Intégration de FDM à Defense Orchestrator

Table des matières

Introduction

Ce document décrit comment intégrer un périphérique géré par Firepower Device Manager (FDM) à Cisco Defense Orchestrator (CDO) à l'aide d'une clé d'enregistrement.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gestionnaire de périphériques Firepower (FDM)
- Cisco Defense Orchestrator (CDO)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Firepower Device Manager (FDM) Azure exécutant la version 7.4.1

Pour obtenir une liste complète des versions et des produits compatibles, consultez le Guide de compatibilité avec la défense pare-feu sécurisée pour plus d'informations.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

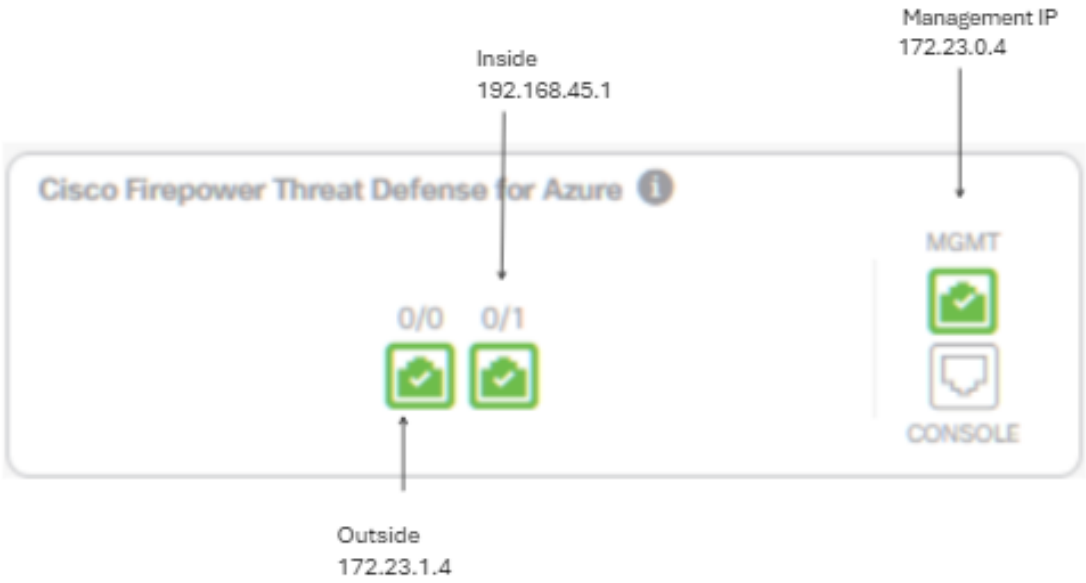
Avant de commencer le processus d'intégration d'un périphérique géré par FDM à Cisco Defense Orchestrator (CDO) à l'aide d'une clé d'enregistrement, assurez-vous que vous remplissez les conditions suivantes :

1. Version compatible : votre périphérique doit exécuter la version 6.6 ou ultérieure.
2. Configuration réseau requise : connexion de Cisco Defense Orchestrator à vos périphériques gérés
3. Logiciel de gestion : le périphérique doit être géré via le Gestionnaire de périphériques de pare-feu sécurisé (FDM).
4. Licences : votre périphérique peut utiliser une licence d'évaluation de 90 jours ou une licence Smart.
5. Enregistrements existants : assurez-vous que le périphérique n'est pas déjà enregistré auprès des services cloud Cisco pour éviter les conflits lors du processus d'intégration.
6. Pending Changes : vérifiez qu'aucune modification n'est en attente sur le périphérique.
7. Configuration DNS : les paramètres DNS doivent être correctement configurés sur votre périphérique géré par FDM.
8. Services de temps : les services de temps sur le périphérique peuvent être configurés avec précision pour assurer la synchronisation avec les protocoles de temps réseau.
9. Exigence d'activation du support FDM. La prise en charge de Firewall Device Manager (FDM) et sa fonctionnalité sont exclusivement accordées sur demande. Les utilisateurs sans prise en charge FDM activée sur leur locataire ne peuvent pas gérer ou déployer des configurations sur des périphériques gérés par FDM. Pour activer cette plate-forme, les utilisateurs doivent envoyer une demande d'activation de l'assistance FDM à l'équipe d'assistance.

Configurer

Diagramme du réseau

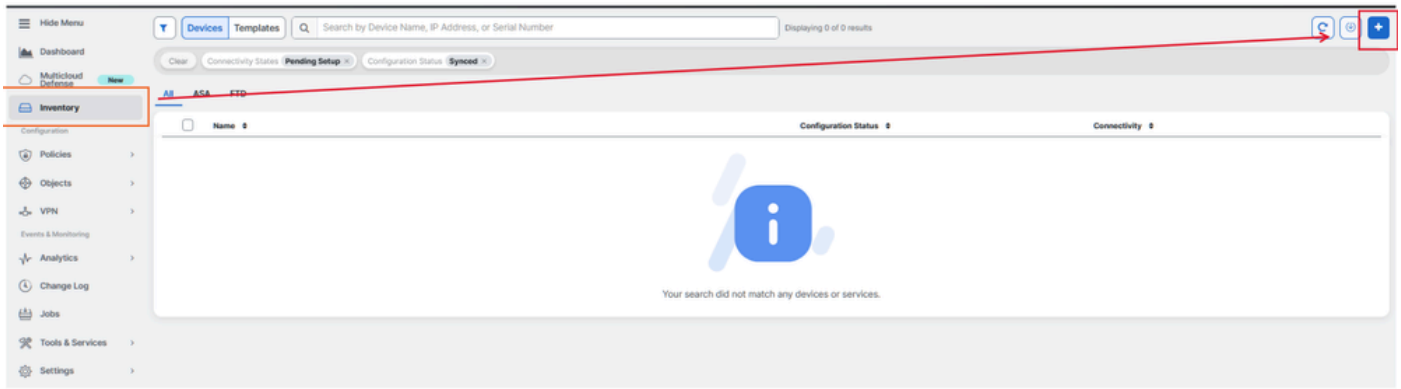
Cet article porte sur un périphérique FDM (Firepower Device Manager), contrôlé via son interface de gestion. Cette interface dispose d'un accès Internet essentiel à l'enregistrement du périphérique auprès de Cisco Defense Orchestrator (CDO).



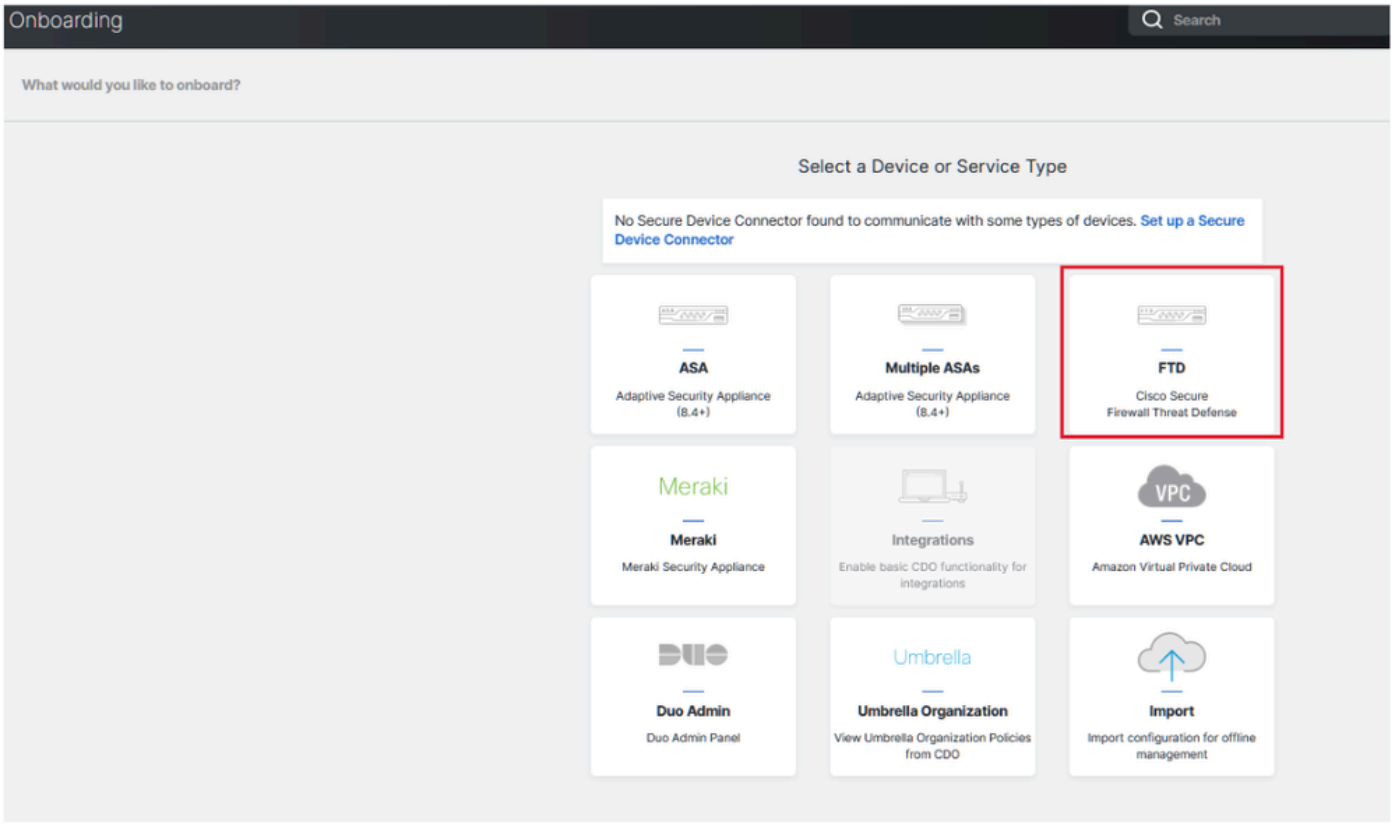
Configurations

Étape 1. Connectez-vous à Cisco Defense Orchestrator (CDO).

Étape 2. Accédez au volet Inventaire et sélectionnez le bouton plus bleu pour intégrer un périphérique.



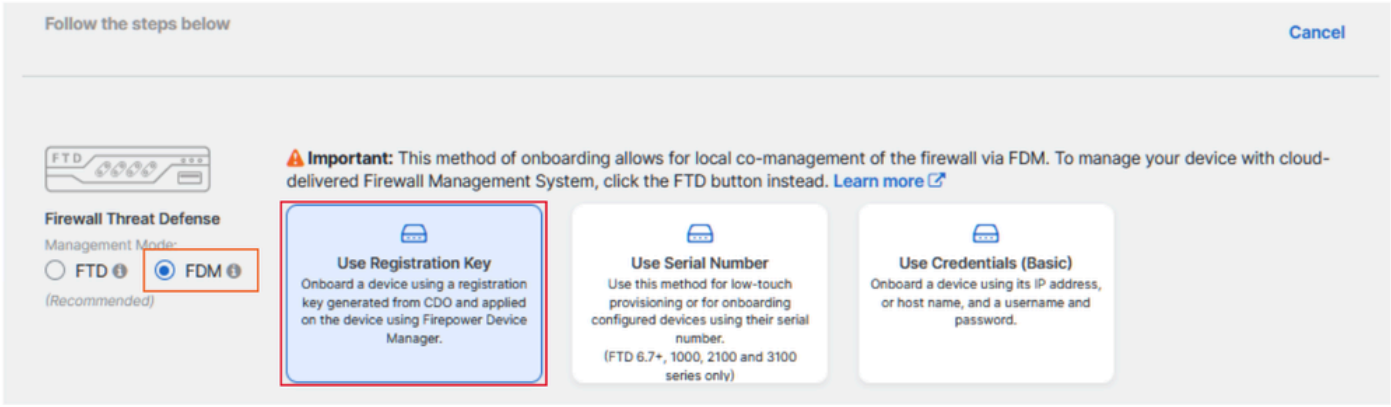
Étape 3. Sélectionnez l'option FTD.



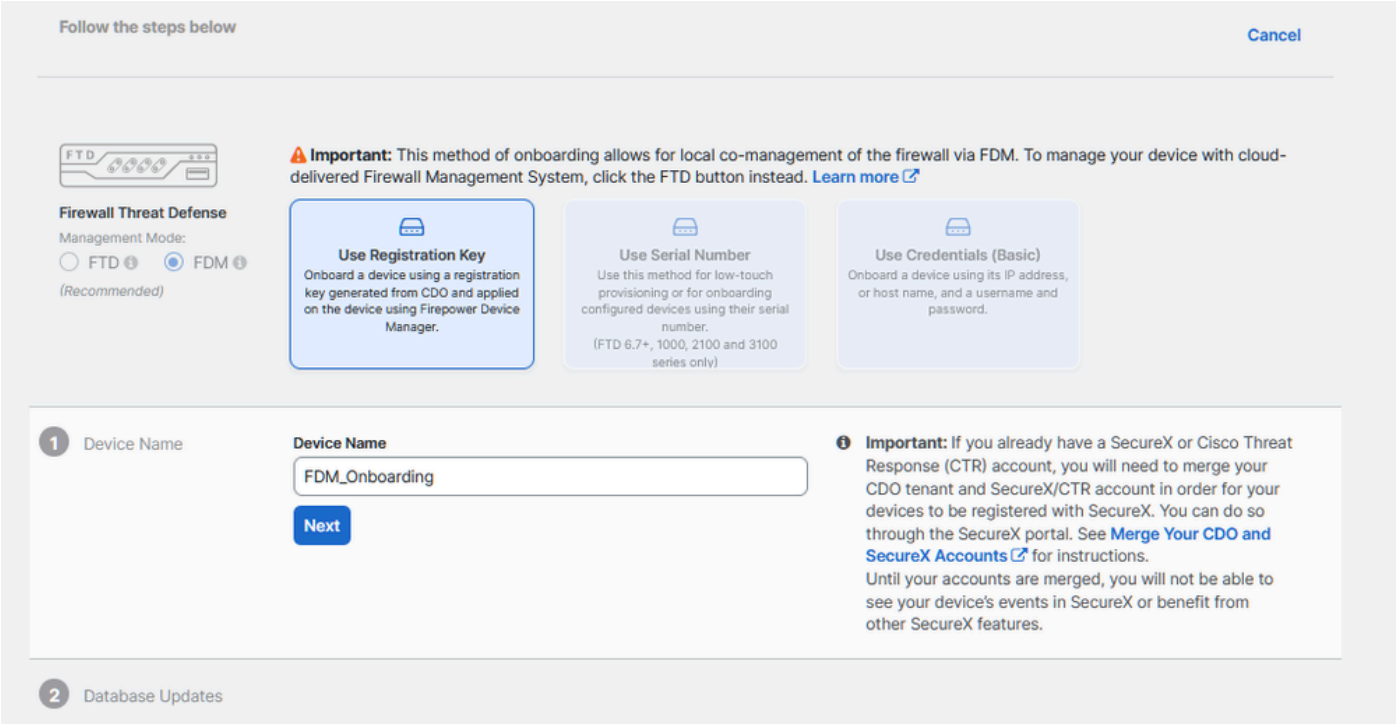
Étape 4 Passez à la section « Périphérique FTD embarqué » pour commencer le processus d'enregistrement. Il est important de noter les méthodes disponibles pour l'intégration d'un périphérique de défense contre les menaces :

- Par numéro de série : cette méthode s'applique aux périphériques physiques tels que les séries Firepower 1000, Firepower 2100 ou Secure Firewall 3100 avec versions logicielles prises en charge. Elle nécessite le numéro de série du châssis ou de l'adaptateur de contrôle d'accès et une connexion réseau à Internet.
- Par clé d'enregistrement : il s'agit de la méthode d'intégration privilégiée, particulièrement avantageuse pour les périphériques qui reçoivent des adresses IP via DHCP, car elle permet de maintenir la connectivité avec CDO même en cas de changement de l'adresse IP du périphérique.
- Utilisation des informations d'identification : cette alternative consiste à saisir les informations d'identification du périphérique et l'adresse IP de son interface externe, interne ou de gestion, en fonction de la configuration du périphérique sur le réseau.

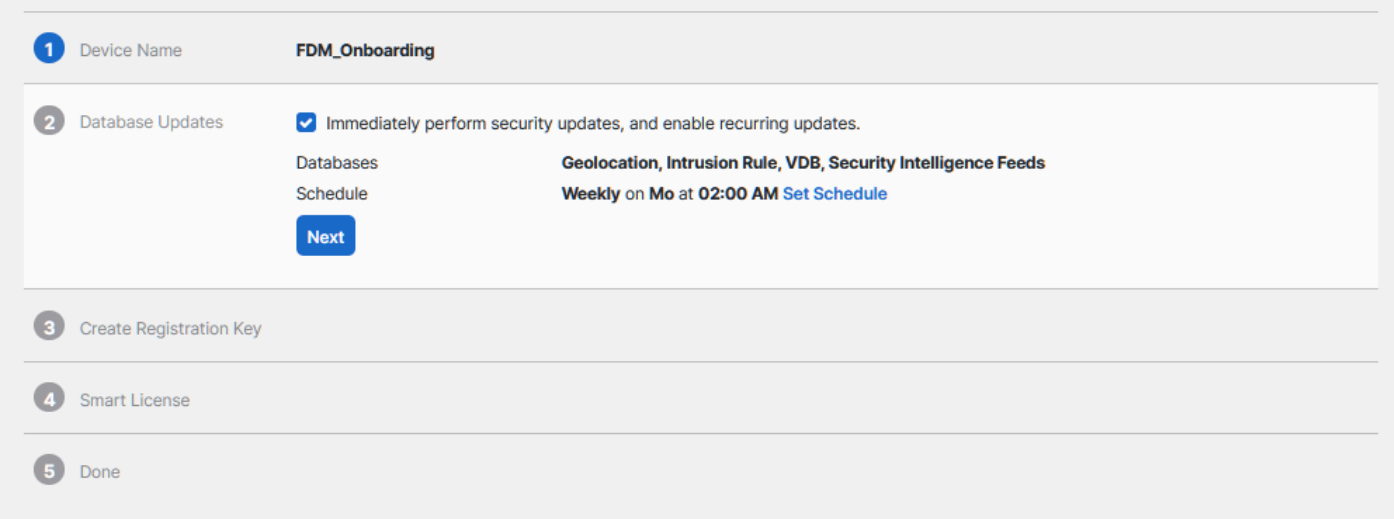
Pour ce processus, sélectionnez l'option FDM, puis l'option Use Registration Key pour assurer une connectivité cohérente à CDO, indépendamment des modifications potentielles de l'adresse IP du périphérique.



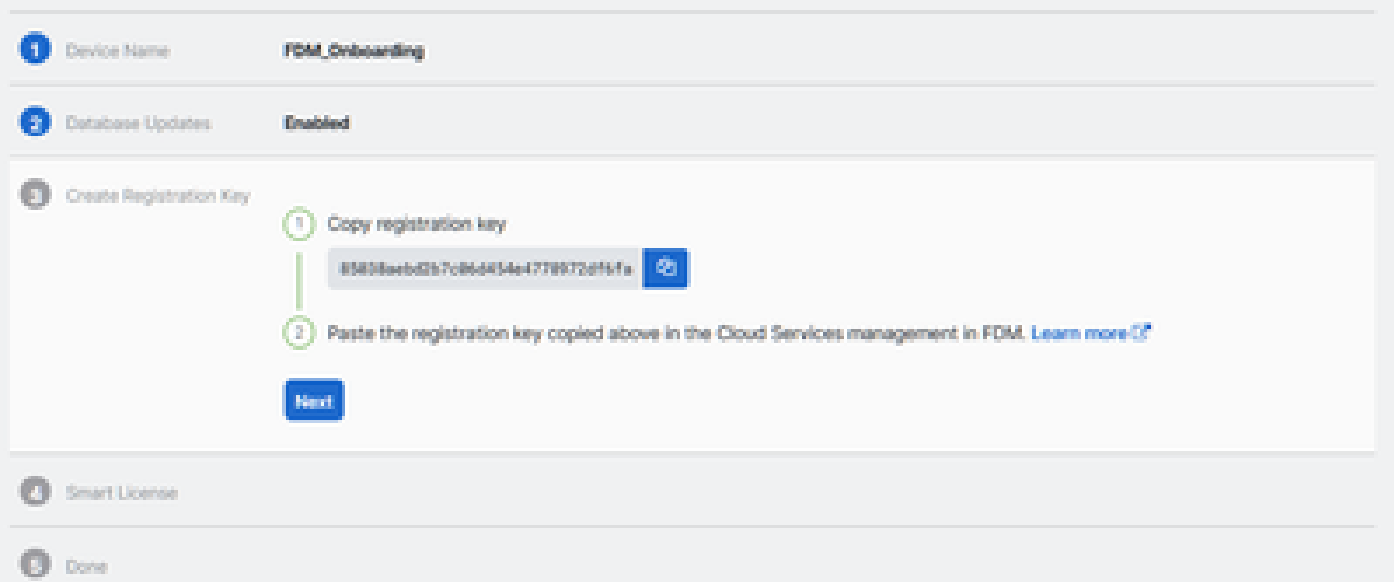
Étape 5. Saisissez le nom du périphérique souhaité dans le champ Device Name (Nom du périphérique) et spécifiez l'affectation de stratégie. Sélectionnez également la licence d'abonnement qui doit être associée au périphérique.



Étape 6. La section Mises à jour de la base de données est configurée par défaut pour exécuter immédiatement les mises à jour de sécurité et configurer les mises à jour récurrentes. La modification de ce paramètre ne modifie pas les calendriers de mise à jour existants établis via le gestionnaire de périphériques Secure Firewall.



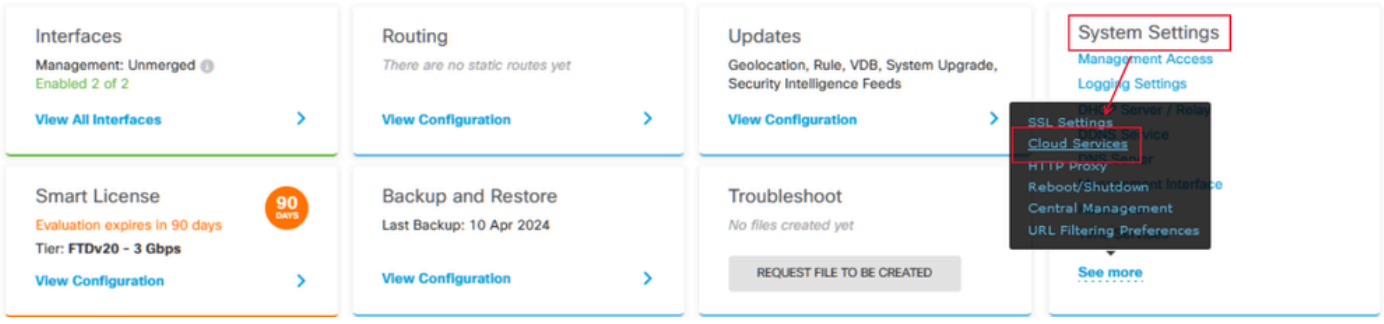
Étape 7. Dans la section Clé d'enregistrement CLI, CDO génère automatiquement une clé d'enregistrement. La fermeture de l'interface d'intégration avant la fin de l'opération entraîne la création d'un espace réservé pour le périphérique dans l'inventaire. La clé d'enregistrement peut être récupérée à partir de cet emplacement ultérieurement, si nécessaire.



Étape 8. Utilisez l'icône Copier pour copier la clé d'enregistrement générée.

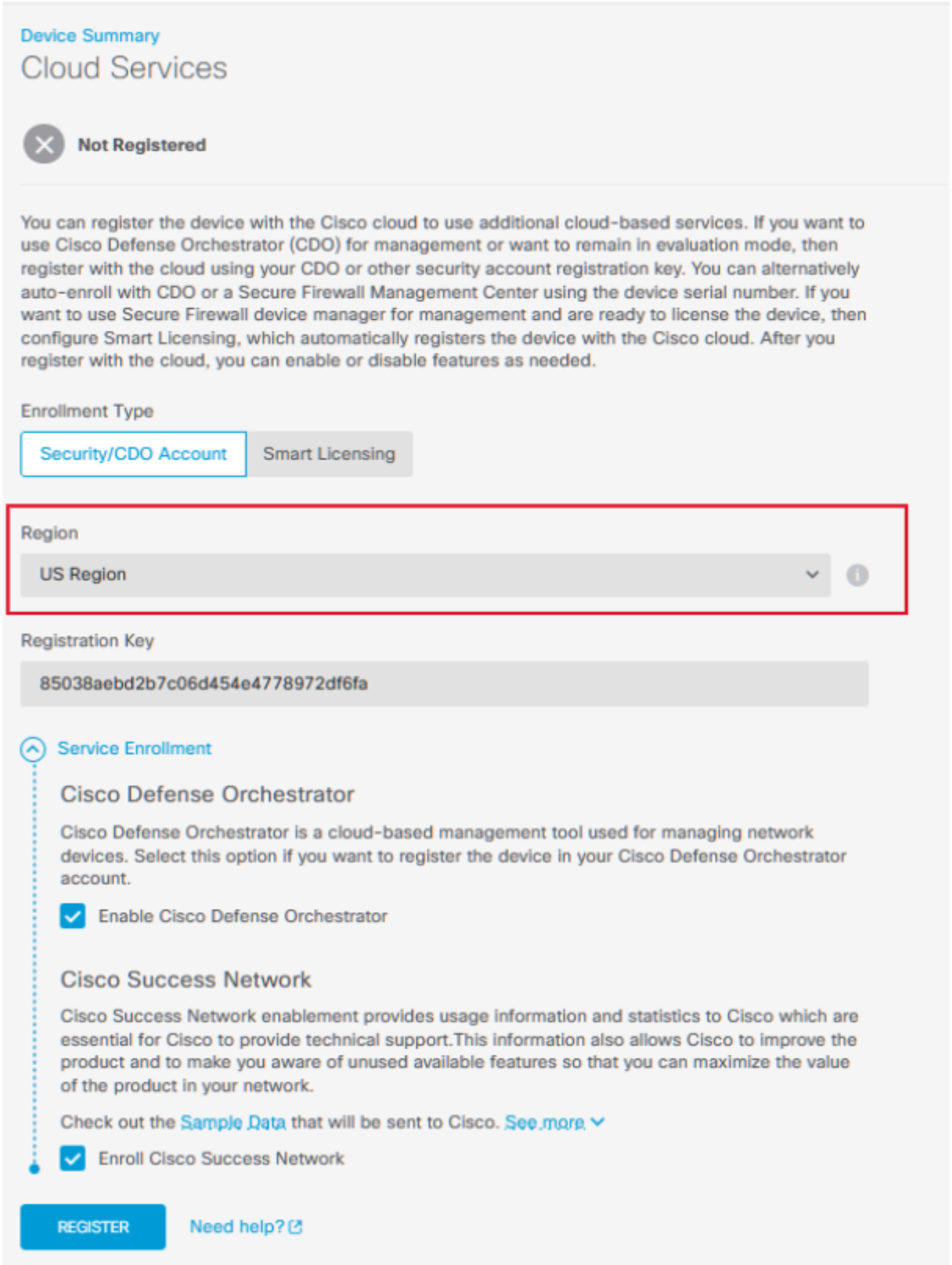
Étape 9. Accédez au périphérique Secure Firewall Device Manager destiné à l'intégration à CDO.

Étape 10. Sélectionnez Services cloud dans le menu Paramètres système.

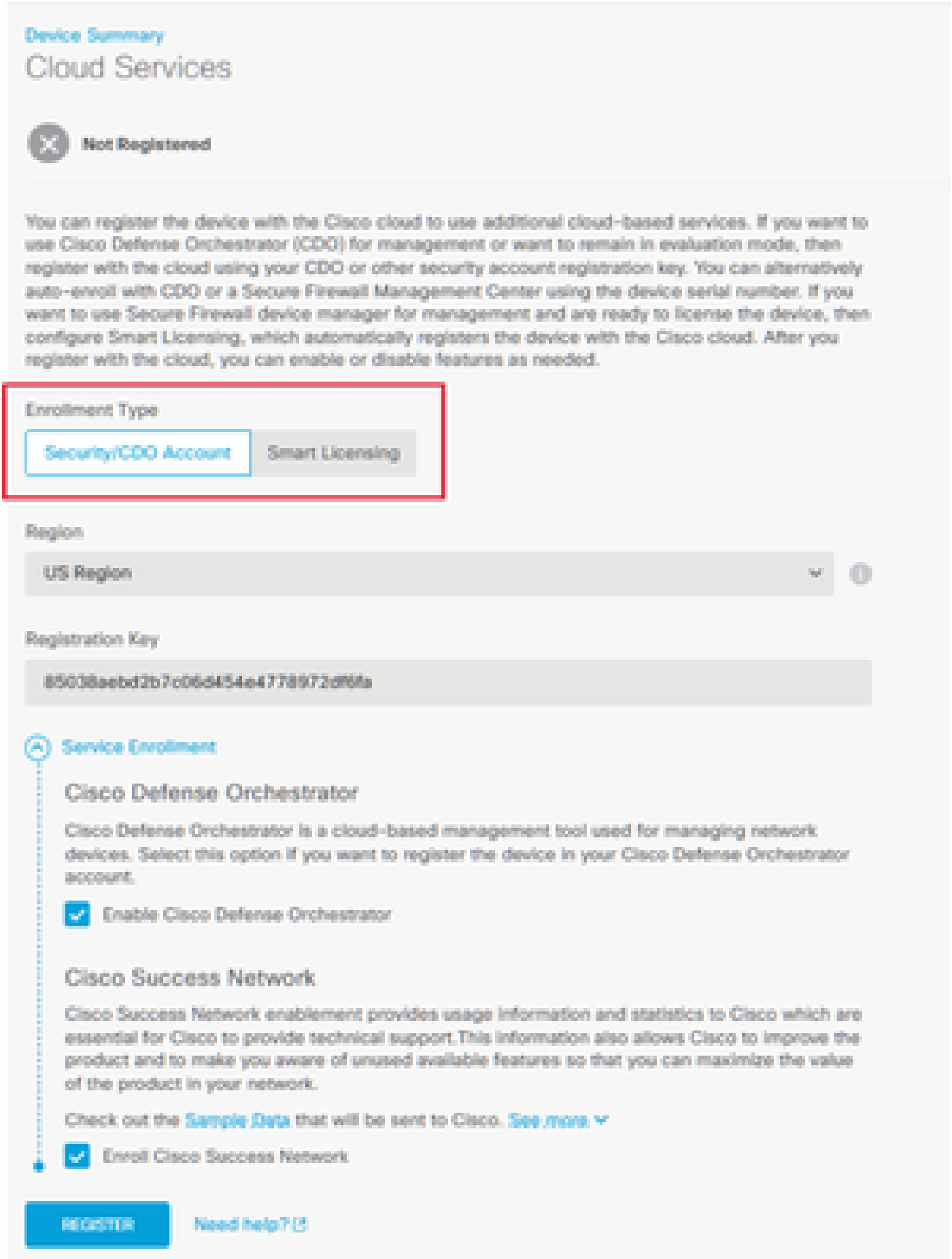


Étape 11. Désignez la région de cloud Cisco appropriée dans la liste déroulante Région, en fonction de l'emplacement géographique du locataire :

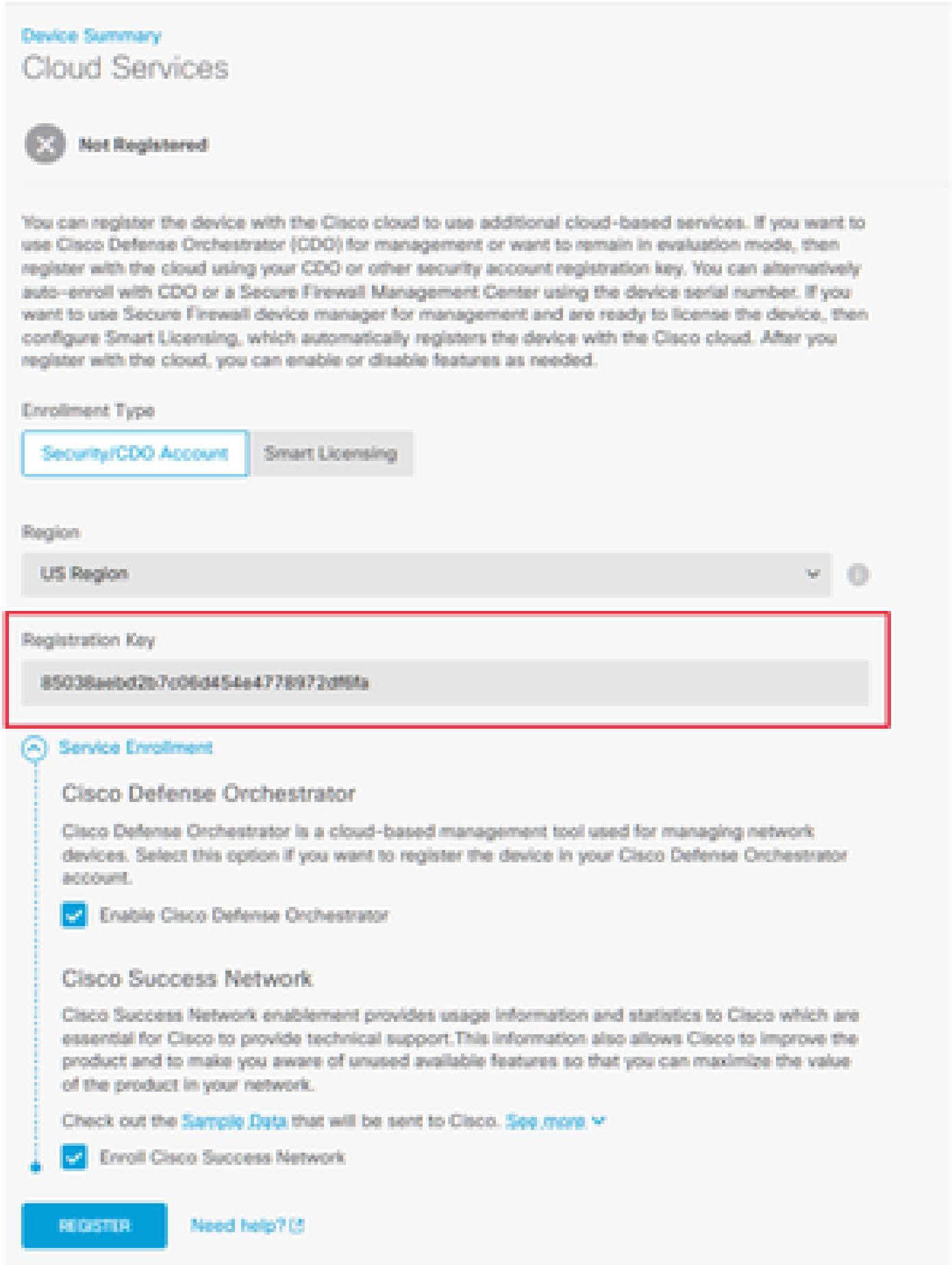
- Pour defenseorchestrator.com, sélectionnez US.
- Pour defenseorchestrator.eu, sélectionnez EU.
- Pour apj.cdo.cisco.com, sélectionnez APJ.



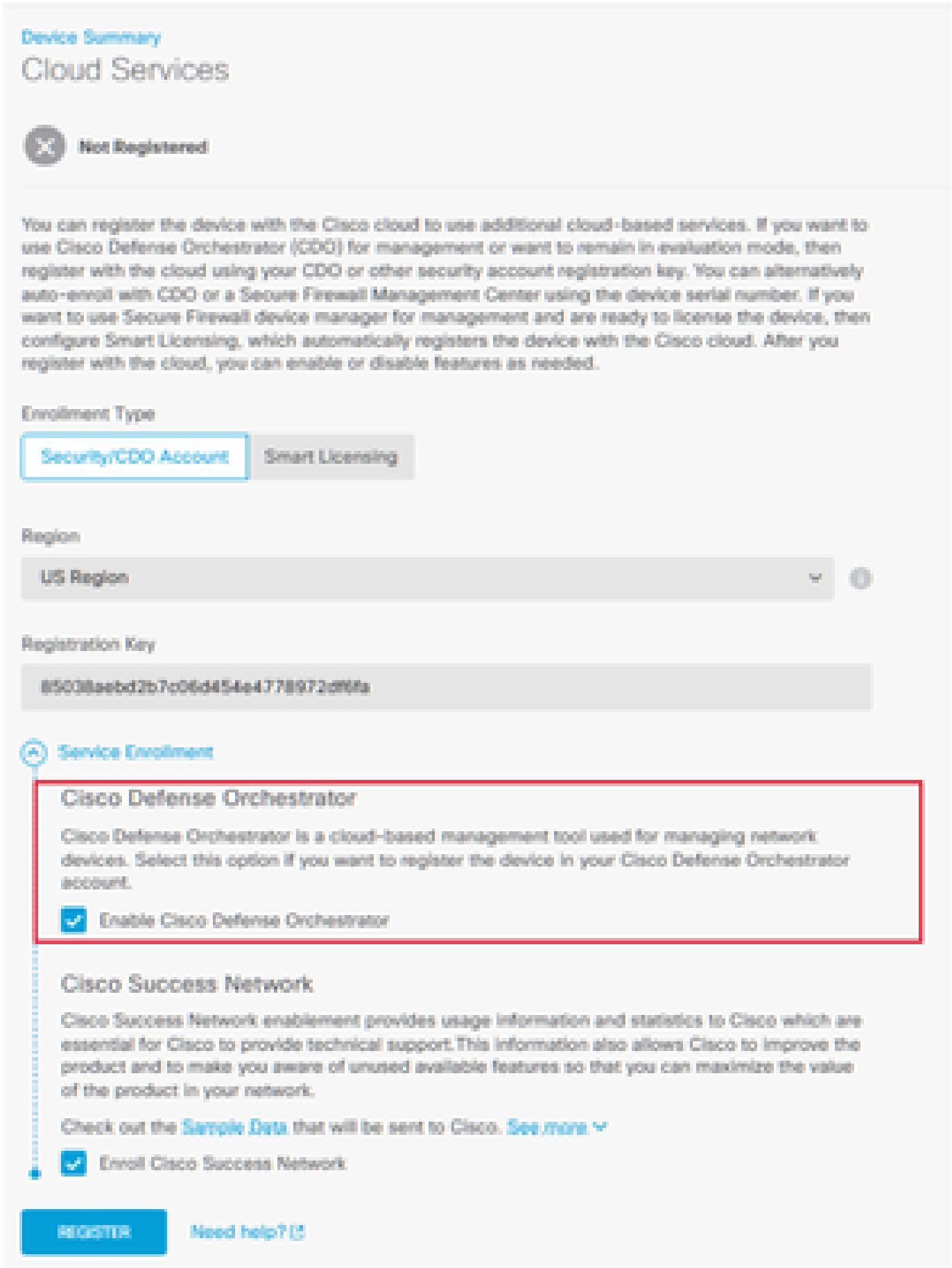
Étape 12. Dans la section Type d'inscription, sélectionnez le compte de sécurité.



Étape 13. Collez la clé d'enregistrement dans le champ Clé d'enregistrement.

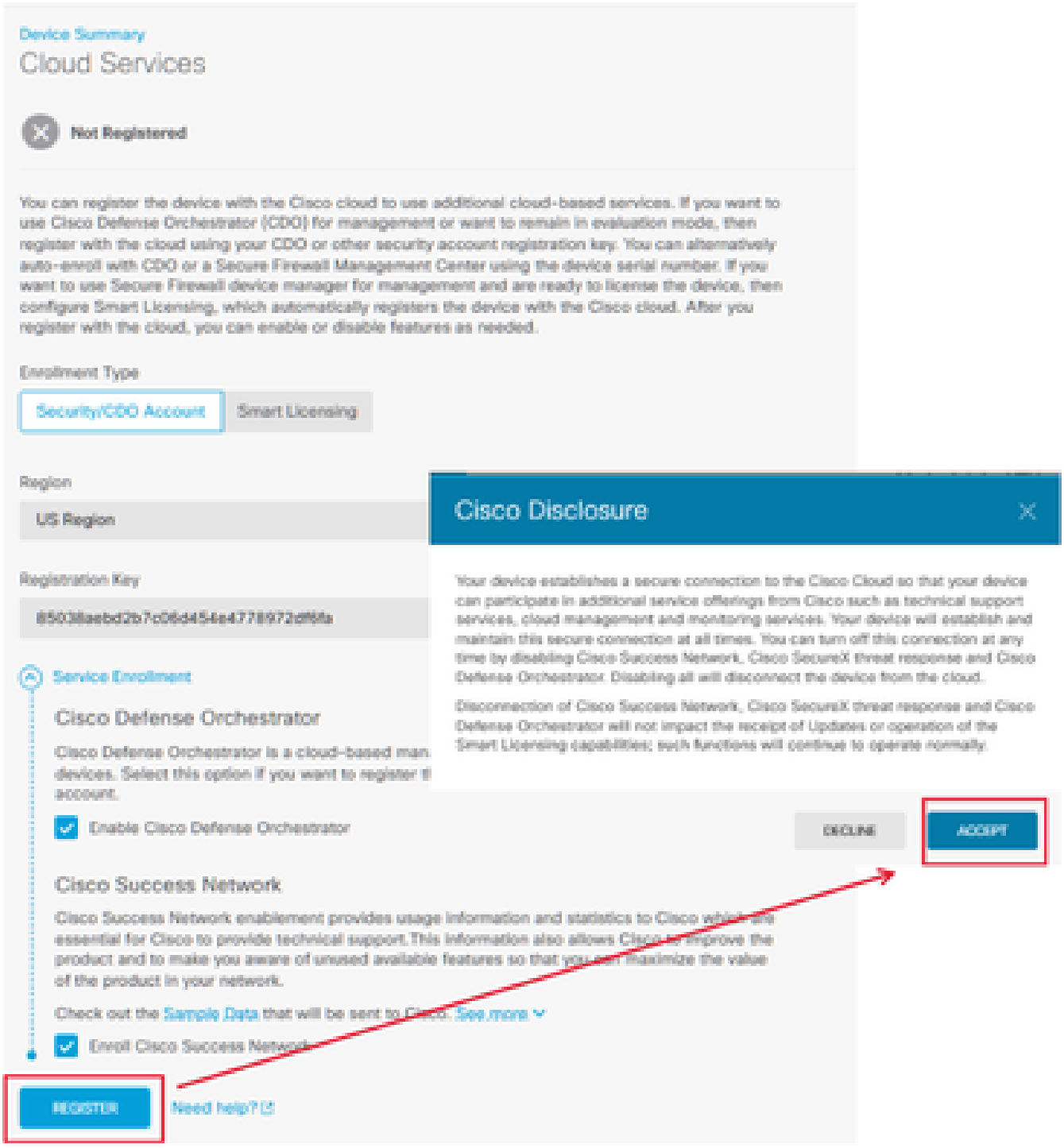


Étape 14. Pour les périphériques de la version 6.7 ou ultérieure, vérifiez que Cisco Defense Orchestrator est activé dans la section Inscription de service.



Étape 15. (Facultatif) Vérifiez les détails de l'inscription Cisco Success Network. Si vous ne souhaitez pas participer, désactivez la case à cocher Inscrire Cisco Success Network.

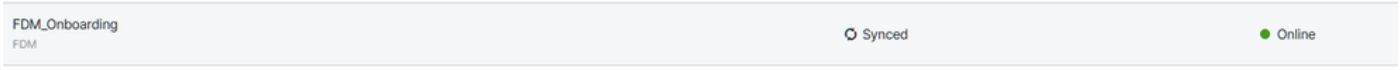
Étape 16. Sélectionnez Register et acceptez la divulgation Cisco. Le Gestionnaire de périphériques de pare-feu sécurisé envoie l'enregistrement à CDO.



Étape 17. Dans CDO, dans la zone de création de la clé d'enregistrement, sélectionnez Suivant.

Étape 18. (Facultatif) Identifiez et sélectionnez les licences destinées au périphérique, puis cliquez sur Next (Suivant).

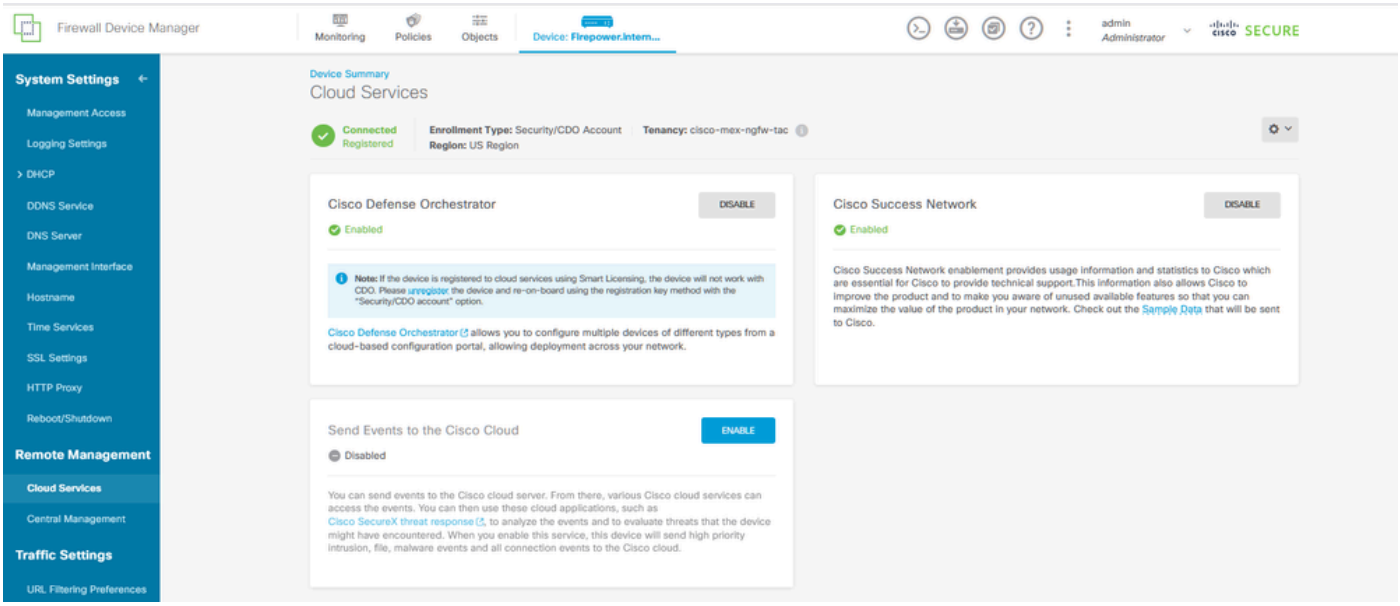
Étape 19. Observez l'état du périphérique dans la transition de l'inventaire CDO de Unprovisioned à Locating, puis à Synchronizing, et enfin, à Synced.



Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Accédez au portail CDO et vérifiez l'état du périphérique, qui indique Online et Synced. En outre, la vérification de l'état peut être effectuée via l'interface utilisateur graphique FDM. Accédez à System > Cloud Services pour observer l'état de la connexion pour Cisco Defense Orchestrator et Cisco Success Network. L'interface affiche un état Connected, confirmant l'intégration réussie avec les services.



Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Résolution de la défaillance FQDN du service cloud

Si l'enregistrement du périphérique échoue en raison d'une incapacité à résoudre le nom de domaine complet du service cloud, vérifiez la connectivité réseau ou la configuration DNS et réessayez d'intégrer le périphérique.

- Erreur de clé d'inscription non valide

Lorsque l'enregistrement du périphérique n'est pas terminé en raison de l'entrée d'une clé d'enregistrement non valide dans le Gestionnaire de périphériques de pare-feu, copiez la clé d'enregistrement correcte à partir de Cisco Defense Orchestrator et recommencez la procédure d'enregistrement. Si le périphérique dispose déjà d'une licence Smart, supprimez-la avant d'entrer la clé d'enregistrement dans le Gestionnaire de périphériques Firewall.

- Problème de licence insuffisant

Dans les cas où l'état de connectivité du périphérique indique « Licence insuffisante », procédez comme suit :

1. Attendez un certain temps pour que le périphérique obtienne la licence, car Cisco Smart Software Manager peut nécessiter un certain temps pour appliquer une nouvelle licence au périphérique.

2. Si l'état du périphérique reste inchangé, actualisez le portail CDO en vous déconnectant, puis en vous reconnectant pour résoudre d'éventuels problèmes de communication réseau entre le serveur de licences et le périphérique.

3. Si l'actualisation du portail ne met pas à jour l'état du périphérique, procédez comme suit :

    - Générez une nouvelle clé d'enregistrement à partir de Cisco Smart Software Manager et copiez-la. Reportez-vous à la vidéo Générer des licences Smart pour obtenir des conseils.
    - Dans la barre de navigation CDO, sélectionnez la page Inventaire.
    - Sélectionnez le périphérique répertorié avec l'état Licence insuffisante.
    - Dans le volet Device Details, cliquez sur Manage Licenses sous l'alerte Insuffisant Licenses. La fenêtre Gérer les licences s'affiche.
    - Dans le champ Activate, collez la nouvelle clé d'enregistrement et sélectionnez Register Device.

Une fois la nouvelle clé d'enregistrement appliquée, l'état de connectivité du périphérique doit passer à « En ligne ».

Pour obtenir des conseils complets sur l'enregistrement de Firepower Device Manager (FDM) à l'aide d'autres méthodes que la clé d'enregistrement, reportez-vous à la documentation détaillée fournie dans le lien : Dépannage des périphériques gérés par FDM.

Cette ressource propose des instructions détaillées et des conseils de dépannage pour différentes techniques d'enregistrement qui peuvent être utilisées pour intégrer avec succès FDM à Cisco Defense Orchestrator (CDO).

Informations connexes

- Dépannage des périphériques gérés par FDM
- Gestion des périphériques FDM avec Cisco Defense Orchestrator
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.