Migración de un FTD de un FMC a otro FMC

Contenido

Introducción

Este documento describe cómo migrar un dispositivo Cisco Firepower Threat Defense (FTD) entre Firepower Management Centers.

Prerequisites

Antes de iniciar el proceso de migración, asegúrese de que se cumplen estos requisitos previos:

- Acceso a los CSP de origen y de destino.
- Credenciales administrativas para los CSP y el FTD.
- Realice una copia de seguridad de la configuración de FMC actual.
- Asegúrese de que los dispositivos FTD que ejecutan una versión de software compatible con el FMC de destino.
- Asegúrese de que el CSP de destino tiene la misma versión que el de origen.

Requirements

- Ambos CSP deben ejecutar versiones de software compatibles.
- Conectividad de red entre el dispositivo FTD y ambos CSP.
- Almacenamiento y recursos adecuados en el CSP de destino para alojar el dispositivo FTD.

Componentes Utilizados

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

Cisco Firepower Threat Defense Virtual (FTDv) versión 7.2.5

Firepower Management Center Virtual (FMCv) versión 7.2.5

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

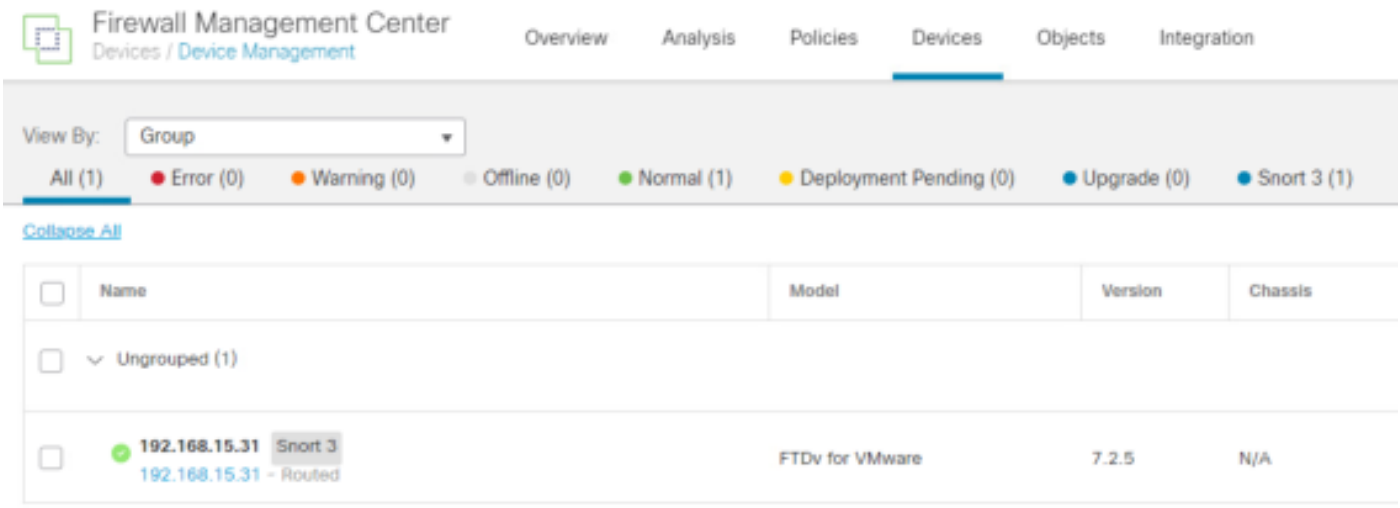
La migración de un dispositivo FTD de un FMC a otro implica varios pasos, incluidos la anulación del registro del dispositivo del FMC de origen, la preparación del FMC de destino y el nuevo registro del dispositivo. Este proceso garantiza que todas las políticas y configuraciones se transfieren y aplican correctamente.

Configurar

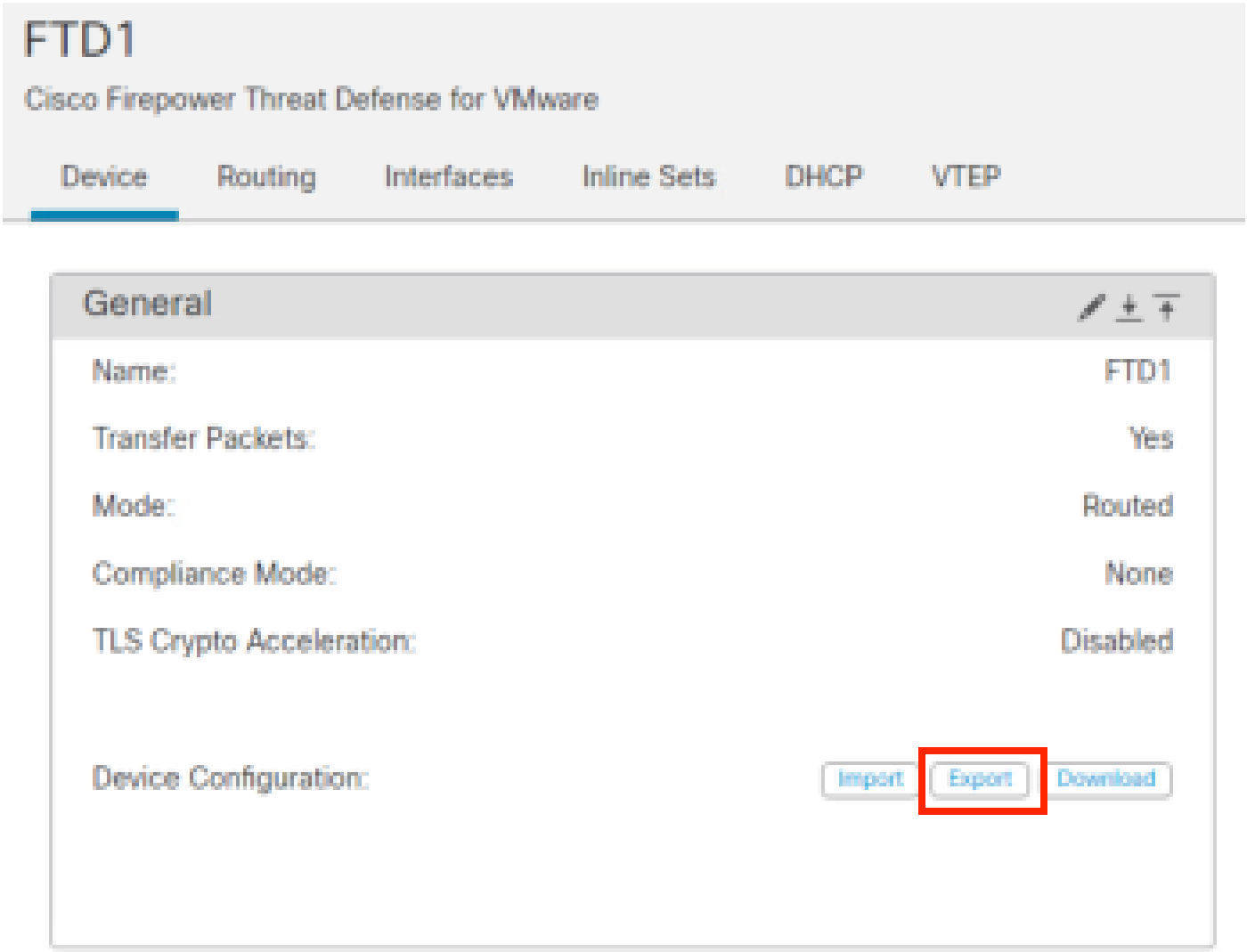
Configuraciones

1. Inicie sesión en el FMC de origen.

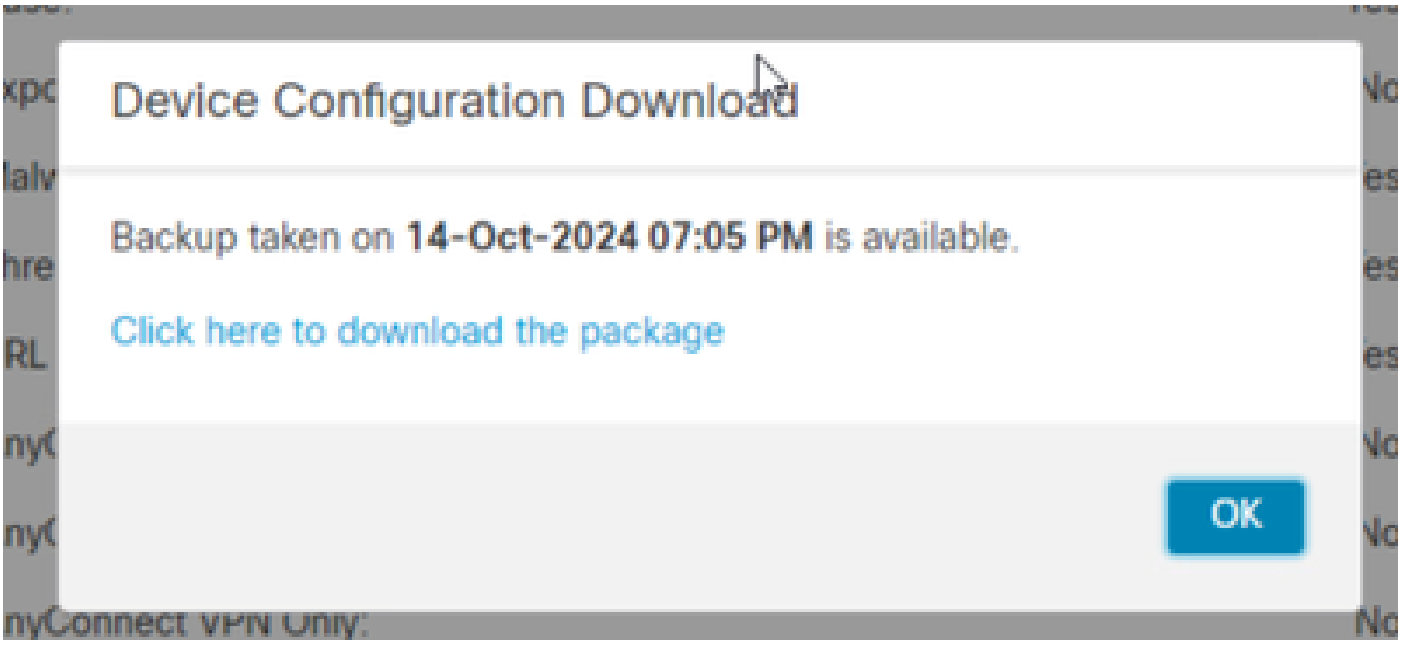
2. Navegue hasta Devices > Device Management y seleccione el dispositivo que desea migrar.

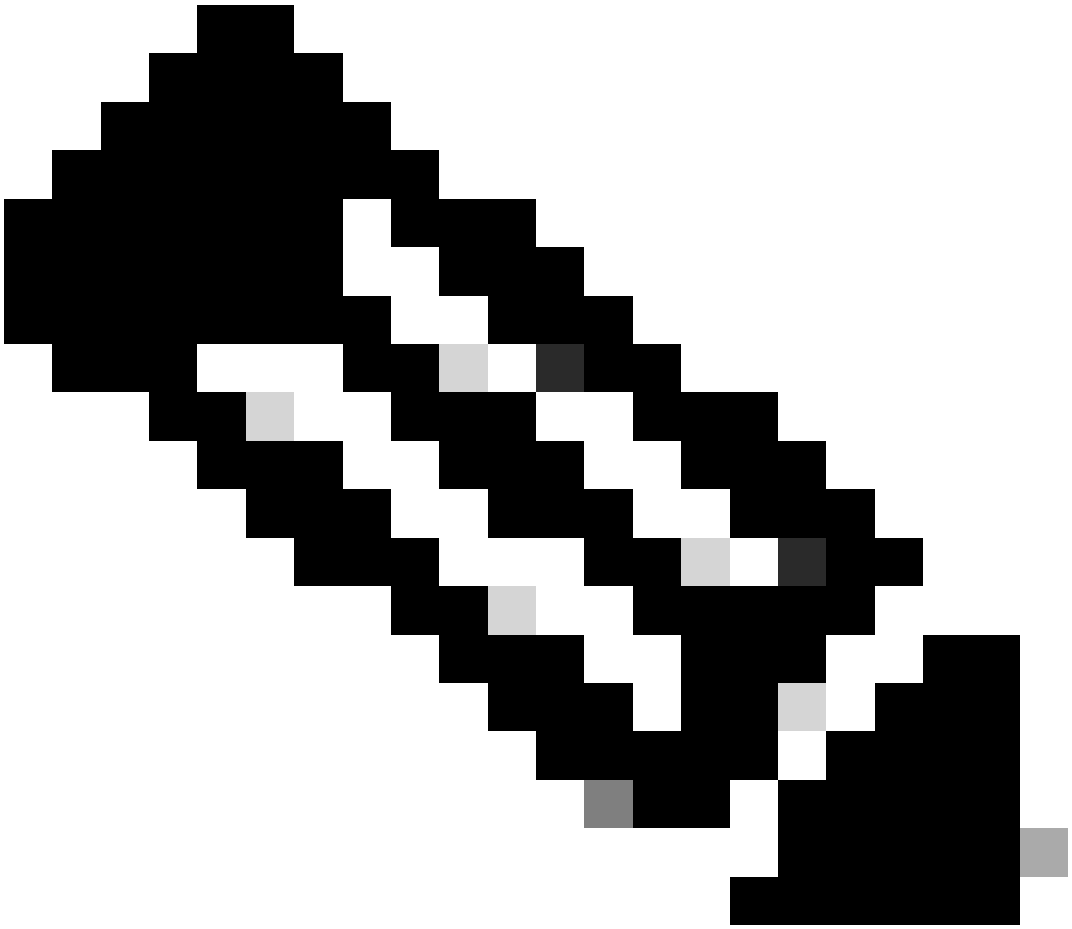


3. En la sección de dispositivos, navegue hasta el dispositivo y haga clic en exportar para exportar su configuración de dispositivo.



4. Una vez exportada la configuración, debe descargarla.

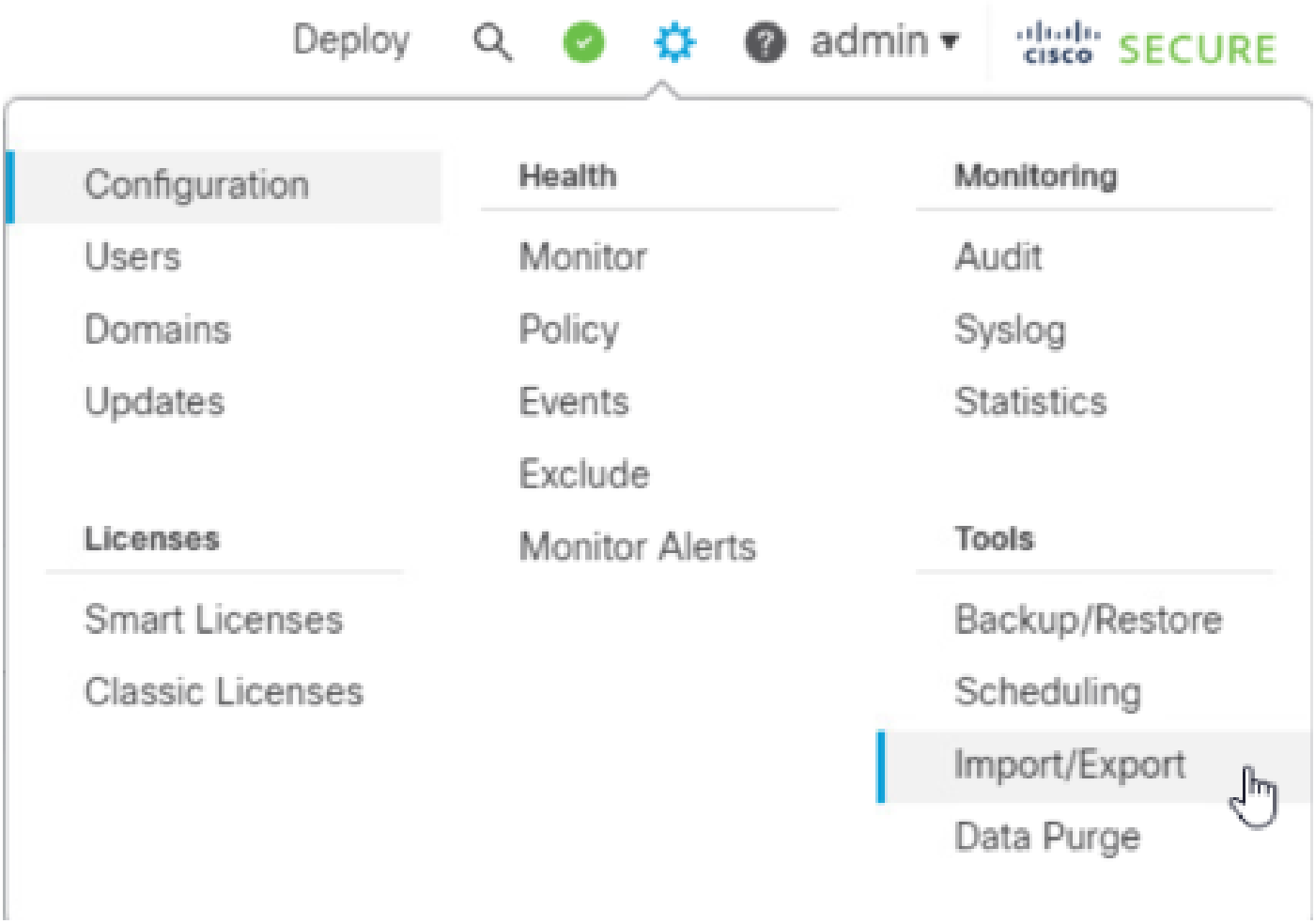


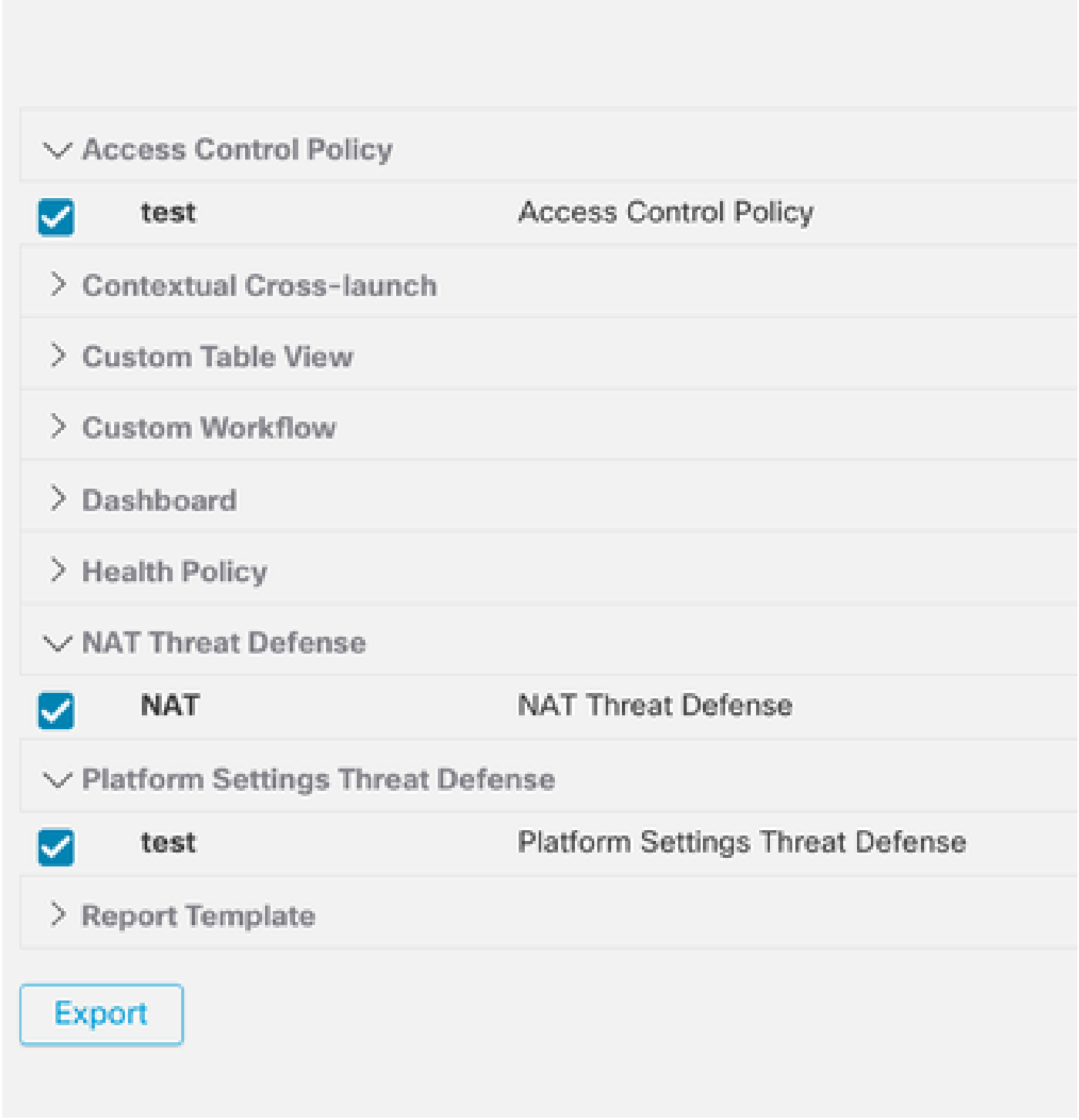


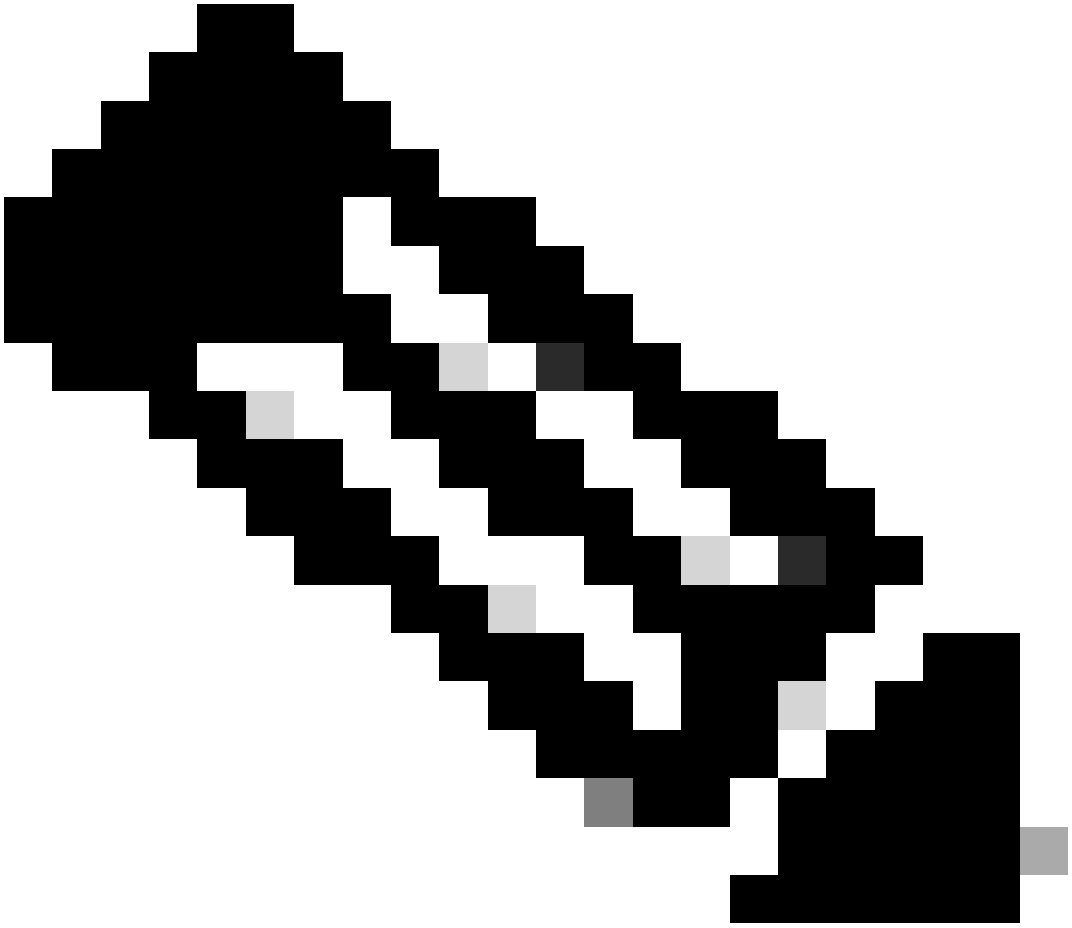
Nota: el archivo descargado debe contener la extensión .SFO y contiene información de

configuración del dispositivo como direcciones IP, zonas de seguridad, rutas estáticas y otros ajustes del dispositivo.

5. Debe exportar las políticas asociadas al dispositivo, navegar hasta System > Tools > Import/Export, seleccionar las políticas que desea exportar y hacer clic en export.

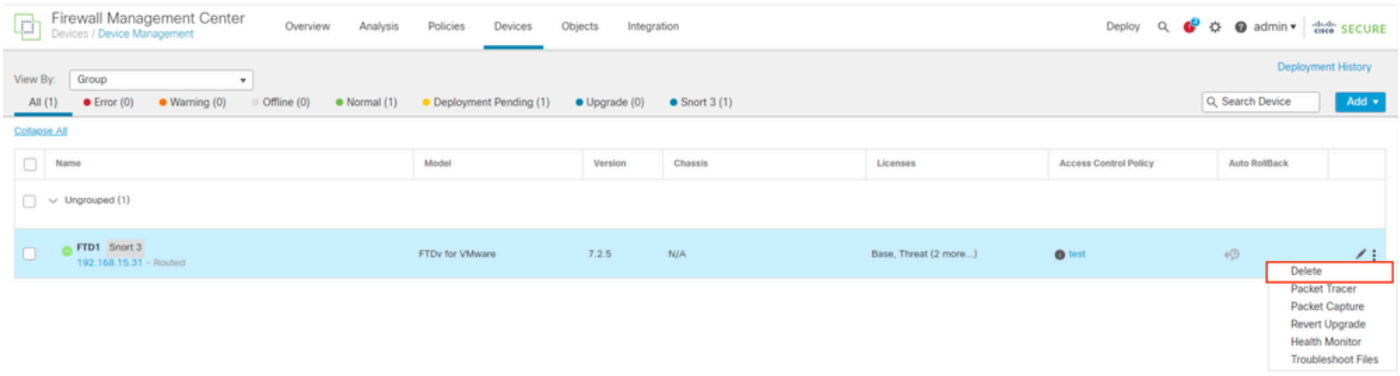



Access Control Policy
test
Access Control Policy
Contextual Cross-launch
Custom Table View
Custom Workflow
Dashboard
Health Policy
NAT Threat Defense
NAT
NAT Threat Defense
Platform Settings Threat Defense
test
Platform Settings Threat Defense
Report Template
Export



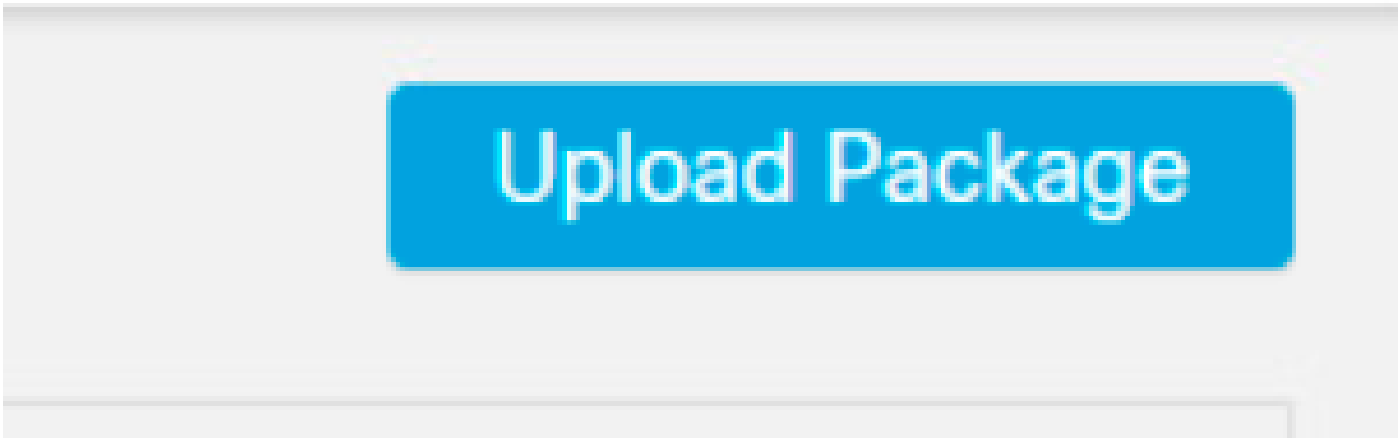
Nota: Asegúrese de que el archivo .SFO se ha descargado correctamente. La descarga se realiza automáticamente después de hacer clic en Export (Exportar). Este archivo contiene las políticas de control de acceso, la configuración de la plataforma, las políticas NAT y otras políticas que son indispensables para la migración, ya que no se exportan junto con la configuración del dispositivo y deben cargarse manualmente en el FMC de destino.

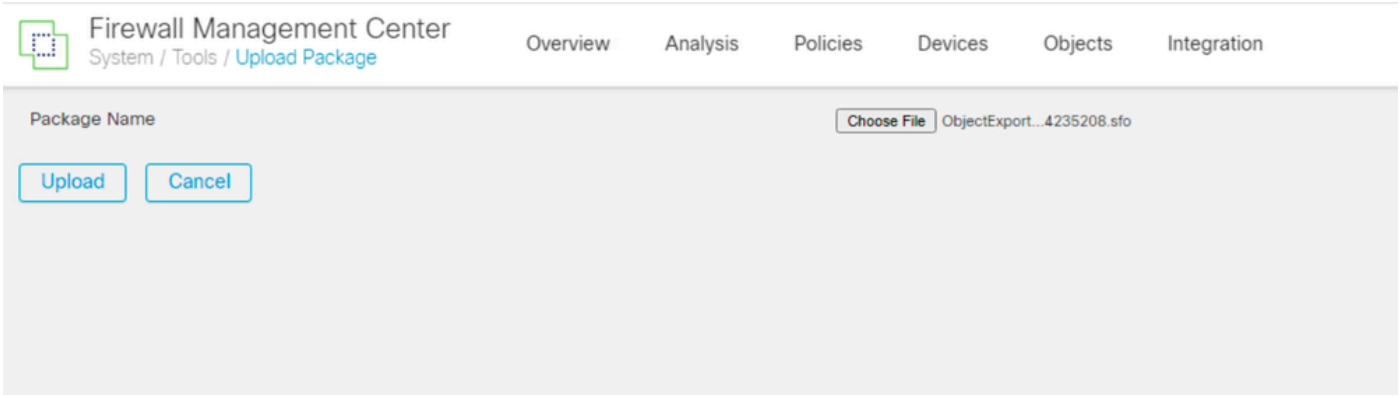
6. Anule el registro del dispositivo FTD en el FMC, navegue hasta Devices > Device management, haga clic en los tres puntos verticales en el lado derecho y seleccione delete.



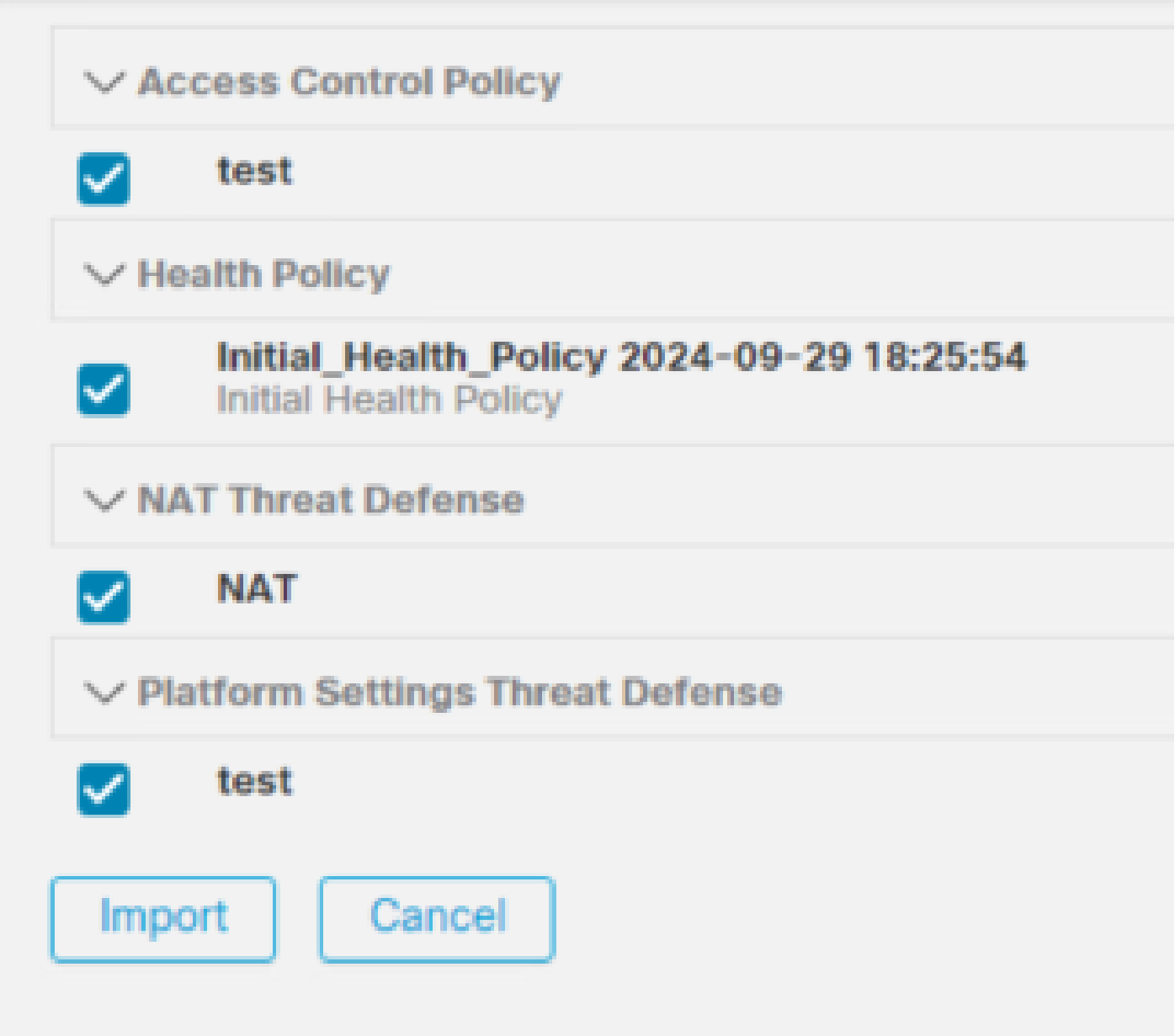
7. Preparar el CSP de destino:

- Inicie sesión en el FMC de destino.
- Asegúrese de que el FMC está listo para aceptar el nuevo dispositivo importando las políticas de FMC de origen que descargó en el paso 5. Navegue hasta System > Tools > Import/Export y haga clic en upload package. Cargue el archivo que desea importar y haga clic en cargar.

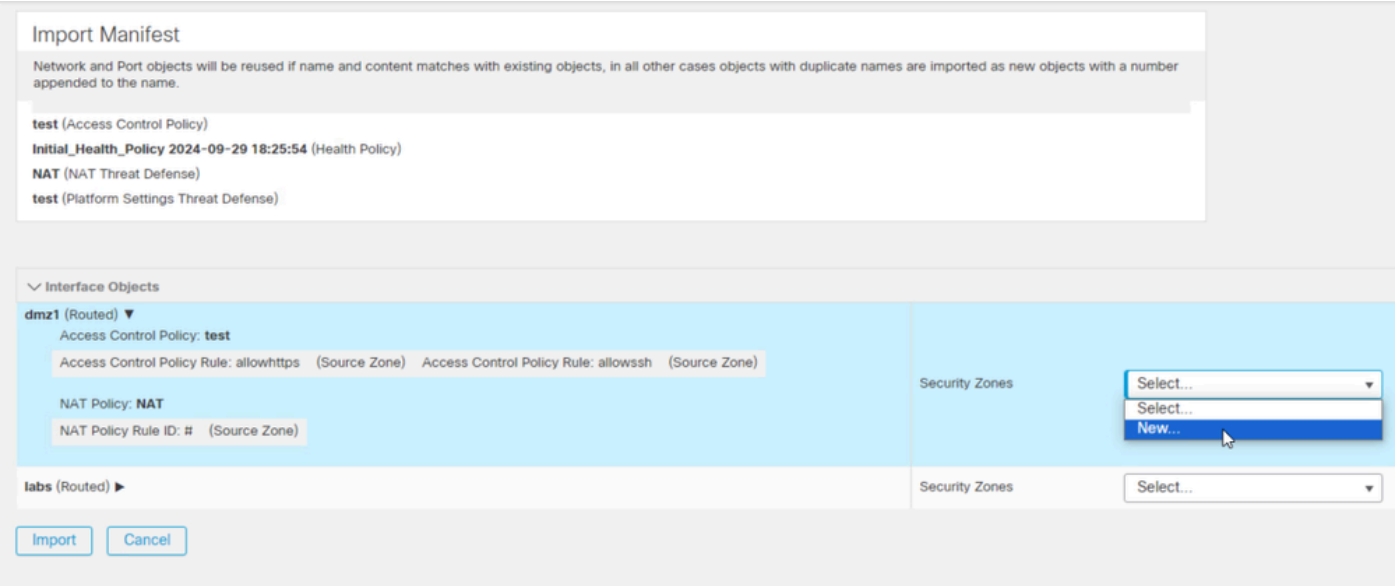




8. Seleccione las políticas que desea importar en el FMC de destino.

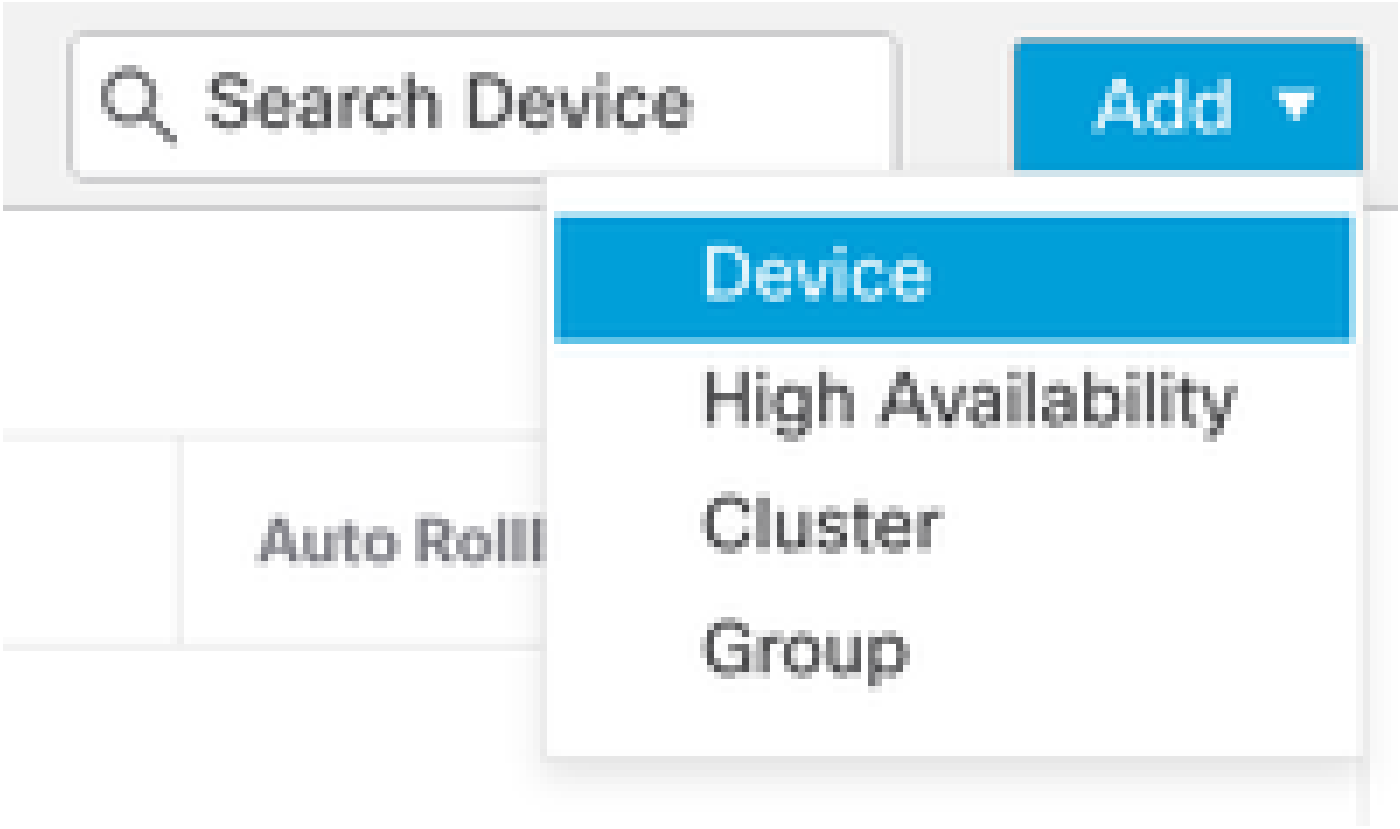


9. En el manifiesto de importación, seleccione una zona de seguridad o cree una nueva para asignarla al objeto de interfaz y haga clic en importar.



10. Registrar el FTD en el CSP de destino:

- En el FMC de destino, navegue hasta la pestaña Device > Management y seleccione Add > Device.
- Complete el proceso de registro respondiendo a las indicaciones.



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

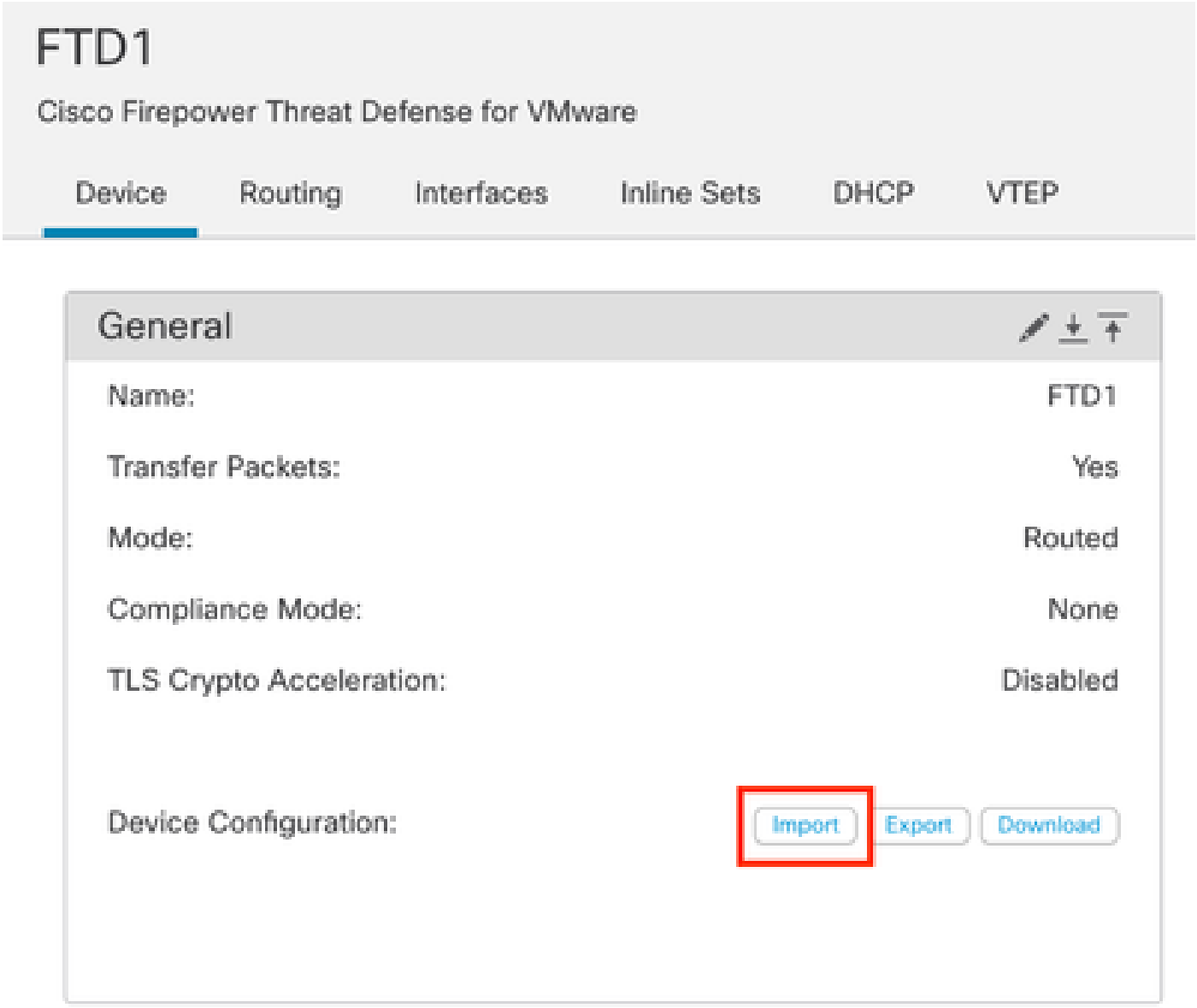
† Either host or NAT ID is required.

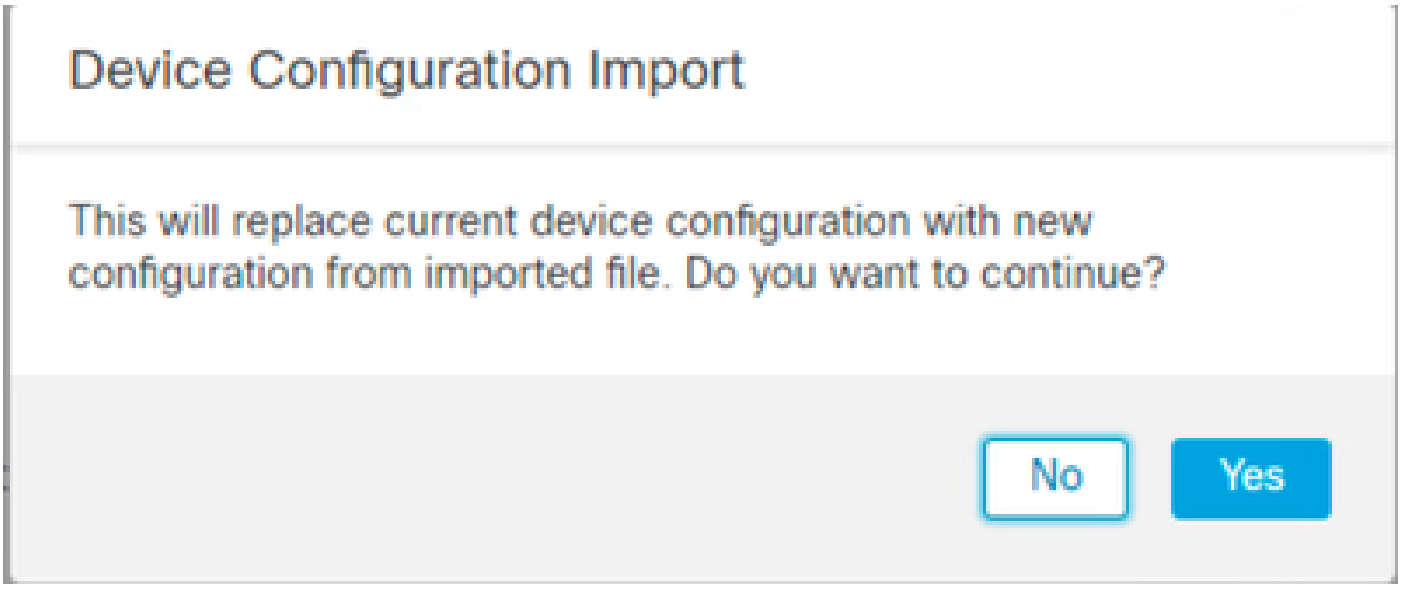
Cancel

Register

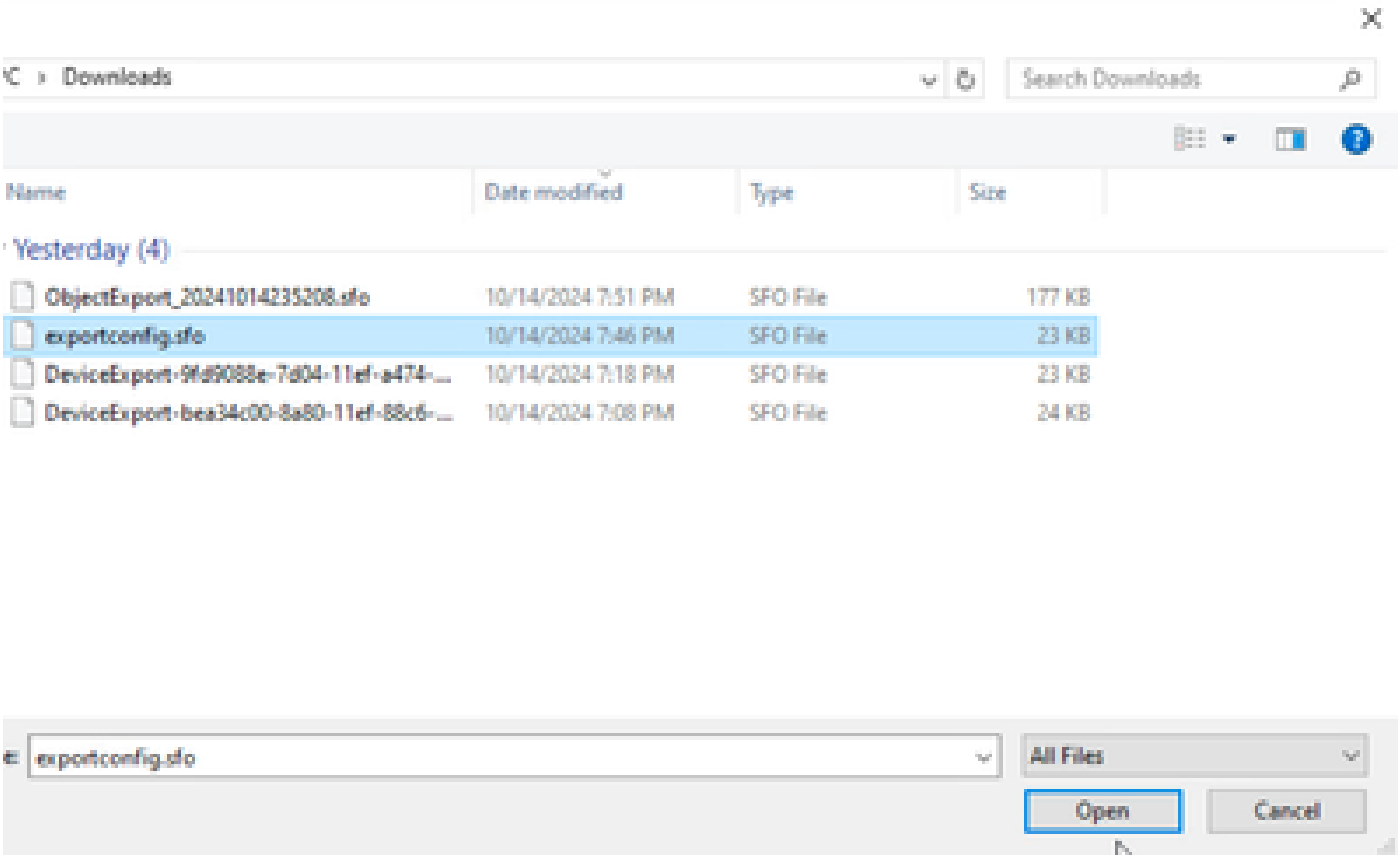
Para obtener más información, consulte la Guía de configuración de Firepower Management Center, Agregar dispositivos a Firepower Management Center

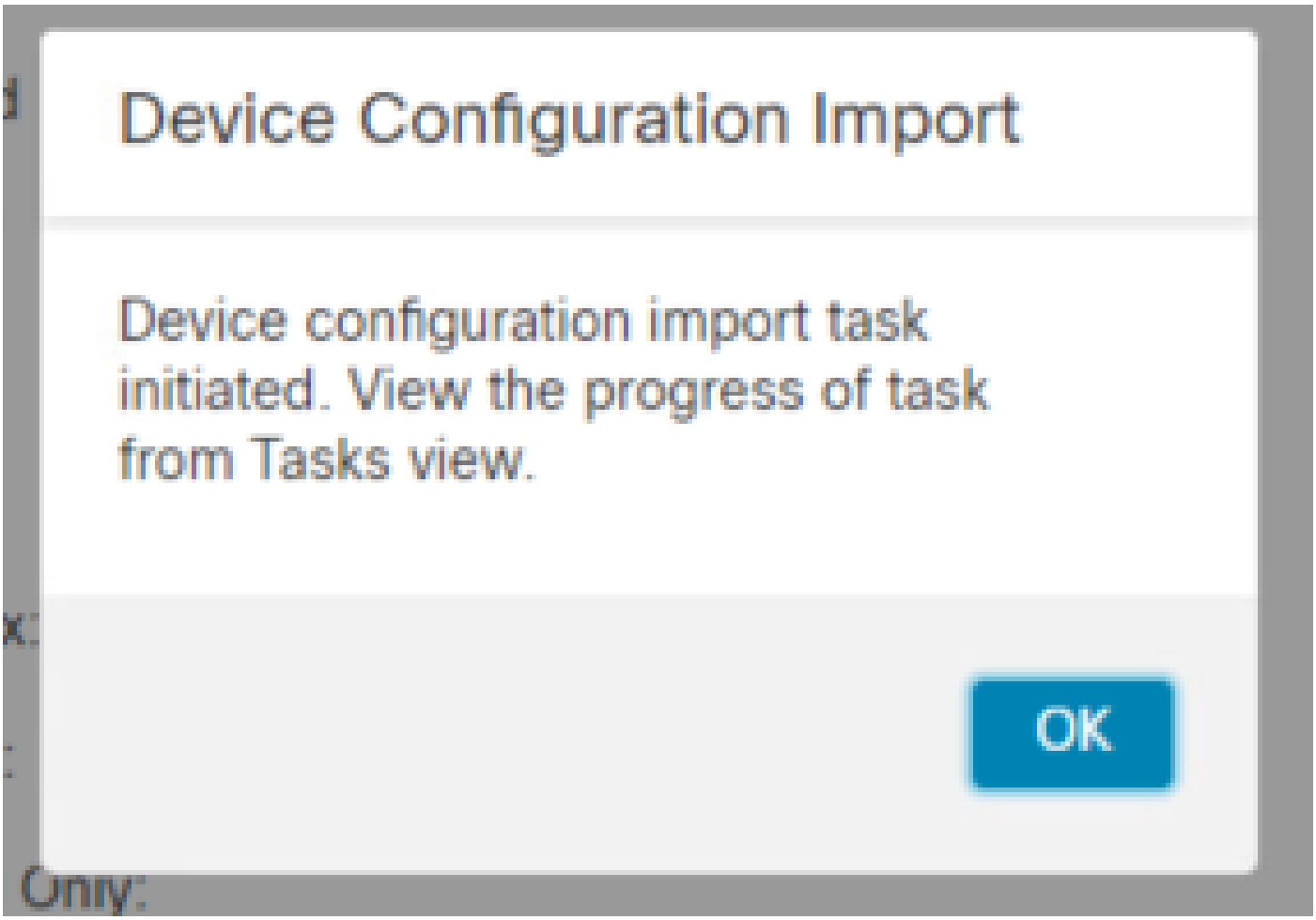
11. Vaya a Device > Device Management > select the FTD > Device y haga clic en import. Aparecerá una advertencia en la que se le solicitará que confirme la sustitución de la configuración del dispositivo. Haga clic en yes (sí).



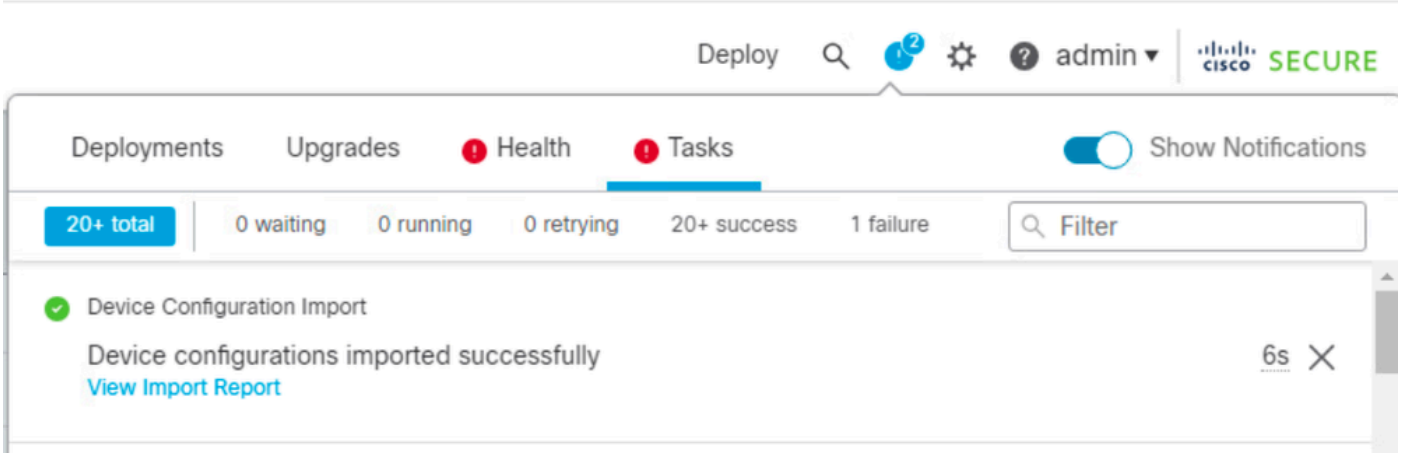


12. Seleccione el archivo de configuración de importación, que debe tener la extensión .SFO, haga clic en cargar y aparecerá un mensaje que indica que la importación se ha iniciado.





13. Por último, se muestra una alerta y se genera un informe automáticamente cuando finaliza la importación, lo que permite revisar los objetos y políticas que se han importado.



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

Verificación

Después de completar la migración, verifique que el dispositivo FTD esté registrado correctamente y funcione correctamente con el FMC de destino:

- Compruebe el estado del dispositivo en el FMC de destino.
- Asegúrese de que todas las directivas y configuraciones se aplican correctamente.
- Realice una prueba para confirmar que el dispositivo está operativo.

Troubleshoot

Si experimenta algún problema durante el proceso de migración, tenga en cuenta los siguientes pasos para la solución de problemas:

- Verifique la conectividad de red entre el dispositivo FTD y ambos FMC.
- Asegúrese de que la versión del software en ambos CSP es la misma.
- Compruebe las alertas de ambos CSP en busca de mensajes de error o advertencias.

Información Relacionada

- Guía de administración de Cisco Secure Firewall Management Center
- Configuración, verificación y resolución de problemas del registro de dispositivos Firepower

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).