Configurar Sincronização de Dispositivos para o Gerenciador de Segurança

Contents

Introdução

Este documento descreve diferentes maneiras de sincronização de configuração de ASA para CSM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Security Manager
- Dispositivo de segurança adaptável

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Security Manager 4.25
- Dispositivo de segurança adaptável

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O gerenciador de segurança da Cisco fornece serviços centralizados de gerenciamento e monitoramento para o dispositivo Cisco ASA.

Metodologia de demonstração

Este documento descreve dois métodos ou opções diferentes para sincronizar a configuração do ASA com o CSM.

- Detecção de dispositivo único
- Redescoberta de dispositivo em massa

Descoberta de um único dispositivo

A descoberta única só pode ser executada se o dispositivo for adicionado ao inventário. Ele só pode ser executado quando o dispositivo tiver

- Configurações de contexto de segurança para dispositivos ASA, PIX e FWSM sendo executados no modo de contexto múltiplo.
- Configurações de sensor virtual para dispositivos IPS.
- Informações do módulo de serviço para dispositivos Catalyst.

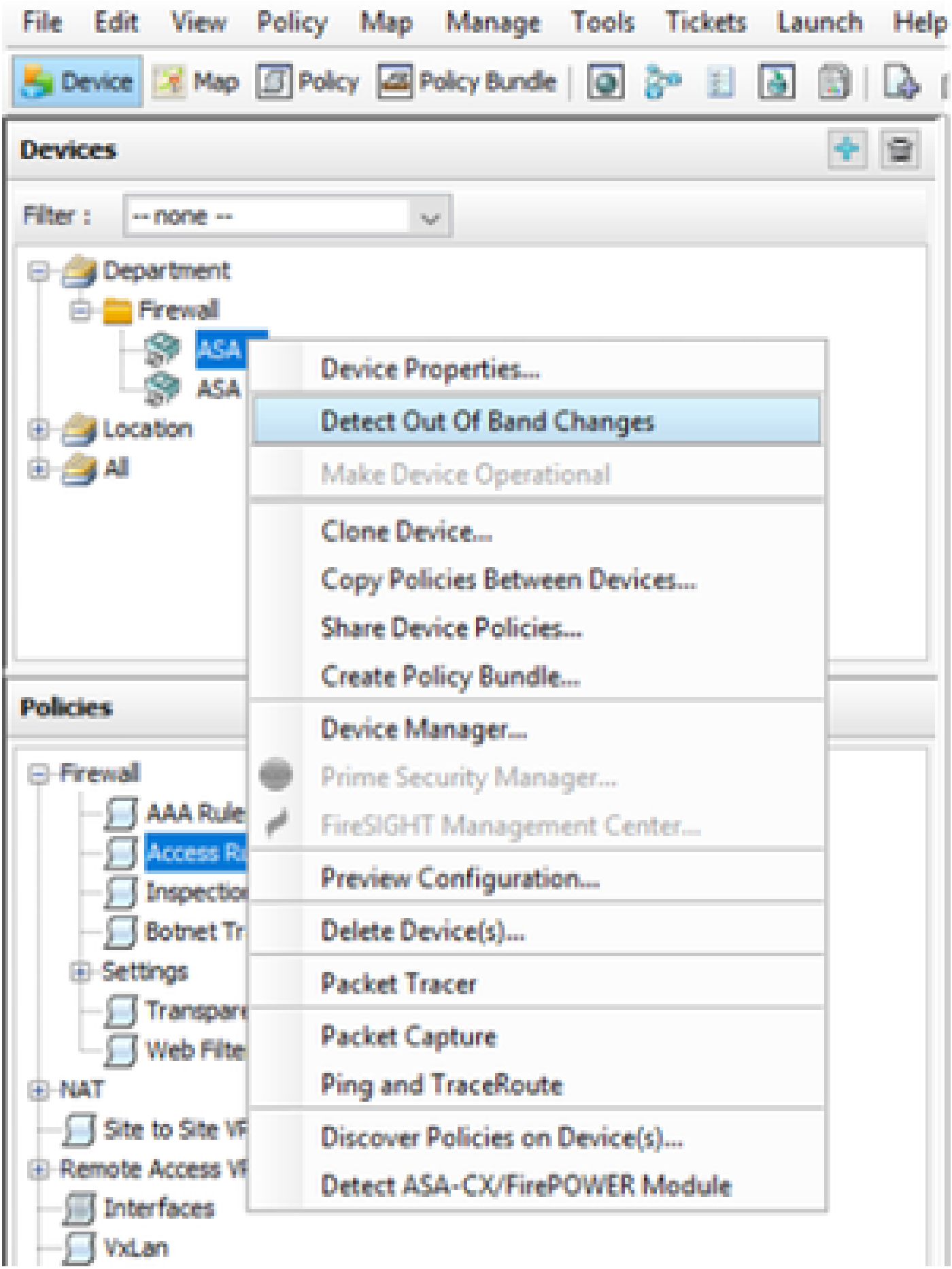
Etapas para executar a descoberta de um único dispositivo:

Você pode executar a descoberta do dispositivo quando tiver executado qualquer alteração na CLI do dispositivo ou se o dispositivo tiver sido removido e adicionado novamente.

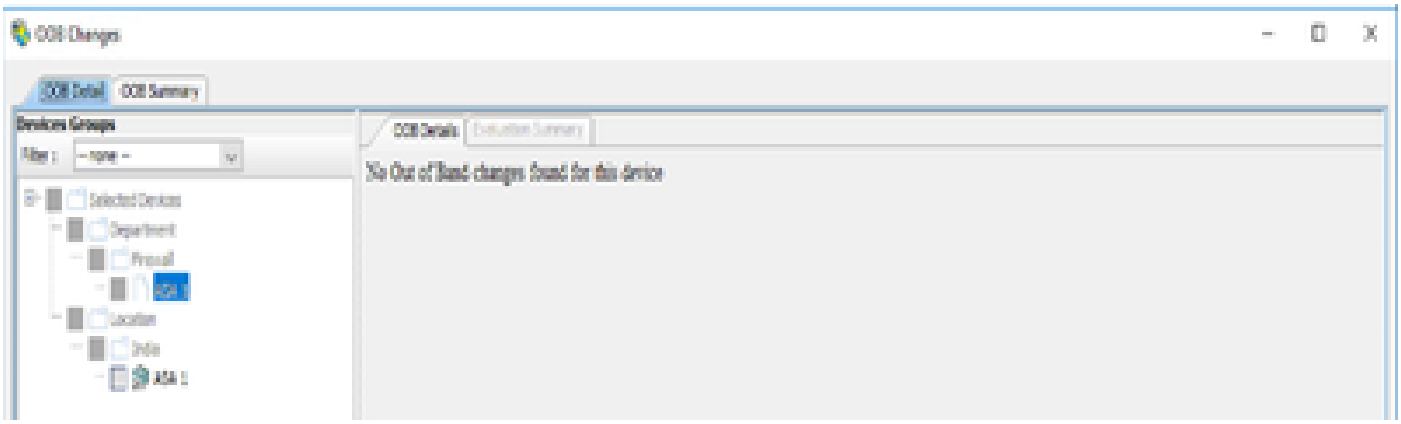
Para verificar se alguma alteração pendente ainda deve ser sincronizada , observe o exemplo mencionado.

Clique com o botão direito no dispositivo respectivo no painel de dispositivos e selecione a opção

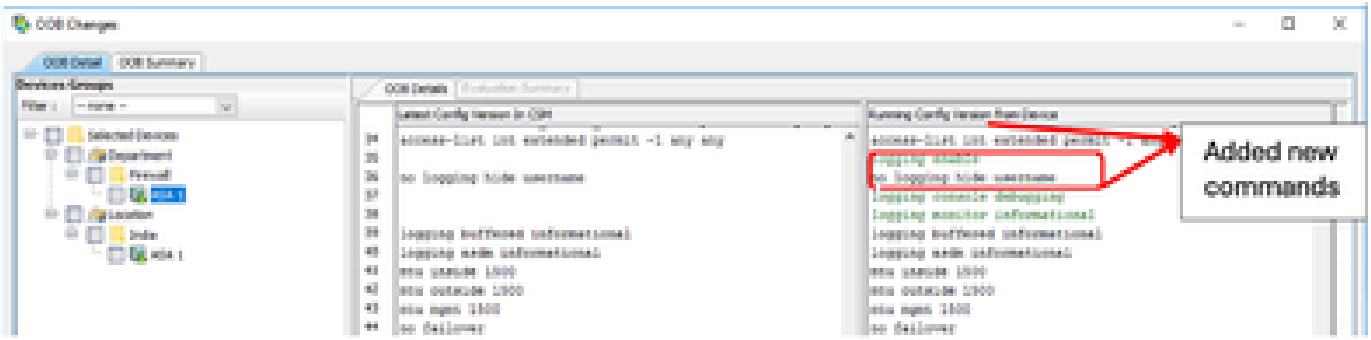
Detectar alterações fora da banda.



Se não houver alterações , a página será exibida como nenhuma alteração fora do limite encontrada para este dispositivo.



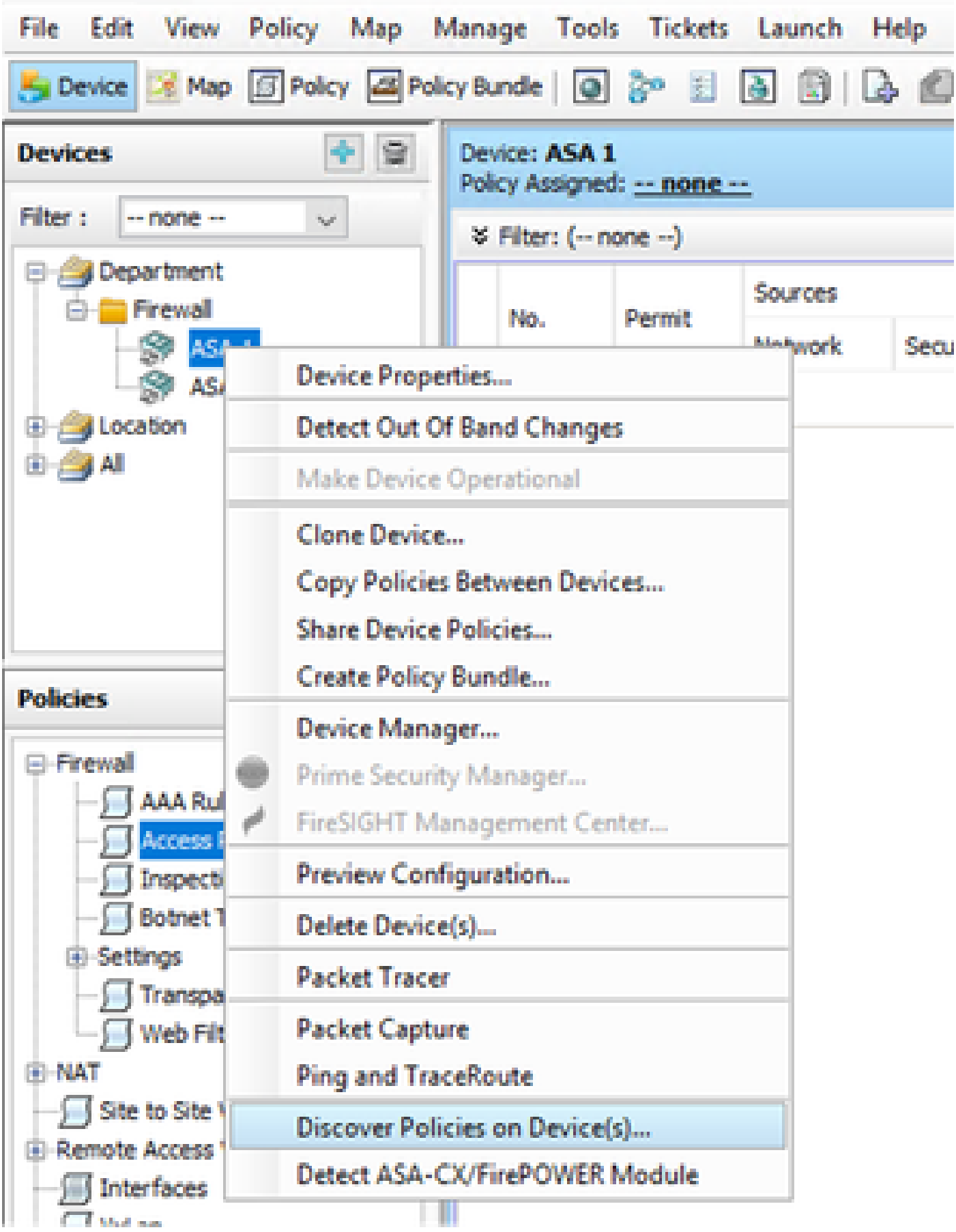
Se alguma alteração tiver sido feita , as linhas serão realçadas de acordo com a legenda.



Etapas para executar a descoberta de um único dispositivo:

Passo 1:

Clique com o botão direito do mouse no nome do dispositivo respectivo no painel de dispositivos e escolha a opção Discover policies on Device(s).

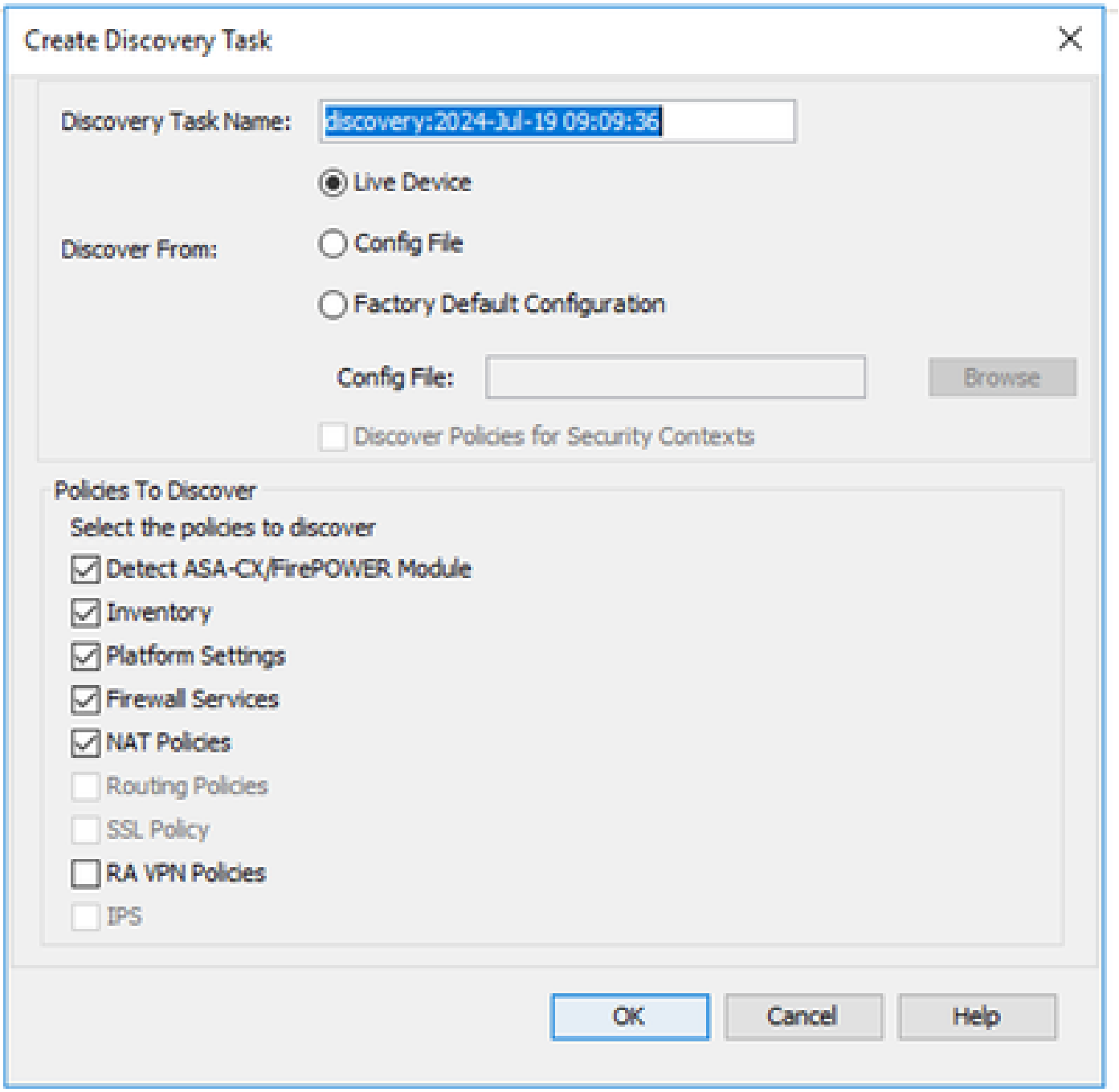

File Edit View Policy Map Manage Tools Tickets Launch Help
Device Map Policy Policy Bundle
Devices
Filter : -- none --
Department
Firewall
Location
All
Device: ASA 1
Policy Assigned: -- none --
Filter: (-- none --)
No.
Permit
Sources
Device Properties...
Detect Out Of Band Changes
Make Device Operational
Clone Device...
Copy Policies Between Devices...
Share Device Policies...
Create Policy Bundle...
Device Manager...
Prime Security Manager...
FireSIGHT Management Center...
Preview Configuration...
Delete Device(s)...
Packet Tracer
Packet Capture
Ping and TraceRoute
Discover Policies on Device(s)...
Detect ASA-CX/FirePOWER Module
Policies
Firewall
Settings
NAT
Interfaces

Passo 2:

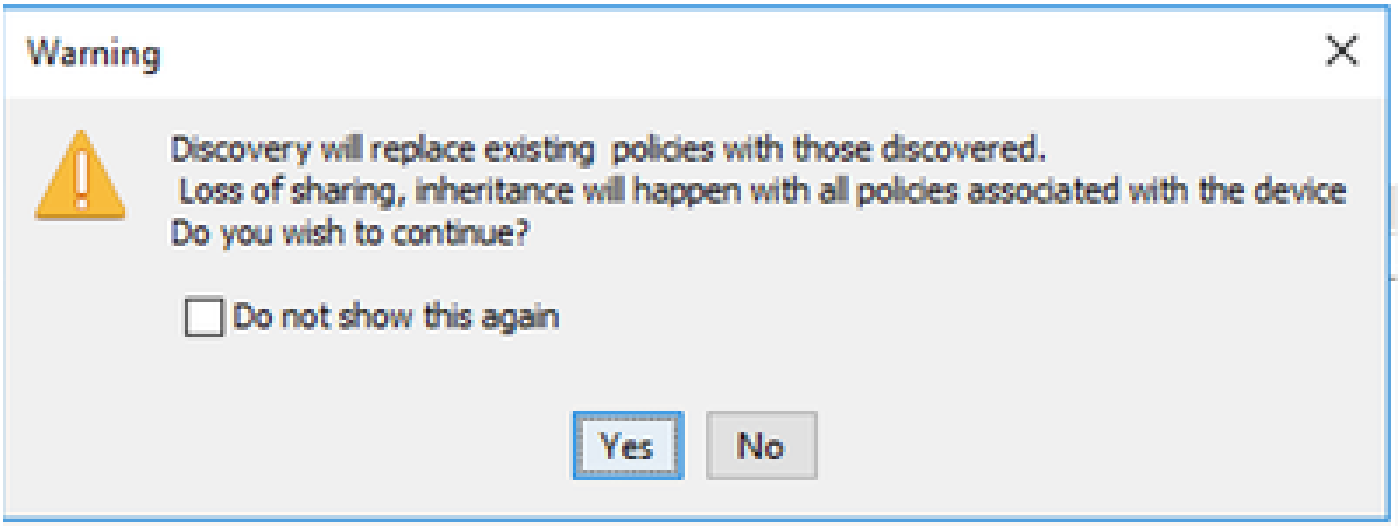
Para o método de recuperação de um único dispositivo, você só pode ver a caixa de diálogo Criar tarefa de descoberta. Caso esteja recebendo uma caixa de diálogo de descoberta em massa , feche-a e abra-a novamente.

Você tem três opções para executar a descoberta.

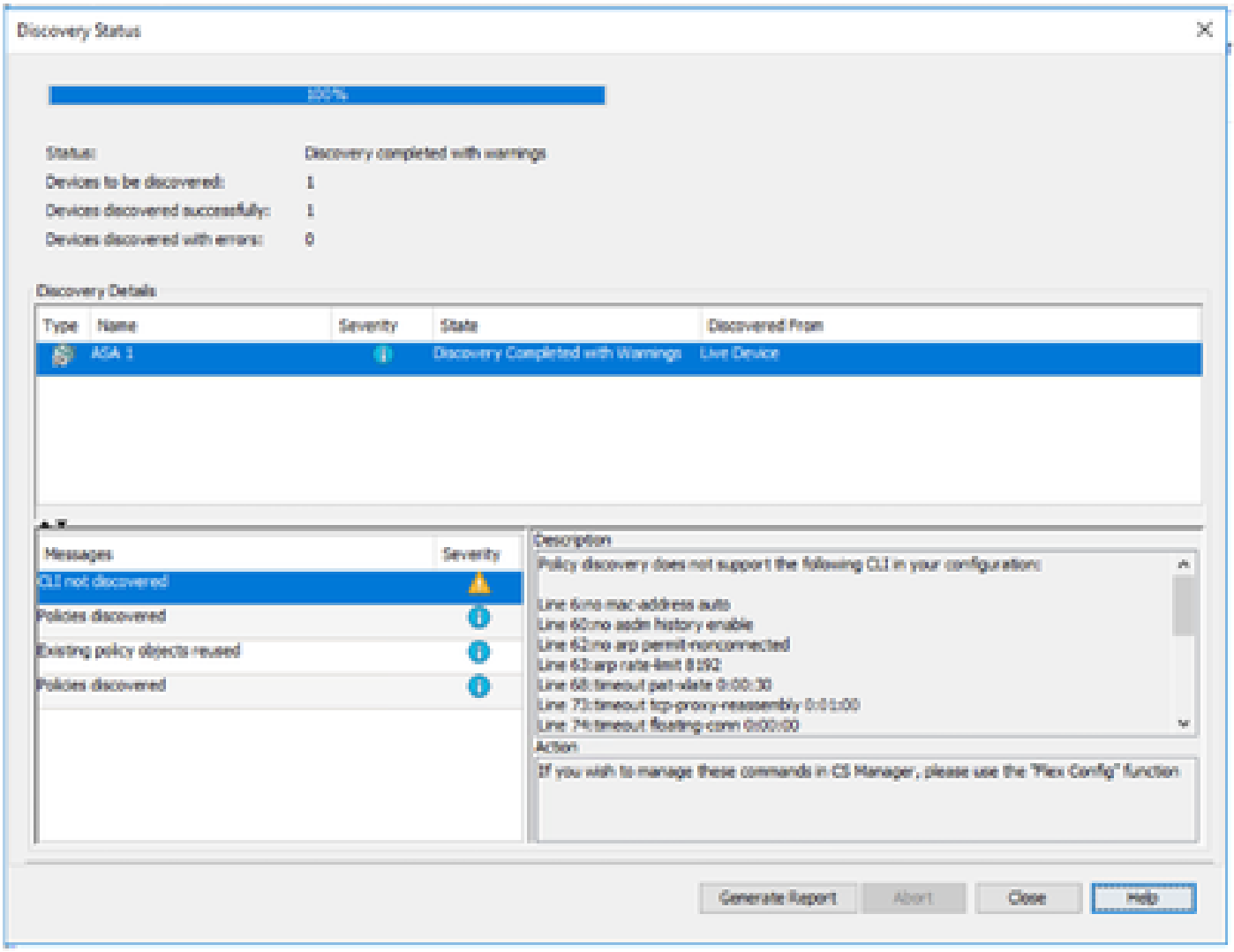
- Dispositivo ativo - Busca a configuração do dispositivo ativo , que está na rede.
- Arquivo de configuração - Você pode escolher o arquivo de configuração e continuar com a descoberta.
- Configuração padrão de fábrica - Redefine o dispositivo para as configurações padrão. Esse método pode ser usado para dispositivos que executam apenas o modo de contexto único ou para dispositivos com contextos de segurança individuais.



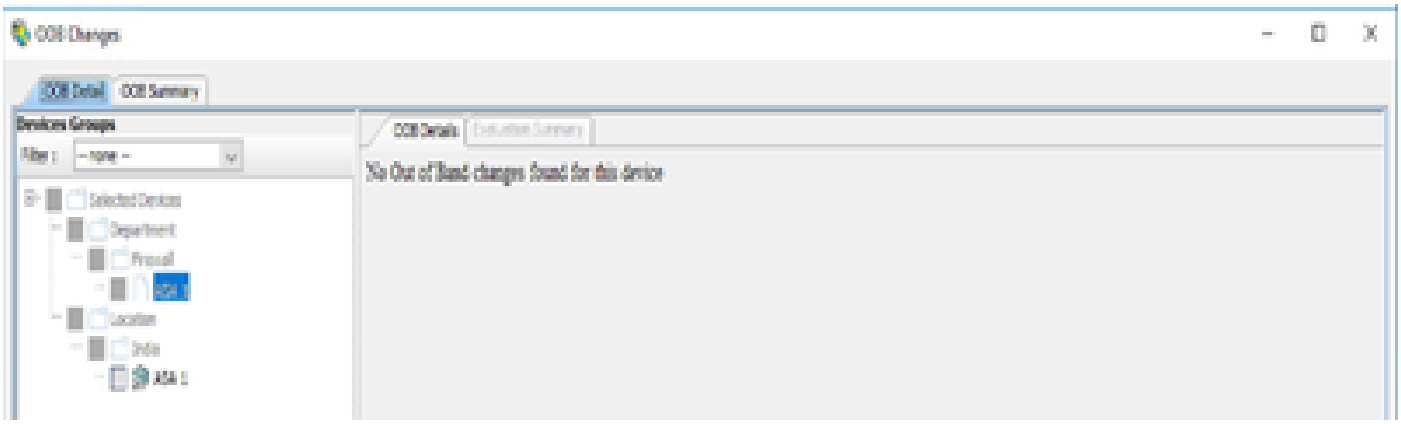
Certifique-se de estar ciente da topologia de rede e das alterações que podem ocorrer na rede antes de continuar com a descoberta.



Quando a descoberta for concluída , você poderá ver a tela pop-up com o status de Descoberta concluída.



Além disso, as alterações fora da banda não podem ter nenhuma alteração.



Descoberta de dispositivos em massa

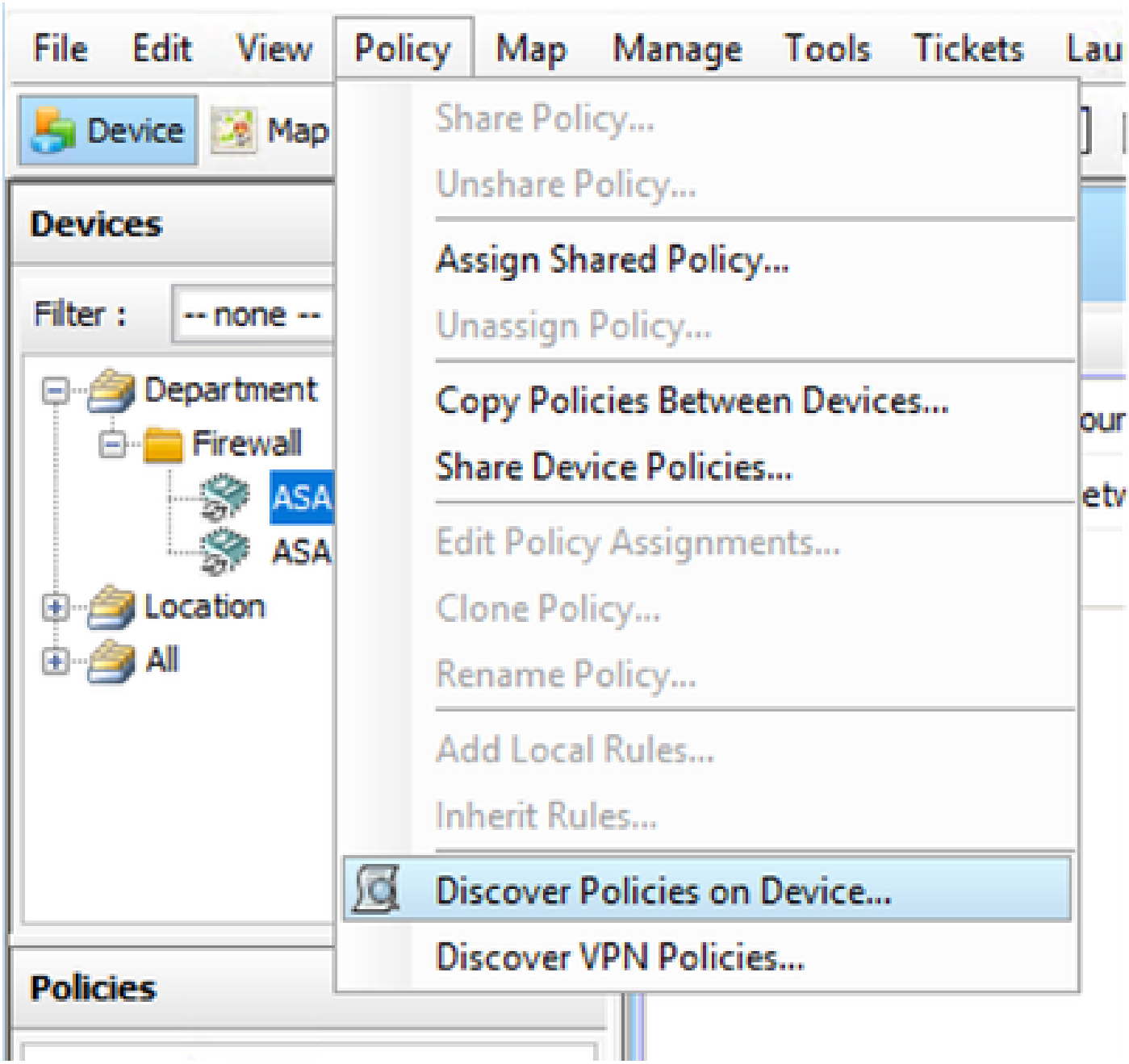
Para descobrir políticas para vários dispositivos, você pode realizar uma redescoberta em massa. É importante observar que a redescoberta em massa é limitada aos dispositivos ativos , aqueles que estão operacionais e acessíveis na rede no momento.

Você não pode executar a descoberta em massa no contexto de segurança, sensores virtuais. Os módulos de serviço podem ser detectados e selecionados separadamente.

Etapas para executar a descoberta de dispositivos em massa:

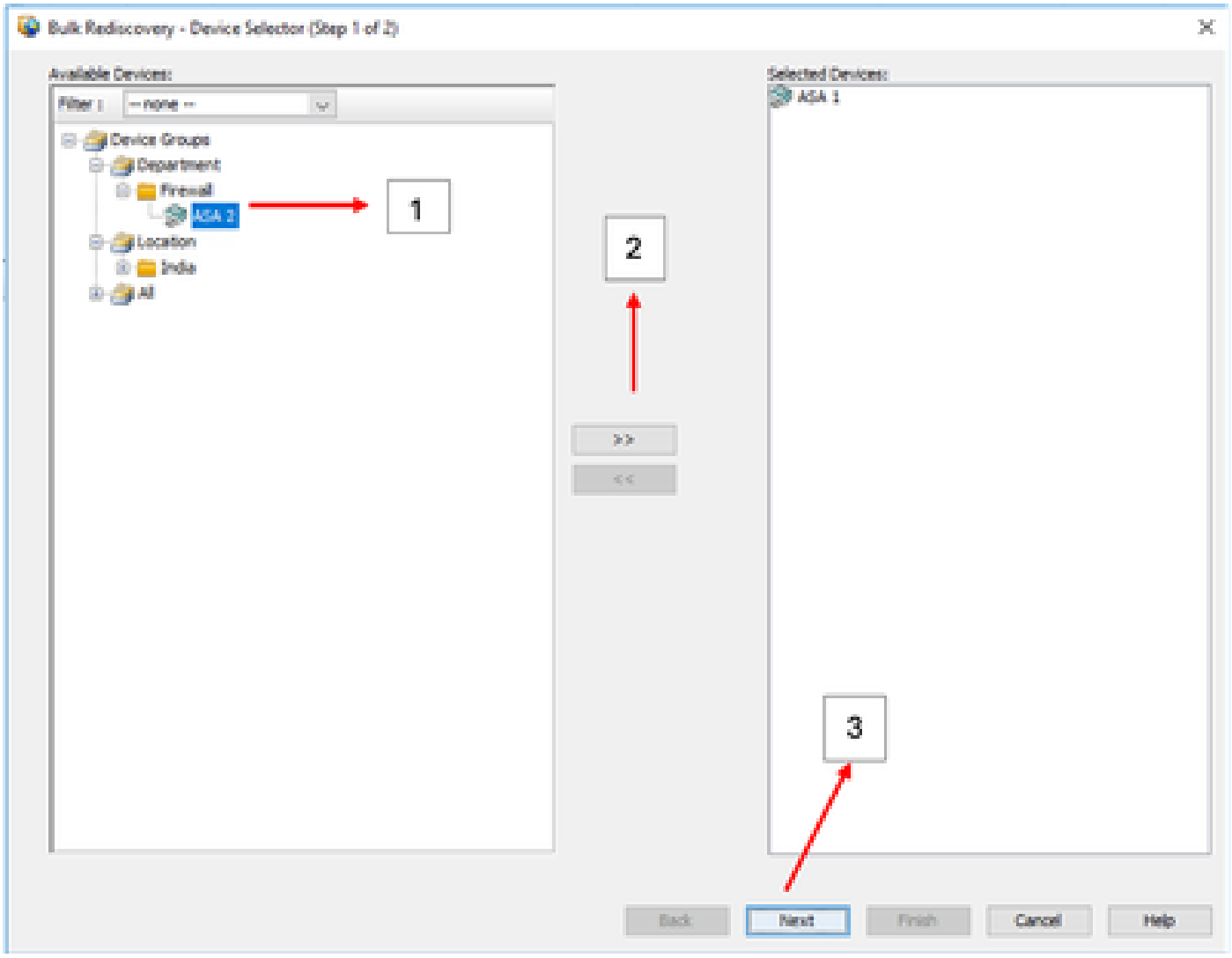
Passo 1:

Navegue até Política > Descobrir políticas no dispositivo



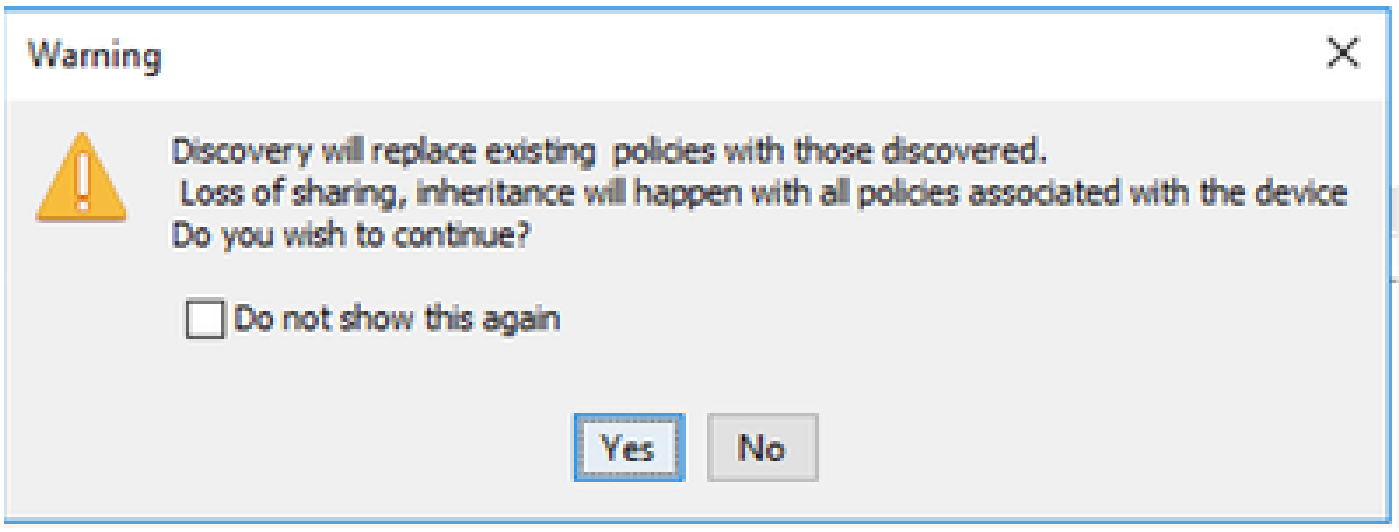
Passo 2:

Se você estiver executando a redescoberta em massa , somente a caixa de diálogo de redescoberta em massa poderá ser exibida.
Em dispositivos disponíveis no painel esquerdo , escolha a lista de dispositivos para os quais deseja descobrir políticas e mova-a para o lado direito.

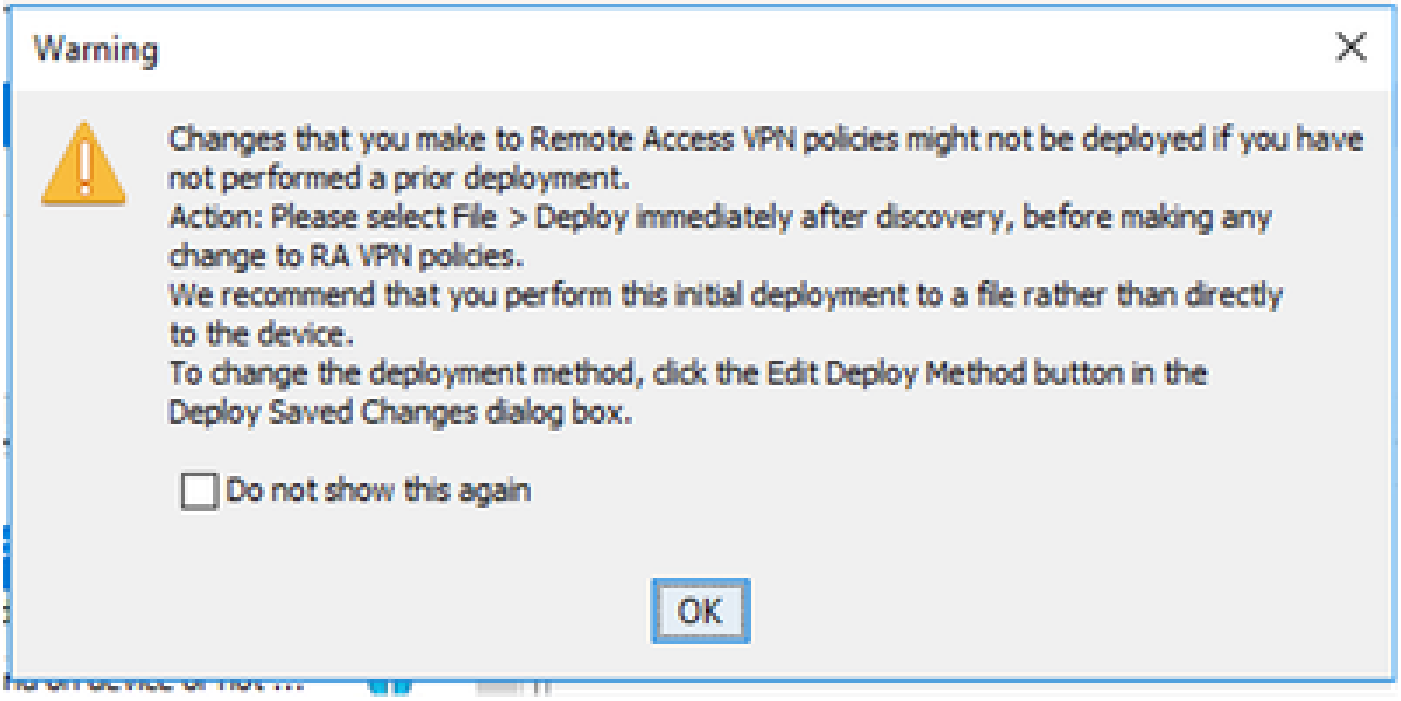


Passo 3:

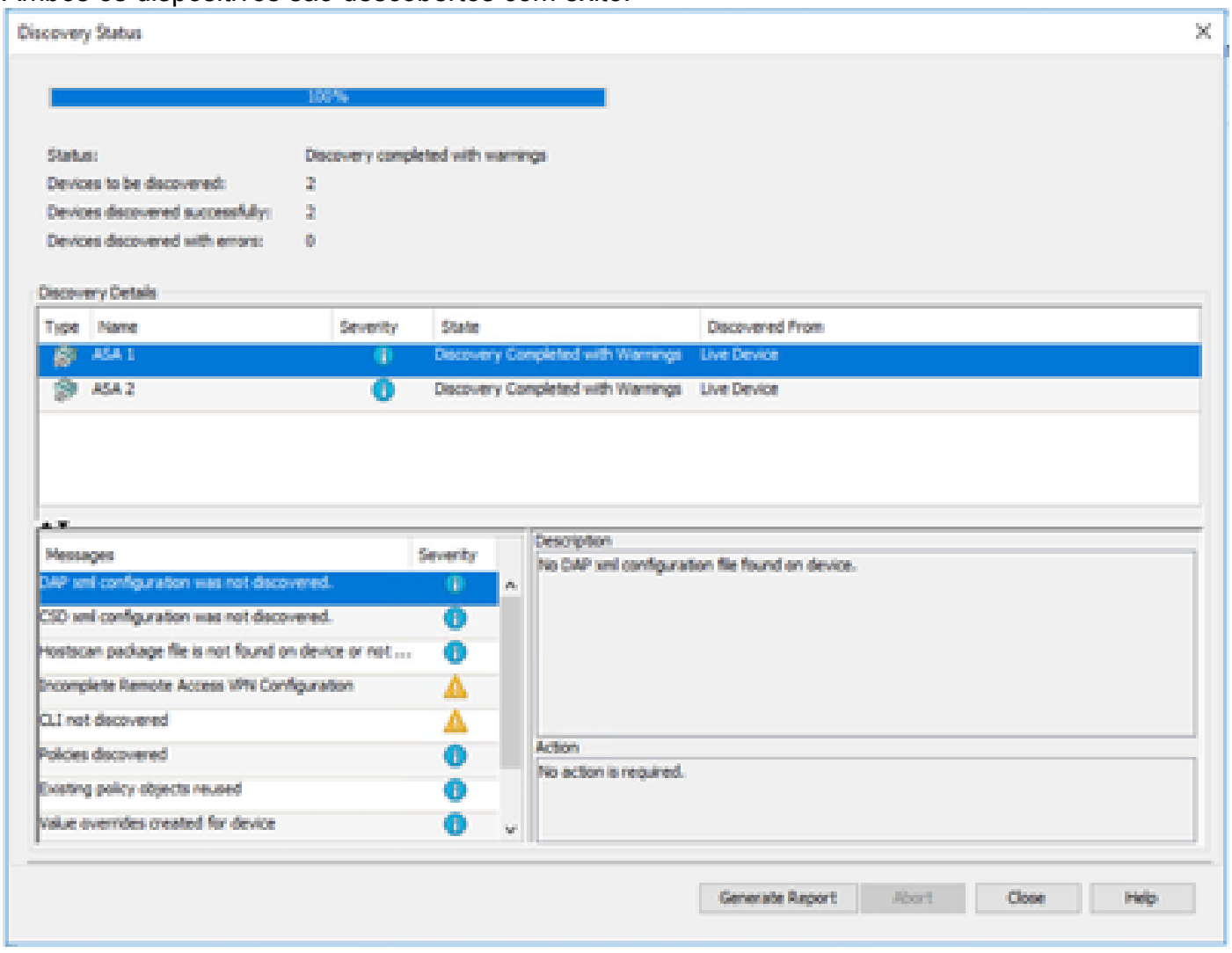
Verifique se todos os dispositivos selecionados estão listados e clique em Concluir para continuar com a redescoberta em massa.
Certifique-se de estar ciente da topologia de rede e das alterações que podem ocorrer na rede antes de continuar com a descoberta.



Quando a descoberta estiver concluída, você poderá ver o exemplo como



Ambos os dispositivos são descobertos com êxito.



Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.