

Étapes de configuration initiale des systèmes de FireSIGHT

Contenu

[Introduction](#)

[Condition préalable](#)

[Configuration](#)

[Étape 1 : Première installation](#)

[Étape 2 : Installs licenses](#)

[Étape 3 : Appliquez la stratégie de système](#)

[Étape 4 : Appliquez la politique sanitaire](#)

[Étape 5 : Périphériques gérés de registre](#)

[Étape 6 : Permis installés par enable](#)

[Étape 7 : Configurez sentir des interfaces](#)

[Étape 8 : Configurez la stratégie d'intrusion](#)

[Étape 9 : Configurez et appliquez une stratégie de contrôle d'accès](#)

[Étape 10 : Vérifiez si le centre de Gestion de FireSIGHT reçoit des événements](#)

[Recommandation supplémentaire](#)

Introduction

Après que vous réimaginez 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

À votre 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 paginée, 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.

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 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.

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
------	-------------	---------

À cette 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.

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 : 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 : **Systeme > permis**.
- Cliquez sur **ajoutent** en fonction le **nouveau permis**.

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 ne recevez 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 santé 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 enregistrez 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.

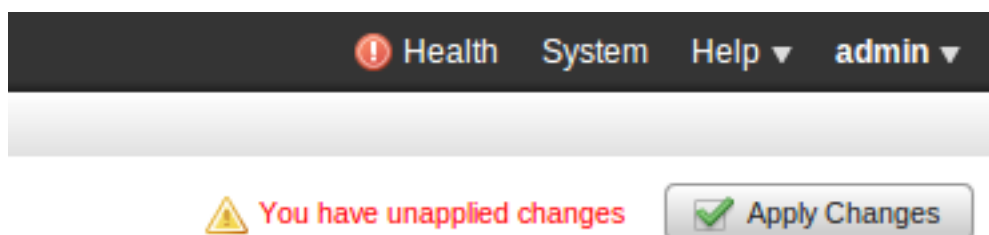
1. Naviguez vers la page suivante : **Périphériques > Gestion de périphériques**.
2. Cliquez sur en fonction le périphérique pour lequel vous voulez activer les permis et écrivez l'onglet de périphérique.
3. Cliquez sur l'**éditer** (icône de *crayon*) à côté du permis.

License

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

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 cliquez 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.

Edit Interface ? X

None Passive Inline Switched Routed HA Link

Please select a type above to configure this interface.

Save Cancel

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 :

Create Intrusion Policy ? X

Policy Information

Name *

Description

Drop when Inline

Base Policy

Variables

Use the system default value

Networks to protect

* Required

Create Policy Create and Edit Policy Cancel

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 **créer 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**.

New Access Control Policy ? X

Name:

Description:

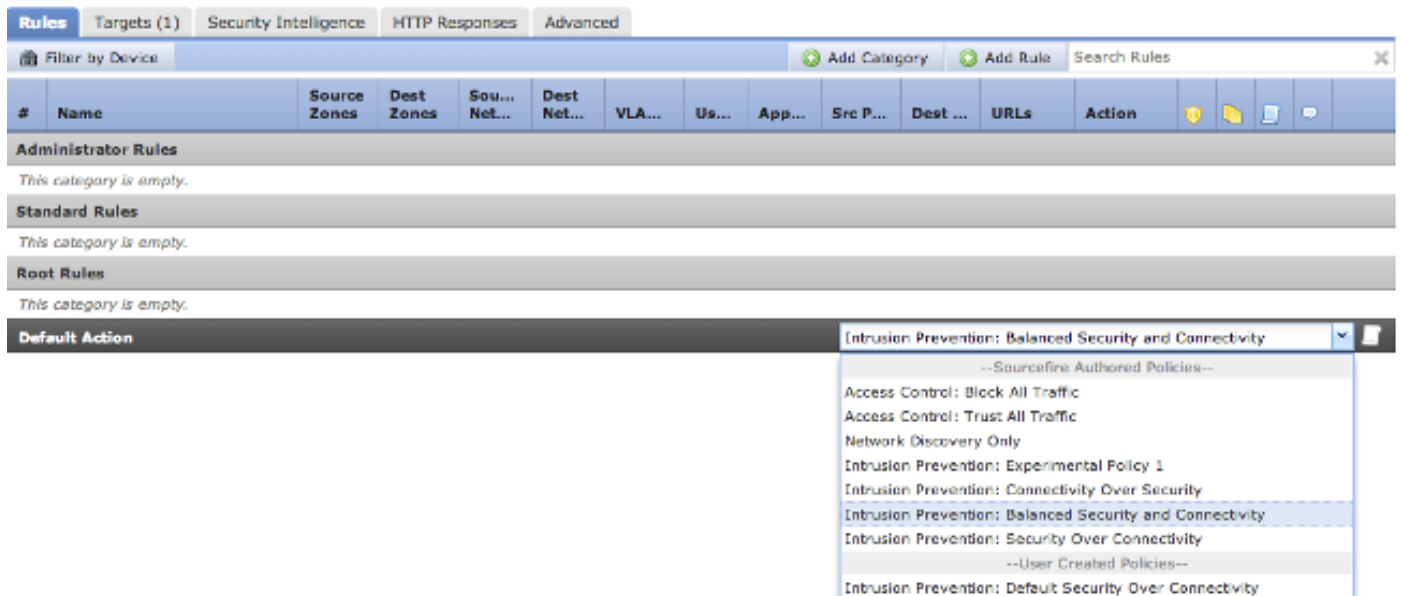
Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

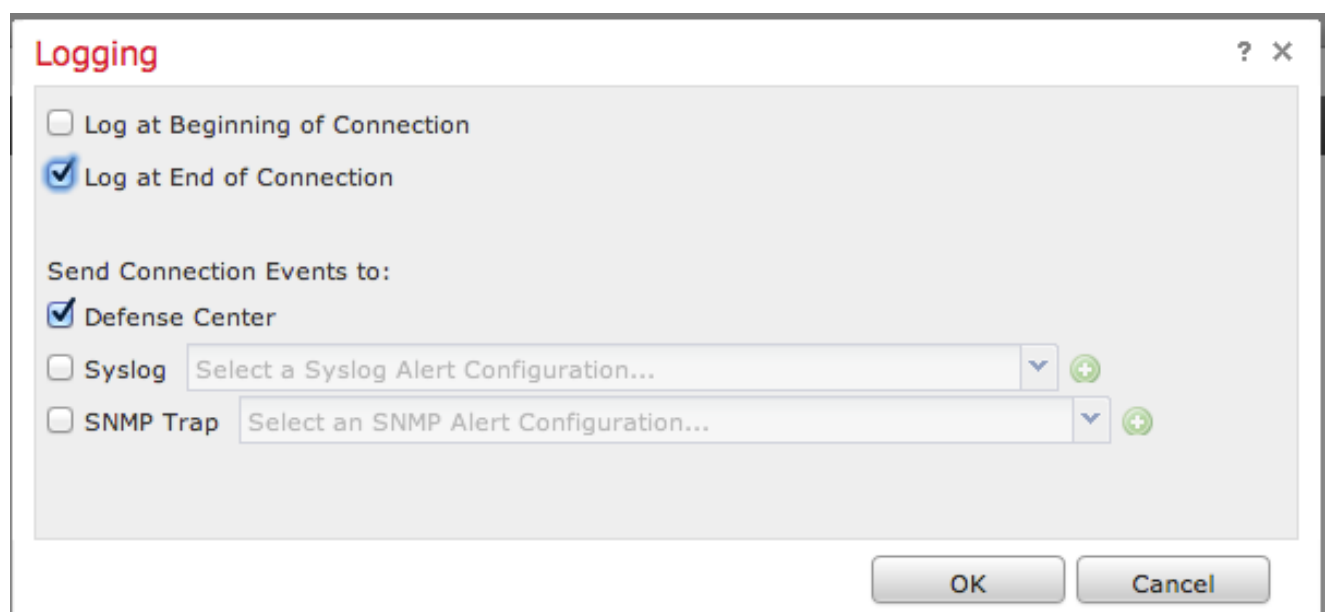
Available Devices

Selected Devices

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** auxquels 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.

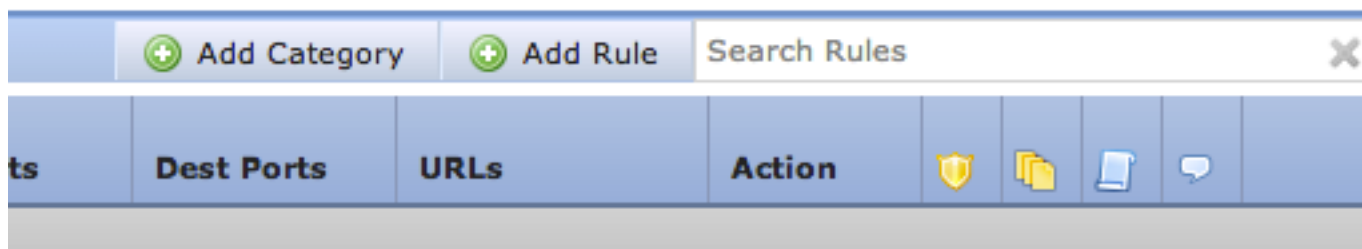
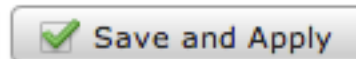
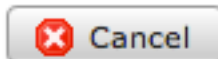
Remarque: Il n'est pas recommandé pour se connecter aux deux extrémités de la connexion parce que chaque connexion (excepté les connexions bloquées) sont enregistré deux fois. Se connecter au début est utile pour les connexions qui seront bloquées, et se connecter à l'extrémité est utile pour toutes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

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

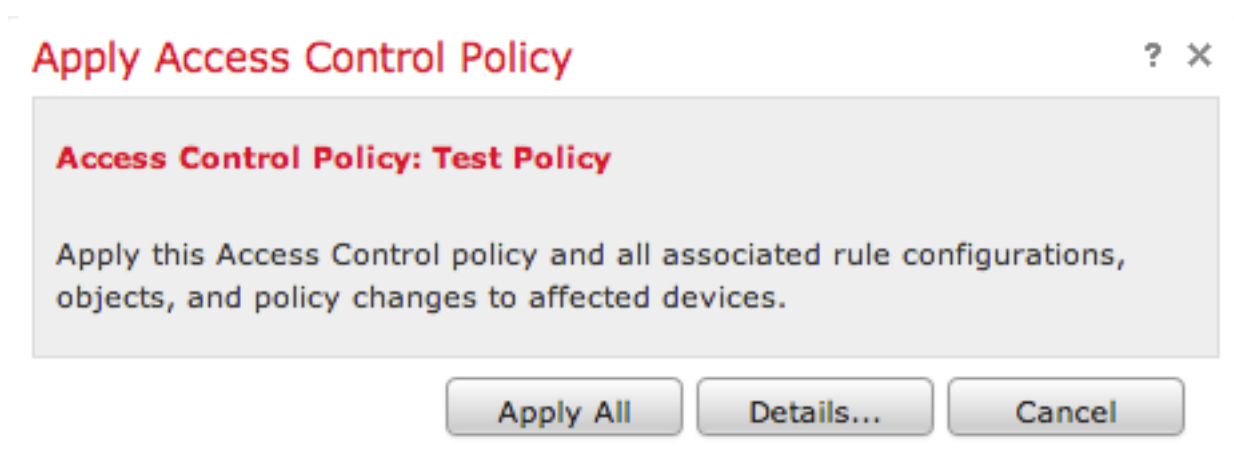
10. Vous pouvez ajouter une **règle de contrôle d'accès** à ce moment. Les options que vous pouvez utiliser dépendent du type de permis vous avez installés.

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.

You have unsaved changes



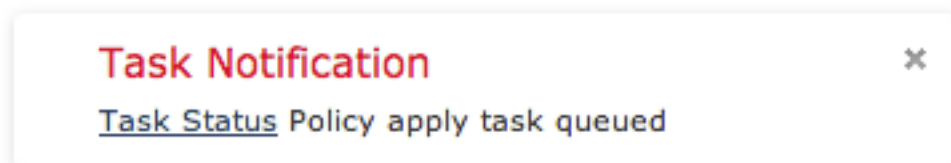
Vous pouvez choisir de **sauvegarder** seulement les modifications ou de cliquer sur **en fonction la sauvegarde et de s'appliquer**. La fenêtre suivante apparaîtra si vous choisissez ce dernier.



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.





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	
 Health Policy apply tasks 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
Health policy apply to appliance Health Policy Apply	Health Policy applied successfully	2013-07-19 18:25:39	2013-07-19 18:26:42	Completed	
 Policy apply tasks 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
Apply Default Access Control to Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

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