한 FMC에서 다른 FMC로 FTD 마이그레이션

목차

소개

이 문서에서는 Cisco FTD(Firepower Threat Defense) 디바이스를 Firepower Management Center 간에 마이그레이션하는 방법에 대해 설명합니다.

사전 요구 사항

마이그레이션 프로세스를 시작하기 전에 다음 전제 조건을 갖추었는지 확인하십시오.

- 소스 및 대상 FMC 모두에 액세스합니다.
- FMC 및 FTD 모두에 대한 관리 자격 증명
- 현재 FMC 컨피그레이션을 백업합니다.
- 대상 FMC와 호환되는 소프트웨어 버전을 실행 중인 FTD 디바이스인지 확인합니다.
- 대상 FMC의 버전이 소스 FMC와 동일해야 합니다.

요구 사항

- 두 FMC 모두 호환 가능한 소프트웨어 버전을 실행해야 합니다.
- FTD 디바이스와 두 FMC 간의 네트워크 연결
- FTD 디바이스를 수용할 수 있는 대상 FMC의 적절한 스토리지 및 리소스

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

Cisco FTDv(Firepower Threat Defense Virtual) 버전 7.2.5

FMCv(firepower Management Center Virtual) 버전 7.2.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

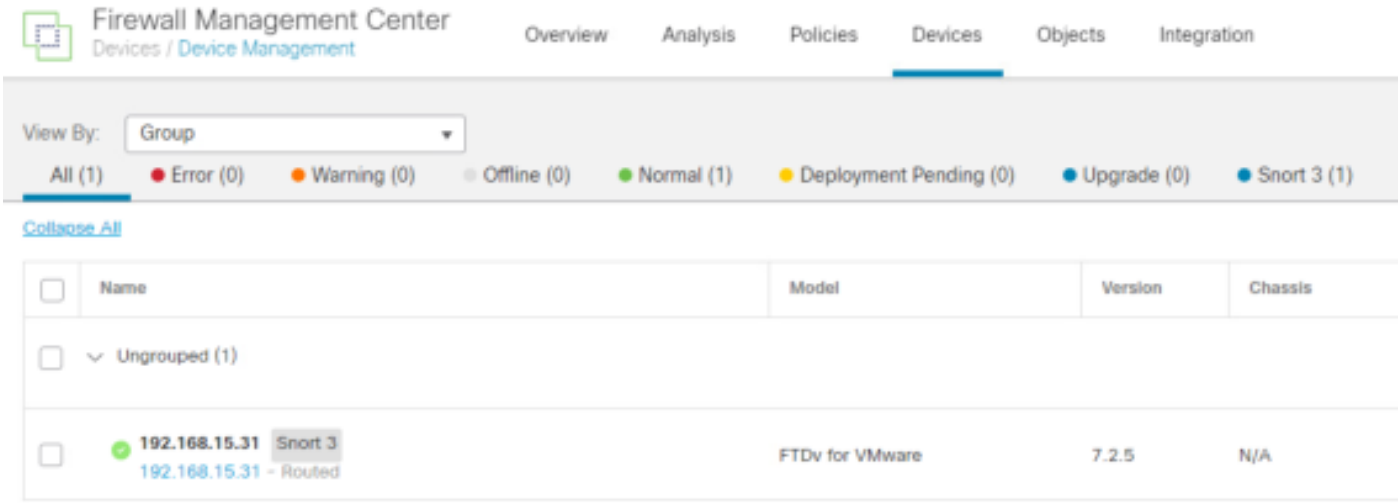
FTD 디바이스를 한 FMC에서 다른 FMC로 마이그레이션하려면 소스 FMC에서 디바이스 등록을 취소하고, 대상 FMC를 준비하고, 디바이스를 다시 등록하는 등 몇 가지 단계가 필요합니다. 이 프로세스는 모든 정책과 컨피그레이션이 올바르게 전송 및 적용되도록 보장합니다.

구성

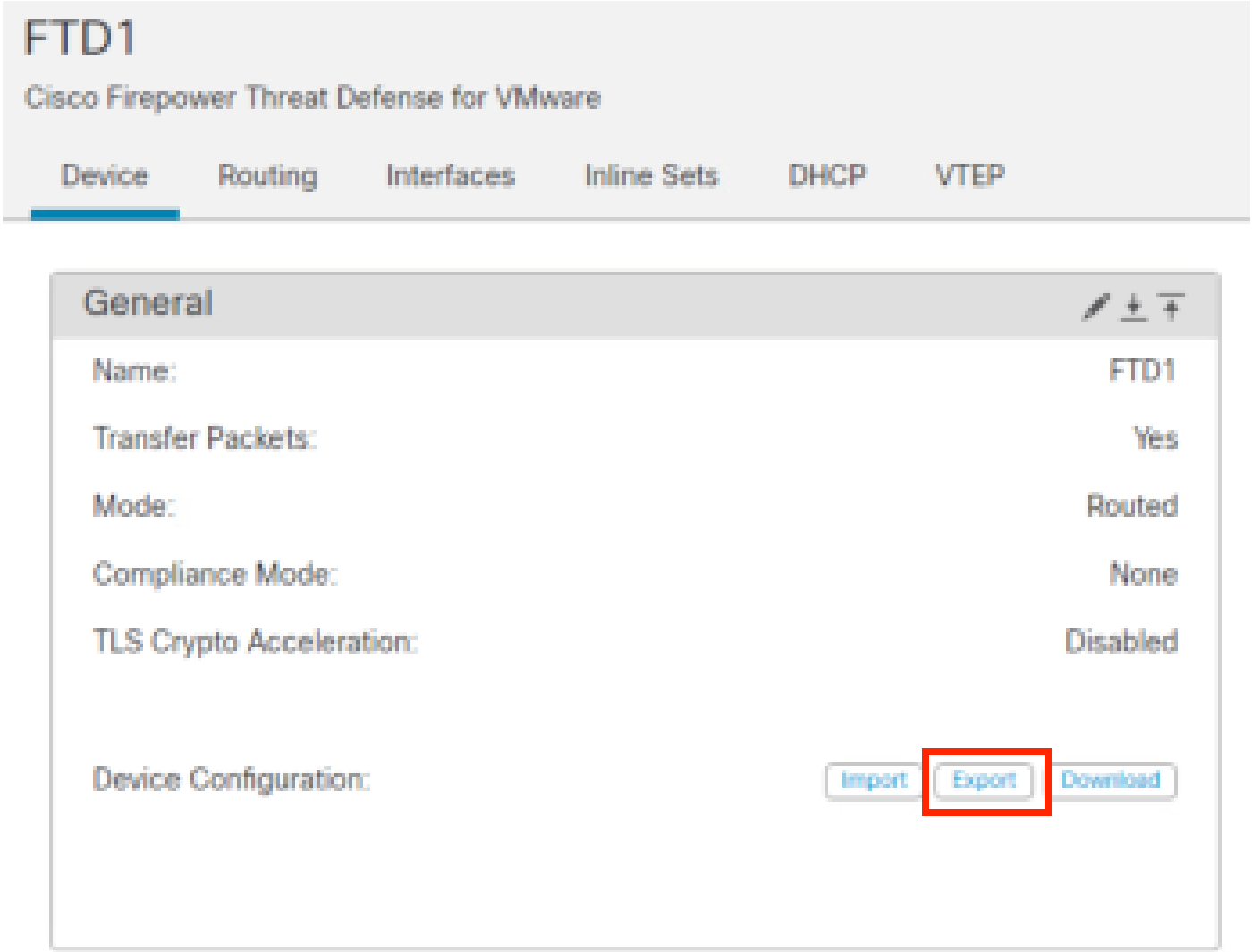
설정

1. 소스 FMC에 로그인합니다.

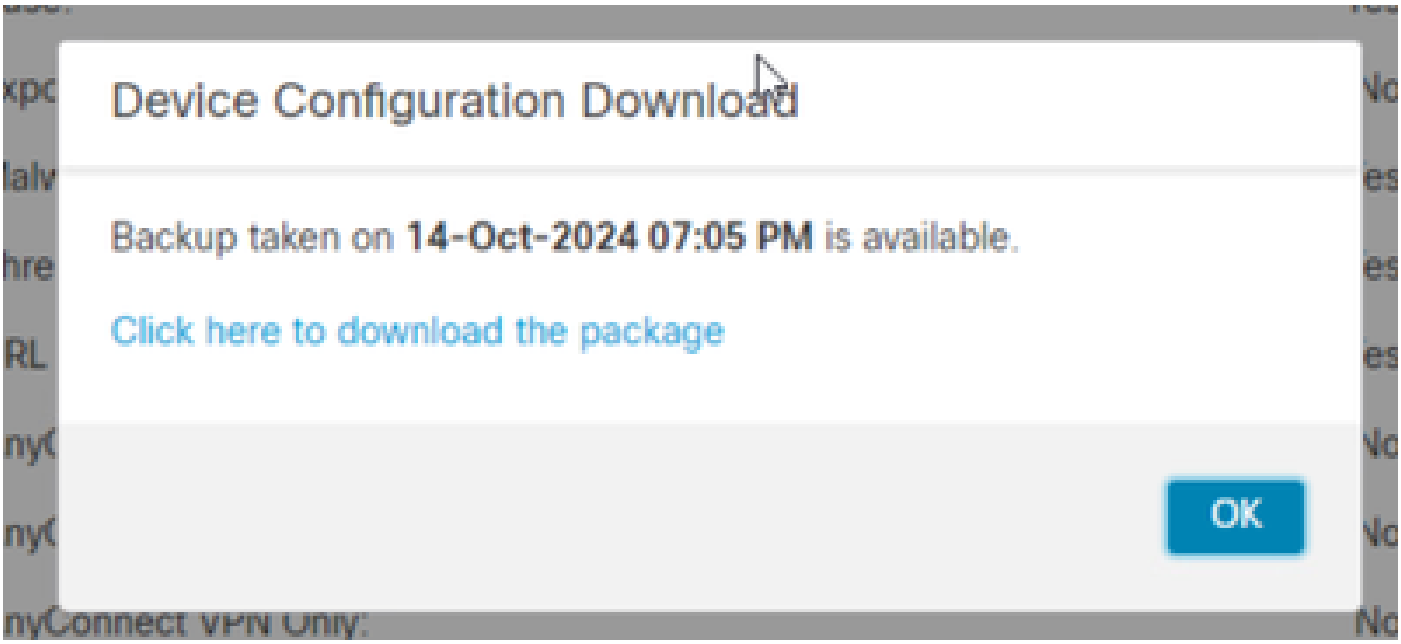
2. Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 마이그레이션할 디바이스를 선택합니다.

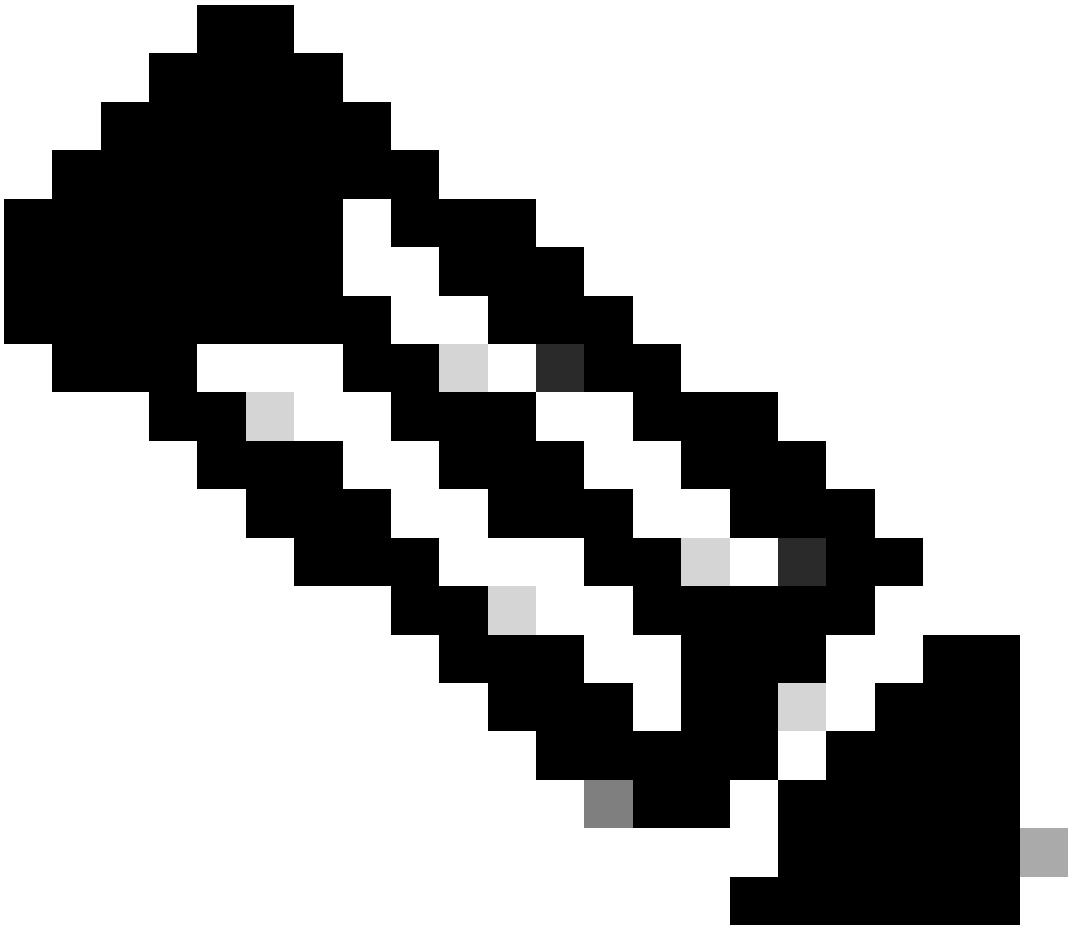


3. 장치 섹션에서 장치로 이동하고 export(내보내기)를 클릭하여 장치 설정을 내보냅니다.



4. 구성을 내보낸 후에는 다운로드해야 합니다.

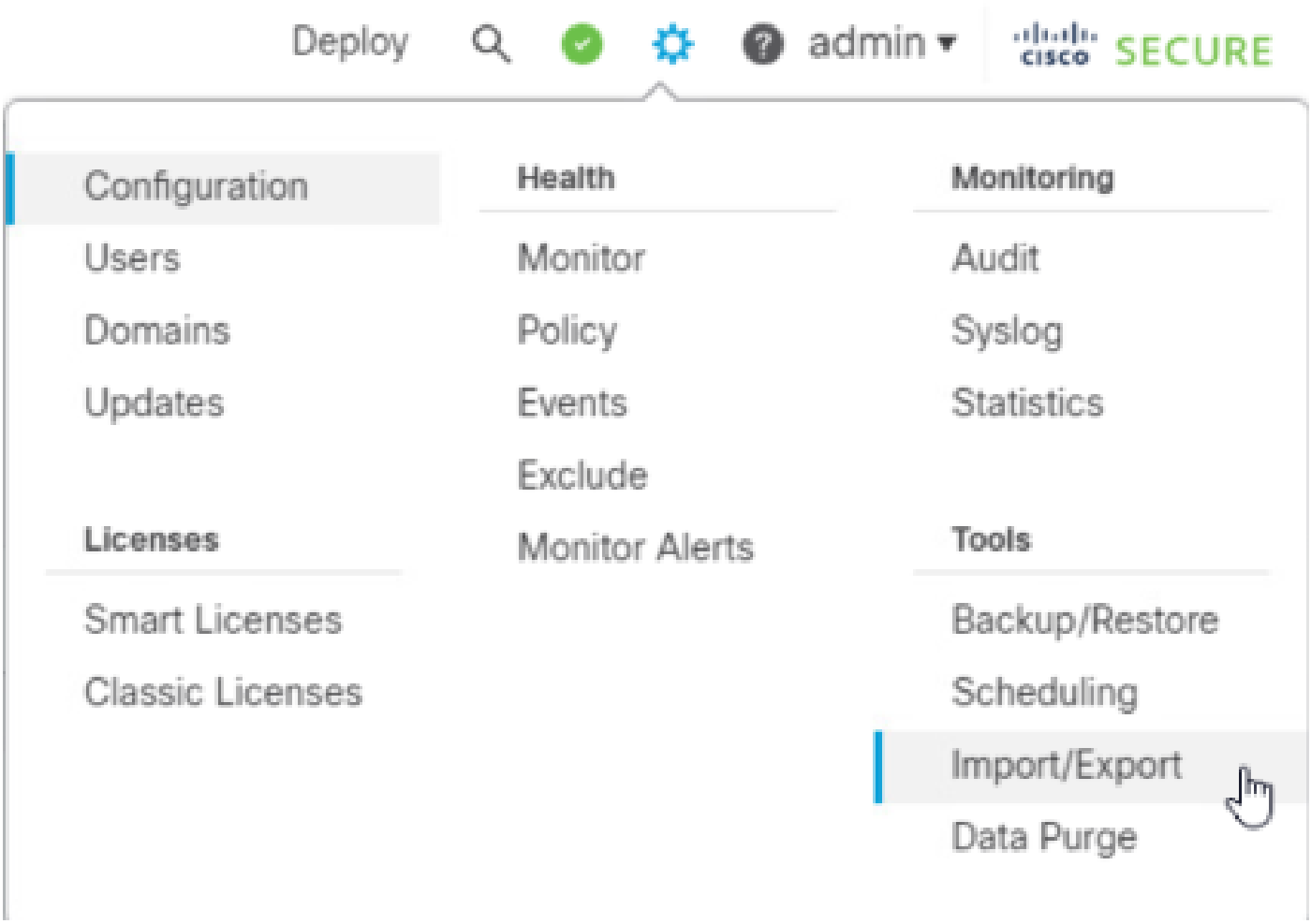


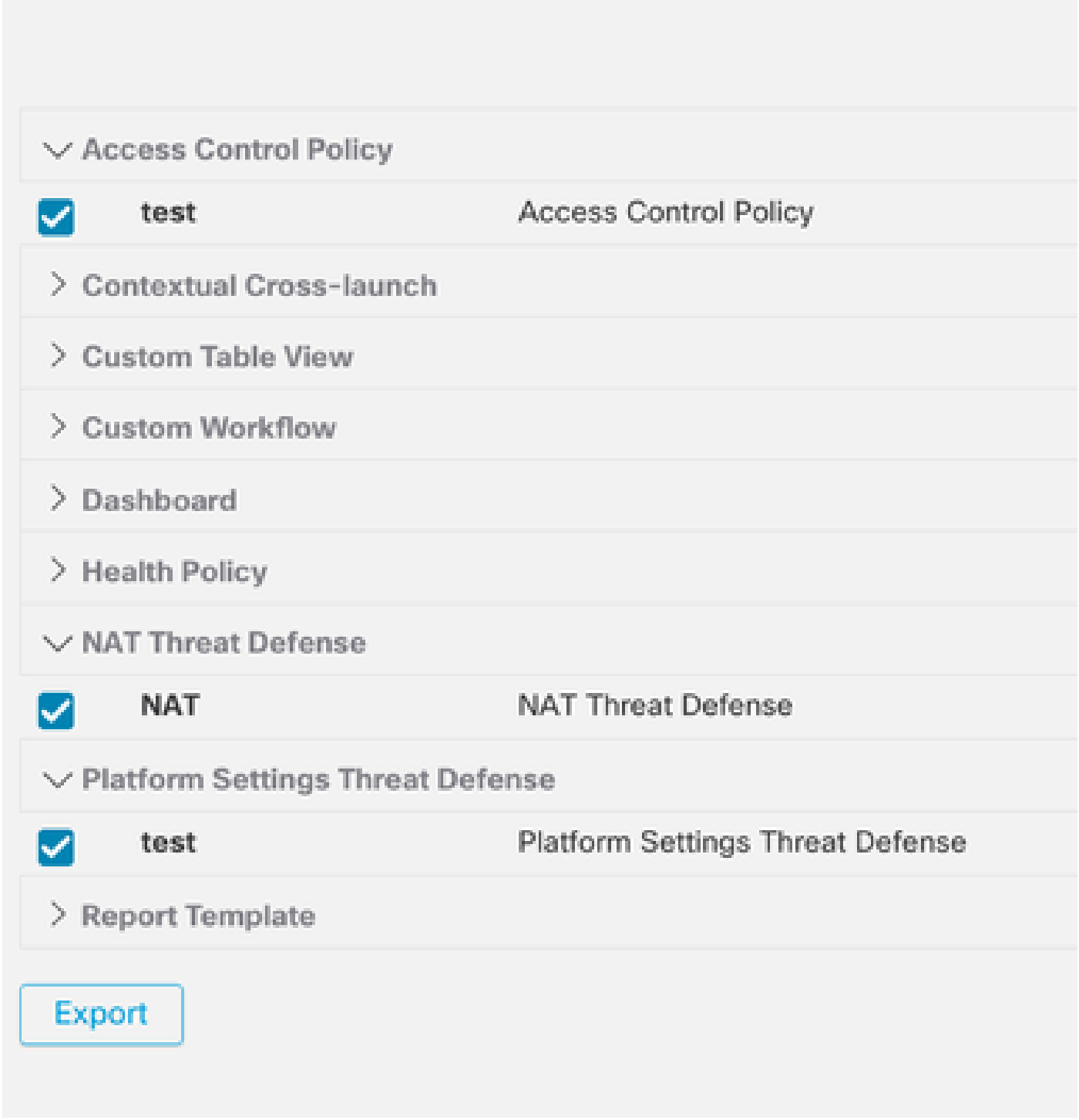


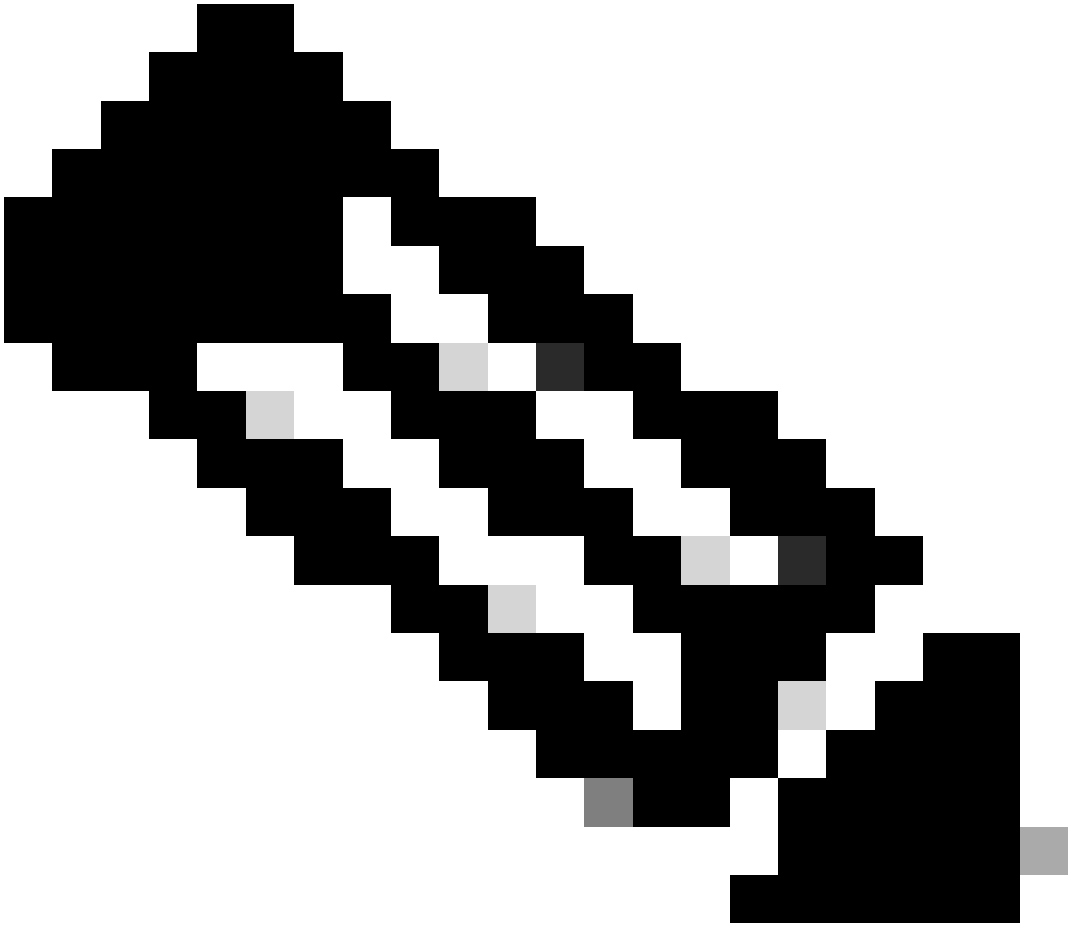
참고: 다운로드한 파일에는 .SFO 확장명이 포함되어야 하며, IP 주소, 보안 영역, 고정 경로

및 기타 디바이스 설정과 같은 디바이스 컨피그레이션 정보가 포함되어야 합니다.

5. 장치와 관련된 정책을 내보내고, 시스템 > 도구 > 가져오기/내보내기로 이동하여, 내보낼 정책을 선택하고 내보내기를 클릭합니다.



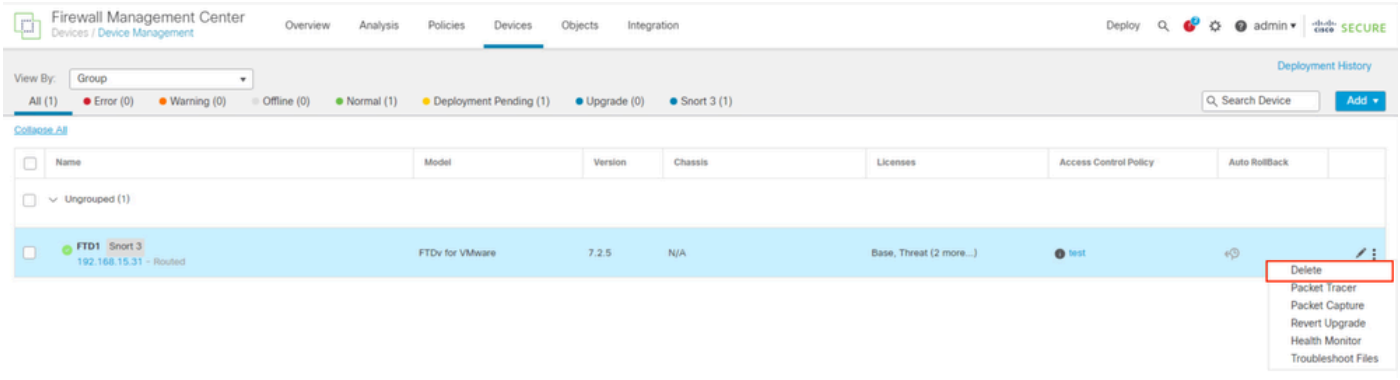

Access Control Policy
test
Access Control Policy
Contextual Cross-launch
Custom Table View
Custom Workflow
Dashboard
Health Policy
NAT Threat Defense
NAT
NAT Threat Defense
Platform Settings Threat Defense
test
Platform Settings Threat Defense
Report Template
Export



참고: .SFO 파일이 성공적으로 다운로드되었는지 확인하십시오. 내보내기를 클릭하면 자동으로 다운로드가 완료됩니다. 이 파일에는 액세스 제어 정책, 플랫폼 설정, NAT 정책 및 기타 정책이 포함되어 있습니다. 이러한 정책은 디바이스 컨피그레이션과 함께 내보내지지 않으며 대상 FMC에 수동으로 업로드해야 하므로 마이그레이션에 필요합니다.

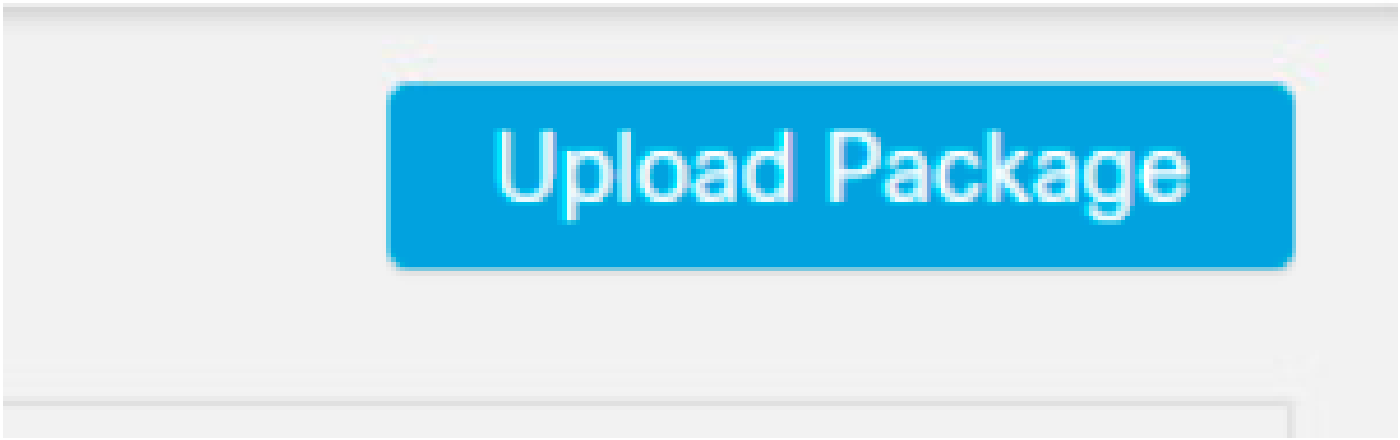
---

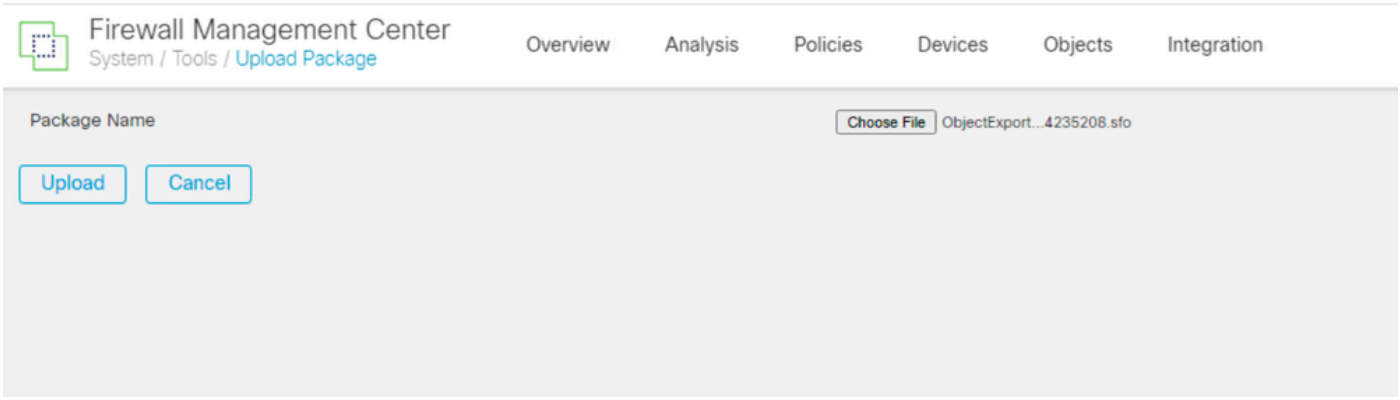
6. FMC에서 FTD 디바이스를 등록 취소하고 Devices(디바이스) > Device management(디바이스 관리)로 이동하여 오른쪽에 있는 세 개의 세로 점을 클릭하고 delete(삭제)를 선택합니다.



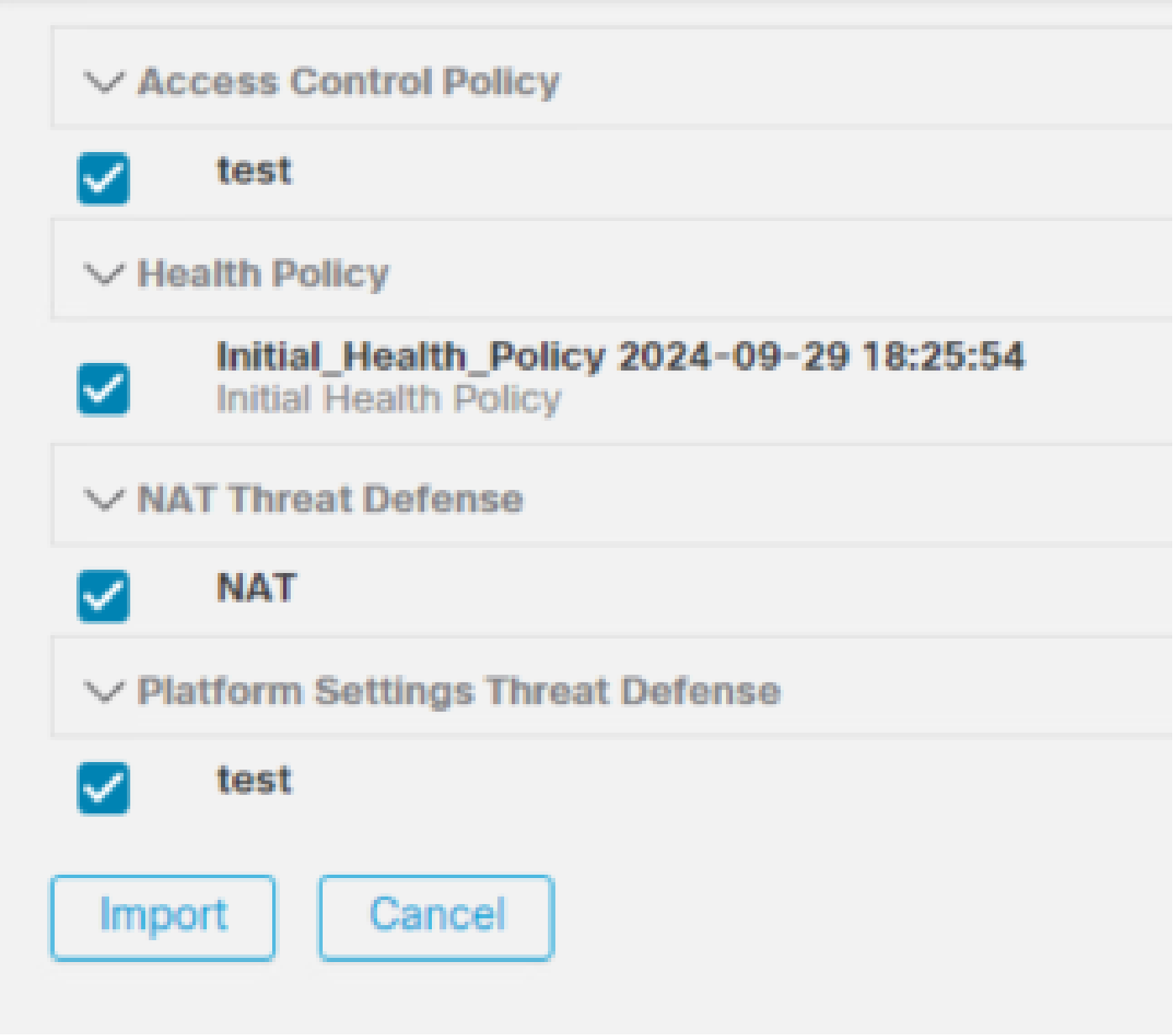
7. 대상 FMC를 준비합니다.

- 대상 FMC에 로그인합니다.
- 5단계에서 다운로드한 소스 FMC 정책을 가져와서 FMC가 새 디바이스를 승인할 준비가 되었는지 확인합니다. System > Tools > Import/Export로 이동하고 upload package를 클릭합니다. 가져올 파일을 업로드하고 업로드를 클릭합니다.

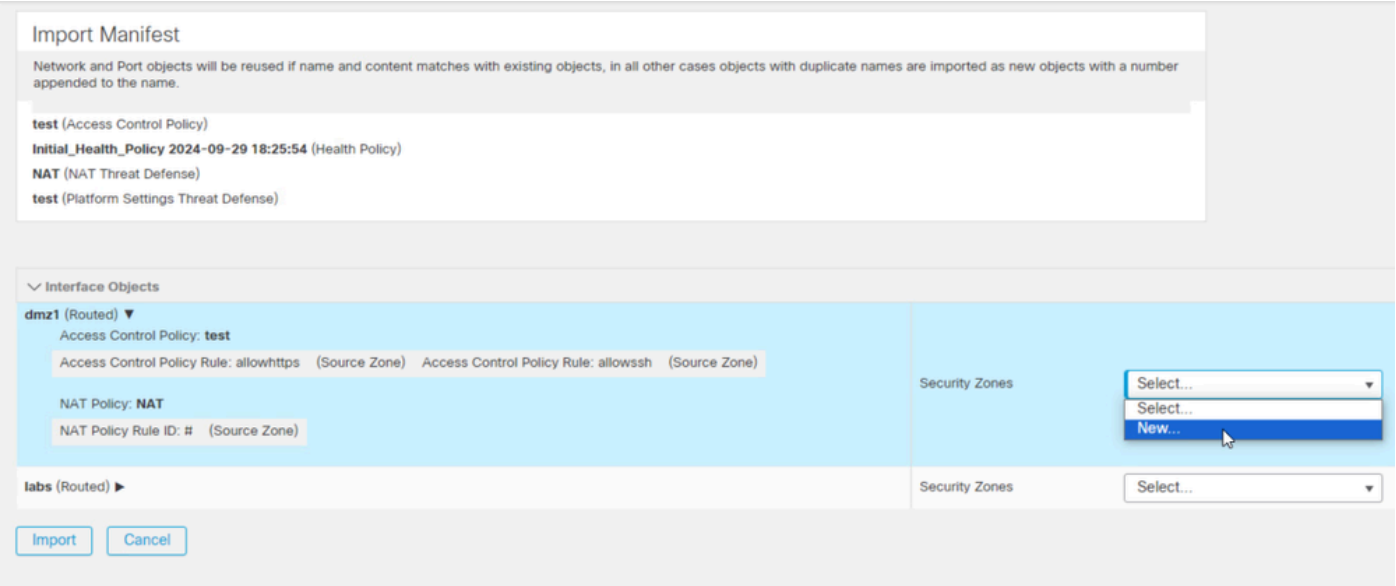




8. 대상 FMC에서 가져올 정책을 선택합니다.

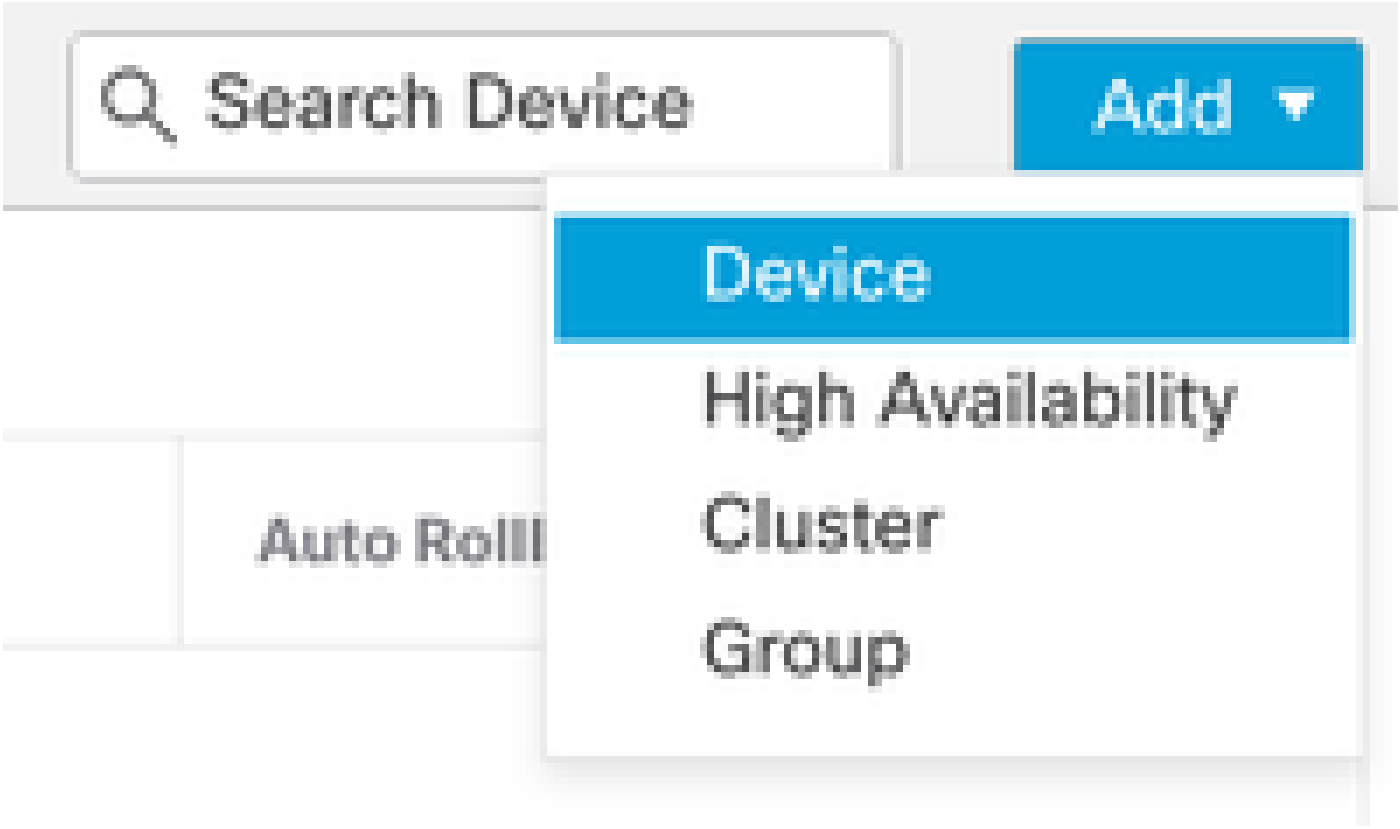


9. 가져오기 매니페스트에서 인터페이스 객체에 할당할 보안 영역을 선택하거나 새 영역을 만들고 가져오기를 클릭합니다.



10. 대상 FMC에 FTD를 등록합니다.

- 대상 FMC에서 Device(디바이스) > Management(관리) 탭으로 이동하고 Add(추가) > Device(디바이스)를 선택합니다.
- 프롬프트에 응답하여 등록 프로세스를 완료합니다.



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

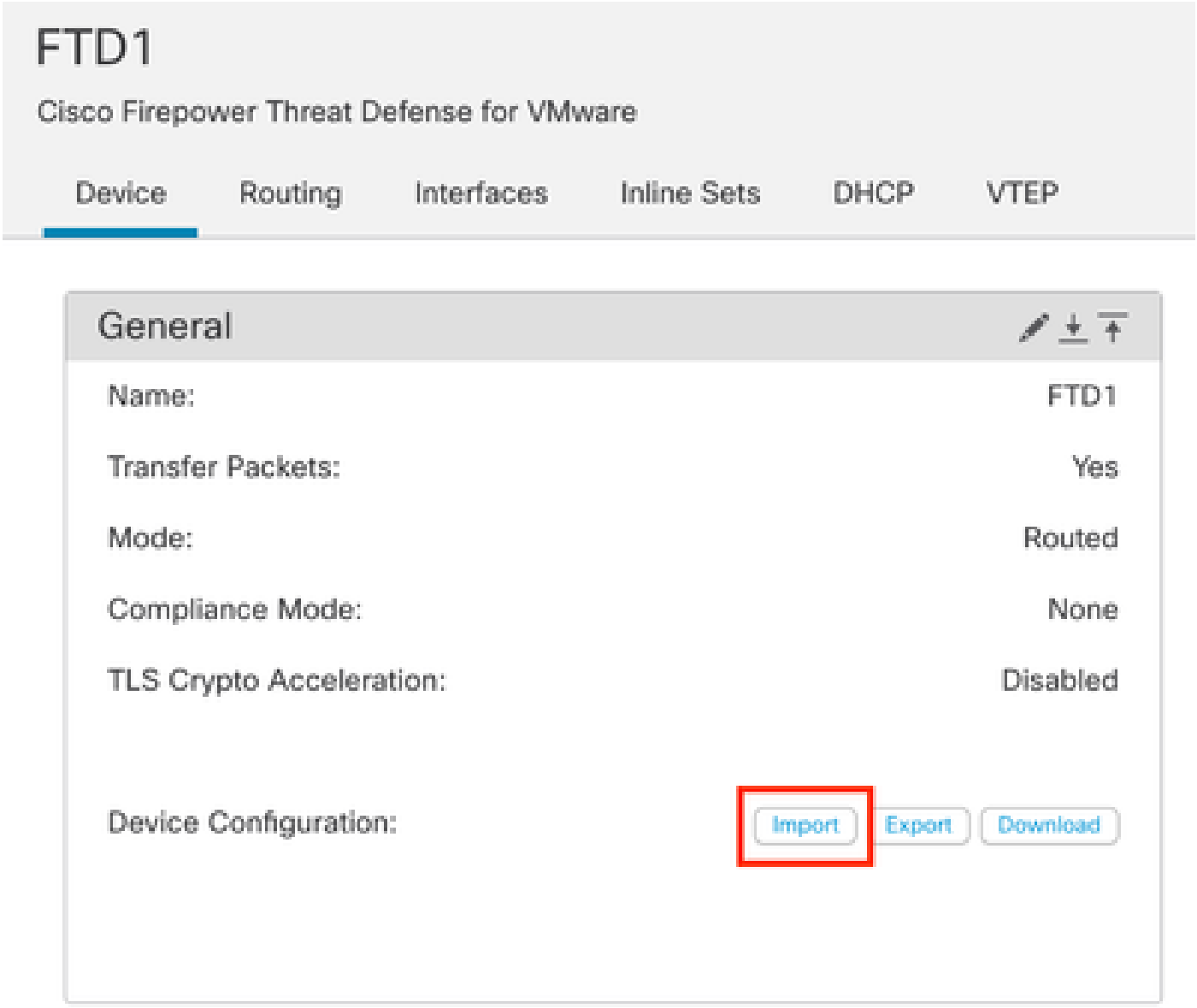
† Either host or NAT ID is required.

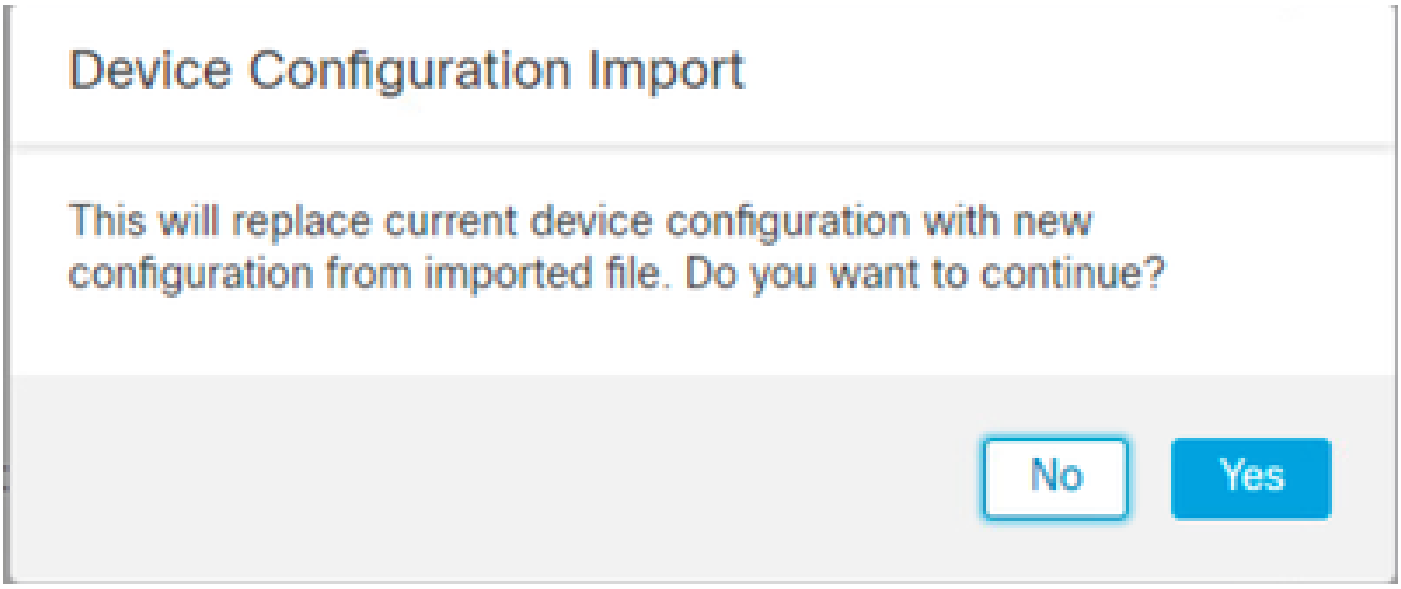
Cancel

Register

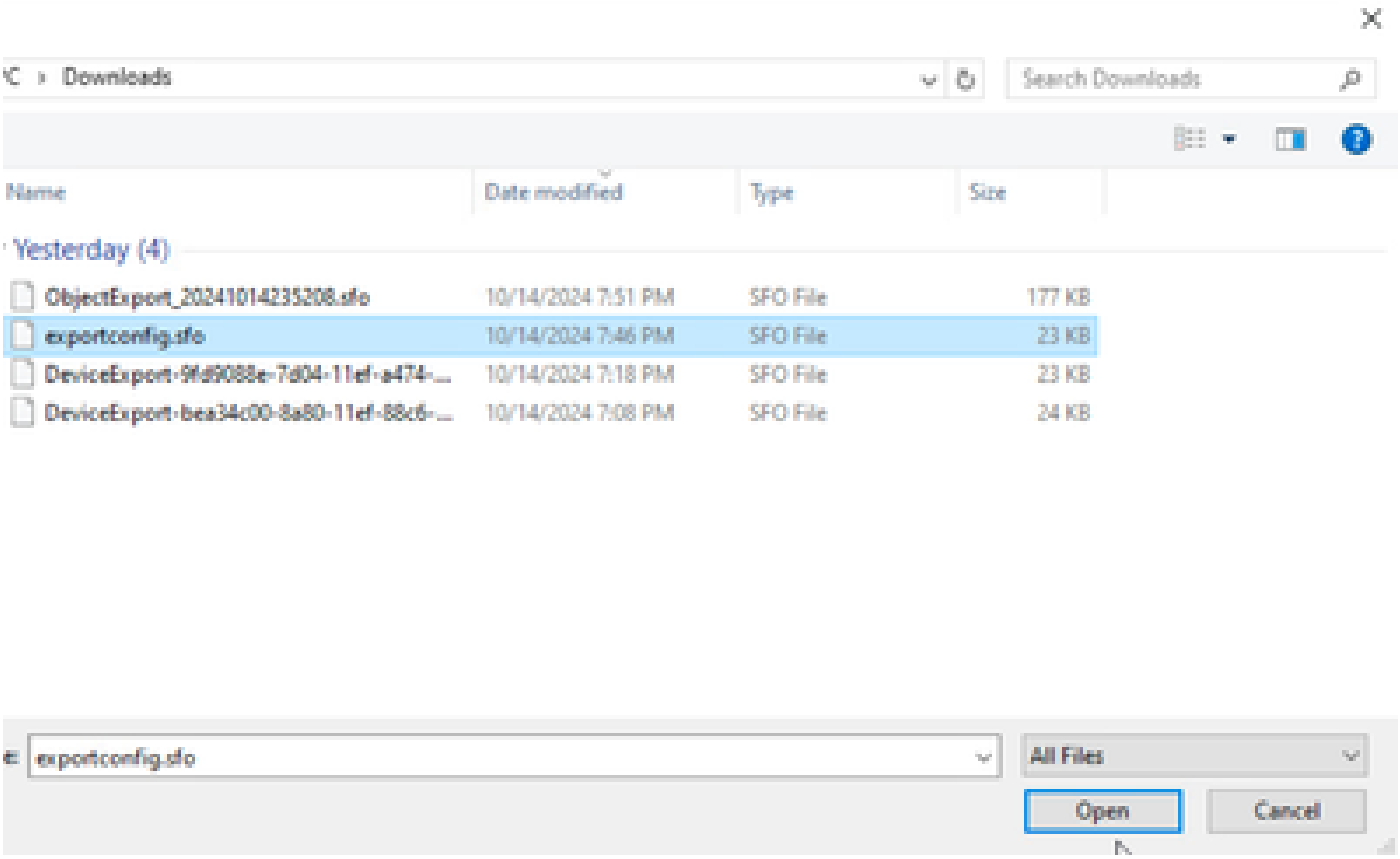
자세한 내용은 Firepower Management Center 컨피그레이션 가이드, Firepower Management Center에 디바이스 추가를 참조하십시오

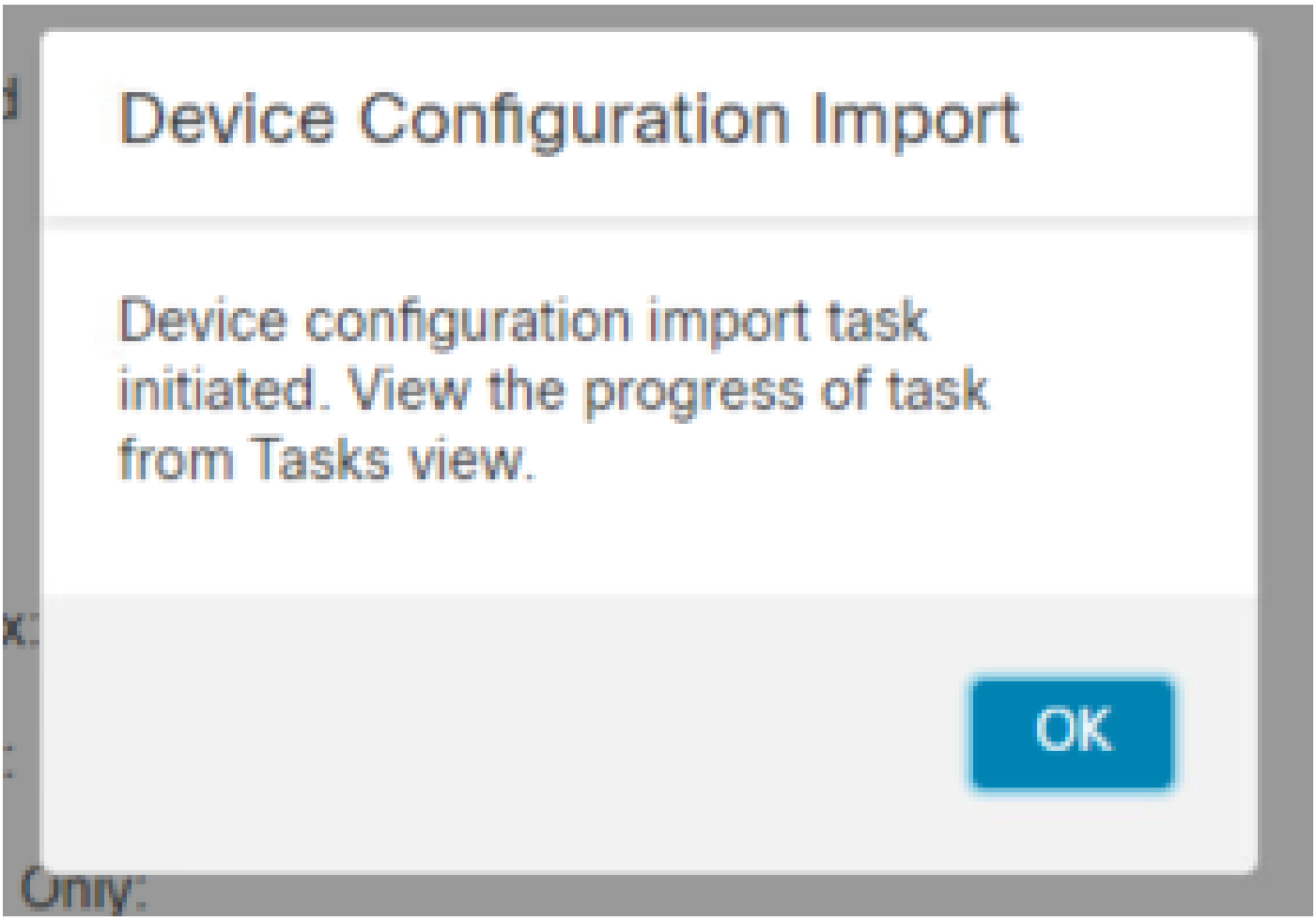
11. Device(디바이스) > Device Management(디바이스 관리)로 이동하고 FTD > Device(디바이스)를 선택한 후 import(가져오기)를 클릭합니다. 장치 컨피그레이션을 교체할지 확인하는 메시지가 표시되면 yes(예)를 클릭합니다.



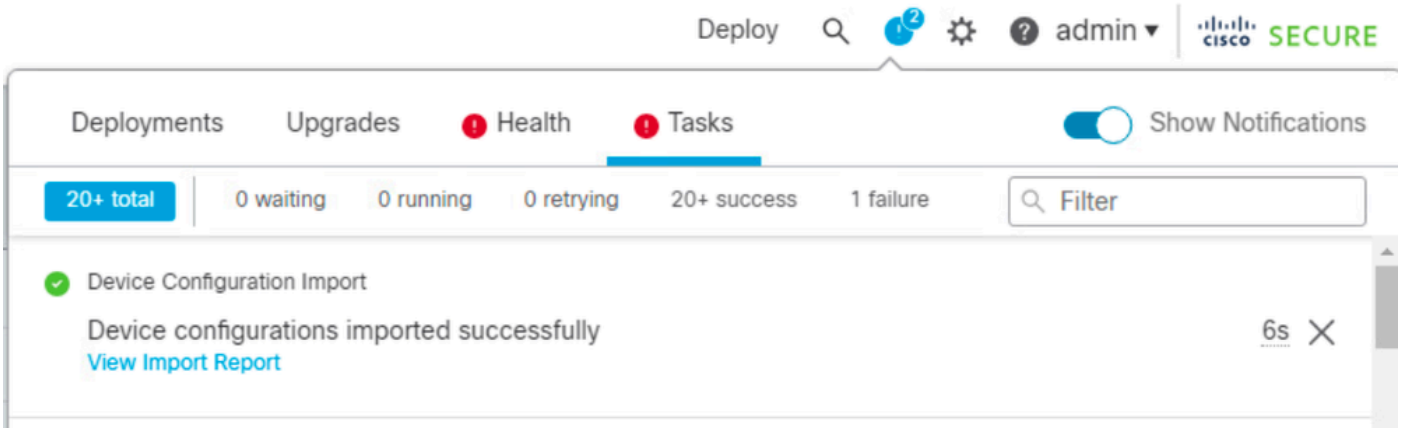


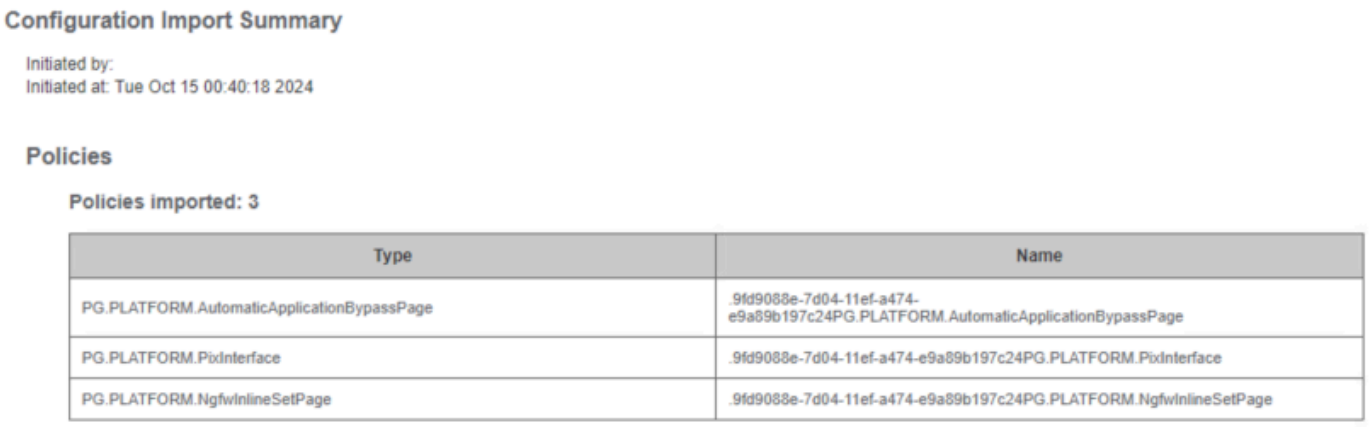
12. .SFO 확장자여야 하는 가져오기 구성 파일을 선택하고 업로드를 누르면 가져오기가 시작되었음을 나타내는 메시지가 나타납니다.





13. 마지막으로, 가져오기가 완료되면 경고가 표시되고 보고서가 자동으로 생성되므로 가져온 객체 및 정책을 검토할 수 있습니다.





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

다음을 확인합니다.

마이그레이션을 완료한 후 FTD 디바이스가 올바르게 등록되었고 대상 FMC에서 작동하는지 확인합니다.

- 대상 FMC에서 디바이스 상태를 확인합니다.
- 모든 정책과 컨피그레이션이 올바르게 적용되었는지 확인합니다.
- 테스트를 수행하여 디바이스가 작동하는지 확인합니다.

문제 해결

마이그레이션 프로세스 중에 문제가 발생하면 다음 트러블슈팅 단계를 고려하십시오.

- FTD 디바이스와 두 FMC 간의 네트워크 연결을 확인합니다.
- 두 FMC의 소프트웨어 버전이 동일한지 확인합니다.
- 두 FMC의 알림에서 오류 메시지 또는 경고를 확인합니다.

관련 정보

- Cisco Secure Firewall Management Center 관리 설명서
- firepower 디바이스 등록 구성, 확인 및 문제 해결

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.