Pasos de la configuración inicial de los sistemas de FireSIGHT

Contenido

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.

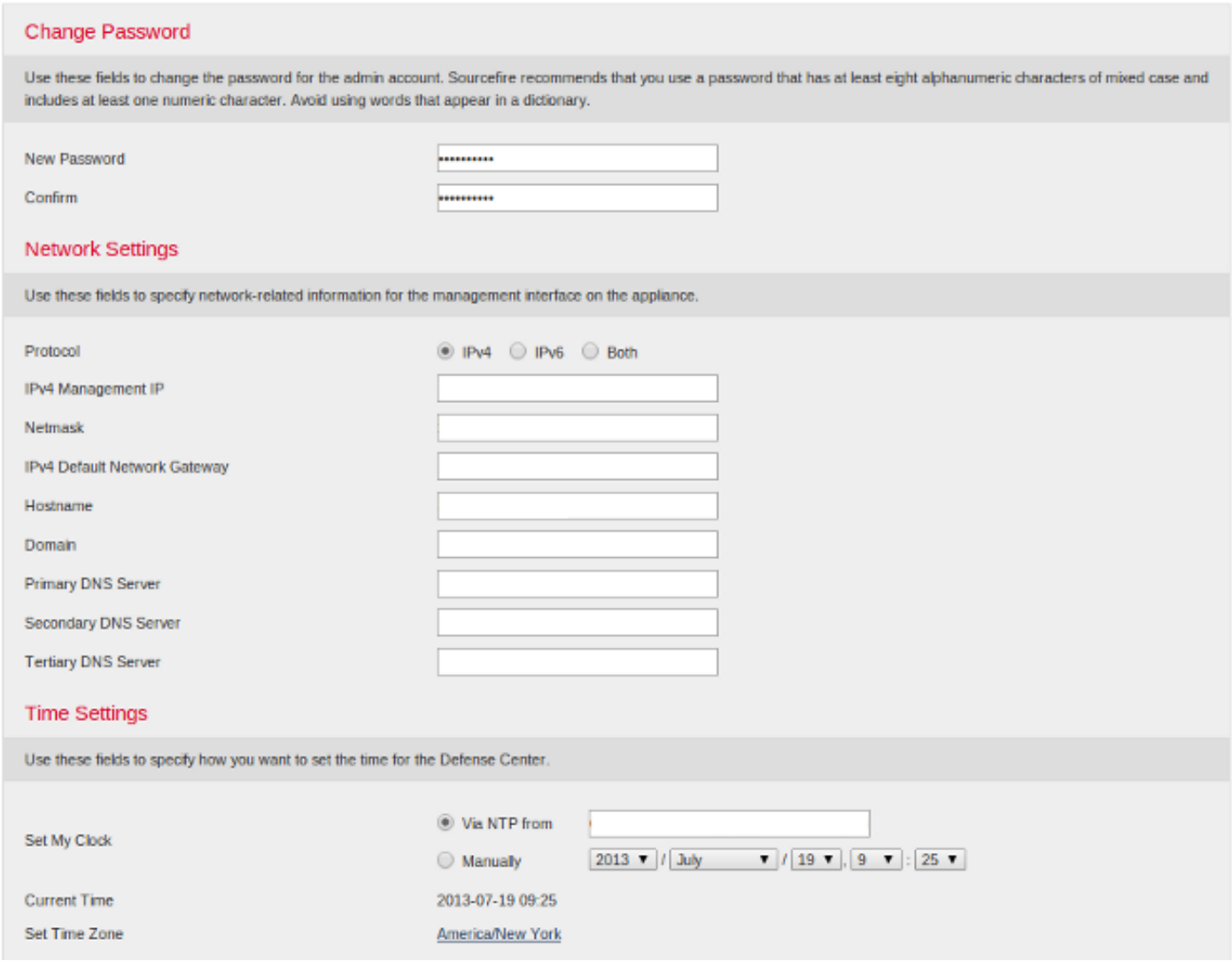
Requisito previo

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

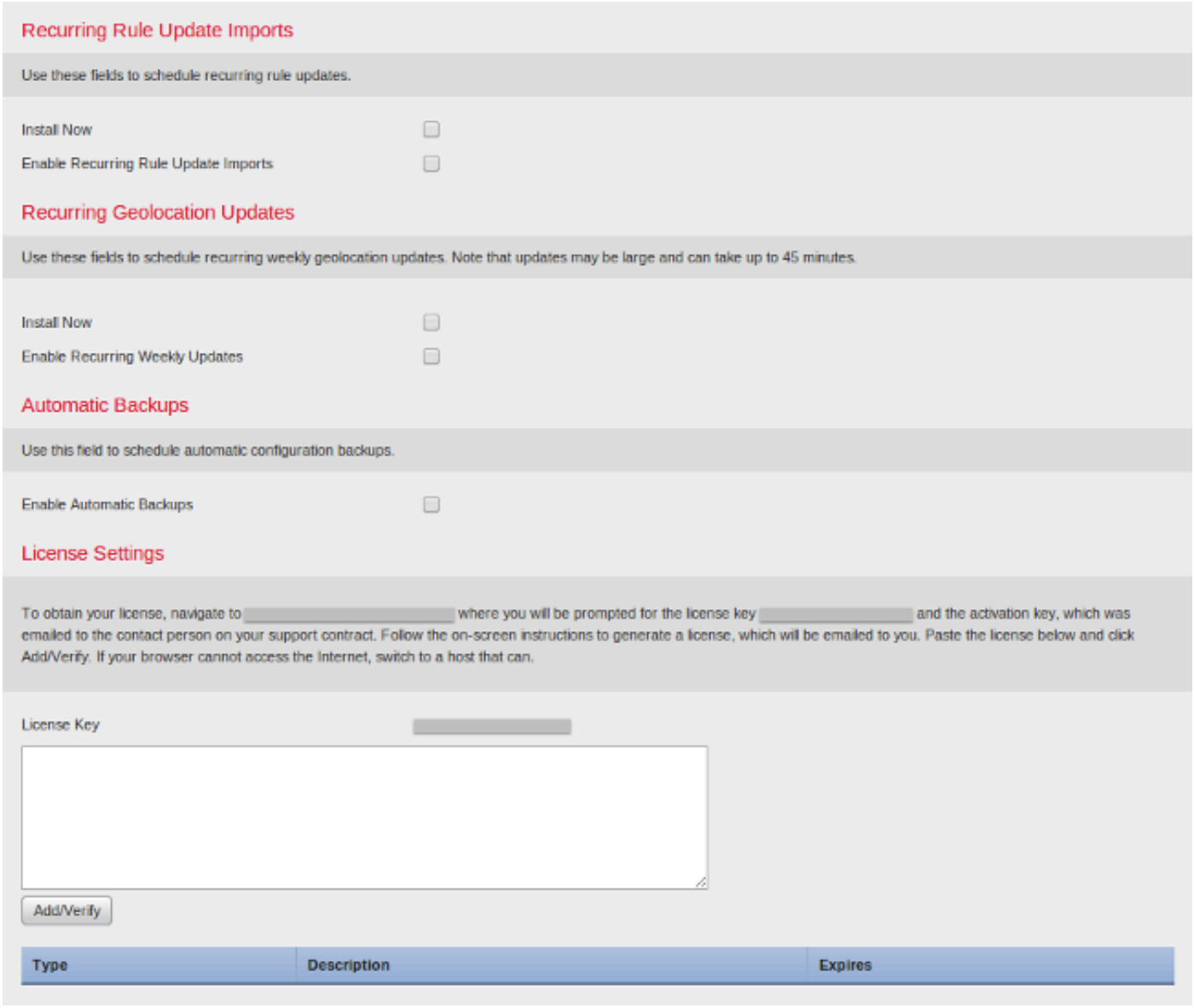
Configuración

Paso 1: Configuración inicial

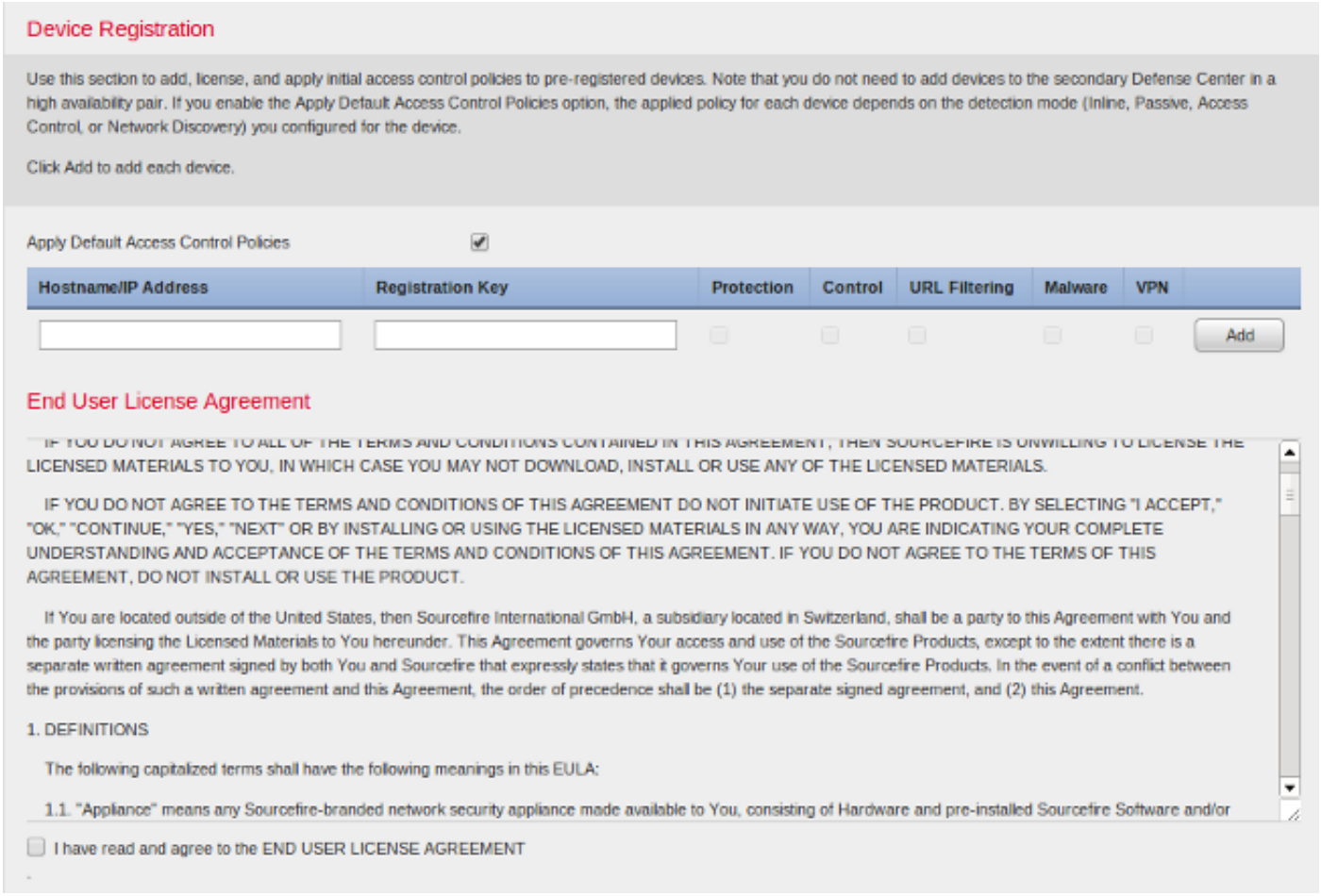
En su centro de administración de FireSIGHT, usted debe completar el proceso de configuración registrando en la interfaz Web y especificando las opciones de configuración inicial en la página de configuración, representada abajo. En esta página, usted debe cambiar la clave del administrador, y puede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



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.



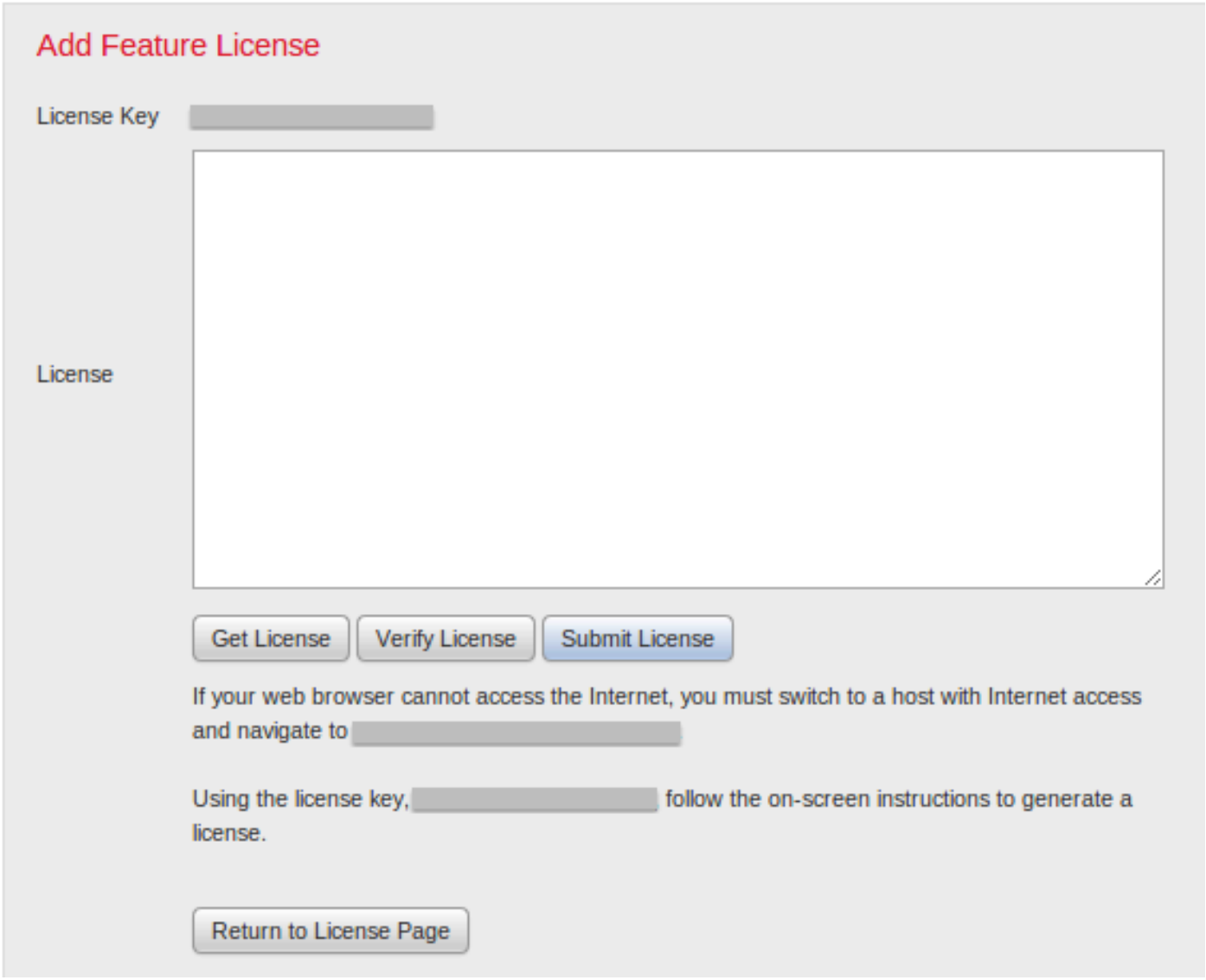
En esta página, usted puede también registrar un dispositivo al centro de administración de FireSIGHT y especificar a un modo de detección. El modo de detección y las otras opciones que usted elige durante el registro determinan las interfaces predeterminadas, los conjuntos en línea, y las zonas que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



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 **agregan la nueva licencia**.



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.

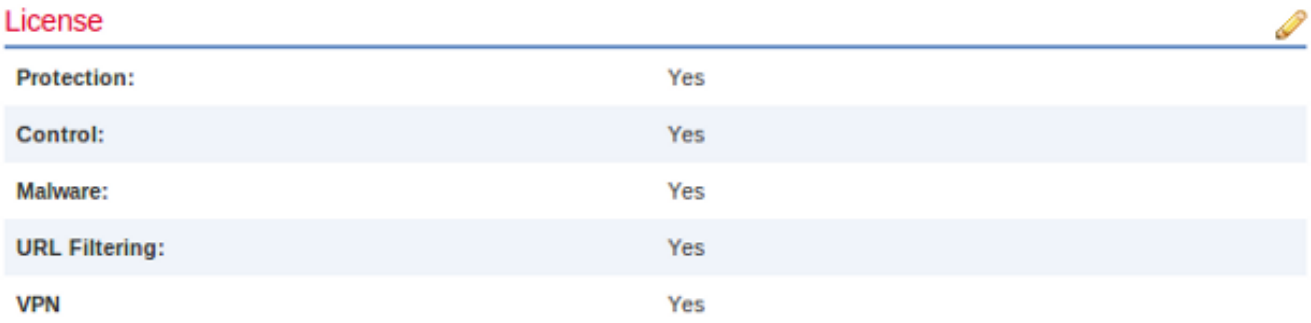
Paso 5: Dispositivos administrados del registro

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

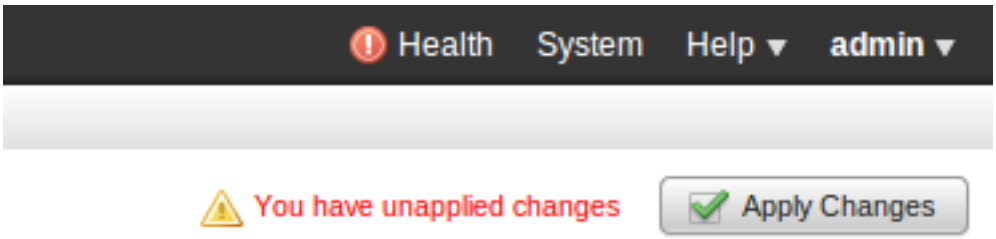
Antes de que usted pueda utilizar cualquier licencia de función en su dispositivo, usted necesita habilitarlo para cada dispositivo administrado.

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 lengueta del dispositivo.
3. Haga clic el **editar** (icono del *lápiz*) al lado de la licencia.



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

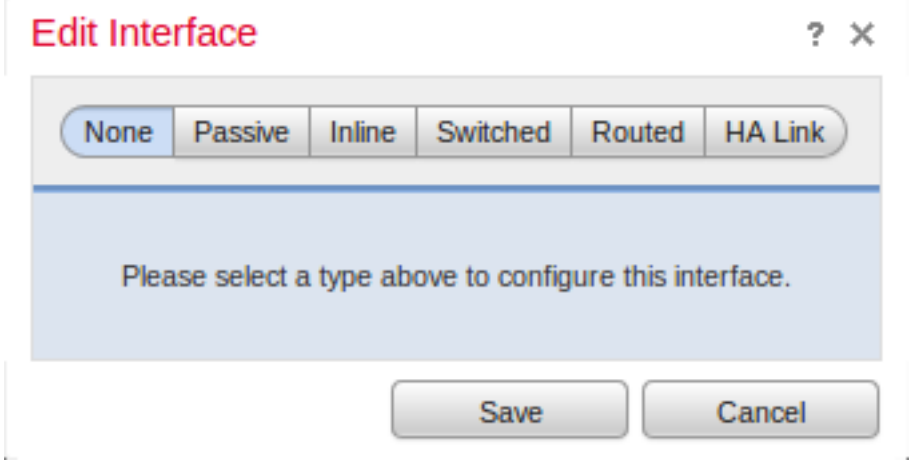
Note el mensaje "*usted para tener cambios inaplicados*" en la esquina superior derecha. Esta advertencia sigue siendo activa incluso si usted navega lejos de la página de la Administración de dispositivos hasta que usted haga clic el botón de los **cambios de la aplicación**.



Paso 7: Configuración que detecta las interfaces

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

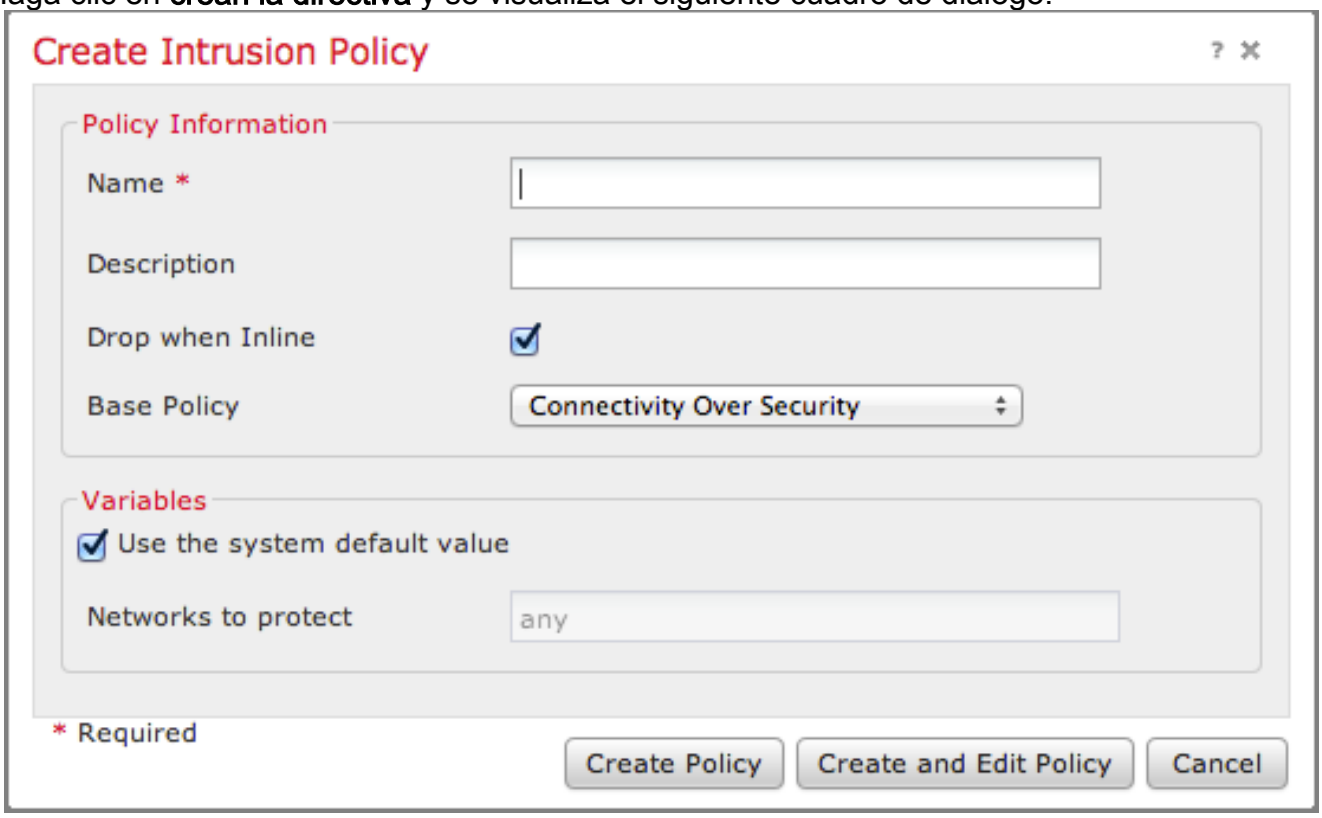
2. Haga clic el icono del **editar** (lápiz) para el sensor de su opción.
3. Bajo **interfaces** tabule, haga clic el icono del **editar** para la interfaz de su opción.



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.

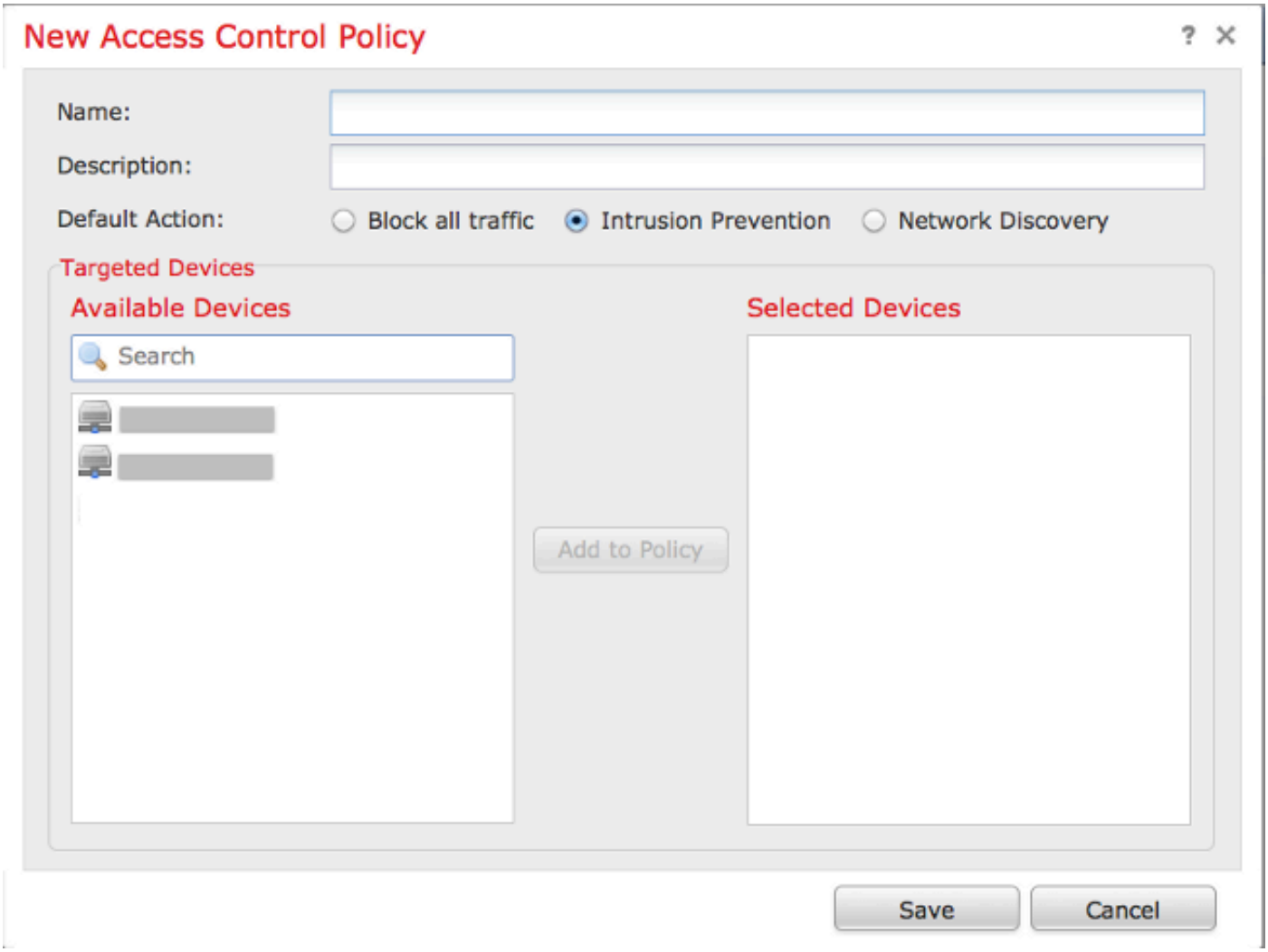
El hacer clic en **crea la directiva** salvará sus configuraciones y creará la directiva IPS. Si usted quiere hacer alguna modificación a la directiva de la intrusión, usted puede elegir **crea y edita la directiva** en lugar de otro.

> **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**.

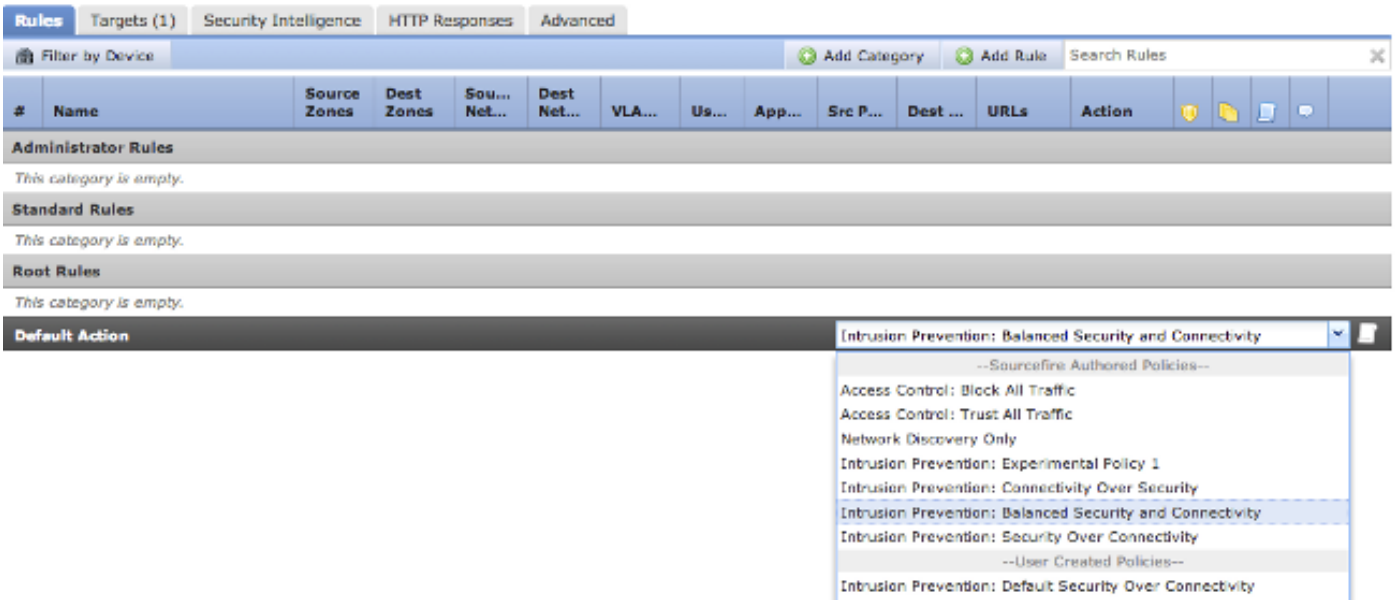


3. Proporcione un **nombre** para la directiva y una **descripción**.

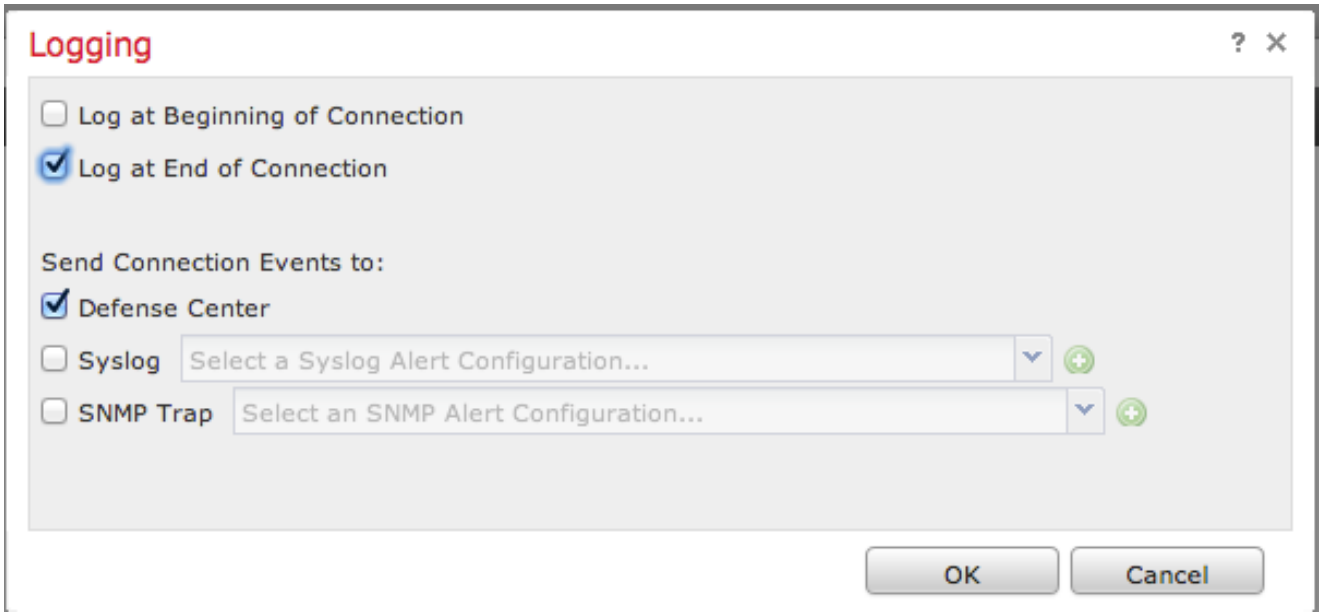
4. Seleccione la **prevención de intrusiones** como la **acción predeterminada de la** directiva del control de acceso.

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.

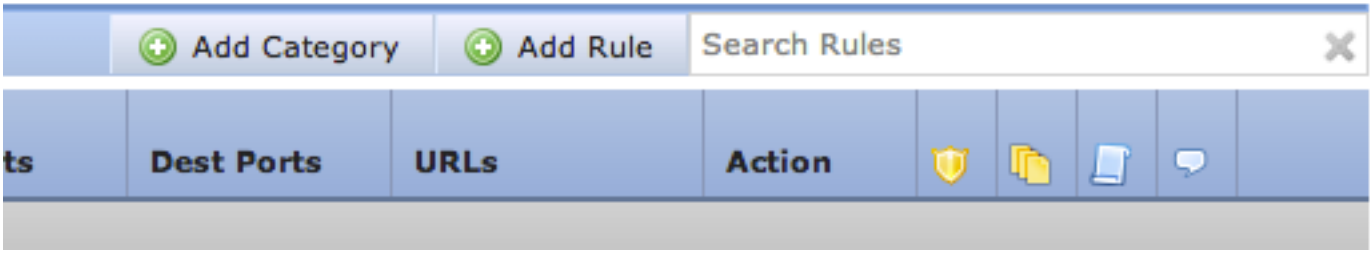
> **Note**: No se recomienda para registrar en los ambos extremos de la conexión porque cada conexión (excepto las conexiones bloqueadas) será registrada dos veces. La registración al principio es útil para las conexiones que serán bloqueadas, y el registro en el extremo es útil para el resto de las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

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

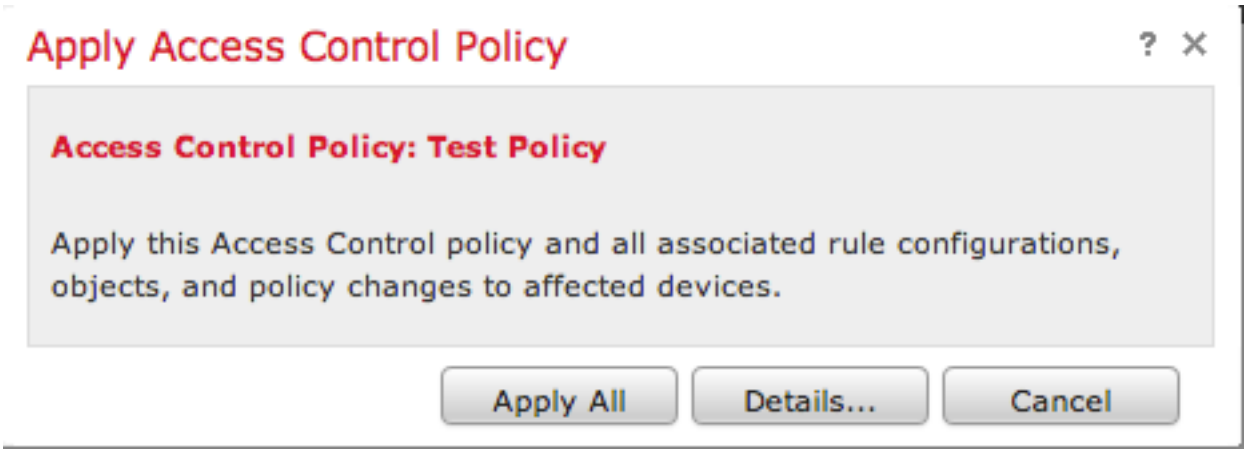
10. Usted puede agregar una **regla del control de acceso** ahora. Las opciones que usted puede utilizar dependen del tipo de licencias usted ha instalado.

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.



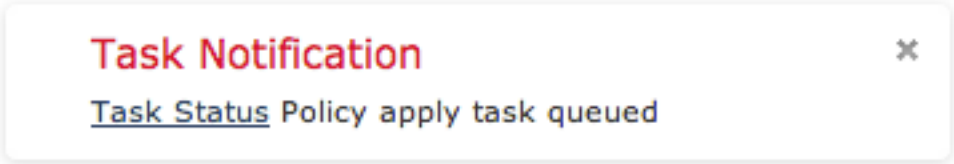
Usted puede elegir **salvar** solamente los cambios o hacer clic en la **salvaguardia y aplicarse**. La ventana siguiente aparecerá si usted elige estos últimos.



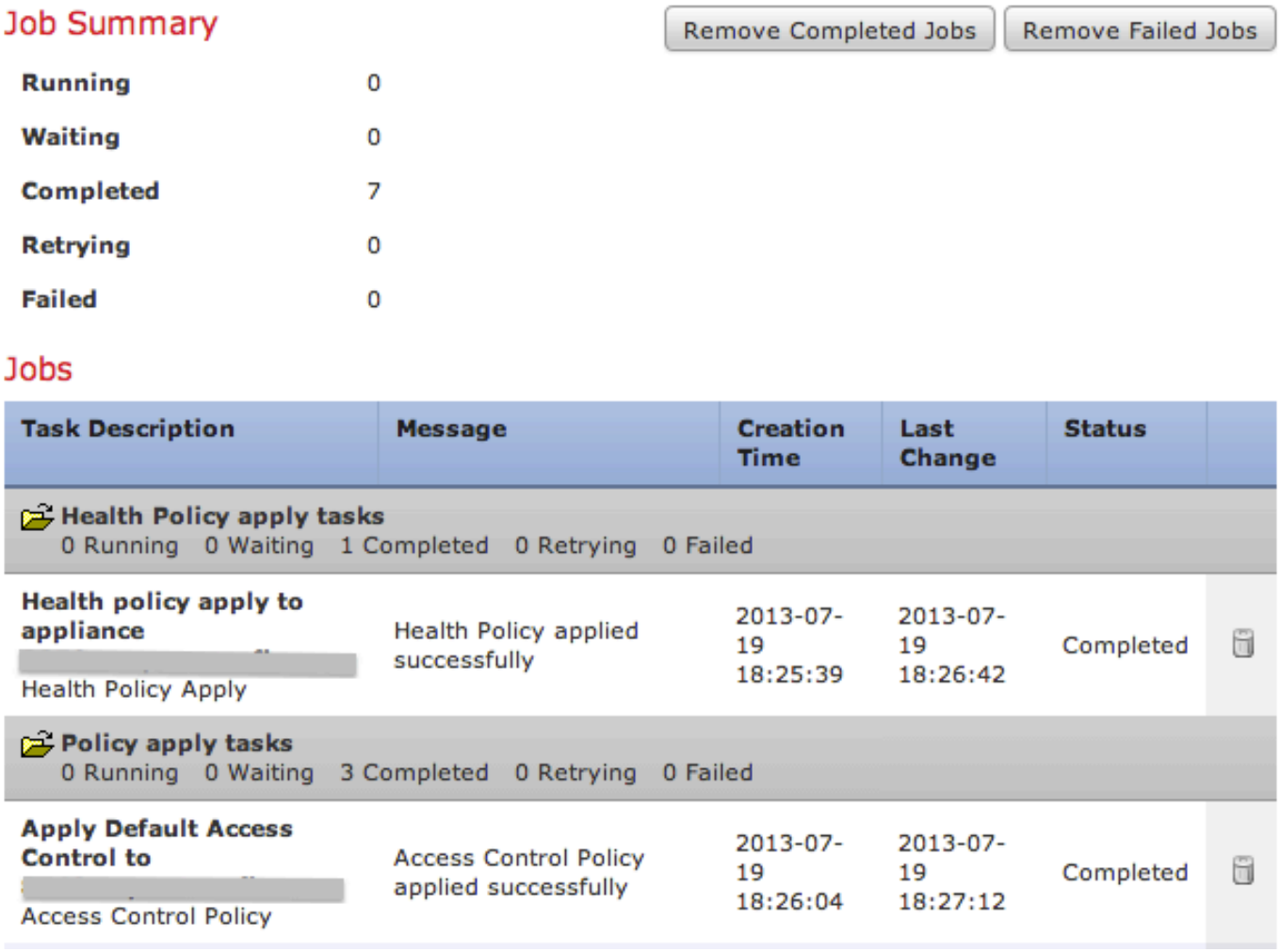
12. **Aplique todos** aplicará la directiva del control de acceso y cualquier directiva asociada de la intrusión a los dispositivos apuntados.

> **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.



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