

Configuración de la sincronización de dispositivos al Administrador de seguridad

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Metodología de demostración](#)

[Detección de un solo dispositivo](#)

[Pasos para realizar la detección de un solo dispositivo:](#)

[Pasos para realizar la detección de un solo dispositivo:](#)

[Paso 1:](#)

[Paso 2:](#)

[Descubrimiento masivo de dispositivos](#)

[Pasos para realizar la detección masiva de dispositivos:](#)

[Paso 1:](#)

[Paso 2:](#)

[Paso 3:](#)

Introducción

Este documento describe diferentes maneras de sincronización de la configuración de ASA a CSM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Security Manager
- Dispositivo de seguridad adaptable

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Security Manager 4.25
- Dispositivo de seguridad adaptable

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El administrador de seguridad de Cisco ofrece servicios de supervisión y gestión centralizados para los dispositivos Cisco ASA.

Metodología de demostración

Este documento describe dos métodos u opciones diferentes para sincronizar la configuración de ASA a CSM.

- Detección de un solo dispositivo
- Redescubrimiento masivo de dispositivos

Detección de un solo dispositivo

La detección única solo se puede realizar si el dispositivo se agrega al inventario. Solo se puede realizar cuando el dispositivo tiene

- Configuraciones de contexto de seguridad para dispositivos ASA, PIX y FWSM que se ejecutan en modo de contexto múltiple.
- Configuraciones de sensores virtuales para dispositivos IPS.
- Información del módulo de servicio para dispositivos Catalyst.

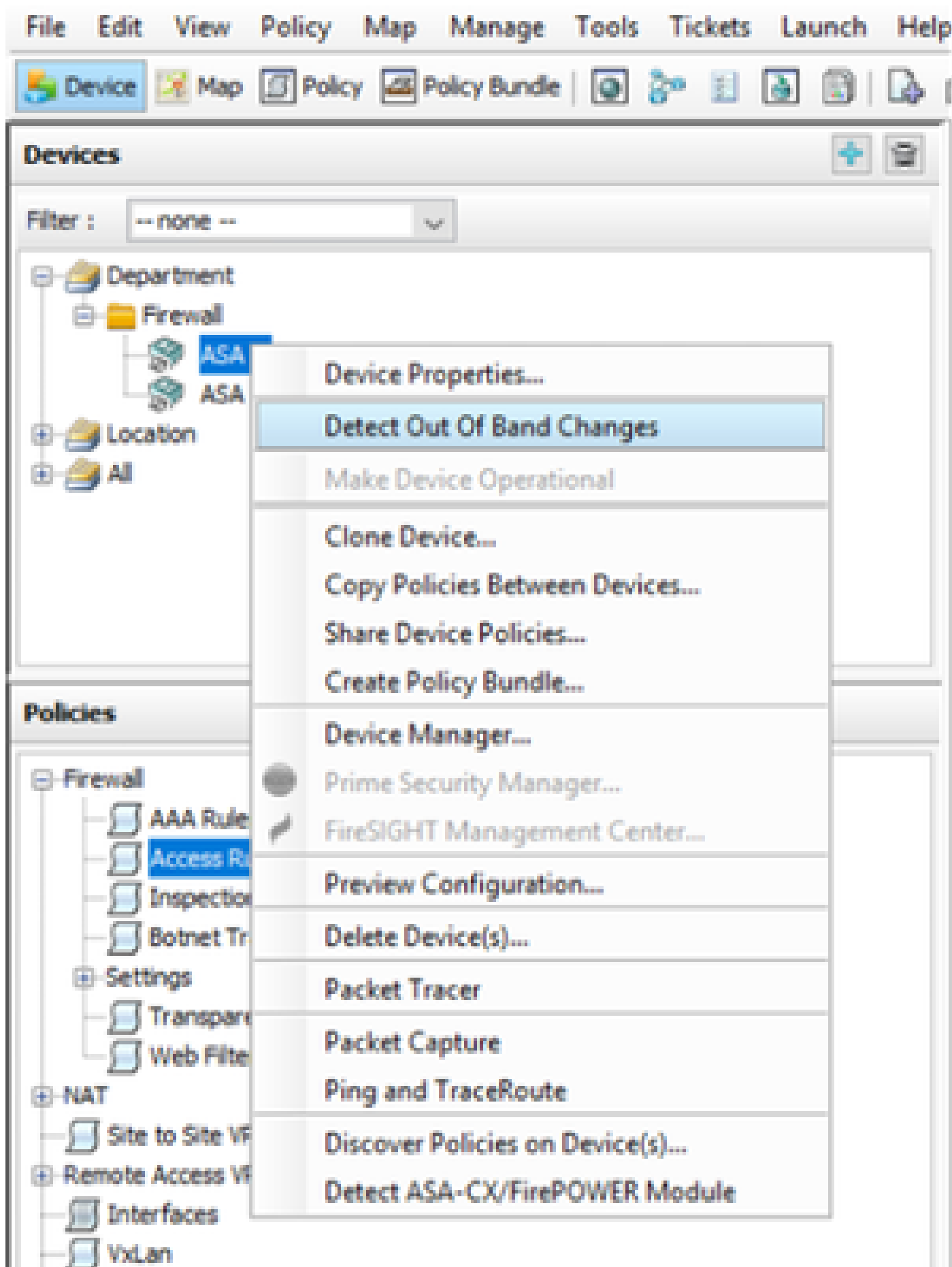
Pasos para realizar la detección de un solo dispositivo:

Puede realizar la detección de dispositivos cuando haya realizado cualquier cambio en la CLI del dispositivo o si el dispositivo se quitó y se volvió a agregar.

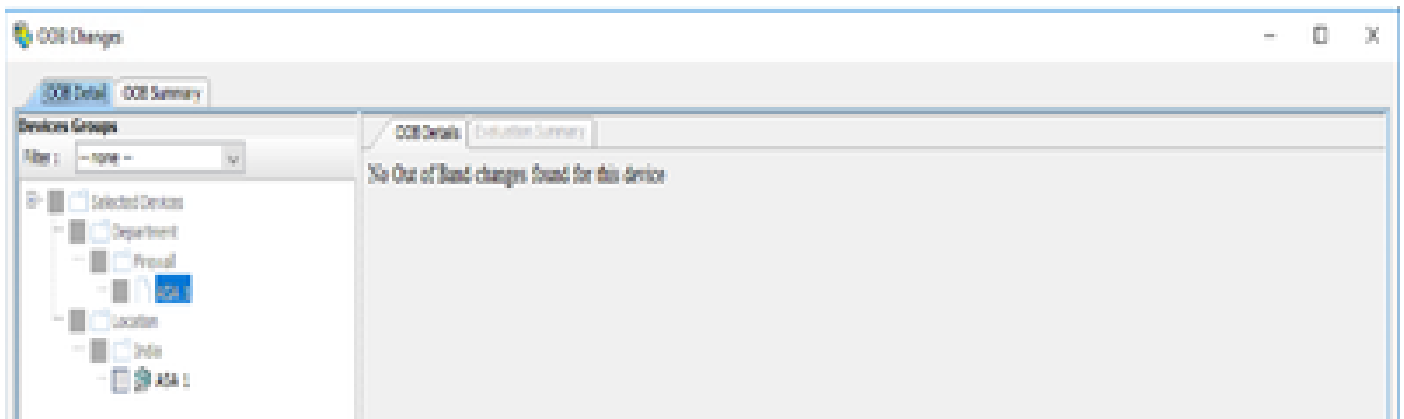
Para comprobar si los cambios pendientes aún no se han sincronizado , observe el ejemplo mencionado.

Haga clic con el botón derecho del ratón en el dispositivo correspondiente del panel del

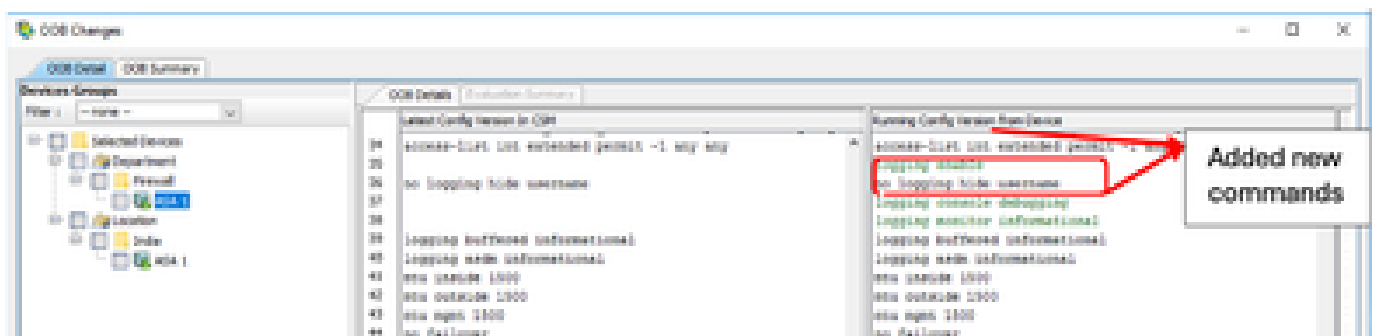
dispositivo y seleccione la opción Detectar cambios fuera de banda.



Si no hay cambios , la página se muestra como no se han encontrado cambios salientes para este dispositivo.



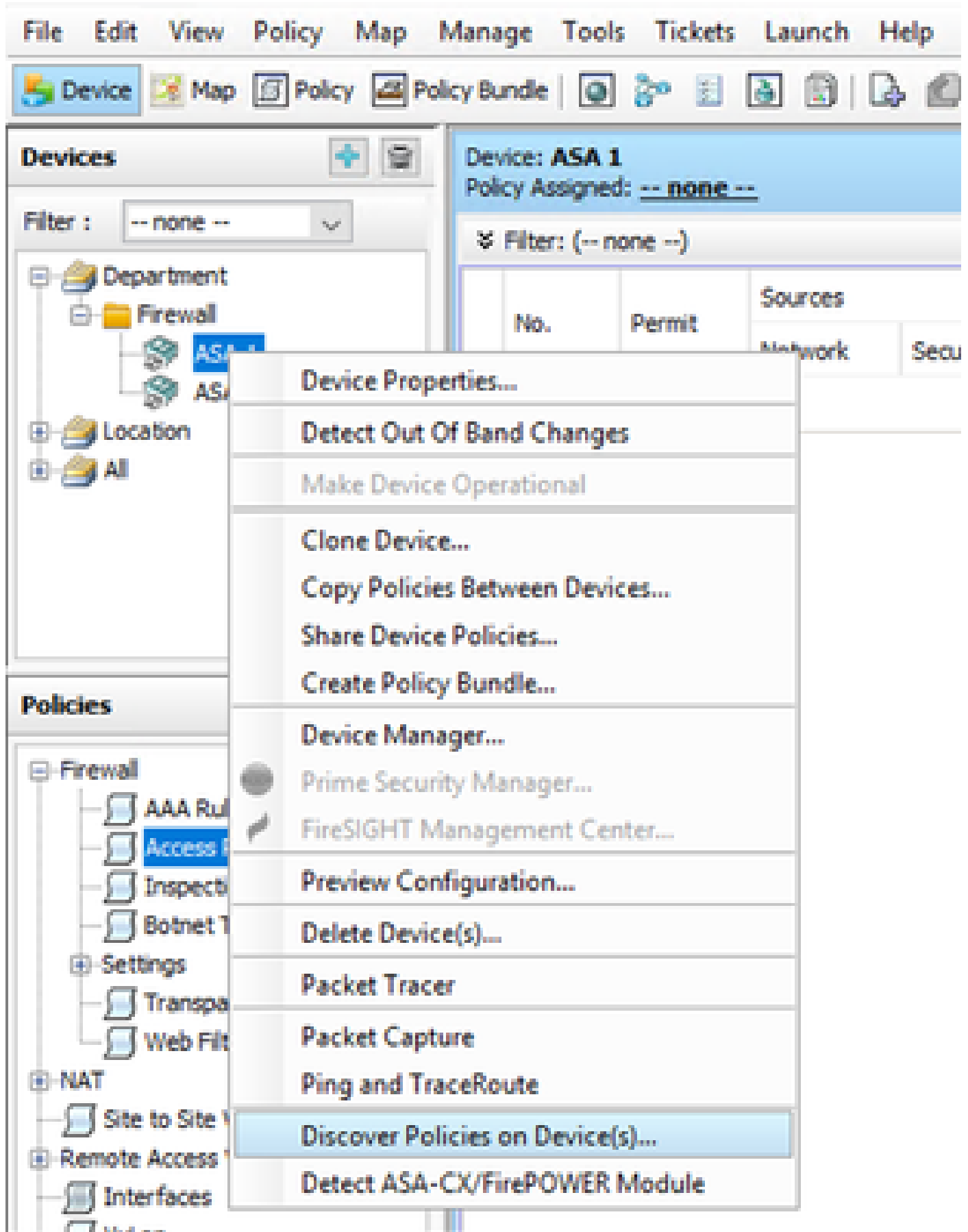
Si se han realizado cambios, las líneas se resaltan según la leyenda.



Pasos para realizar la detección de un solo dispositivo:

Paso 1:

Haga clic con el botón derecho del ratón en el nombre del dispositivo correspondiente del panel del dispositivo y elija la opción Detectar directivas en los dispositivos.



Paso 2:

Para el método de recuperación de un solo dispositivo, sólo puede ver el cuadro de diálogo Crear tarea de detección. En caso de que esté recibiendo un cuadro de diálogo de detección masiva , cierre y vuelva a abrirlo.

Dispone de 3 opciones para realizar la detección.

- Dispositivo en vivo: Obtiene la configuración del dispositivo en vivo , que está en la red.
- Archivo de configuración: Puede elegir el archivo de configuración y continuar con la detección.
- Configuración predeterminada de fábrica: restablece el dispositivo a las configuraciones predeterminadas. Este método se puede utilizar para dispositivos que sólo ejecutan el modo de contexto único o para dispositivos con contextos de seguridad individuales.

Create Discovery Task [X]

Discovery Task Name:

Discover From:

- Live Device
- Config File
- Factory Default Configuration

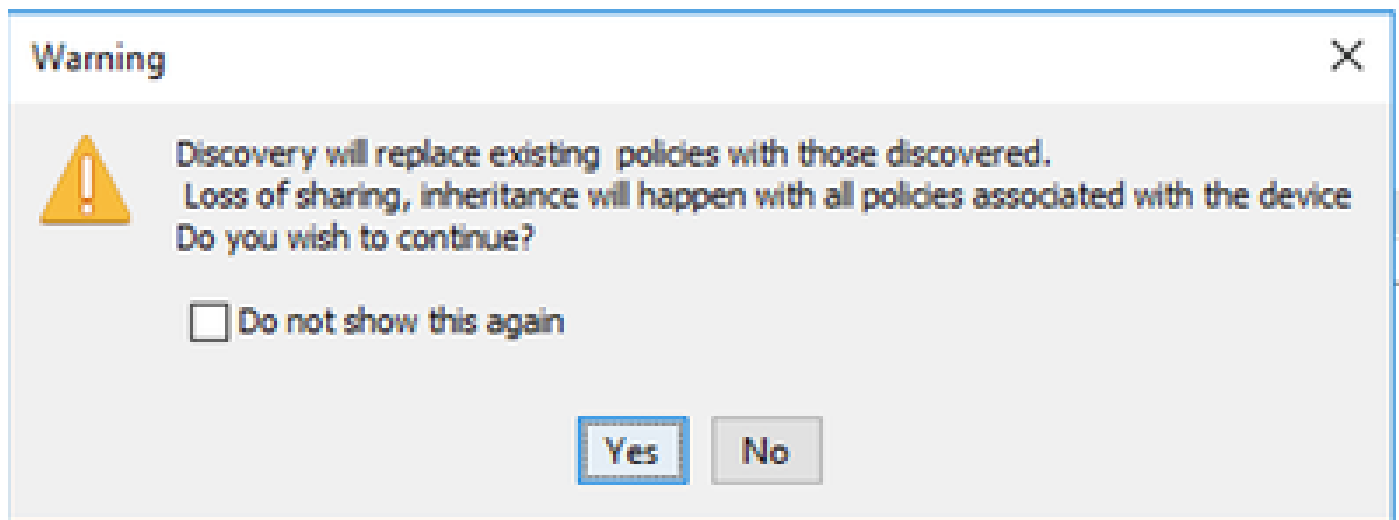
Config File:

Discover Policies for Security Contexts

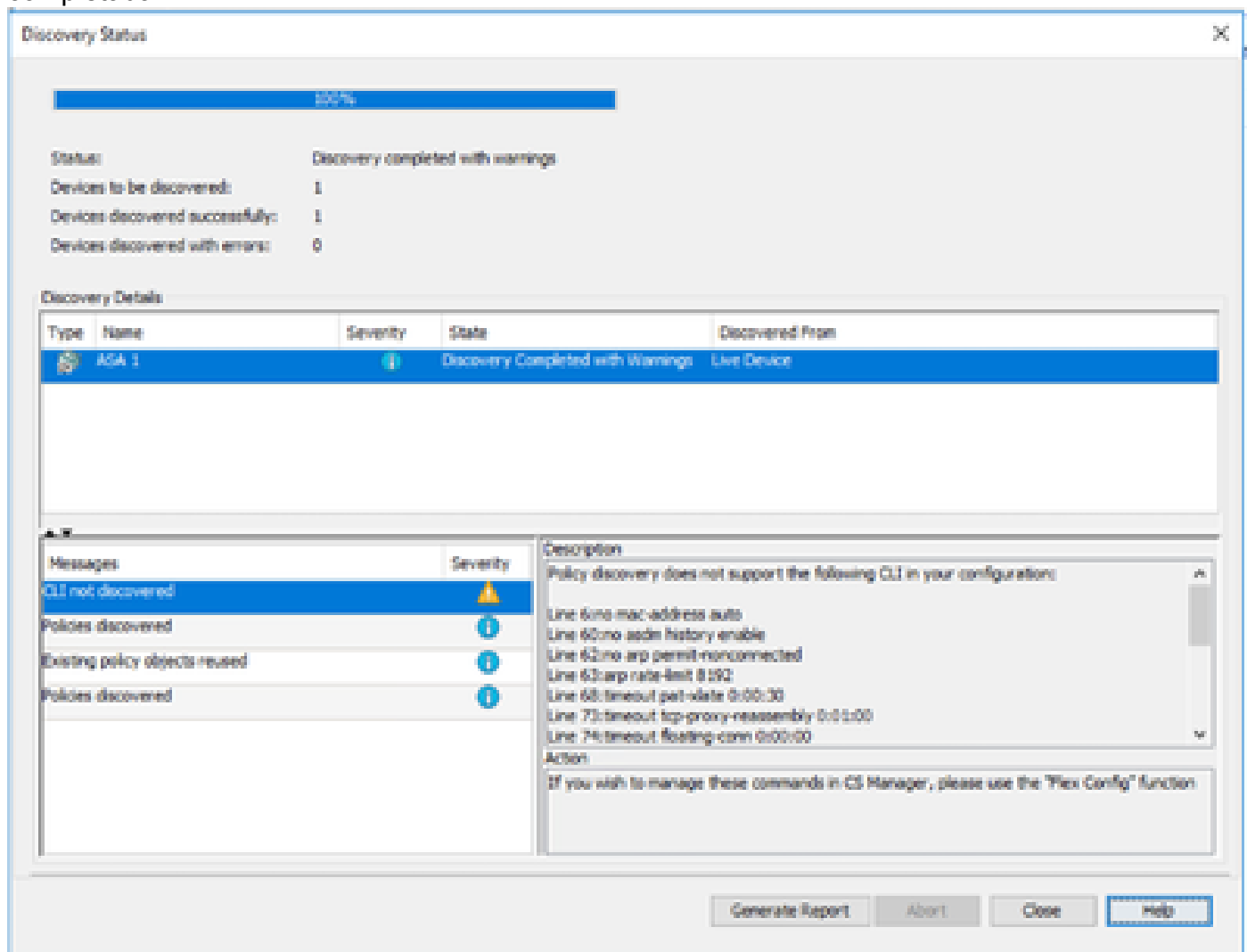
Policies To Discover
Select the policies to discover

- Detect ASA-CX/FirePOWER Module
- Inventory
- Platform Settings
- Firewall Services
- NAT Policies
- Routing Policies
- SSL Policy
- RA VPN Policies
- IPS

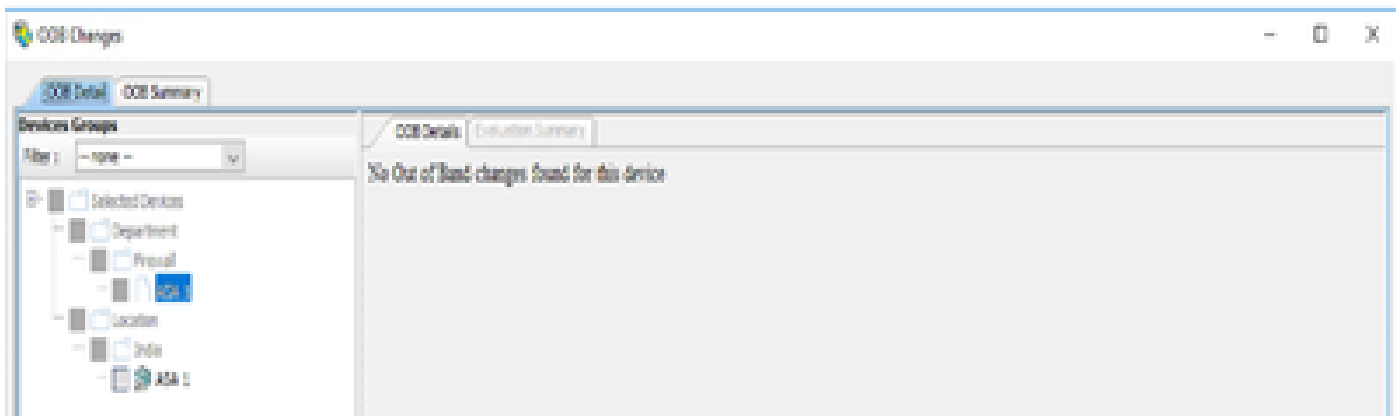
Asegúrese de conocer la topología de red y los cambios que pueden producirse en ella antes de continuar con la detección.



Una vez completada la detección, puede ver la pantalla emergente con el estado de Detección completada.



Y de los cambios fuera de banda tampoco puede tener ningún cambio.



Descubrimiento masivo de dispositivos

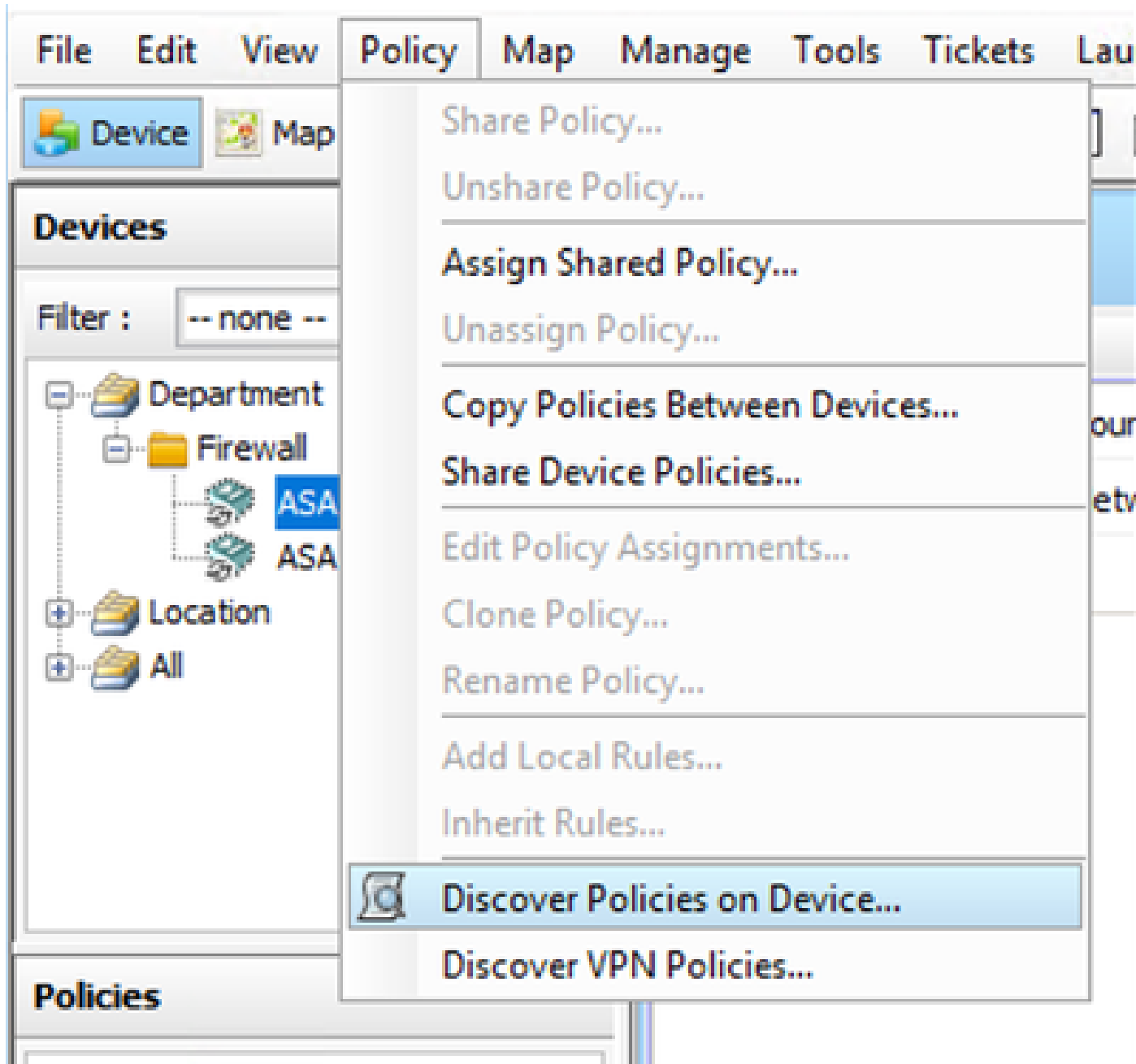
Para detectar políticas para varios dispositivos, puede llevar a cabo un redescubrimiento masivo. Es importante tener en cuenta que el redescubrimiento masivo se limita a los dispositivos activos , aquellos que están actualmente operativos y accesibles dentro de su red.

No puede realizar la detección masiva en el contexto de seguridad, sensores virtuales. Los módulos de servicio se pueden detectar si se seleccionan por separado.

Pasos para realizar la detección masiva de dispositivos:

Paso 1:

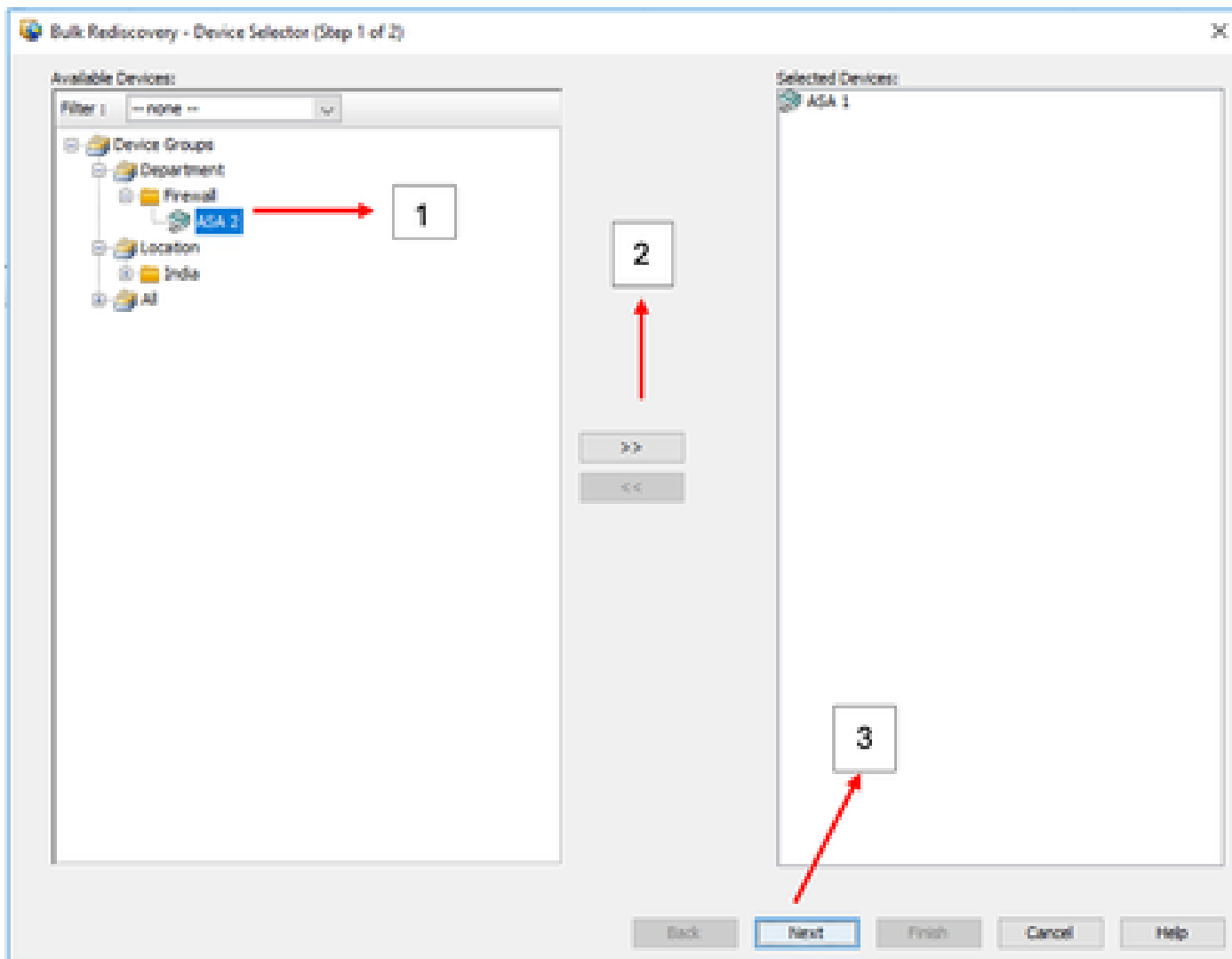
Vaya a Política > Detectar políticas en el dispositivo



Paso 2:

Si va a realizar una redetección masiva, sólo puede aparecer el cuadro de diálogo de redetección masiva.

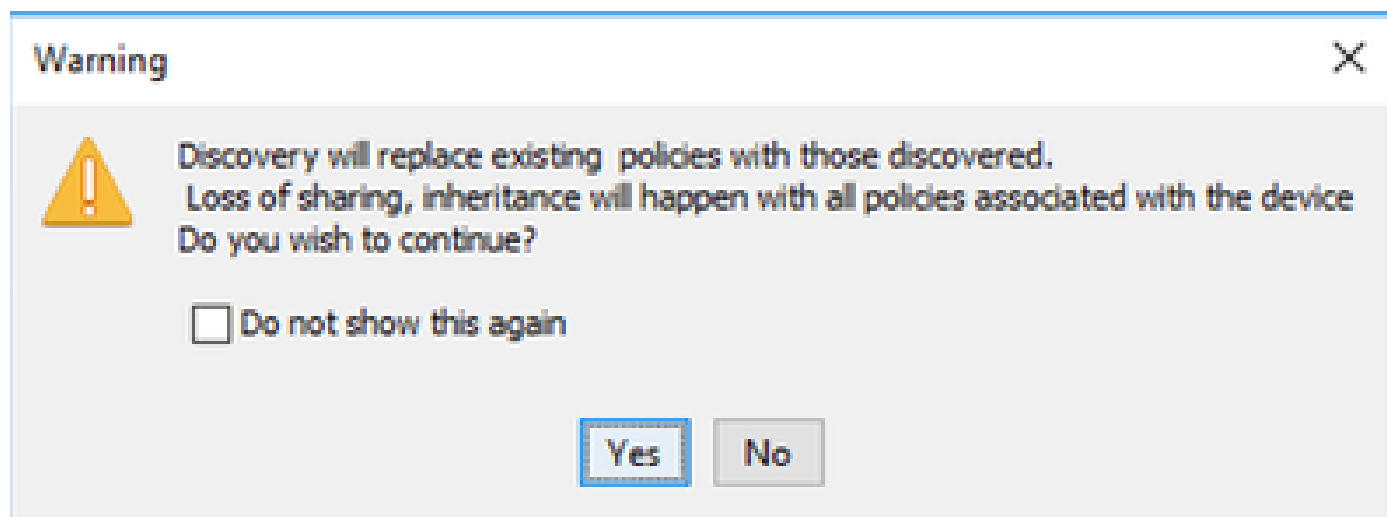
Desde los dispositivos disponibles en el panel izquierdo , elija la lista de dispositivos para los que desea detectar políticas y muévalos al lado derecho.



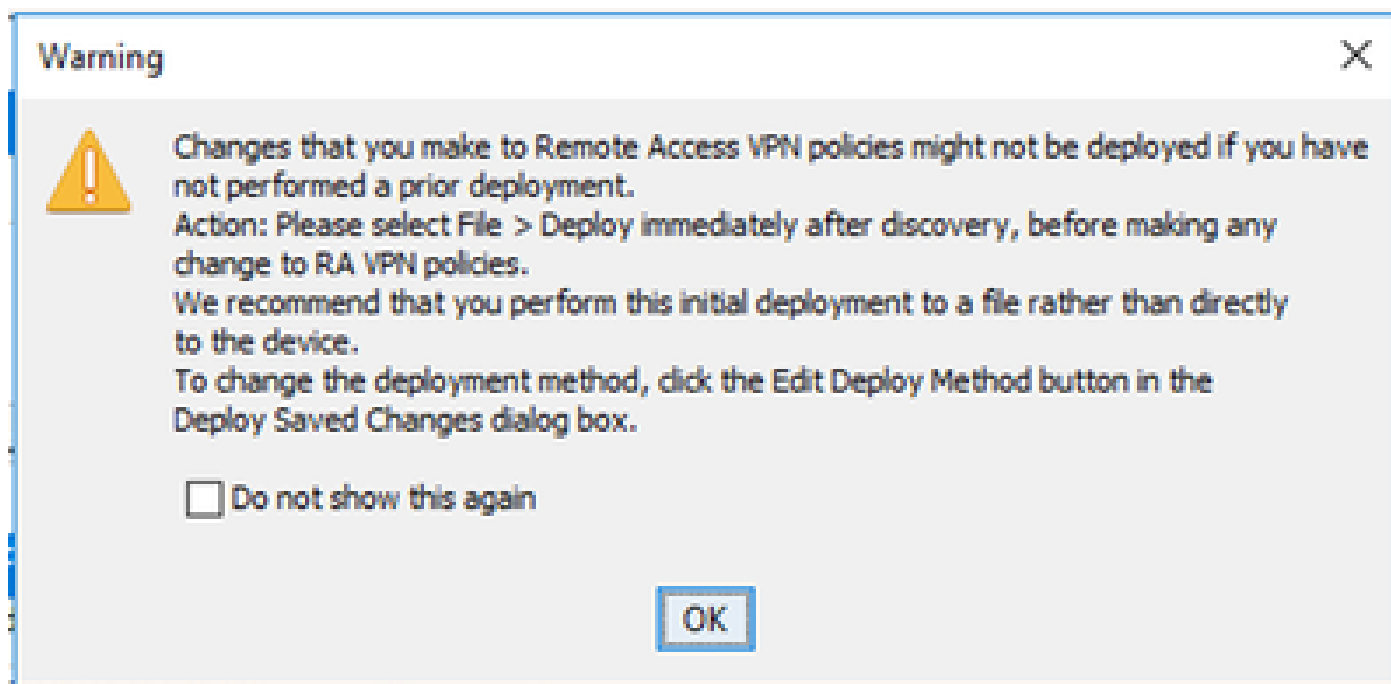
Paso 3:

Compruebe si todos los dispositivos seleccionados aparecen en la lista y haga clic en Finish (Finalizar) para continuar con el redescubrimiento masivo.


Asegúrese de conocer la topología de red y los cambios que pueden producirse en ella antes de continuar con la detección.



Una vez completada la detección, puede ver el ejemplo como



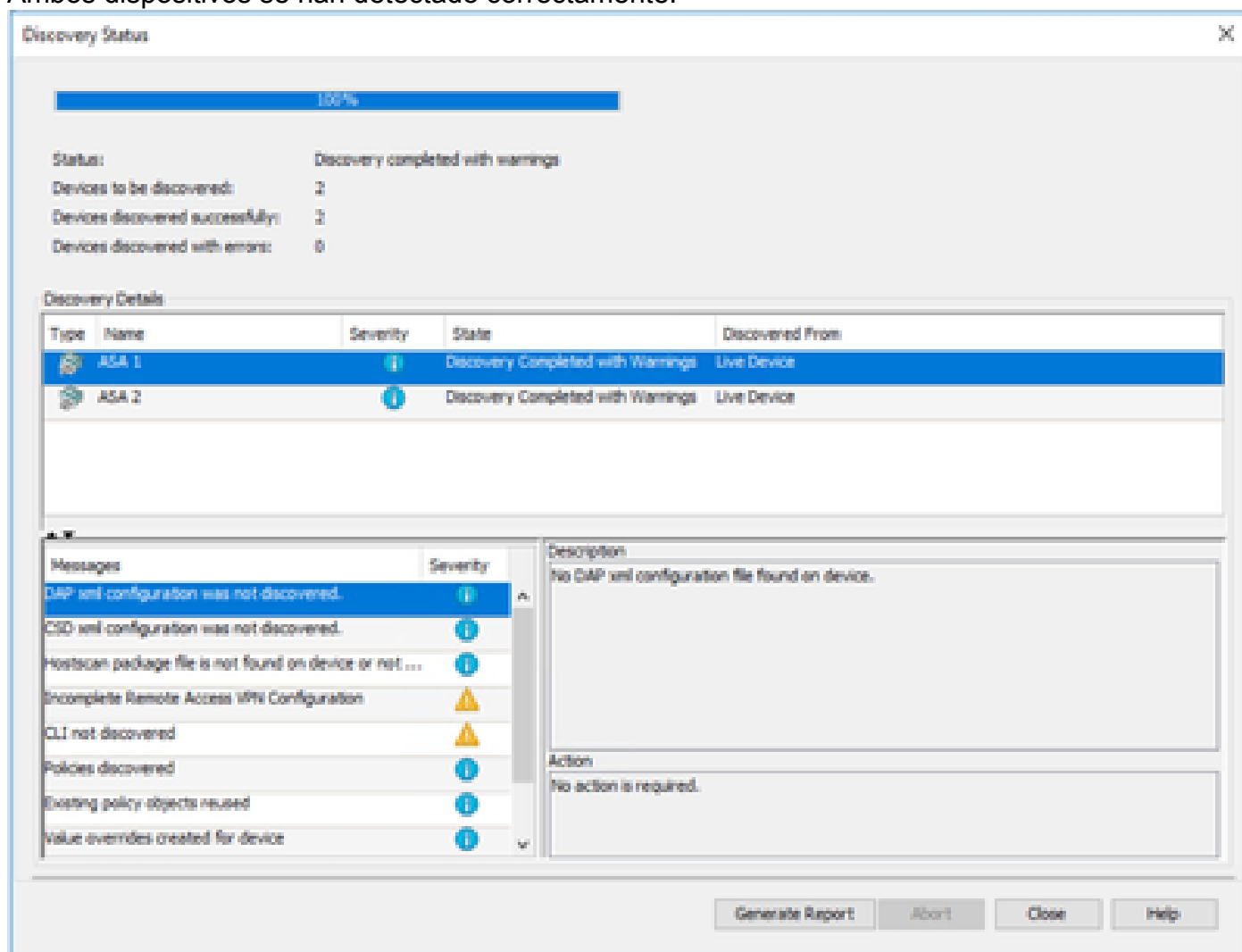
Warning [X]

 Changes that you make to Remote Access VPN policies might not be deployed if you have not performed a prior deployment.
Action: Please select File > Deploy immediately after discovery, before making any change to RA VPN policies.
We recommend that you perform this initial deployment to a file rather than directly to the device.
To change the deployment method, click the Edit Deploy Method button in the Deploy Saved Changes dialog box.

Do not show this again

OK

Ambos dispositivos se han detectado correctamente.



Discovery Status [X]

100%





Status: Discovery completed with warnings

Devices to be discovered: 2









Devices discovered successfully: 2

Devices discovered with errors: 0

Discovery Details

Type	Name	Severity	State	Discovered From
	ASA 1		Discovery Completed with Warnings	Live Device
	ASA 2		Discovery Completed with Warnings	Live Device

Messages

Messages	Severity
DAP xml configuration was not discovered.	
CSD xml configuration was not discovered.	
Hostscan package file is not found on device or not ...	
Incomplete Remote Access VPN Configuration	
CLI not discovered	
Policies discovered	
Existing policy objects reused	
Value overrides created for device	

Description

No DAP xml configuration file found on device.

Action

No action is required.

Generate Report Abort Close Help

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).