

Pasos iniciales de configuración de FireSIGHT Systems

Contenido

[Introducción](#)

[Requisito previo](#)

[Configuración](#)

[Paso 1: Configuración inicial](#)

[Paso 2: Instalar licencias](#)

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

[Paso 4: Aplicación de la política de estado](#)

[Paso 5: Registrar dispositivos gestionados](#)

[Paso 6: Habilitar licencias instaladas](#)

[Paso 7: Configurar interfaces de detección](#)

[Paso 8: Configuración de la política de intrusiones](#)

[Paso 9: Configurar y aplicar una política de control de acceso](#)

[Paso 10: Verifique si FireSIGHT Management Center recibe eventos](#)

[Recomendación adicional](#)

Introducción

Después de recrear la imagen de un FireSIGHT Management Center o de un dispositivo FirePOWER, debe completar varios pasos para que el sistema funcione correctamente y generar alertas para eventos de intrusión; por ejemplo, instalación de licencias, registro de dispositivos, aplicación de políticas de estado, políticas del sistema, política de control de acceso, política de intrusiones, etc. Este documento es un suplemento de la Guía de instalación del sistema FireSIGHT.

Requisito previo

En esta guía se asume que ha leído cuidadosamente la Guía de instalación del sistema FireSIGHT.

Configuración

Paso 1: Configuración inicial

En FireSIGHT Management Center, debe completar el proceso de configuración iniciando sesión en la interfaz web y especificando las opciones de configuración iniciales en la página de configuración, que se muestra a continuación. En esta página, debe cambiar la contraseña de administrador y también puede especificar la configuración de red, como servidores DNS y de dominio, y la configuración de hora.

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](#)

Opcionalmente, puede configurar actualizaciones de geolocalización y reglas recurrentes, así como copias de seguridad automáticas. En este momento también se pueden instalar licencias de funciones.

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, también puede registrar un dispositivo en FireSIGHT Management Center y especificar un modo de detección. El modo de detección y otras opciones que elija durante el registro determinan las interfaces predeterminadas, los conjuntos en línea y las zonas que crea el sistema, así como las políticas que aplica 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="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: Instalar licencias

Si no instaló licencias durante la página de configuración inicial, puede completar la tarea siguiendo estos pasos:

- Vaya a la página siguiente: **System > Licenses**.
- Haga clic en **Add New License**.

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 no ha recibido una licencia, póngase en contacto con el representante de ventas de su cuenta.

Paso 3: Aplicación de la política del sistema

La política del sistema especifica la configuración para los perfiles de autenticación y la sincronización horaria entre el FireSIGHT Management Center y los dispositivos administrados. Para configurar o aplicar la política del sistema, navegue hasta **System > Local > System Policy**. Se proporciona una política del sistema predeterminada, pero debe aplicarse a cualquier dispositivo administrado.

Paso 4: Aplicación de la política de estado

La política de estado se utiliza para configurar cómo los dispositivos administrados informan de su estado de salud al FireSIGHT Management Center. Para configurar o aplicar la política de estado, vaya a **Health > Health Policy**. Se proporciona una política de estado predeterminada, pero debe aplicarse a cualquier dispositivo administrado.

Paso 5: Registrar dispositivos gestionados

Si no registró los dispositivos durante la página de configuración inicial, lea [este documento](#) para obtener instrucciones sobre cómo registrar un dispositivo en FireSIGHT Management Center.

Paso 6: Habilitar licencias instaladas

Antes de poder utilizar cualquier licencia de función del dispositivo, debe habilitarla para cada dispositivo administrado.

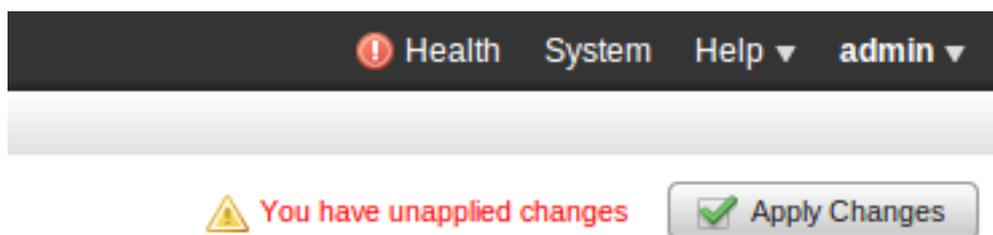
1. Vaya a la página siguiente: **Dispositivos > Administración de dispositivos**.
2. Haga clic en el dispositivo para el que desea habilitar las licencias e introduzca la ficha Dispositivo.
3. Haga clic en el icono **Edit (lápiz)** situado junto a License.

License

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

Habilite las licencias necesarias para este dispositivo y haga clic en **Guardar**.

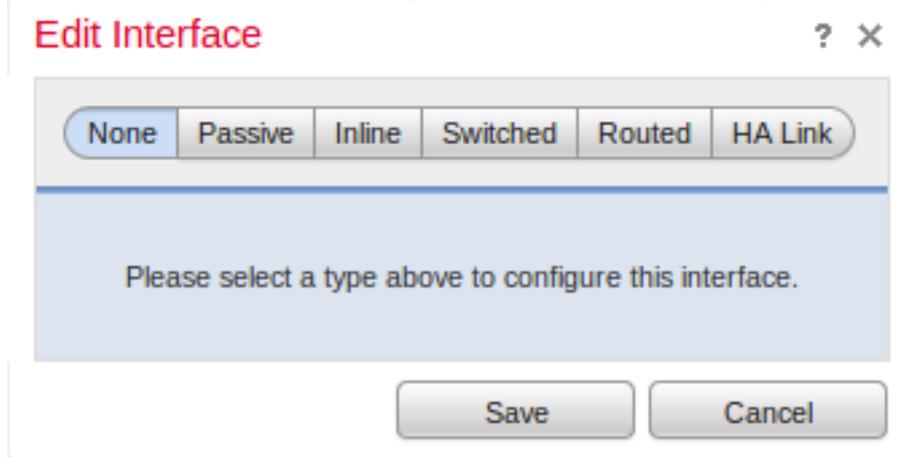
Observe el mensaje "*Tiene cambios no aplicados*" en la esquina superior derecha. Esta advertencia permanece activa incluso si se desplaza de la página de administración de dispositivos hasta que haga clic en el botón **Aplicar cambios**.



Paso 7: Configurar interfaces de detección

1. Navegue a la siguiente página **Dispositivos > Administración de dispositivos**.
2. Haga clic en el icono **Editar** (lápiz) del sensor que desee.

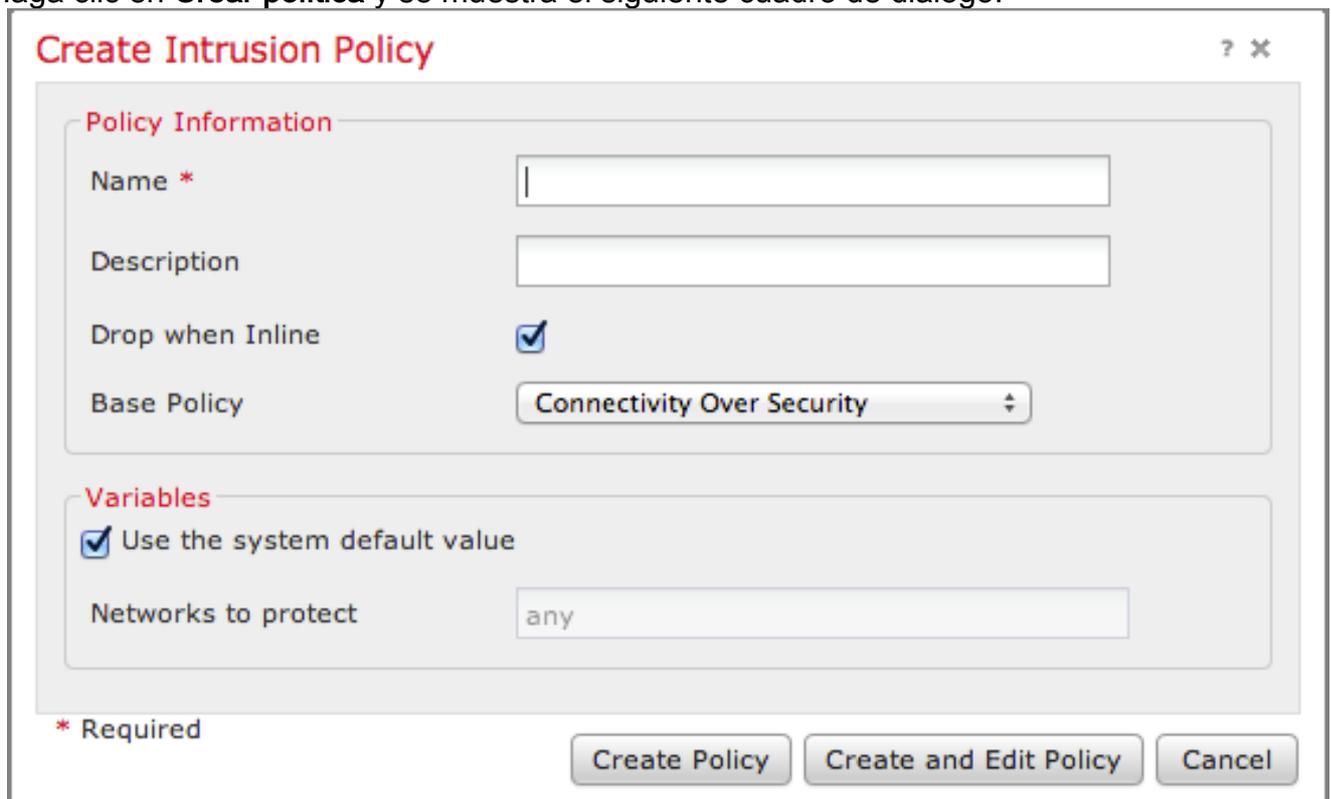
3. En la pestaña **Interfaces**, haga clic en el icono **Editar** para la interfaz que elija.



Seleccione una configuración de interfaz pasiva o en línea. Las interfaces conmutadas y enrutadas están fuera del alcance de este artículo.

Paso 8: Configuración de la política de intrusiones

- Navegue a la página siguiente: **Políticas > Intrusión > Política de intrusiones**.
- Haga clic en **Crear política** y se muestra el siguiente cuadro de diálogo:



Debe asignar un nombre y definir la política base que se utilizará. Dependiendo de su implementación, puede optar por la opción **Drop when Inline** enabled. Defina las redes que desea proteger para reducir los falsos positivos y mejorar el rendimiento del sistema.

Al hacer clic en **Crear política** se guardarán los parámetros y se creará la política IPS. Si desea realizar alguna modificación en la política de intrusiones, puede elegir **Crear y editar política** en su

lugar.

Nota: Las políticas de intrusiones se aplican como parte de la política de control de acceso. Después de aplicar una directiva de intrusión, cualquier modificación se puede aplicar sin volver a aplicar la política de control de acceso completa haciendo clic en el botón **Volver a aplicar**.

Paso 9: Configurar y aplicar una política de control de acceso

1. Vaya a **Políticas > Control de acceso**.
2. Haga clic en **Nueva política**.

New Access Control Policy ? X

Name:

Description:

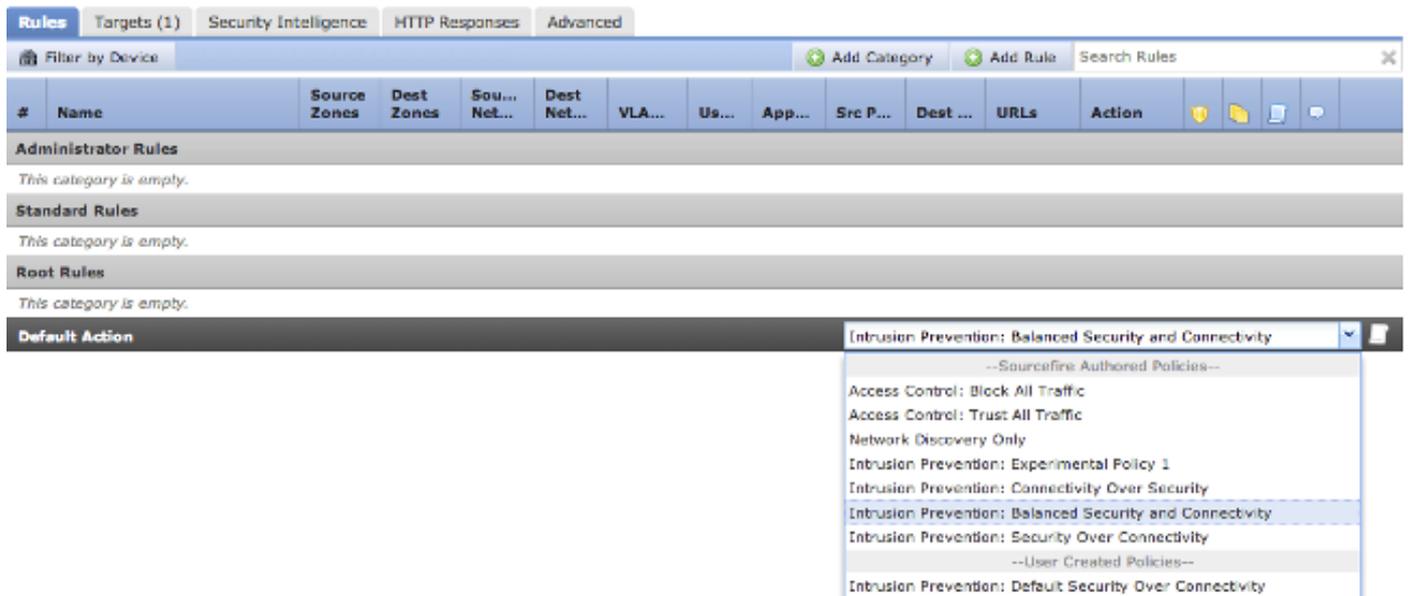
Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

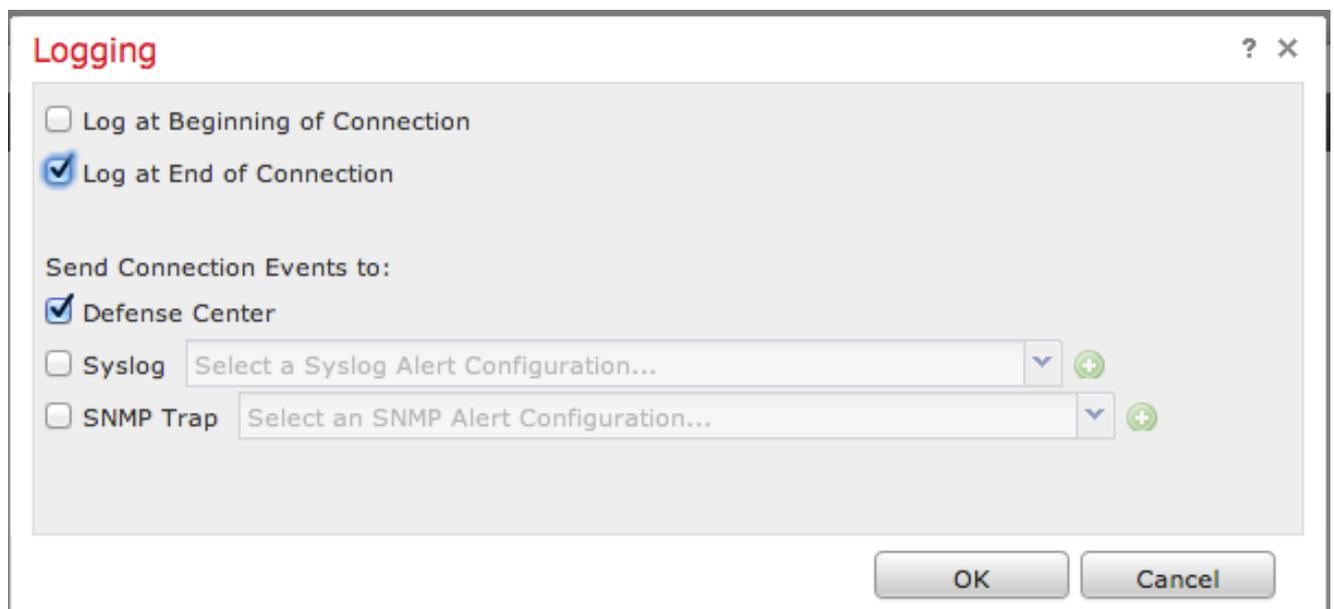
Available Devices

Selected Devices

3. Proporcione un **Nombre** para la política y una **Descripción**.
4. Seleccione **Prevención de intrusiones** como **Acción predeterminada** de la política de control de acceso.
5. Por último, seleccione los **Dispositivos objetivo** a los que desea aplicar la política de control de acceso y haga clic en **Guardar**.
6. Seleccione la política de intrusiones para la acción predeterminada.



7. El registro de la conexión debe estar habilitado para generar eventos de conexión. Haga clic en el menú desplegable que se encuentra a la derecha de la **Acción predeterminada**.



8. Seleccione esta opción para registrar las conexiones al principio o al final de la conexión. Los eventos se pueden registrar en el FireSIGHT Management Center, una ubicación de syslog o a través de SNMP.

Nota: No se recomienda iniciar sesión en ambos extremos de la conexión porque cada conexión (excepto las conexiones bloqueadas) se registrará dos veces. El registro al principio es útil para las conexiones que se bloquearán y el registro al final es útil para el resto de conexiones.

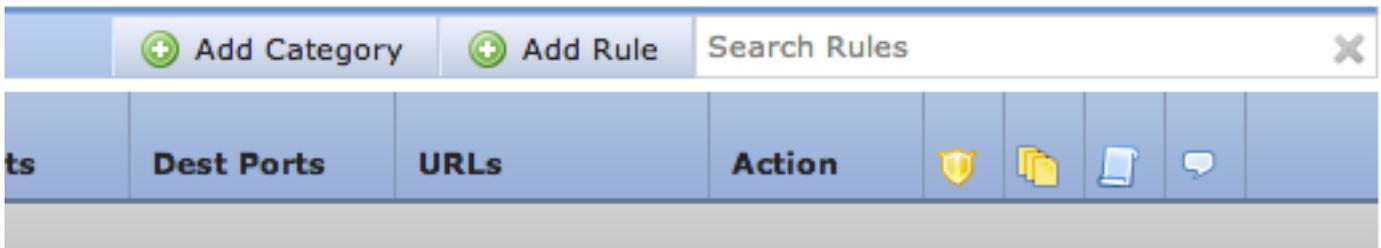
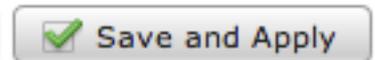
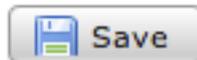
9. Click OK. Tenga en cuenta que el color del icono de registro ha cambiado.

10. Puede agregar una **regla de control de acceso** en este momento. Las opciones que puede utilizar dependen del tipo de licencias que haya instalado.

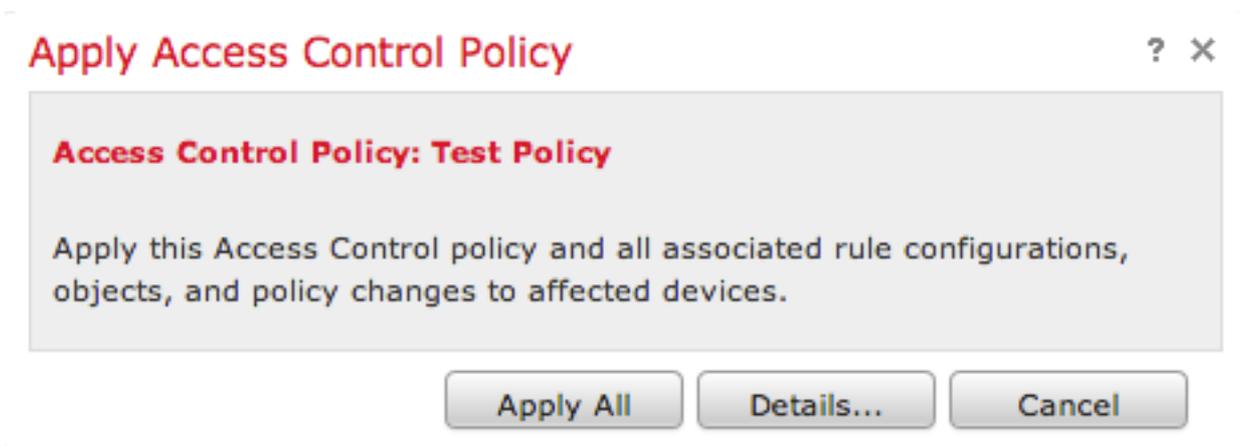
11. Cuando haya terminado de realizar cambios, haga clic en el botón **Guardar y aplicar**.

Aparecerá un mensaje que indica que ha realizado cambios sin guardar en la directiva en la esquina superior derecha hasta que se haya hecho clic en el botón.

You have unsaved changes



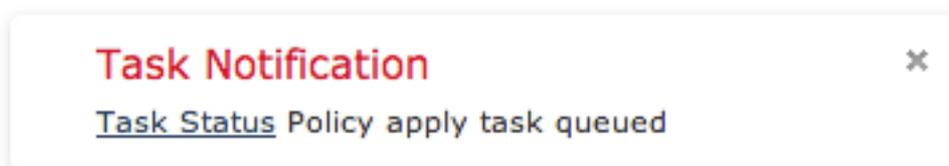
Sólo puede elegir **Guardar** los cambios o hacer clic en **Guardar y aplicar**. Aparecerá la siguiente ventana si elige la segunda.



12. **Aplicar todo** aplicará la política de control de acceso y cualquier política de intrusión asociada a los dispositivos de destino.

Nota: Si se aplica una política de intrusiones por primera vez, no se puede anular la selección.

13. Puede supervisar el estado de la tarea haciendo clic en el enlace **Estado de la tarea** en la notificación que se muestra en la parte superior de la página, o bien navegar hasta: **System > Monitoring > Task Status**



14. Haga clic en el enlace Estado de la tarea para supervisar el progreso de la política de control de acceso aplicada.

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 FireSIGHT Management Center recibe eventos

Una vez que se haya completado la aplicación de la política de control de acceso, debería empezar a ver los eventos de conexión y dependiendo de los eventos de intrusión de tráfico.

Recomendación adicional

También puede configurar las siguientes funciones adicionales en su sistema. Consulte la guía del usuario para obtener más información sobre la implementación.

- Copias de seguridad programadas
- Actualizaciones automáticas de software, SRU, VDB e instalaciones GeoLocation.
- Autenticación externa a través de LDAP o RADIUS