

Etapas da configuração inicial dos sistemas FireSIGHT

Contents

[Introduction](#)

[Pré-requisito](#)

[Configuração](#)

[Passo 1: Configuração inicial](#)

[Passo 2: Instalar licenças](#)

[Passo 3: Aplicar a política do sistema](#)

[Passo 4: Aplicar a política de integridade](#)

[Passo 5: Registrar dispositivos gerenciados](#)

[Passo 6: Ativar licenças instaladas](#)

[Passo 7: Configurar interfaces de detecção](#)

[Passo 8: Configurar a política de intrusão](#)

[Etapa 9: Configurar e aplicar uma política de controle de acesso](#)

[Etapa 10: Verifique se o FireSIGHT Management Center recebe eventos](#)

[Recomendação adicional](#)

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.

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](#)

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.

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

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.

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

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**.

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.

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.

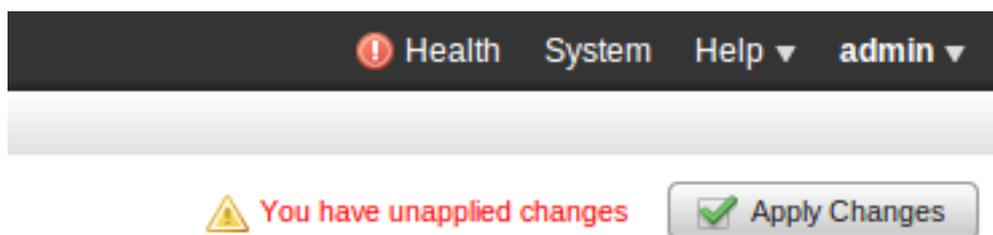
1. Navegue até a seguinte página: **Dispositivos > Gerenciamento de dispositivos**.
2. Clique no dispositivo para o qual deseja habilitar as licenças e digite a guia Device (Dispositivo).
3. Clique em **Editar** (ícone *de lápis*) ao lado de Licença.

License

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

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

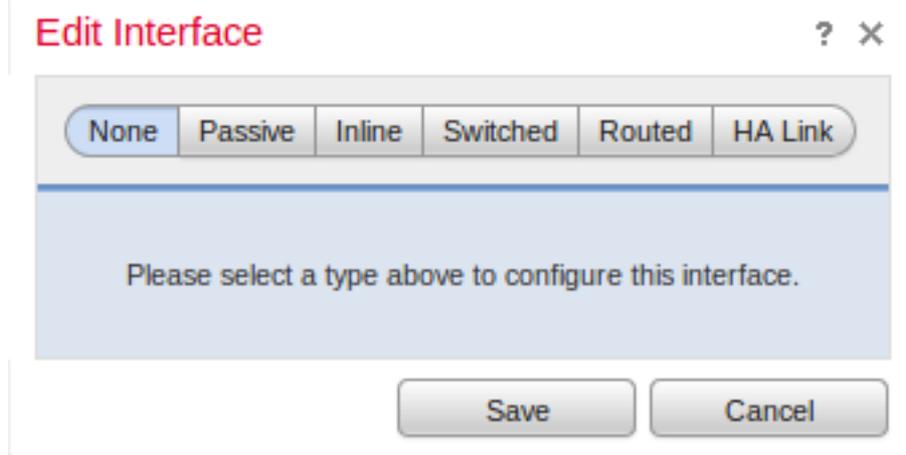
Observe a mensagem "*Você tem alterações não aplicadas*" no canto superior direito. Este aviso permanecerá ativo mesmo que você navegue para fora da página de gerenciamento de dispositivos até clicar no botão **Aplicar alterações**.



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.

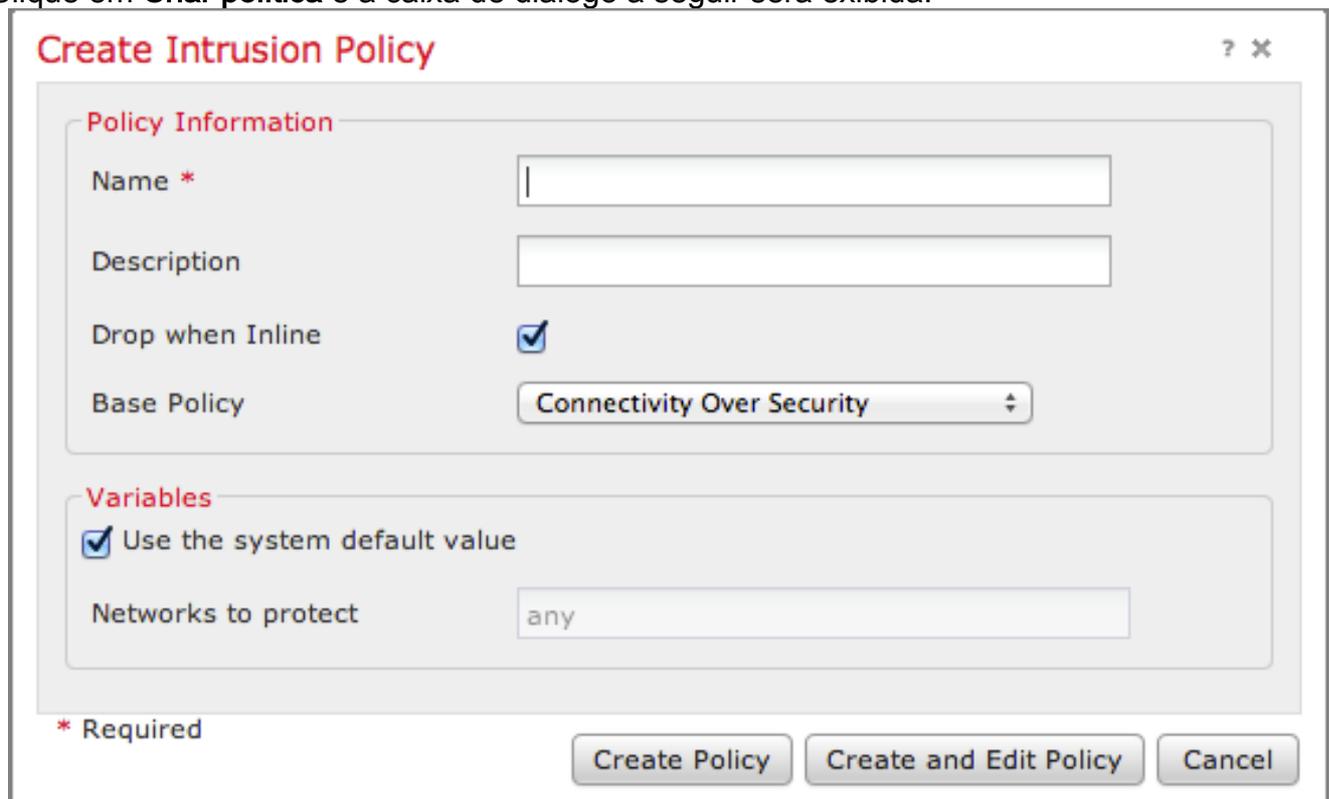
3. Na guia **Interfaces**, clique no ícone **Edit** da interface de sua escolha.



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 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**.

New Access Control Policy ? X

Name:

Description:

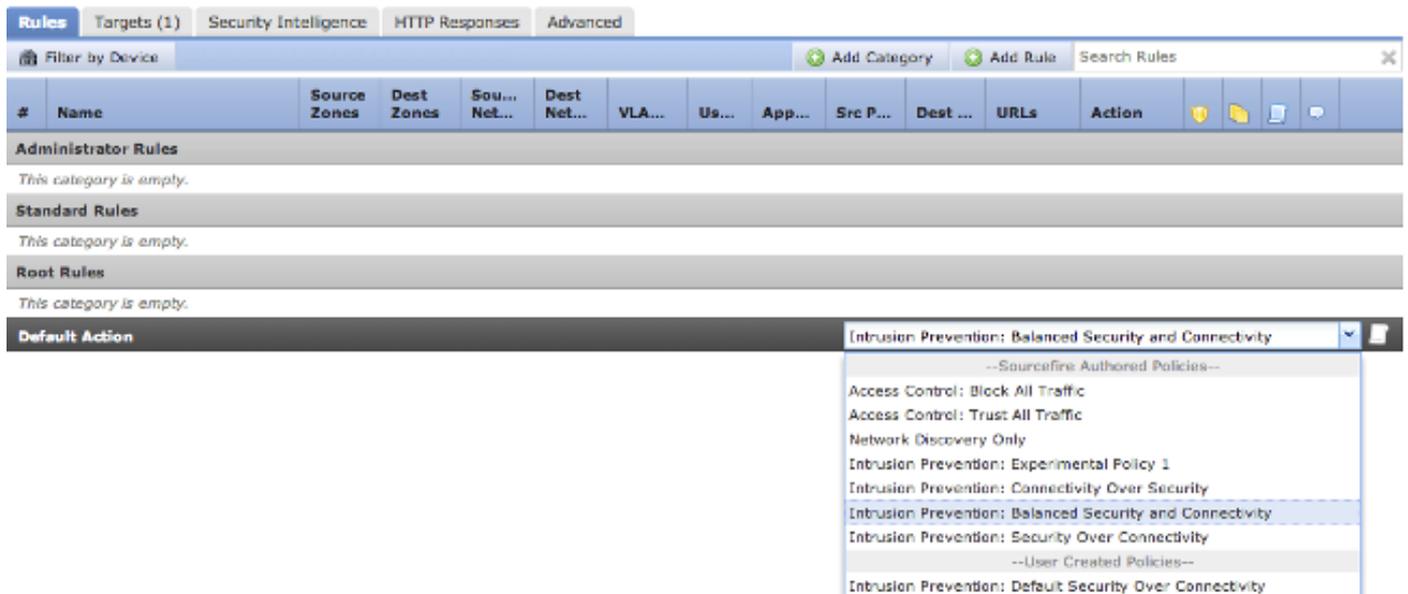
Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

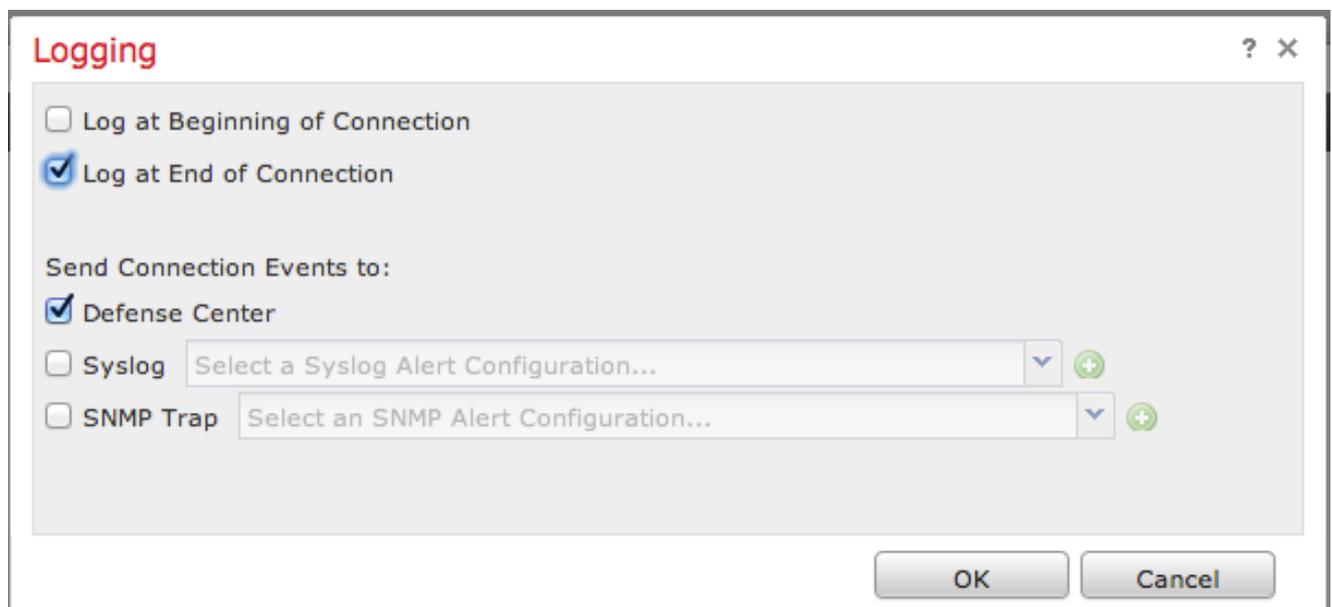
Available Devices

Selected Devices

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.

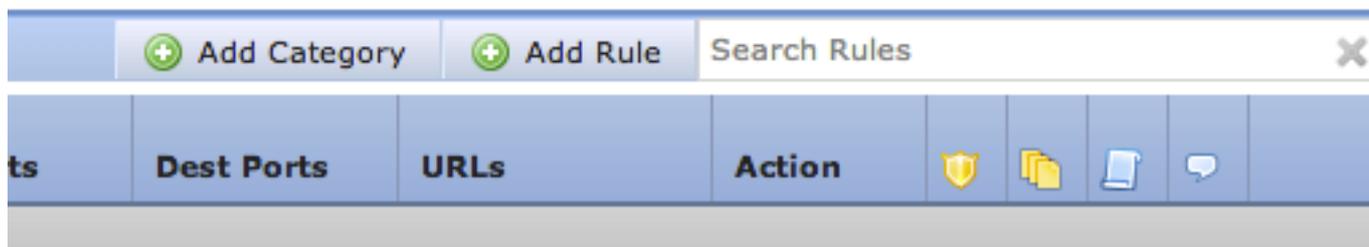
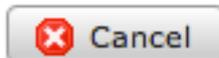
Note: Não é recomendável fazer logon em ambas as extremidades da conexão porque cada conexão (exceto conexões bloqueadas) será registrada duas vezes. O registro no início é útil para conexões que serão bloqueadas e o registro no final é útil para todas as outras conexões.

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

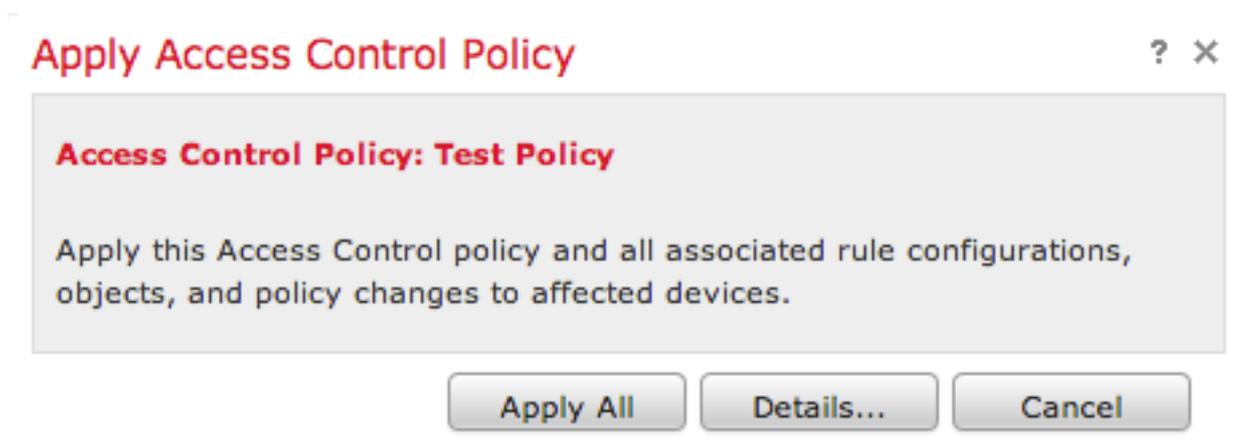
10. Você pode adicionar uma **regra de controle de acesso** no momento. As opções que você pode usar dependem do tipo de licença instalada.

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.

You have unsaved changes



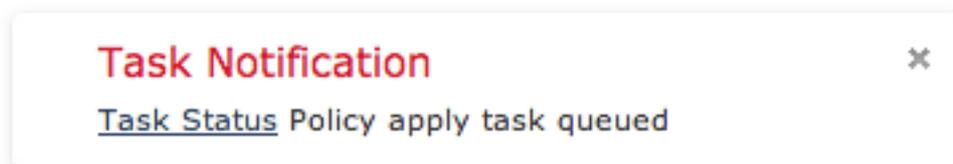
Você pode escolher apenas **Salvar** as alterações ou clicar em **Salvar e aplicar**. A janela a seguir será exibida se você escolher a última.



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.

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	

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