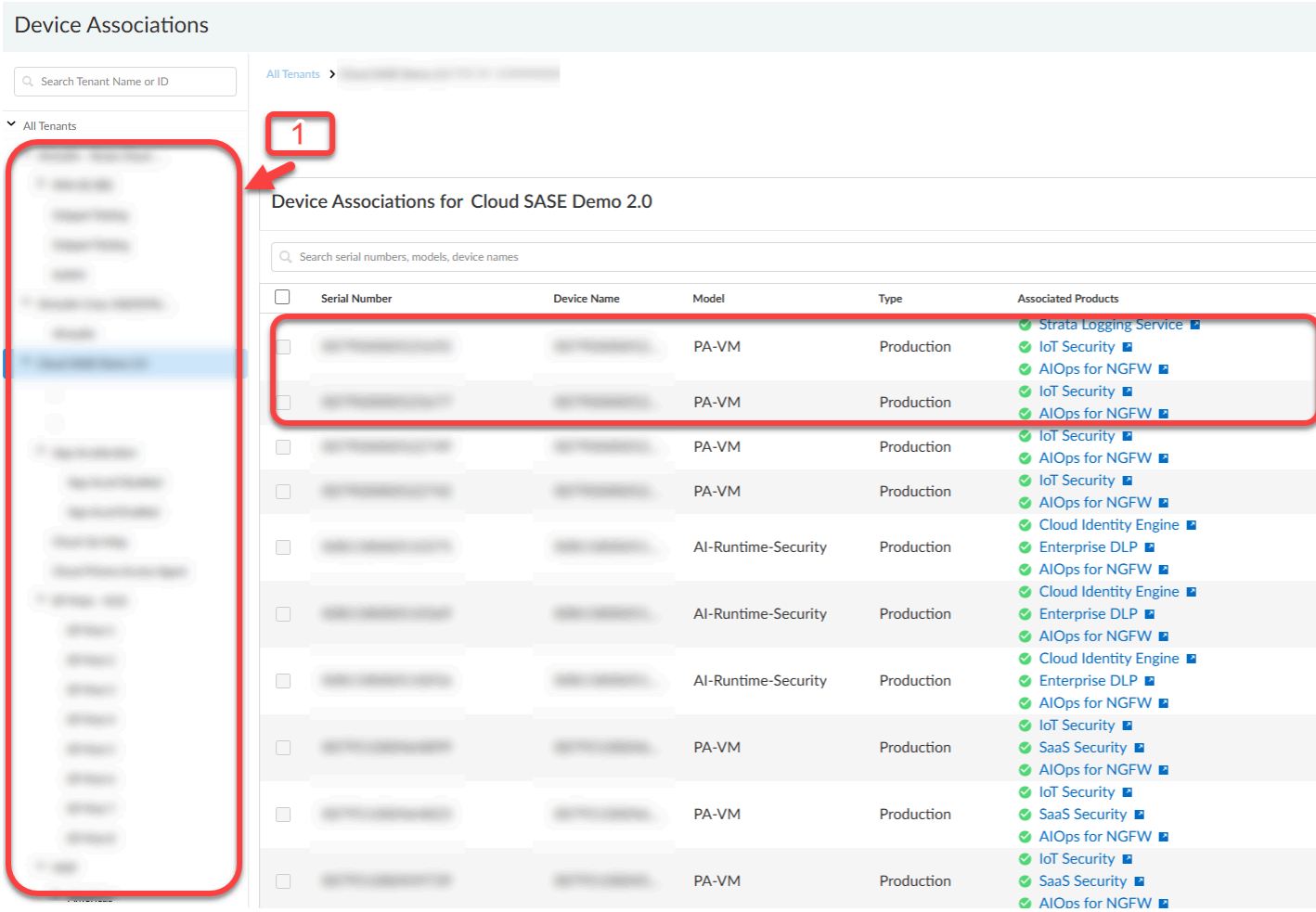
Associations de périphériques dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	Un des éléments suivants : ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Si vous avez commencé à utiliser Strata Cloud Manager avant l'introduction de ces niveaux de licence, vos licences restent prises en charge.

Composant de Strata Cloud Manager et des services communs, **Device Associations** fournit une vue de gestion centralisée de tous les périphériques de votre déploiement. Il vous permet d'organiser les périphériques en groupes de services aux locataires (conteneurs logiques pour organiser les périphériques) et facilite l'association de produits pris en charge à vos périphériques.

Vous pouvez utiliser Device Associations avec les produits suivants :

- ❑ Strata Cloud Manager
- ❑ AIOps for NGFW
- ❑ IoT Security (Contrat de licence d'entreprise)
- ❑ Next-Generation CASB for Prisma Access and NGFW (CASB-X)
- ❑ SaaS Security Inline
- ❑ Strata Logging Service



1. Dans **Device Associations (Associations de périphériques) (Settings (Paramètres) > Device Associations (Associations de périphériques)**, vous pouvez afficher une liste de tous les groupes de services aux locataires (TSG) associés à votre compte de support client.
2. Sélectionnez un TSG pour afficher les pare-feu ou les appareils Panorama qui lui sont associés. Si vous n'en voyez aucun, vous pouvez utiliser l'option **Add Devices (Ajouter des périphériques)** à partir de votre compte de support client.
3. Utilisez l'option **Add Device (Ajouter un périphérique)** chaque fois que vous devez associer de nouveaux périphériques à votre TSG.
4. Après avoir ajouté un pare-feu ou un appareil Panorama, vous pouvez utiliser l'option **Associate Products (Associer des produits)** pour commencer à utiliser l'appareil avec les produits que vous avez activés. L'application doit être compatible avec le modèle de matériel de votre périphérique. Sinon, le périphérique n'apparaîtra pas lors de l'association de l'application.

- Associer des périphériques
- Associer des produits
- Supprimer des associations

Associations de périphériques (associer des périphériques à un locataire)

Avant de pouvoir commencer à utiliser un pare-feu ou un appareil Panorama avec des produits sous licence que vous avez activés, vous devez d'abord l'associer au locataire dans lequel vous avez activé un produit compatible.

STEP 1 | Accédez à **Device Associations** en utilisant le hub ou Strata Cloud Manager.

1. (Facultatif) Connectez-vous au hub en utilisant vos identifiants du CSP de Palo Alto Networks et sélectionnez **Common Services (Services communs)** > **Device Associations (Associations de périphériques)**.

2. (Facultatif) Connectez-vous à Strata Cloud Manager et sélectionnez **Settings (Paramètres)** > **Device Associations (Associations de périphériques)**.

STEP 2 | Ajoutez le pare-feu ou l'appareil Panorama à votre locataire.

1. Sélectionnez **Add Device (Ajouter un périphérique)**.

   Votre **Customer Support Account (Compte de support client)** est automatiquement sélectionné en fonction des produits activés dans le locataire dans lequel vous vous trouvez. Si vous n'avez activé aucun produit prenant en charge Device Associations, l'option **Add Device (Ajouter un périphérique)** sera grisée.

2. Sélectionnez un ou plusieurs pare-feu ou appareils Panorama.

   Vous pouvez utiliser un numéro de série pour rechercher un périphérique spécifique.

3. **Save (Enregistrer)**.

STEP 3 | Continuez à associer des produits avec des périphériques.

Associations de périphériques (associer des périphériques à un produit)

Après avoir activé la licence pour un produit pris en charge, vous utilisez l'option **Device Associations (Associations de périphériques)** pour spécifier les pare-feu ou les appareils Panorama que vous souhaitez utiliser avec le produit.

STEP 1 | Activez votre licence de produit.

La procédure d'activation varie en fonction de la licence. Reportez-vous à la documentation spécifique du produit pour plus d'informations. Vous pouvez également consulter la compatibilité de la licence avec Strata Cloud Manager ici.

STEP 2 | Accédez à **Device Associations** en utilisant le hub ou Strata Cloud Manager.

1. (Facultatif) Connectez-vous au hub en utilisant vos identifiants du CSP de Palo Alto Networks et sélectionnez **Common Services (Services communs)** > **Device Associations (Associations de périphériques)**.
2. (Facultatif) Connectez-vous à Strata Cloud Manager et sélectionnez **Settings (Paramètres)** > **Device Associations (Associations de périphériques)**.

STEP 3 | Associez des produits à des pare-feu ou à des appareils Panorama.

1. Sélectionnez **Associate Products (Associer des produits)**.
2. Dans la colonne de sélection des produits, sélectionnez le produit que vous souhaitez associer.
3. Le cas échéant, sélectionnez le type de licence.

   Certains produits ont des licences pour des conditions de validité et des modèles de périphériques spécifiques. Seuls les périphériques compatibles avec le type de licence que vous avez sélectionné apparaîtront pour l'association.
4. Sélectionnez des périphériques.
5. Cliquez sur **Save (Enregistrer)** ou **Apply Licenses (Appliquer les licences)**.

STEP 4 | Vérifiez que l'association a réussi.

Si l'association a échoué, copiez l'ID d'erreur et suivez les étapes pour ouvrir une demande de support. Lorsque vous ouvrez la demande de support, assurez-vous d'inclure l'ID d'erreur, le numéro de série du périphérique, l'ID TSG et le nom du produit dont l'association a échoué.

STEP 5 | Revenez à la documentation du produit que vous associez pour d'autres étapes d'intégration.

Associations de périphériques (Supprimer des associations de périphériques)

Vous pouvez supprimer les associations de périphériques si, par exemple, vous retirez ou renvoyez un pare-feu ou un appareil Panorama, ou si vous souhaitez l'associer à un autre groupe de services aux locataires (TSG).

Si vous essayez de convertir une licence d'essai en licence de production, convertissez la licence au lieu de la dissocier.

STEP 1 | Accédez à **Device Associations** en utilisant le hub ou Strata Cloud Manager.

1. (Facultatif) Connectez-vous au hub en utilisant vos identifiants du CSP de Palo Alto Networks et sélectionnez **Common Services (Services communs)** > **Device Associations (Associations de périphériques)**.

2. (Facultatif) Connectez-vous à Strata Cloud Manager et sélectionnez **Settings (Paramètres)** > **Device Associations (Associations de périphériques)**.

STEP 2 | Supprimez des associations de produits.

Si vous souhaitez supprimer un pare-feu ou un appareil Panorama de votre TSG, vous devez d'abord supprimer tous les produits associés.

1. Sélectionnez les pare-feu ou les appareils Panorama dont vous souhaitez dissocier les produits.
2. Sélectionnez **Remove Associations (Supprimer les associations)** > **Remove product association (Supprimer l'association de produits)**.
3. Sélectionnez les produits que vous souhaitez supprimer et cliquez sur **Remove Associations (Supprimer les associations)**.

STEP 3 | Supprimer une association de locataires.

Vous pouvez supprimer les associations de locataires uniquement des périphériques qui n'ont pas d'associations d'applications. Si le périphérique est associé à une application, supprimez l'association d'application avant de poursuivre.

1. Sélectionnez les pare-feu ou les appareils Panorama que vous souhaitez supprimer de votre locataire.
2. Sélectionnez **Remove Associations (Supprimer les associations)** > **Remove tenant association (Supprimer l'association de locataire)**.
3. Confirmez que vous voulez poursuivre et cliquez sur **Remove (Supprimer)**.

STEP 4 | Si vous supprimez un pare-feu ou un appareil Panorama pour l'ajouter à un nouveau TSG, associez-le au nouveau TSG.

Compatibilité des modèles de périphériques

Il s'agit des modèles de périphériques que vous pouvez associer à différentes applications.

- AIOps for NGFW ou Strata Cloud Manager
- CASB-X
- IoT Security
- SaaS Security

AIOps for NGFW ou Strata Cloud Manager

Série	Modèles
Appareils virtuels Panorama	• PRA-25 • PRA-100 • PRA-1000
VM-Series	• VM-200 • VM-300 • VM-500 • VM-600 • VM-700
200	• 220
400	• 410 • 410R • 440 • 445 • 450 • 450R • 460
800	• 820 • 850
3000	• 3220 • 3250 • 3260 • 3410 • 3420

Série	Modèles
	• 3430 • 3440
5 000	• 5220 • 5250 • 5260 • 5280 • 5410 • 5420 • 5430 • 5445 • 5450
7000	• 7050 • 7080

CASB-X

Série	Modèles
200	• 220
400	• 400 • 410 • 415 • 440 • 445 • 450 • 450R • 460
800	• 820 • 850
1000	• 1410 • 1420
3000	• 3200 • 3220

Série	Modèles
	• 3250 • 3260 • 3410 • 3420 • 3430 • 3440
5 000	• 5220 • 5250 • 5260 • 5280 • 5400 • 5420 • 5430 • 5440 • 5445 • 5450
7000	• 7050 • 7080

IoT Security

Ce tableau contient uniquement les modèles de périphériques que vous pouvez associer à IoT Security dans Device Associations. Le tableau ne contient pas d'informations sur les fonctionnalités IoT Security disponibles avec différentes combinaisons de modèles de périphériques et de versions de PAN-OS.

Série	Modèles
VM-Series	• VM-100 • VM-300 • VM-500 • VM-700
200	• 200 • 220 • 220R

Série	Modèles
400	• 410 • 410R • 440 • 450 • 450R • 460
500	• 500
800	• 820 • 850
3000	• 3020 • 3050 • 3060 • 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
7000	• 7050 • 7080

SaaS Security

Ce tableau contient uniquement les modèles de périphériques que vous pouvez associer à SaaS Security dans Device Associations. Le tableau ne contient pas d'informations sur les fonctionnalités SaaS Security disponibles avec différentes combinaisons de modèles de périphériques et de versions de PAN-OS.

Série	Modèles
200	• 220 • 220R
400	• 410 • 410R

Série	Modèles
	• 440 • 440R • 450 • 450R • 460 • 460R
800	• 820 • 850
3000	• 3220 • 3250 • 3260 • 3410 • 3420 • 3430 • 3440
5 000	• 5220 • 5250 • 5260 • 5280 • 5410 • 5420 • 5430 • 5450
7000	• 7050 • 7080

Compatibilité des types de pare-feu et de licences

Certains abonnements aux produits ont différents types de licences, ce qui les rend compatibles uniquement avec des types spécifiques de pare-feu et d'appareils. Lorsque vous associez des produits à des périphériques et sélectionnez votre licence de produit, seuls les périphériques correspondant au type de licence apparaîtront. Cependant, certains types de licence, tels que les licences d'évaluation, les licences d'essai et le contrat de licence d'entreprise (ELA), sont compatibles avec tous les modèles de pare-feu.

Un type de pare-feu est défini par le SKU du pare-feu. Pour voir le SKU d'un pare-feu, connectez-vous à votre compte du portail de support client et sélectionnez **Assets (Ressources)** > **Devices (Périphériques)** et vérifiez l'entrée du numéro de série de votre pare-feu dans la colonne du nom du modèle. Il s'agit du SKU qui indique le type de pare-feu comme suit :

- Un SKU de prod. se termine par le nom du modèle de pare-feu ; par exemple, PAN-PA-410
- Un SKU d'éval. se termine par -E60, ce qui signifie *Évaluation + 60 jours* ; par exemple, PAN-PA-410-E60
- Un SKU de lab. se termine par -LAB ; par exemple, PAN-PA-410-LAB

Consultez ci-dessous les combinaisons de types de pare-feu et de licences que votre application prend en charge.

- #unique_38
- AIOps for NGFW
- IoT Security
- SaaS Security Inline

AIOps for NGFW

Types de licences AIOps for NGFW	Types de pare-feu			
	NFR	LAB	PROD	ÉVAL
ESSAI	Non	**Oui**	**Oui**	**Oui**
ÉVAL	Non	**Oui**	**Oui**	**Oui**
NFR	**Oui**	Non	Non	Non
LAB	Non	**Oui**	Non	Non
PROD	Non	Non	**Oui**	Non

IoT Security

Types de licences IoT Security	Types de pare-feu			
	NFR	LAB	PROD	ÉVAL
ESSAI	Non	**Oui**	**Oui**	**Oui**
ÉVAL	Non	**Oui**	**Oui**	**Oui**
NFR	**Oui**	Non	Non	Non
LAB	Non	**Oui**	Non	Non
PROD	Non	Non	**Oui**	Non

SaaS Security Inline

Types de licences SaaS Security Inline	Types de pare-feu			
	NFR	LAB	PROD	ÉVAL
ESSAI	Non	**Oui**	**Oui**	**Oui**
ÉVAL	Non	**Oui**	**Oui**	**Oui**
NFR	**Oui**	Non	Non	Non
LAB	Non	**Oui**	Non	Non
PROD	Non	Non	**Oui**	Non