

Pasos de la configuración inicial de los sistemas de FireSIGHT

Contenido

[Introducción](#)

[Requisito previo](#)

[Configuración](#)

[Paso 1: Configuración inicial](#)

[Paso 2: Instale las licencias](#)

[Paso 3: Aplique la política del sistema](#)

[Paso 4: Aplique la política sanitaria](#)

[Paso 5: Dispositivos administrados del registro](#)

[Paso 6: Licencias instaladas permiso](#)

[Paso 7: Configuración que detecta las interfaces](#)

[Paso 8: Configure la directiva de la intrusión](#)

[Paso 9: Configure y aplique una directiva del control de acceso](#)

[Paso 10: Verifique si el centro de administración de FireSIGHT recibe los eventos](#)

[Recomendación adicional](#)

Introducción

Después de que usted nueva imagen un centro de administración de FireSIGHT o un dispositivo de FirePOWER, usted necesite completar varios pasos para hacer el sistema completamente - funcional y generar las alertas para los eventos de la intrusión; por ejemplo, instalando la licencia, registrando los dispositivos, aplicando la política sanitaria, la política del sistema, la directiva del control de acceso, la directiva etc. de la intrusión. Este documento es un suplemento a la guía de instalación del sistema de FireSIGHT.

Requisito previo

Esta guía asume que usted ha leído cuidadosamente la guía de instalación del sistema de FireSIGHT.

Configuración

Paso 1: Configuración inicial

En su centro de administración de FireSIGHT, usted debe completar el proceso de configuración registrando en la interfaz Web y especificando las opciones de configuración inicial en la página de configuración, representada abajo. En esta página, usted debe cambiar la clave del administrador, y puede también especificar las configuraciones de red tales como dominio y servidores DNS, y la configuración del tiempo.

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 / / , :

Current Time 2013-07-19 09:25

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

Usted puede configurar opcionalmente las actualizaciones de la regla que se repiten y del geolocation así como los respaldos automáticos. Cualquier licencia de función se puede también instalar en este momento.

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

En esta página, usted puede también registrar un dispositivo al centro de administración de FireSIGHT y especificar a un modo de detección. El modo de detección y las otras opciones que usted elige durante el registro determinan las interfaces predeterminadas, los conjuntos en línea, y las zonas que el sistema crea, así como las directivas que aplican inicialmente a los dispositivos administrados.

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

Paso 2: Instale las licencias

Si usted no instaló las licencias durante la página de la configuración inicial, usted puede completar la tarea siguiendo los siguientes pasos:

- Navegue a la página siguiente: **Sistema > licencias**.
- Haga clic en **agregar la nueva licencia**.

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 usted no recibió una licencia, entre en contacto el Representante representante de ventas de su cuenta.

Paso 3: Aplique la política del sistema

La política del sistema especifica la configuración para los perfiles de la autenticación y la sincronización horaria entre el centro de administración de FireSIGHT y los dispositivos administrados. Para configurar o aplicar la política del sistema navegue al **sistema > al Local > a la política del sistema**. Una directiva del sistema predeterminado se proporciona pero necesita ser aplicada a cualquier dispositivo administrado.

Paso 4: Aplique la política sanitaria

La política sanitaria se utiliza para configurar cómo los dispositivos administrados señalan su estado de salud al centro de administración de FireSIGHT. Para configurar o aplicar la política sanitaria navegue a la **salud > a la política sanitaria**. Una política sanitaria predeterminada se proporciona pero necesita ser aplicada a cualquier dispositivo administrado.

Paso 5: Dispositivos administrados del registro

Si usted no se registró los dispositivos durante la configuración inicial paginan, leen [este documento](#) para las instrucciones en cómo registrar un dispositivo a un centro de administración de FireSIGHT.

Paso 6: Licencias instaladas permiso

Antes de que usted pueda utilizar cualquier licencia de función en su dispositivo, usted necesita habilitarlo para cada dispositivo administrado.

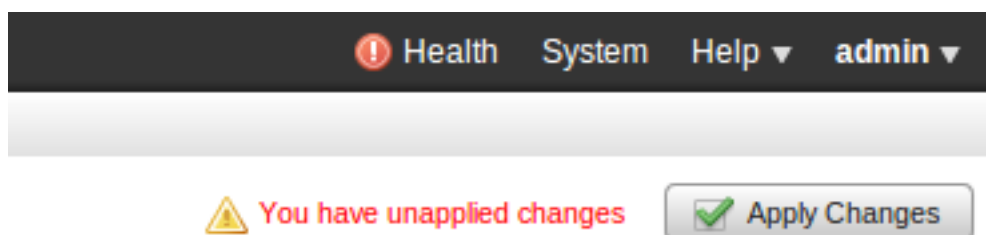
1. Navegue a la página siguiente: **Dispositivos > Administración de dispositivos**.
2. Haga clic en el dispositivo para el cual usted quiere habilitar las licencias y ingresa la lengüeta del dispositivo.
3. Haga clic el **editar** (icono del *lápiz*) al lado de la licencia.

License

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

Habilite las licencias requeridas para este dispositivo y haga clic la **salvaguardia**.

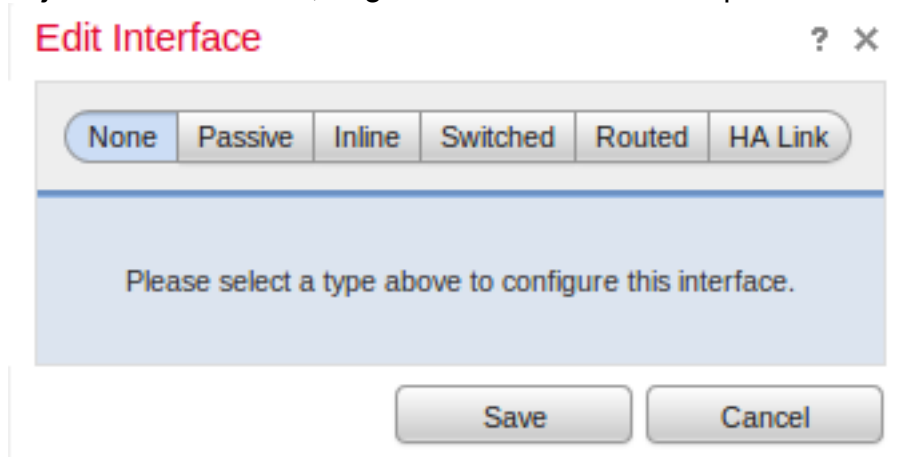
Note el mensaje “*usted para tener cambios inaplicados*” en la esquina superior derecha. Esta advertencia sigue siendo activa incluso si usted navega lejos de la página de la Administración de dispositivos hasta que usted haga clic el botón de los **cambios de la aplicación**.



Paso 7: Configuración que detecta las interfaces

1. Navegue a los **dispositivos > a la Administración de dispositivos** siguientes de la página.

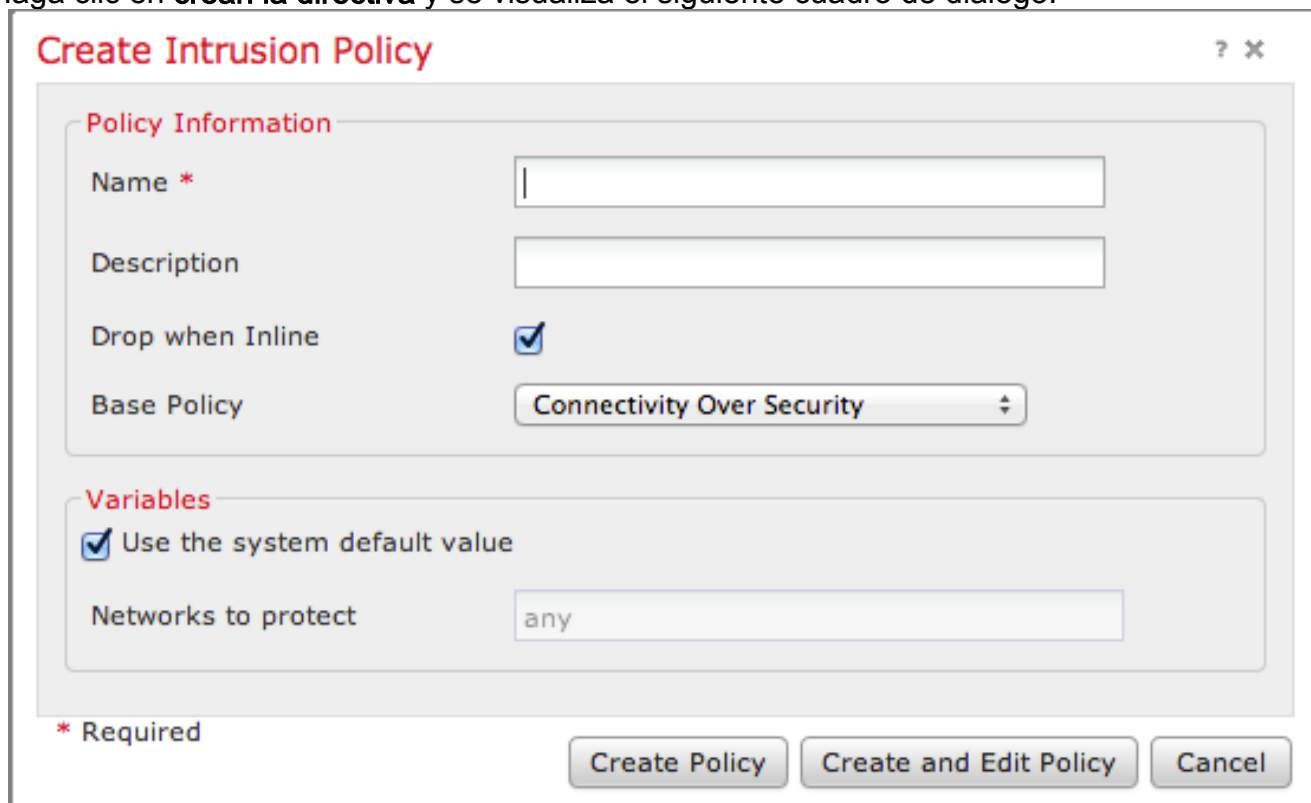
2. Haga clic el icono del **editar** (lápiz) para el sensor de su opción.
3. Bajo **interfaces** tabule, haga clic el icono del **editar** para la interfaz de su opción.



Seleccione una configuración de la interfaz pasiva o en línea. Conmutado y las interfaces ruteadas esté fuera del alcance de este artículo.

Paso 8: Configure la directiva de la intrusión

- Navegue a la página siguiente: **Directivas > intrusión > directiva de la intrusión.**
- Haga clic en **crean la directiva** y se visualiza el siguiente cuadro de diálogo:



Usted debe asignar un nombre y definir la directiva baja que se utilizará. Dependiendo de su despliegue que usted puede eligió tener el **descenso de la** opción **cuando en línea** estaba habilitado. Defina las redes que usted quiere proteger para reducir los falsos positivos y para mejorar el funcionamiento del sistema.

El hacer clic en **crea la directiva** salvará sus configuraciones y creará la directiva IPS. Si usted quiere hacer alguna modificación a la directiva de la intrusión, usted puede elegir **crea y edita la directiva** en lugar de otro.

Note: Las directivas de la intrusión son aplicadas como parte de la directiva del control de acceso. Después de que una directiva de la intrusión sea aplicada, cualquier modificación puede ser aplicada sin reaplicar la directiva entera del control de acceso haciendo clic el botón del **reaplicar**.

Paso 9: Configure y aplique una directiva del control de acceso

1. Navegue a las **directivas > al control de acceso**.
2. Haga clic en la **nueva directiva**.

New Access Control Policy ? X

Name:

Description:

Default Action: Block all traffic Intrusion Prevention Network Discovery

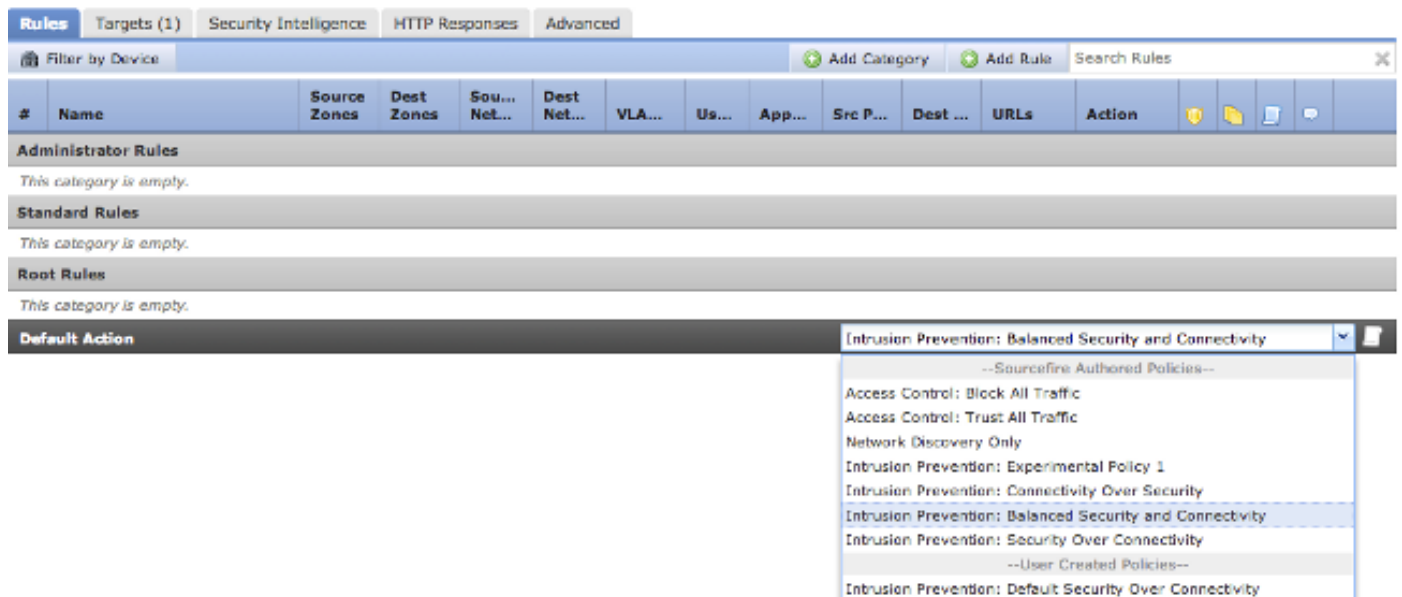
Targeted Devices

Available Devices

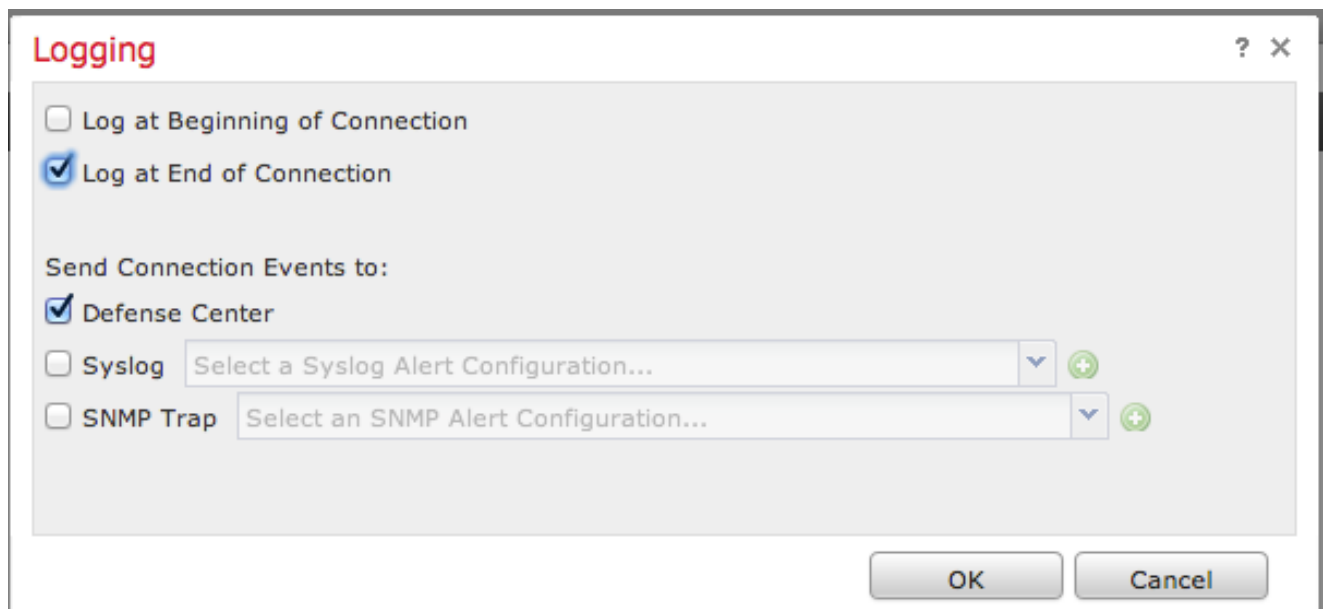
Selected Devices

3. Proporcione un **nombre** para la directiva y una **descripción**.
4. Seleccione la **prevención de intrusiones** como la **acción predeterminada de la** directiva del control de acceso.
5. Finalmente seleccione los **dispositivos apuntados a** los cuales usted quiere aplicar la directiva del control de acceso, y haga clic la **salvaguardia**.

6. Seleccione su directiva de la intrusión para la acción predeterminada.



7. El registro de la conexión se debe habilitar para generar los eventos de conexión. Haga clic el menú desplegable que correcto de la **acción predeterminada**.



8. Elija registrar las conexiones en el principio o el extremo de la conexión. Los eventos se pueden abrir una sesión el centro de administración de FireSIGHT, una ubicación del Syslog, o con el SNMP.

Note: No se recomienda para registrar en los ambos extremos de la conexión porque cada conexión (excepto las conexiones bloqueadas) será registrada dos veces. La registración al principio es útil para las conexiones que serán bloqueadas, y el registro en el extremo es útil para el resto de las conexiones.

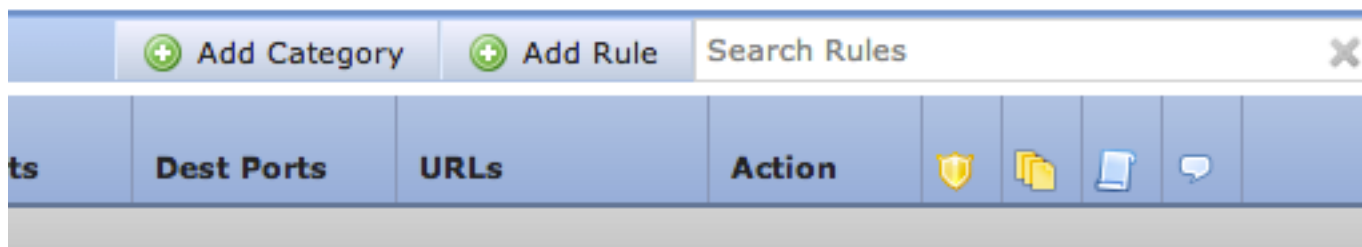
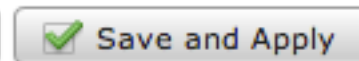
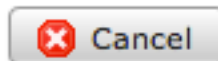
9. Click OK. Observe que el color del icono del registro ha cambiado.

10. Usted puede agregar una **regla del control de acceso** ahora. Las opciones que usted puede utilizar dependen del tipo de licencias usted ha instalado.

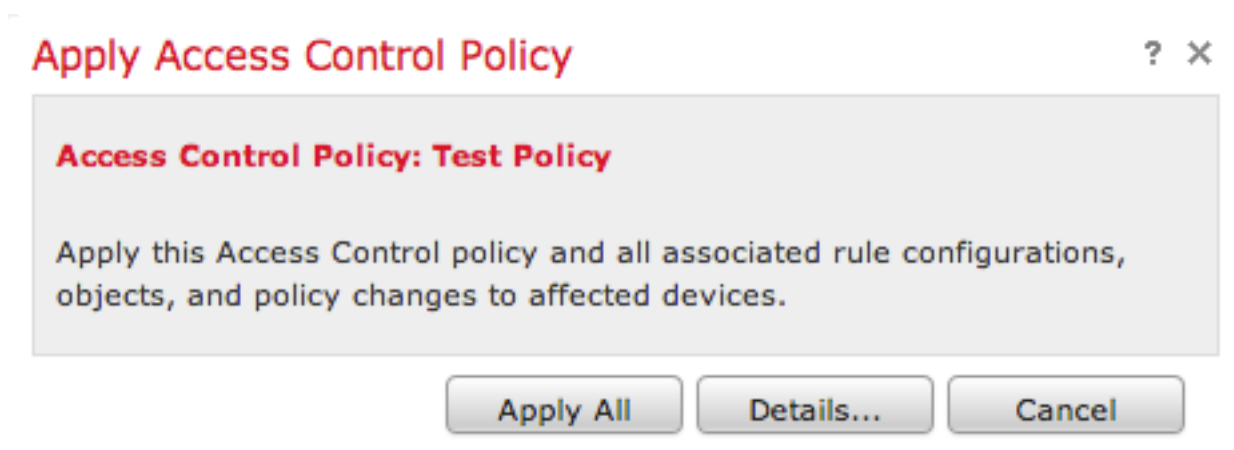
11. Cuando usted es fabricación acabada cambia. haga clic la **salvaguardia** y el botón **Apply**

Button. Usted notará un mensaje el indicar de usted para tener cambios unsaved en su directiva en la esquina superior derecha hasta que se haga clic el botón.

You have unsaved changes



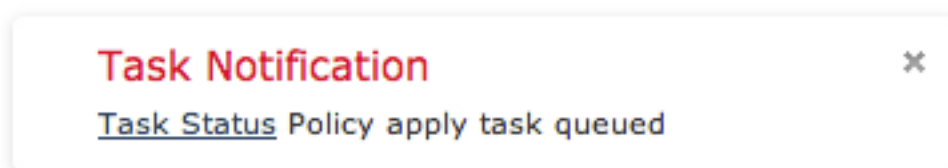
Usted puede elegir **salvar** solamente los cambios o hacer clic en la **salvaguardia y aplicarse**. La ventana siguiente aparecerá si usted elige estos últimos.



12. **Aplique todos** aplicará la directiva del control de acceso y cualquier directiva asociada de la intrusión a los dispositivos apuntados.

Note: Si una directiva de la intrusión es aplicada por primera vez, no puede ser no seleccionada.

13. Usted puede monitorear el estatus de la tarea que hace clic en el link del **estatus de la tarea** en la notificación mostrada en la cima de la página, o navegando a: **Estatus del sistema > de la supervisión > de la tarea**



14. Haga clic el link del estatus de la tarea para monitorear el progreso de la directiva del control de acceso se aplican.





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 [redacted] 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 [redacted] Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

Paso 10: Verifique si el centro de administración de FireSIGHT recibe los eventos

Después de que la directiva del control de acceso se aplique haya completado, usted debe comenzar a ver los eventos de las conexiones y dependiendo de los eventos de la intrusión del tráfico.

Recomendación adicional

Usted puede también configurar las características adicionales siguientes en su sistema. Refiera por favor al guía del usuario para los detalles de instrumentación.

- Backups planificados
- Actualización de software automática, SRU, VDB, y descargas de GeoLocation/instalaciones.
- Autenticación externa con el LDAP o el RADIUS