

配置从设备到安全管理器的同步

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[演示方法](#)

[单个设备发现](#)

[执行单设备发现的步骤：](#)

[执行单设备发现的步骤：](#)

[步骤 1：](#)

[步骤 2：](#)

[批量设备发现](#)

[执行批量设备发现的步骤：](#)

[步骤 1：](#)

[步骤 2：](#)

[步骤 3：](#)

简介

本文档介绍从ASA到CSM的不同配置同步方式。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Security Manager
- 自适应安全设备

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科安全管理器4.25
- 自适应安全设备

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

思科安全管理器为Cisco ASA设备提供集中管理和监控服务。

演示方法

本文档介绍将配置从ASA同步到CSM的两种不同方法或选项。

- 单个设备发现
- 批量设备重新发现

单个设备发现

仅当设备已添加到资产中时，才能执行单一发现。仅当设备具有

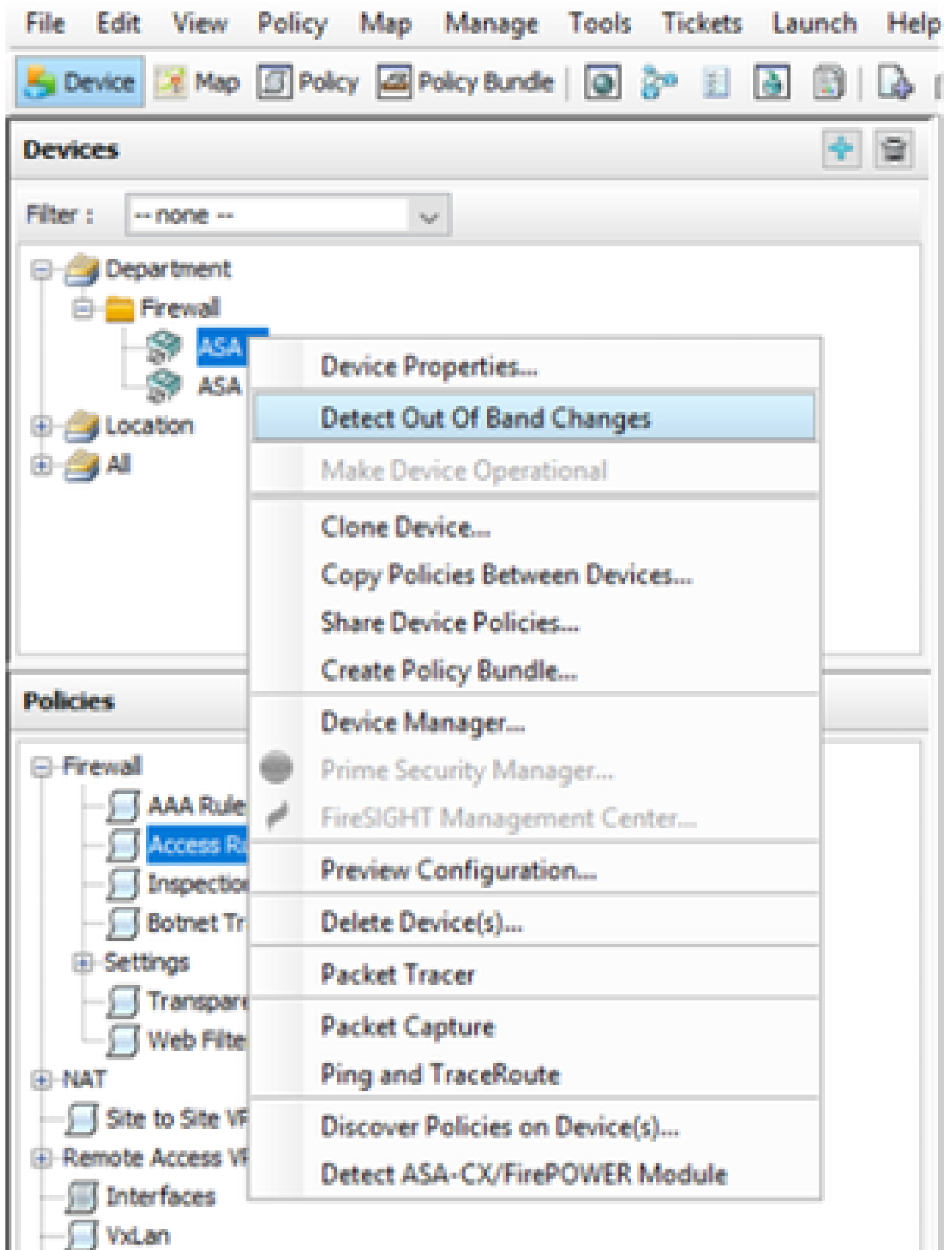
- 在多情景模式下运行的ASA、PIX和FWSM设备的安全情景配置。
- IPS设备的虚拟传感器配置。
- Catalyst设备的服务模块信息。

执行单设备发现的步骤：

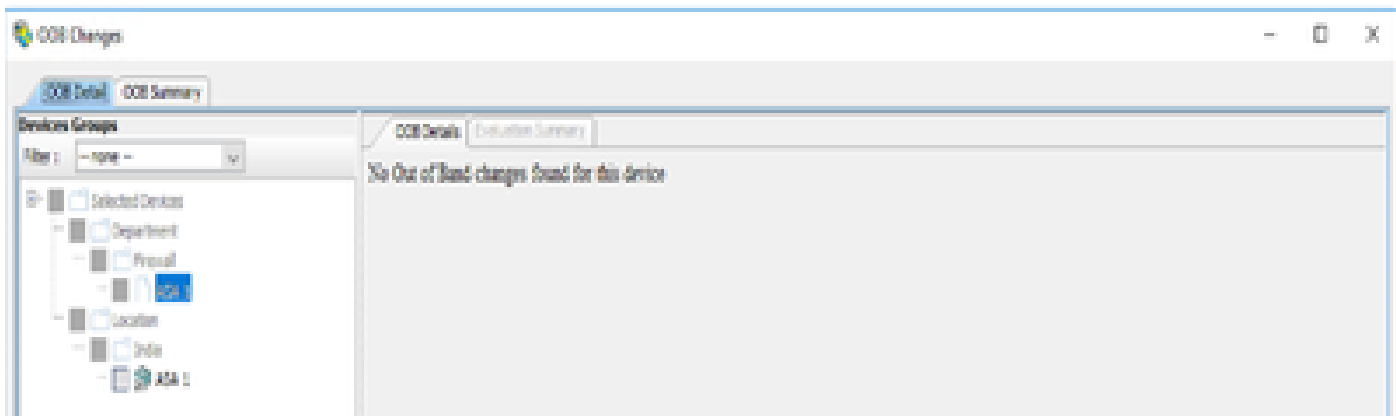
当您已对设备CLI执行任何更改或者设备已移除并添加回时，可以执行设备发现。

要检查是否有任何待执行的更改尚未同步（请参阅前面提到的示例），请执行以下操作：

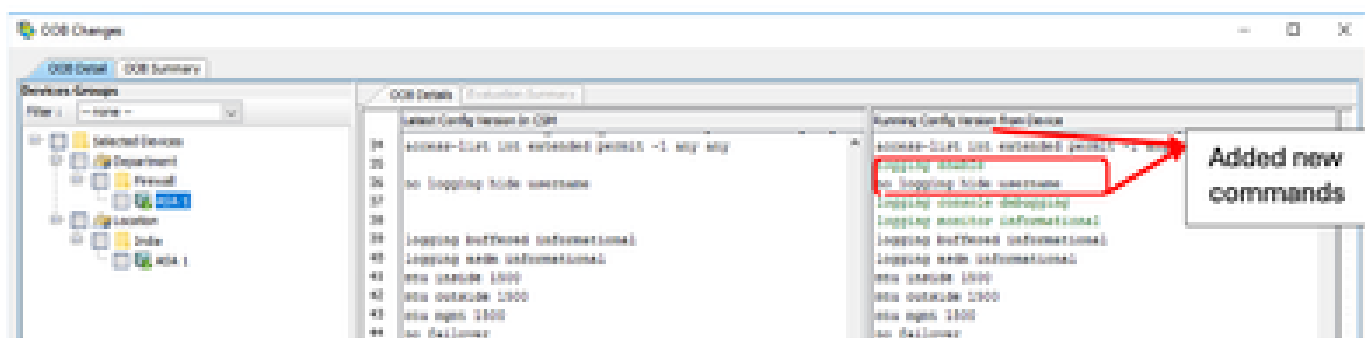
在设备窗格中右键单击相应的设备，然后选择检测带外更改选项。



如果未发生更改（例如，更改未生效），则页面会显示为“未找到此设备的出站更改”。



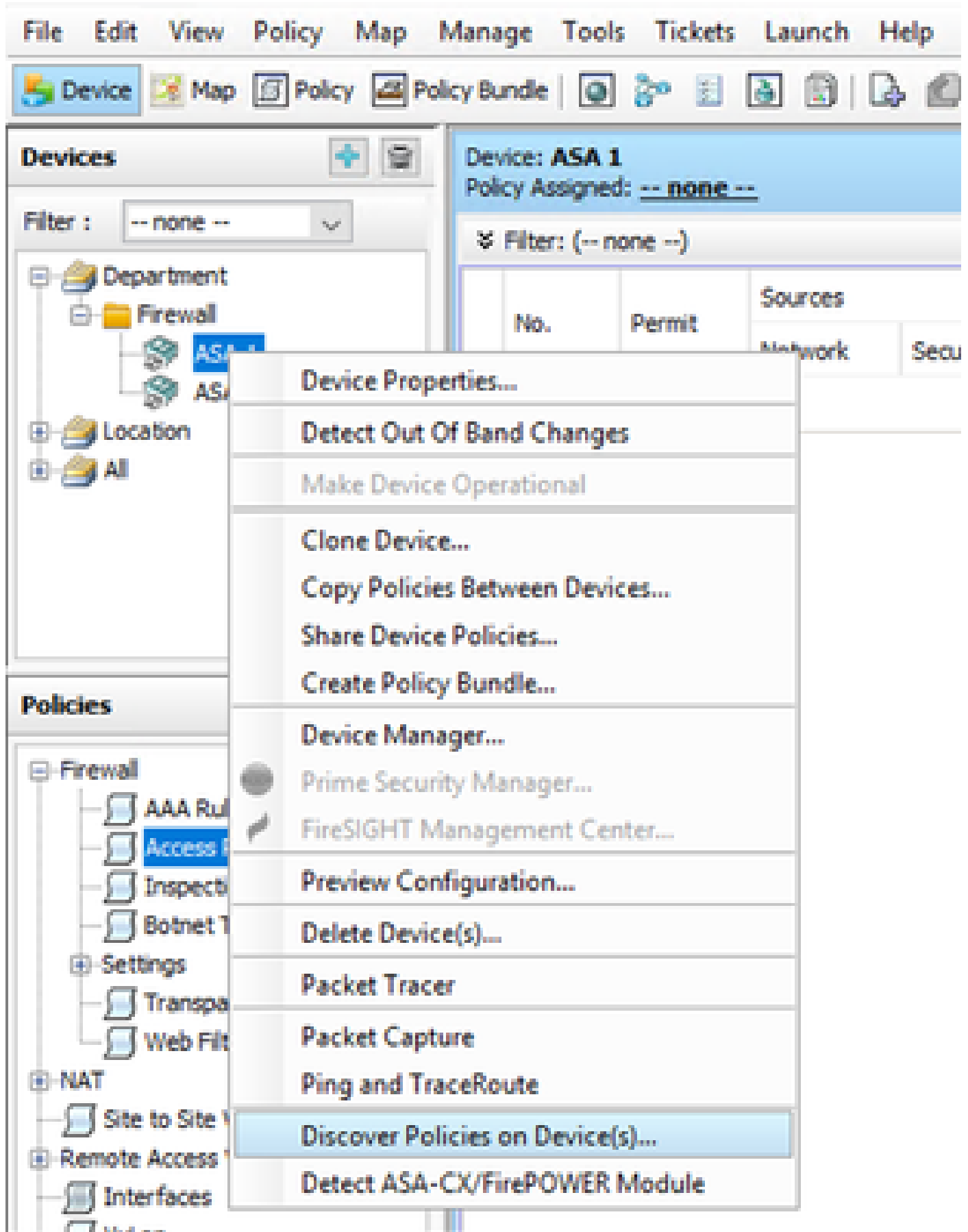
如果进行了任何更改（例如，更改了图例），则这些行会根据图例突出显示。



执行单设备发现的步骤：

步骤 1：

右键点击来自设备窗格的各个设备名称，然后选择选项Discover policies on Device(s)。



步骤 2 :

对于单设备恢复方法，只能看到Create Discovery Task对话框。如果您正在获取批量发现对话框（请参阅本文档的“配置”），请关闭并再次打开它。

您有3个选项来执行发现。

- 实时设备 -从网络中的实时设备（本地或远程）获取配置。
- 配置文件- 您可以选择配置文件并继续执行发现。
- 出厂默认配置 -将设备重置为默认配置。此方法可用于仅运行单情景模式的设备，或用于具有单个安全情景的设备。

Create Discovery Task

Discovery Task Name:

Discover From:

- Live Device
- Config File
- Factory Default Configuration

Config File:

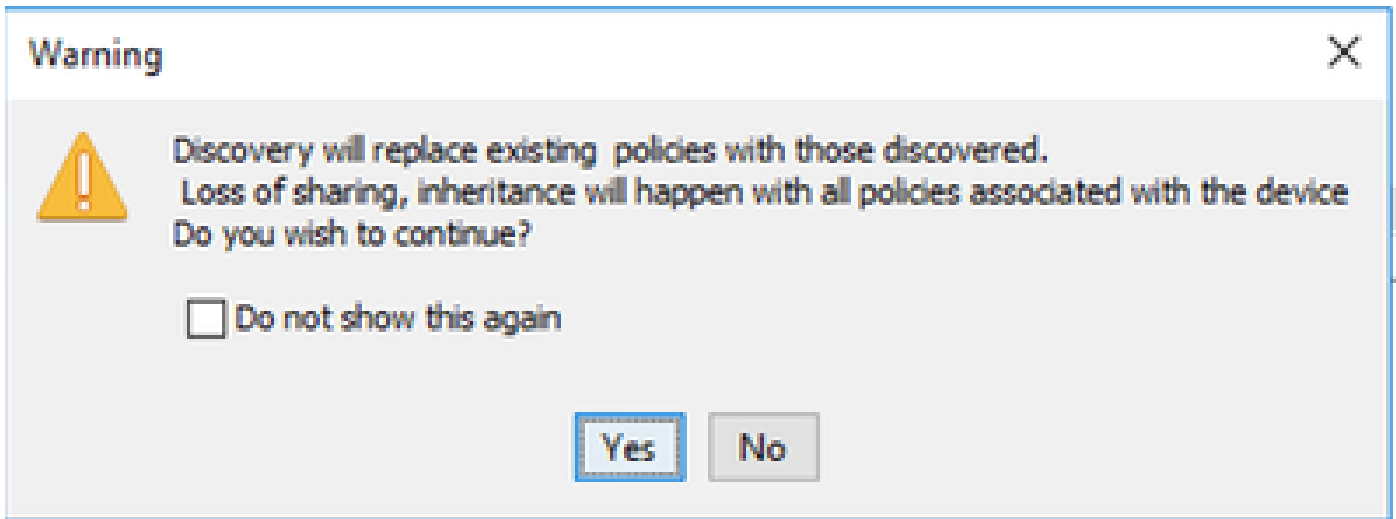
Discover Policies for Security Contexts

Policies To Discover

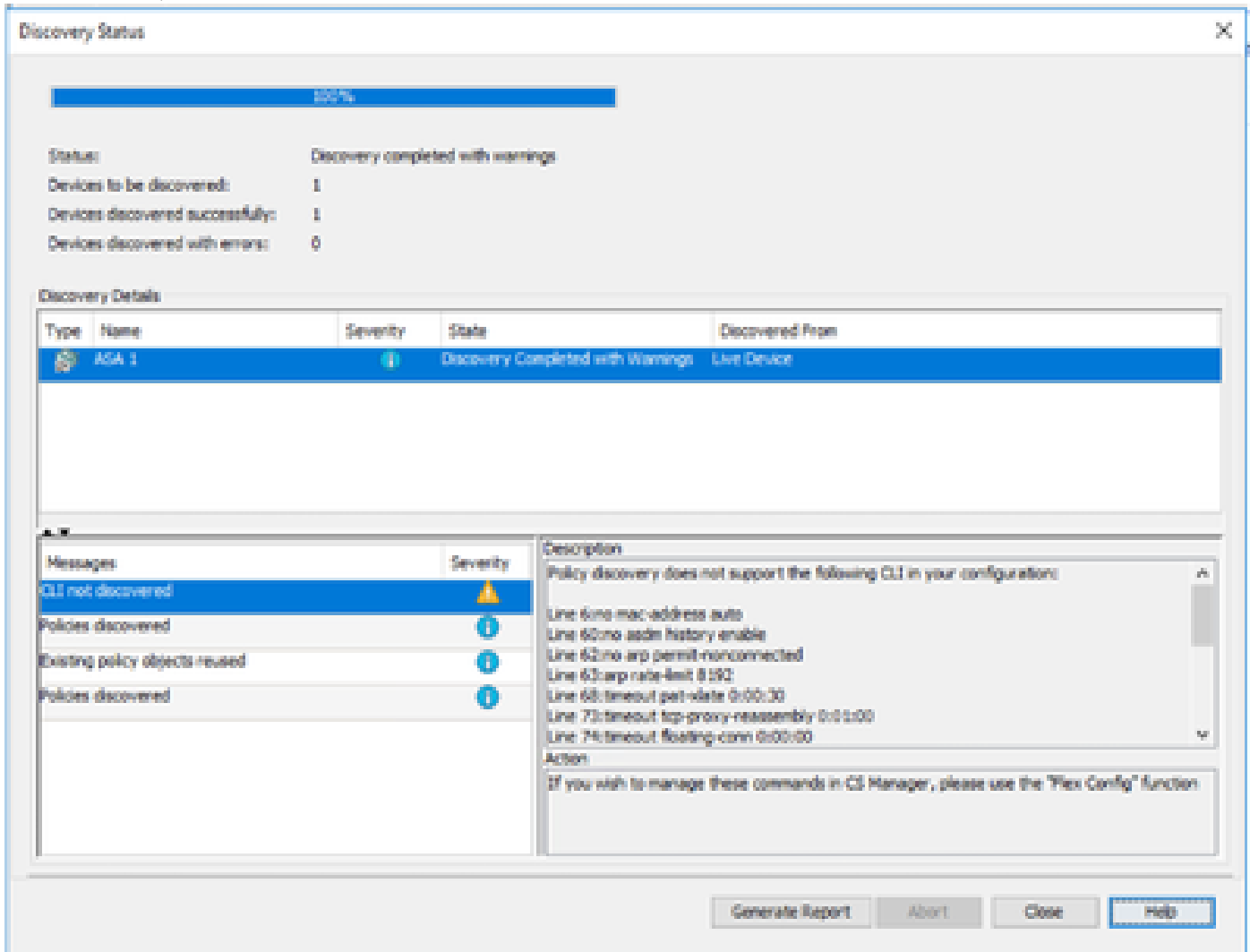
Select the policies to discover

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

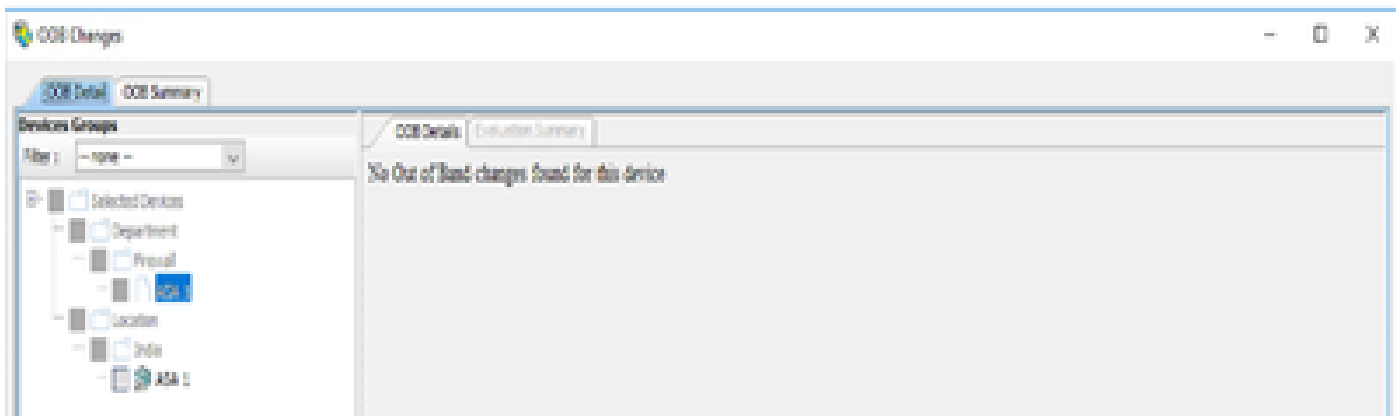
继续进行发现之前，请确保您了解网络拓扑和网络中可能发生的更改。



发现完成后，您会看到状态为发现完成的弹出屏幕。



并且从带外更改中也不能有任何更改。



批量设备发现

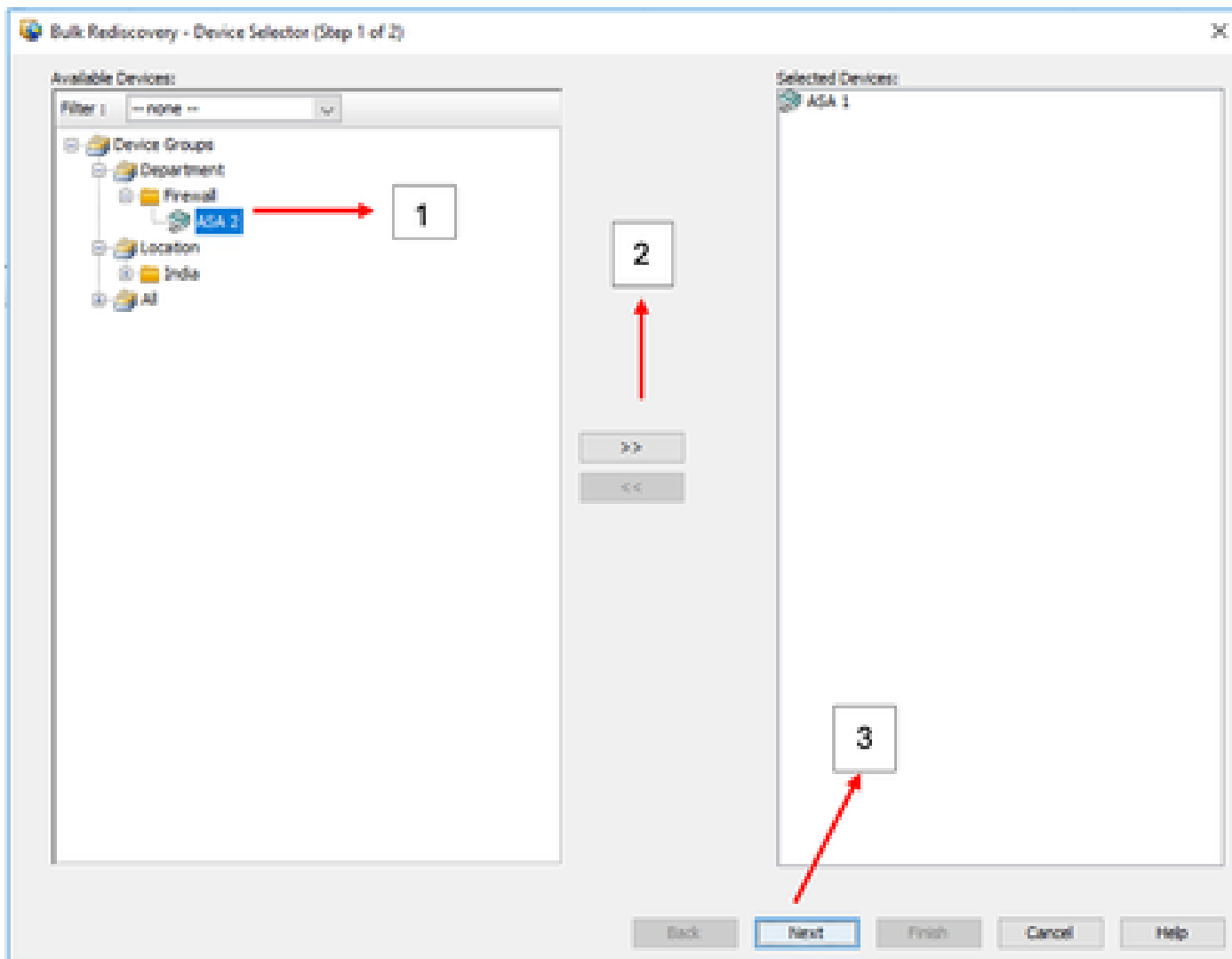
要发现多个设备的策略，可以执行批量重新发现。请务必注意，批量重新发现仅限于当前运行并在您的网络中可访问的设备。

您无法在安全情景（虚拟传感器）上执行批量发现。服务模块可单独选择进行发现。

执行批量设备发现的步骤：

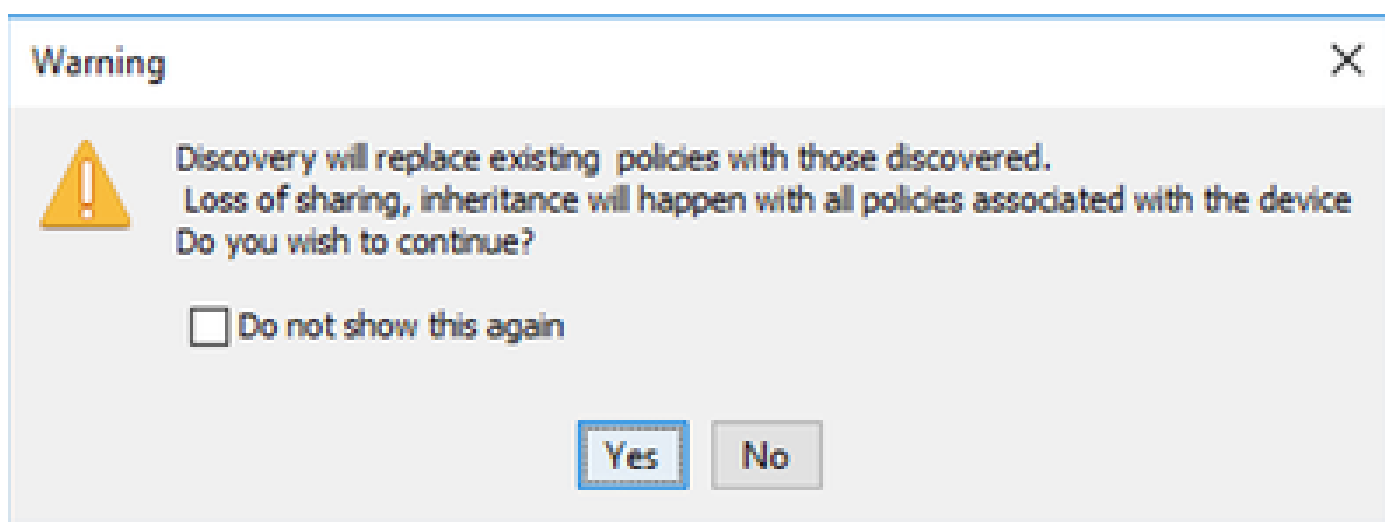
步骤 1：

导航到设备上的策略>发现策略




步骤 3 :

验证是否已列出所有选定的设备，并点击Finish以继续进行批量重新发现。
继续进行发现之前，请确保您了解网络拓扑和网络中可能发生的更改。



发现完成后，您可以看到

Warning ✕

 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

两个设备都已成功发现。

Discovery Status ✕

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	Severity	Description
DAP xml configuration was not discovered.		No DAP xml configuration file found on device.
CSD xml configuration was not discovered.		
Hostscan package file is not found on device or net ...		
Incomplete Remote Access VPN Configuration		
CLI not discovered		
Policies discovered		
Existing policy objects reused		
Value overrides created for device		

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。