Étapes de configuration initiale des systèmes FireSIGHT

Contenu

[Introduction](#)
[Prérequis](#)
[Configuration](#)
[Étape 1 : Configuration initiale](#)
[Étape 2 : Installer les licences](#)
[Étape 3 : Appliquer la stratégie système](#)
[Étape 4 : Appliquer la stratégie de santé](#)
[Étape 5 : Enregistrer les périphériques gérés](#)
[Étape 6 : Activer les licences installées](#)
[Étape 7 : Configuration des interfaces de détection](#)
[Étape 8 : Configurer la stratégie d'intrusion](#)
[Étape 9 : Configurer et appliquer une stratégie de contrôle d'accès](#)
[Étape 10 : Vérifier si FireSIGHT Management Center reçoit des événements](#)
[Recommandation supplémentaire](#)

Introduction

Après avoir réinstallé FireSIGHT Management Center ou un périphérique FirePOWER, vous devez effectuer plusieurs étapes pour rendre le système entièrement fonctionnel et générer des alertes pour les événements d'intrusion ; par exemple, installation de la licence, enregistrement des appliances, application de la stratégie d'intégrité, de la stratégie système, de la stratégie de contrôle d'accès, de la stratégie d'intrusion, etc. Ce document est un supplément au Guide d'installation du système FireSIGHT.

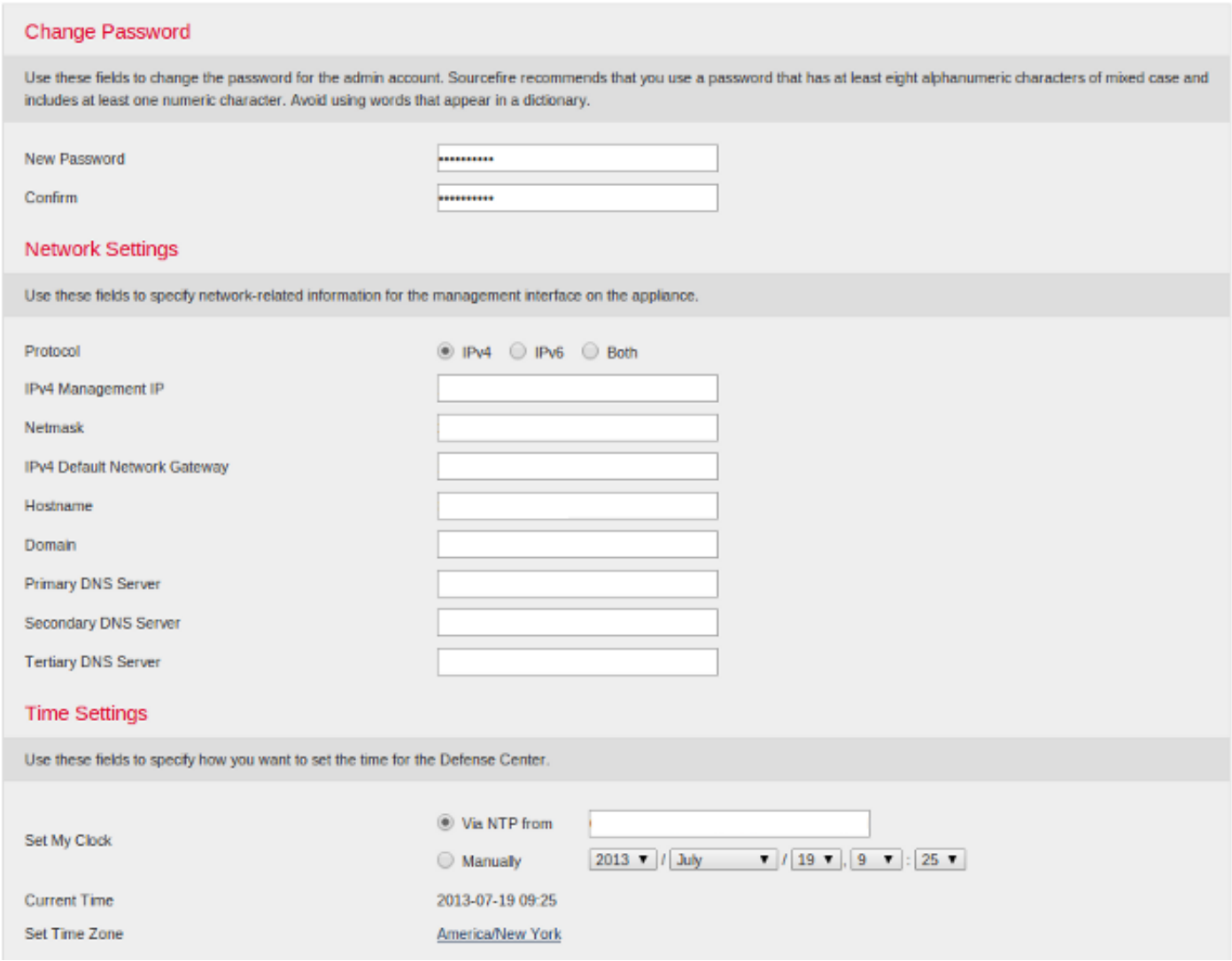
Prérequis

Ce guide suppose que vous avez lu attentivement le Guide d'installation du système FireSIGHT.

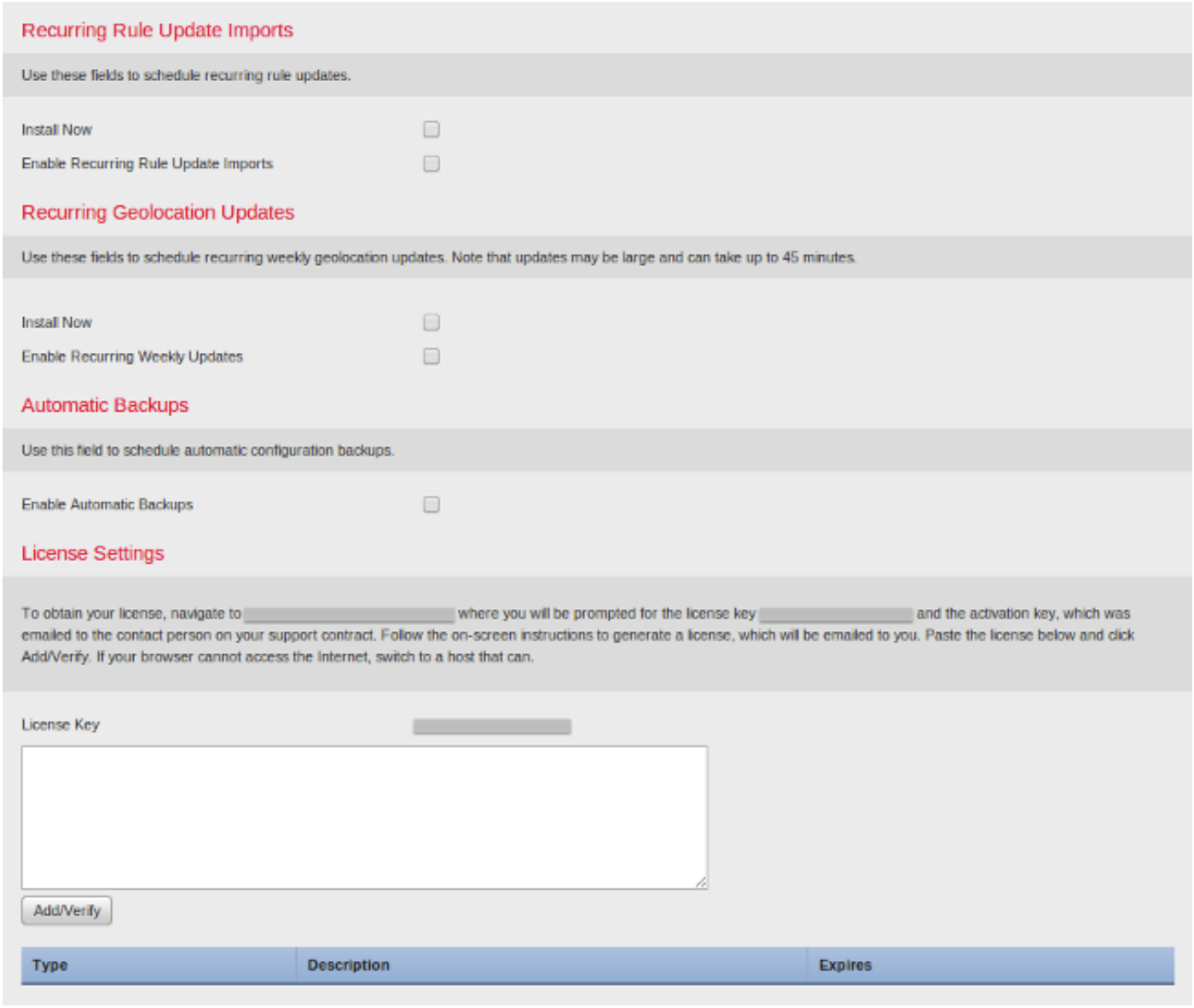
Configuration

Étape 1 : Configuration initiale

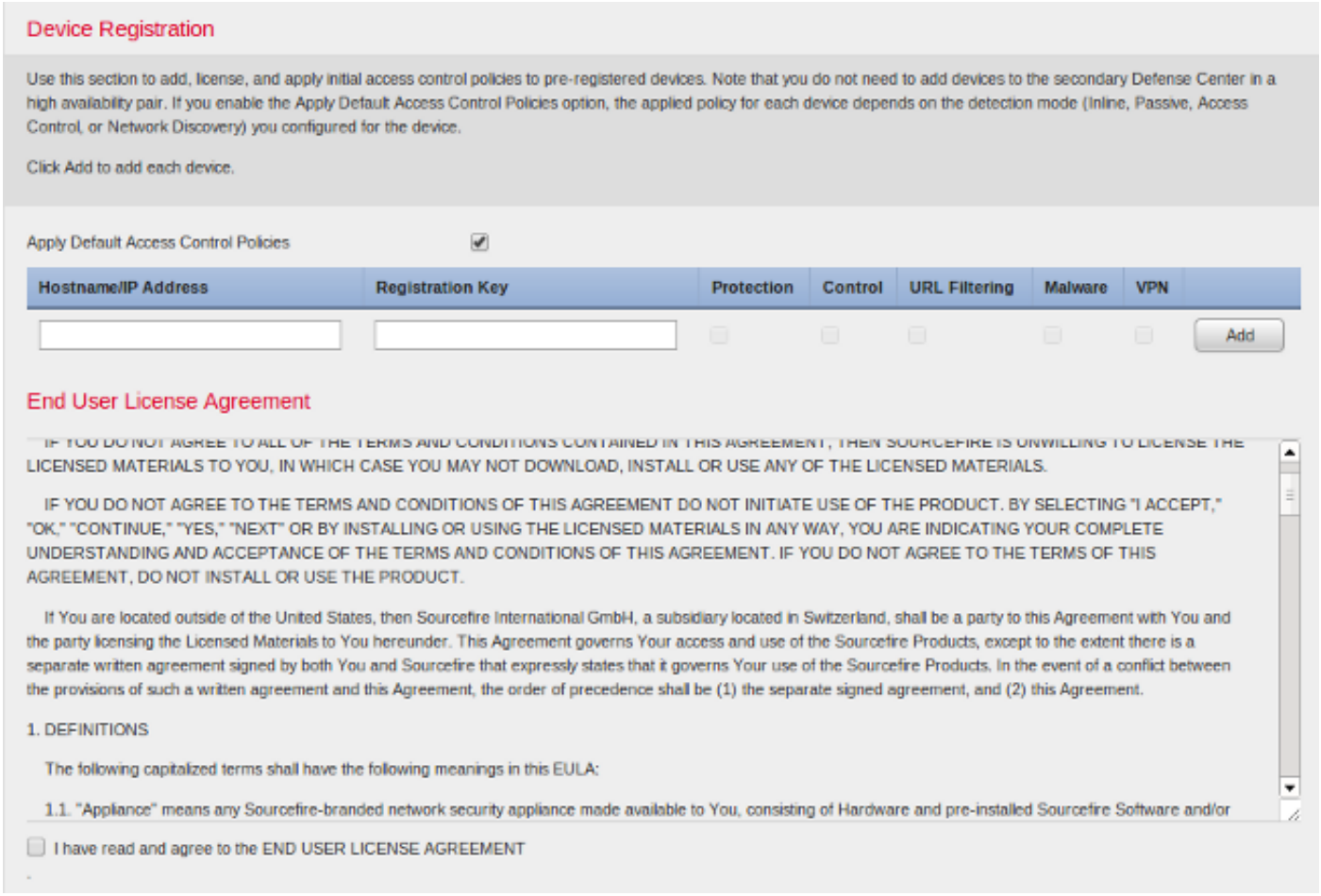
Sur FireSIGHT Management Center, vous devez terminer le processus de configuration en vous connectant à l'interface Web et en spécifiant les options de configuration initiale sur la page de configuration, représentée ci-dessous. Sur cette page, vous devez modifier le mot de passe admin et pouvez également spécifier les paramètres réseau tels que les serveurs DNS et de domaine, ainsi que la configuration de l'heure.



Vous pouvez éventuellement configurer des mises à jour récurrentes des règles et de la géolocalisation ainsi que des sauvegardes automatiques. Toutes les licences de fonction peuvent également être installées à ce stade.



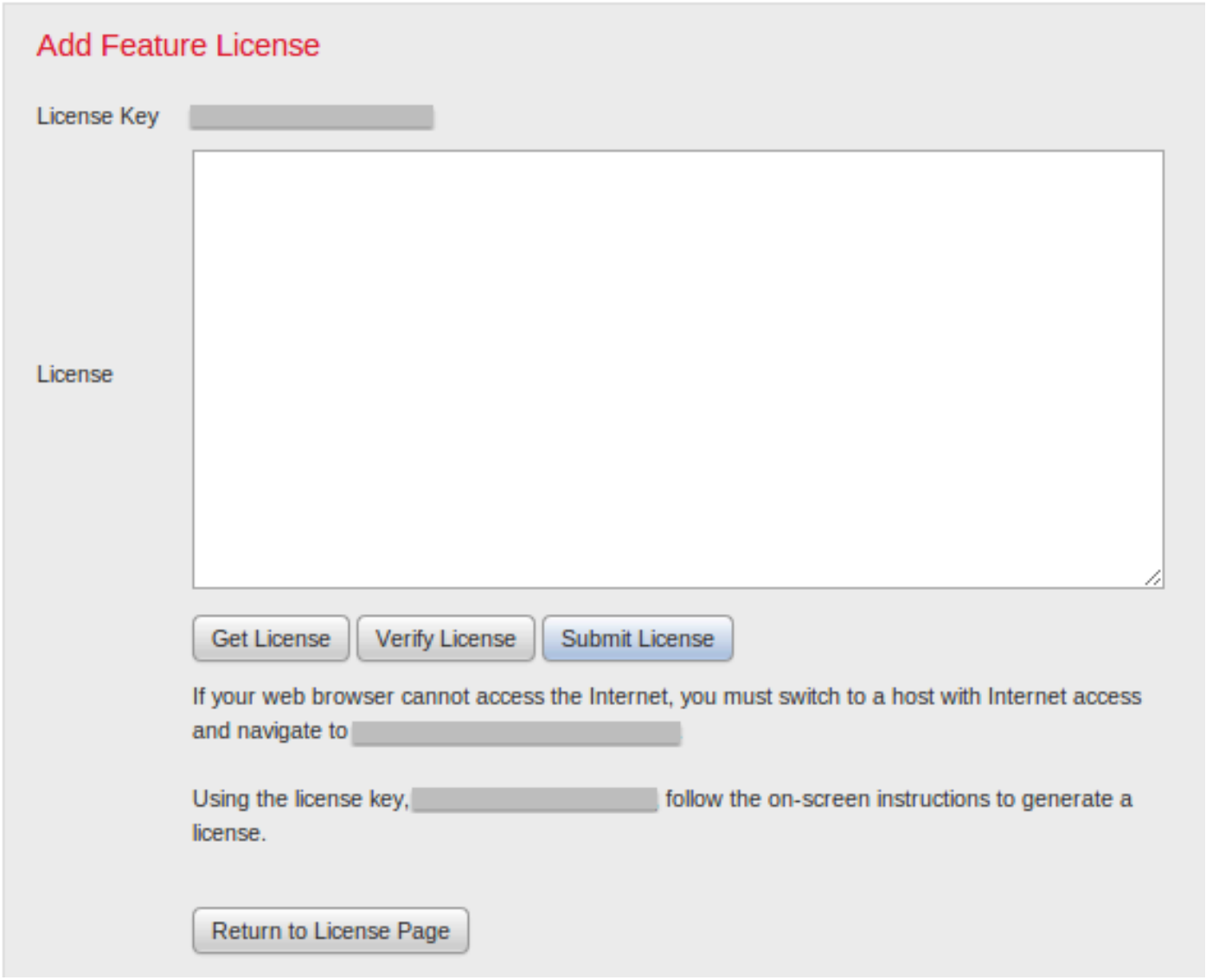
Sur cette page, vous pouvez également enregistrer un périphérique dans FireSIGHT Management Center et spécifier un mode de détection. Le mode de détection et les autres options que vous choisissez lors de l'enregistrement déterminent les interfaces par défaut, les jeux en ligne et les zones que le système crée, ainsi que les stratégies qu'il applique initialement aux périphériques gérés.



Étape 2 : Installer les licences

Si vous n'avez pas installé de licences pendant la page de configuration initiale, vous pouvez effectuer la tâche en procédant comme suit :

- Accédez à la page suivante : **Système > Licences**.
- Cliquez sur **Ajouter une nouvelle licence**.



Si vous n'avez pas reçu de licence, contactez le représentant commercial de votre compte.

Étape 3 : Appliquer la stratégie système

La stratégie système spécifie la configuration des profils d'authentification et de la synchronisation temporelle entre FireSIGHT Management Center et les périphériques gérés. Pour configurer ou appliquer la stratégie système, accédez à **System > Local > System Policy**. Une stratégie système par défaut est fournie mais doit être appliquée à tous les périphériques gérés.

Étape 4 : Appliquer la stratégie de santé

La stratégie Health permet de configurer la manière dont les périphériques gérés signalent leur état de santé à FireSIGHT Management Center. Pour configurer ou appliquer la stratégie d'intégrité, accédez à **Health > Health Policy**. Une stratégie d'intégrité par défaut est fournie mais doit être appliquée à tous les périphériques gérés.

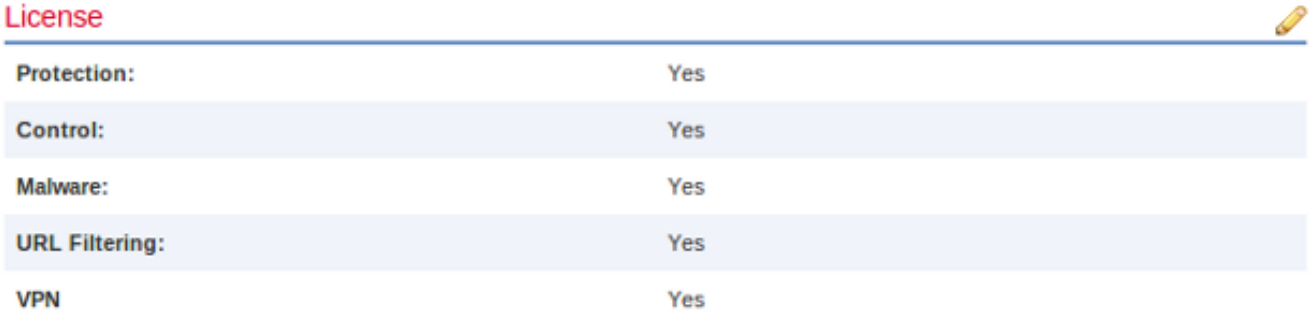
Étape 5 : Enregistrer les périphériques gérés

Si vous n'avez pas enregistré de périphériques au cours de la page de configuration initiale, lisez ce document pour obtenir des instructions sur l'enregistrement d'un périphérique dans FireSIGHT Management Center.

Étape 6 : Activer les licences installées

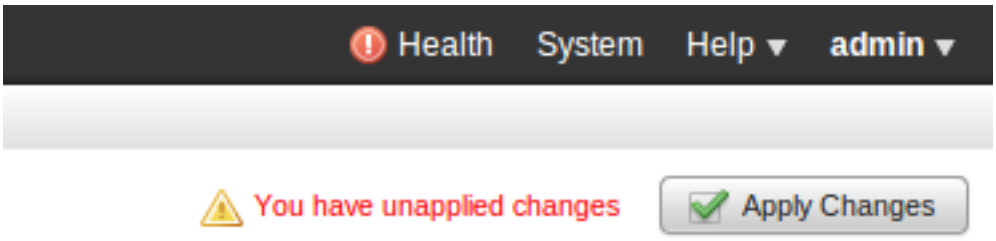
Avant de pouvoir utiliser une licence de fonction sur votre appareil, vous devez l'activer pour chaque appareil géré.

1. Accédez à la page suivante : **Périphériques > Gestion des périphériques**.
2. Cliquez sur le périphérique pour lequel vous souhaitez activer les licences et saisissez l'onglet Périphérique.
3. Cliquez sur l'icône **Modifier** (*crayon*) en regard de Licence.



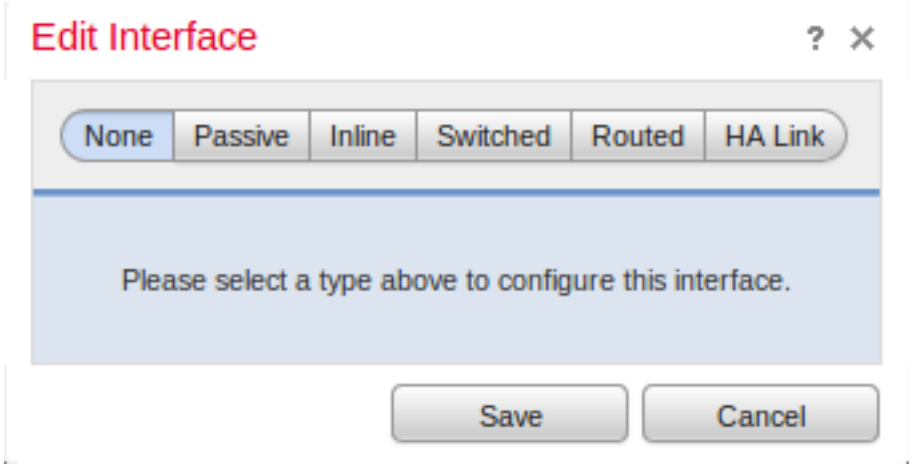
Activez les licences requises pour ce périphérique et cliquez sur **Enregistrer**.

Notez le message "*Vous avez des modifications non appliquées*" dans le coin supérieur droit. Cet avertissement reste actif même si vous quittez la page de gestion des périphériques jusqu'à ce que vous cliquiez sur le bouton **Appliquer les modifications**.



Étape 7 : Configuration des interfaces de détection

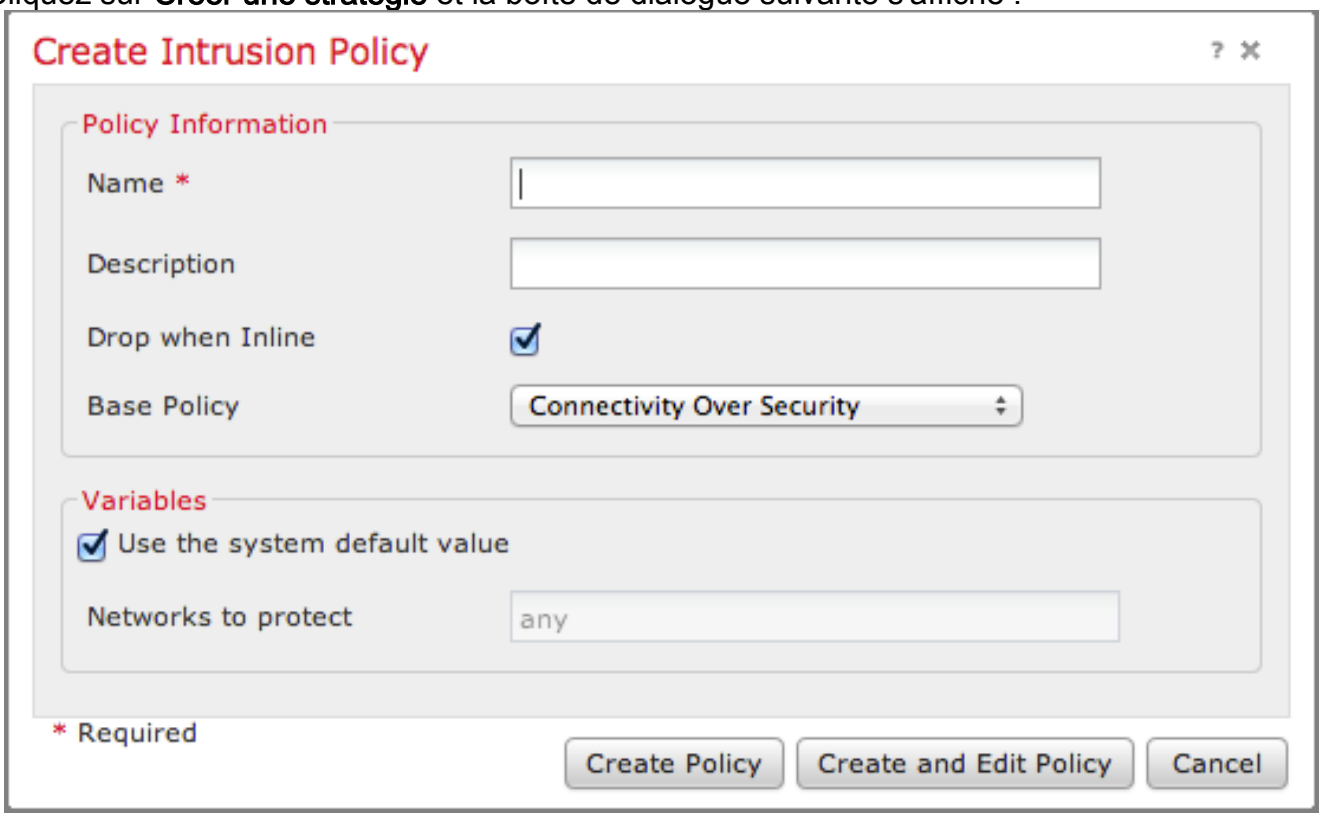
1. Accédez à la page **Périphériques > Gestion des périphériques** suivante.
2. Cliquez sur l'icône **Edit** (crayon) du capteur de votre choix.
3. Sous l'onglet **Interfaces**, cliquez sur l'icône **Modifier** de l'interface de votre choix.



Sélectionnez une configuration d'interface passive ou en ligne. Les interfaces commutées et routées sortent du cadre de cet article.

Étape 8 : Configurer la stratégie d'intrusion

- Accédez à la page suivante : **Politiques > Intrusion > Intrusion Policy.**
- Cliquez sur **Créer une stratégie** et la boîte de dialogue suivante s'affiche :



Vous devez attribuer un nom et définir la stratégie de base à utiliser. En fonction de votre déploiement, vous pouvez choisir d'utiliser l'option **Supprimer lorsque Inline** est activée. Définissez les réseaux à protéger pour réduire les faux positifs et améliorer les performances du système.

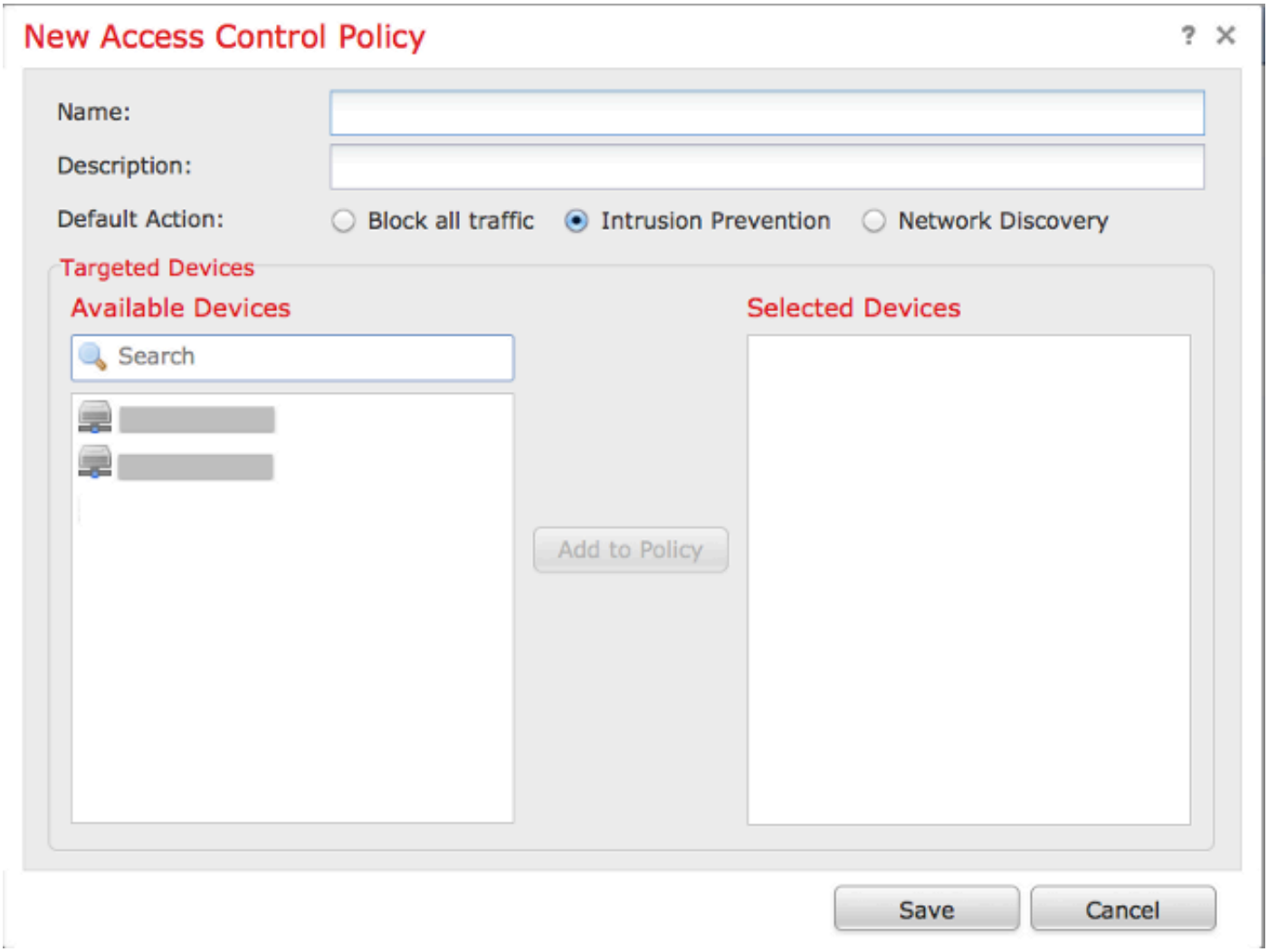
Cliquez sur **Créer une stratégie** pour enregistrer vos paramètres et créer la stratégie IPS. Si vous souhaitez modifier la stratégie d'intrusion, vous pouvez choisir **Créer et modifier la stratégie** à la place.

Note: Les stratégies d'intrusion sont appliquées dans le cadre de la stratégie de contrôle d'accès. Après l'application d'une stratégie d'intrusion, toutes les modifications peuvent être appliquées sans appliquer à nouveau l'ensemble de la stratégie de contrôle d'accès en cliquant sur le bouton **Réappliquer**.

Étape 9 : Configurer et appliquer une stratégie de contrôle d'accès

1. Accédez à **Politiques > Contrôle d'accès**.

2. Cliquez sur **Nouvelle politique**.

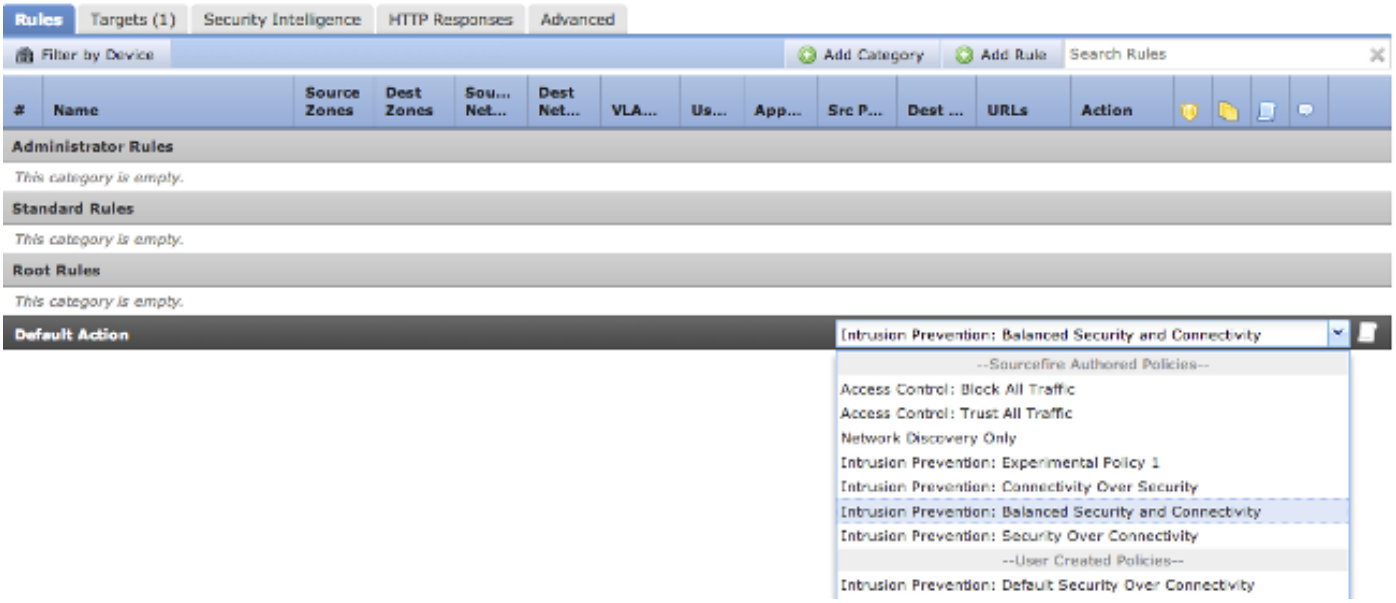


3. Indiquez un **nom** pour la stratégie et une **description**.

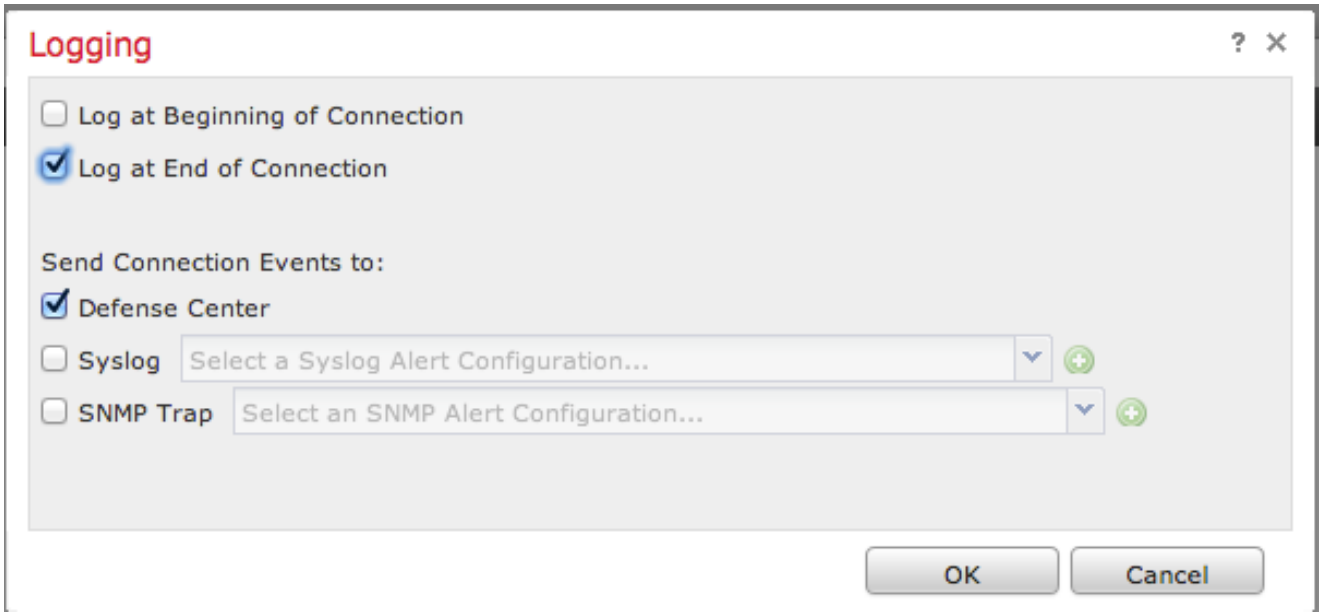
4. Sélectionnez **Intrusion Prevention** comme **Action par défaut** de la stratégie de contrôle d'accès.

5. Enfin, sélectionnez les **périphériques ciblés** auxquels vous voulez appliquer la stratégie de contrôle d'accès, puis cliquez sur **Enregistrer**.

6. Sélectionnez votre stratégie d'intrusion pour l'action par défaut.



7. La journalisation des connexions doit être activée pour générer des événements de connexion. Cliquez sur le menu déroulant situé à droite de l'**action par défaut**.



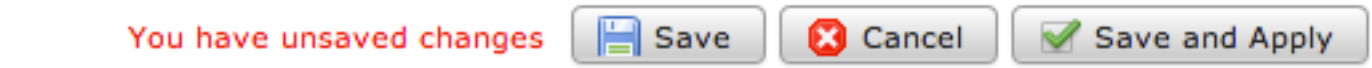
8. Choisissez de consigner les connexions au début ou à la fin de la connexion. Les événements peuvent être connectés à FireSIGHT Management Center, à un emplacement Syslog ou via SNMP.

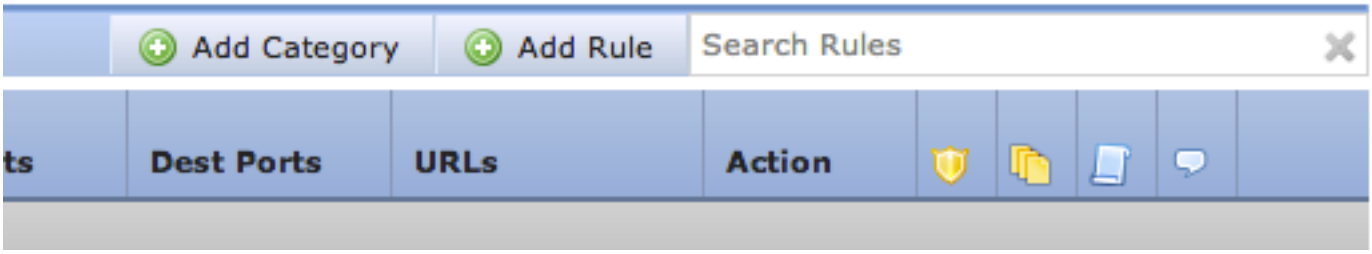
> **Note**: Il n'est pas recommandé de se connecter aux deux extrémités de la connexion, car chaque connexion (à l'exception des connexions bloquées) sera consignée deux fois. La journalisation au début est utile pour les connexions qui seront bloquées et la journalisation à la fin est utile pour toutes les autres connexions.

9. Click OK. Notez que la couleur de l'icône de journalisation a changé.

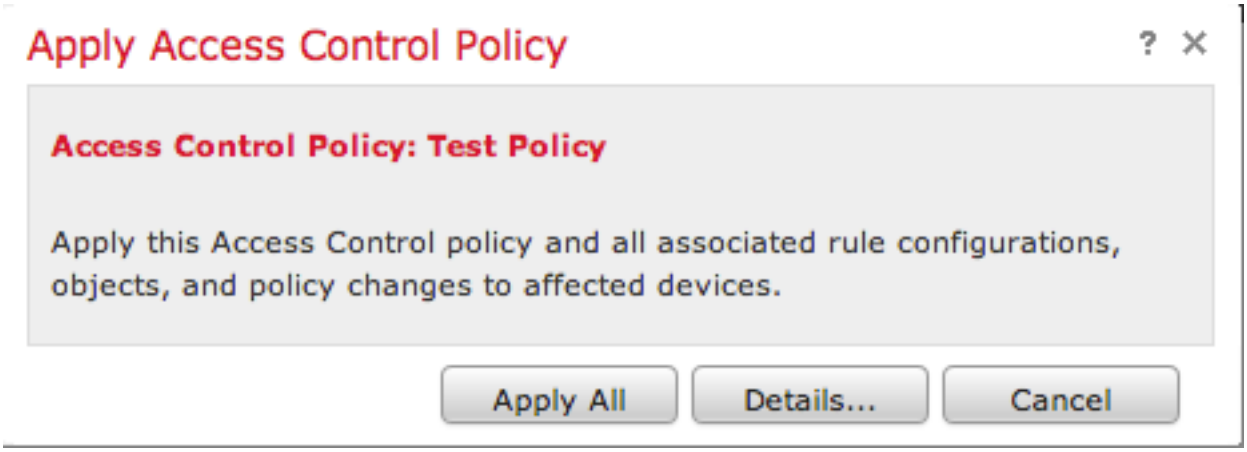
10. Vous pouvez ajouter une **règle de contrôle d'accès** à ce stade. Les options que vous pouvez utiliser dépendent du type de licence que vous avez installé.

11. Lorsque vous avez terminé d'apporter des modifications. cliquez sur le bouton **Enregistrer et appliquer**. Vous remarquerez qu'un message indique que des modifications non enregistrées sont apportées à votre stratégie dans le coin supérieur droit jusqu'à ce que vous cliquiez sur le bouton.





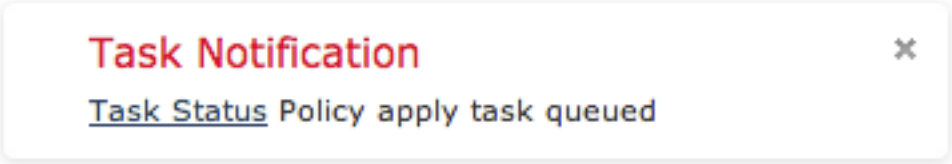
Vous pouvez choisir d'**enregistrer** uniquement les modifications ou de cliquer sur **Enregistrer et appliquer**. La fenêtre suivante s'affiche si vous choisissez cette dernière option.



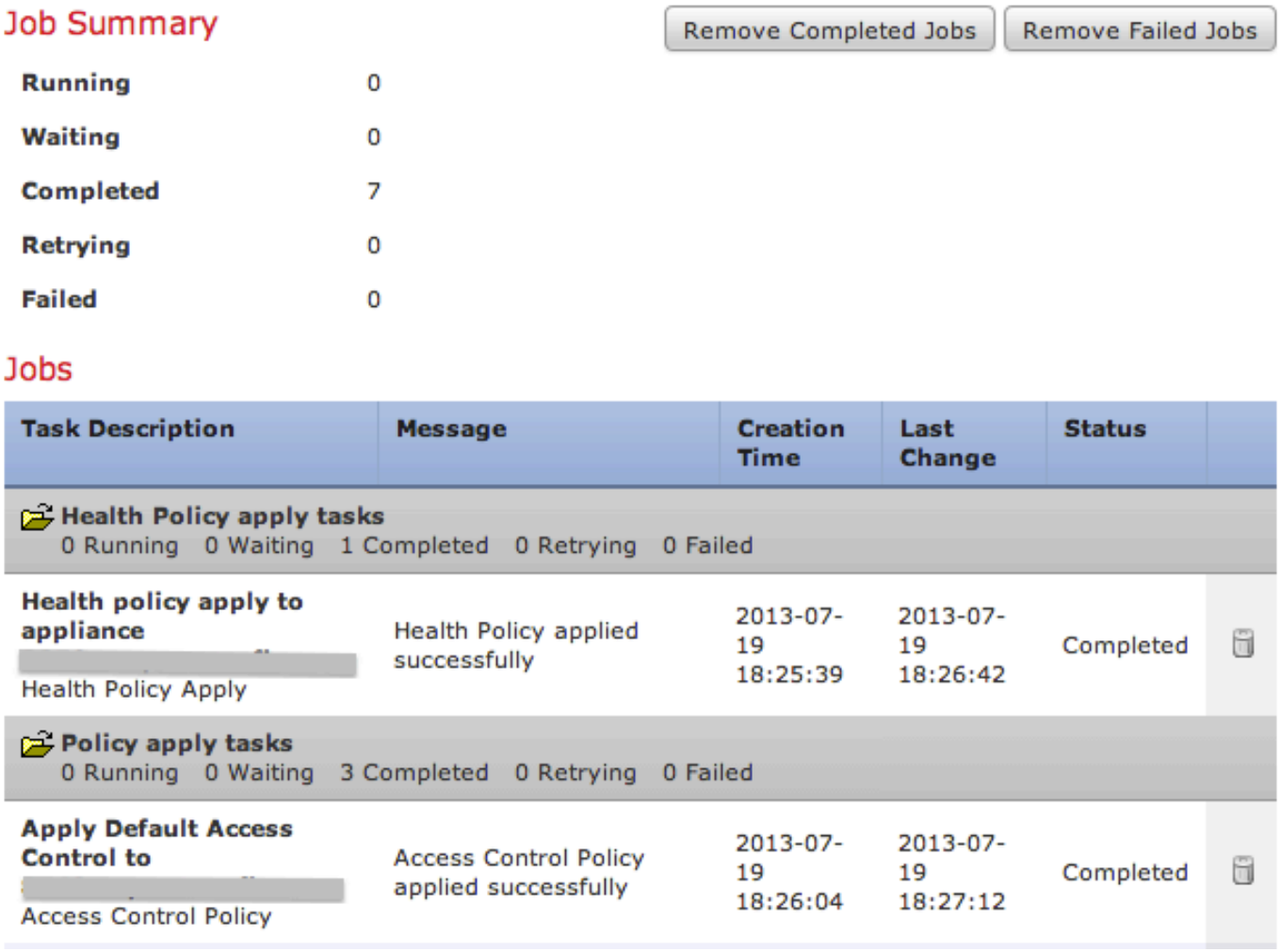
12. **Appliquer tout** appliquera la stratégie de contrôle d'accès et les stratégies d'intrusion associées aux périphériques cibles.

> **Note**: Si une stratégie d'intrusion est appliquée pour la première fois, elle ne peut pas être désactivée.

13. Vous pouvez surveiller l'état de la tâche en cliquant sur le lien **Statut de la tâche** dans la notification affichée en haut de la page, ou en naviguant vers : **Système > Surveillance > État de la tâche**



14. Cliquez sur le lien État de la tâche pour surveiller l'avancement de la stratégie de contrôle d'accès.



Étape 10 : Vérifier si FireSIGHT Management Center reçoit des événements

Une fois la stratégie de contrôle d'accès appliquée terminée, vous devez commencer à voir les événements de connexion et en fonction des événements d'intrusion de trafic.

Recommandation supplémentaire

Vous pouvez également configurer les fonctions supplémentaires suivantes sur votre système. Reportez-vous au Guide de l'utilisateur pour plus de détails sur la mise en oeuvre.

- Sauvegardes planifiées
- Téléchargements/installations de mise à jour automatique des logiciels, SRU, VDB et GeoLocation.
- Authentification externe via LDAP ou RADIUS

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.