将FTD从一个FMC迁移到另一个FMC

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 配置

验证

故障排除

相关信息

简介

本文档介绍如何在Firepower管理中心之间迁移思科Firepower威胁防御(FTD)设备。

先决条件

开始迁移过程之前，请确保满足以下前提条件：

- 访问源和目标FMC。
- FMC和FTD的管理凭证。
- 备份当前FMC配置。
- 确保运行与目标FMC兼容的软件版本的FTD设备。
- 确保目标FMC的版本与源FMC的版本相同。

要求

- 两个FMC必须运行兼容的软件版本。
- FTD设备和两个FMC之间的网络连接。
- 目标FMC上足够的存储和资源，以容纳FTD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Firepower威胁防御虚拟(FTDv)版本7.2.5

Firepower管理中心虚拟(FMCv)版本7.2.5

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

将FTD设备从一个FMC迁移到另一个FMC涉及多个步骤，包括从源FMC注销设备、准备目标FMC以及重新注册设备。此过程可确保正确传输和应用所有策略和配置。

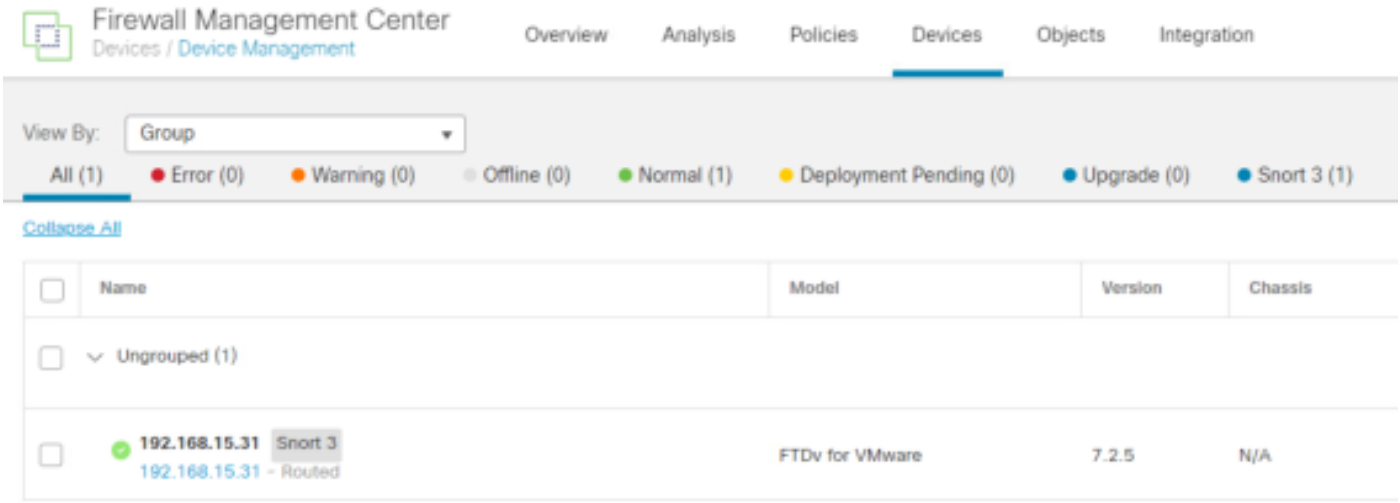
配置

配置

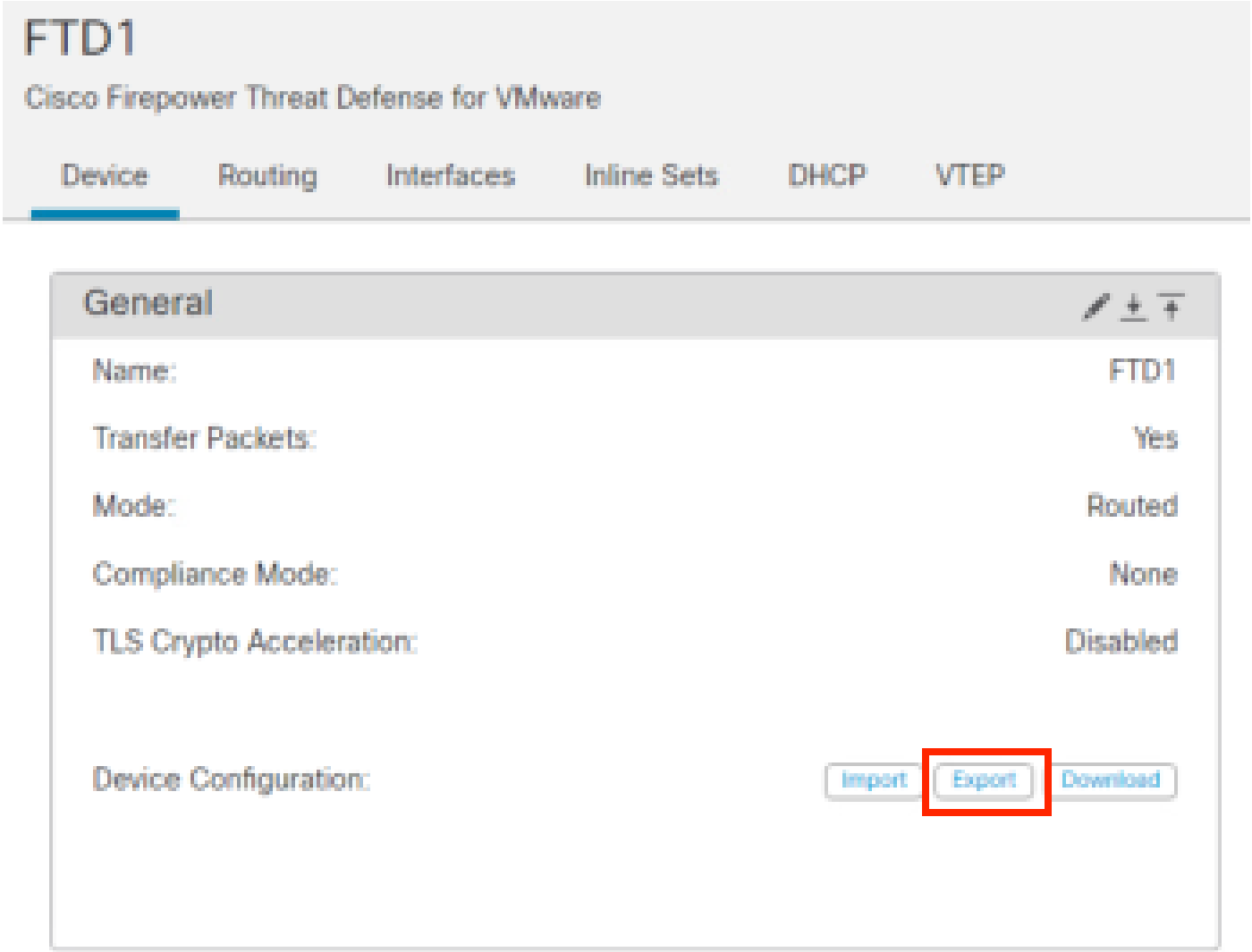
1. 登录源FMC。



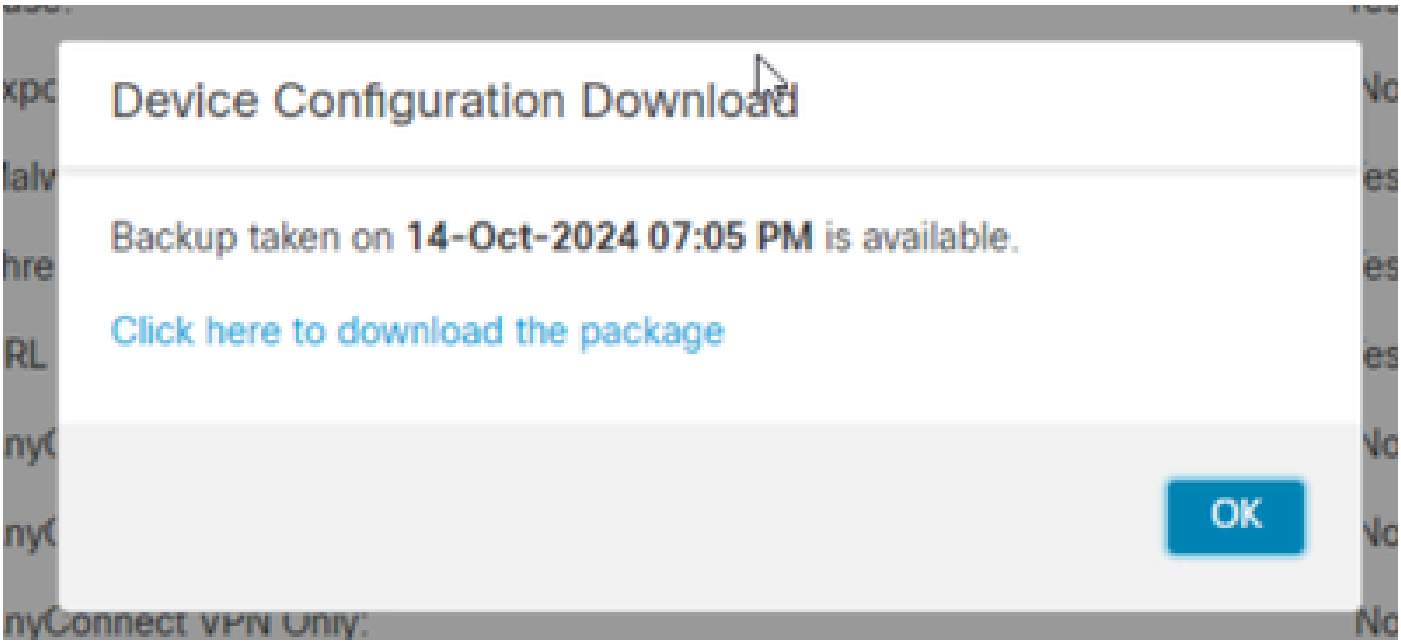
2. 导航到设备>设备管理，选择要迁移的设备。

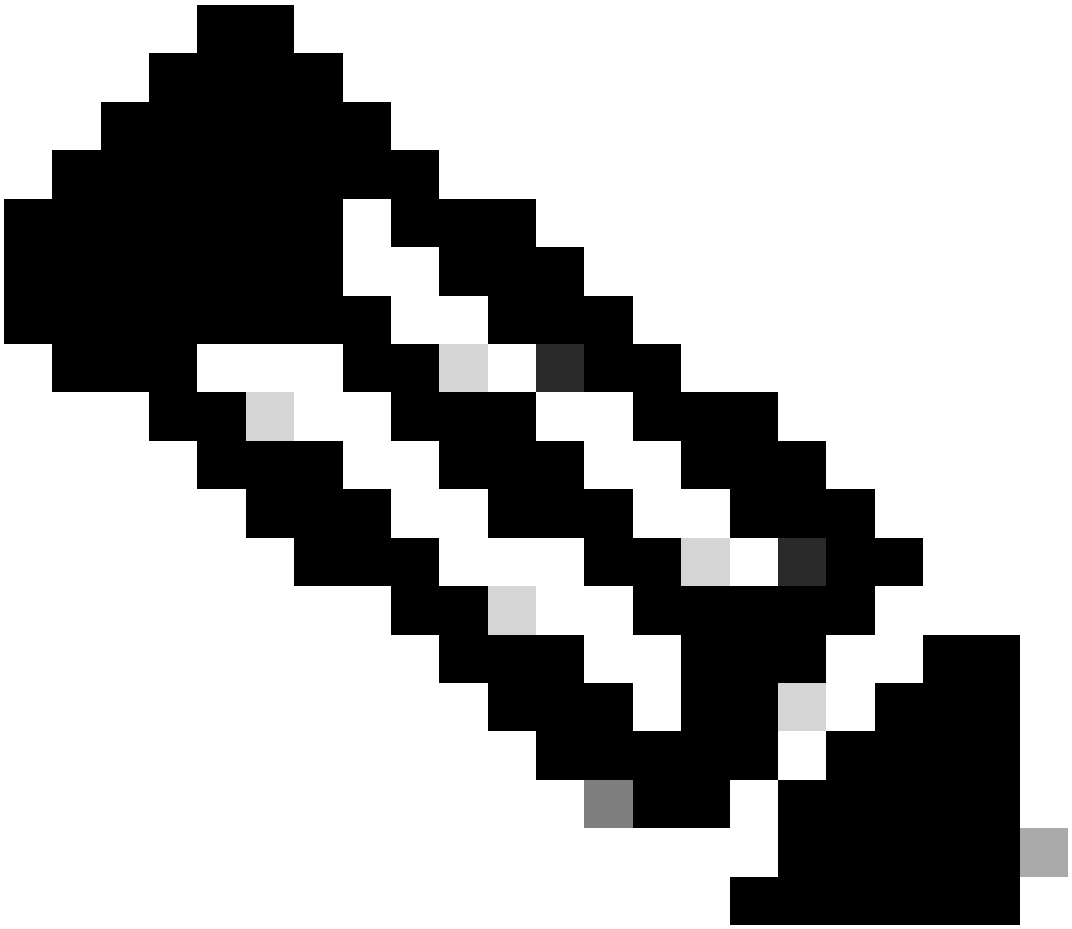


3. 在“设备”部分中，导航至设备，然后点击导出以导出您的设备设置。



4. 导出配置后，必须下载该配置。

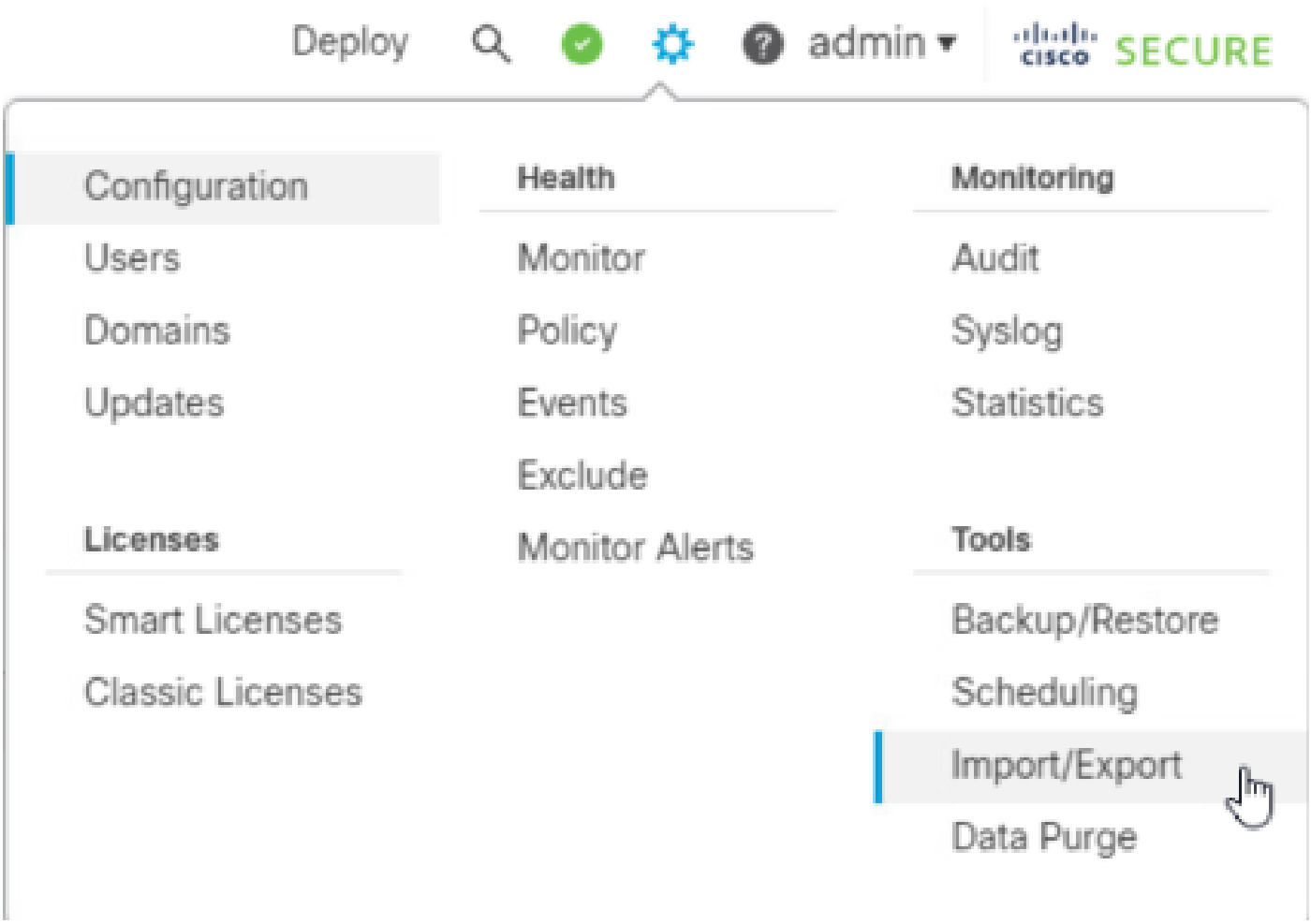


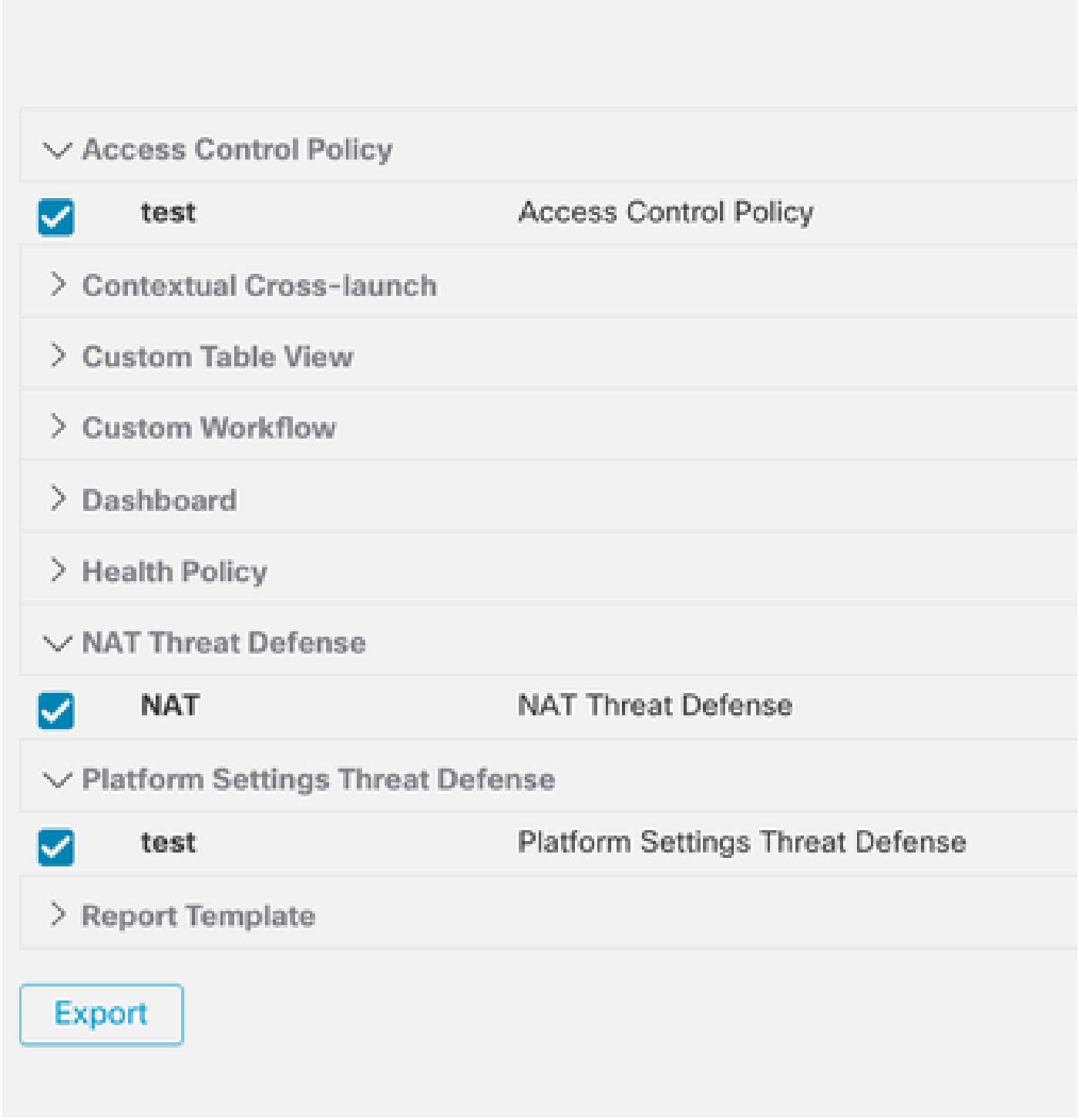


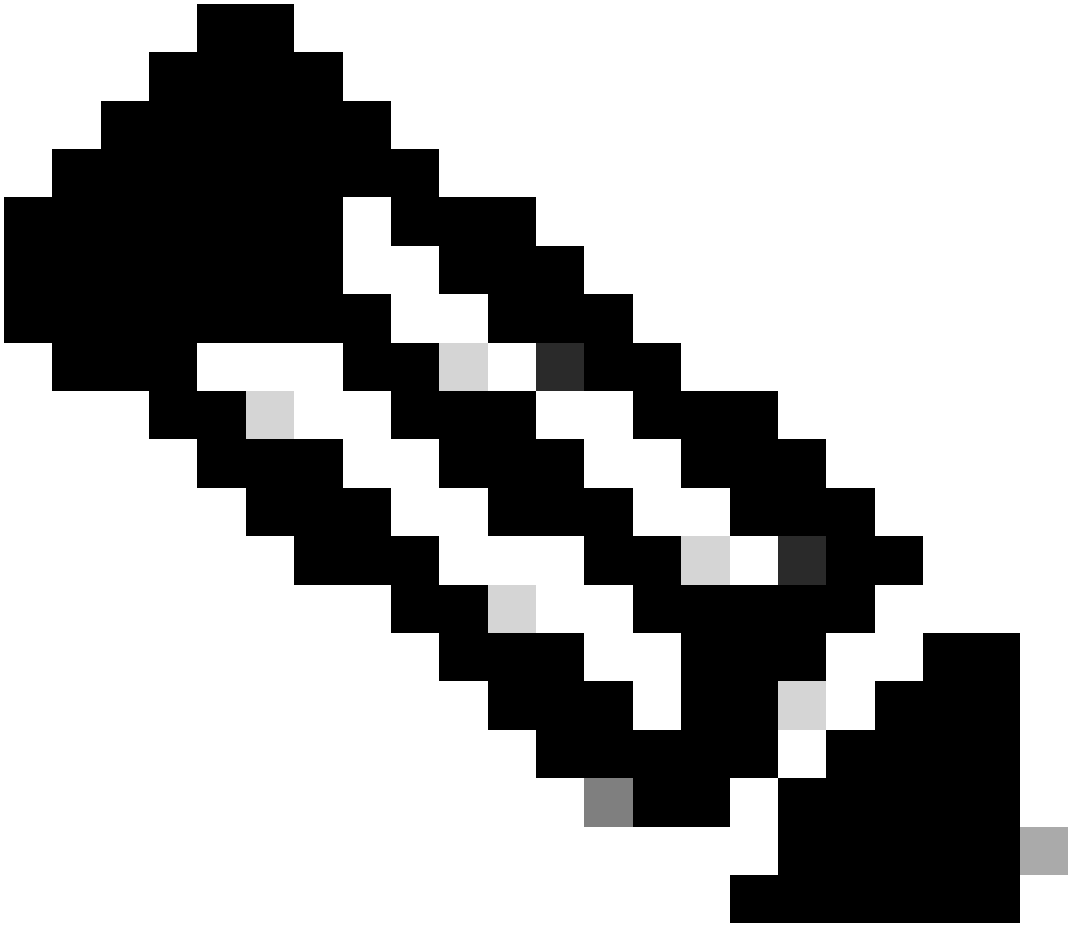
注意：下载的文件必须包含.SFO扩展名，并且包含IP地址、安全区域、静态路由和其他设

备设置等设备配置信息。

5. 您必须导出与设备关联的策略，导航到系统>工具>导入/导出，选择要导出的策略，然后单击导出。

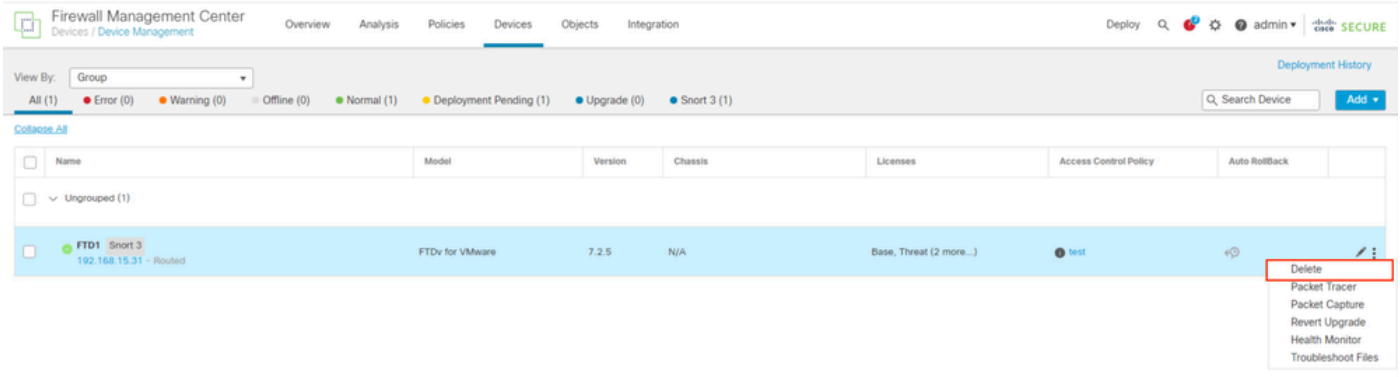



Access Control Policy
test
Access Control Policy
Contextual Cross-launch
Custom Table View
Custom Workflow
Dashboard
Health Policy
NAT Threat Defense
NAT
NAT Threat Defense
Platform Settings Threat Defense
test
Platform Settings Threat Defense
Report Template
Export



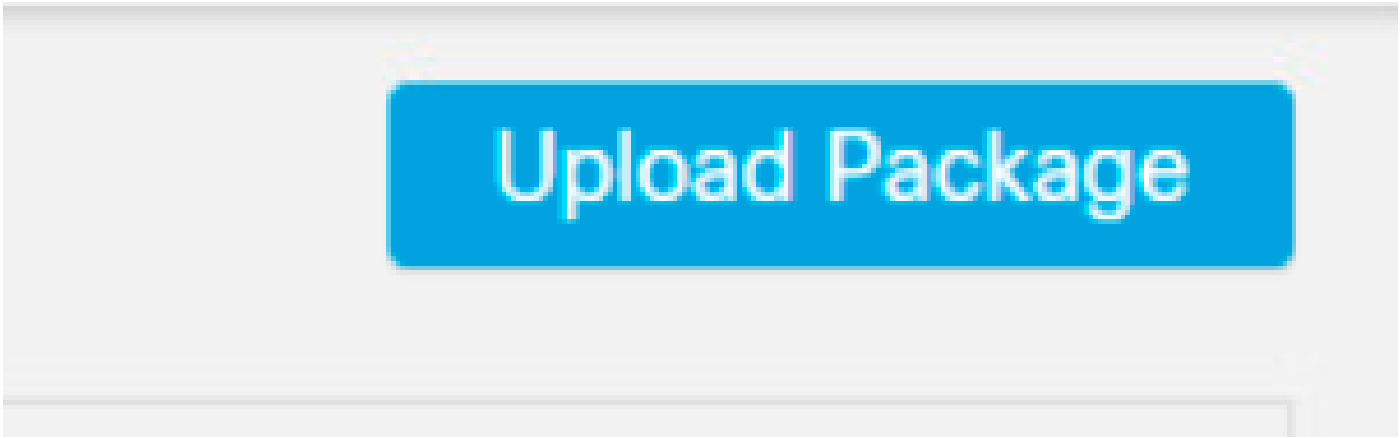
注意：请确保已成功下载.SFO文件。点击导出后，下载将自动完成。此文件包含访问控制策略、平台设置、NAT策略以及迁移不可或缺的其他策略，因为它们不是与设备配置一起导出的，必须手动上传到目标FMC。

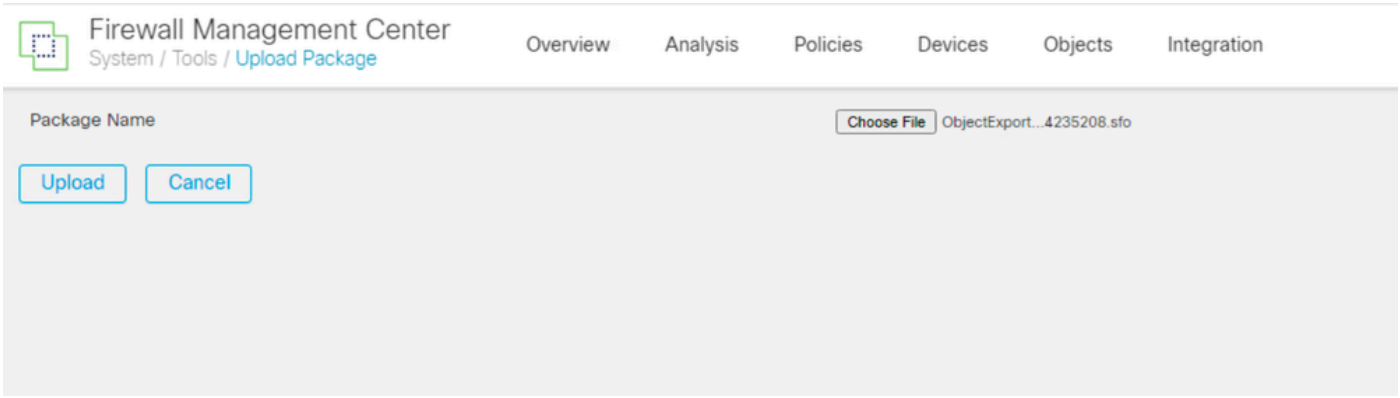
6. 从FMC取消注册FTD设备，导航到设备>设备管理，点击右侧的三个垂直点，然后选择删除。



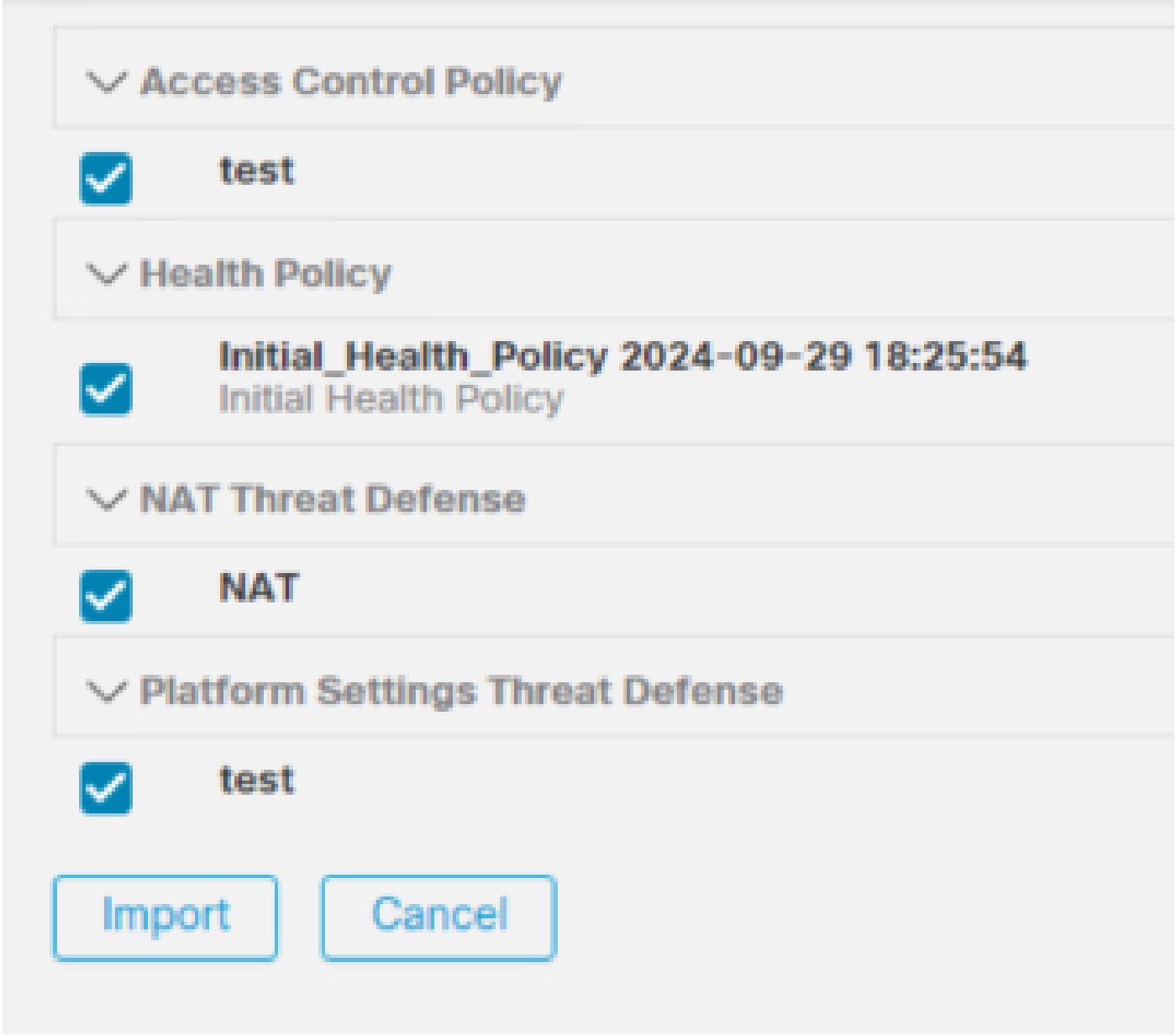
7. 准备目标FMC：

- 登录到目标FMC。
- 通过导入您在第5步中下载的源FMC策略，确保FMC已准备好接受新设备。导航到系统>工具>导入/导出，然后单击上传数据包。上传要导入的文件并点击上传。

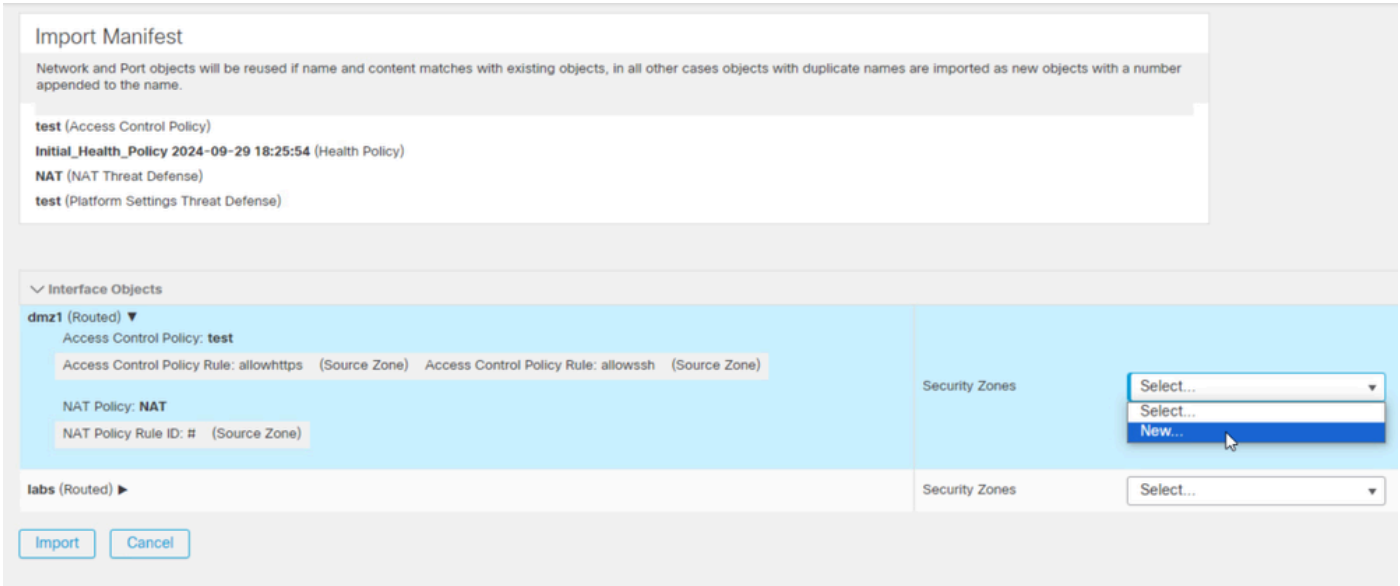




8. 选择要导入目标FMC中的策略。

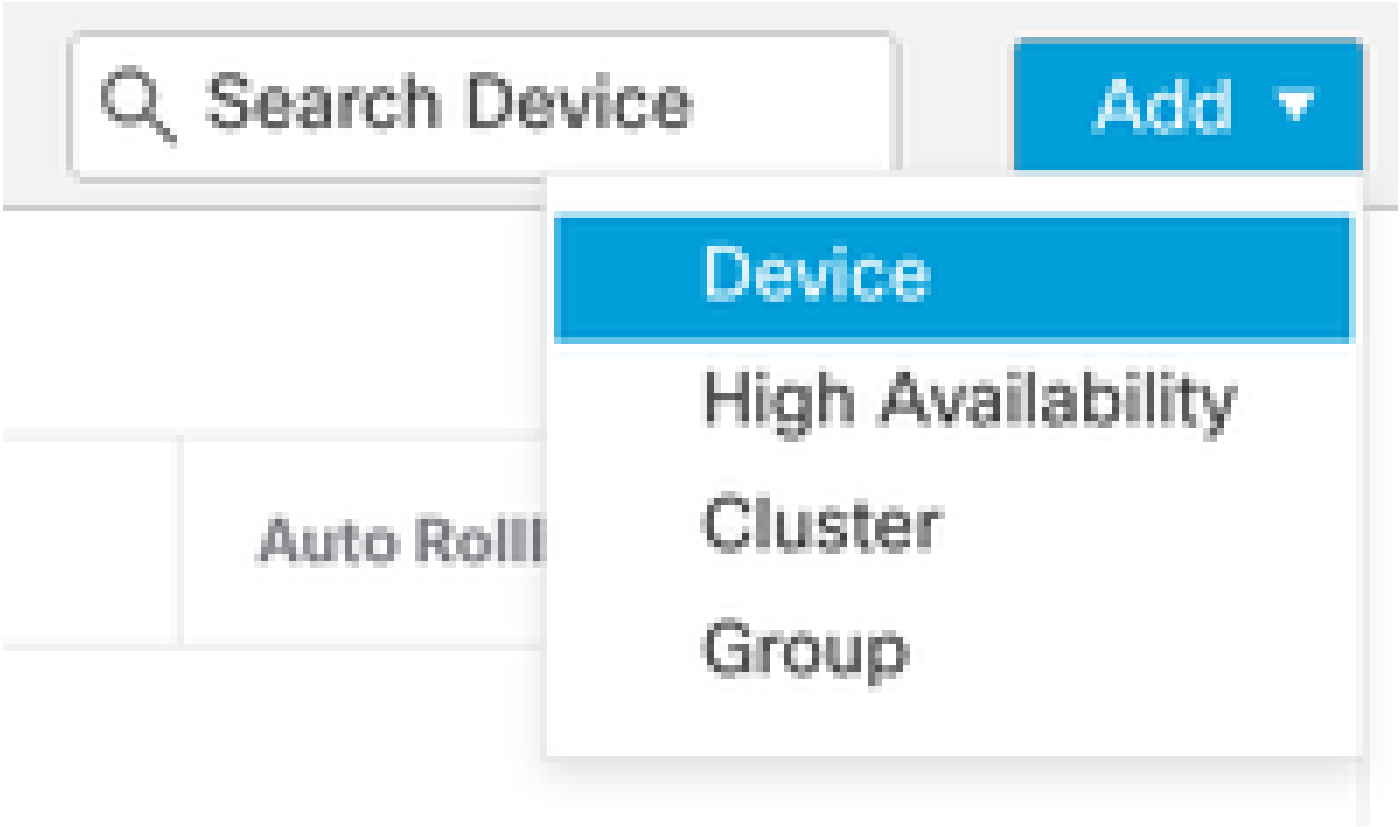


9. 在导入清单中，选择安全区域或创建新区域以分配给接口对象，然后单击导入。



10. 将FTD注册到目标FMC：

- 在目标FMC上，导航到Device > Management 选项卡，然后选择Add > Device。
- 响应提示，完成注册过程。



Add Device

CDO Managed Device

Host:†

Display Name:

Registration Key:*

Group:

None

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Select a recommended Tier

Malware

Threat

URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

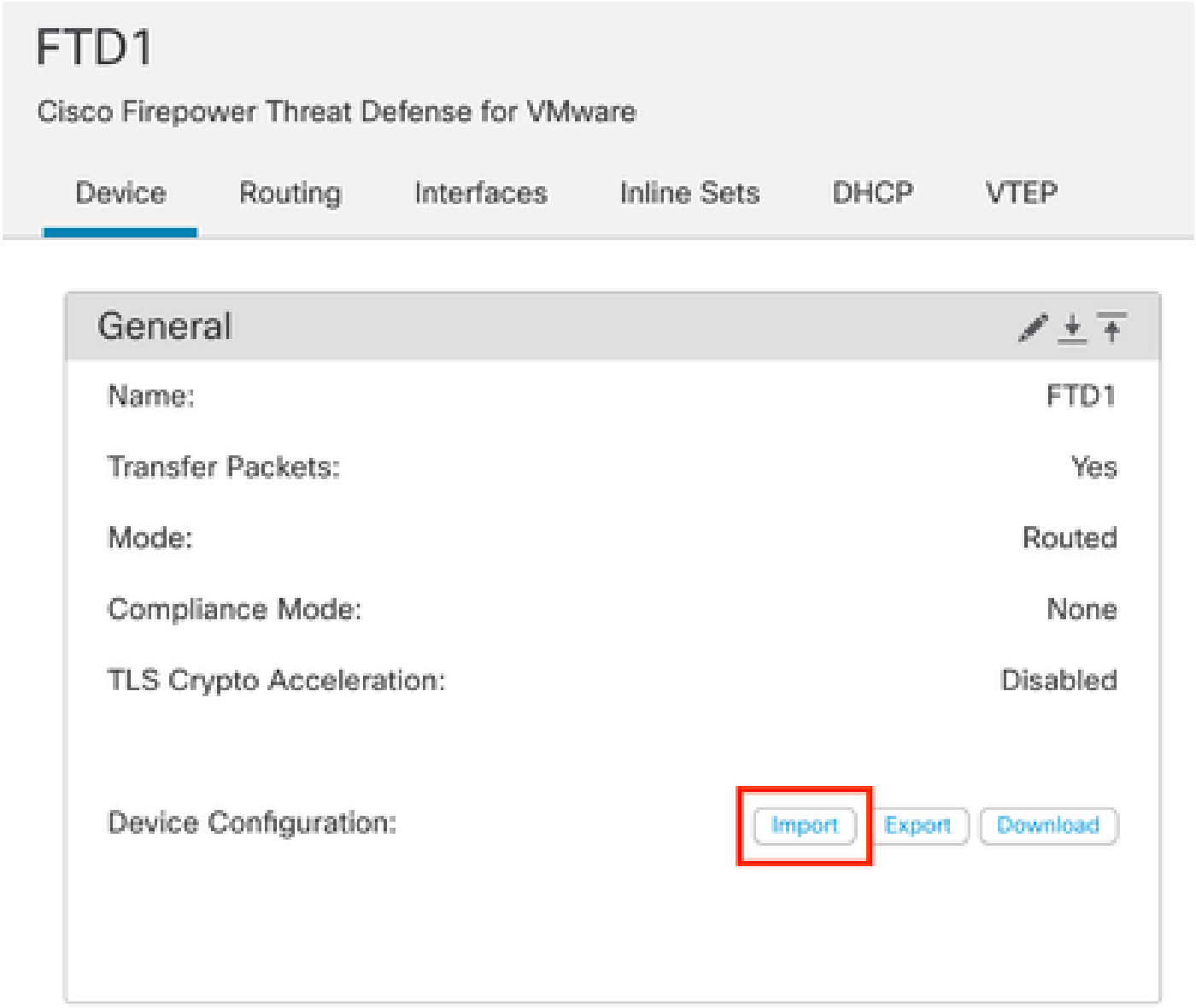
† Either host or NAT ID is required.

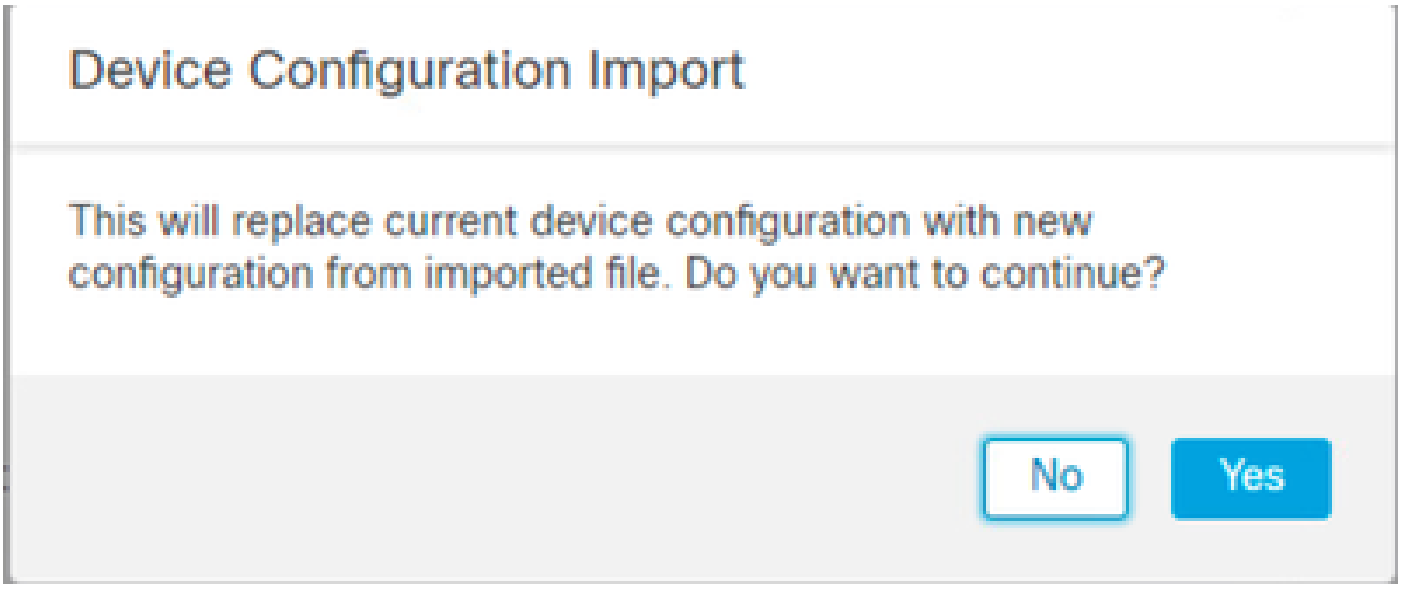
Cancel

Register

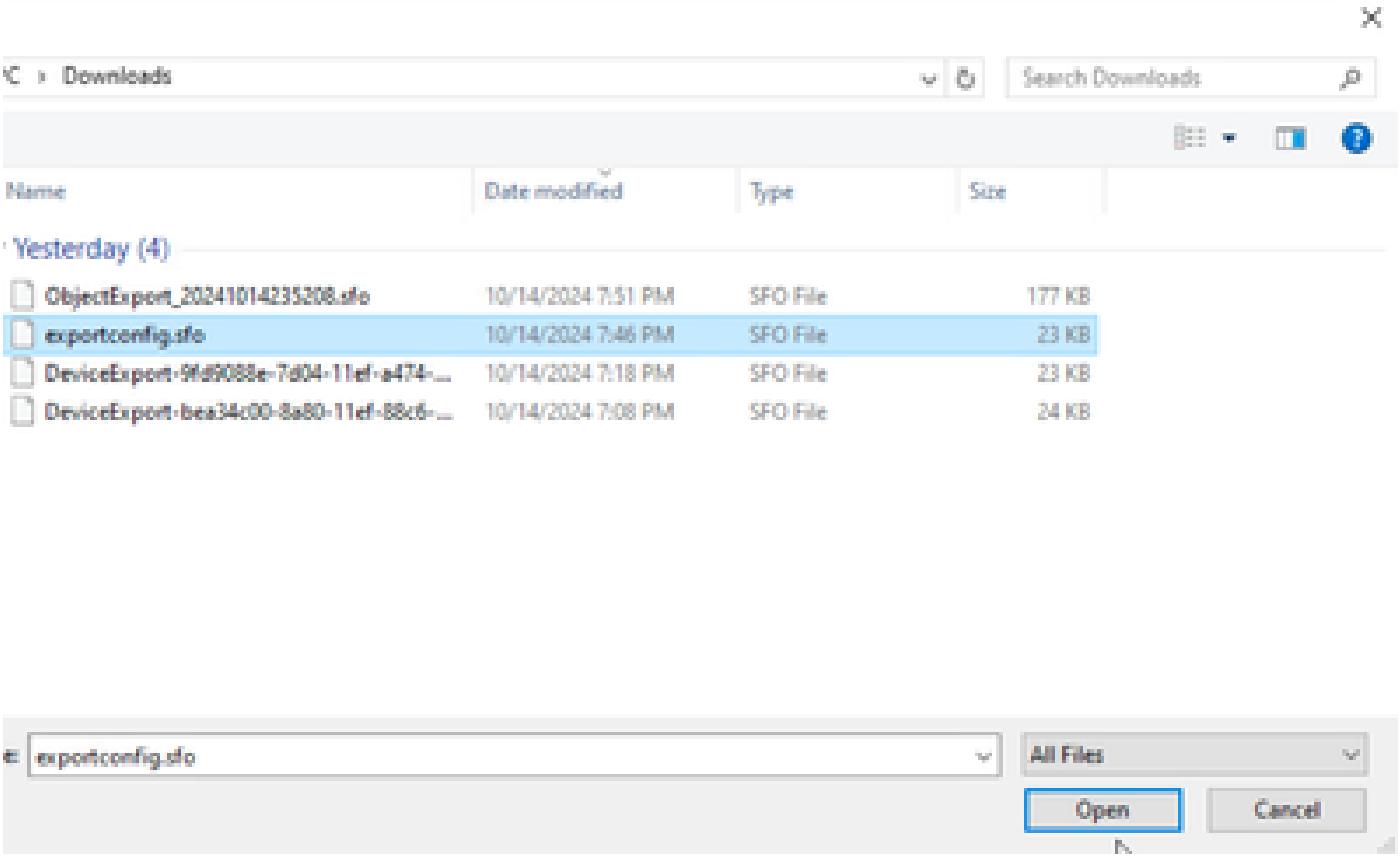
有关其他详细信息，请查看《Firepower管理中心配置指南》，向Firepower管理中心添加设备

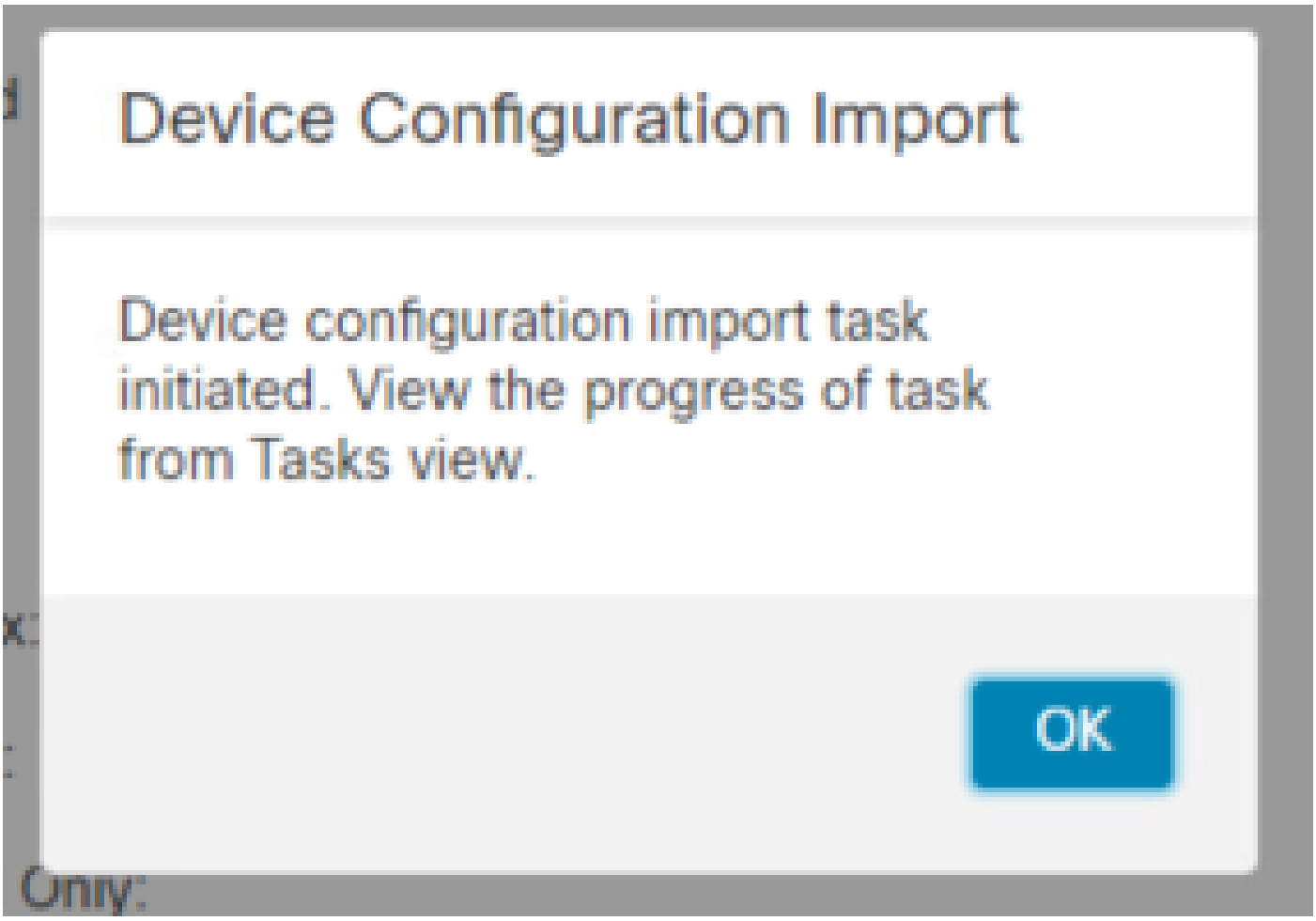
11. 导航到设备>设备管理>选择FTD >设备，然后单击导入。 系统将显示警告，要求您确认是否更换设备配置，然后单击yes。



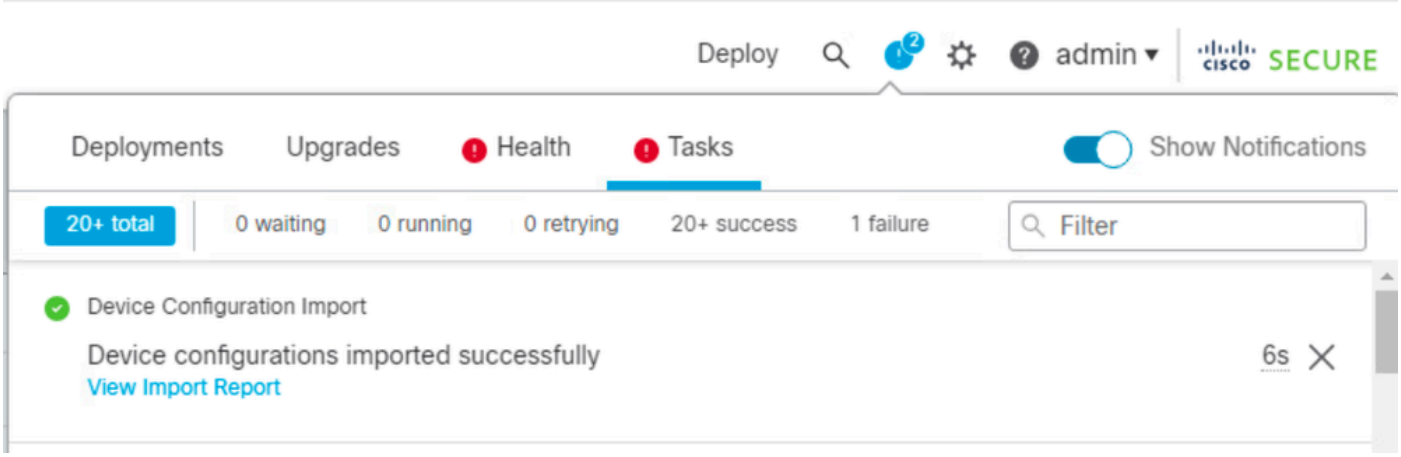


12. 选择必须是.SFO扩展名的导入配置文件，点击上传，您会看到指示导入已启动的消息。





13.最后，系统会在导入完成时自动显示警报并生成报告，从而允许您查看已导入的对象和策略。



Configuration Import Summary

Initiated by:
Initiated at: Tue Oct 15 00:40:18 2024

Policies

Policies imported: 3

Type	Name
PG.PLATFORM.AutomaticApplicationBypassPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.AutomaticApplicationBypassPage
PG.PLATFORM.PixInterface	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.PixInterface
PG.PLATFORM.NgfwInlineSetPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.NgfwInlineSetPage

验证

完成迁移后，验证FTD设备已正确注册并在目标FMC中正常运行：

- 检查目标FMC上的设备状态。
- 确保所有策略和配置均已正确应用。
- 执行测试以确认设备运行正常。

故障排除

如果在迁移过程中遇到任何问题，请考虑以下故障排除步骤：

- 检验FTD设备和两个FMC之间的网络连接。
- 确保两个FMC上的软件版本相同。
- 检查两个FMC上的警报以了解任何错误消息或警告。

相关信息

- Cisco Secure Firewall Management Center管理指南
- 配置、验证Firepower设备注册并对其进行故障排除

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）。

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）。