Étapes de configuration initiale des systèmes de FireSIGHT

Contenu

Introduction

Après que vous réimagiez un centre de Gestion de FireSIGHT ou un périphérique de puissance de feu, vous devez se terminer plusieurs étapes pour faire le système entièrement - fonctionnel et pour générer des alertes pour des événements d'intrusion ; comme, installant le permis, enregistrant les appliances, appliquant la politique sanitaire, la stratégie de système, la stratégie de contrôle d'accès, la stratégie etc. d'intrusion. Ce document est un supplément au guide d'installation de système de FireSIGHT.

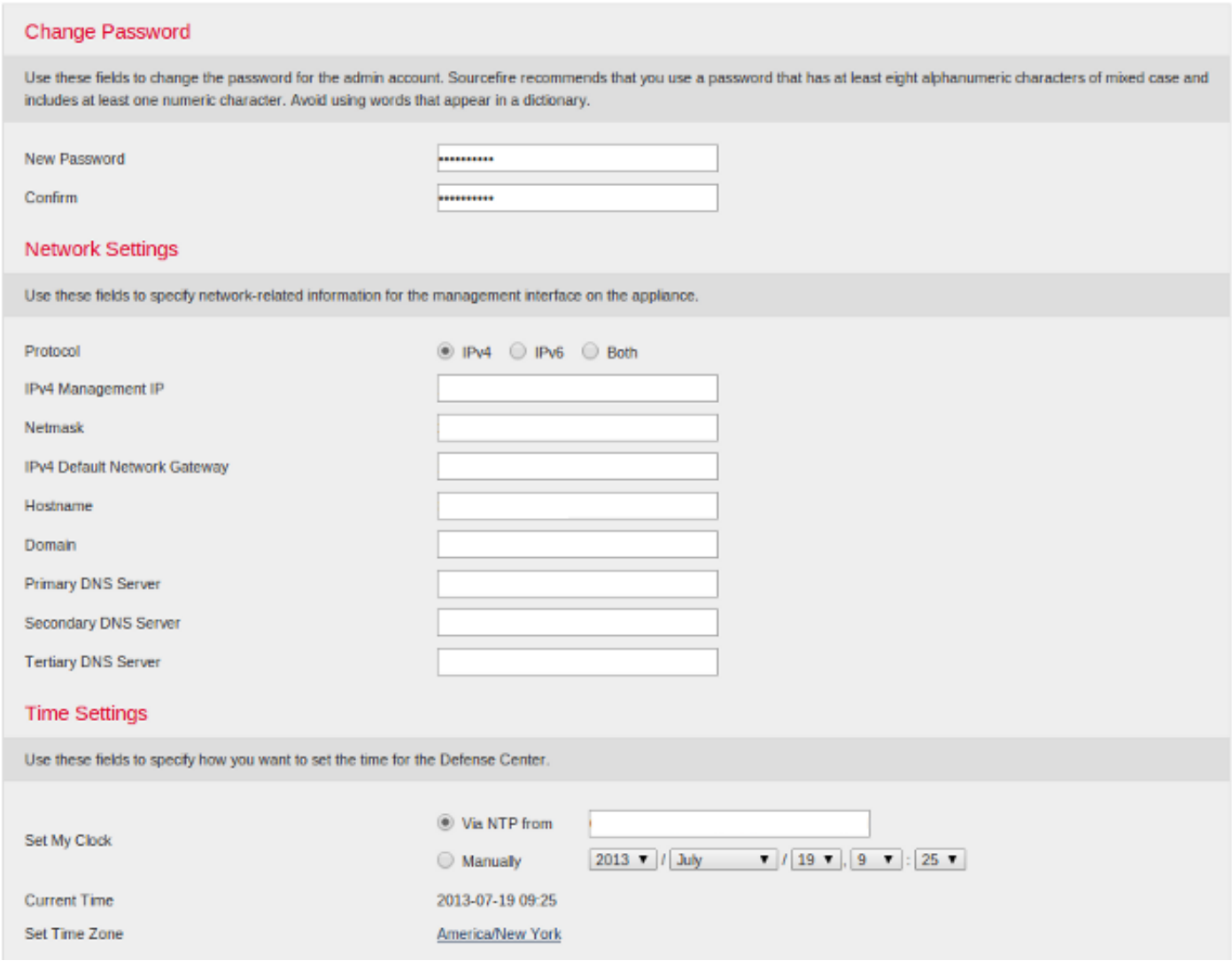
Condition préalable

Ce guide suppose que vous avez soigneusement lu le guide d'installation de système de FireSIGHT.

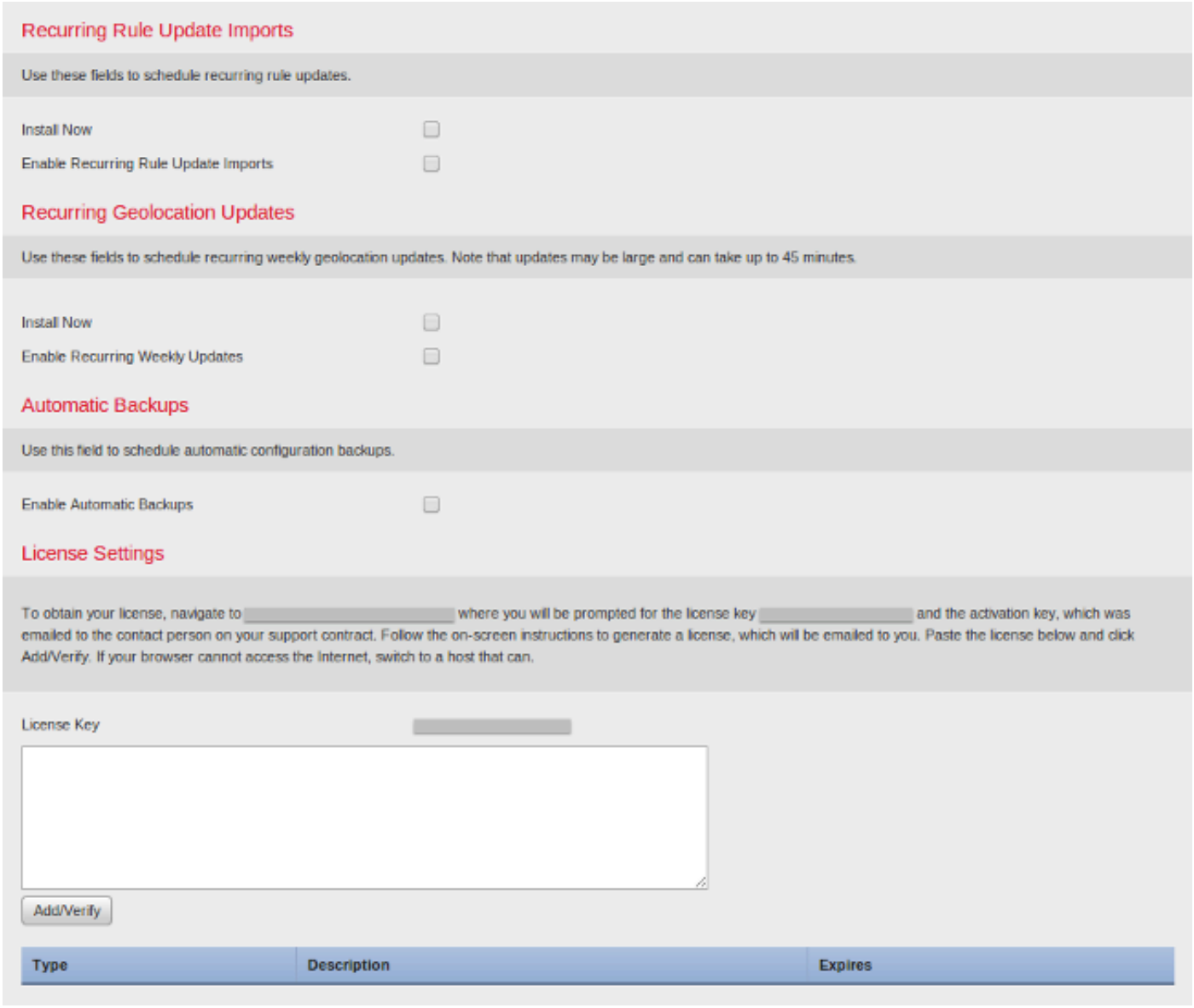
Configuration

Étape 1 : Première installation

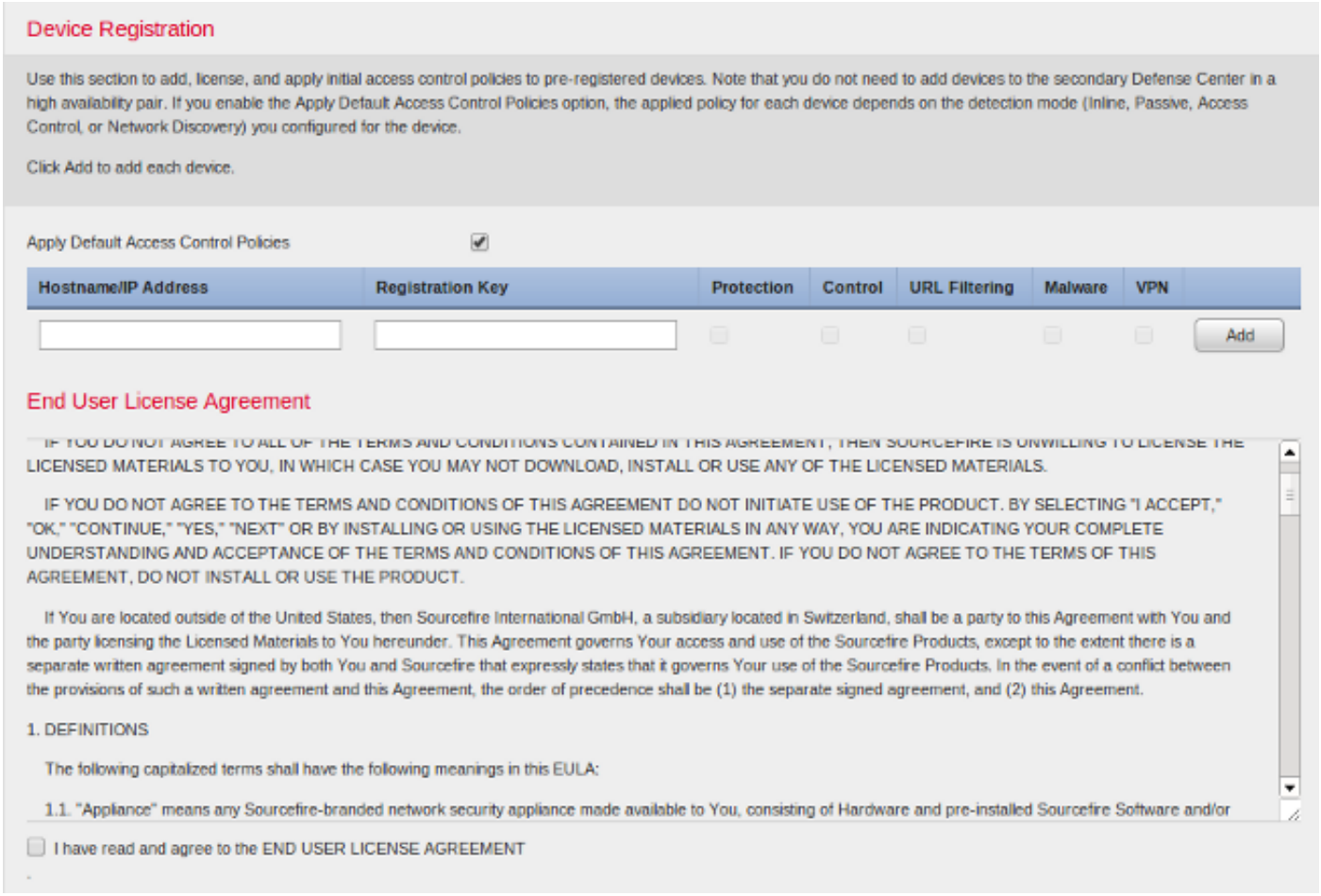
Àvotre centre de Gestion de FireSIGHT, vous devez compléter la procédure d'installation en se connectant dans l'interface web et en spécifiant des options de configuration initiale sur l'installation paginez, représenté ci-dessous. À cette page, vous devez changer le mot de passe administrateur, et pouvez également spécifier des paramètres réseau tels que le domaine et les serveurs DNS, et la configuration de temps.



Vous pouvez sur option configurer les mises à jour récurrentes de règle et de geolocation aussi bien que les sauvegardes automatiques. Tous les permis de caractéristique peuvent également être installés en ce moment.



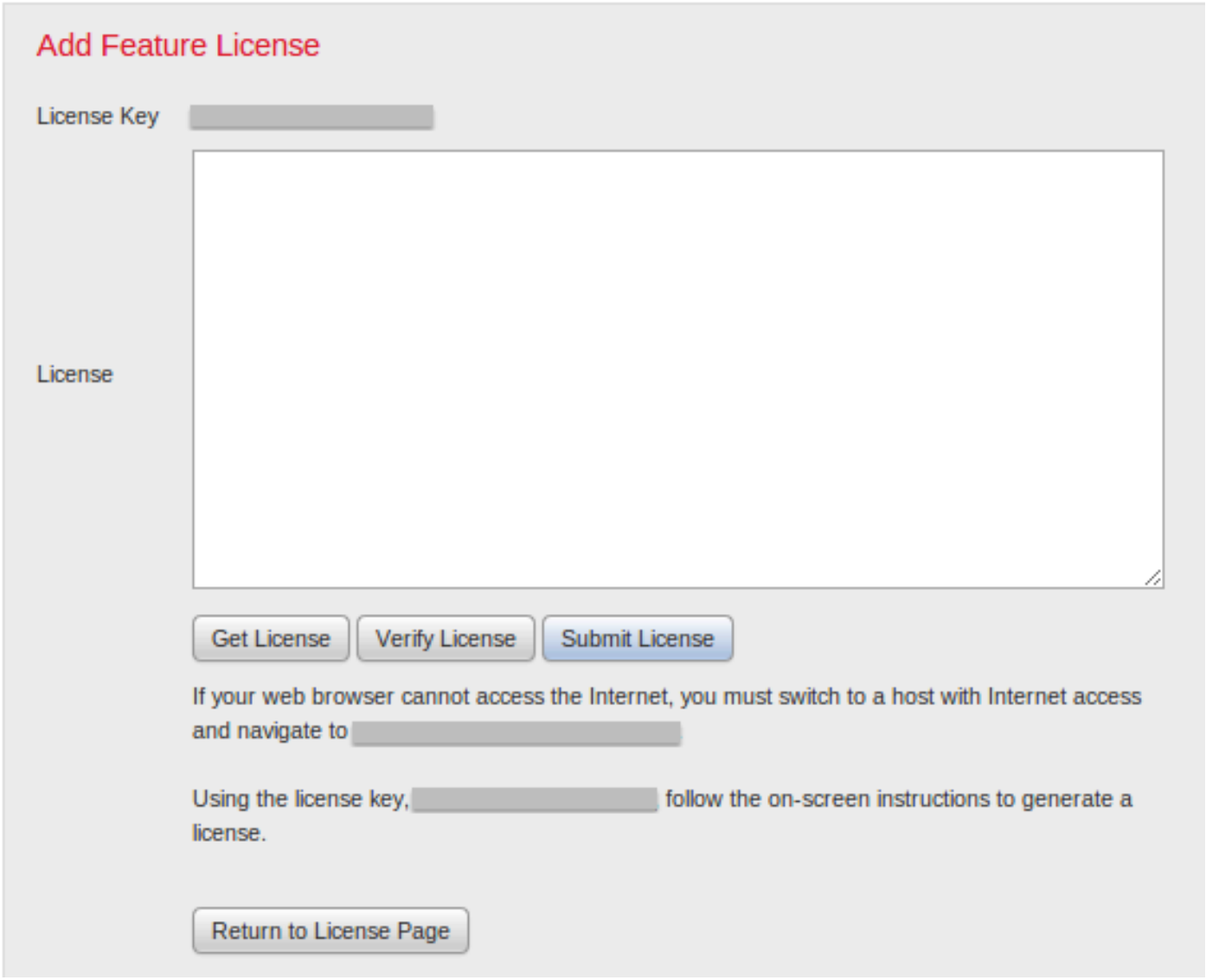
Àcette page, vous pouvez également enregistrer un périphérique au centre de Gestion de FireSIGHT et spécifier un mode de détection. Le mode de détection et d'autres options que vous choisissez pendant l'enregistrement déterminent les interfaces par défaut, les positionnements intégrés, et les zones que le système crée, aussi bien que les stratégies qu'elles appliquent au commencement aux périphériques gérés.



Étape 2 : Installs licenses

Si vous ne faisiez pas des installs licenses pendant la page de première installation, vous pouvez se terminer la tâche en suivant ces étapes :

- Naviguez vers la page suivante : **Système > permis**.
- Cliquez sur **ajoutent** en fonction le **nouveau permis**.



Si vous ne receviez pas un permis, entrez en contact avec le représentant de commerce de votre compte.

Étape 3 : Appliquez la stratégie de système

La stratégie de système spécifie la configuration pour des profils d'authentification et la synchronisation horaire entre le centre de Gestion de FireSIGHT et les périphériques gérés. Pour configurer ou appliquer la stratégie de système naviguez vers le **système > la stratégie de gens du pays > de système**. Une stratégie par défaut de système est fournie mais doit être appliquée à tous les périphériques gérés.

Étape 4 : Appliquez la politique sanitaire

La politique sanitaire est utilisée pour configurer comment les périphériques gérés signalent leur état de santés au centre de Gestion de FireSIGHT. Pour configurer ou appliquer la politique sanitaire naviguez vers des **santés > la politique sanitaire**. Une politique sanitaire par défaut est fournie mais doit être appliquée à tous les périphériques gérés.

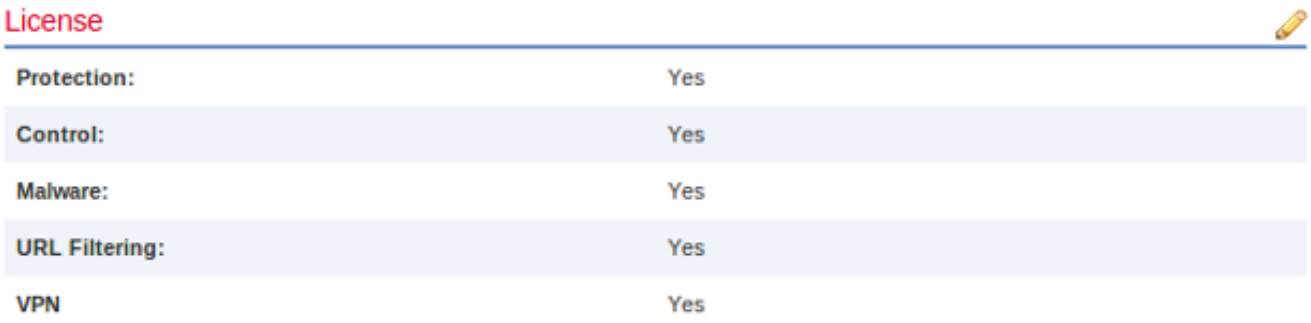
Étape 5 : Périphériques gérés de registre

Si vous ne vous enregistriez pas les périphériques pendant la première installation paginent, indiquent ce document pour des instructions sur la façon dont enregistrer un périphérique à un centre de Gestion de FireSIGHT.

Étape 6 : Permis installés par enable

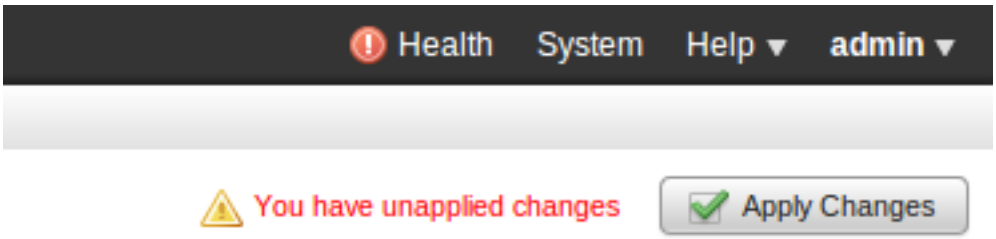
Avant que vous puissiez utiliser n'importe quel permis de caractéristique sur votre appliance, vous devez l'activer pour chaque périphérique géré.

1. Naviguez vers la page suivante : **Périphériques > Gestion de périphériques**.
2. Cliquez sur en fonction le périphérique pour lequel vous voulez activer les permis et écrivez l'onglet de périphérique.
3. Cliquez sur l'**éditer** (icône de *crayon*) à côté du permis.



Activez les permis requis pour ce périphérique et cliquez sur la **sauvegarde**.

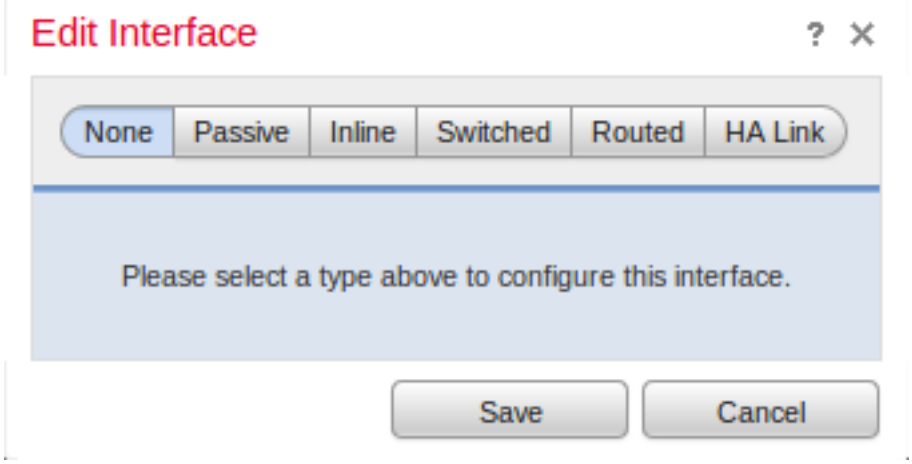
Notez le message « *vous pour avoir les modifications inappliquées* » sur le coin haut droit. Cet avertissement demeure actif même si vous naviguez à partir de la page de Gestion de périphériques jusqu'à ce que vous cliquiez sur le bouton de **modifications d'application**.



Étape 7 : Configurez sentir des interfaces

1. Naviguez vers les **périphériques > la Gestion de périphériques** suivants de page.

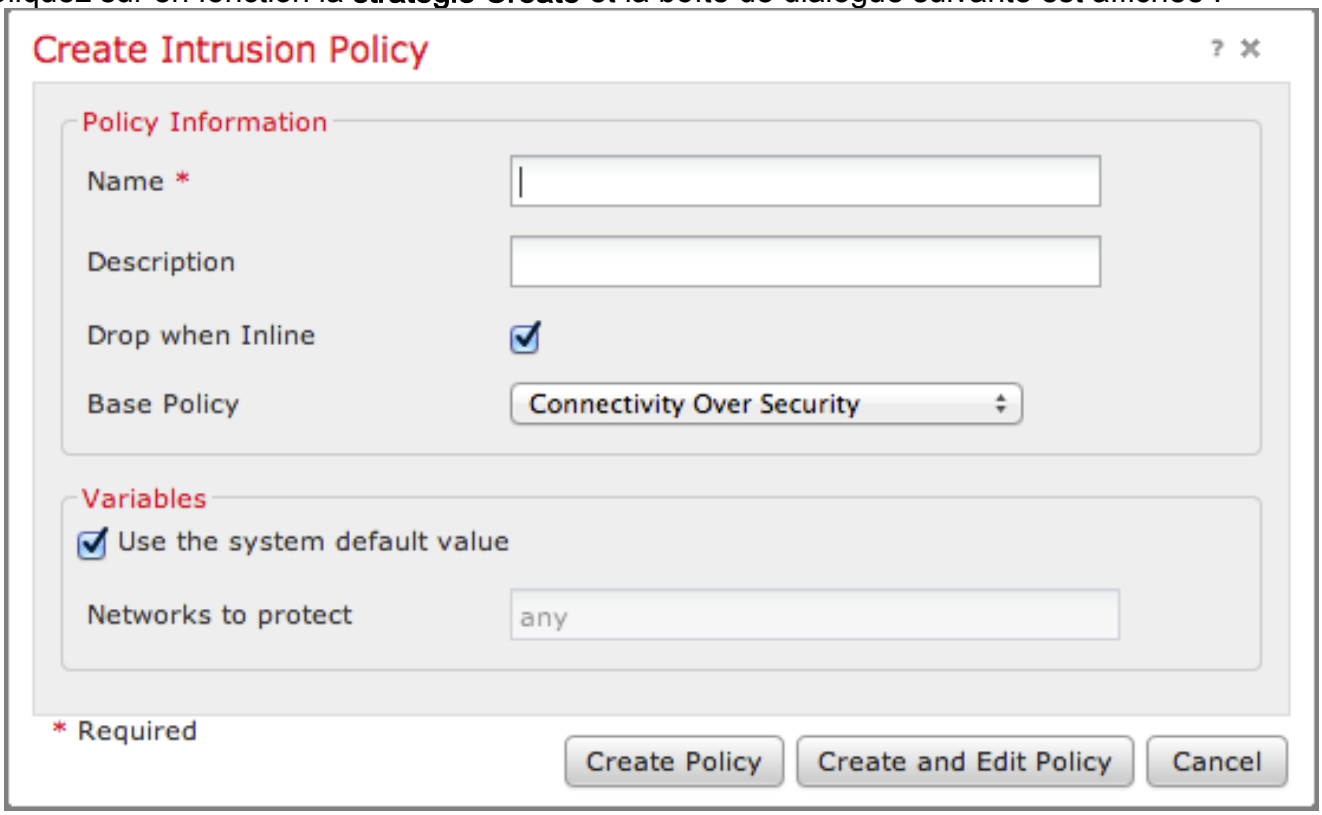
2. Cliquez sur l'icône d'**éditer** (crayon) pour le capteur de votre choix.
3. Sous les **interfaces** tabulez, cliquez sur l'icône d'**éditer** pour l'interface de votre choix.



Sélectionnez une configuration d'interface passive ou intégrée. Les interfaces commutées et conduites sont hors de portée de cet article.

Étape 8 : Configurez la stratégie d'intrusion

- Naviguez vers la page suivante : **Stratégies > intrusion > stratégie d'intrusion.**
- Cliquez sur en fonction la **stratégie Create** et la boîte de dialogue suivante est affichée :



Vous devez assigner un nom et définir la stratégie de base à utiliser. Selon votre déploiement que vous pouvez a choisi d'avoir la **baisse d'**option **quand l'en ligne** a activé. Définissez les réseaux que vous voulez se protéger pour réduire des faux positifs et pour améliorer les performances du système.

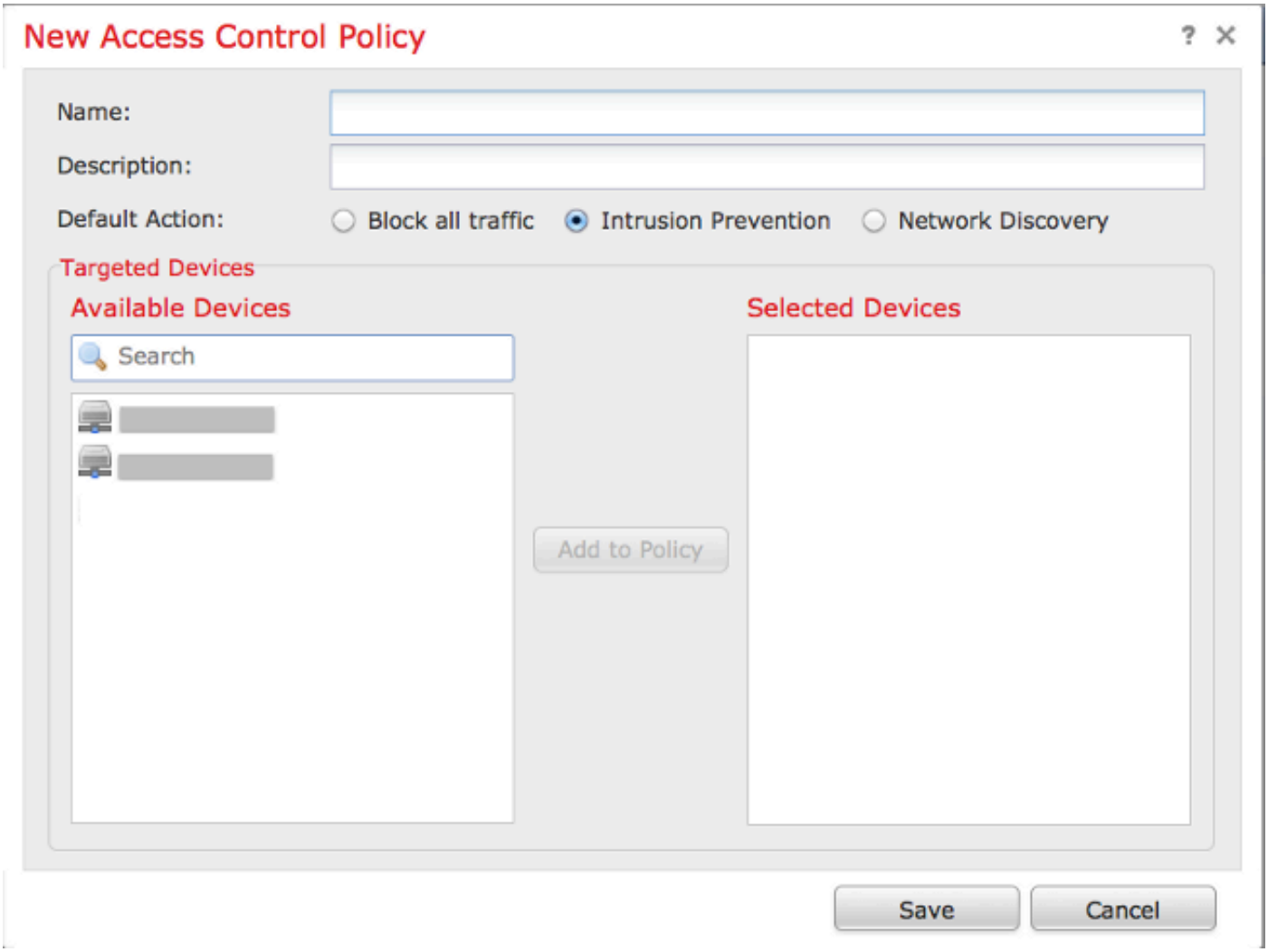
Cliquer sur sur la **stratégie Create** sauvegardera vos configurations et créera la stratégie IPS. Si vous voulez apporter n'importe quelle modification à la stratégie d'intrusion, vous pouvez choisir **créez et éditez la stratégie** à la place.

> Remarque: Les stratégies d'intrusion sont appliquées en tant qu'élément de la stratégie de contrôle d'accès. Après qu'une stratégie d'intrusion soit appliquée, toutes les modifications peuvent être appliquées sans réappliquer la stratégie entière de contrôle d'accès en cliquant sur le bouton de **réapplication**.

Étape 9 : Configurez et appliquez une stratégie de contrôle d'accès

1. Naviguez vers les **stratégies > le contrôle d'accès**.

2. Cliquez sur en fonction la **nouvelle stratégie**.

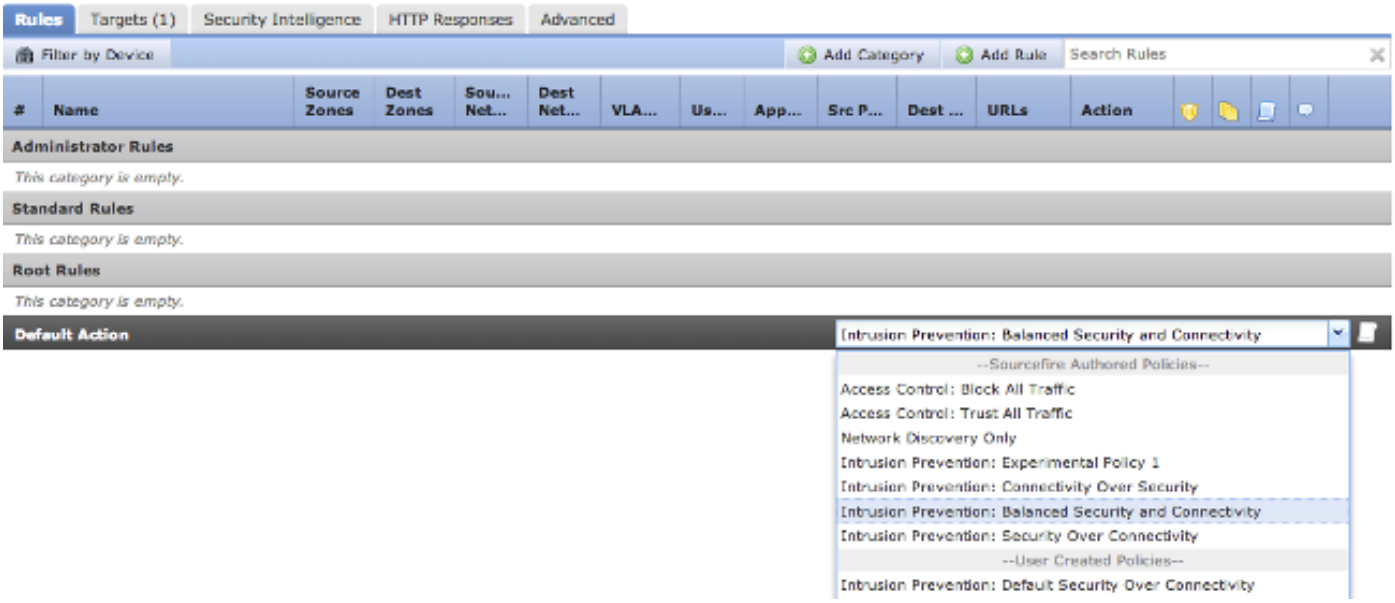


3. Fournissez un **nom** pour la stratégie et une **description**.

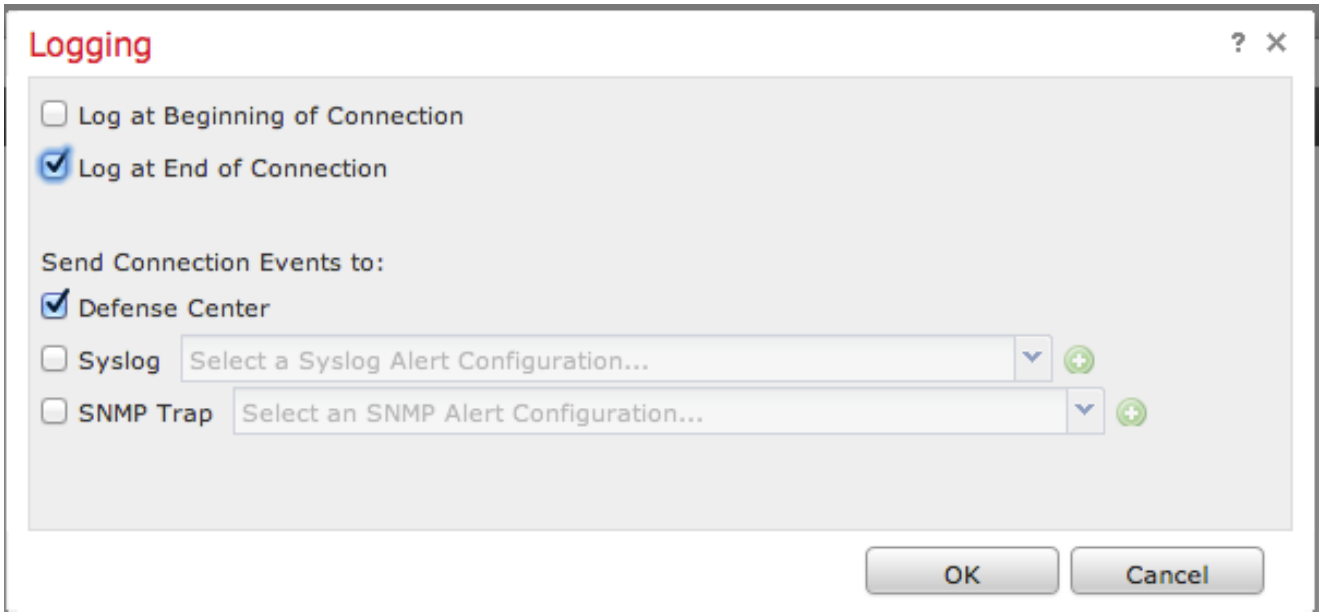
4. **Prévention des intrusions** choisie comme **action par défaut de la** stratégie de contrôle d'accès.

5. Sélectionnez enfin les **périphériques visés aux**quels vous voulez appliquer la stratégie de contrôle d'accès, et cliquez sur la **sauvegarde**.

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



7. Se connecter de connexion doit être activé générer des événements de connexion. Cliquez sur le menu de baisse vers le bas qui est juste de l'**action par défaut**.



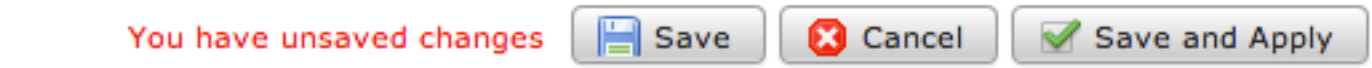
8. Choisissez de se connecter des connexions au début ou à la fin de la connexion. Les événements peuvent être ouverts une session le centre de Gestion de FireSIGHT, un emplacement de Syslog, ou par le SNMP.

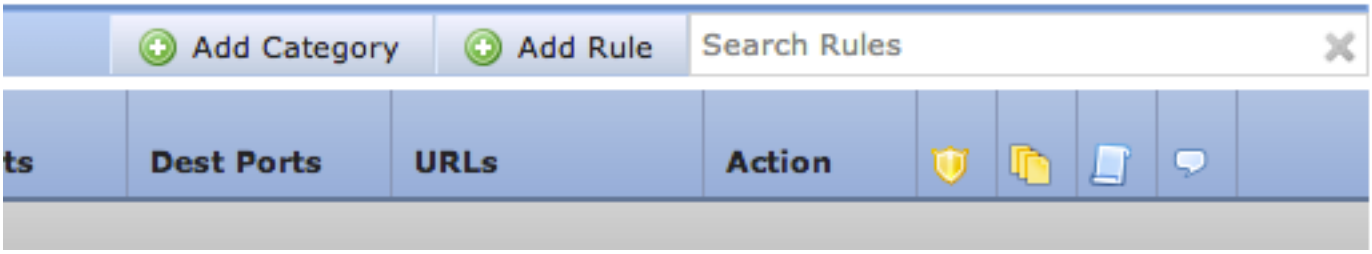
> Remarque: Il n'est pas recommandé pour se connecter aux deux extrémités de la connexion parce que chaque connexion (excepté les connexions bloquées) sont enregistré deux fois. Se connecter au début est utile pour les connexions qui seront bloquées, et se connecter à l'extrémité est utile pour toutes autres connexions.

9. Cliquez sur **OK**. Notez que la couleur de l'icône se connectante a changé.

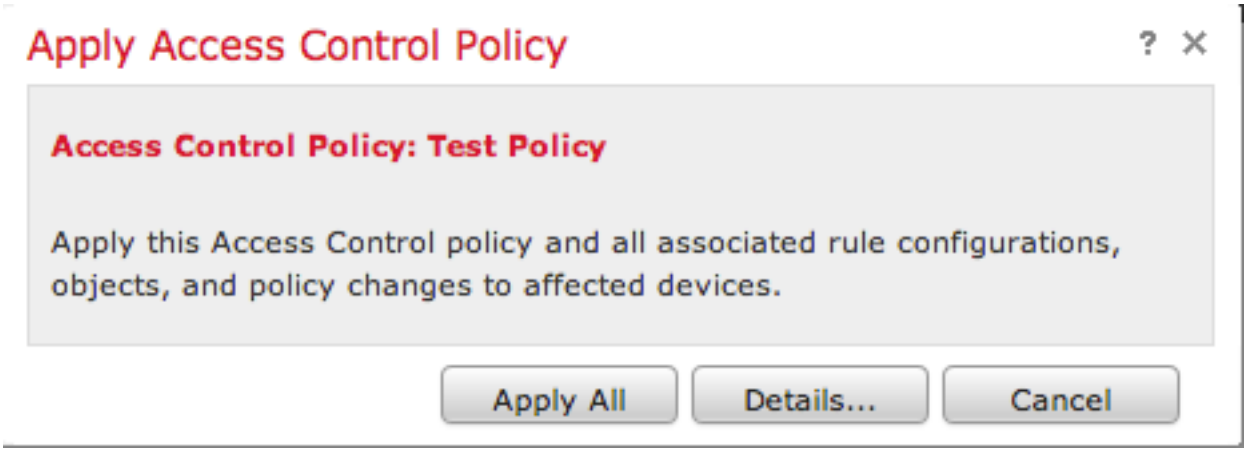
10. Vous pouvez ajouter une **règle de contrôle d'accès** à ce moment. Les options que vous pouvez utiliser dépendent du type de permis vous avez installés.

11. Quand vous êtes apporter des modifications de finition. cliquez sur la **sauvegarde et le bouton Apply**. Vous noterez un message vous indiquer pour avoir les modifications unsaved sur votre stratégie sur le coin supérieur droit jusqu'à ce que le bouton soit cliqué sur.





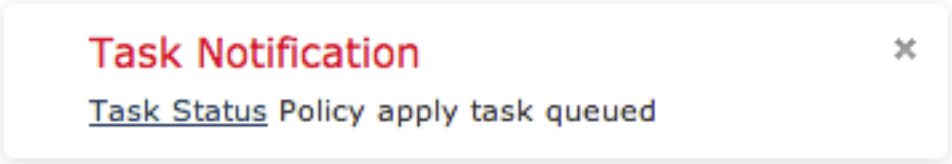
Vous pouvez choisir **de sauvegarder** seulement les modifications ou de cliquer sur en fonction la **sauvegarde et de s'appliquer**. La fenêtre suivante apparaîtra si vous choisissez ce dernier.



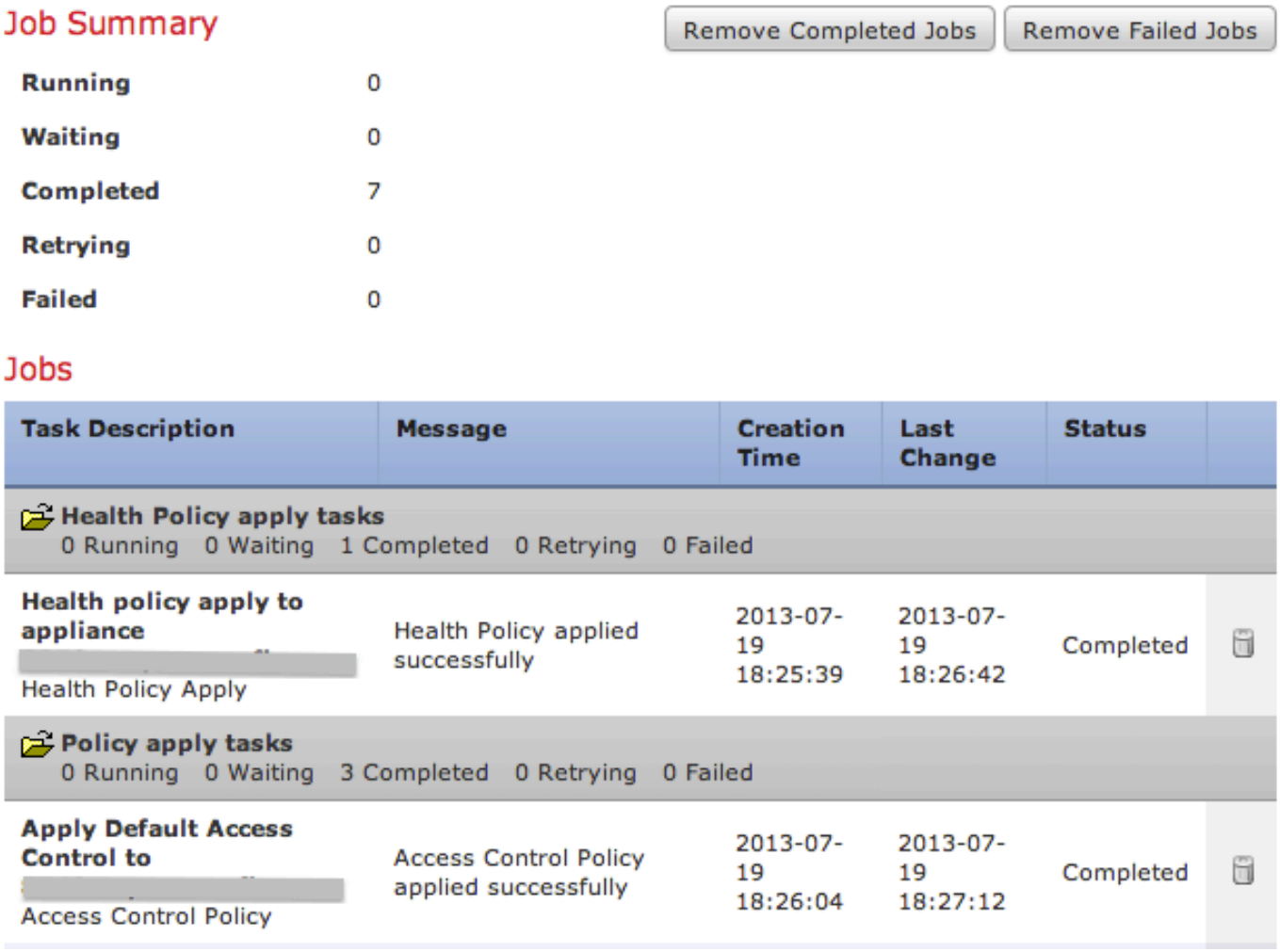
12. **Appliquez tous** appliquera la stratégie de contrôle d'accès et n'importe quelles stratégies associées d'intrusion aux périphériques visés.

> Remarque: Si une stratégie d'intrusion sera appliquée pour la première fois, elle ne peut pas être non sélectionnée.

13. Vous pouvez surveiller le statut de la tâche cliquant sur sur le lien d'**état de tâche** sur la notification affichée en haut de la page, ou en naviguant vers : **État de système > de surveillance > de tâche**



14. Cliquez sur le lien d'état de tâche pour surveiller la progression de la stratégie de contrôle d'accès s'appliquent.



Étape 10 : Vérifiez si le centre de Gestion de FireSIGHT reçoit des événements

Après que la stratégie de contrôle d'accès s'appliquent se soit terminée, vous devriez commencer voir des événements de connexions et selon des événements d'intrusion du trafic.

Recommandation supplémentaire

Vous pouvez également configurer les fonctionnalités supplémentaires suivantes sur votre système. Veuillez se référer au guide utilisateur pour des détails d'implémentation.

- Sauvegardes programmées
- Mise à jour logicielle automatique, SRU, VDB, et téléchargements de GeoLocation/installations.
- Authentification externe par le LDAP ou le RAYON