Etapas da configuração inicial dos sistemas FireSIGHT

Contents

Introduction

Depois de recriar um FireSIGHT Management Center ou um dispositivo FirePOWER, você precisa concluir várias etapas para tornar o sistema totalmente funcional e gerar alertas para eventos de intrusão; por exemplo, instalar licença, registrar os dispositivos, aplicar política de saúde, política de sistema, política de controle de acesso, política de intrusão, etc. Este documento é um suplemento do Guia de instalação do sistema FireSIGHT.

Pré-requisito

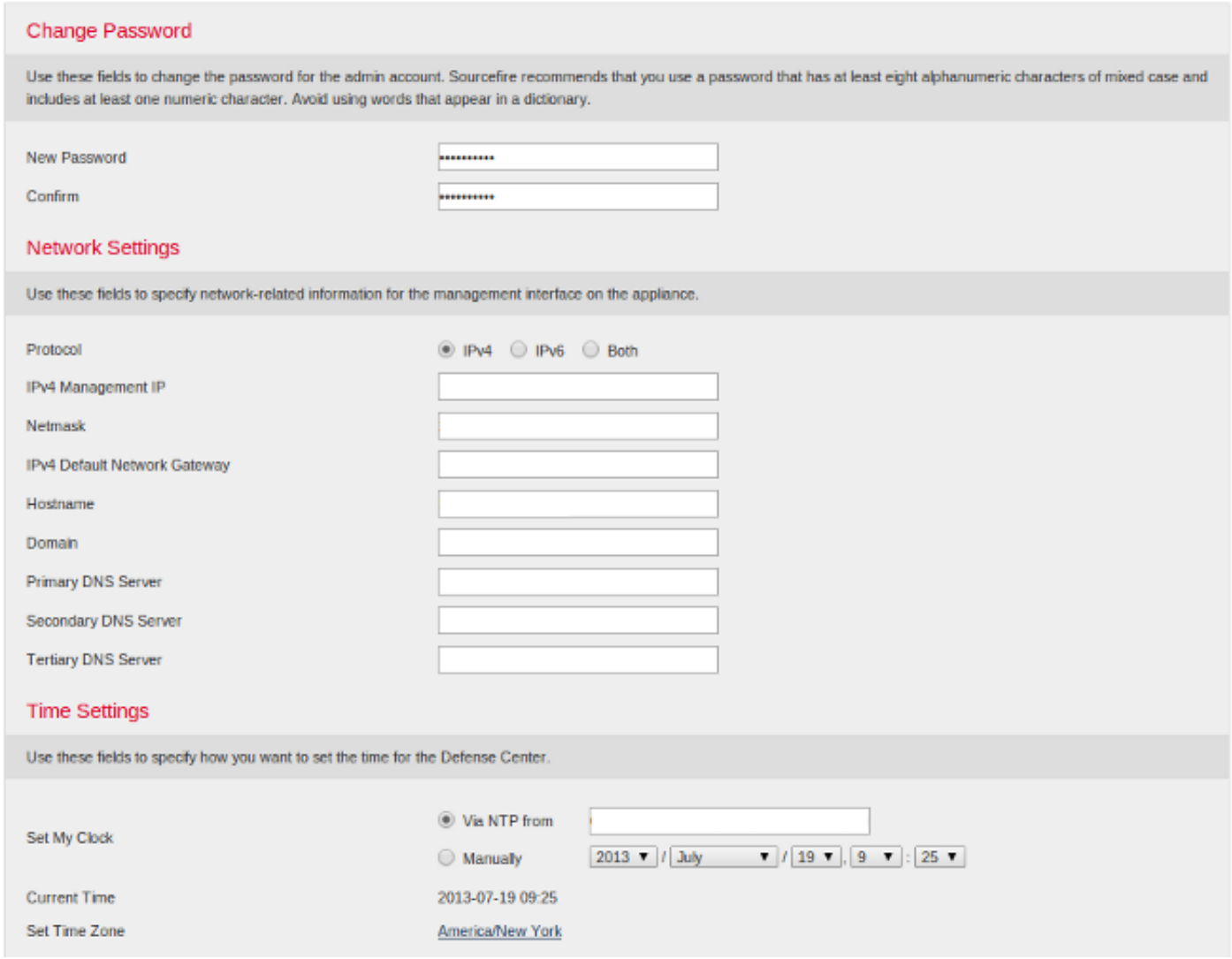
Este guia pressupõe que você leu com atenção o Guia de instalação do sistema FireSIGHT.

Configuração

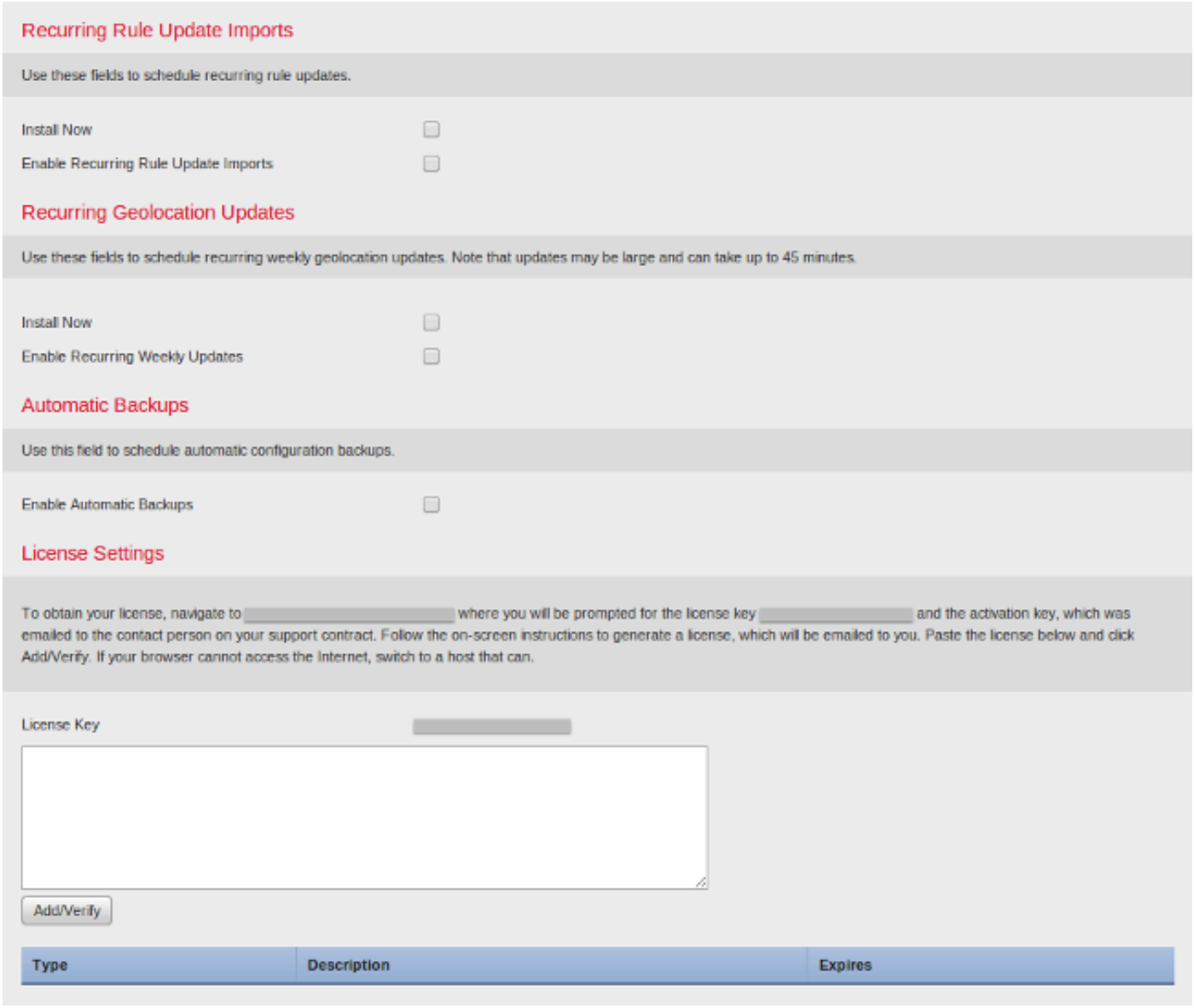
Passo 1: Configuração inicial

No FireSIGHT Management Center, você deve concluir o processo de configuração fazendo login

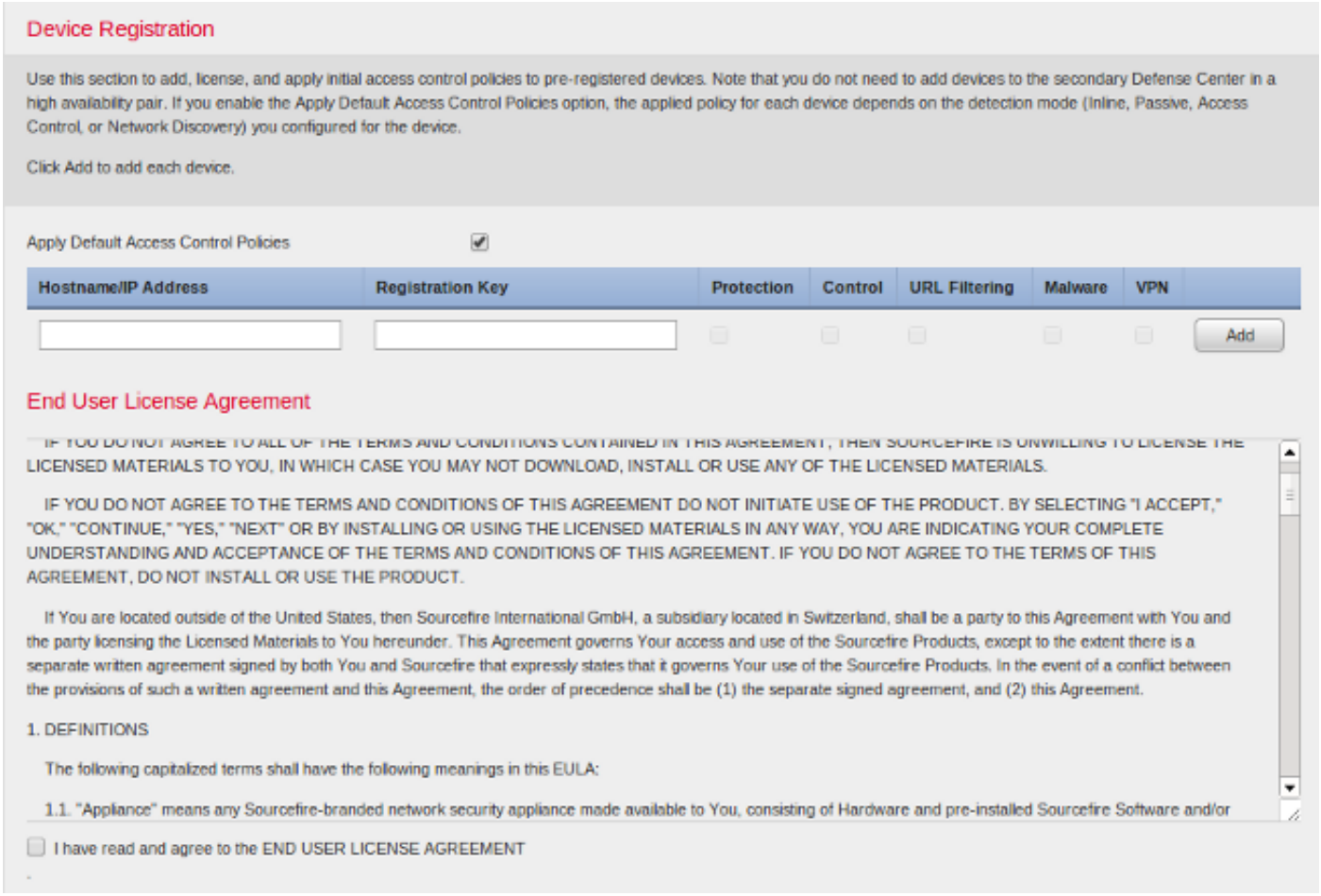
na interface da Web e especificando as opções de configuração inicial na página de configuração, descrita abaixo. Nesta página, você deve alterar a senha do administrador e também pode especificar configurações de rede, como servidores de Domínio e DNS, e a configuração de hora.



Opcionalmente, você pode configurar as atualizações de regras recorrentes e de geolocalização, bem como backups automáticos. Qualquer licença de recurso também pode ser instalada neste ponto.



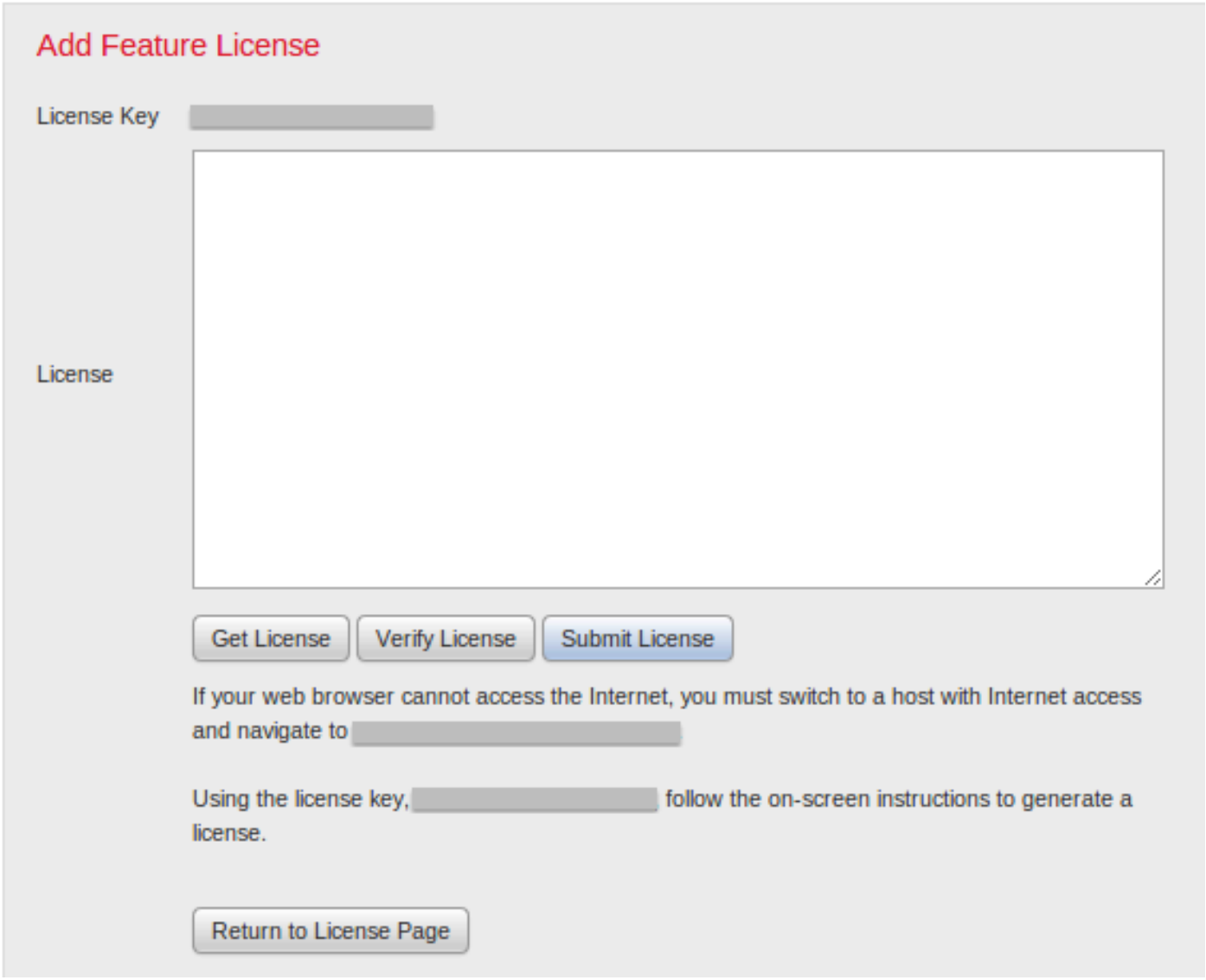
Nesta página, você também pode registrar um dispositivo no FireSIGHT Management Center e especificar um modo de detecção. O modo de detecção e outras opções escolhidas durante o registro determinam as interfaces padrão, os conjuntos em linha e as zonas que o sistema cria, bem como as políticas que inicialmente aplica aos dispositivos gerenciados.



Passo 2: Instalar licenças

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

- Navegue até a seguinte página: **Sistema > Licenças**.
- Clique em **Adicionar nova licença**.



Se você não recebeu uma licença, entre em contato com o representante de vendas da sua conta.

Passo 3: Aplicar a política do sistema

A política do sistema especifica a configuração para perfis de autenticação e sincronização de tempo entre o FireSIGHT Management Center e os dispositivos gerenciados. Para configurar ou aplicar a política do sistema, navegue para **System > Local > System Policy**. Uma política de sistema padrão é fornecida, mas precisa ser aplicada a qualquer dispositivo gerenciado.

Passo 4: Aplicar a política de integridade

A política de integridade é usada para configurar como os dispositivos gerenciados relatam seu status de integridade ao FireSIGHT Management Center. Para configurar ou aplicar a política de integridade, navegue para **Integridade > Política de integridade**. Uma política de integridade padrão é fornecida, mas precisa ser aplicada a qualquer dispositivo gerenciado.

Passo 5: Registrar dispositivos gerenciados

Se você não registrou dispositivos durante a página de configuração inicial, leia este documento para obter instruções sobre como registrar um dispositivo em um FireSIGHT Management Center.

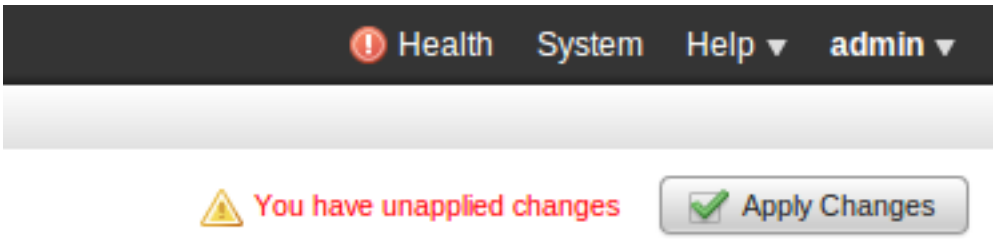
Passo 6: Ativar licenças instaladas

Antes de poder usar qualquer licença de recurso em seu dispositivo, você precisa ativá-la para cada dispositivo gerenciado.

1. Navegue até a seguinte página: **Dispositivos > Gerenciamento de dispositivos**.
2. Clique no dispositivo para o qual deseja habilitar as licenças e digite a guia Device (Dispositivo).
3. Clique em **Editar** (ícone *de lápis*) ao lado de Licença.

Ative as licenças necessárias para este dispositivo e clique em **Salvar**.

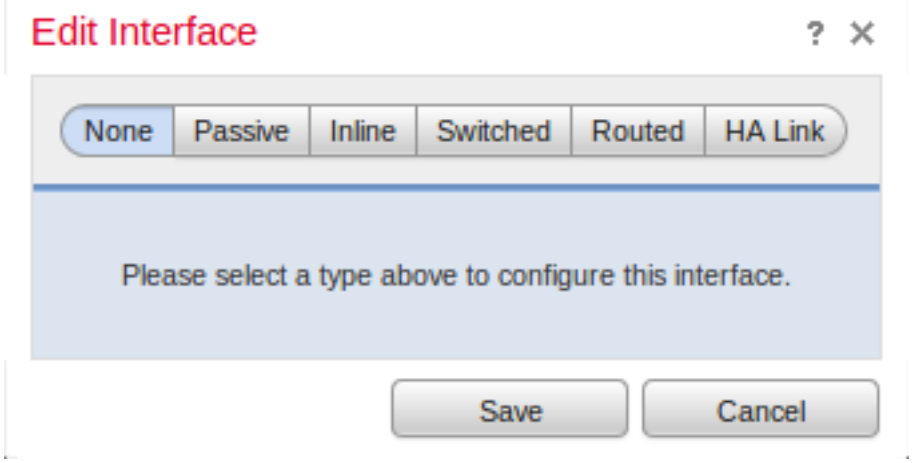
Observe a mensagem "*Você tem alterações não aplicadas*" no canto superior direito. Este aviso permanecerá ativo mesmo que você navegue para fora da página de gerenciamento de dispositivos até clicar no botão **Aplicar alterações**.



Passo 7: Configurar interfaces de detecção

1. Navegue até a seguinte página **Dispositivos > Gerenciamento de dispositivos**.
2. Clique no ícone **Editar** (lápis) do sensor de sua escolha.

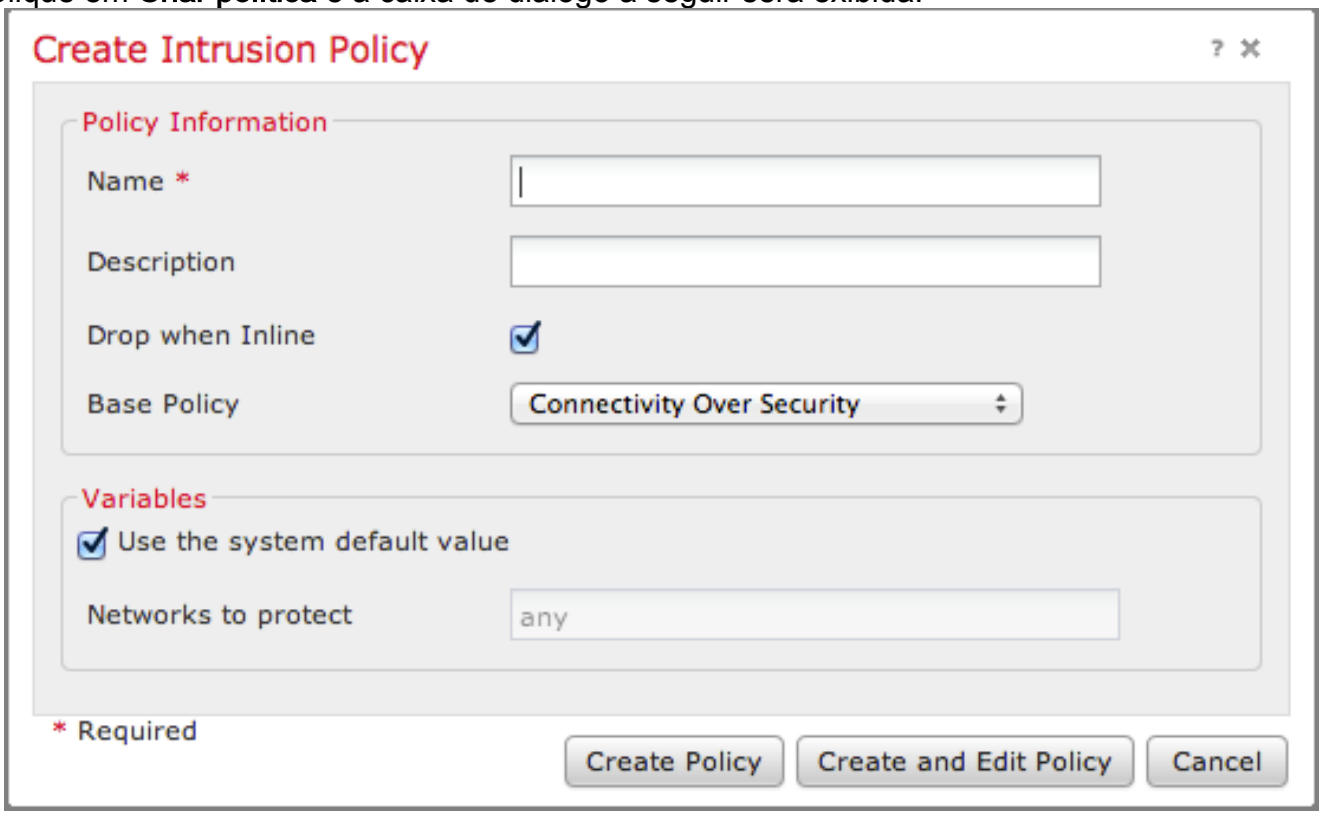
3. Na guia **Interfaces**, clique no ícone **Edit** da interface de sua escolha.



Selecione uma configuração de interface Passiva ou Inline. As interfaces comutadas e roteadas estão além do escopo deste artigo.

Passo 8: Configurar a política de intrusão

- Navegue até a seguinte página: **Políticas > Intrusão > Política de intrusão.**
- Clique em **Criar política** e a caixa de diálogo a seguir será exibida:



Você deve atribuir um nome e definir a política base a ser usada. Dependendo da sua implantação, você pode optar por ter a opção **Drop quando Inline** habilitado. Defina as redes que deseja proteger para reduzir falsos positivos e melhorar o desempenho do sistema.

Clicar em **Create Policy** salvará suas configurações e criará a política IPS. Se quiser fazer qualquer modificação na política de intrusão, você pode escolher **Criar e Editar Política** em vez

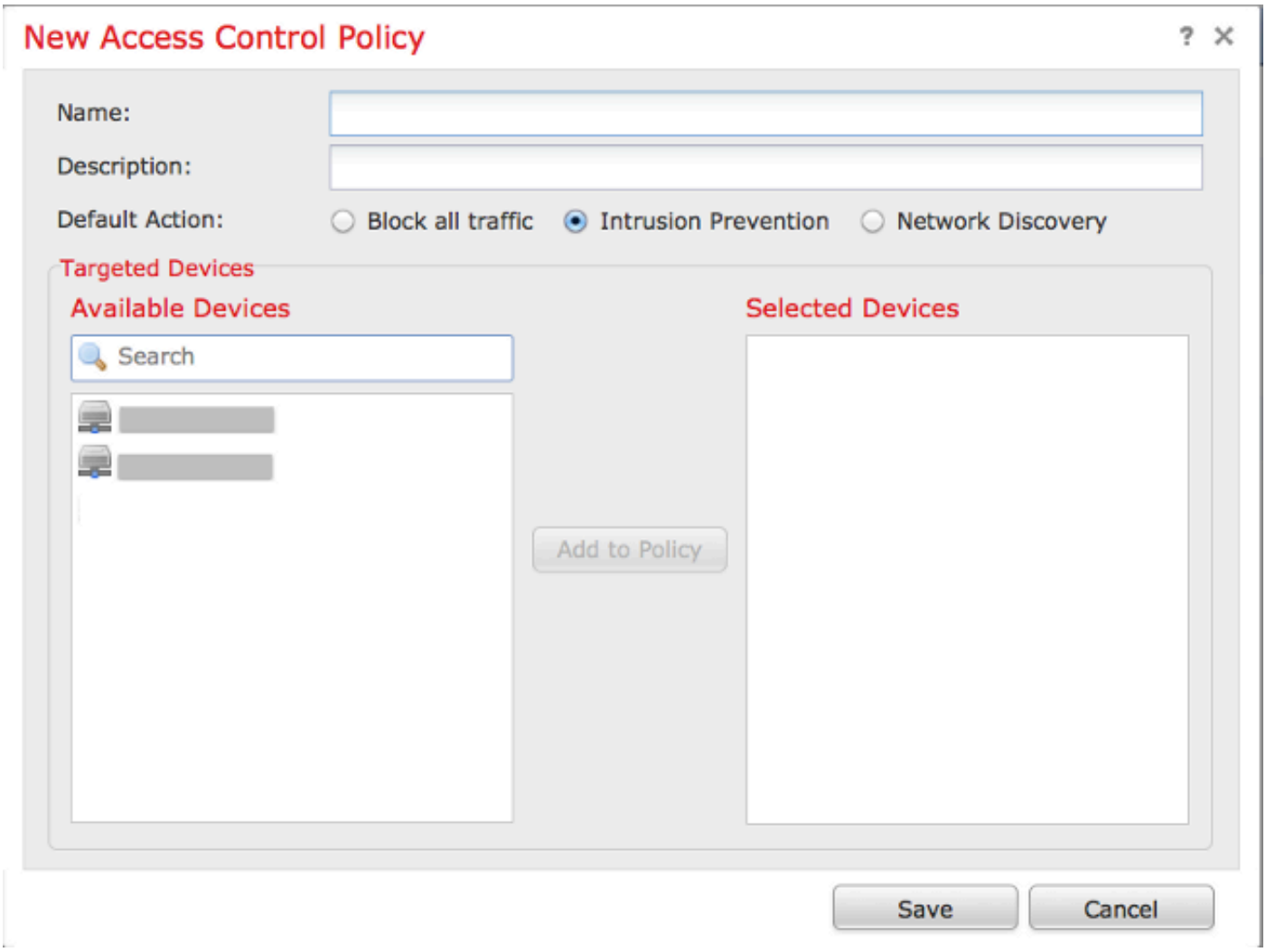
disso.

> **Note**: As políticas de intrusão são são aplicadas como parte da política de controle de acesso. Após a aplicação de uma política de intrusão, qualquer modificação pode ser aplicada sem reaplicar toda a política de Controle de Acesso clicando no botão **Reaplicar**.

Etapa 9: Configurar e aplicar uma política de controle de acesso

1. Navegue até **Políticas > Controle de acesso**.

2. Clique em **Nova política**.

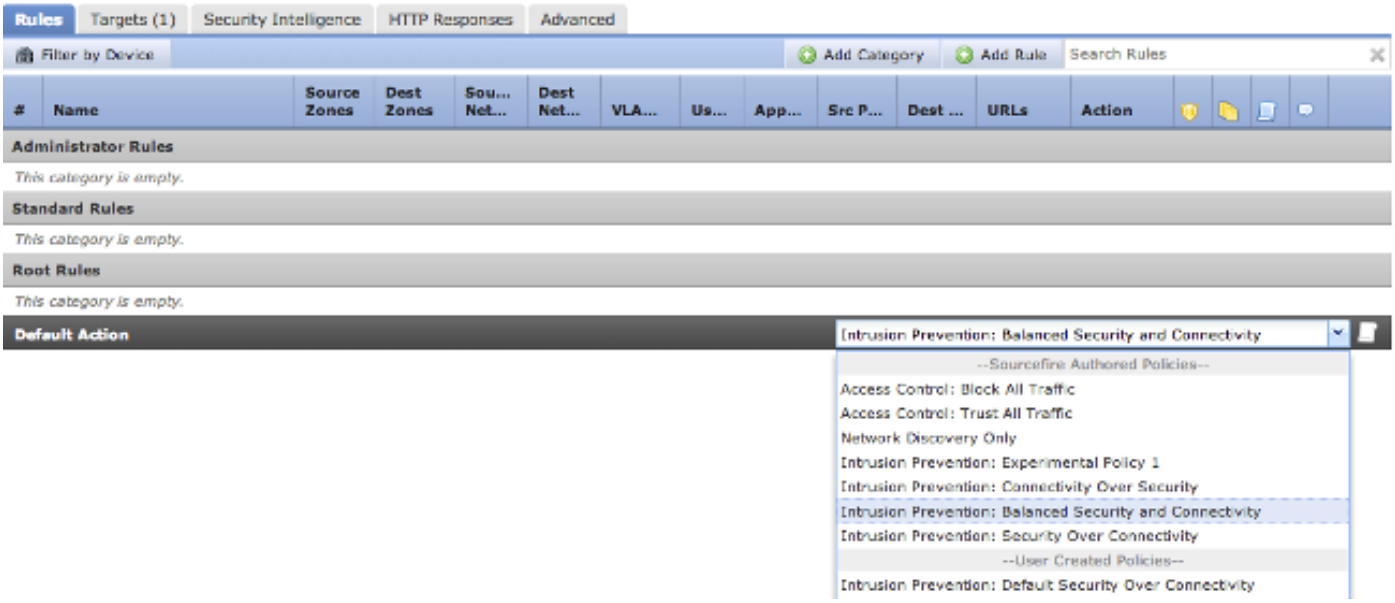


3. Forneça um **Nome** para a política e uma **Descrição**.

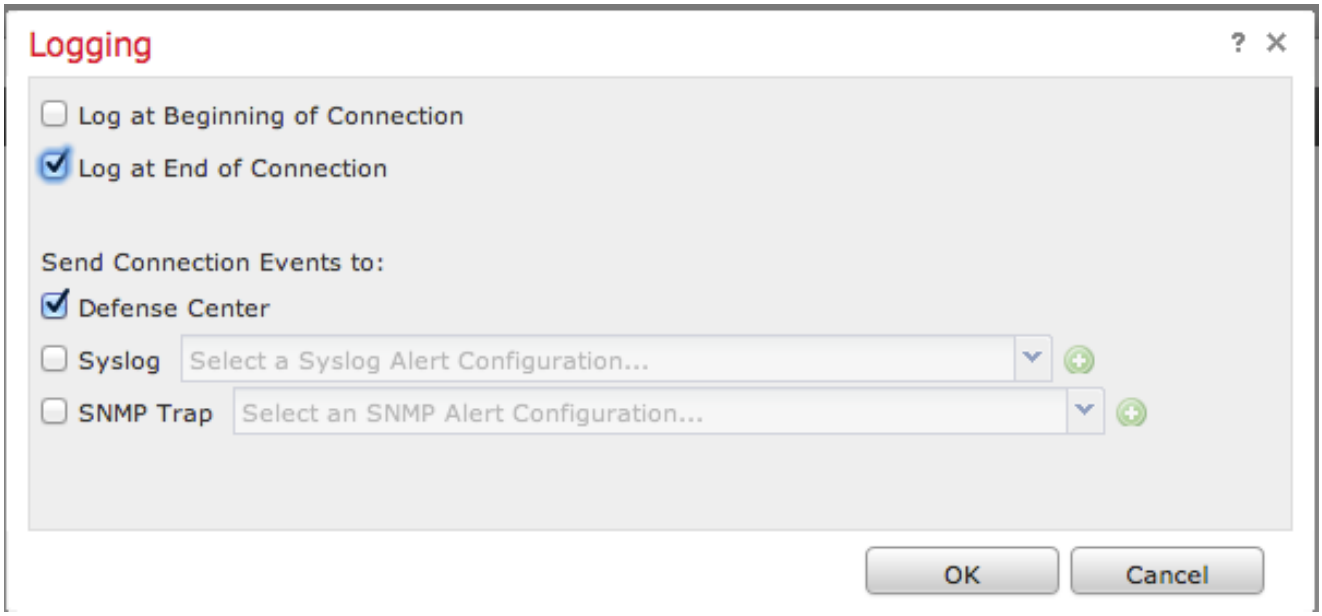
4. Selecione **Intrusion Prevention** como a **Ação Padrão** da política de Controle de Acesso.

5. Por fim, selecione os **dispositivos direcionados** aos quais deseja aplicar a política de controle de acesso e clique em **Salvar**.

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



7. O registro de conexão deve ser ativado para gerar eventos de conexão. Clique no menu suspenso à direita de **Ação padrão**.



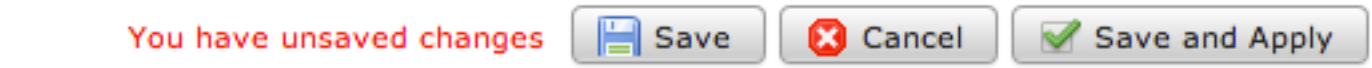
8. Escolha registrar conexões no início ou no fim da conexão. Os eventos podem ser registrados no FireSIGHT Management Center, em um local de syslog ou através do SNMP.

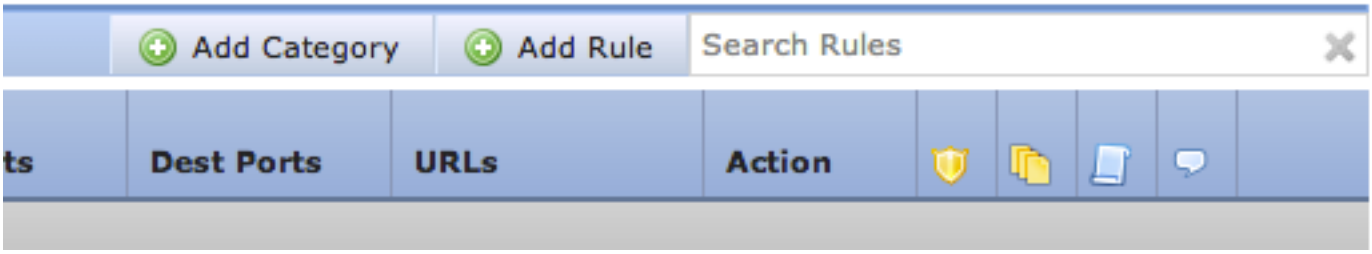
> **Note**: Não é recomendável fazer logon em ambas as extremidades da conexão porque cada conexão (exceto conexões bloqueadas) será registrada duas vezes. O registro no início é útil para conexões que serão bloqueadas e o registro no final é útil para todas as outras conexões.

9. Click **OK**. Observe que a cor do ícone de registro foi alterada.

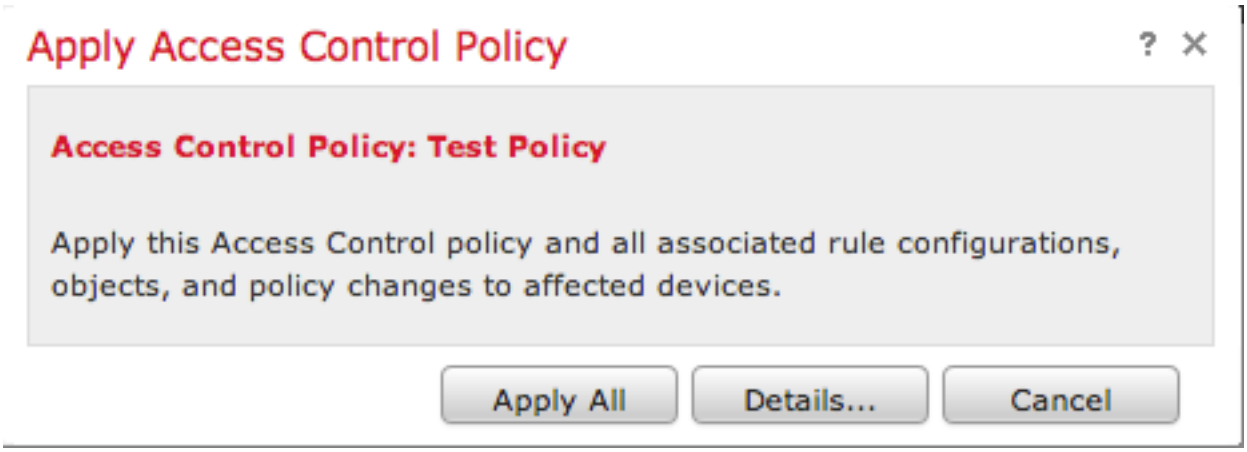
10. Você pode adicionar uma **regra de controle de acesso** no momento. As opções que você pode usar dependem do tipo de licença instalada.

11. Quando terminar de fazer alterações. clique no botão **Salvar e aplicar**. Você notará uma mensagem indicando que possui alterações não salvas em sua política no canto superior direito até que o botão seja clicado.





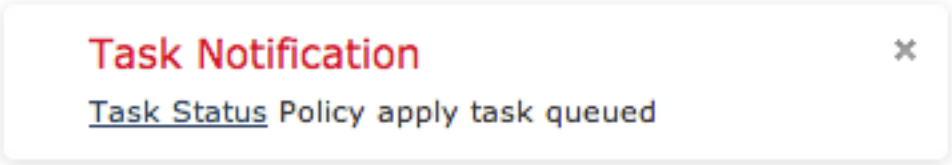
Você pode escolher apenas **Salvar** as alterações ou clicar em **Salvar e aplicar**. A janela a seguir será exibida se você escolher a última.



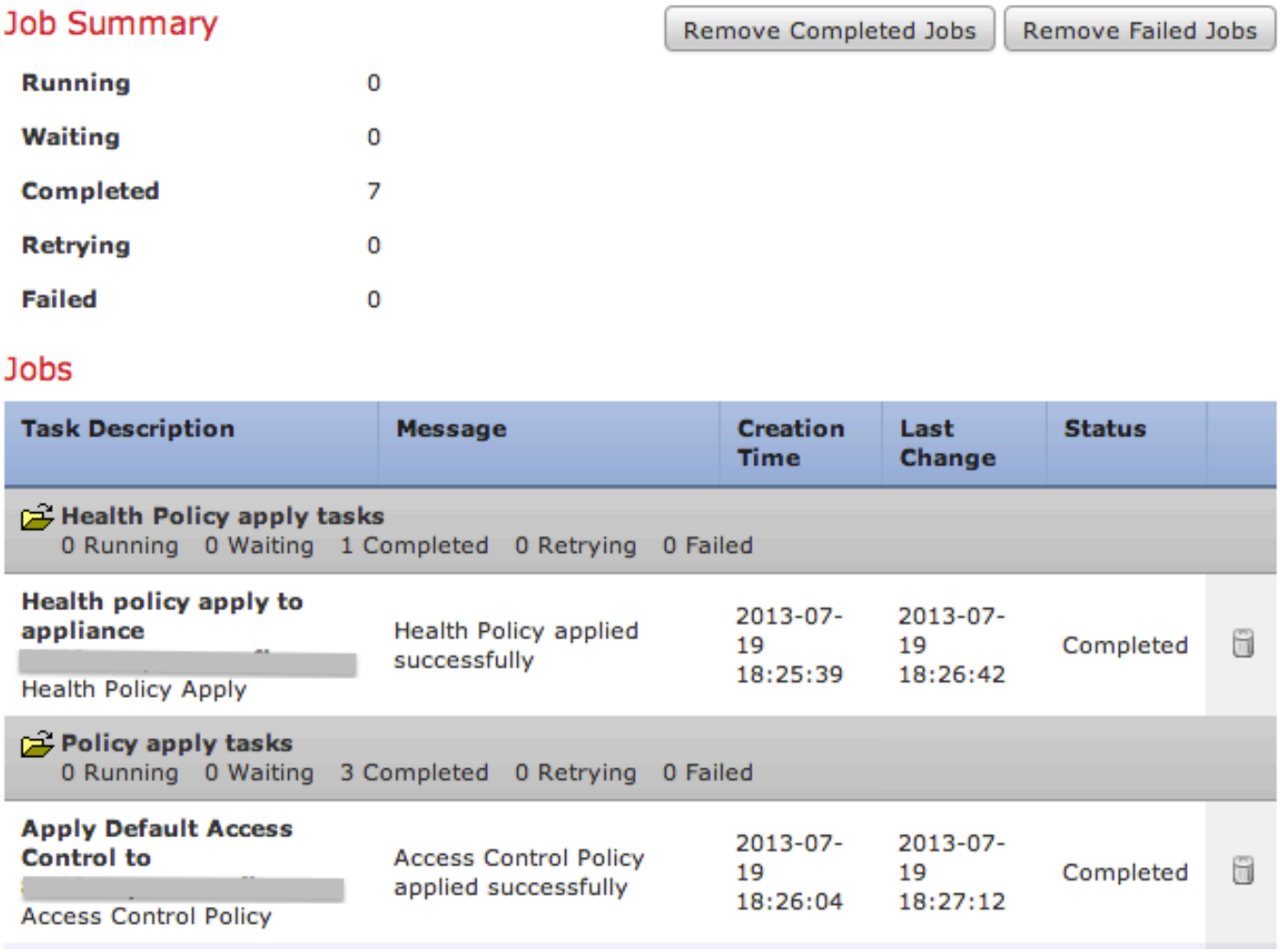
12. **Aplicar tudo** aplicará a política de controle de acesso e qualquer política de intrusão associada aos dispositivos de destino.

> **Note**: Se uma política de intrusão for aplicada pela primeira vez, ela não poderá ser desmarcada.

13. Você pode monitorar o status da tarefa clicando no link **Status da Tarefa** na notificação mostrada na parte superior da página ou navegando para: **Sistema > Monitoramento > Status da Tarefa**



14. Clique no link Status da tarefa para monitorar o progresso da aplicação da política de controle de acesso.



Etapa 10: Verifique se o FireSIGHT Management Center recebe eventos

Após a conclusão da aplicação da política de controle de acesso, você deve começar a ver os eventos de conexões e dependendo dos eventos de intrusão de tráfego.

Recomendação adicional

Você também pode configurar os seguintes recursos adicionais em seu sistema. Consulte o Guia do usuário para obter detalhes sobre a implementação.

- Backups programados
- Atualização automática de software, SRU, VDB e downloads/instalações de GeoLocation.
- Autenticação externa por LDAP ou RADIUS