FMC 6.6.1+ - Conseils pour avant et après une mise à niveau

Contenu

Introduction

Ce document décrit les meilleures pratiques de vérification et de configuration à effectuer avant et après la mise à niveau de Cisco Secure Firewall Management Center (FMC) vers la version

6.6.1+.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Matériel : Cisco FMC 1000
- le logiciel Cisco IOS: Version 7.0.0 (build 94)

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.

Principales choses à faire avant la mise à niveau de FMC

Choisir la version du logiciel cible FMC

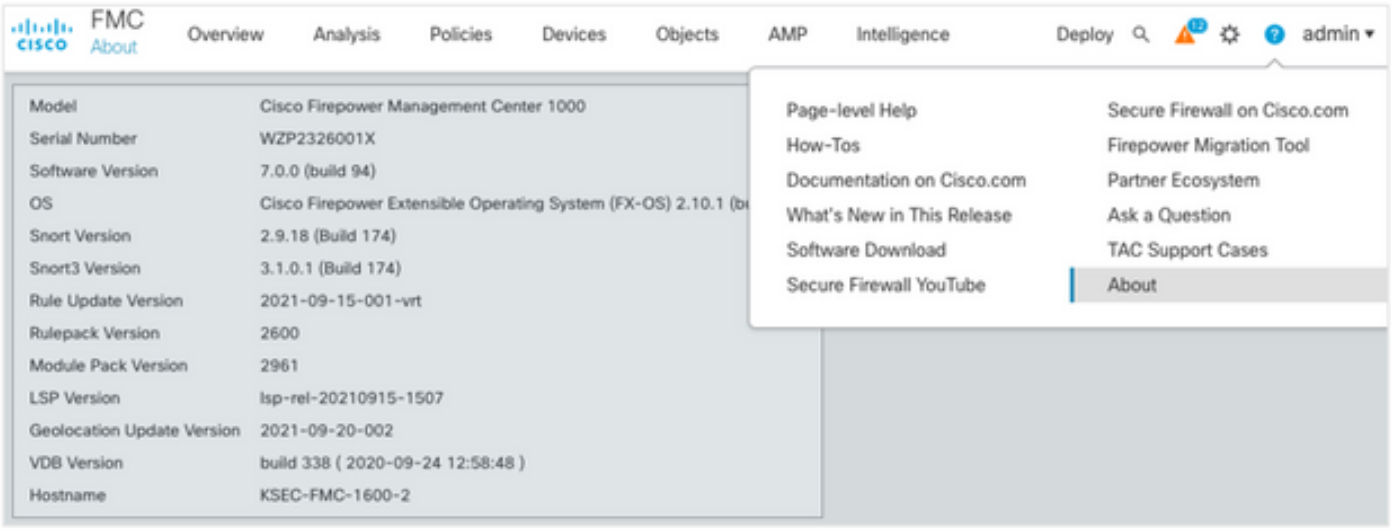
Consultez les notes de version de Firepower pour la version cible et familiarisez-vous avec :

- Compatibilité
- Fonctionnalités
- Problèmes résolus
- Problèmes identifiés

Vérifier le modèle FMC et la version logicielle actuels

Vérifiez le modèle FMC et la version du logiciel actuels :

1. Accédez à **Aide > À propos de**.
2. Vérifiez le **modèle** et la **version du logiciel**.



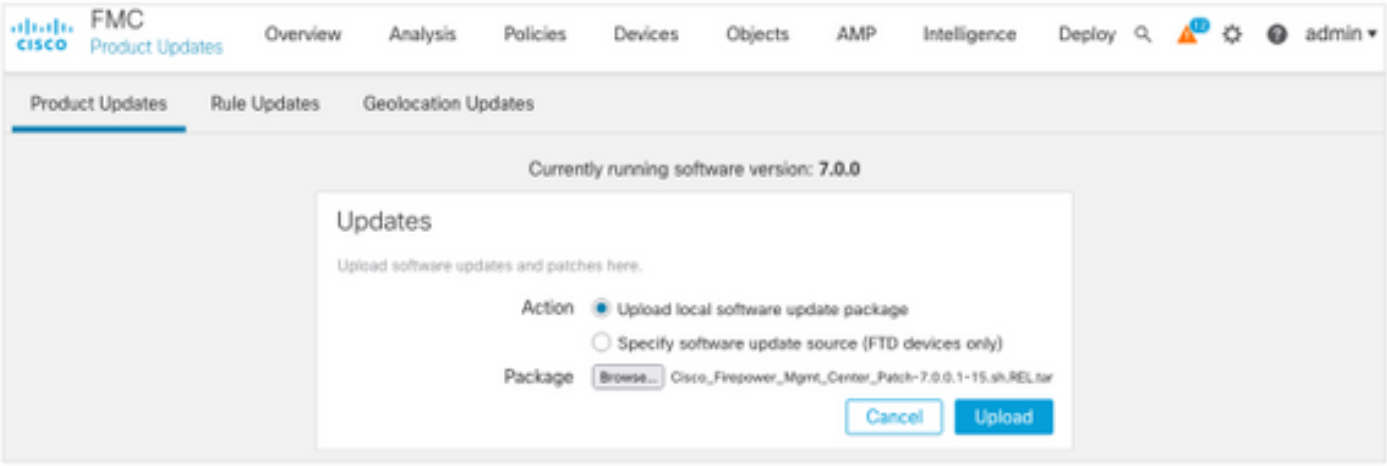
Planification du chemin de mise à niveau

Sous réserve de la version actuelle et cible du logiciel FMC, une mise à niveau intermédiaire peut être nécessaire. Dans le Guide de mise à niveau de Cisco Firepower Management Center, consultez le **chemin de mise à niveau : Firepower Management Center** et planifiez le chemin de mise à niveau.

Télécharger les packages de mise à niveau

Afin de télécharger le package de mise à niveau sur le périphérique, procédez comme suit :

1. Téléchargez le package de mise à niveau depuis la page Téléchargement de logiciel.
2. Dans FMC, accédez à **System > Updates**.
3. Sélectionnez la **mise à jour de téléchargement**.
4. Cliquez sur la case d'option **Télécharger le package de mise à jour logicielle local**.
5. Cliquez sur **Parcourir** et choisissez le package.
6. Cliquez sur **Upload** (charger).



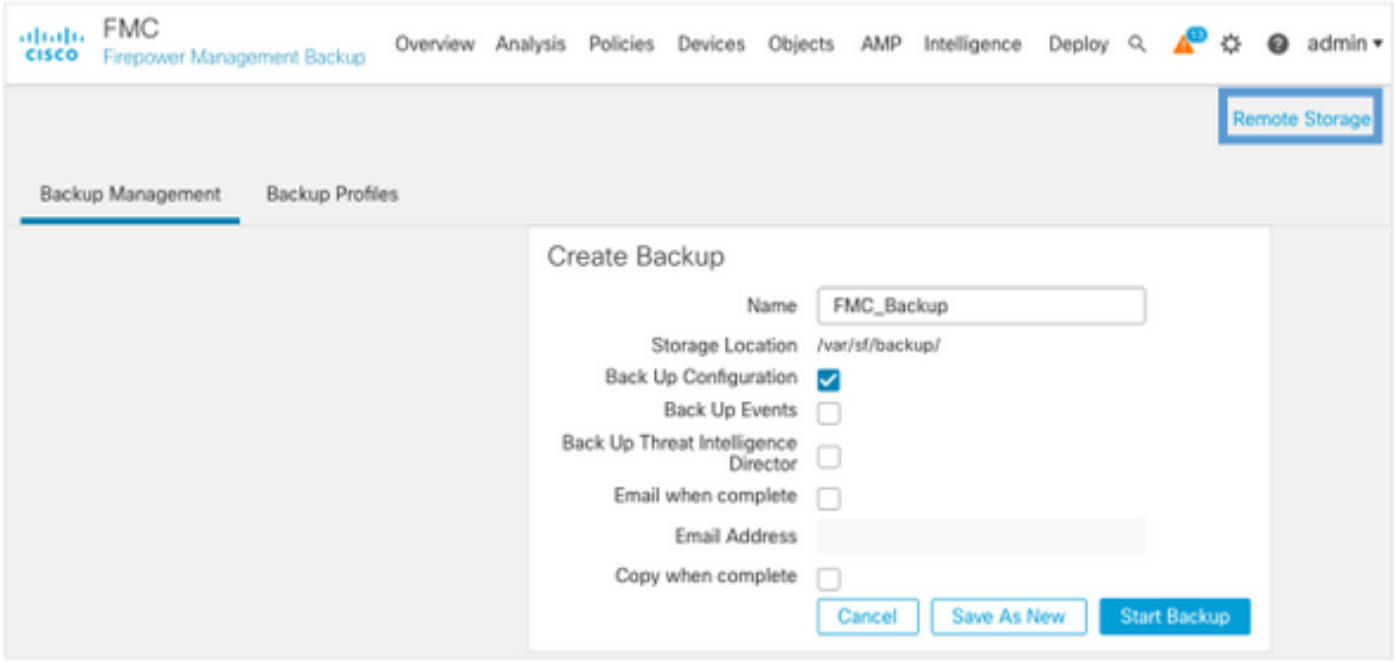
Créer la sauvegarde FMC

La sauvegarde est une étape importante de reprise après sinistre, qui permet de restaurer la configuration en cas d'échec catastrophique d'une mise à niveau.

1. Accédez à **System > Tools > Backup/Restore**.

2. Choisissez la **sauvegarde de gestion Firepower**.
3. Dans le champ **Nom**, saisissez le nom de sauvegarde.
4. Choisissez l'emplacement de stockage et les informations à inclure dans la sauvegarde.
5. Cliquez sur **Démarrer la sauvegarde**.
6. Dans **Notification > Tasks**, surveillez la progression de la création de sauvegarde.

Astuce : Nous vous recommandons vivement de sauvegarder sur un site distant sécurisé et de vérifier la réussite du transfert. Le stockage distant peut être configuré à partir de la page Gestion des sauvegardes.



Pour plus d'informations, consultez :

- Guide de configuration de Firepower Management Center, version 7.0 - Chapitre : Sauvegarde et restauration
- Guide de configuration de Firepower Management Center, version 7.0 - Gestion du stockage à distance

Vérification de la synchronisation NTP

Pour une mise à niveau FMC réussie, une synchronisation NTP est requise. Pour vérifier la synchronisation NTP, procédez comme suit :

1. Accédez à **System > Configuration > Time**.
2. Vérifiez l'**état NTP**.

Note: État : « En cours d'utilisation » indique que l'appliance est synchronisée avec le serveur NTP.

Current Setting Via NTP (based on System Configuration Time Synchronization)
Current Time 2021-09-21 13:50

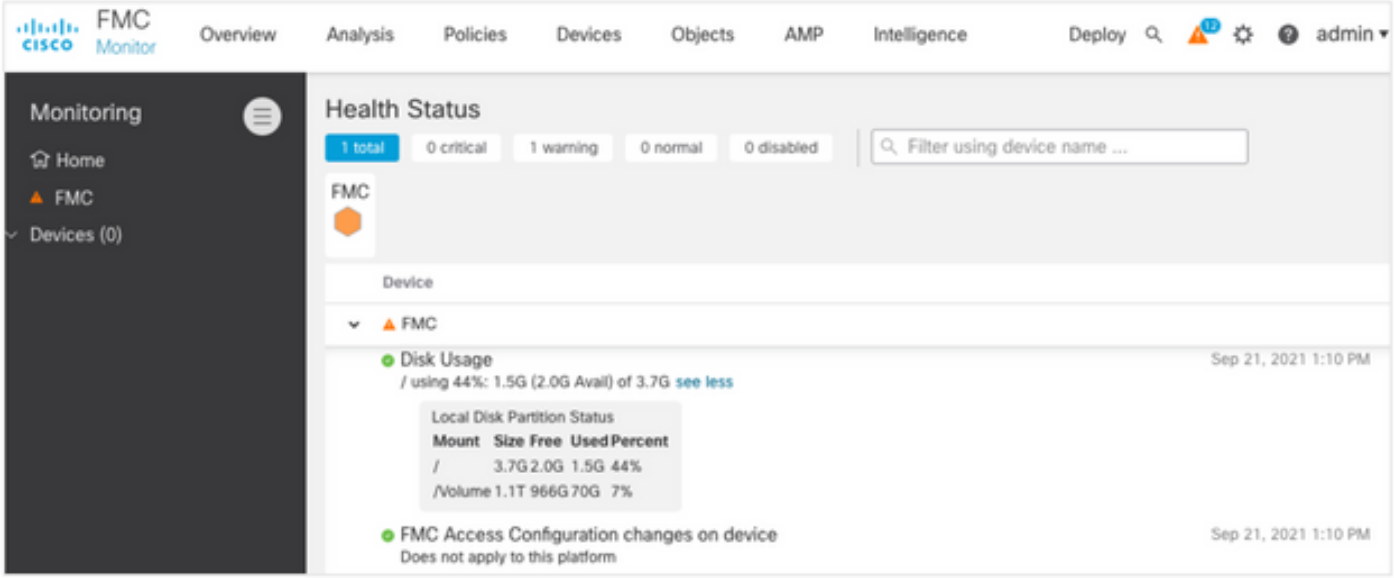
NTP Server	Status	Authentication	Offset	Last Update
173.38.201.115	Being Used	none	+0.011(milliseconds)	126(seconds)
173.38.201.67	Available	none	+0.042(milliseconds)	223(seconds)
127.127.1.1	Unknown	none	+0.000(milliseconds)	12d(seconds)

Pour plus d'informations, consultez Guide de configuration de Firepower Management Center, Version 7.0 - Synchronisation de l'heure et de l'heure.

Vérifier l'espace disque

En fonction du modèle FMC et de la version cible, assurez-vous que l'espace disque disponible est suffisant, sinon la mise à niveau échoue. Pour vérifier l'espace disque disponible de FMC, procédez comme suit :

1. Accédez à **System > Health > Monitor**.
2. Sélectionnez FMC.
3. Développez le menu et recherchez **Utilisation des disques**.
4. Les besoins en espace disque se trouvent dans Tests temporels et Espace disque requis.

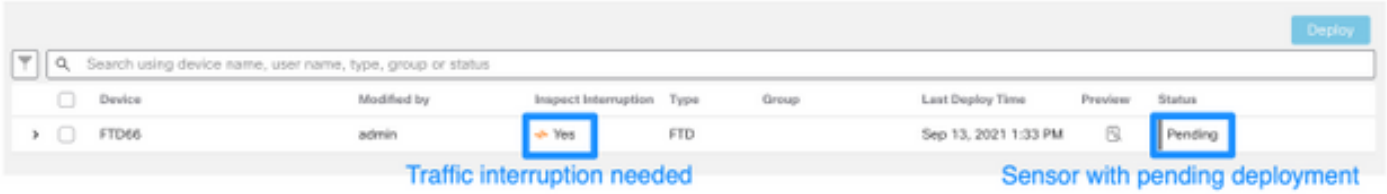


Déployer toutes les modifications de stratégie en attente

Avant l'installation de la mise à jour ou du correctif, il est nécessaire de déployer les modifications dans les capteurs. Pour vous assurer que toutes les modifications en attente sont déployées, procédez comme suit :

1. Accédez à **Déployer > Déploiement**.
2. Choisissez tous les périphériques de la liste et **Déployer**.

Attention : La colonne Interruption d'inspection indique une interruption du trafic

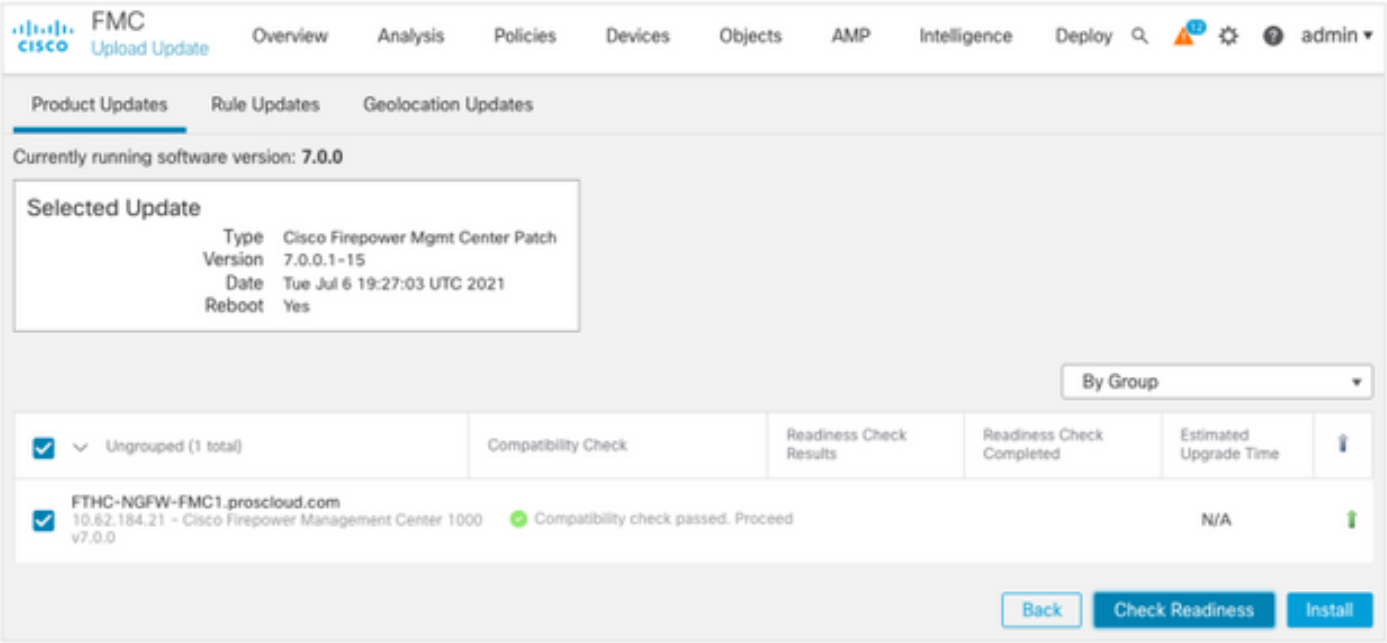


Exécuter les vérifications de préparation du logiciel Firepower

Les contrôles de préparation évaluent la préparation d'un appareil Firepower à une mise à niveau logicielle.

Afin d'effectuer les vérifications de préparation logicielle, procédez comme suit :

1. Accédez à **System > Updates**.
2. Sélectionnez l'icône **Installer** en regard de la version cible.
3. Choisissez le FMC et cliquez sur **Vérifier la préparation**.
4. Dans la fenêtre contextuelle, cliquez sur **OK**.
5. Surveillez le processus de vérification du niveau de préparation à partir de **Notifications > Tâches**.



Pour plus d'informations, reportez-vous au Guide de mise à niveau de Cisco Firepower Management Center - Contrôles de préparation du logiciel Firepower.

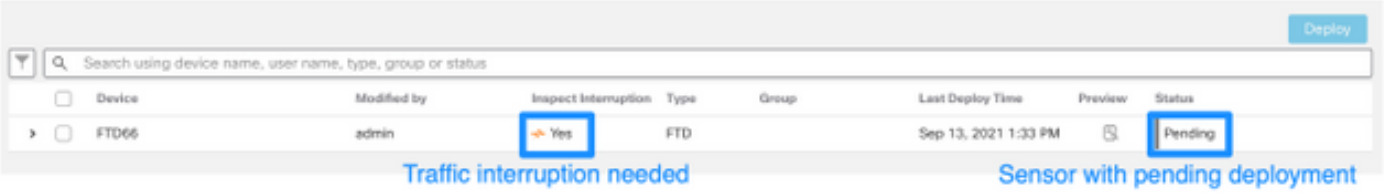
Principales choses à faire après la mise à niveau de FMC

Déployer toutes les modifications de stratégie en attente

Immédiatement après chaque mise à jour ou installation de correctifs, il est nécessaire de déployer les modifications dans les capteurs. Pour vous assurer que toutes les modifications en attente sont déployées, procédez comme suit :

1. Accédez à **Déployer > Déploiement**.
2. Choisissez tous les périphériques de la liste et cliquez sur **Déployer**.

Attention : La colonne Interruption d'inspection indique une interruption du trafic



Vérifier si la dernière base de données de vulnérabilité et d'empreintes digitales est installée

Afin de vérifier la version actuelle de l'empreinte digitale (VDB), procédez comme suit :

1. Accédez à **Aide > À propos de**.
2. Vérifiez la **version VDB**.

Afin de télécharger les mises à jour VDB directement à partir de cisco.com, l'accessibilité de FMC à cisco.com est requise.

1. Accédez à **System > Updates > Product Updates**.
2. Sélectionnez **Télécharger les mises à jour**.
3. Installez la dernière version disponible.
4. Vous devez redéployer les capteurs par la suite.

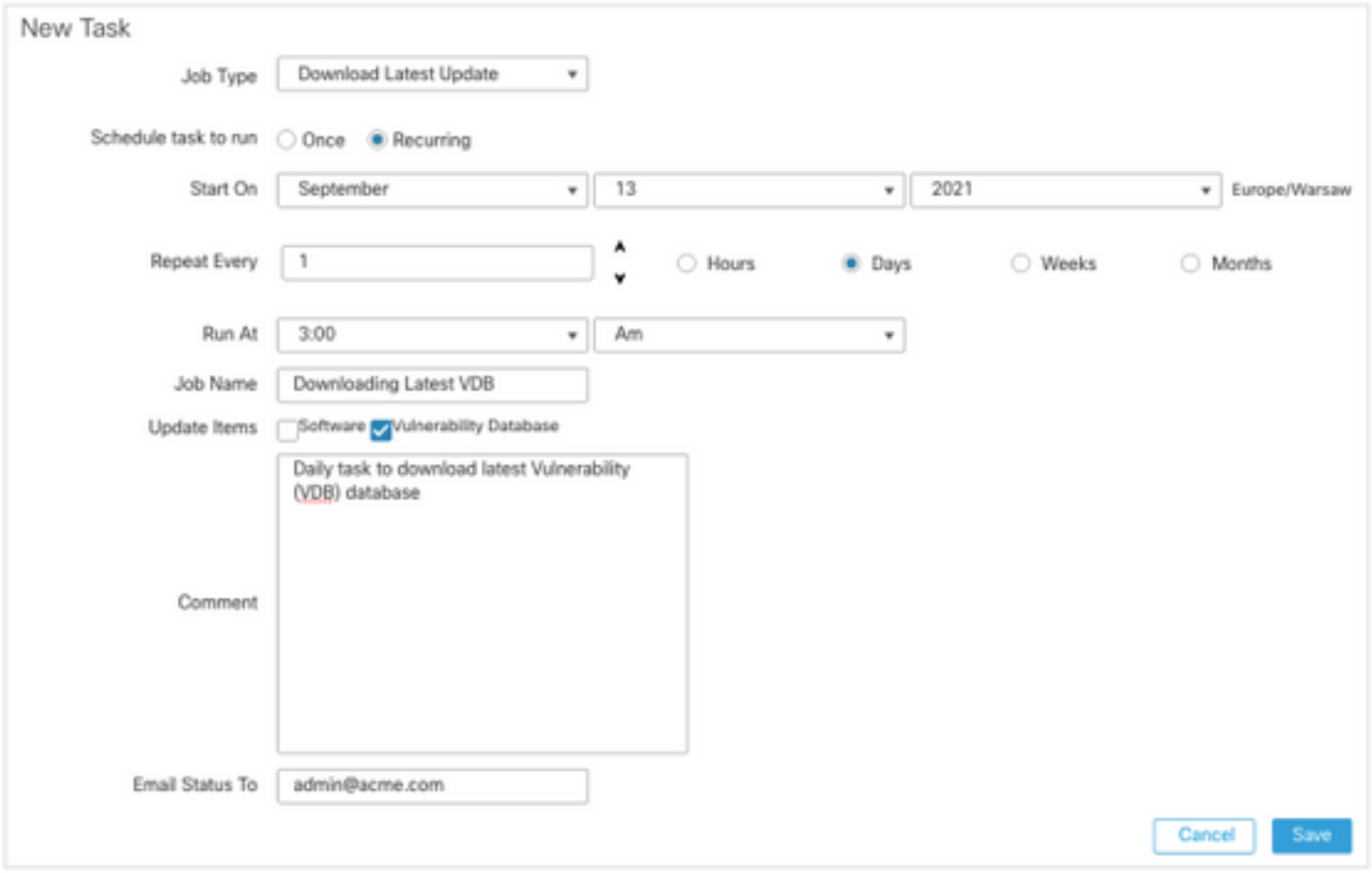
Note: Si le FMC n'a pas accès à Internet, le package VDB peut être téléchargé directement à partir de software.cisco.com.

Il est recommandé de planifier des tâches pour effectuer des téléchargements et des installations automatiques de packages VDB.

Par mesure de précaution, vérifiez les mises à jour VDB quotidiennes et installez-les sur le FMC pendant les week-ends.

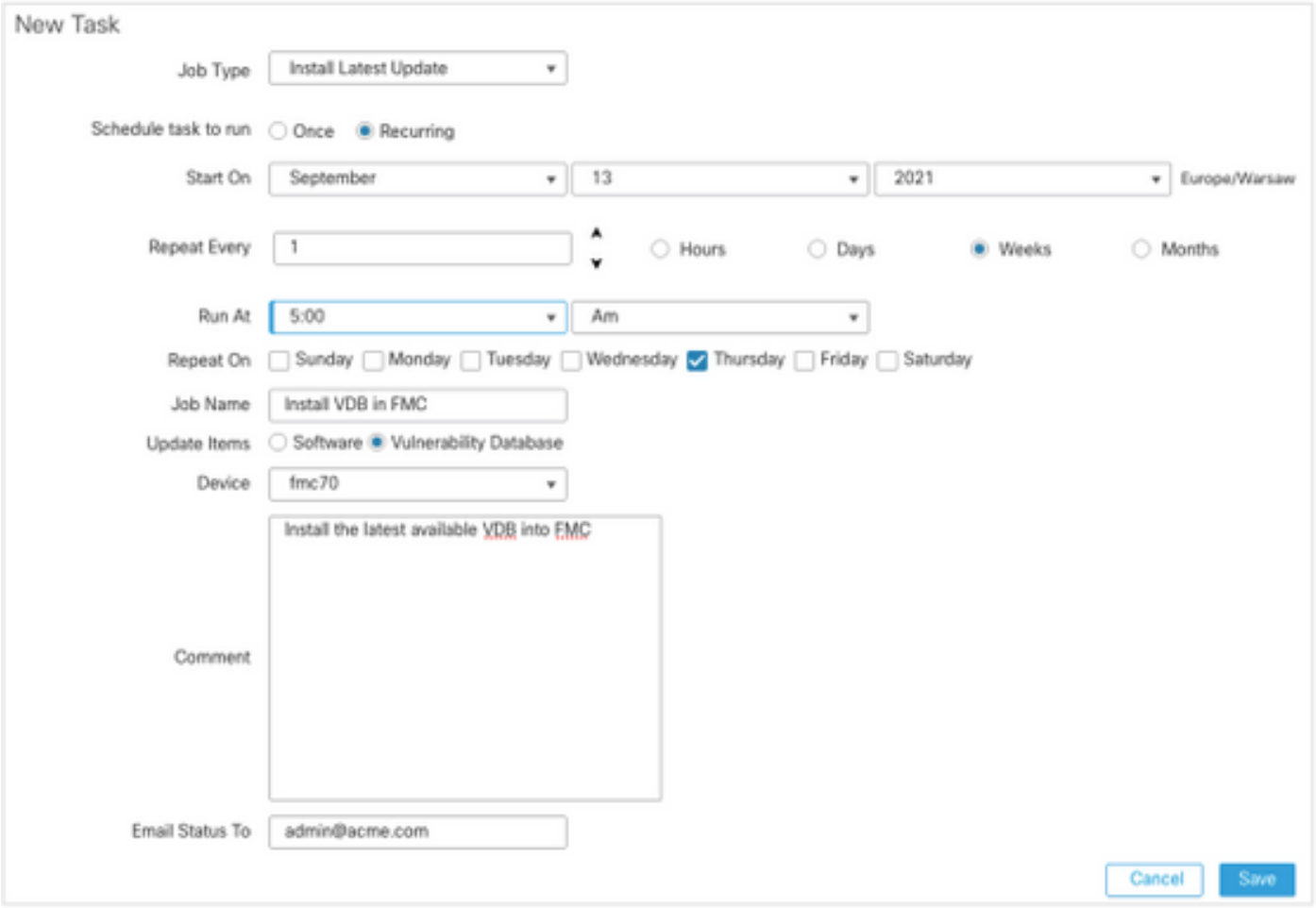
Afin de vérifier la VDB quotidiennement à partir de www.cisco.com, complétez ces étapes :

1. Accédez à **Système > Outils > Planification**.
2. Cliquez sur **Ajouter une tâche**.
3. Dans la liste déroulante **Type de tâche**, sélectionnez **Télécharger la dernière mise à jour.**
4. Pour **exécuter la tâche Planification**, cliquez sur la case d'option **Périodique.**
5. Répétez la tâche tous les jours et exécutez-la à 3h00 ou en dehors des heures de bureau.
6. Pour les **éléments de mise à jour**, cochez la case **Base de données de vulnérabilité.**



Afin d'installer la dernière VDB dans le FMC, définissez la tâche périodique chaque semaine :

1. Accédez à **Système > Outils > Planification**.
2. Cliquez sur **Ajouter une tâche**.
3. Dans la liste déroulante **Type de tâche**, sélectionnez **Installer la dernière mise à jour**.
4. Pour **programmer l'exécution de la tâche**, cliquez sur la case d'option **Périodique**.
5. Répétez la tâche toutes les 1 semaines et exécutez-la à 5h00 ou en dehors des heures de bureau.
6. Pour les **éléments de mise à jour**, cochez la case **Base de données de vulnérabilité.**



Pour plus d'informations, consultez Guide de configuration de Firepower Management Center, Version 7.0 - Mise à jour de la base de données de vulnérabilité (VDB)

Vérifier la version actuelle de la règle Snort et du package de sécurité léger

Afin de vérifier les versions actuelles de la règle Snort (SRU), du package de sécurité léger (LSP) et de la géolocalisation, procédez comme suit :

1. Accédez à **Aide > À propos de**.
2. Vérifiez la **version de mise à jour des règles** et la **version LSP**.

Pour télécharger la SRU et le LSP directement à partir de www.cisco.com, il est nécessaire d'être joignable de la FMC à www.cisco.com.

1. Accédez à **System > Updates > Rule Updates**.
2. Dans l'onglet **One-Time Rule Update/Rules Import**, sélectionnez **Download new rule update from the Support Site**.
3. Choisissez **Importer**.
4. Déployez ensuite la configuration sur les capteurs.

Note: Si le FMC n'a pas accès à Internet, les packages SRU et LSP peuvent être téléchargés directement à partir de software.cisco.com.

Les mises à jour des règles d'intrusion sont cumulatives et il est recommandé de toujours importer la dernière mise à jour.

Afin d'activer le téléchargement et le déploiement hebdomadaires des mises à jour des règles Snort (SRU/LSP), procédez comme suit :

1. Accédez à **System > Updates > Rule Updates**.
2. Dans l'onglet **Importations de mise à jour périodique des règles**, cochez la case **Activer les importations de mise à jour périodique des règles à partir du site de support**.
3. Choisissez la fréquence d'importation hebdomadaire, choisissez un jour de la semaine et en fin d'après-midi pour le téléchargement et le déploiement des stratégies.
4. Click **Save**.

Pour plus d'informations, consultez Guide de configuration de Firepower Management Center, Version 7.0 - Mettre à jour les règles d'intrusion.

Vérifier la version actuelle de la mise à jour de géolocalisation

Afin de vérifier la version actuelle de Geolocation, procédez comme suit :

1. Accédez à **Aide > À propos de**.
2. Vérifiez la **version de mise à jour de géolocalisation**.

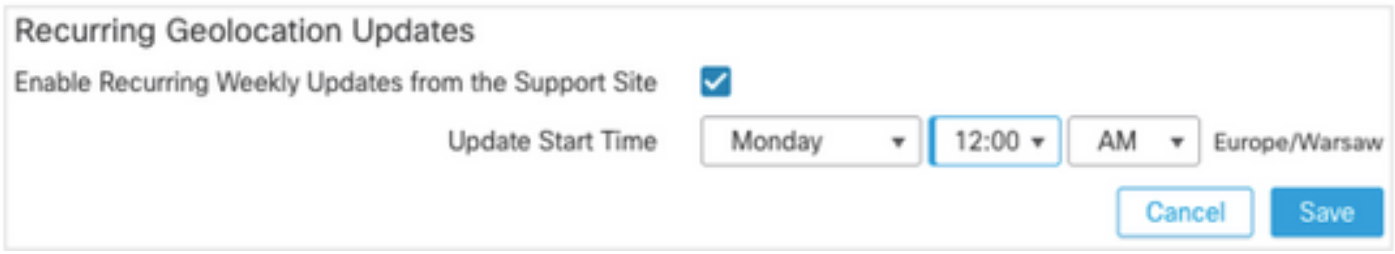
Pour télécharger les mises à jour de géolocalisation directement à partir de www.cisco.com, il est nécessaire d'être joignable du FMC à www.cisco.com.

1. Accédez à **Système > Mises à jour > Mises à jour de géolocalisation**.
2. Dans l'onglet **Mise à jour ponctuelle de la géolocalisation**, sélectionnez **Télécharger et installer la mise à jour de la géolocalisation à partir du site de support**.
3. Cliquez sur **Import**.

Note: Si le FMC n'a pas accès à Internet, le package Geolocation Updates peut être téléchargé directement à partir de software.cisco.com.

Pour activer les mises à jour de géolocalisation automatiques, procédez comme suit :

1. Accédez à **Système > Mises à jour > Mises à jour de géolocalisation**.
2. Dans la section Mises à jour de géolocalisation récurrentes, cochez la case **Activer les mises à jour hebdomadaires récurrentes à partir du site de support**.
3. Choisissez la fréquence d'importation hebdomadaire, choisissez le lundi à minuit.
4. Click **Save**.

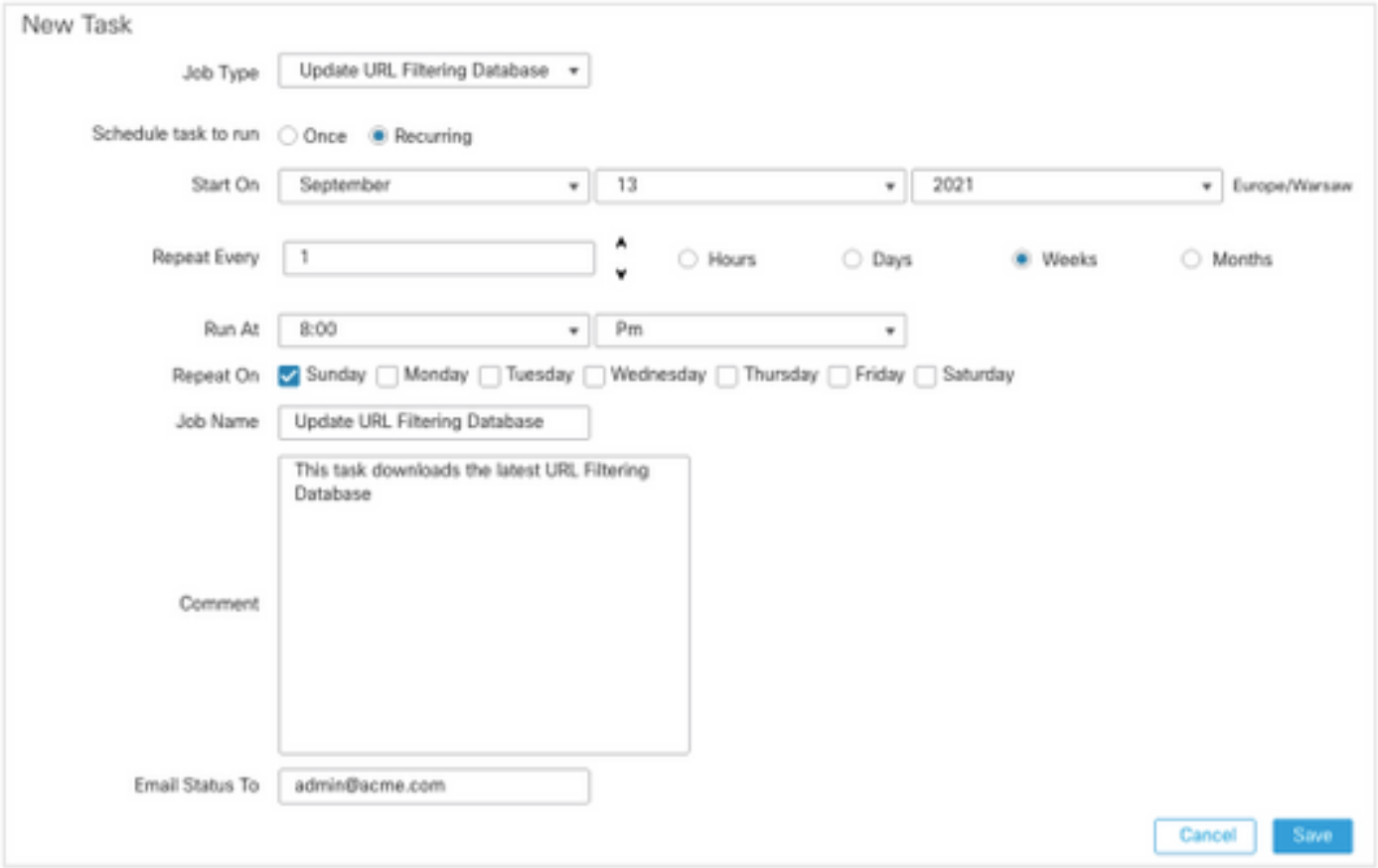


Pour plus d'informations, consultez Guide de configuration de Firepower Management Center, Version 7.0 - Mettre à jour la base de données de géolocalisation (GeoDB).

Automatiser la mise à jour de la base de données de filtrage des URL avec une tâche planifiée

Afin de s'assurer que les données de menace pour le filtrage des URL sont à jour, le système doit obtenir des mises à jour de données à partir du cloud Cisco CSI (Collective Security Intelligence). Pour automatiser ce processus, procédez comme suit :

1. Accédez à **Système > Outils > Planification**.
2. Cliquez sur **Ajouter une tâche**.
3. Dans la liste déroulante **Type de tâche**, sélectionnez **Mettre à jour la base de données de filtrage des URL.**
4. Pour **exécuter la tâche Planification**, cliquez sur la case d'option **Périodique**.
5. Répétez la tâche chaque semaine et exécutez-la à 20 h le dimanche ou en dehors des heures d'ouverture.
6. Click **Save**.

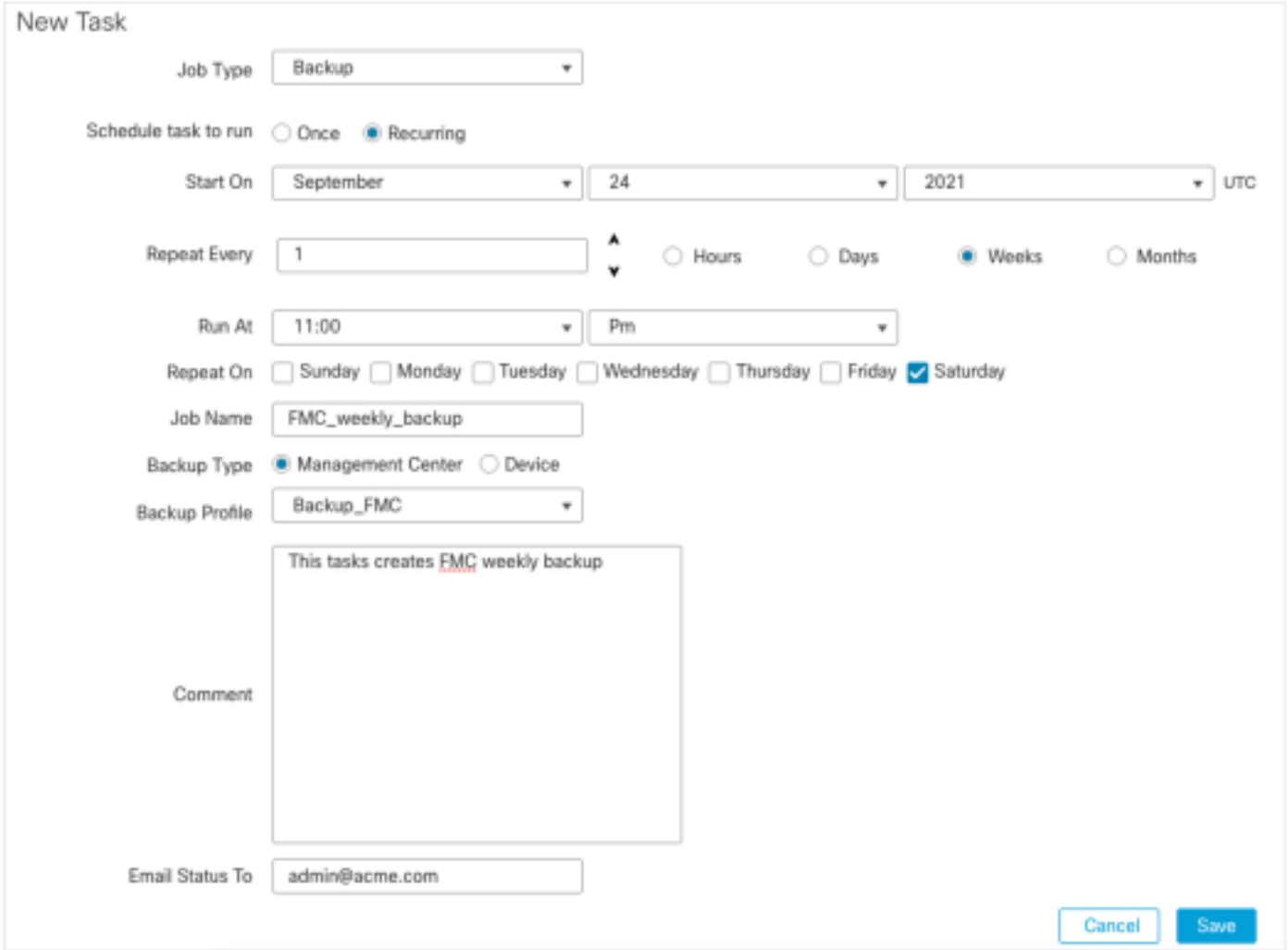


Pour plus d'informations, reportez-vous au Guide de configuration de Firepower Management Center, Version 7.0 - Automating URL Filtering Updates Using a Scheduled Task.

Configurer des sauvegardes périodiques

Dans le cadre du plan de reprise après sinistre, il est recommandé d'effectuer des sauvegardes périodiques.

1. Vérifiez que vous êtes dans le **domaine global**.
2. Créez le profil de sauvegarde FMC. Pour plus d'informations, consultez la section **Créer la sauvegarde FMC**.
3. Accédez à **Système > Outils > Planification**.
4. Cliquez sur **Ajouter une tâche**.
5. Dans la liste déroulante **Type de tâche**, sélectionnez **Sauvegarder.**
6. Pour **exécuter la tâche Planification**, cliquez sur la case d'option **Périodique**.
   La fréquence de sauvegarde doit être ajustée en fonction des besoins de l'entreprise. Nous vous recommandons de créer des sauvegardes lors d'une fenêtre de maintenance ou d'autres périodes d'utilisation réduite.
7. Pour **Type de sauvegarde**, cliquez sur la case d'option **Management Center**.
8. Dans la liste déroulante **Profil de sauvegarde**, sélectionnez Profil de sauvegarde.
9. Click **Save**.

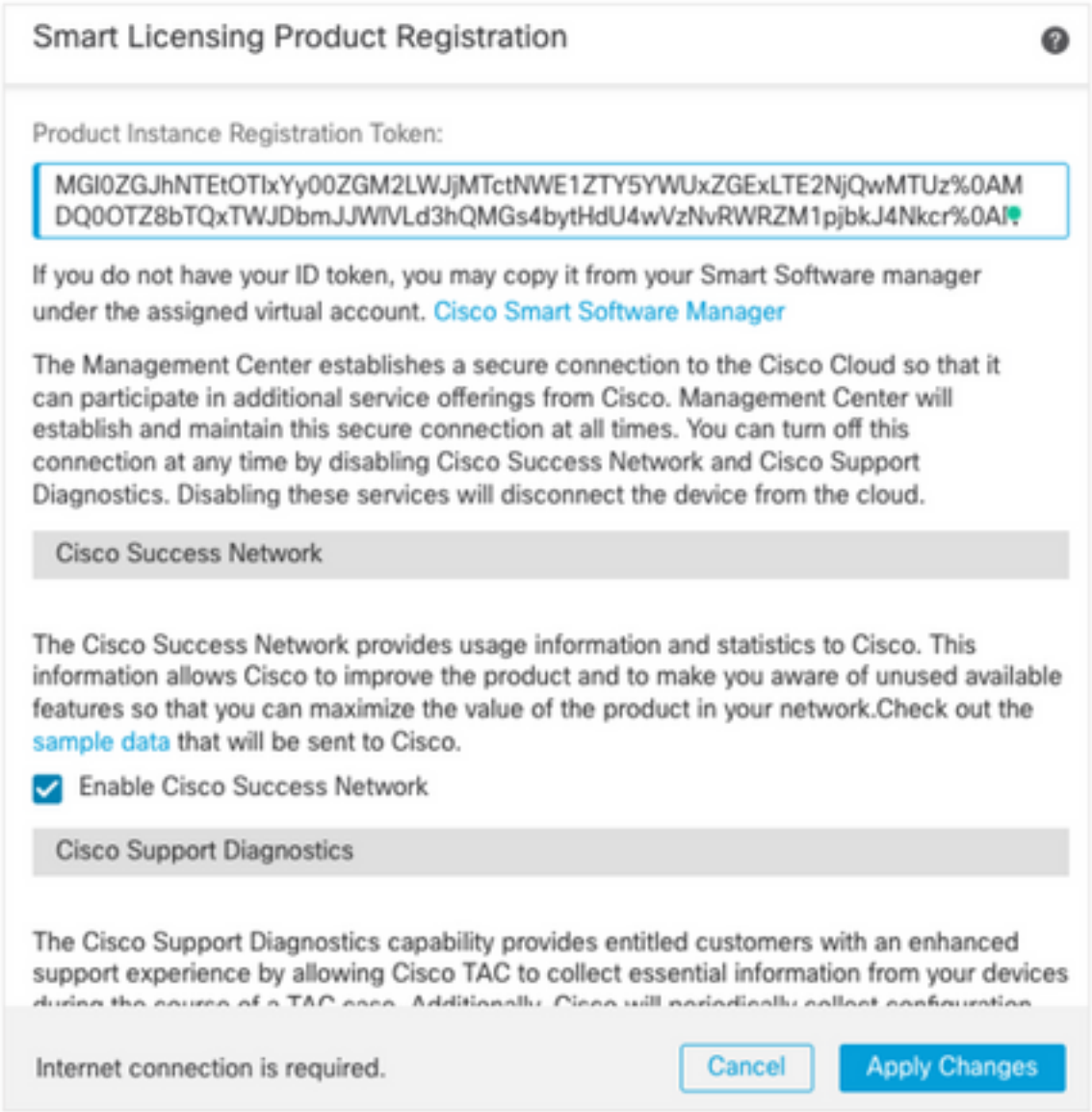


Pour plus d'informations, consultez Guide de configuration de Firepower Management Center, Version 7.0 - Chapitre : Sauvegarde et restauration.

S'assurer que la licence Smart est enregistrée

Pour enregistrer Cisco Firewall Management Center auprès de Cisco Smart Software Manager, procédez comme suit :

1. Dans https://software.cisco.com, accédez à **Smart Software Manager > Gérer les licences**.
2. Accédez à **Inventory > General** tab et créez un **nouveau jeton**.
3. Dans l'interface FMC, accédez à **System > Licenses > Smart Licenses**.
4. Cliquez sur **Register**.
5. Insérez le jeton généré dans le portail Cisco Smart Software Licensing.
6. Assurez-vous que **Cisco Success Network est activé**.
7. Cliquez sur **Appliquer les modifications**.
8. Vérifiez L'État De La Licence Smart.



Pour plus d'informations, consultez Guide de configuration de Firepower Management Center, Version 7.0 - Enregistrer les licences Smart.

Vérifier la configuration des jeux de variables

Assurez-vous que la variable HOME_NET contient uniquement les réseaux/sous-réseaux internes de l'organisation. Une définition incorrecte des jeux de variables a un impact négatif sur les performances du pare-feu.

1. Accédez à **Objets > Jeu de variables**.
2. Modifiez le jeu de variables utilisé par votre stratégie d'intrusion. Il est autorisé à avoir une variable définie par stratégie d'intrusion avec différents paramètres.
3. Ajustez les variables en fonction de votre environnement et cliquez sur **Enregistrer**.

Les autres variables d'intérêt sont DNS_SERVERS OU HTTP_SERVERS.

Pour plus d'informations, consultez Guide de configuration de Firepower Management Center, Version 7.0 - Jeux de variables.

Vérification de l'activation des services cloud

Afin de tirer parti des différents services cloud, nAccédez à **System > Integration > Cloud Services**.

Filtrage des URL

1. Activez le filtrage des URL et activez les mises à jour automatiques, puis interrogez Cisco Cloud sur les URL inconnues.
   Une expiration plus fréquente des URL du cache nécessite davantage de requêtes vers le cloud, ce qui entraîne des charges Web plus lentes.
2. **Enregistrer les modifications.**

Astuce : Pour l'expiration de l'URL du cache, laissez la valeur par défaut **Jamais**. Si une reclassification Web plus stricte est nécessaire, ce paramètre peut être modifié en conséquence.

AMP pour les réseaux

1. Vérifiez que les deux paramètres sont activés : **Activez les mises à jour locales automatiques de détection des programmes malveillants** et **partagez l'URI des événements de programmes malveillants avec Cisco**.
2. Dans FMC 6.6.X, désactivez l'utilisation du port hérité 32137 pour AMP for Networks, de sorte que le port TCP utilisé à la place est 443.
3. **Enregistrer les modifications.**

Note: Ce paramètre n'est plus disponible dans FMC 7.0+ et le port est toujours 443.

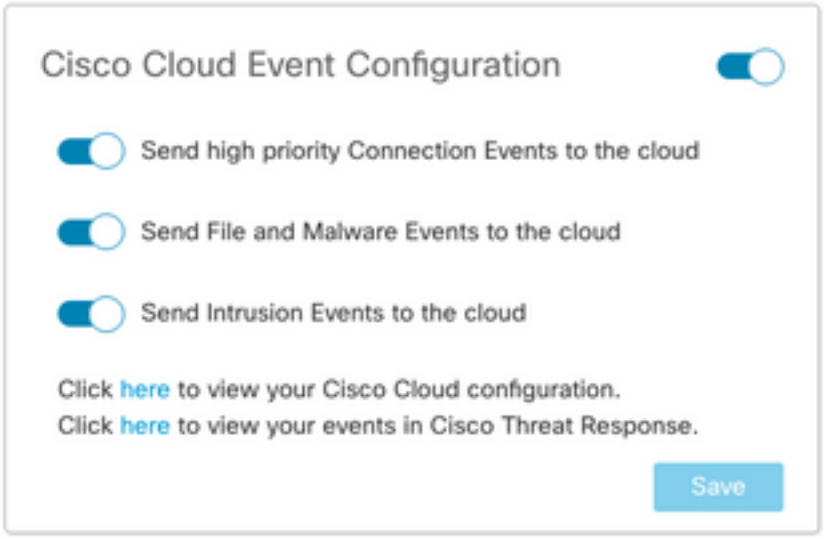
Région cloud de Cisco

1. La région du cloud doit correspondre à la région de l'organisation SecureX. Si l'organisation SecureX n'est pas créée, choisissez la région la plus proche de l'installation FMC : région APJ, région UE ou région US.
2. **Enregistrer les modifications.**

Configuration des événements cloud Cisco

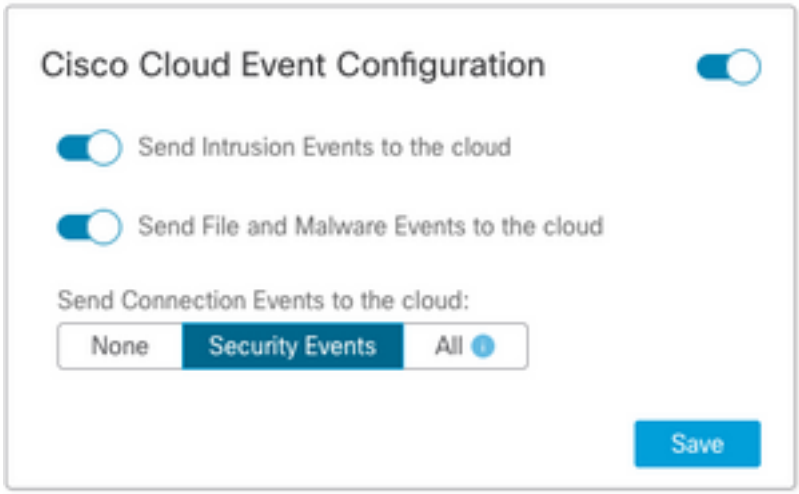
Pour FMC 6.6.x

1. Vérifiez les trois options : **Envoyez des événements de connexion hautement prioritaires dans le cloud**, **envoyez des événements de fichiers et de programmes malveillants dans le cloud** et **envoyez des événements d'intrusion dans le cloud**.
2. **Enregistrer les modifications.**



Pour FMC 7.0+

1. Assurez-vous que les deux options sont sélectionnées : **Envoyer des événements d'intrusion dans le cloud** et **envoyer des événements de fichiers et de programmes malveillants dans le cloud**.
2. Pour le type d'événements de connexion, sélectionnez **Tous** si la solution Security Analytics and Logging est utilisée. Pour SecureX, sélectionnez uniquement **Événements de sécurité**.
3. **Enregistrer les modifications.**



Activer l'intégration SecureX

L'intégration de SecureX offre une visibilité instantanée sur le paysage des menaces à travers vos produits de sécurité Cisco. Pour connecter SecureX et activer le ruban, procédez comme suit :

Intégrer le ruban SecureX

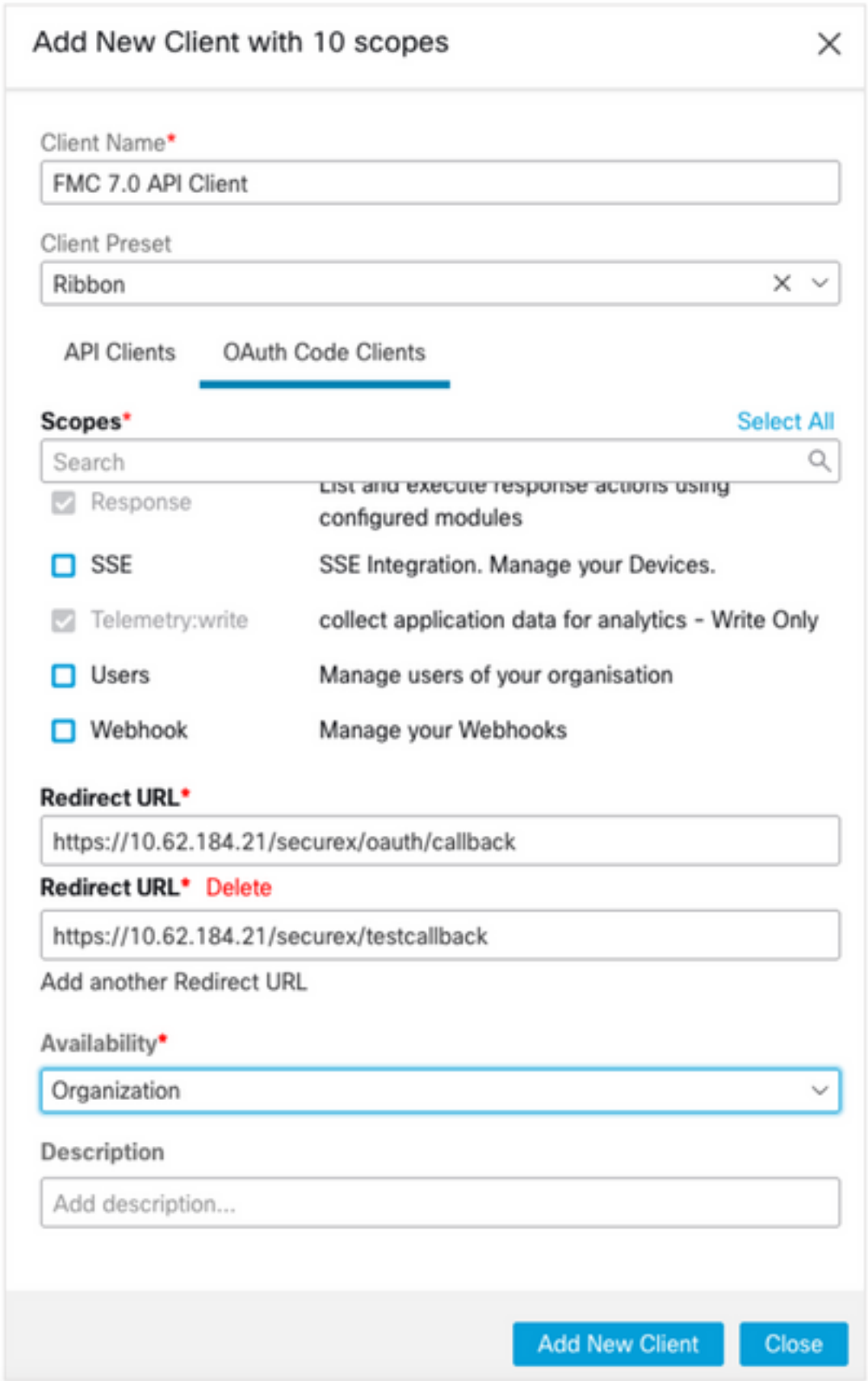
Note: Cette option est disponible pour FMC version 7.0+.

1. Connectez-vous à SecureX et créez un client API : Dans le champ **Nom du client**, saisissez un nom descriptif du FMC. Par exemple, le client API FMC 7.0.Cliquez sur l'onglet **Clients de code de** qualité.Dans la liste déroulante **Client Preset**, sélectionnez **Ruban**. Il choisit les étendues : Casebook, Enrich:read, Global Intel:read, Inspect:read, Notification, Orbital, Private Intel, Profile, Response, Telemetry:write.Ajoutez les deux URL de redirection présentées dans le FMC :

URL de redirection : <URL_FMC>/securex/oauth/callback

Deuxième URL de redirection : <URL_FMC>/securex/testcallback

1. Dans la liste déroulante **Disponibilité**, sélectionnez **Organisation**.Cliquez sur **Ajouter un nouveau client**.



2. À partir du FMC, accédez à **System > SecureX**.

3. Activez la bascule dans le coin supérieur droit et vérifiez que la région affichée correspond à l'organisation SecureX.

4. Copiez l'**ID client** et le **mot de passe client** et collez-les dans le FMC.

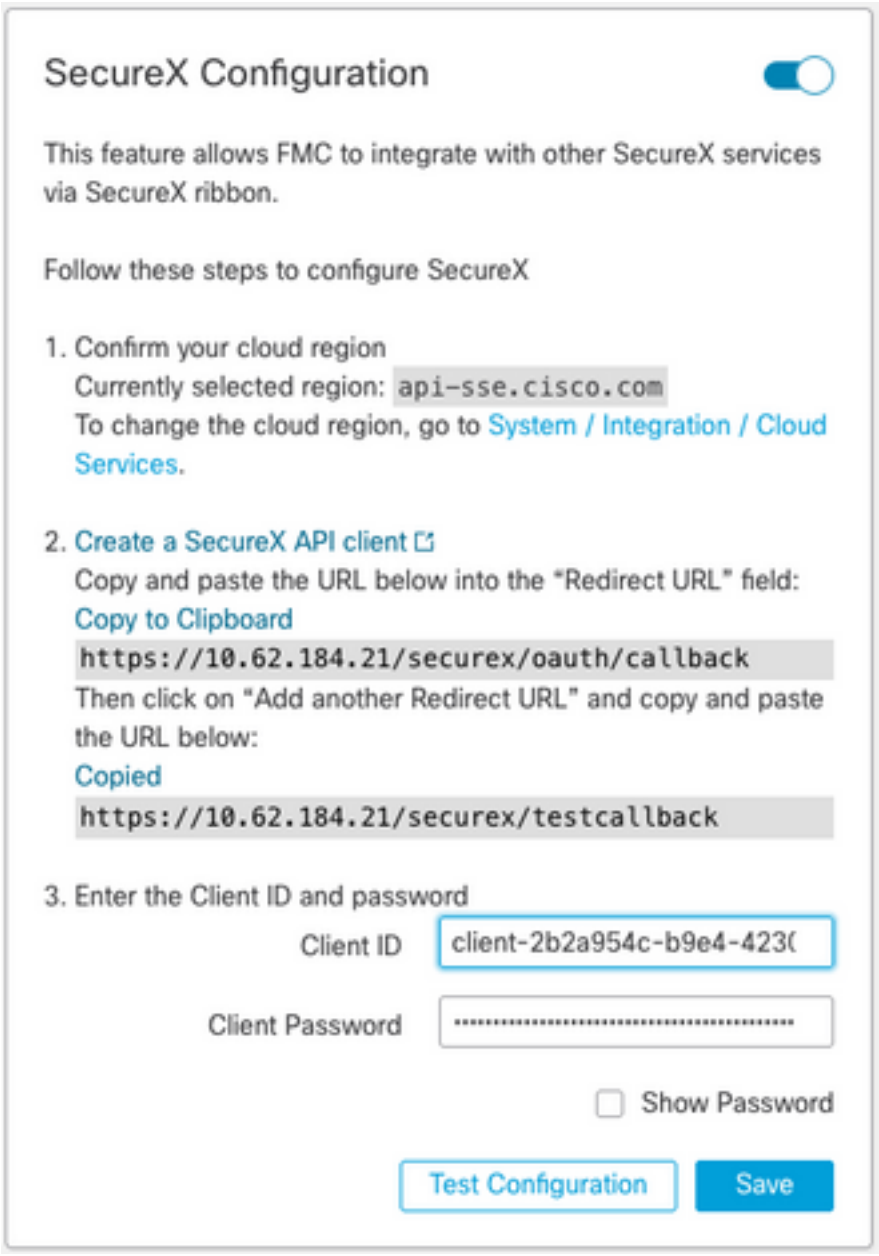
5. Choisissez **test de la configuration**.

6. Connectez-vous à SecureX pour autoriser le client API.

7. Enregistrez les modifications et actualisez le navigateur afin de voir le ruban affiché en bas.

8. Développez le ruban et choisissez **Get SecureX**. Saisissez les informations d'identification SecureX si vous y êtes invité.

9. Le ruban SecureX est maintenant entièrement fonctionnel pour votre utilisateur FMC.

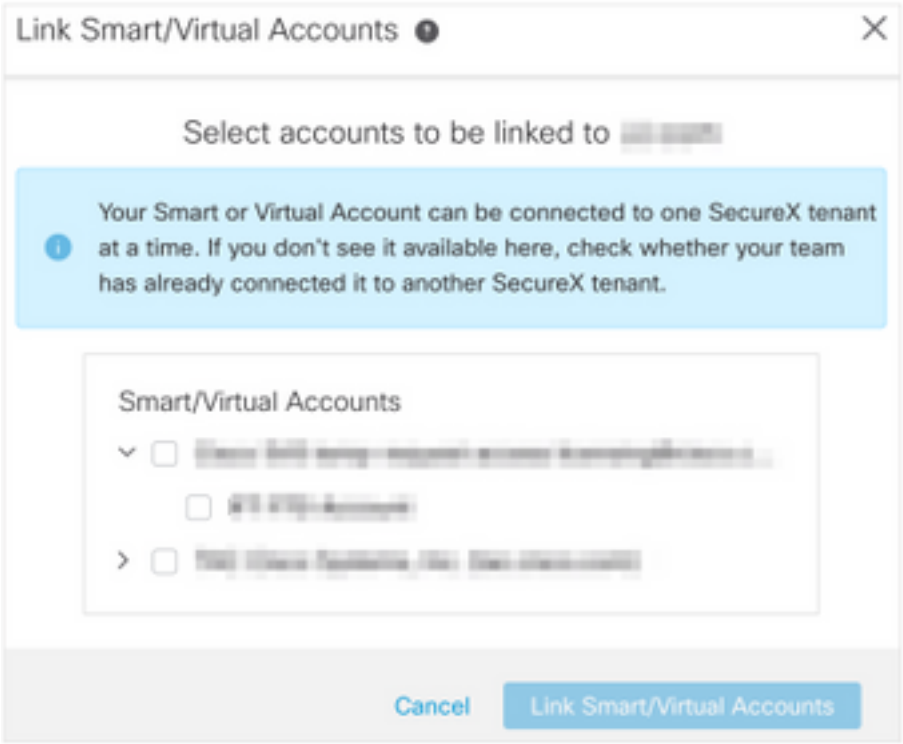


5YVPsGdzrkX8q8q0yYl-tDitezO6p_17MtH6NATx68fUZ5u9T3qOEQ

> **Note**: Si un autre utilisateur FMC a besoin d'accéder au ruban, cet utilisateur doit se connecter au ruban avec des informations d'identification SecureX.

Envoyer les événements de connexion à SecureX

1. Dans le FMC, accédez à **System > Integration > Cloud Services** et assurez-vous que la **configuration des événements cloud de Cisco** envoie des événements d'intrusion, de fichiers et de programmes malveillants comme expliqué dans la section **Activer les services cloud**.
2. Assurez-vous que le FMC est enregistré avec une licence Smart comme expliqué dans la section **Enregistrer les licences Smart**.
3. Prenez note du nom du **compte virtuel affecté** tel qu'il apparaît dans FMC sous **System > Licenses > Smart Licenses**.
4. Enregistrez le FMC dans SecureX : Dans SecureX, accédez à **Administration > Devices**.Sélectionnez **Gérer les périphériques**.Assurez-vous que les fenêtres contextuelles sont autorisées dans le navigateur.Connectez-vous à Security Services Exchange (SSE).Accédez au **menu Outils > Lier des comptes Smart/virtuels**.Choisissez **Lier d'autres comptes**.Sélectionnez le compte virtuel attribué au FMC (étape 3).Choisissez **Lier les comptes Smart/virtuels.**



- Assurez-vous que le périphérique FMC figure dans la liste Périphériques.
- Accédez à l'onglet **Cloud Services**, activez les fonctions **Cisco SecureX de réponse aux menaces** et **Événement**.
- Sélectionnez les **paramètres de service supplémentaires** (icône d'engrenage) en regard de la fonction Évolution.
- Dans l'onglet Général, sélectionnez **Partager les données d'événement avec Talos**.
- Dans l'onglet Evénements de promotion automatique, dans la section Par type d'événement, sélectionnez tous les types d'événements disponibles et **Enregistrer**.

5. Dans le portail principal SecureX, accédez à **Modules d'intégration > Firepower** et ajoutez le module d'intégration Firepower.

6. Créez un tableau de bord.

7. Ajoutez les vignettes liées à Firepower.

Intégrer les terminaux sécurisés (AMP for Endpoints)

Afin d'activer l'intégration de Secure Endpoint (AMP for Endpoints) à votre déploiement Firepower, procédez comme suit :

1. Accédez à **AMP > AMP Management**.
2. Choisissez **Ajouter une connexion cloud AMP**.
3. Sélectionnez le cloud et **Inscrivez-vous**.

Note: L'état **Activé** signifie que la connexion au cloud est établie.

Intégrer Analyse sécurisée des programmes malveillants (Threat Grid)

Par défaut, Firepower Management Center peut se connecter au cloud public Cisco Threat Grid pour l'envoi de fichiers et la récupération de rapports. Il n'est pas possible de supprimer cette connexion. Néanmoins, il est recommandé de choisir le cloud le plus proche de votre déploiement :

1. Accédez à **AMP > Connexions d'analyse dynamique**.
2. Cliquez sur **Modifier** (icône de crayon) dans la section Action.
3. Choisissez le nom de cloud approprié.
4. Pour associer le compte Threat Grid aux fonctionnalités avancées de création de rapports et de sandbox, cliquez sur l'icône **Associer**.

Pour plus d'informations, reportez-vous au Guide de configuration de Firepower Management Center, Version 7.0 - Activation de l'accès aux résultats de l'analyse dynamique dans le cloud public.

Pour obtenir des informations sur l'intégration de l'appliance Thread Grid sur site, reportez-vous au Guide de configuration de Firepower Management Center, Version 7.0 - Dynamic Analysis On Premises Appliance (Cisco Threat Grid) .