Migrazione di un FTD da un FMC a un altro FMC

Sommario

Introduzione

In questo documento viene descritto come eseguire la migrazione di un dispositivo Cisco Firepower Threat Defense (FTD) da un centro di gestione di Firepower all'altro.

Prerequisiti

Prima di avviare il processo di migrazione, assicurarsi di disporre dei seguenti prerequisiti:

- accedere ai CCP di origine e di destinazione;
- Credenziali amministrative per i CCP e i FTD.
- Esegue il backup della configurazione corrente di FMC.
- Accertarsi che i dispositivi FTD che eseguono una versione software compatibile con il CCP di destinazione.
- Assicurarsi che il CCP di destinazione abbia la stessa versione del CCP di origine.

Requisiti

- Entrambi i CCP devono eseguire versioni software compatibili.
- Connettività di rete tra il dispositivo FTD e entrambi i CCP.
- Adeguato storage e risorse sul CCP di destinazione per ospitare il dispositivo FTD.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Cisco Firepower Threat Defense Virtual (FTDv) versione 7.2.5

Firepower Management Center Virtual (FMCv) versione 7.2.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

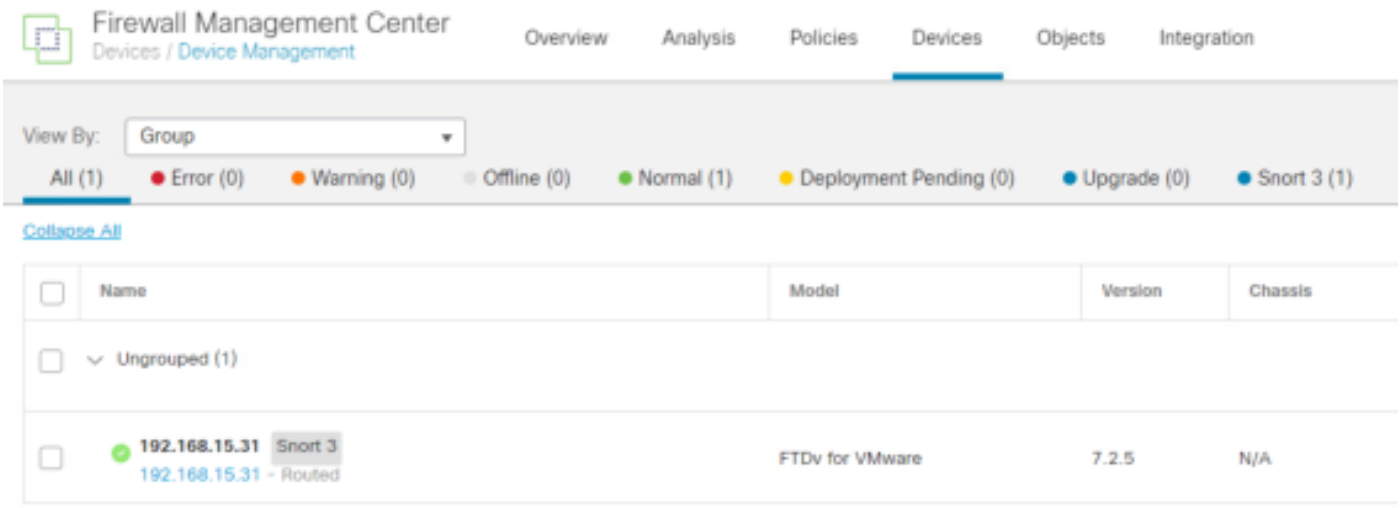
La migrazione di un dispositivo FTD da un CCP a un altro comporta diverse operazioni, tra cui la cancellazione della registrazione del dispositivo dal CCP di origine, la preparazione del CCP di destinazione e la nuova registrazione del dispositivo. Questo processo garantisce che tutte le policy e le configurazioni vengano trasferite e applicate correttamente.

Configurazione

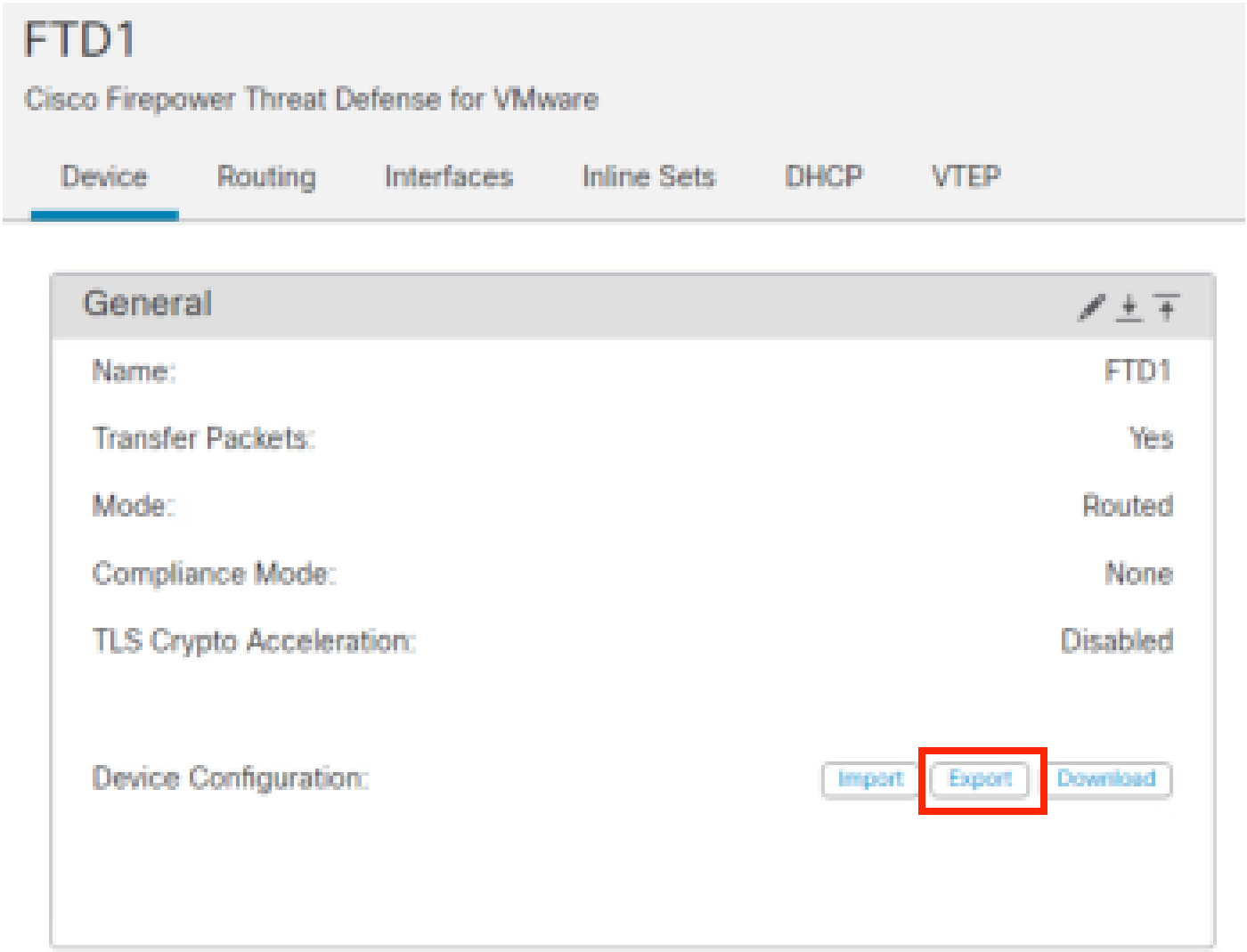
Configurazioni

1. Accedere al CCP di origine.

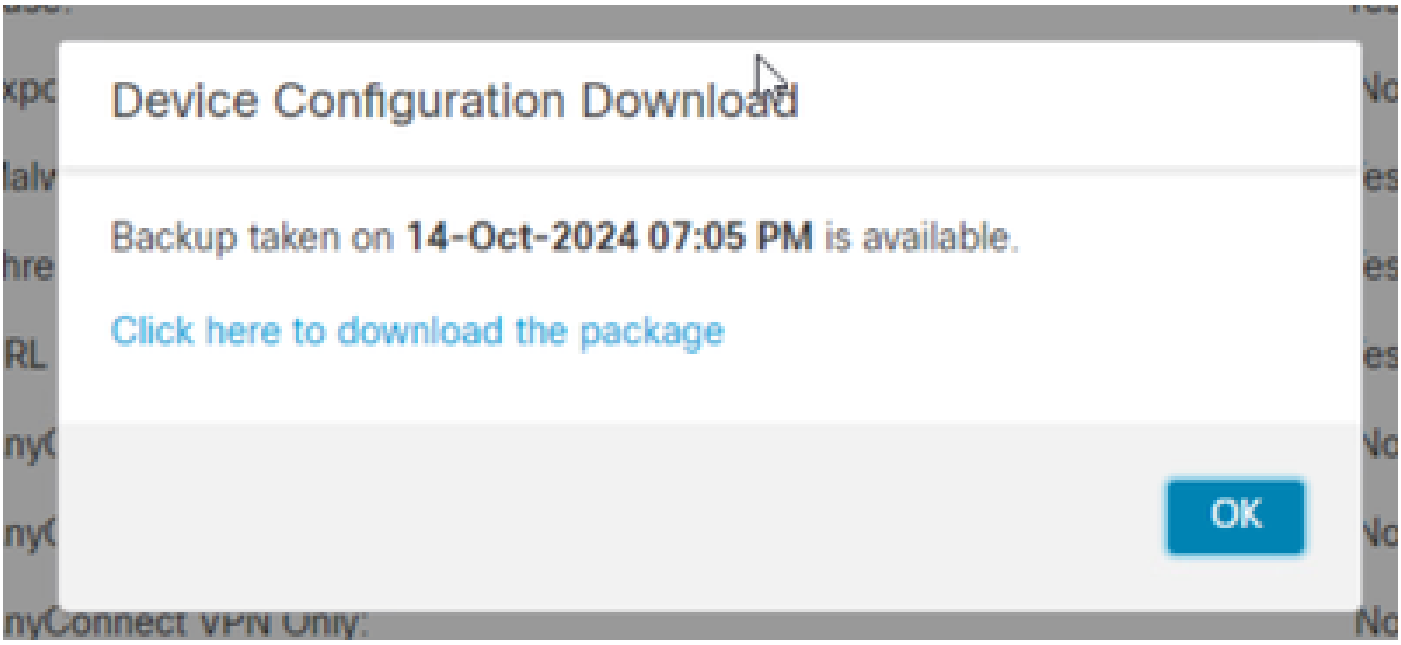
2. Passare a Dispositivi > Gestione dispositivi e selezionare il dispositivo di cui eseguire la migrazione.

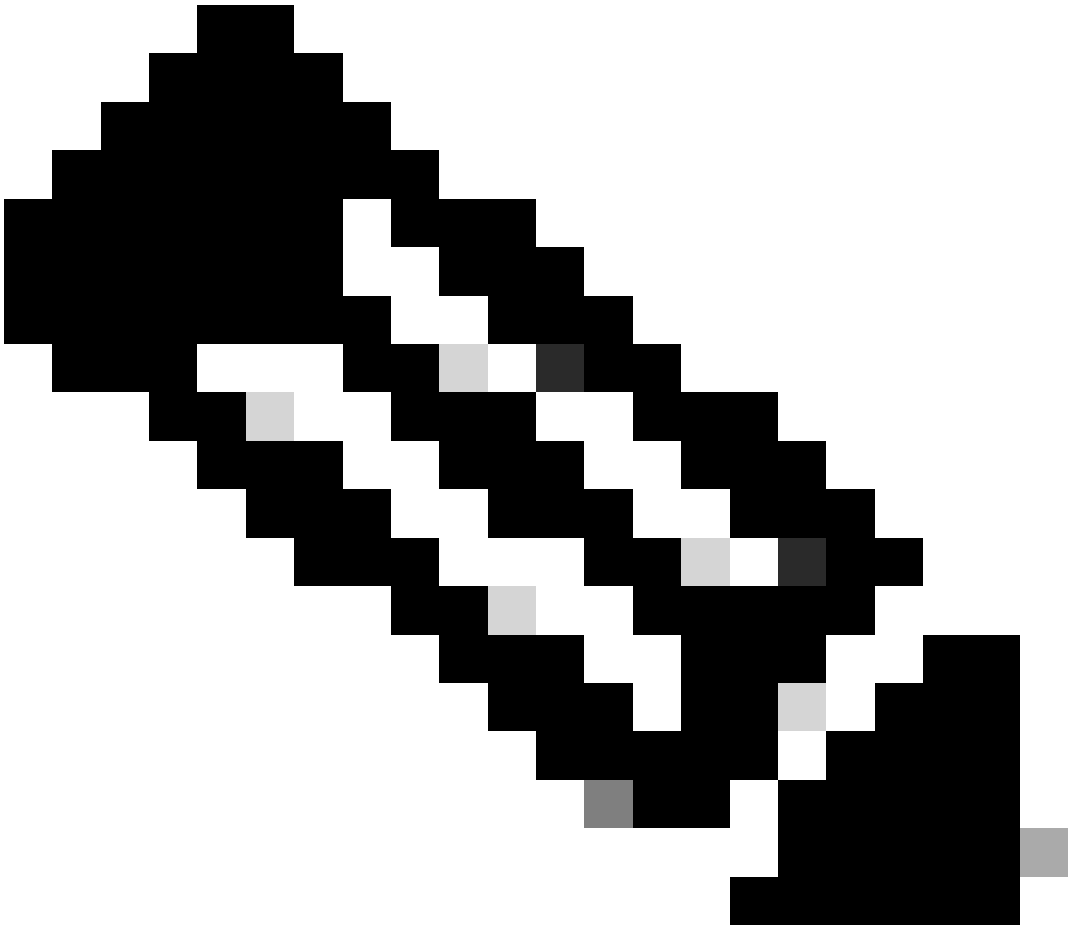


3. All'interno della sezione del dispositivo, passare a dispositivo e fare clic su esporta per esportare le impostazioni del dispositivo.



4. Una volta esportata la configurazione, è necessario scaricarla.

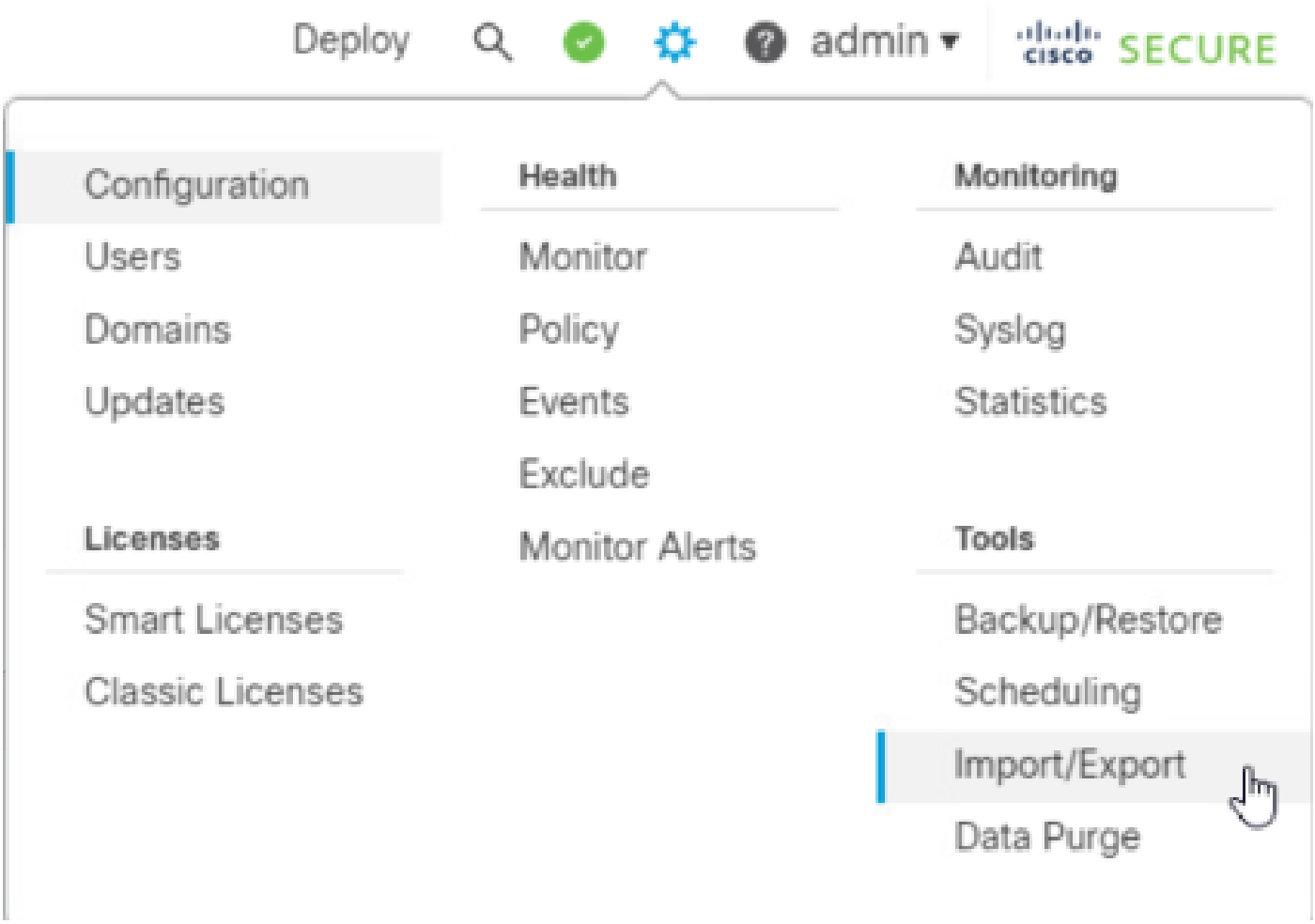


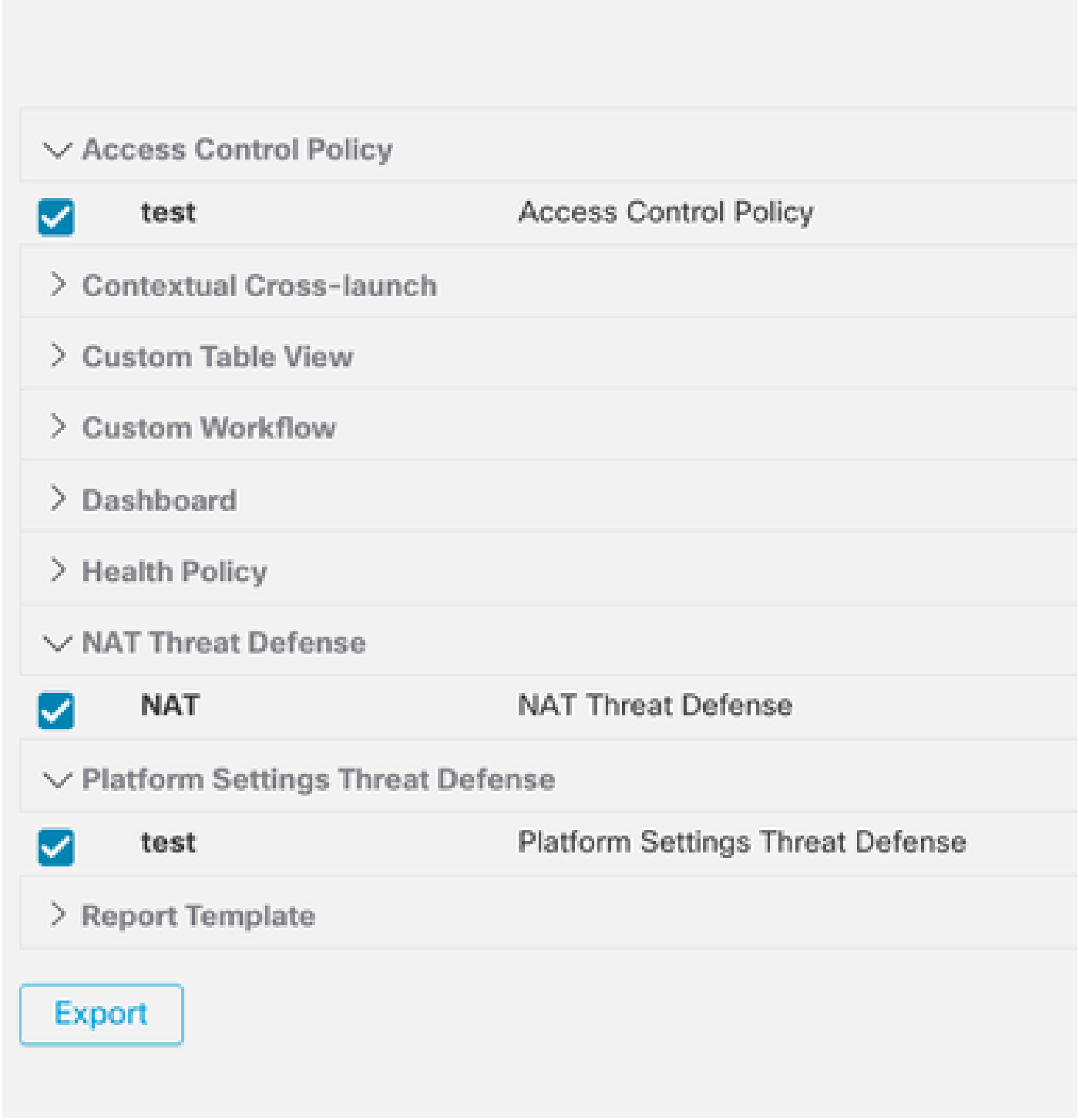


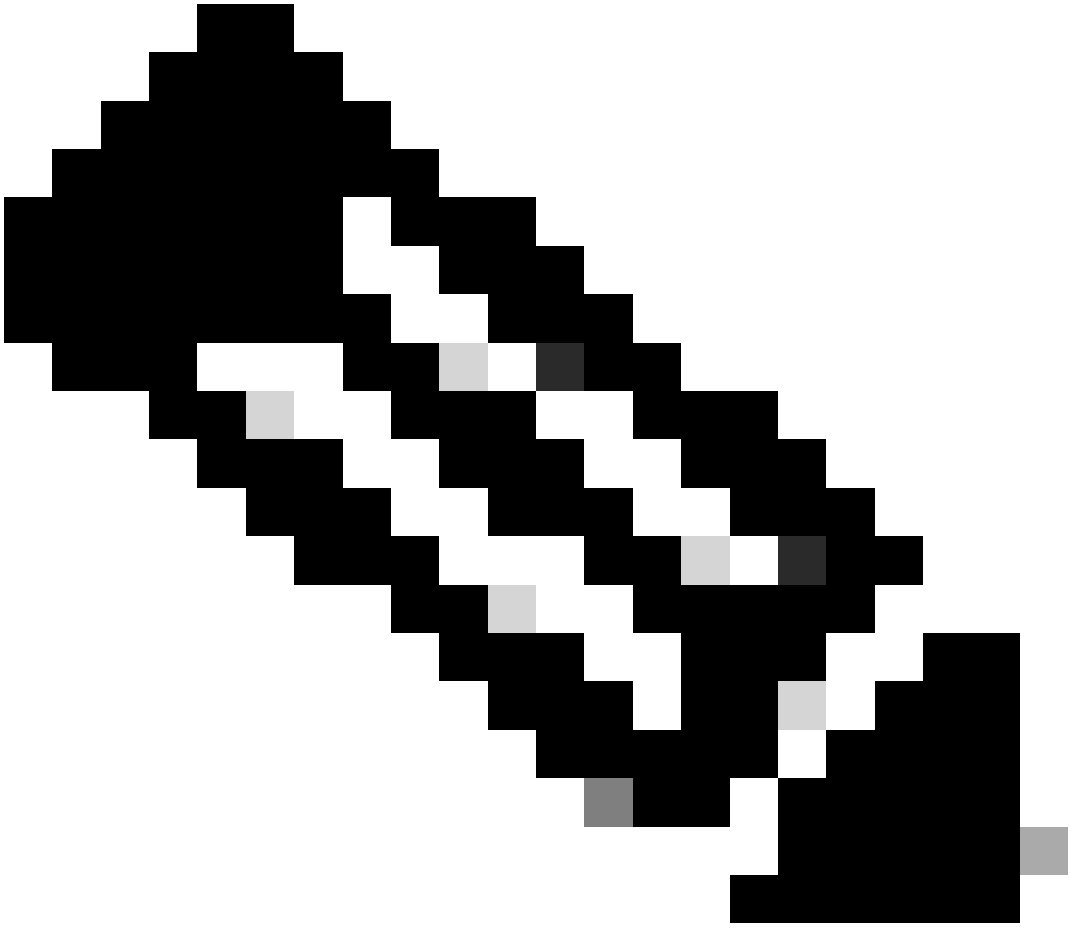
Nota: il file scaricato deve contenere l'estensione .SFO e contenere le informazioni di

configurazione del dispositivo, ad esempio indirizzi IP, aree di protezione, route statiche e altre impostazioni del dispositivo.

5. È necessario esportare i criteri associati al dispositivo, selezionare Sistema > Strumenti > Importa/Esporta, selezionare i criteri da esportare e fare clic su Esporta.

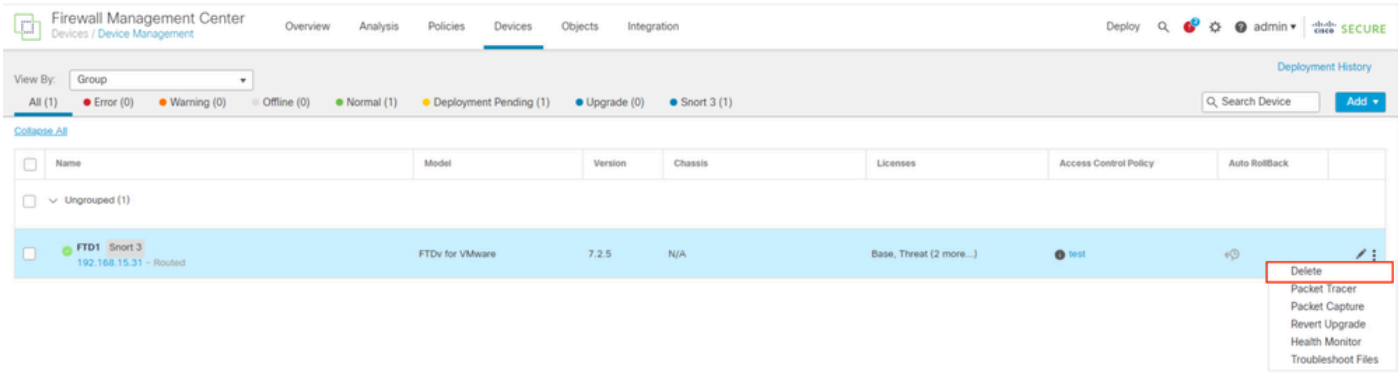



Access Control Policy
test
Access Control Policy
Contextual Cross-launch
Custom Table View
Custom Workflow
Dashboard
Health Policy
NAT Threat Defense
NAT
NAT Threat Defense
Platform Settings Threat Defense
test
Platform Settings Threat Defense
Report Template
Export



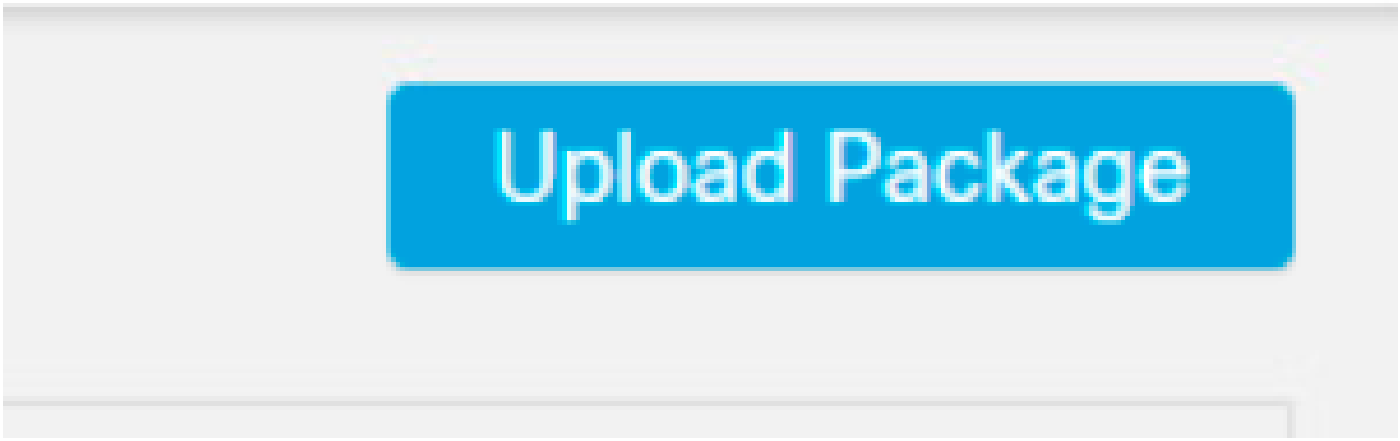
Nota: assicurarsi che il file SFO sia stato scaricato correttamente. Il download viene eseguito automaticamente dopo aver fatto clic su Esporta. Questo file contiene le policy di controllo dell'accesso, le impostazioni della piattaforma, le policy NAT e altre policy indispensabili per la migrazione poiché non vengono esportate insieme alla configurazione del dispositivo e devono essere caricate manualmente nel CCP di destinazione.

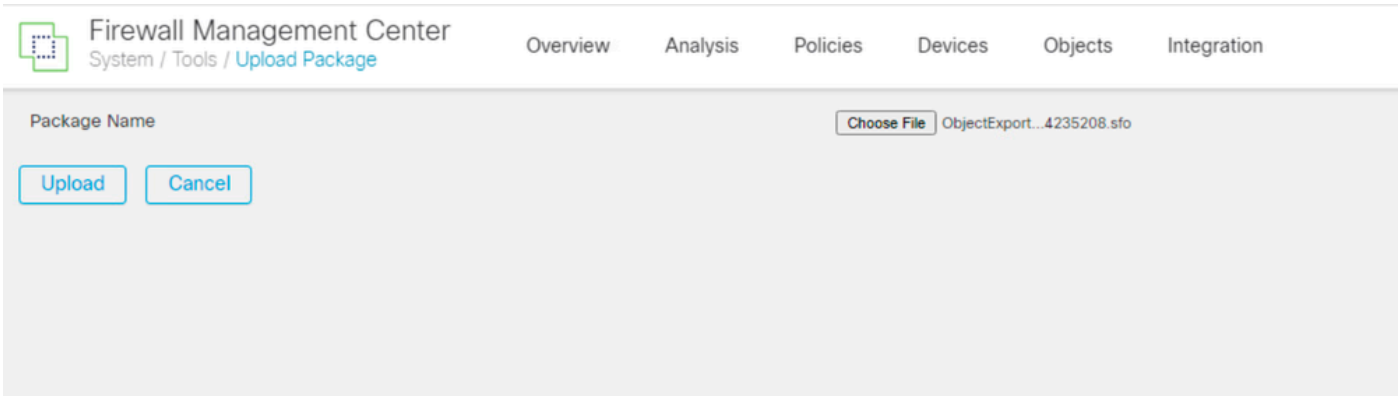
6. Annullare la registrazione del dispositivo FTD dal FMC, selezionare Dispositivi > Gestione dispositivi, fare clic sui tre punti verticali sul lato destro e selezionare Elimina.



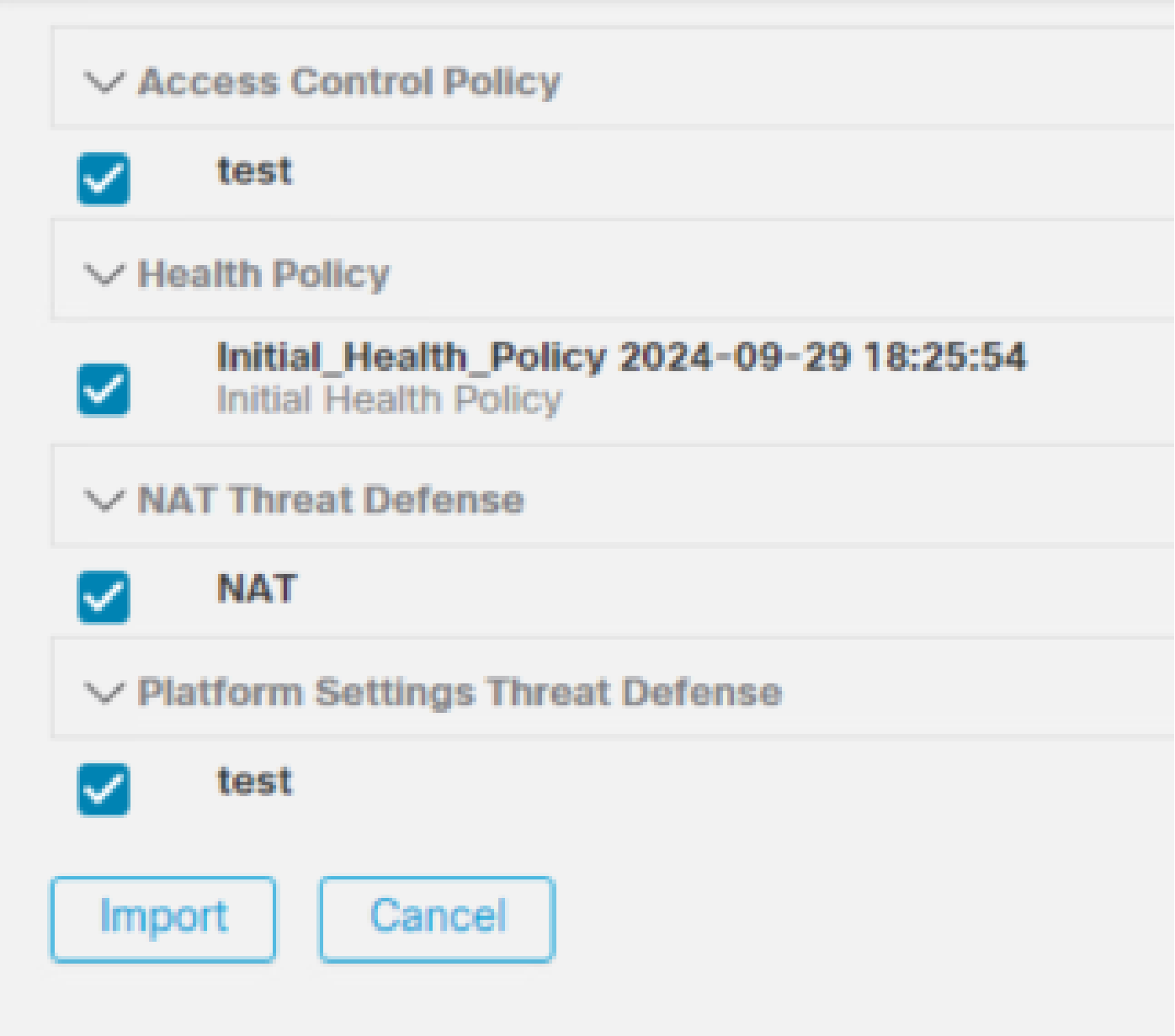
7. Preparare il CCP di destinazione:

- Accedere al CCP di destinazione.
- Verificare che il CCP sia pronto ad accettare il nuovo dispositivo importando i criteri del CCP di origine scaricati al passaggio 5. Selezionare Sistema > Strumenti > Importa/esporta e fare clic su Carica package. Caricare il file da importare e fare clic su upload.

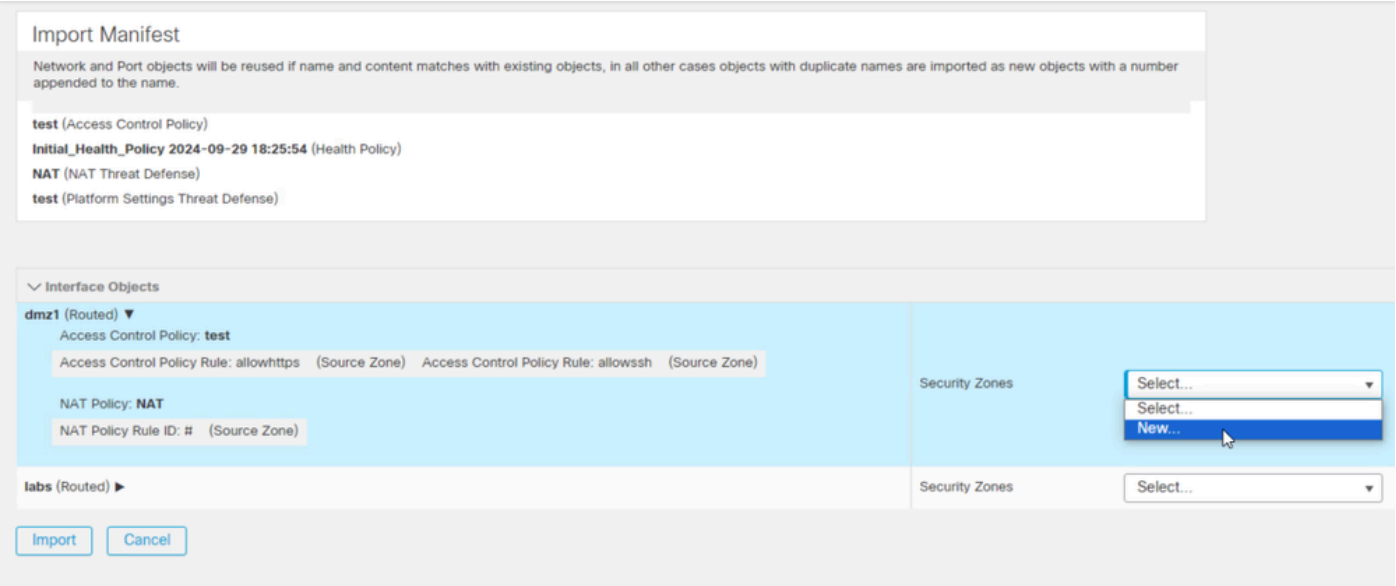




8. Selezionare i criteri da importare nel CCP di destinazione.

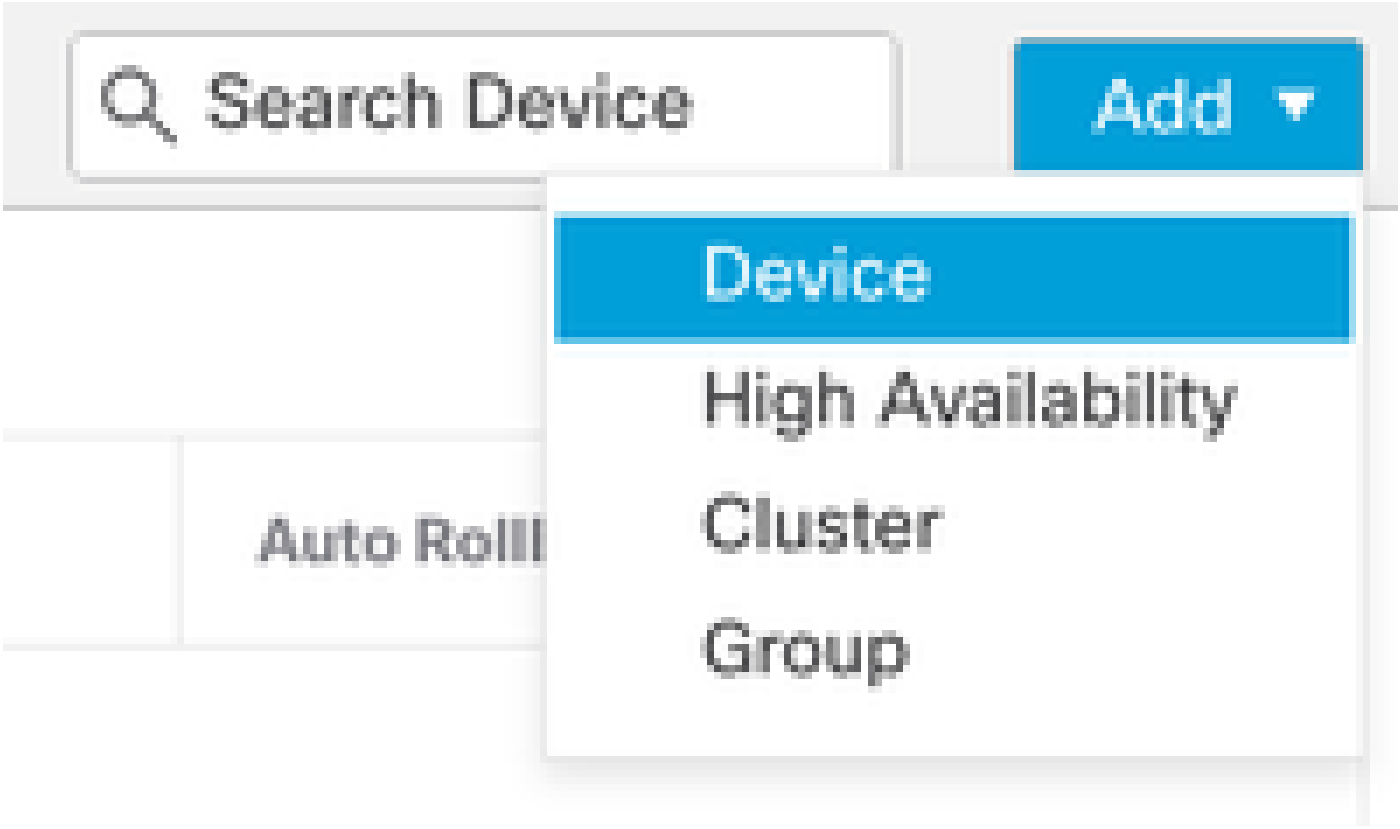


9. Nel manifesto di importazione, selezionare un'area di protezione o crearne una nuova da assegnare all'oggetto interfaccia e fare clic su importa.



10. Registrare l'FTD nel CCP di destinazione:

- Nel FMC di destinazione, selezionare Device > Management (Dispositivo > Scheda Gestione) e selezionare Add > Device (Aggiungi > Dispositivo).
- Completate il processo di registrazione rispondendo ai prompt.



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

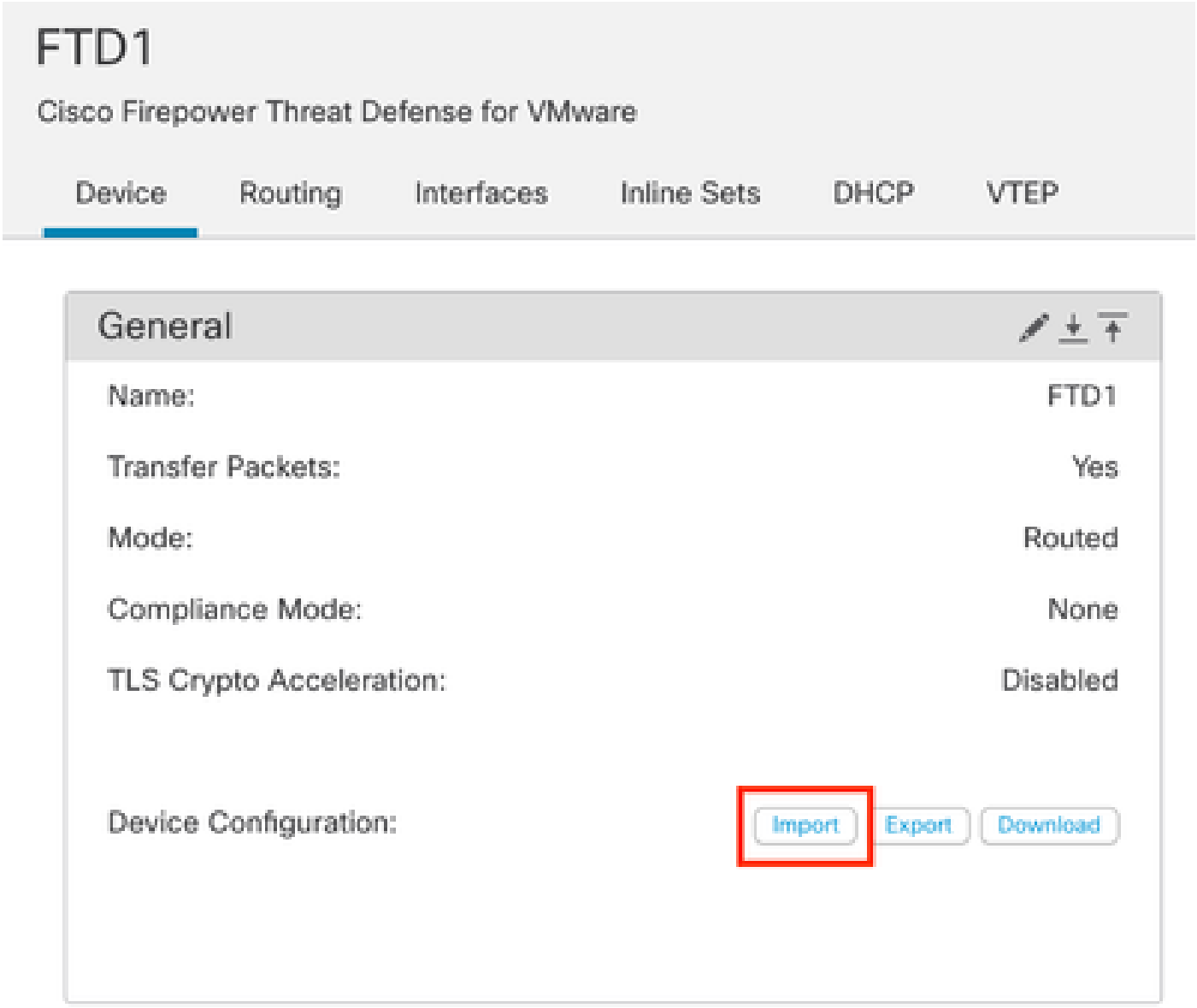
† Either host or NAT ID is required.

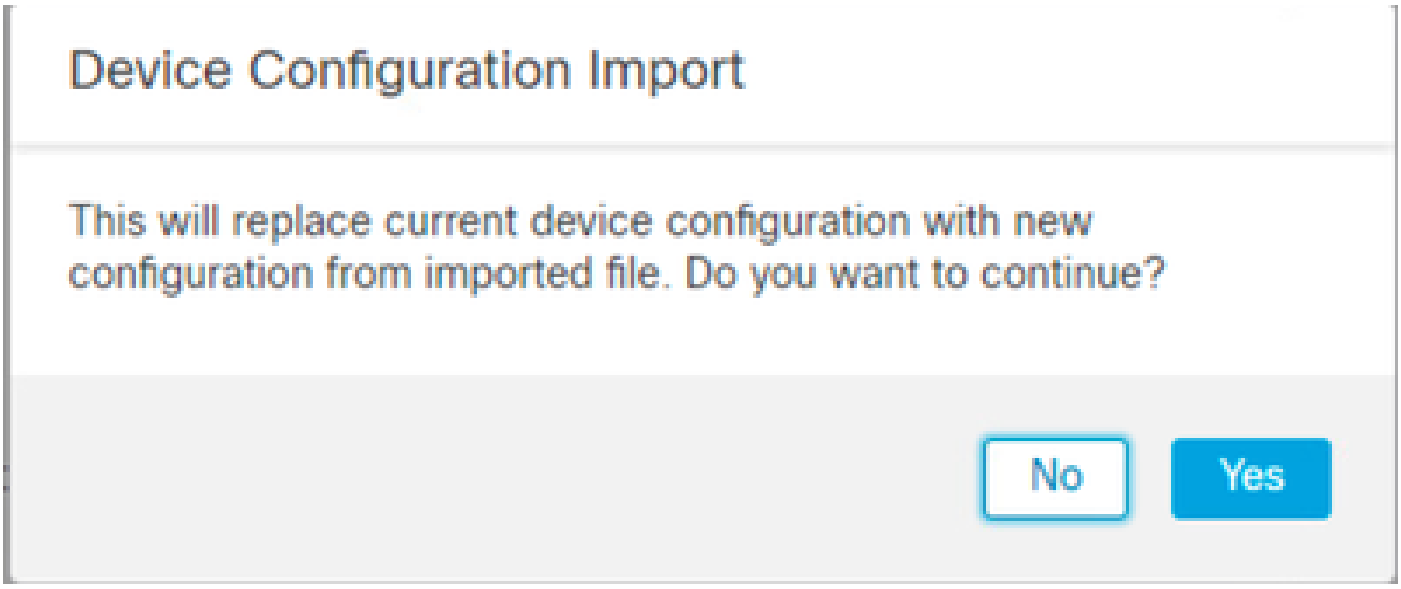
Cancel

Register

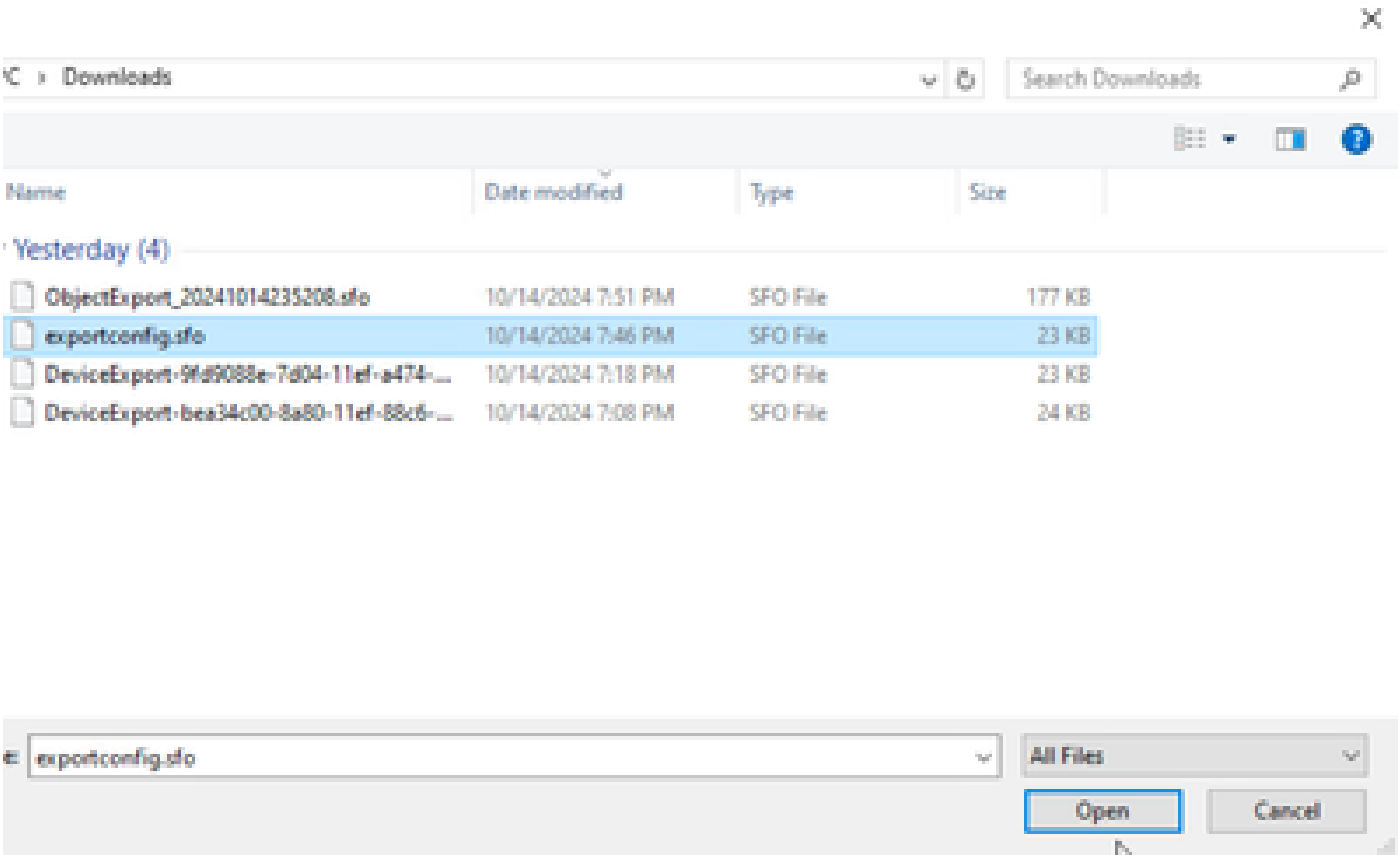
Per ulteriori informazioni, consultare la guida alla configurazione di Firepower Management Center, [Add Devices to the Firepower Management Center]

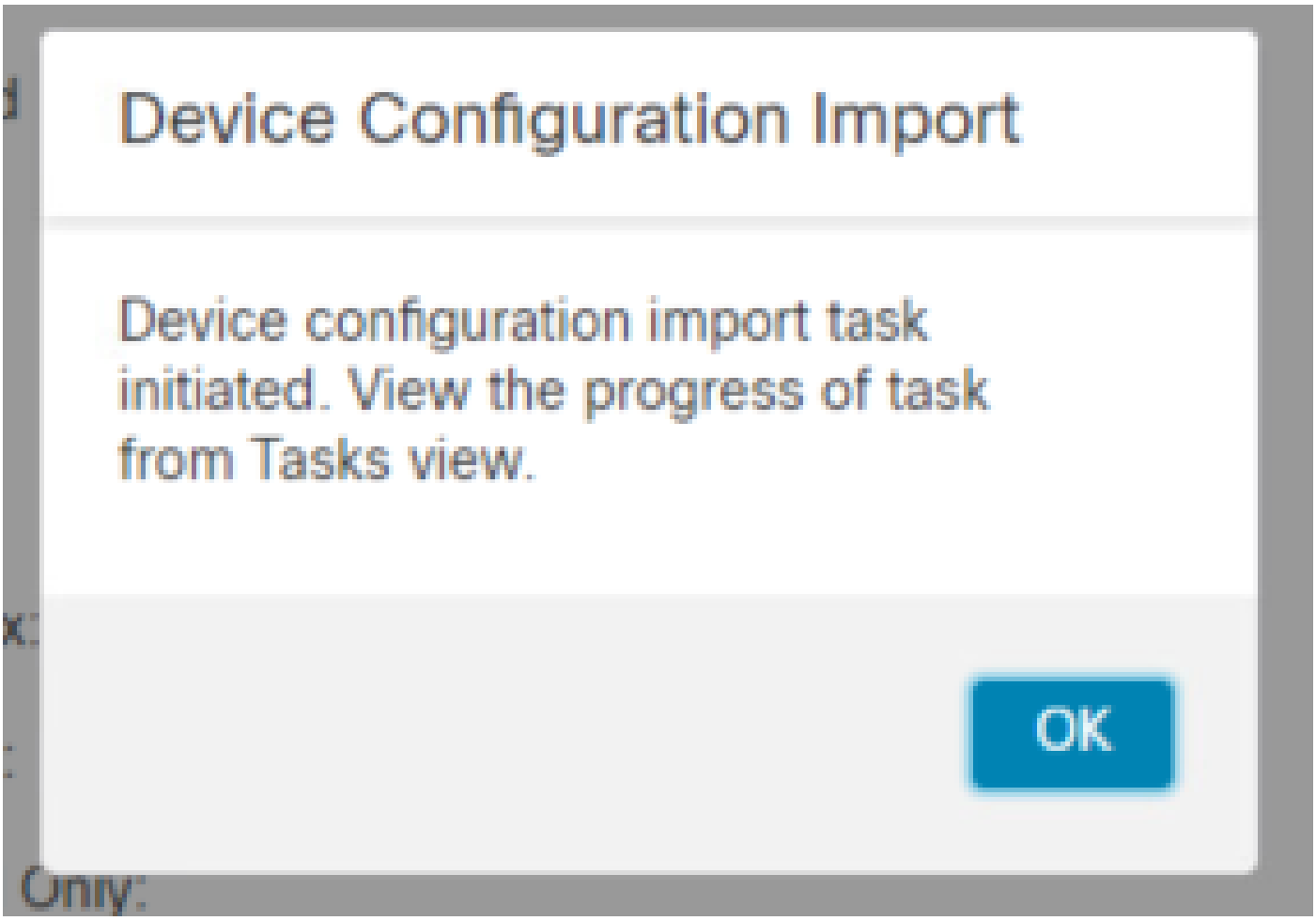
11. Passare a Dispositivo > Gestione dispositivi > selezionare FTD > Dispositivo e fare clic su Importa. Viene visualizzato un avviso in cui viene richiesto di confermare la sostituzione della configurazione del dispositivo. Fare clic su Sì.



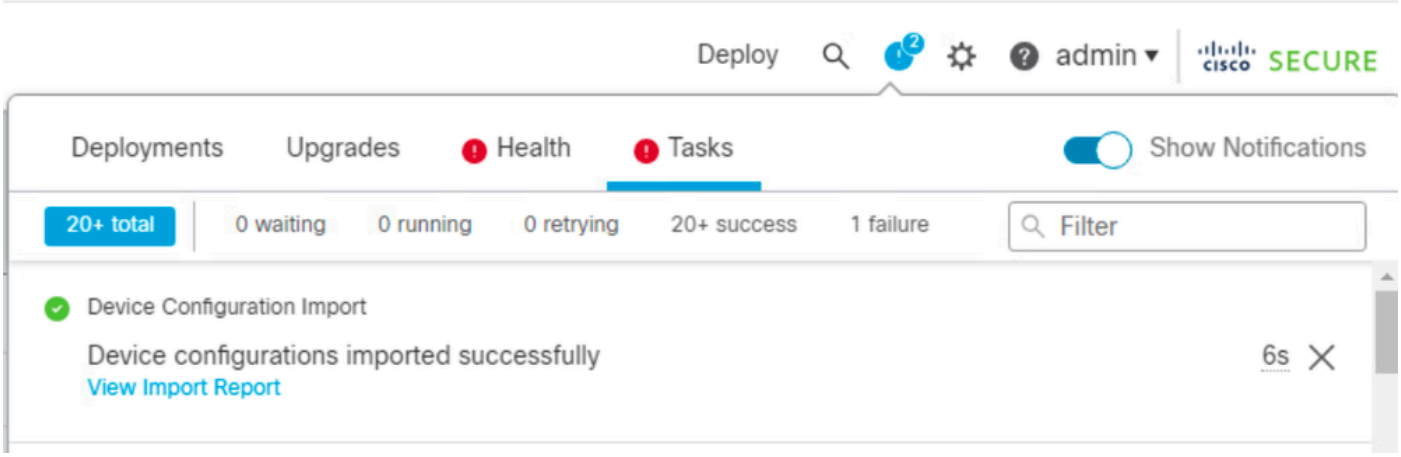


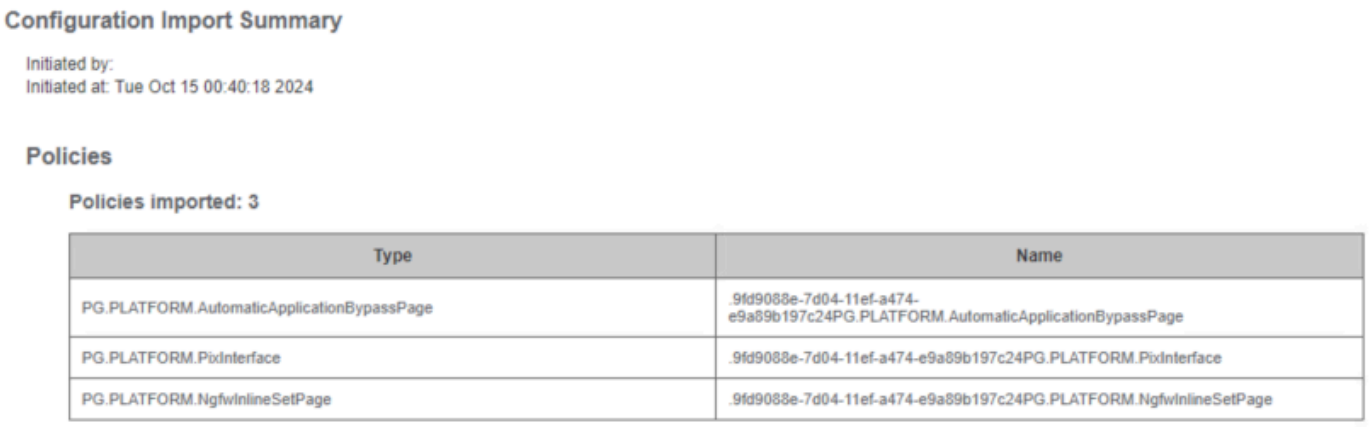
12. Selezionare il file di configurazione di importazione che deve avere l'estensione .SFO, fare clic su carica e verrà visualizzato un messaggio che indica che l'importazione è stata avviata.





13. Infine, al termine dell'importazione viene visualizzato un avviso e viene generato automaticamente un report che consente di esaminare gli oggetti e i criteri importati.





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

Verifica

Al termine della migrazione, verificare che il dispositivo FTD sia registrato correttamente e funzioni correttamente con il CCP di destinazione:

- Controllare lo stato della periferica nel CCP di destinazione.
- Accertarsi che tutti i criteri e le configurazioni siano applicati correttamente.
- Eseguire un test per verificare che il dispositivo sia in funzione.

Risoluzione dei problemi

In caso di problemi durante il processo di migrazione, considerare le seguenti procedure di risoluzione dei problemi:

- Verificare la connettività di rete tra il dispositivo FTD e entrambi i CCP.
- Verificare che la versione del software su entrambi i CCP sia la stessa.
- Verificare la presenza di eventuali messaggi di errore o avvisi negli avvisi di entrambi i CCP.

Informazioni correlate

- Guida all'amministrazione di Cisco Secure Firewall Management Center
- Configurazione, verifica e risoluzione dei problemi di registrazione delle periferiche Firepower

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).