

# 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.

**Change Password**

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password

Confirm

**Network Settings**

Use these fields to specify network-related information for the management interface on the appliance.

Protocol  IPv4  IPv6  Both

IPv4 Management IP

Netmask

IPv4 Default Network Gateway

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

**Time Settings**

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock  Via NTP from

Manually 2013 ▾ / July ▾ / 19 ▾ , 9 ▾ : 25 ▾

Current Time 2013-07-19 09:25

Set Time Zone [America/New York](#)

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.

## Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

- Install Now
- Enable Recurring Rule Update Imports

## Recurring Geolocation Updates

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

- Install Now
- Enable Recurring Weekly Updates

## Automatic Backups

Use this field to schedule automatic configuration backups.

- Enable Automatic Backups

## License Settings

To obtain your license, navigate to \_\_\_\_\_ where you will be prompted for the license key \_\_\_\_\_ and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can.

License Key \_\_\_\_\_

Add/Verify

Type	Description	Expires
------	-------------	---------

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.

## Device Registration

Use this section to add, license, and apply initial access control policies to pre-registered devices. Note that you do not need to add devices to the secondary Defense Center in a high availability pair. If you enable the Apply Default Access Control Policies option, the applied policy for each device depends on the detection mode (Inline, Passive, Access Control, or Network Discovery) you configured for the device.

Click Add to add each device.

Apply Default Access Control Policies

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Add"/>

## End User License Agreement

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT, THEN SOURCEFIRE IS UNWILLING TO LICENSE THE LICENSED MATERIALS TO YOU, IN WHICH CASE YOU MAY NOT DOWNLOAD, INSTALL OR USE ANY OF THE LICENSED MATERIALS.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT INITIATE USE OF THE PRODUCT. BY SELECTING "I ACCEPT," "OK," "CONTINUE," "YES," "NEXT" OR BY INSTALLING OR USING THE LICENSED MATERIALS IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE PRODUCT.

If You are located outside of the United States, then Sourcefire International GmbH, a subsidiary located in Switzerland, shall be a party to this Agreement with You and the party licensing the Licensed Materials to You hereunder. This Agreement governs Your access and use of the Sourcefire Products, except to the extent there is a separate written agreement signed by both You and Sourcefire that expressly states that it governs Your use of the Sourcefire Products. In the event of a conflict between the provisions of such a written agreement and this Agreement, the order of precedence shall be (1) the separate signed agreement, and (2) this Agreement.

### 1. DEFINITIONS

The following capitalized terms shall have the following meanings in this EULA:

1.1. "Appliance" means any Sourcefire-branded network security appliance made available to You, consisting of Hardware and pre-installed Sourcefire Software and/or

I have read and agree to the END USER LICENSE AGREEMENT

## 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 : **Systeme > Licences**.
- Cliquez sur **Ajouter une nouvelle licence**.

## Add Feature License

License Key

License

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to

Using the license key,  follow the on-screen instructions to generate a license.

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.

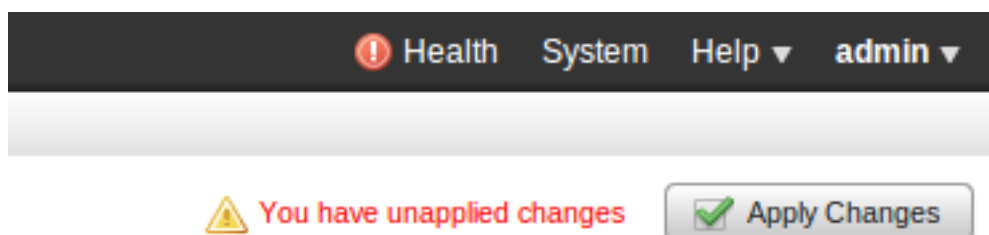
1. Accédez à la page suivante : **Périphériques > Gestion des périphériques**.
2. Cliquez sur le périphérique pour lequel vous souhaitez activer les licences et saisissez l'onglet Périphérique.
3. Cliquez sur l'icône **Modifier** (*crayon*) en regard de Licence.

### License

Protection:	Yes
Control:	Yes
Malware:	Yes
URL Filtering:	Yes
VPN	Yes

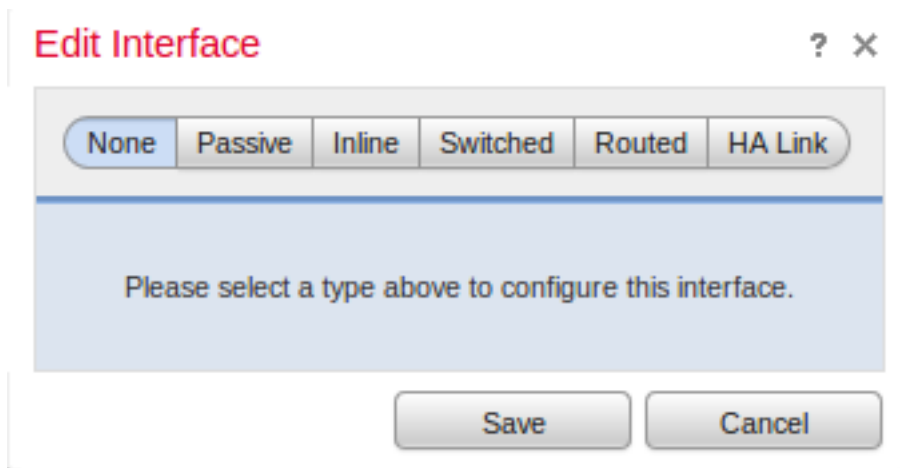
Activez les licences requises pour ce périphérique et cliquez sur **Enregistrer**.

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 :

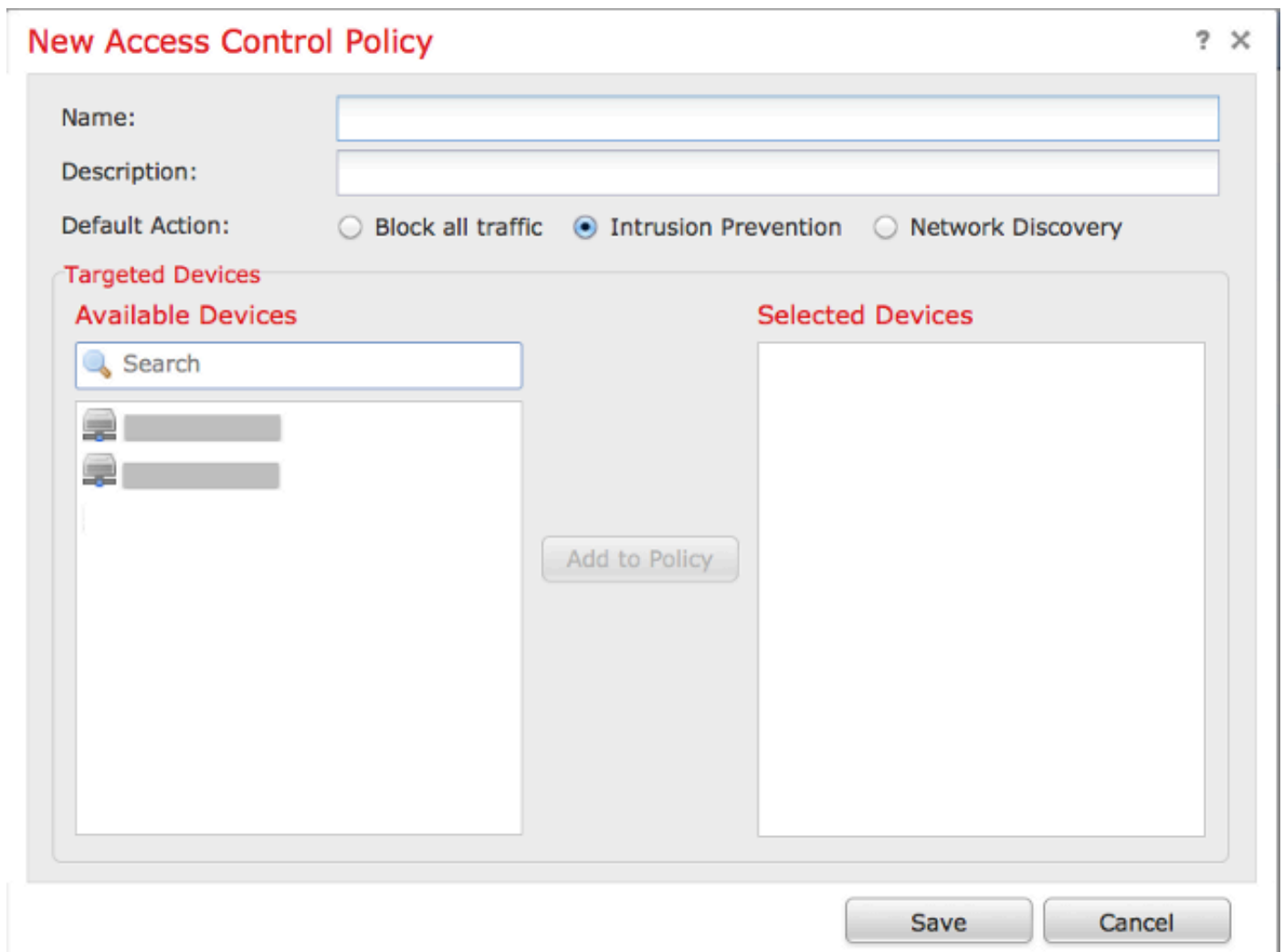
Vous devez attribuer un nom et définir la stratégie de base à utiliser. En fonction de votre déploiement, vous pouvez choisir d'utiliser l'option **Supprimer lorsque Inline** est activée. Définissez les réseaux à protéger pour réduire les faux positifs et améliorer les performances du système.

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**.



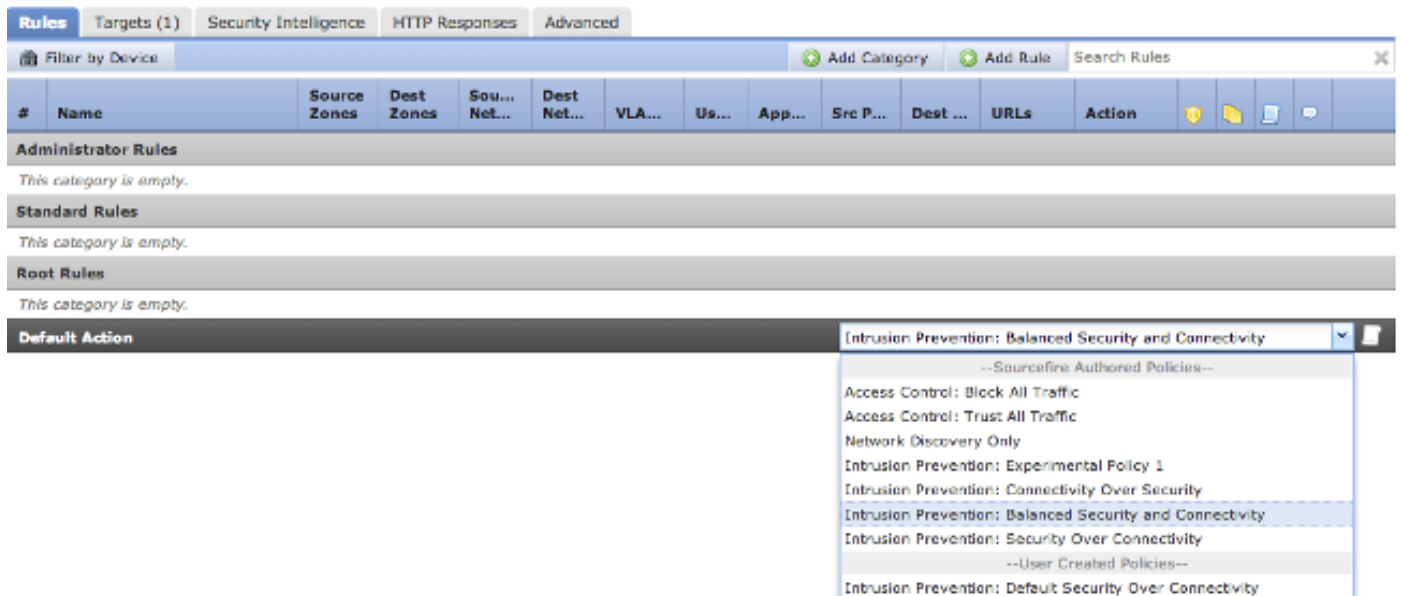
The screenshot shows a window titled "New Access Control Policy" with a search icon and a close button in the top right corner. The window contains the following fields and options:

- Name:** A text input field.
- Description:** A text input field.
- Default Action:** Three radio button options: "Block all traffic", "Intrusion Prevention" (which is selected), and "Network Discovery".
- Targeted Devices:** A section with two columns:
  - Available Devices:** A list of devices with a search bar above it. Two device icons are visible.
  - Selected Devices:** An empty list box.
  - Add to Policy:** A button located between the two columns.

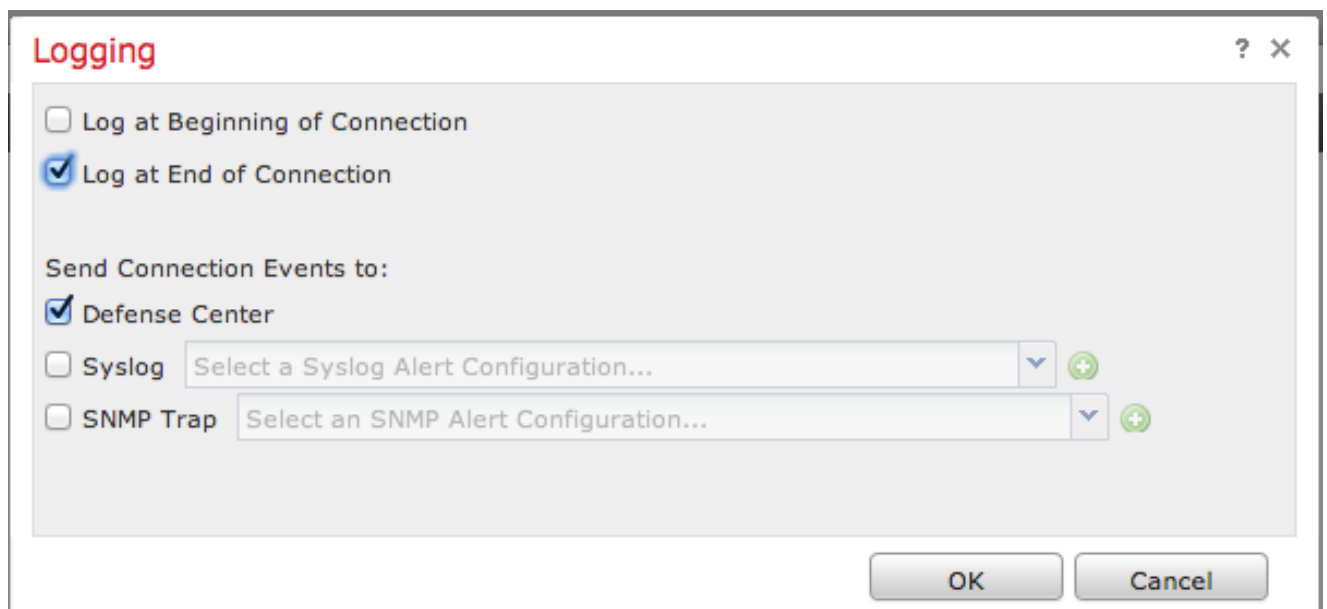
At the bottom right of the window, there are two buttons: "Save" and "Cancel".

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.

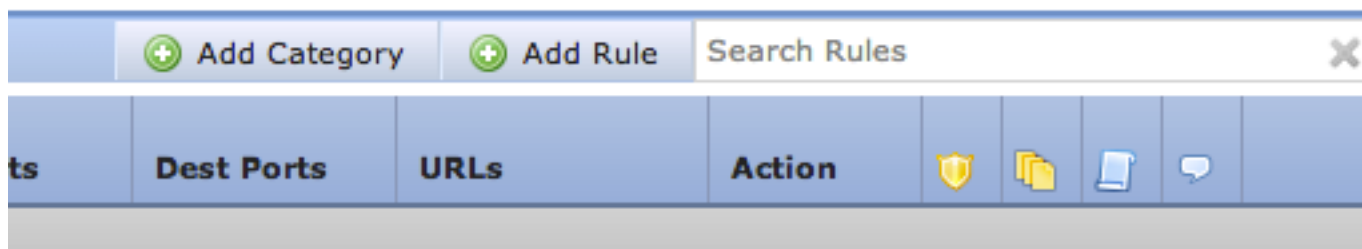
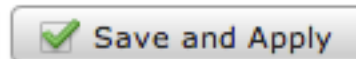
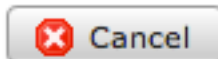
**Note:** Il n'est pas recommandé de se connecter aux deux extrémités de la connexion, car chaque connexion (à l'exception des connexions bloquées) sera consignée deux fois. La journalisation au début est utile pour les connexions qui seront bloquées et la journalisation à la fin est utile pour toutes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

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

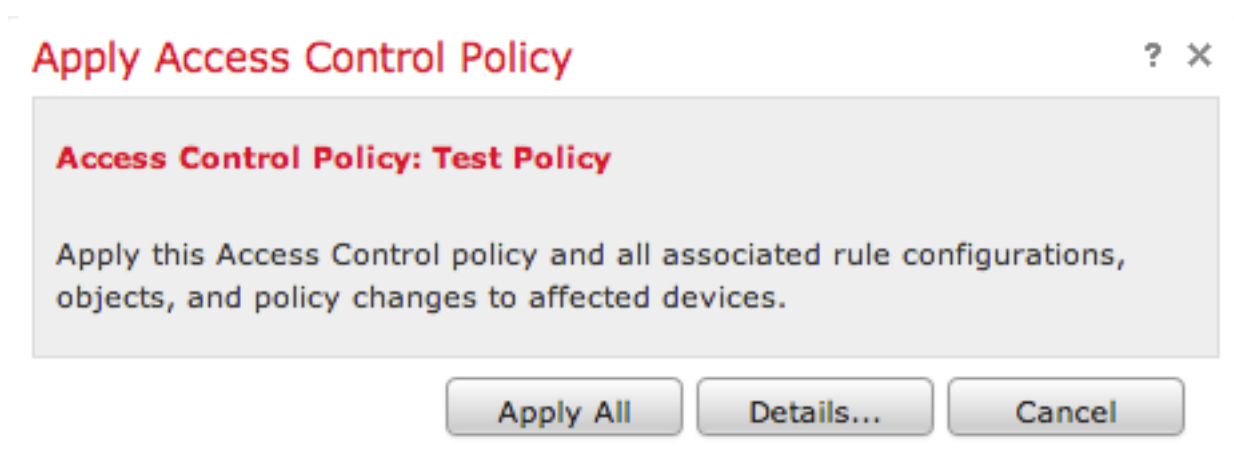
10. Vous pouvez ajouter une **règle de contrôle d'accès** à ce stade. Les options que vous pouvez utiliser dépendent du type de licence que vous avez installé.

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.

You have unsaved changes



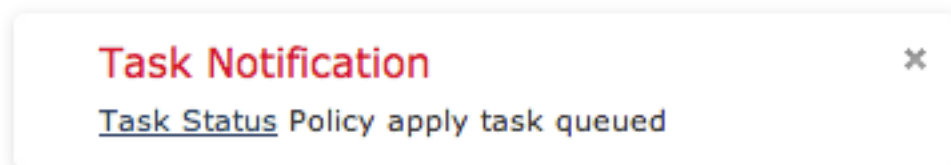
Vous pouvez choisir d'enregistrer uniquement les modifications ou de cliquer sur **Enregistrer et appliquer**. La fenêtre suivante s'affiche si vous choisissez cette dernière option.



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.





## Job Summary

Remove Completed Jobs

Remove Failed Jobs

Running	0
Waiting	0
Completed	7
Retrying	0
Failed	0

## Jobs

Task Description	Message	Creation Time	Last Change	Status	
 <b>Health Policy apply tasks</b> 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
<b>Health policy apply to appliance</b> [redacted] Health Policy Apply	Health Policy applied successfully	2013-07-19 18:25:39	2013-07-19 18:26:42	Completed	
 <b>Policy apply tasks</b> 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
<b>Apply Default Access Control to</b> [redacted] Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

## 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