Migrate an FTD from One FMC to another FMC

Contents

Introduction

This document describes how to migrate a Cisco Firepower Threat Defense (FTD) device between Firepower Management Centers.

Prerequisites

Before starting the migration process, ensure that you have these prerequisites in place:

- Access to both the source and destination FMCs.
- Administrative credentials for both FMCs and FTD.
- Backup the current FMC configuration.
- Make sure that the FTD devices running a compatible software version with the destination FMC.
- Make sure that the destination FMC has the same version as the source FMC.

Requirements

- Both FMCs must be running compatible software versions.
- Network connectivity between the FTD device and both FMCs.
- Adequate storage and resources on the destination FMC to accommodate the FTD device.

Components Used

The information in this document is based on these software and hardware versions:

Cisco Firepower Threat Defense Virtual (FTDv) Version 7.2.5

Firepower Management Center Virtual (FMCv) Version 7.2.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

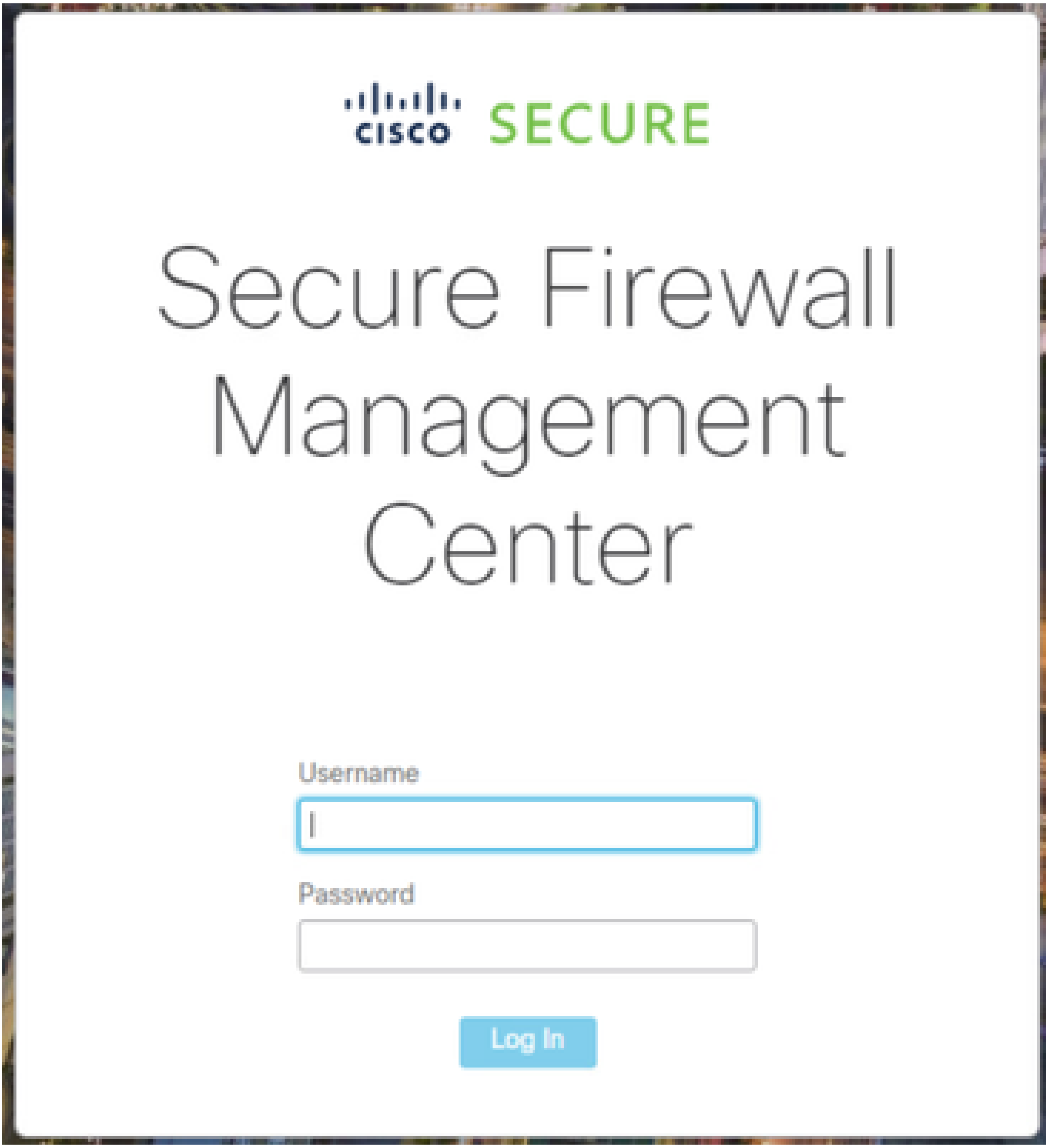
Background Information

Migrating an FTD device from one FMC to another involves several steps, including deregistering the device from the source FMC, preparing the destination FMC, and re-registering the device. This process ensures that all policies and configurations are correctly transferred and applied.

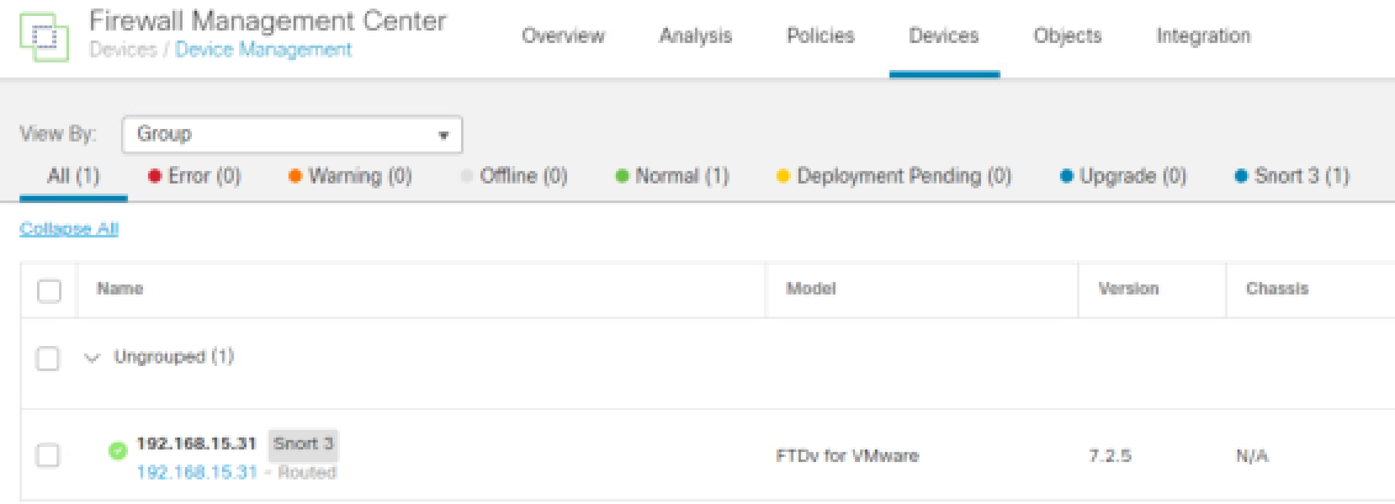
Configure

Configurations

1. Log in to the source FMC.



2. Navigate to **Devices** > **Device Management** and select the device to be migrated.

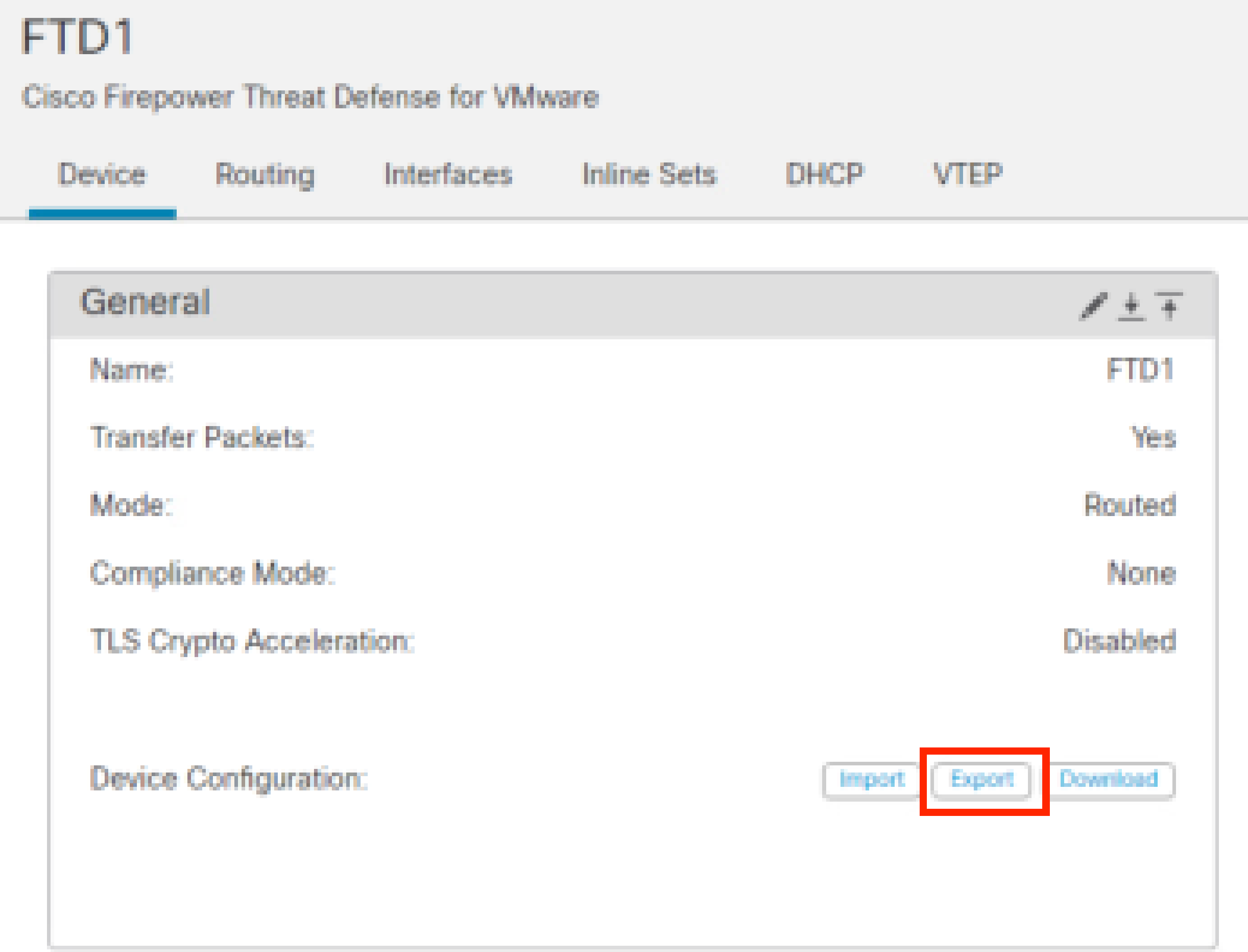


View By: Group

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (1)

□	Name	Model	Version	Chassis
□	⌄ Ungrouped (1)			
□	● 192.168.15.31 Snort 3 192.168.15.31 - Routed	FTDv for VMware	7.2.5	N/A

3. Within the device section, navigate to device and click **export to export your device** settings.



Name: FTD1

Transfer Packets: Yes

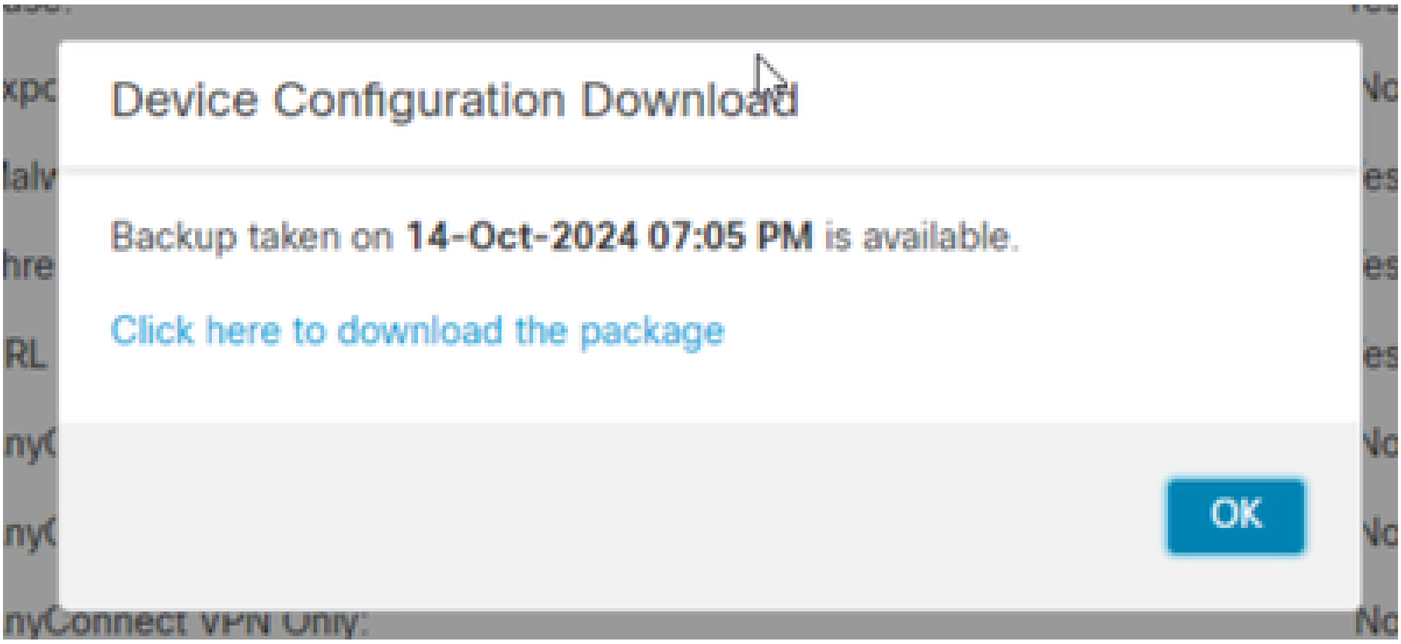
Mode: Routed

Compliance Mode: None

TLS Crypto Acceleration: Disabled

Device Configuration:

4. Once the configuration has been exported, you must download it.



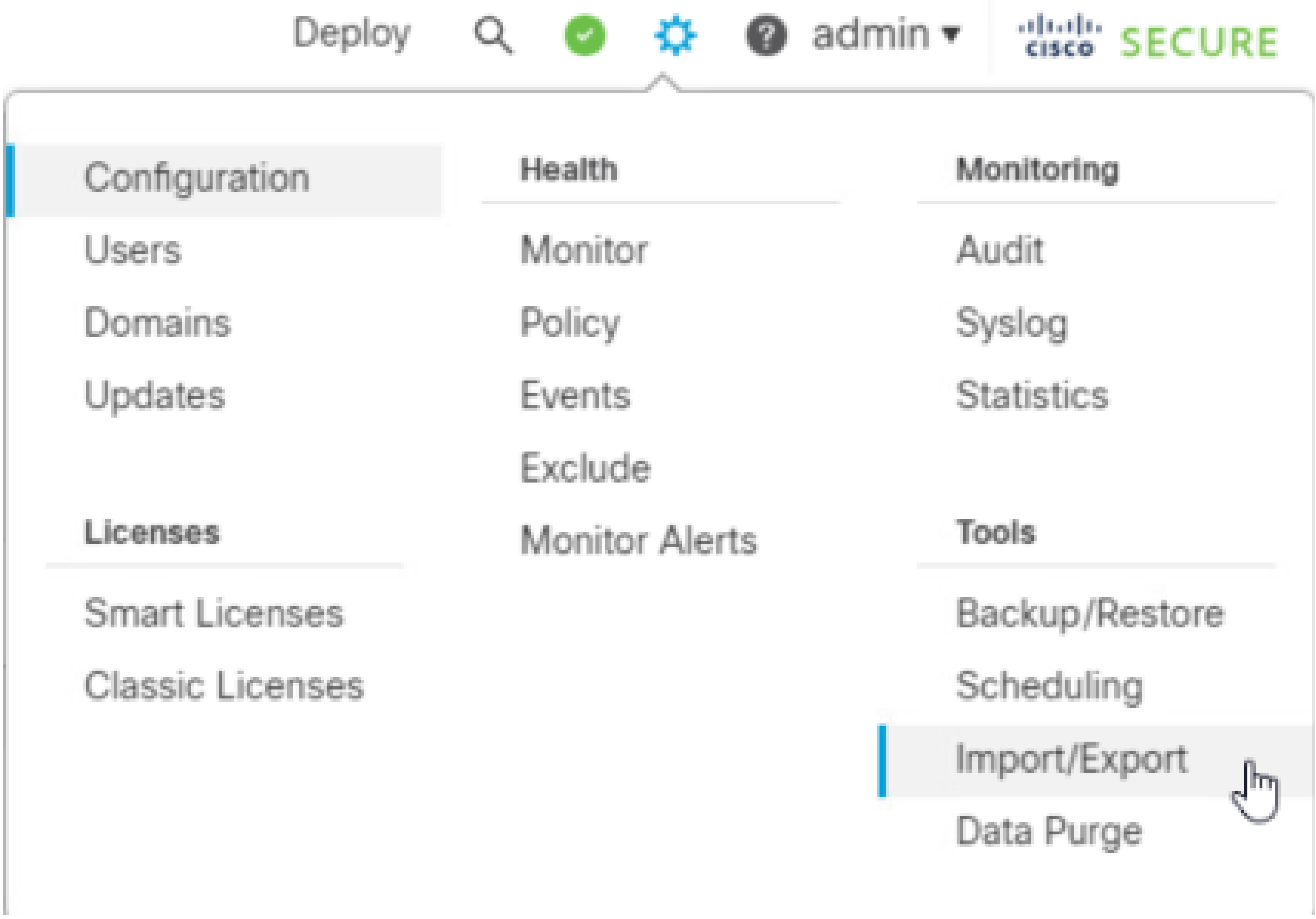
Device Configuration Download

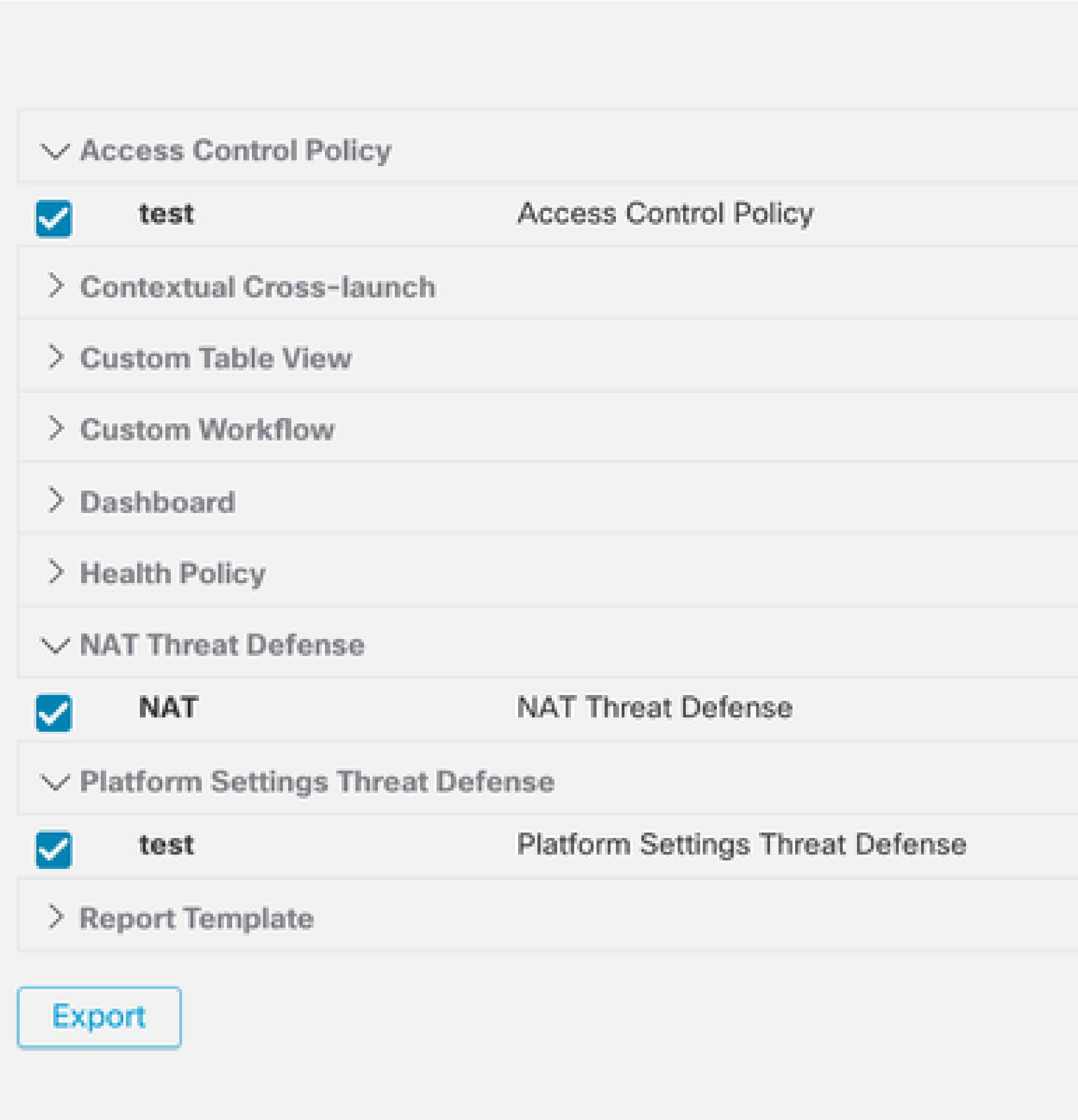
Backup taken on **14-Oct-2024 07:05 PM** is available.

Click here to download the package

Note: The downloaded file must contain the .SFO extension and contains device configuration information such as IP addresses, security zones, static routes, and other device settings.

5. You must export the policies associated with the device, navigate to **System** > **Tools** > **Import/Export**, select the policies you want to **export** and click **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

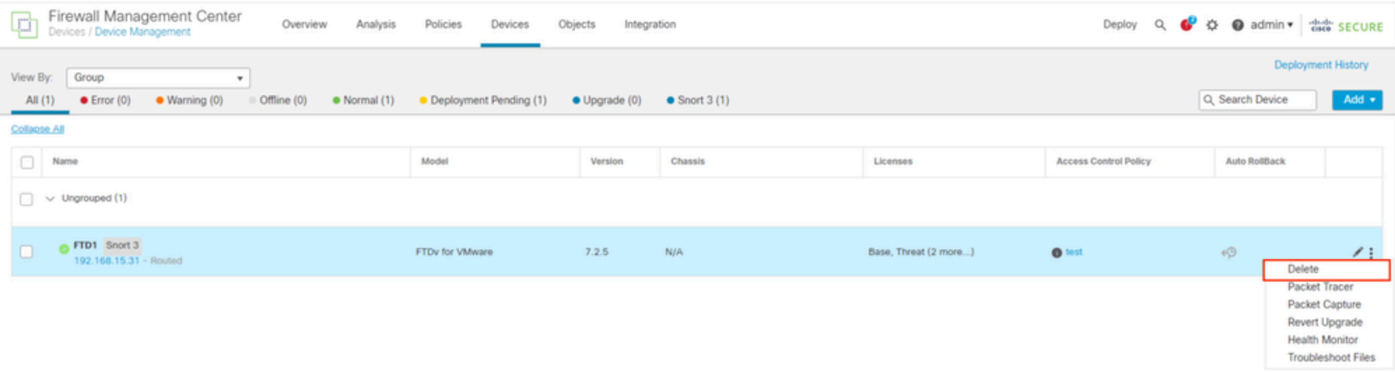
Platform Settings Threat Defense

☑ test — Platform Settings Threat Defense

Report Template

Note: Make sure that the .SFO file has been downloaded successfully. The download is done automatically after clicking on export. This file contains the access control policies, platform settings, NAT policies, and other policies which are indispensable for the migration since they are not exported together with the device configuration and have to be uploaded manually to the destination FMC.

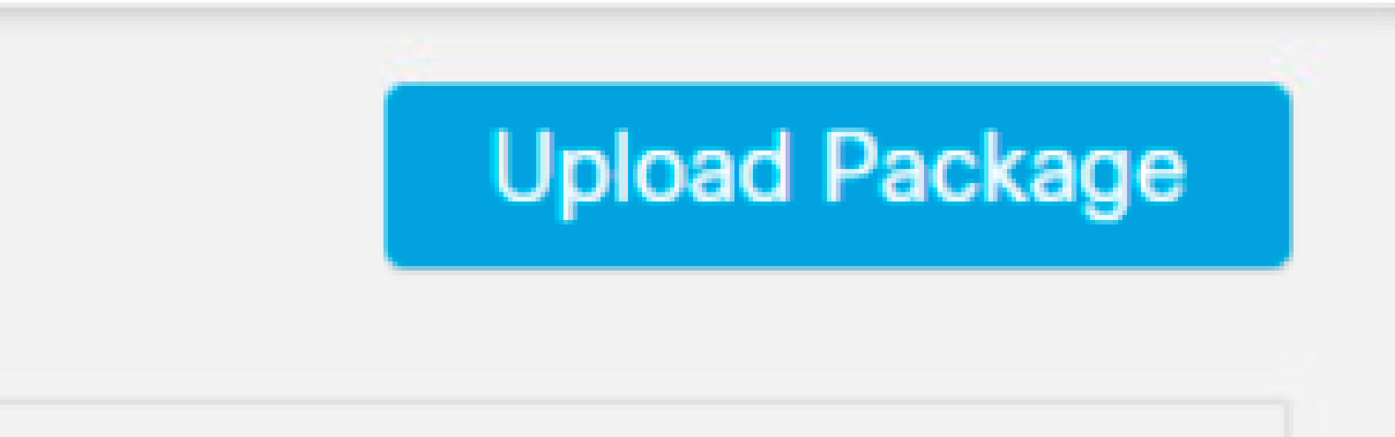
6. Deregister the FTD device from the FMC, navigate to **Devices > Device management**, click the **three vertical dots** on the right side and select **delete**.

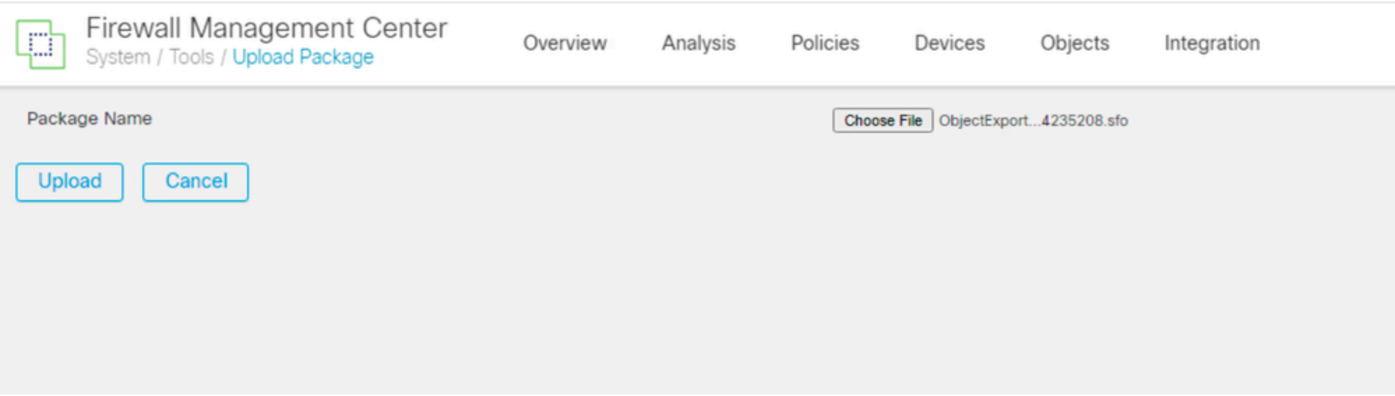


☐	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
☐	⌄ Ungrouped (1)							
☐	● FTD1 Snort 3 192.168.15.31 - Routed	FTDv for VMware	7.2.5	N/A	Base, Threat (2 more...)	● test		⋮

7. Prepare the Destination FMC:

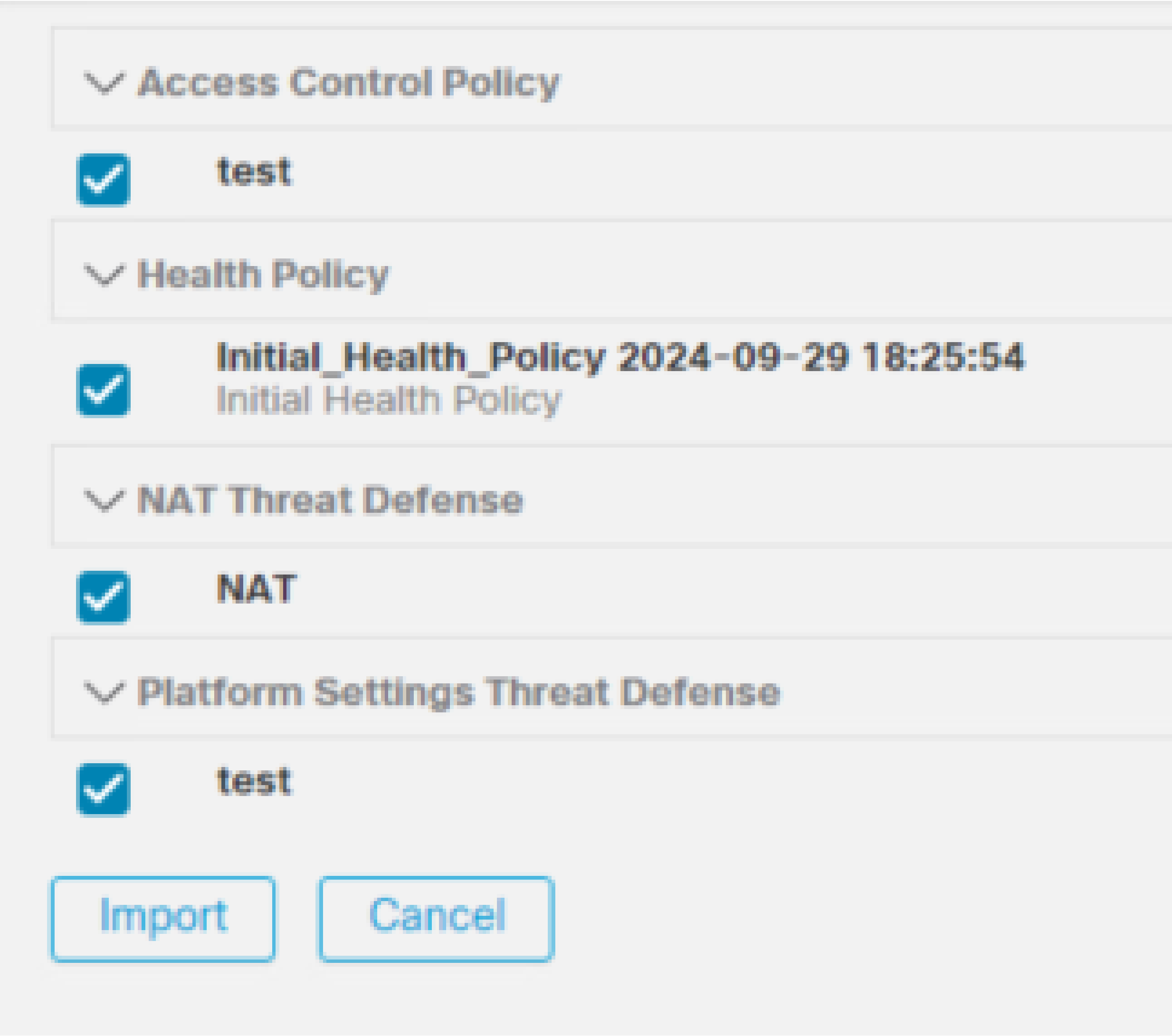
- Log in to the destination FMC.
- Make sure that the FMC is ready to accept the new device by importing the source FMC policies you downloaded in step 5. Navigate to **System > Tools > Import/Export** and click **upload package**. Upload the file to import and click **upload**.





Package Name ObjectExport...4235208.sfo

8. Select the policies to import in the destination FMC.



﹀ Access Control Policy

☑ test

﹀ Health Policy

☑ Initial_Health_Policy 2024-09-29 18:25:54
Initial Health Policy

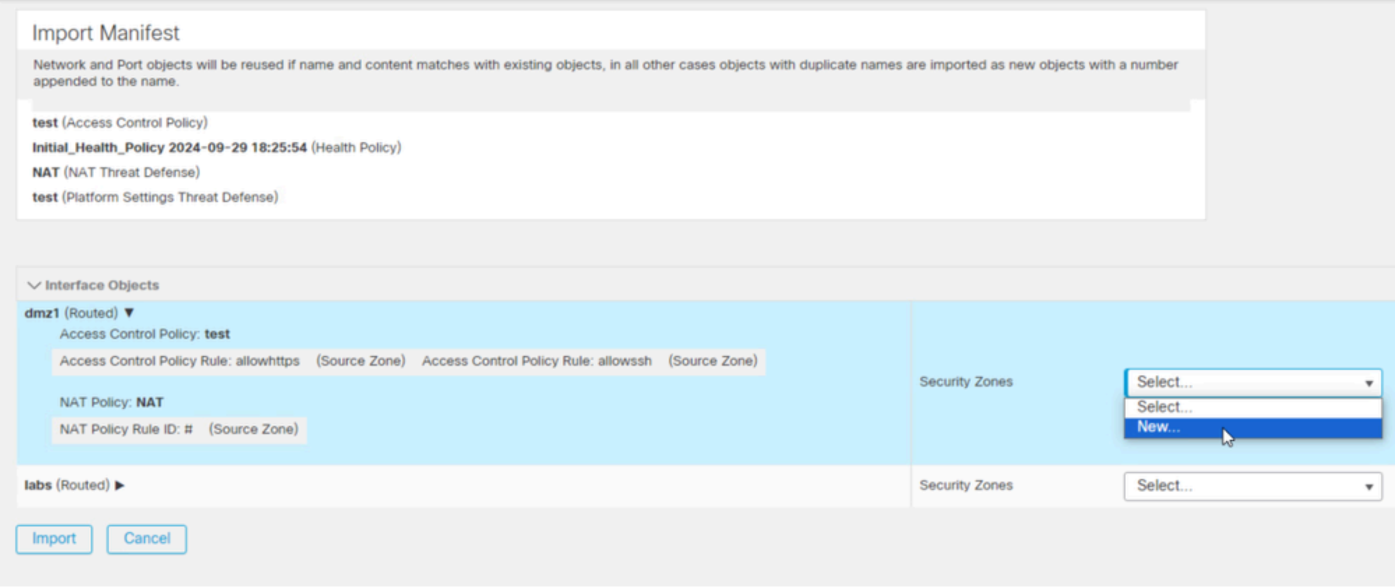
﹀ NAT Threat Defense

☑ NAT

﹀ Platform Settings Threat Defense

☑ test

9. In the import manifest, select a **security zone** or create a **new one** to assign to the interface object and click **import**.



Import Manifest

Network and Port objects will be reused if name and content matches with existing objects, in all other cases objects with duplicate names are imported as new objects with a number appended to the name.

test (Access Control Policy)
Initial_Health_Policy 2024-09-29 18:25:54 (Health Policy)
NAT (NAT Threat Defense)
test (Platform Settings Threat Defense)

﹀ Interface Objects

dmz1 (Routed) ▼
Access Control Policy: **test**
Access Control Policy Rule: allowhttps (Source Zone) Access Control Policy Rule: allowssh (Source Zone)
NAT Policy: **NAT**
NAT Policy Rule ID: # (Source Zone)

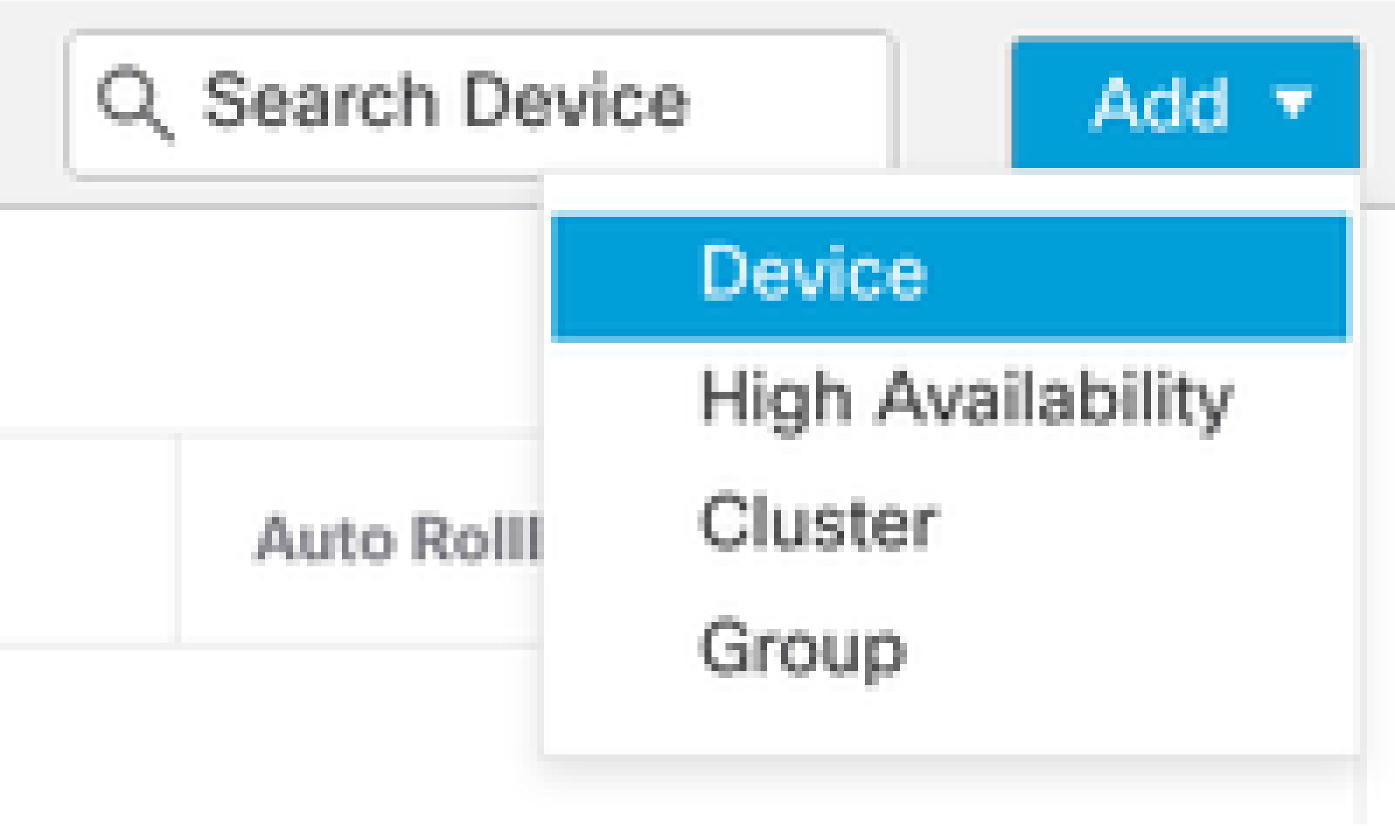
Security Zones: Select...

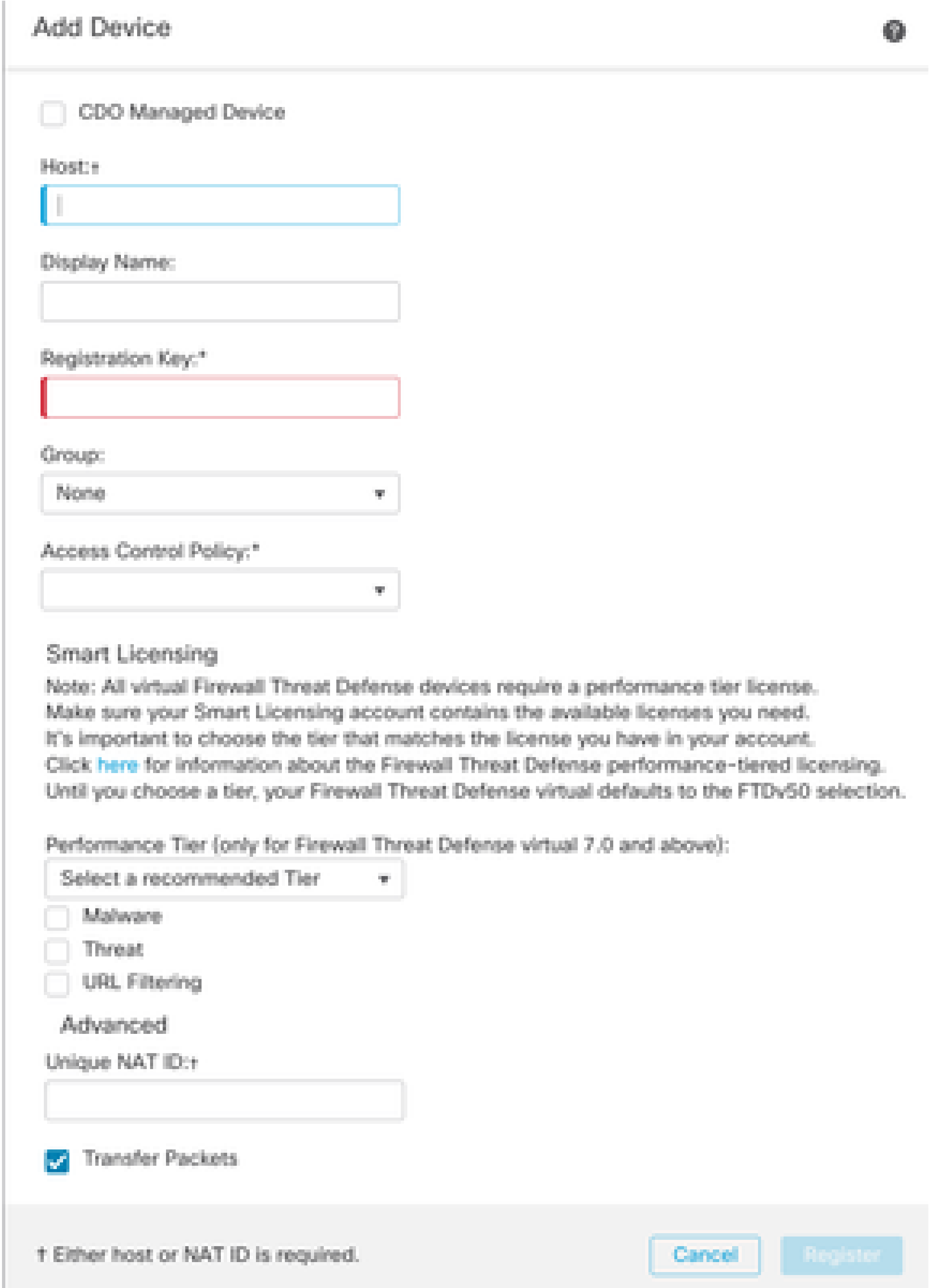
labs (Routed) ▶

Security Zones: Select...

10. Register the FTD to the Destination FMC:

- On the destination FMC, navigate to **Device** > **Management** tab and select **Add** > **Device**.
- Complete the registration process by responding to the prompts.





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

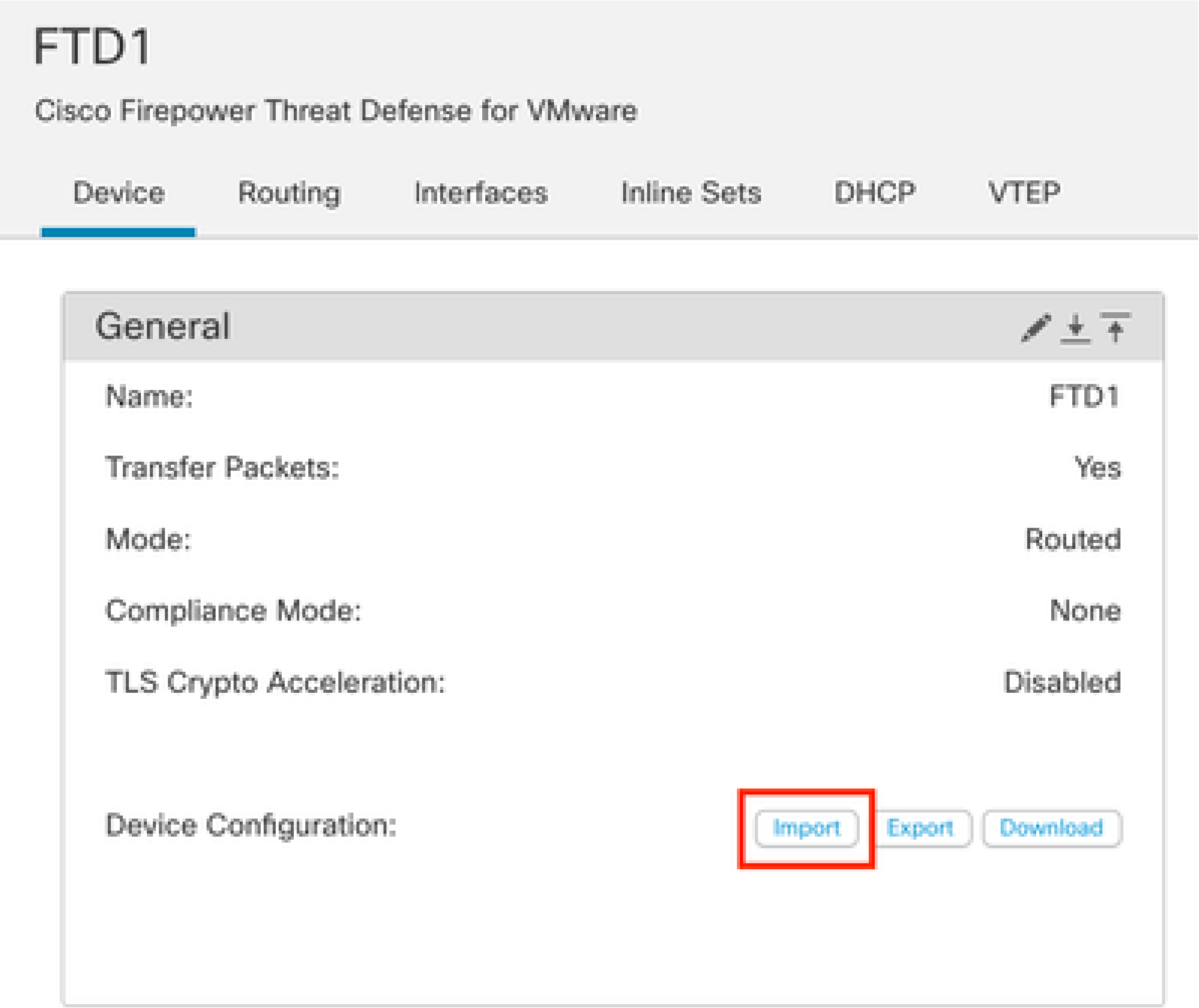
Unique NAT ID:†

☑ Transfer Packets

† Either host or NAT ID is required.

For additional details, check the Firepower Management Center Configuration Guide, Add Devices to the Firepower Management Center

11. Navigate to **Device** > **Device Management** > **select the FTD** > **Device** and click **import**. A warning shows asking for your confirmation to replace the device configuration, click **yes**.



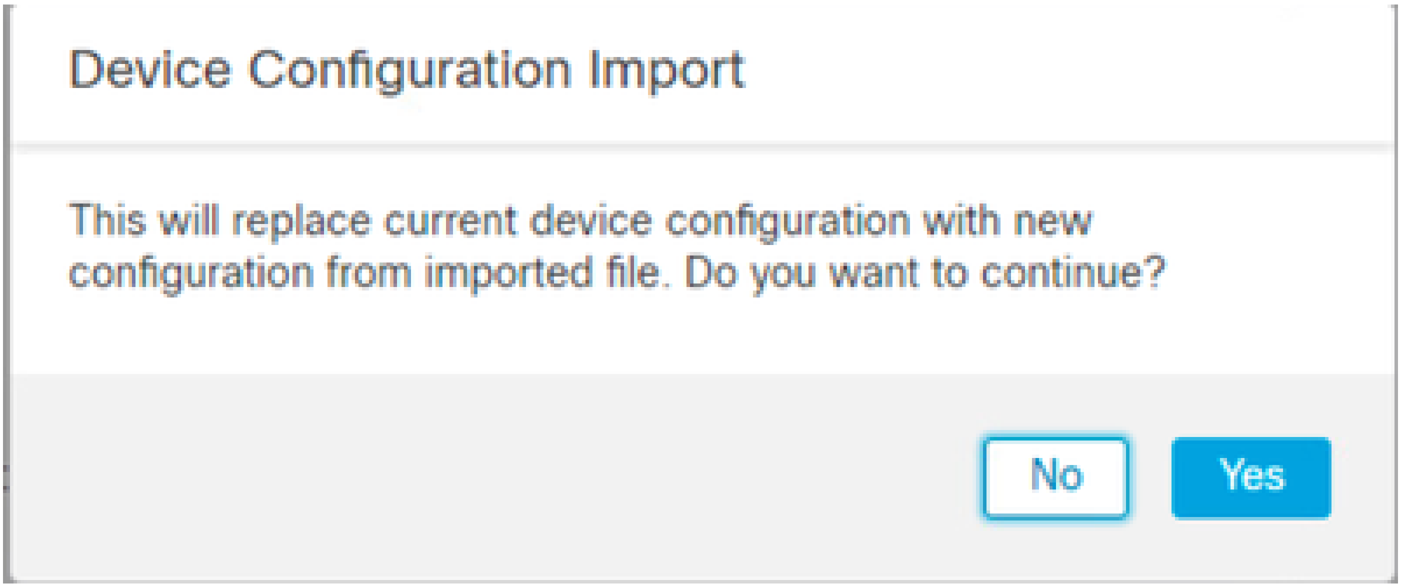
FTD1

Cisco Firepower Threat Defense for VMware

General

Name:	FTD1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled

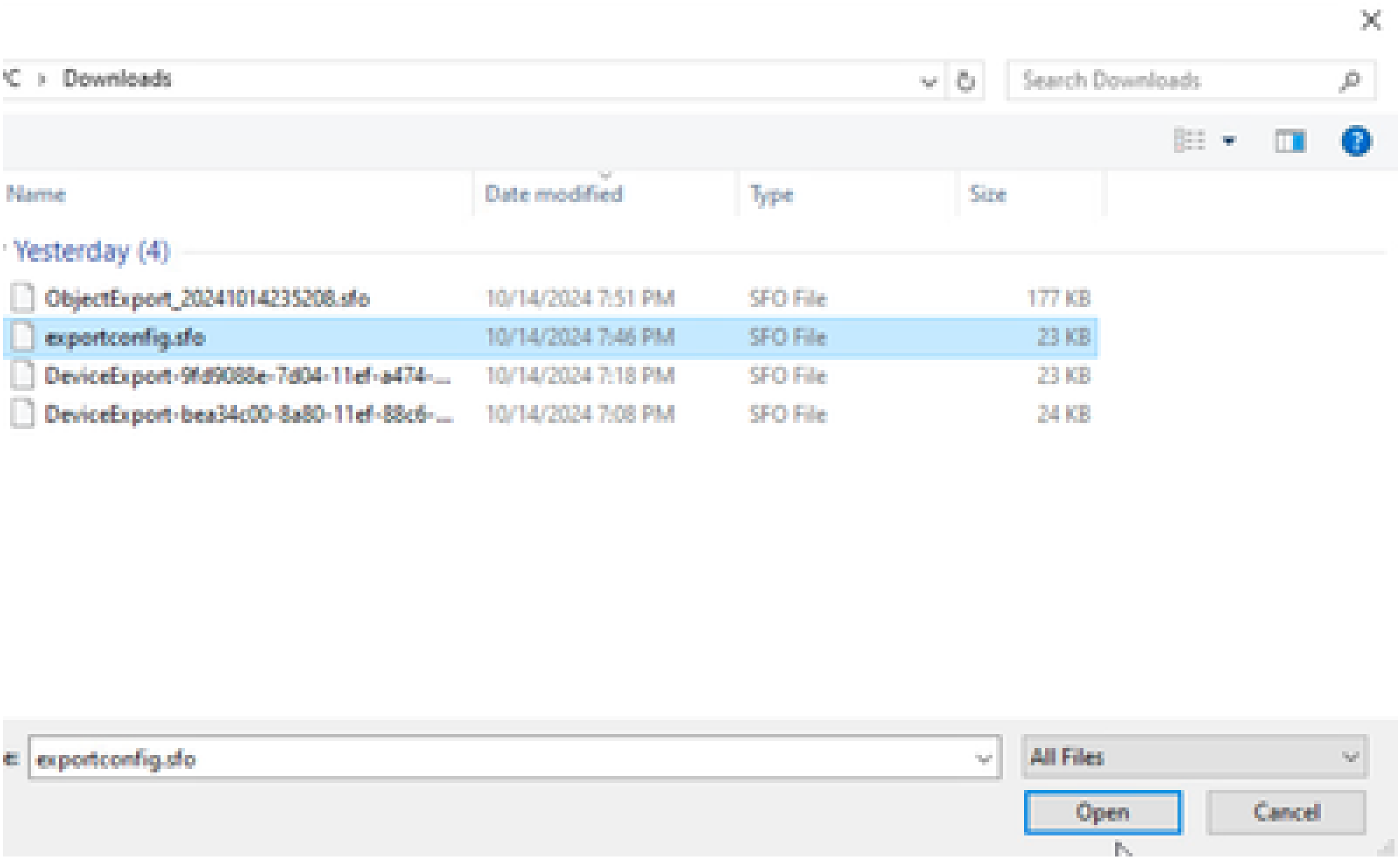
Device Configuration:



Device Configuration Import

This will replace current device configuration with new configuration from imported file. Do you want to continue?

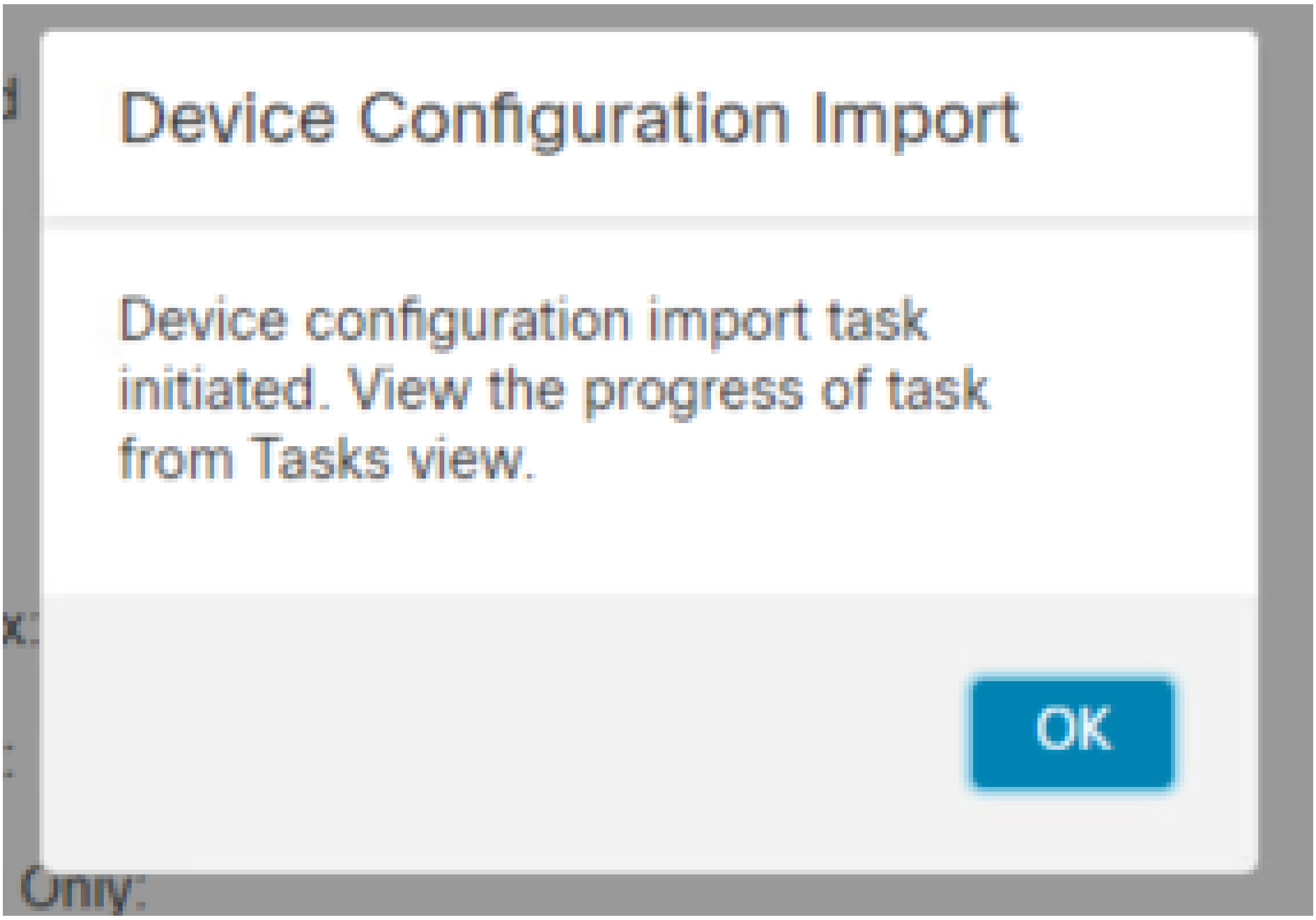
12. Select the import configuration file which must be .SFO extension, click **upload**, and you see a message appears indicating that the import has started.



Name	Date modified	Type	Size
Yesterday (4)			
ObjectExport_20241014235208.sfo	10/14/2024 7:51 PM	SFO File	177 KB
exportconfig.sfo	10/14/2024 7:46 PM	SFO File	23 KB
DeviceExport-9fd9088e-7d04-11ef-a474-...	10/14/2024 7:18 PM	SFO File	23 KB
DeviceExport-bea34c00-8a80-11ef-88c6-...	10/14/2024 7:08 PM	SFO File	24 KB

e: exportconfig.sfo

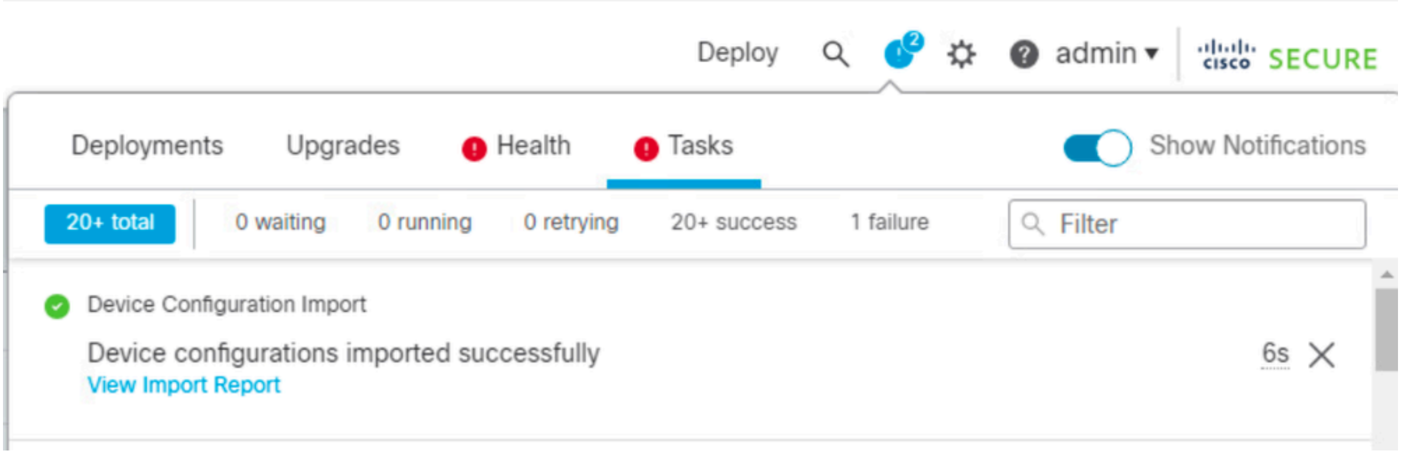
All Files



Device Configuration Import

Device configuration import task initiated. View the progress of task from Tasks view.

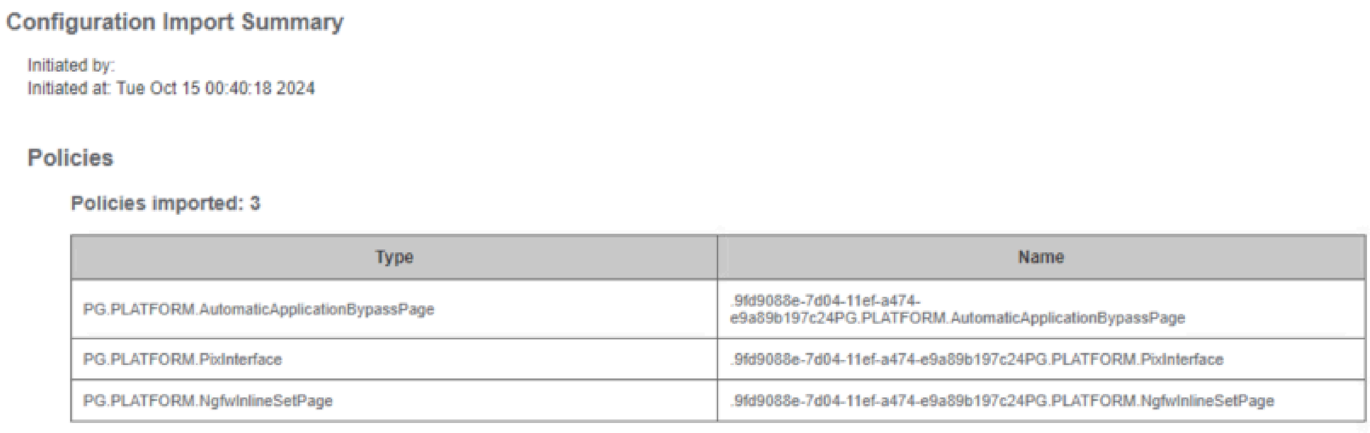
13. Finally, an alert is displayed and a report is generated automatically when the import is complete, allowing you to review the objects and policies that have been imported.



Device Configuration Import

Device configurations imported successfully

View Import Report



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

Verify

After completing the migration, verify that the FTD device is correctly registered and functioning with the destination FMC:

- Check the device status on the destination FMC.
- Make sure that all policies and configurations are correctly applied.
- Perform a test to confirm that the device is operational.

Troubleshoot

If you encounter any issues during the migration process, consider these troubleshooting steps:

- Verify network connectivity between the FTD device and both FMCs.
- Make sure that the software version on both FMCs are the same.
- Check the alerts on both FMCs for any error message or warnings.

Related Information

- Cisco Secure Firewall Management Center Administration Guide
- Configure, Verify and Troubleshoot Firepower Device Registration