Etapas da configuração inicial de sistemas de FireSIGHT

Índice

[Introdução](#)
[Pré-requisito](#)
[Configuração](#)
[Passo 1: Instalação inicial](#)
[Passo 2: Instale licenças](#)
[Passo 3: Aplique a política do sistema](#)
[Passo 4: Aplique a política sanitária](#)
[Passo 5: Dispositivos gerenciado do registro](#)
[Passo 6: Permita licenças instaladas](#)
[Etapa 7: Configurar a detecção de relações](#)
[Passo 8: Configurar a política da intrusão](#)
[Etapa 9: Configurar e aplique uma política do controle de acesso](#)
[Etapa 10: Verifique se o centro de gerenciamento de FireSIGHT recebe eventos](#)
[Recomendação adicional](#)

Introdução

Depois que você nova imagem um centro de gerenciamento de FireSIGHT ou um dispositivo de FirePOWER, você precisa de terminar diversas etapas para fazer inteiramente o sistema - funcional e para gerar alertas para eventos da intrusão; como, instalando a licença, registrando os dispositivos, aplicando a política sanitária, a política do sistema, a política do controle de acesso, a política etc. da intrusão. Este original é um suplemento ao guia de instalação de sistema de FireSIGHT.

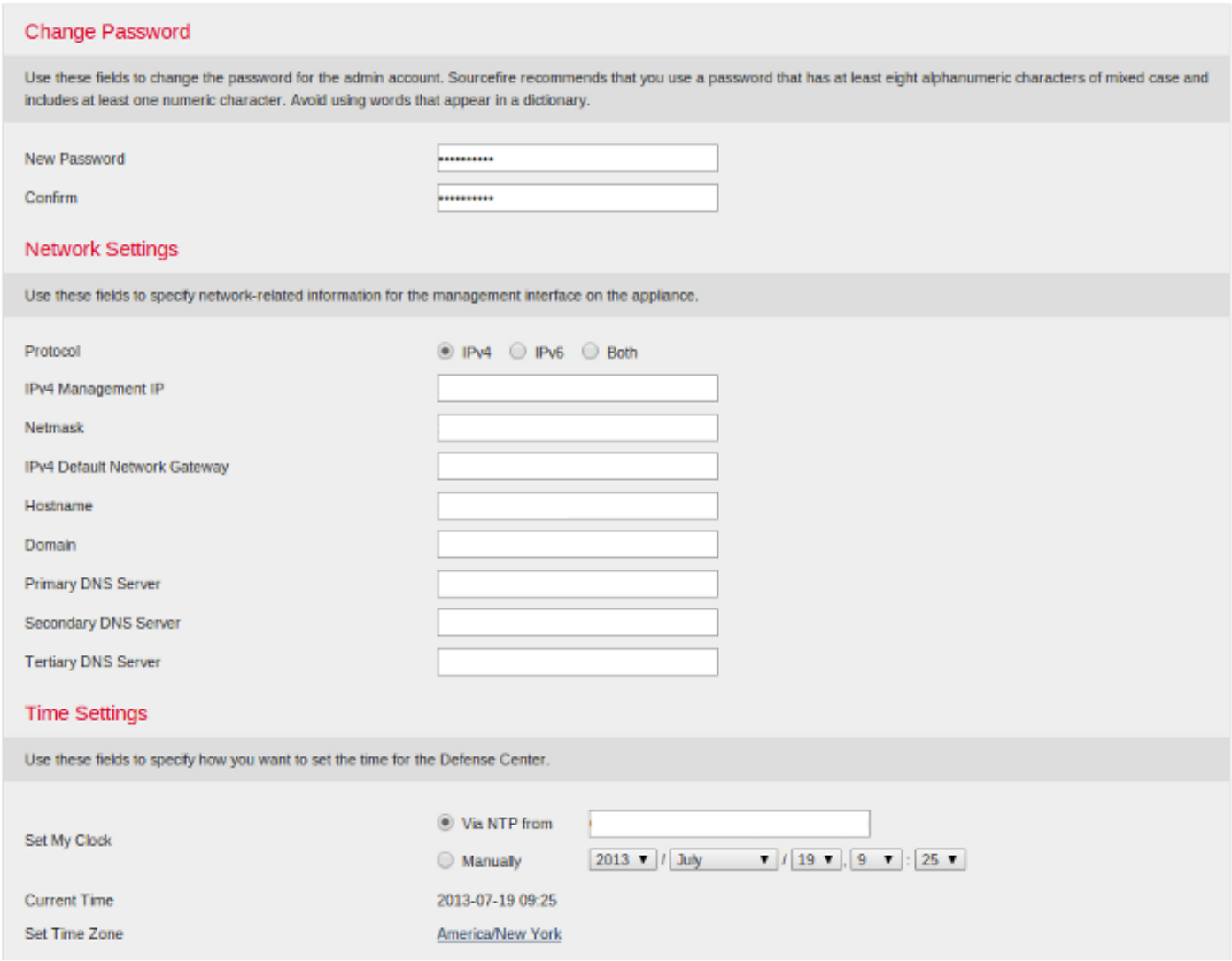
Pré-requisito

Este guia supõe que você leu com cuidado o guia de instalação de sistema de FireSIGHT.

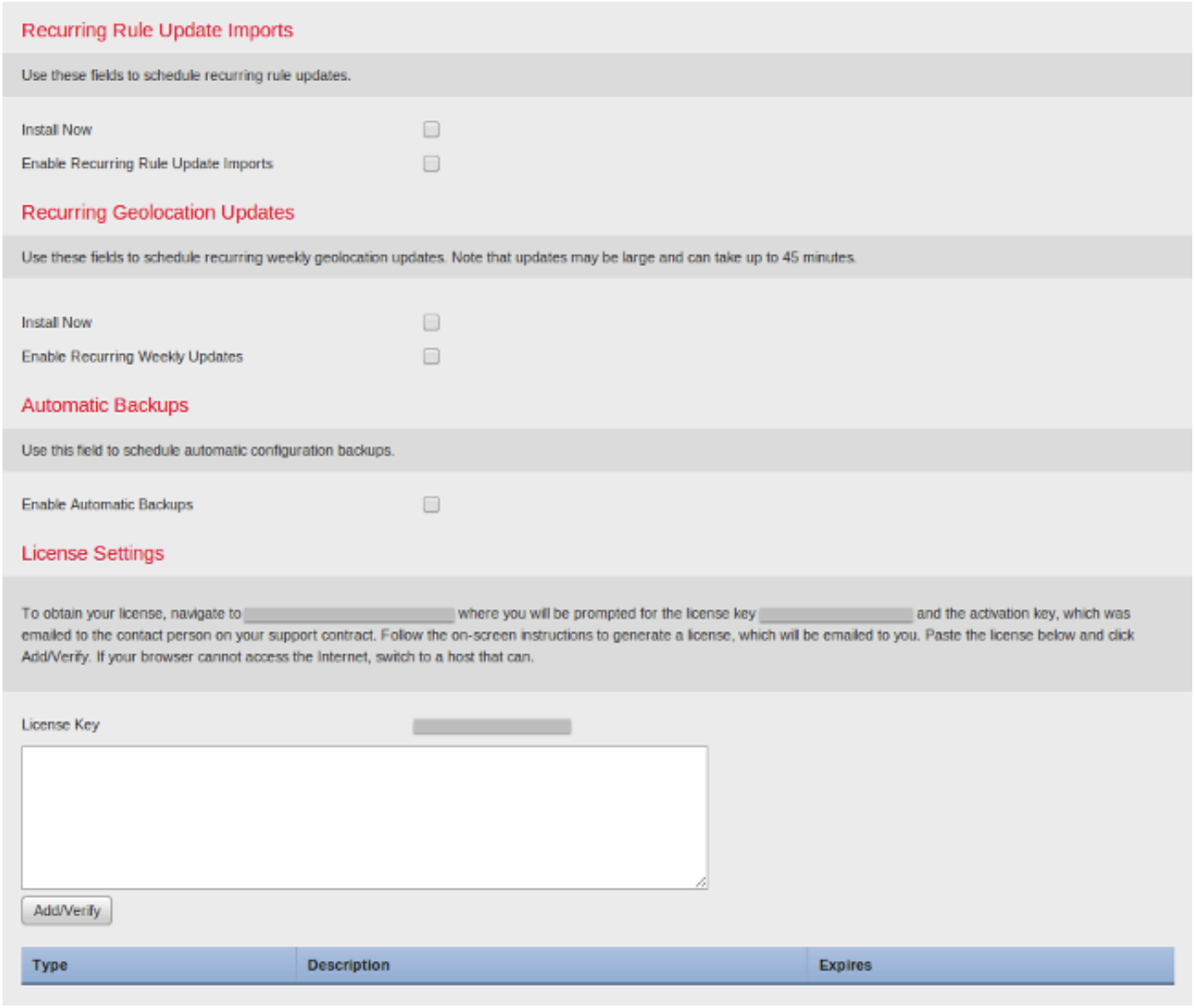
Configuração

Passo 1: Instalação inicial

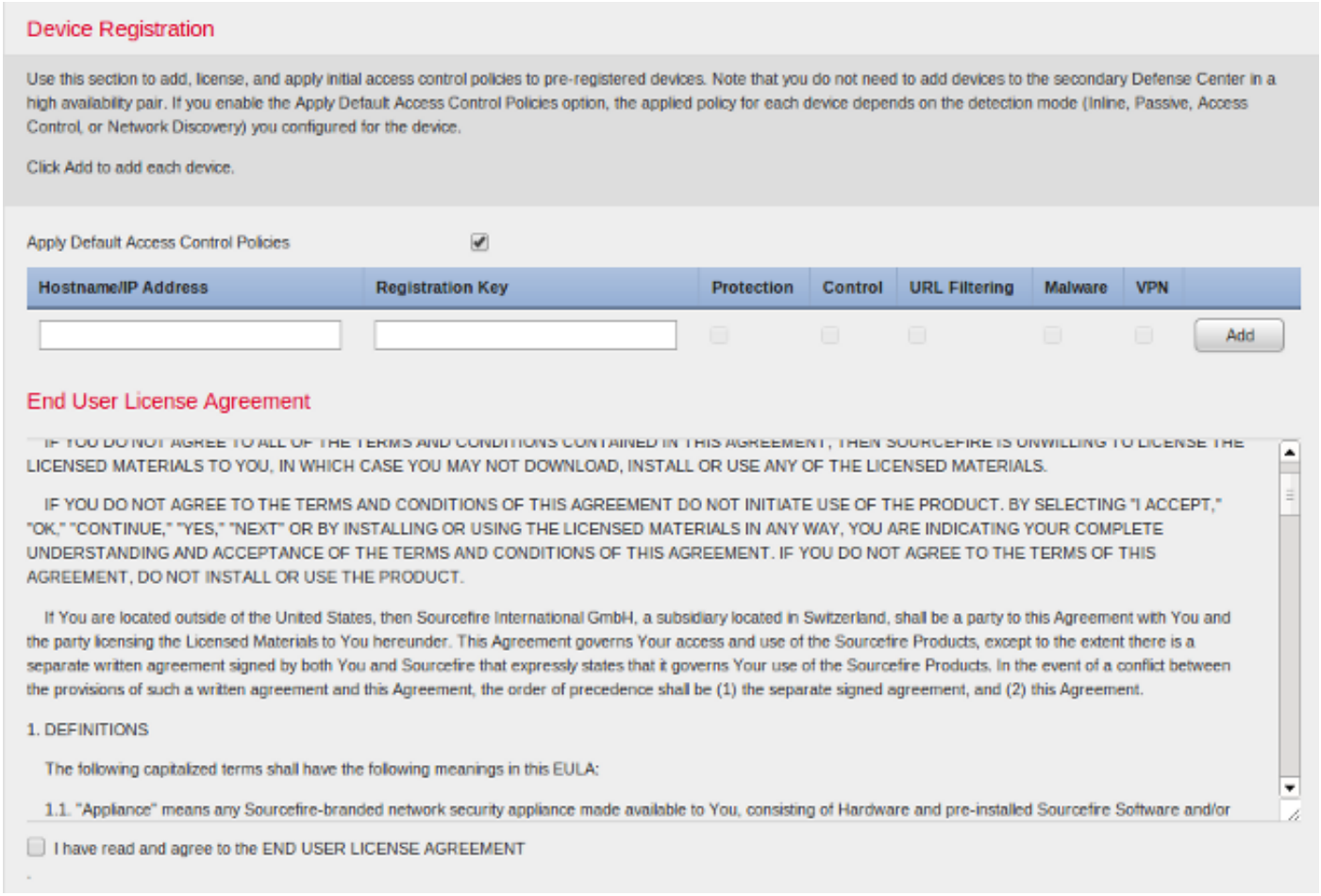
Em seu centro de gerenciamento de FireSIGHT, você deve terminar o processo de instalação registrando na interface da WEB e especificando opções de configuração inicial na página de instalação, descrita abaixo. Nesta página, você deve mudar a senha de admin, e pode igualmente especificar configurações de rede tais como o domínio e os servidores DNS, e a configuração do tempo.



Você pode opcionalmente configurar atualizações de retorno da regra e do geolocation assim como backup automáticos. Todas as licenças de recurso podem igualmente ser instaladas neste momento.



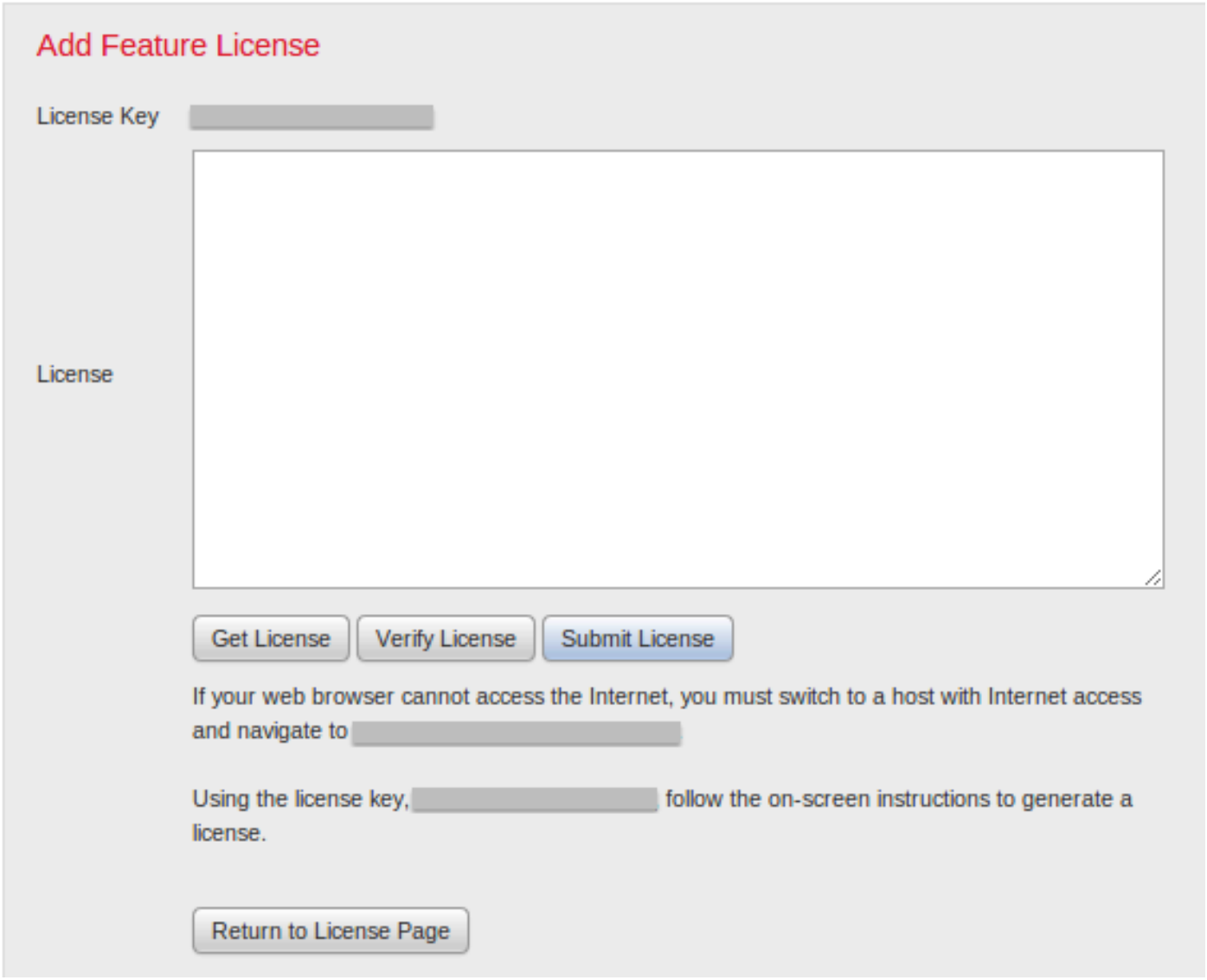
Nesta página, você pode igualmente registrar um dispositivo ao centro de gerenciamento de FireSIGHT e especificar um modo de detecção. O modo de detecção e as outras opções que você escolhe durante o registro determinam as interfaces padrão, os grupos inline, e as zonas que o sistema cria, assim como as políticas que aplicam inicialmente aos dispositivos gerenciado.



Passo 2: Instale licenças

Se você não instalou licenças durante a página de instalação inicial, você pode terminar a tarefa seguindo estas etapas:

- Navegue à seguinte página: **Sistema > licenças**.
- Clique **adicionam** sobre a **licença nova**.



Se você não recebeu uma licença, contacte o representante de vendas de sua conta.

Passo 3: Aplique a política do sistema

A política do sistema especifica a configuração para perfis da autenticação e a sincronização de tempo entre o centro de gerenciamento de FireSIGHT e os dispositivos gerenciado. Para configurar ou aplicar a política do sistema navegue ao **sistema > à política do Local > do sistema**. Uma política do sistema padrão é fornecida mas precisa de ser aplicada a todos os dispositivos gerenciado.

Passo 4: Aplique a política sanitária

A política sanitária é usada para configurar como os dispositivos gerenciado relatam seu estado de saúde ao centro de gerenciamento de FireSIGHT. Para configurar ou aplicar a política sanitária navegue à **saúde > à política sanitária**. Uma política sanitária do padrão é fornecida mas precisa de ser aplicada a todos os dispositivos gerenciado.

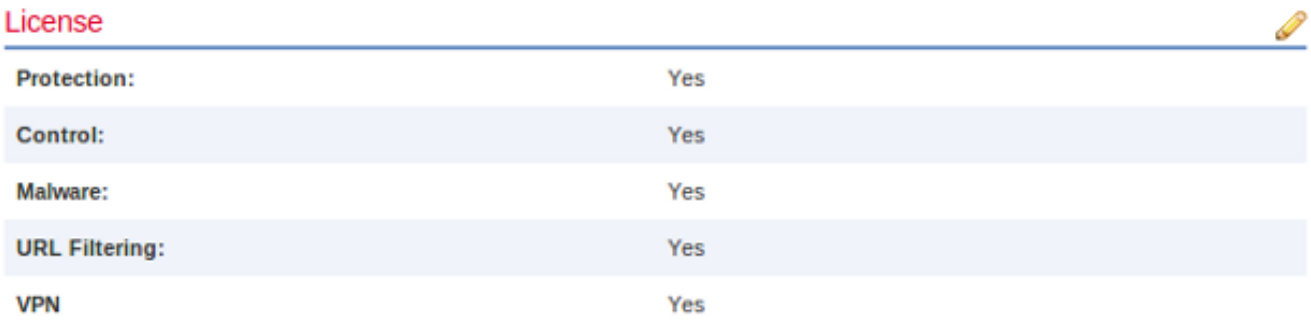
Passo 5: Dispositivos gerenciado do registro

Se você não registrou dispositivos durante a página de instalação inicial, leia este original para instruções em como registrar um dispositivo a um centro de gerenciamento de FireSIGHT.

Passo 6: Permita licenças instaladas

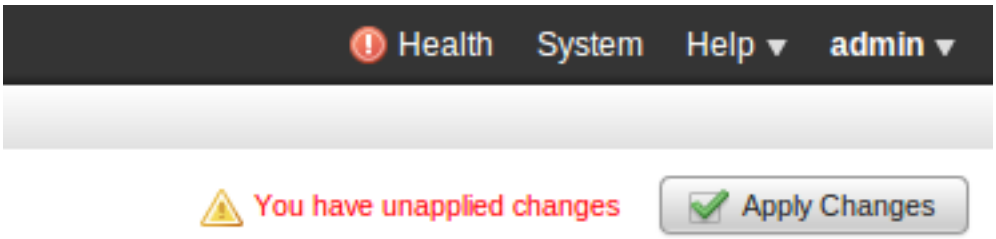
Antes que você possa usar toda a licença de recurso em seu dispositivo, você precisa de permiti-lo para cada dispositivo gerenciado.

1. Navegue à seguinte página: **Dispositivos > Gerenciamento de dispositivos**.
2. Clique sobre o dispositivo para que você quer permitir as licenças e incorpora a aba do dispositivo.
3. Clique a **edição** (ícone do *lápis*) ao lado da licença.



Permita as licenças exigidas para este dispositivo e clique a **salvaguarda**.

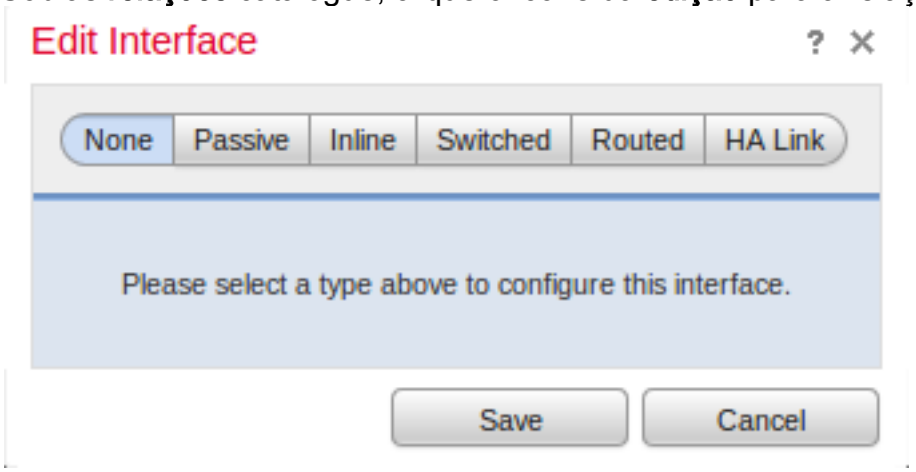
Observe a mensagem "*você para ter mudanças unapplied*" no canto superior direito. Este aviso permanece ativo mesmo se você navega longe da página do Gerenciamento de dispositivos até que você clique o botão das **mudanças da aplicação**.



Etapa 7: Configurar a detecção de relações

1. Navegue aos seguintes **dispositivos > Gerenciamento de dispositivos da** página.
2. Clique o ícone da **edição** (lápis) para o sensor de sua escolha.

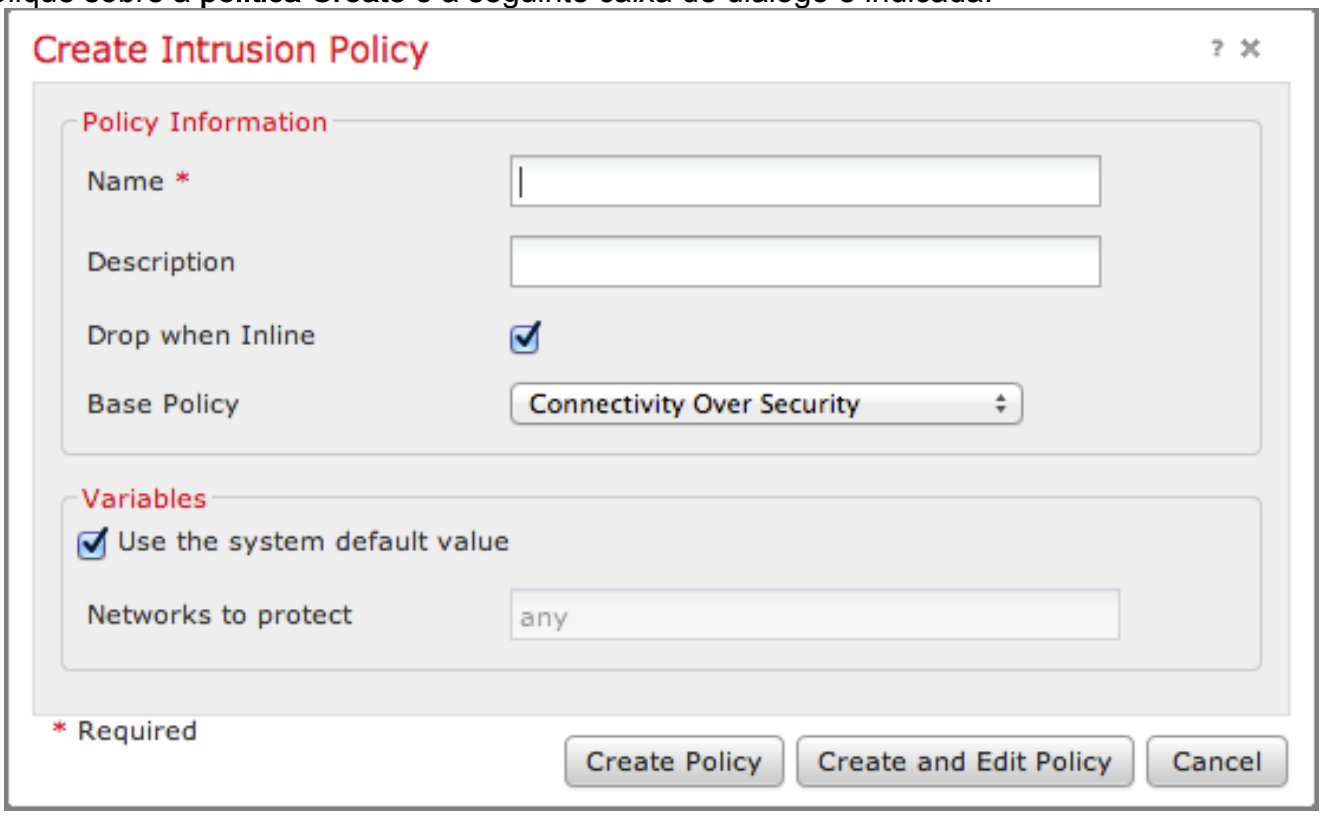
3. Sob as **relações** catalogue, clique o ícone da **edição** para a relação de sua escolha.



Selecione uma configuração da interface passiva ou Inline. Comutado e as interfaces roteada são além do alcance deste artigo.

Passo 8: Configurar a política da intrusão

- Navegue à seguinte página: **Políticas > intrusão > política da intrusão.**
- Clique sobre a **política Create** e a seguinte caixa de diálogo é indicada:



Você deve atribuir um nome e definir a política baixa a ser usada. Segundo seu desenvolvimento que você pode escolheu ter a **gota da** opção **quando** permitido **Inline**. Defina as redes que você quer proteger para reduzir falsos positivos e melhorar o desempenho do sistema.

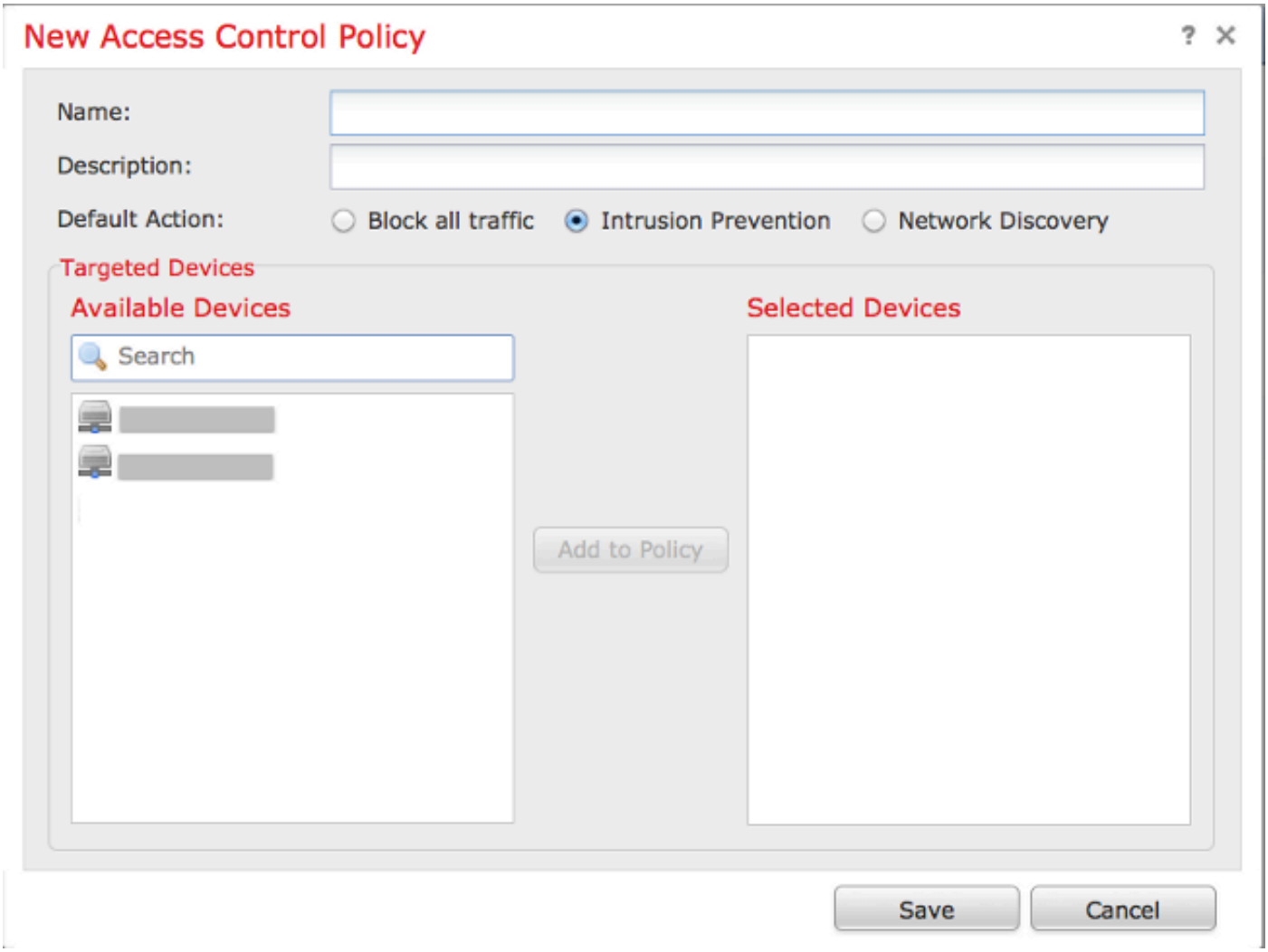
Clicar na **política Create** salvar seus ajustes e criará a política IPS. Se você quer fazer alguma alteração à política da intrusão, você pode escolher **cria e edita a política** pelo contrário.

Nota: As políticas da intrusão são aplicadas como parte da política do controle de acesso. Depois que uma política da intrusão é aplicada, todas as alterações podem ser aplicadas sem reaplicar a política inteira do controle de acesso clicando o botão **reaplicar**.

Etapa 9: Configurar e aplique uma política do controle de acesso

1. Navegue às **políticas > ao controle de acesso**.

2. Clique sobre a **política nova**.

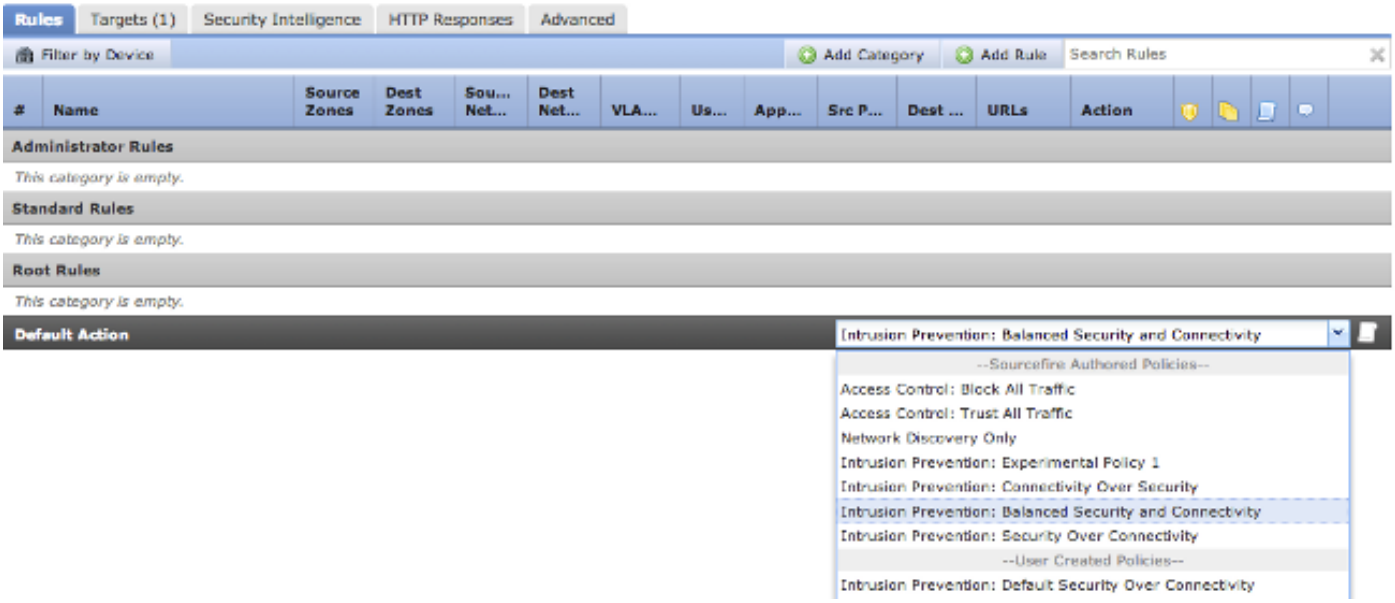


3. Forneça um **nome** para a política e uma **descrição**.

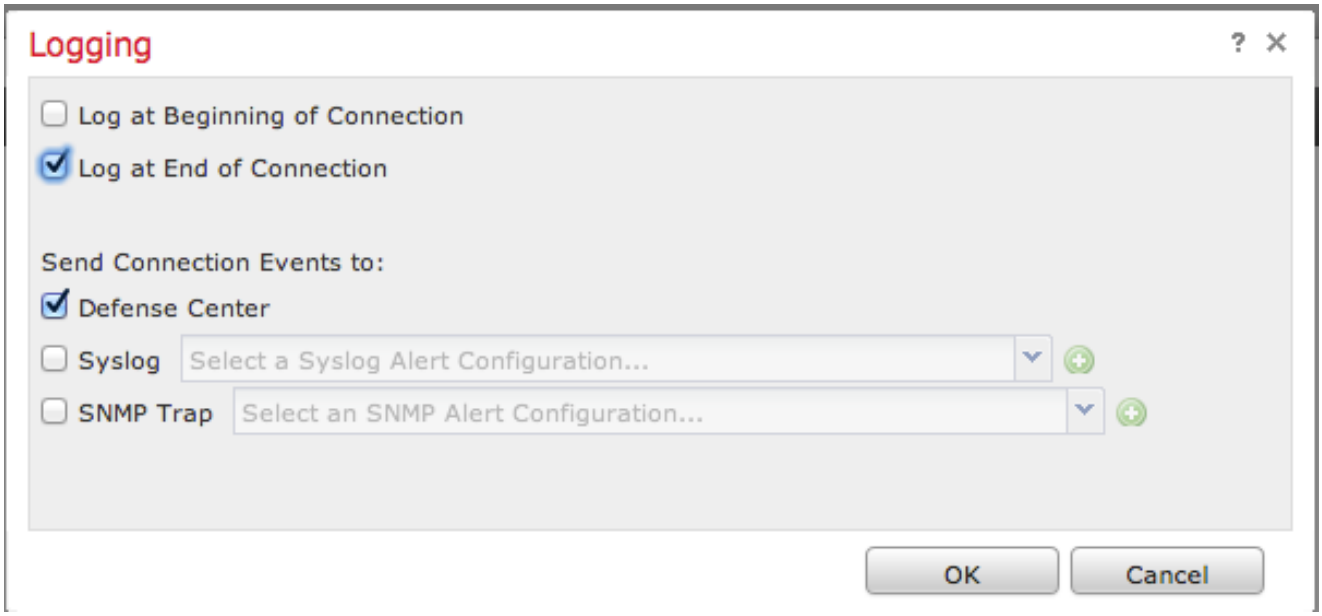
4. Selecione a **prevenção de intrusão** como a **ação padrão da** política do controle de acesso.

5. Selecione finalmente os **dispositivos visados a** que você quer aplicar a política do controle de acesso, e clique a **salvaguarda**.

6. Selecione sua política da intrusão para a ação padrão.



7. O registro da conexão deve ser permitido de gerar eventos de conexão. Clique o menu de gota para baixo que é direito da **ação padrão**.



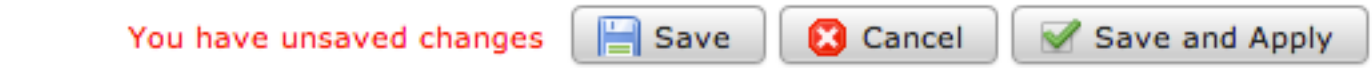
8. Escolha registrar conexões no começo ou na extremidade da conexão. Os eventos podem ser entrados o centro de gerenciamento de FireSIGHT, um lugar do Syslog, ou com o SNMP.

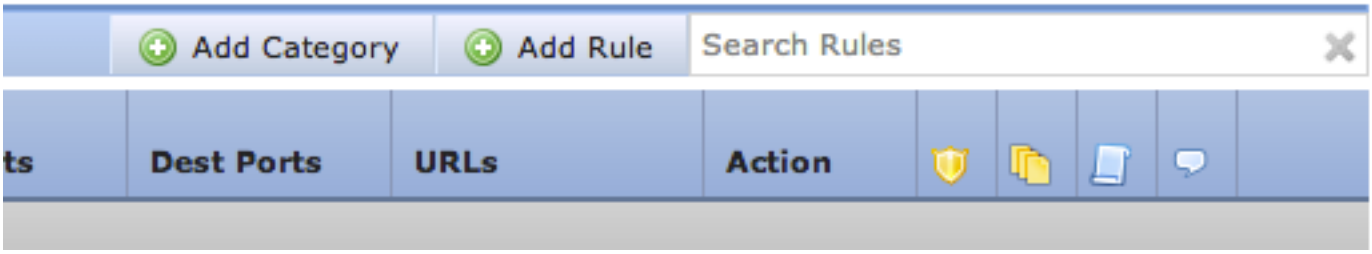
> Nota: Não se recomenda registrar no ambas as extremidades da conexão porque cada conexão (exceto conexões obstruídas) será registrada duas vezes. Registrar no início é útil para as conexões que serão obstruídas, e registrar na extremidade é útil para todas conexões restantes.

9. Clique em **OK**. Note que a cor do ícone de registro mudou.

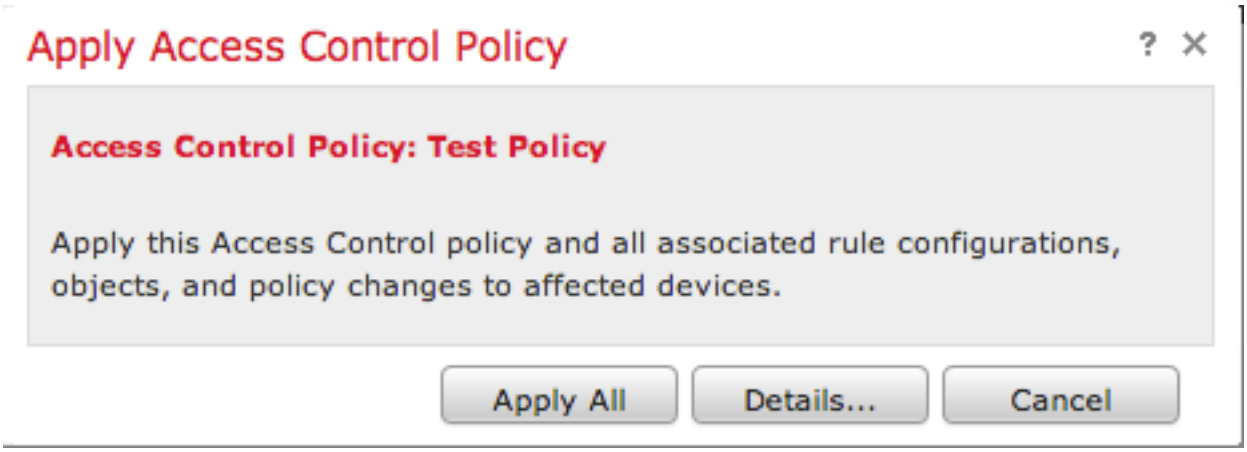
10. Você pode adicionar uma **regra do controle de acesso** neste tempo. As opções que você pode se usar dependem do tipo de licenças você instalou.

11. Quando você é fatura terminada muda. clique a **salvaguarda e o botão Apply Button**. Você observará uma mensagem indicá-lo para ter mudanças unsaved em sua política no canto superior direito até que o botão esteja clicado.





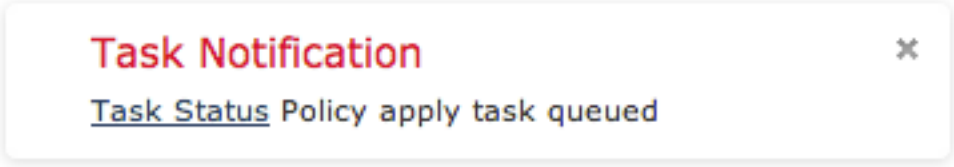
Você pode escolher **salvar** somente as mudanças ou clicar sobre a **salvaguarda e aplicar-se**. o seguinte indicador aparecerá se você escolhe os últimos.



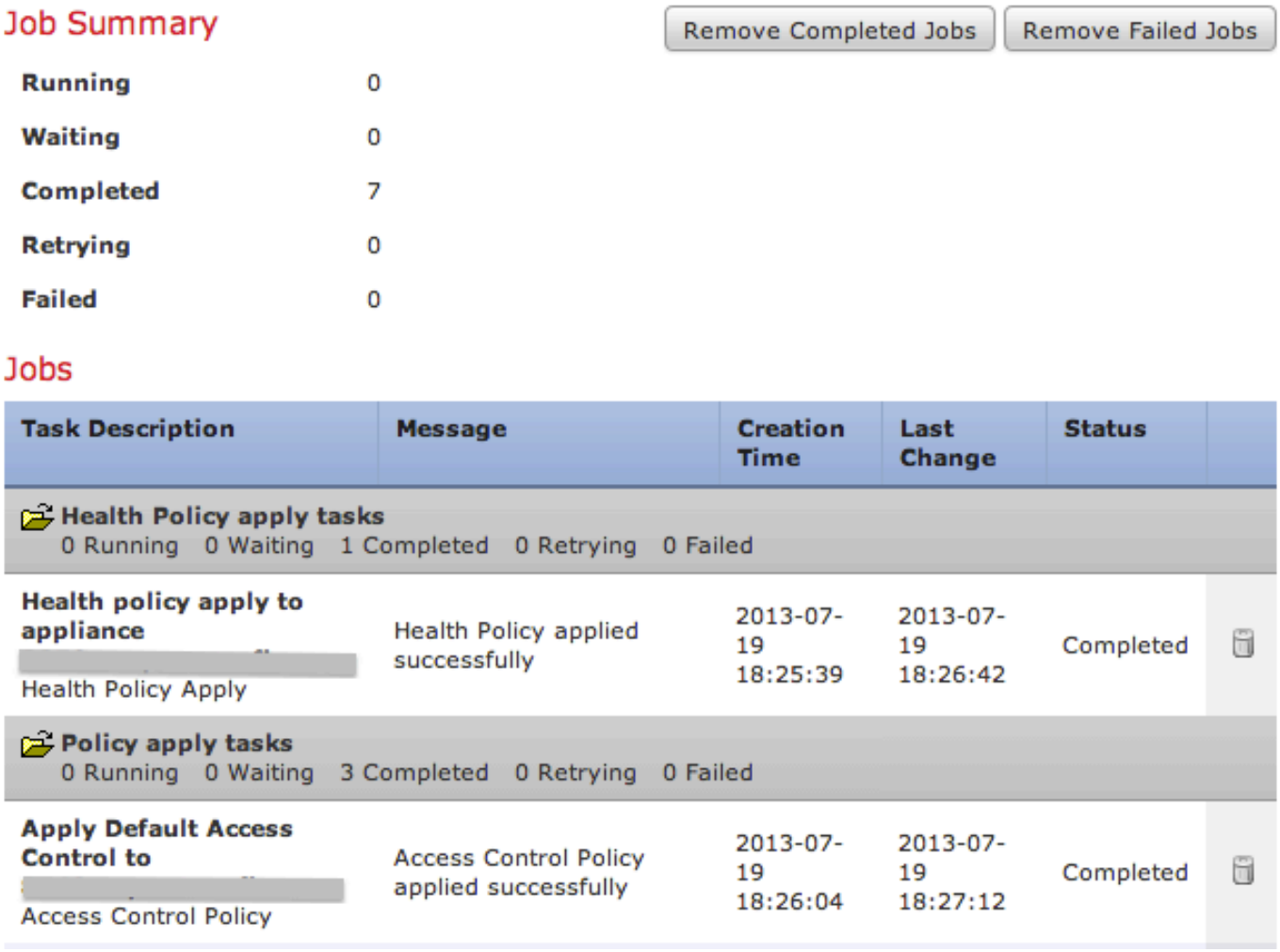
12. **Aplique tudo** aplicará a política do controle de acesso e todas as políticas associadas da intrusão aos dispositivos visados.

Nota: Se uma política da intrusão será aplicada pela primeira vez, não pode ser unselected.

13. Você pode monitorar o estado da tarefa que clica na relação do **estado da tarefa na** notificação mostrada na parte superior da página, ou navegando a: **Estado do sistema > da monitoração > da tarefa**



14. Clique a relação do estado da tarefa para monitorar o progresso da política do controle de acesso aplicam-se.



Etapa 10: Verifique se o centro de gerenciamento de FireSIGHT recebe eventos

Depois que a política do controle de acesso se aplica terminou, você deve começar ver eventos das conexões e segundo eventos da intrusão do tráfego.

Recomendação adicional

Você pode igualmente configurar os seguintes recursos adicionais em seu sistema. Refira por favor o Guia do Usuário para detalhes de implementação.

- Backup agendado
- Atualização de software automática, SRU, VDB, e transferências de GeoLocation/instalações.
- Autenticação externa através do LDAP ou do RAIO