Configuration.zip 파일을 사용하여 FMT를 통해 FDM을 FMC로 마이그레이션

목차

소개

이 문서에서는 FMT를 사용하여 FMC로 마이그레이션할 FDM(Secure Firewall Device Manager)의 configuration file.zip을 생성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD(방화벽 위협 방어)
- Cisco FMC(Firewall Management Center)
- FMT(Firewall Migration Tool)
- Postman API 플랫폼

사용되는 구성 요소

이 문서의 정보는 이러한 소프트웨어 버전을 기반으로 합니다.

FTD 7.4.2

FMC 7.4.2

FMT 7.7.0.1

Postman 11.50.0

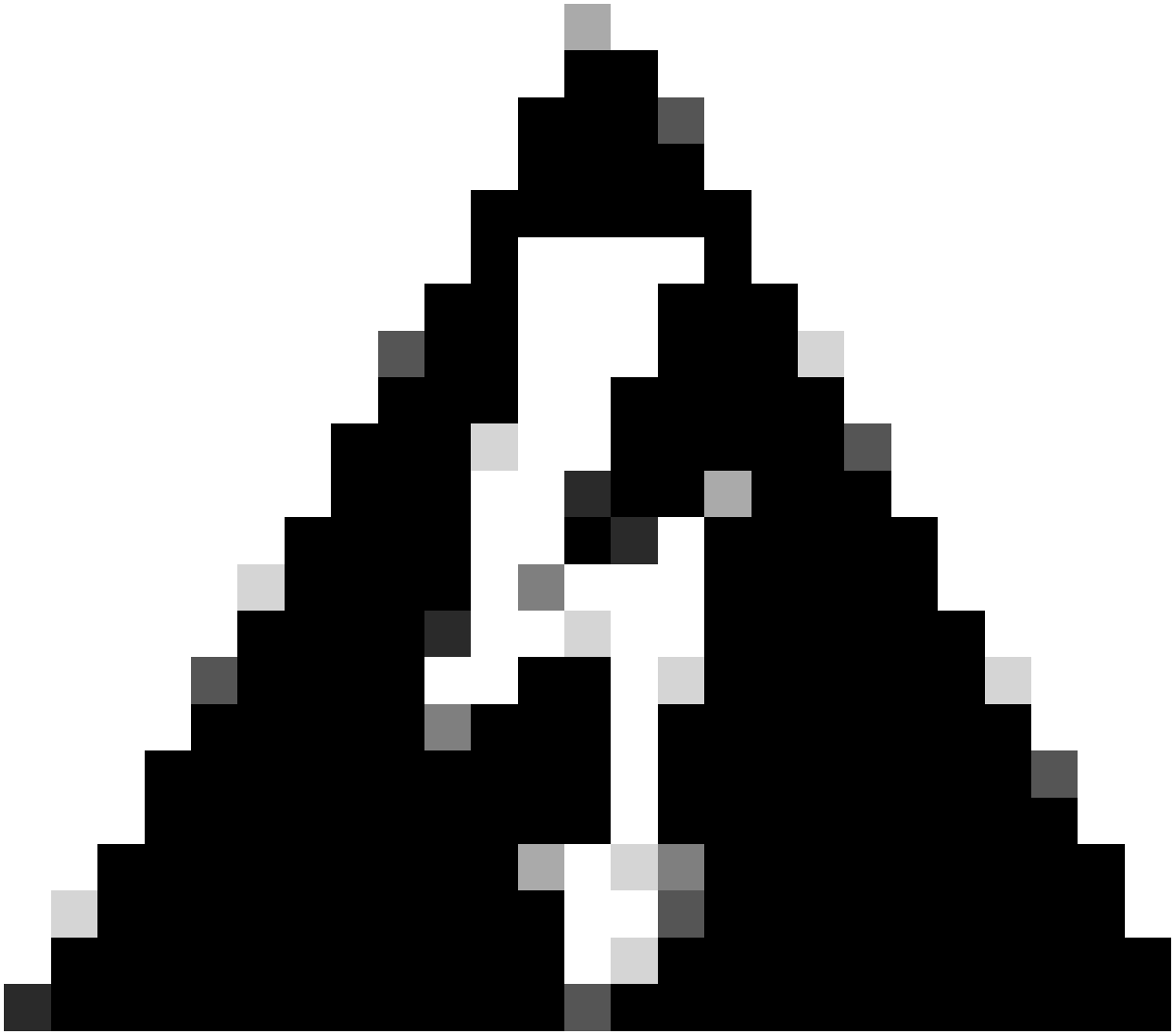
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

- 이제 FDM을 다양한 방법으로 FMC로 마이그레이션할 수 있습니다. 이 문서에서 살펴볼 시나리오는 API 요청을 사용하여 configuration .zip 파일을 생성한 다음 나중에 해당 파일을 FMT에 업로드하여 컨피그레이션을 FMC로 마이그레이션하는 것입니다.
- 이 문서에 표시된 단계는 Postman을 직접 사용하기 시작하므로 Postman을 이미 설치한 것이 좋습니다. 사용할 PC 또는 랩톱은 FDM 및 FMC에 액세스할 수 있어야 하며 FMT를 설치하고 실행해야 합니다.

고려 사항

- 이 문서는 FMT 사용보다 구성 .zip 파일 생성에 중점을 두고 있습니다.
- 구성 .zip 파일을 사용하는 FDM 마이그레이션은 비라이브 마이그레이션용이며 즉시 대상 FTD가 필요하지 않습니다.

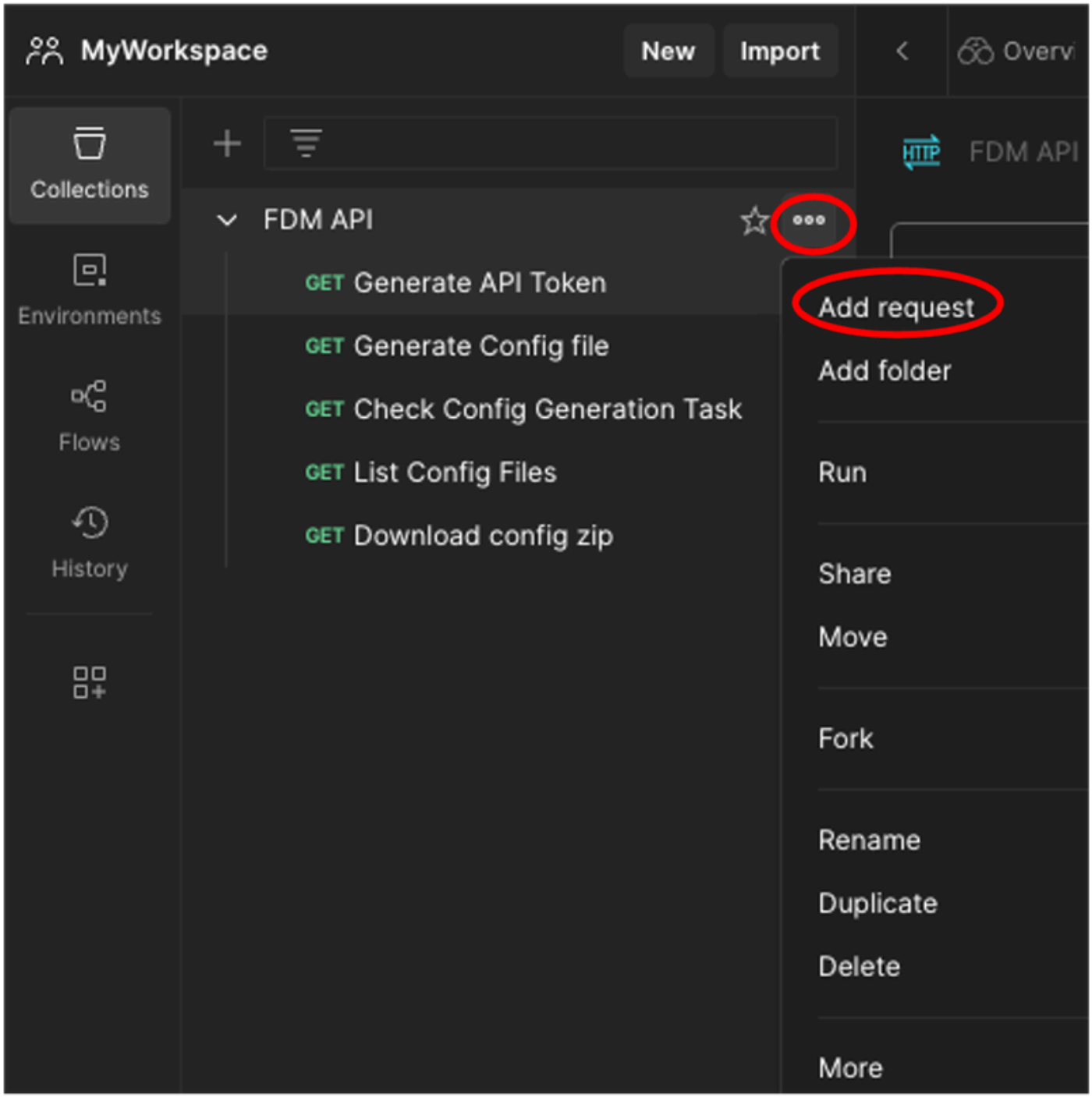


경고: 이 모드를 선택하면 ACP(Access Control Policy), NAT(Network Address Translation Policy) 및 객체만 마이그레이션할 수 있습니다. ACP 규칙 또는 NAT에서 사용해야 하는 객체와 관련해서는 마이그레이션해야 합니다. 그렇지 않으면 이러한 객체는 무시됩니다.

설정

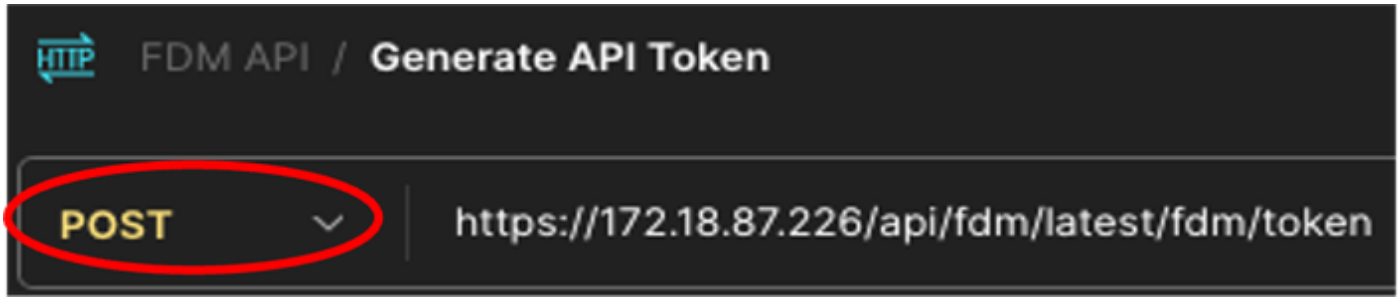
API 요청 - Postman

1. Postman에서 새 컬렉션을 생성합니다(이 시나리오에서는 FDM API가 사용됨).
2. 3개의 점을 클릭하고 Add request(요청 추가)를 클릭합니다.



Postman - 컬렉션 만들기 및 추가 요청

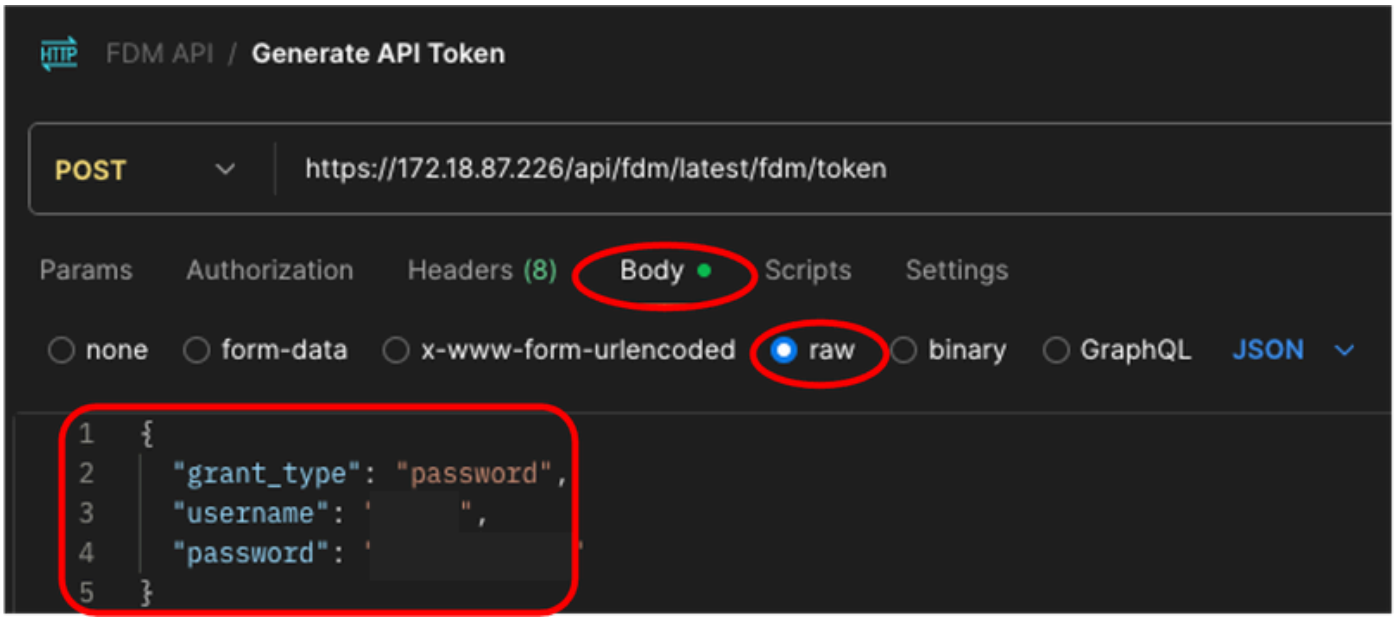
3. 이 새 요청 호출: API 토큰 생성 GET 요청으로 생성되지만 이 요청을 실행할 때 드롭다운 메뉴에서 POST를 선택해야 합니다. POST 옆의 텍스트 상자에서 다음 줄 https://<FDM IP ADD>/api/fdm/latest/fdm/token을 소개합니다.



Postman - 토큰 요청

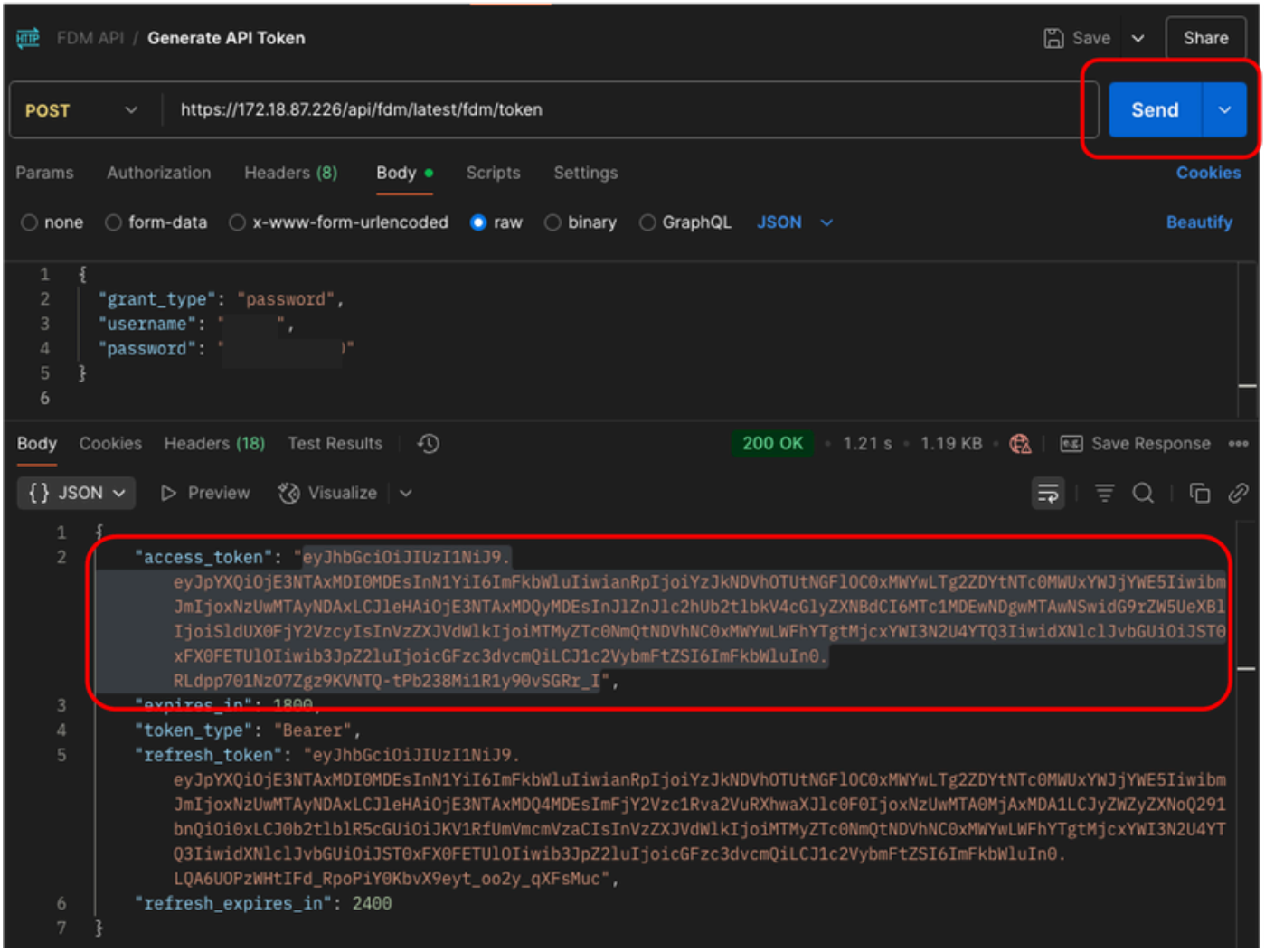
4. [본문] 탭에서 원시 옵션을 선택하고 이 형식을 사용하여 FTD(FDM) 장치에 액세스하기 위한 인증서를 제공합니다.

```
{

  "grant_type": "비밀번호",

  "사용자 이름": "사용자 이름",

  "암호": "암호"

}
```



Postman - 토큰 요청 본문

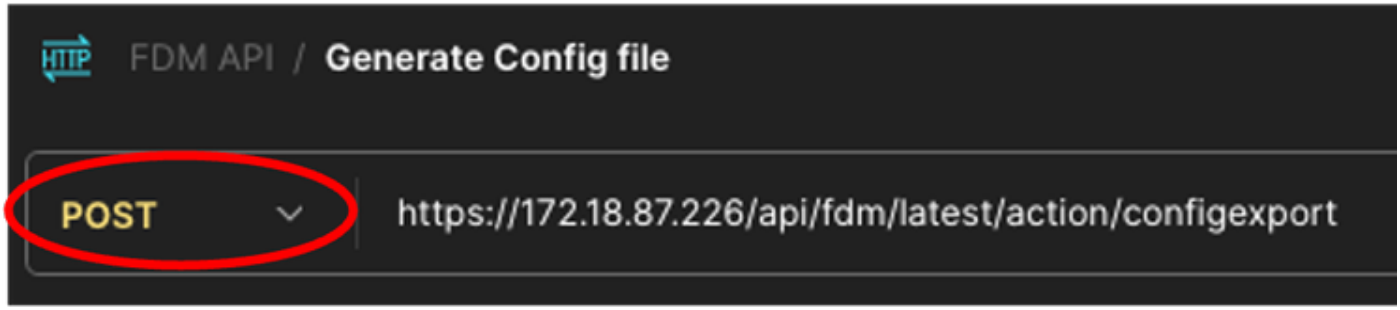
5. 마지막으로, Send(보내기)를 클릭하여 액세스 토큰을 가져옵니다. 모든 것이 정상인 경우 200 OK 응답을 받습니다. 전체 토큰(큰따옴표 안)은 이후 단계에서 사용될 것이므로 복사본을 만듭니다.



Postman - 토큰이 생성됨

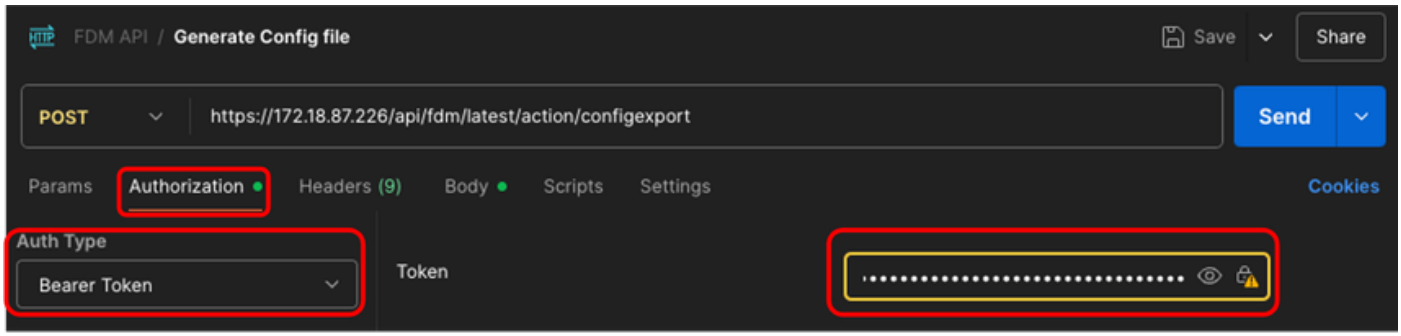
6. 2단계를 반복하여 새 요청을 생성하면 POST가 다시 사용됩니다.

7. 이 신규 요청을 호출합니다. 구성 파일을 생성합니다. GET 요청으로 생성되지만 이 요청을 실행할 때 드롭다운 메뉴에서 POST를 선택해야 합니다. POST 옆의 텍스트 상자에서 다음 줄 https://<FDM IP ADD>/api/fdm/latest/action/configexport를 소개합니다.



Postman - 구성 파일 요청 생성

8. Authorization 탭의 드롭다운 메뉴에서 Bearer Token as Auth Type을 선택하고 Token 옆의 텍스트 상자에서 5단계에서 복사한 토큰을 붙여넣습니다.



Postman - Generate Config File Request(컨피그레이션 파일 요청 생성) - Authorization(권한 부여)

9. 본문 탭에서 원시 옵션을 선택하고 이 정보를 소개합니다.

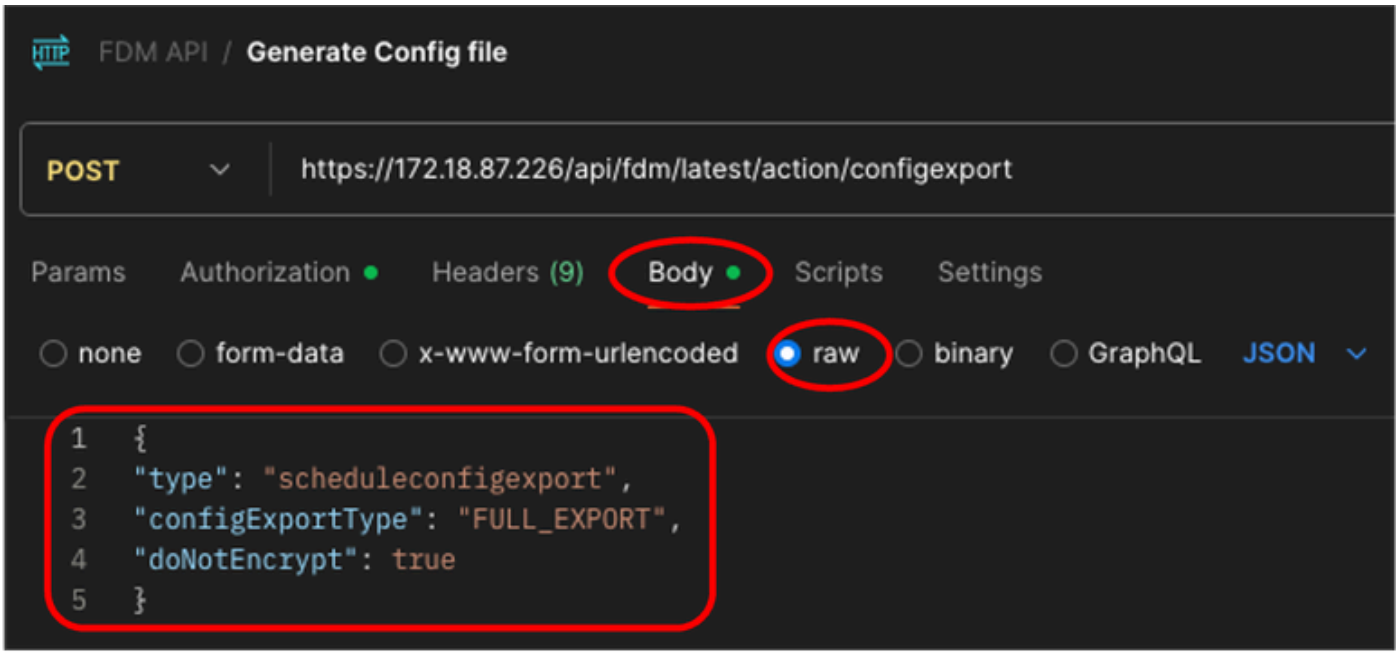
{

"유형": "일정구성 내보내기",

"configExportType": "FULL_EXPORT",

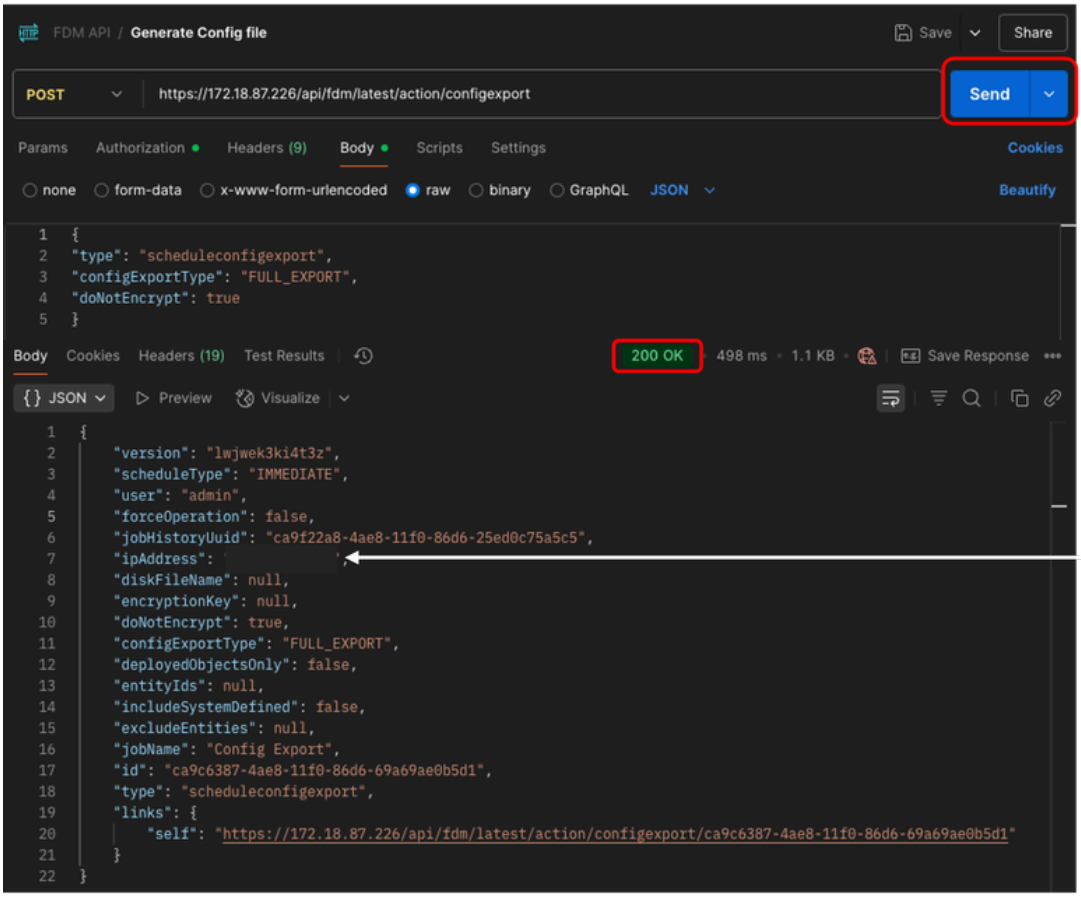
"암호화하지 않음": 참

}



Postman - 구성 파일 요청 생성 - 본문

10. 마지막으로 전송을 클릭합니다. 모든 것이 정상인 경우 200 OK 응답을 받습니다.

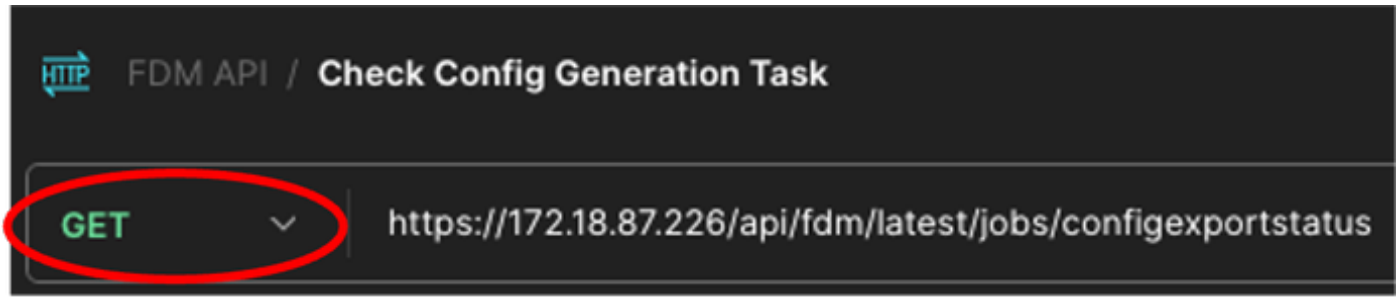


This IP address is the one that is connecting to the FTD through the requests.

Postman - 구성 파일 요청 생성 - 출력

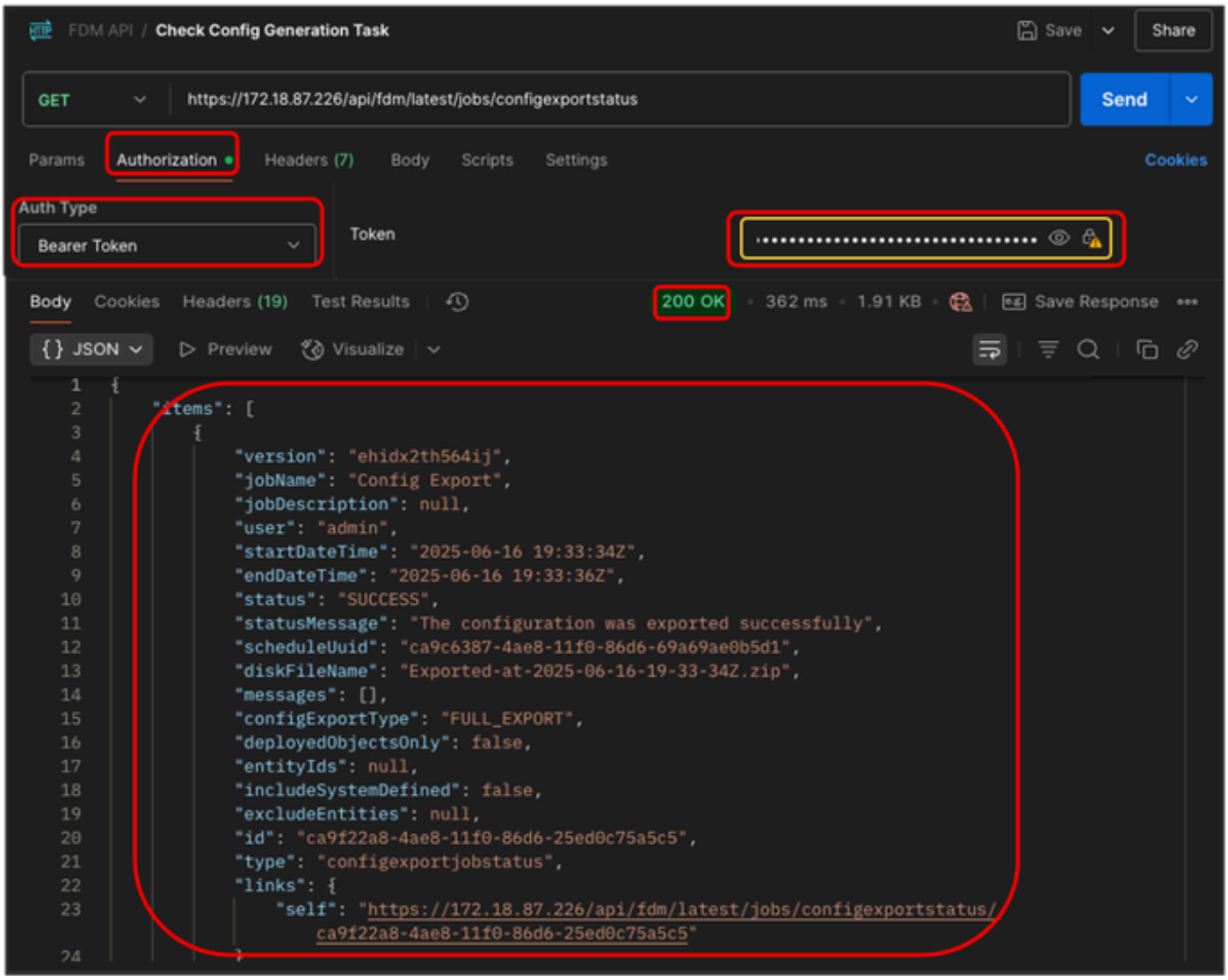
11. 2단계를 반복하여 새 요청을 생성합니다. GET이 이번에 사용됩니다.

12. 이 신규 요청을 호출합니다. 컨피그레이션 생성 작업을 확인합니다. GET 요청으로 생성됩니다. 또한 이 작업을 실행하는 동안 드롭다운 메뉴에서 GET을 선택해야 합니다. GET 옆의 텍스트 상자에 https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus 다음 줄을 도입합니다.



Postman - 컨피그레이션 내보내기 상태 요청 확인

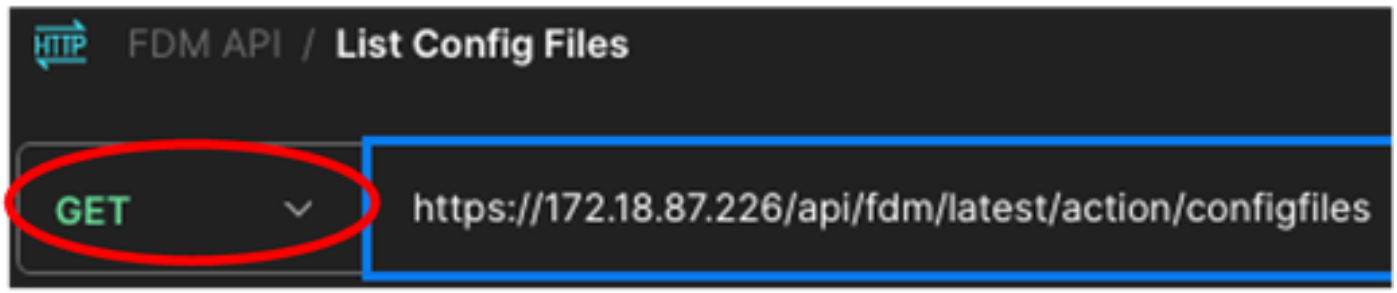
13. Authorization 탭의 드롭다운 메뉴에서 Bearer Token as Auth Type을 선택하고 Token 옆의 텍스트 상자에서 5단계에서 복사한 토큰을 붙여넣습니다. 마지막으로 Send를 클릭합니다. 모든 것이 정상인 경우 200 OK 응답을 받으며 JSON 필드에서 작업 상태 및 기타 세부사항을 볼 수 있습니다.



Postman - 컨피그레이션 내보내기 상태 요청 - 권한 부여 및 출력

14. 2단계를 반복하여 새 요청을 생성하면 이번에 GET이 사용됩니다.

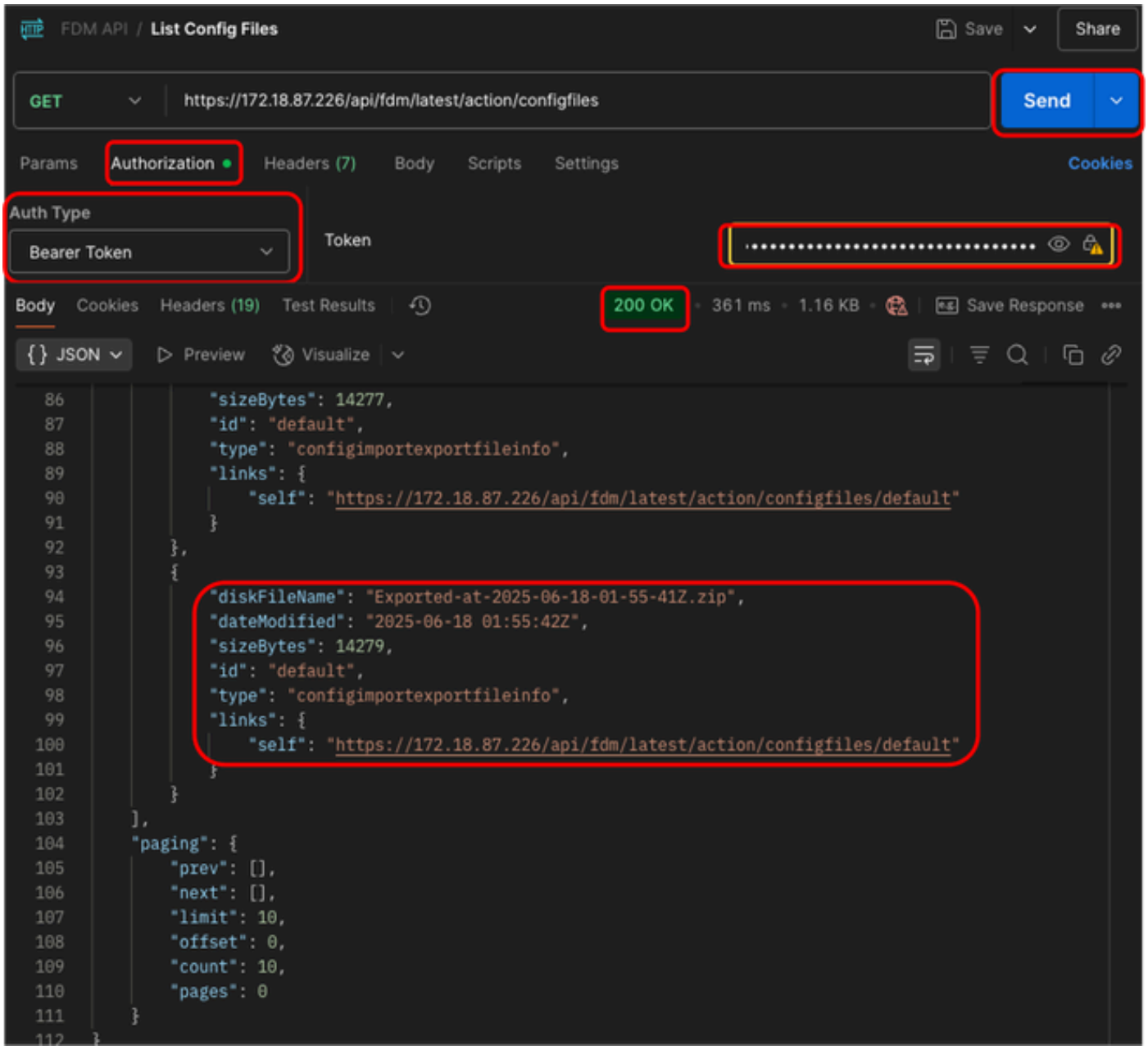
15. 이 신규 요청을 호출합니다. 컨피그레이션 파일을 나열합니다. GET 요청으로 생성되며, 이 요청을 실행할 때 드롭다운 메뉴에서 GET을 선택해야 합니다. GET 옆의 텍스트 상자에서 다음 줄 https://<FDM IP ADD>/api/fdm/latest/action/configfiles를 소개합니다.



Postman - 내보낸 컨피그레이션 파일 요청 나열

16. Authorization(권한 부여) 탭의 드롭다운 메뉴에서 Bearer Token as Auth Type(베어러 토큰을 인증 유형으로)을 선택하고 Token(토큰) 옆의 텍스트 상자에서 5단계에서 복사한 토큰을 붙여넣습니다. 마지막으로 Send(보내기)를 클릭합니다. 모든 것이 정상인 경우 200 OK 응답을 받으며

JSON 필드에 내보낸 파일 목록이 표시됩니다. 가장 최근의 것은 맨 아래에 나와 있습니다. 마지막 단계에서 사용되므로 최신 파일 이름(파일 이름의 최신 날짜)을 복사합니다.



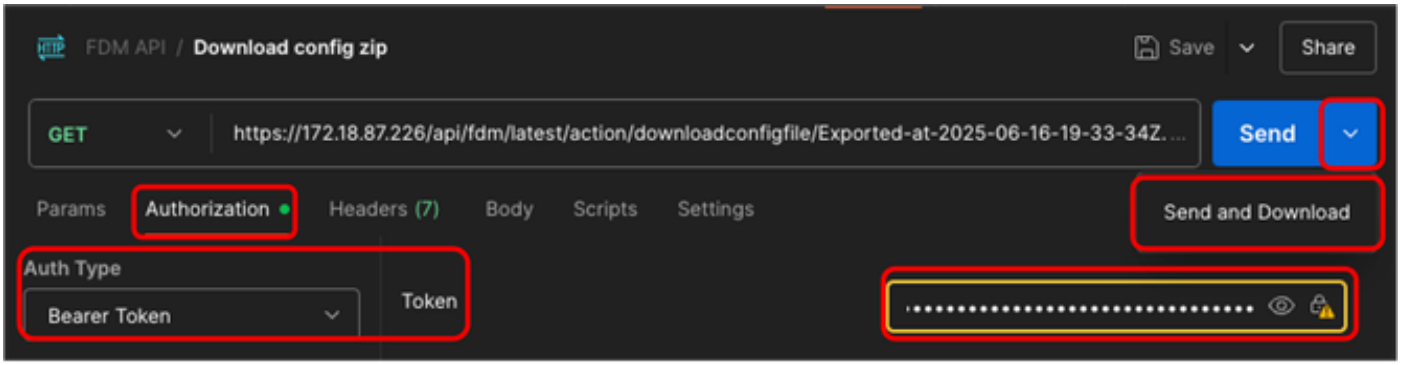
Postman - 내보낸 컨피그레이션 파일 나열 요청 - 권한 부여 및 출력

17. 2단계를 반복하여 새 요청을 생성하면 이번에 GET이 사용됩니다.

18. 이 신규 요청을 호출합니다. 구성 zip을 다운로드합니다. GET 요청으로 생성되며, 이 요청을 실행할 때 드롭다운 메뉴에서 GET을 선택해야 합니다. GET 옆의 텍스트 상자에 16단계에서 복사한 파일 이름 끝에 다음 줄을 붙여 넣습니다. https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >

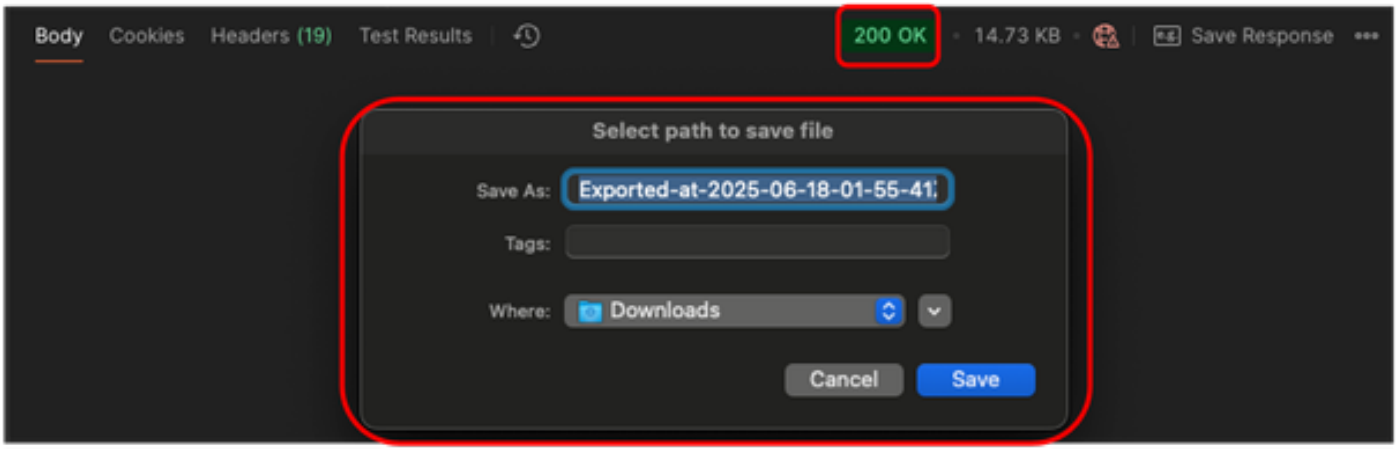
Postman - Config.zip 파일 요청 다운로드

19. Authorization(권한 부여) 탭의 드롭다운 메뉴에서 Bearer Token as Auth Type(베어러 토큰을 인증 유형으로)을 선택하고 Token(토큰) 옆의 텍스트 상자에서 단계 5에서 복사한 토큰을 붙여넣습니다. 마지막으로 Send(보내기) 옆의 아래쪽 화살표를 클릭하고 Send and Download(보내기 및 다운로드)를 선택합니다.



Postman - Config.zip 파일 다운로드 요청 - 권한 부여

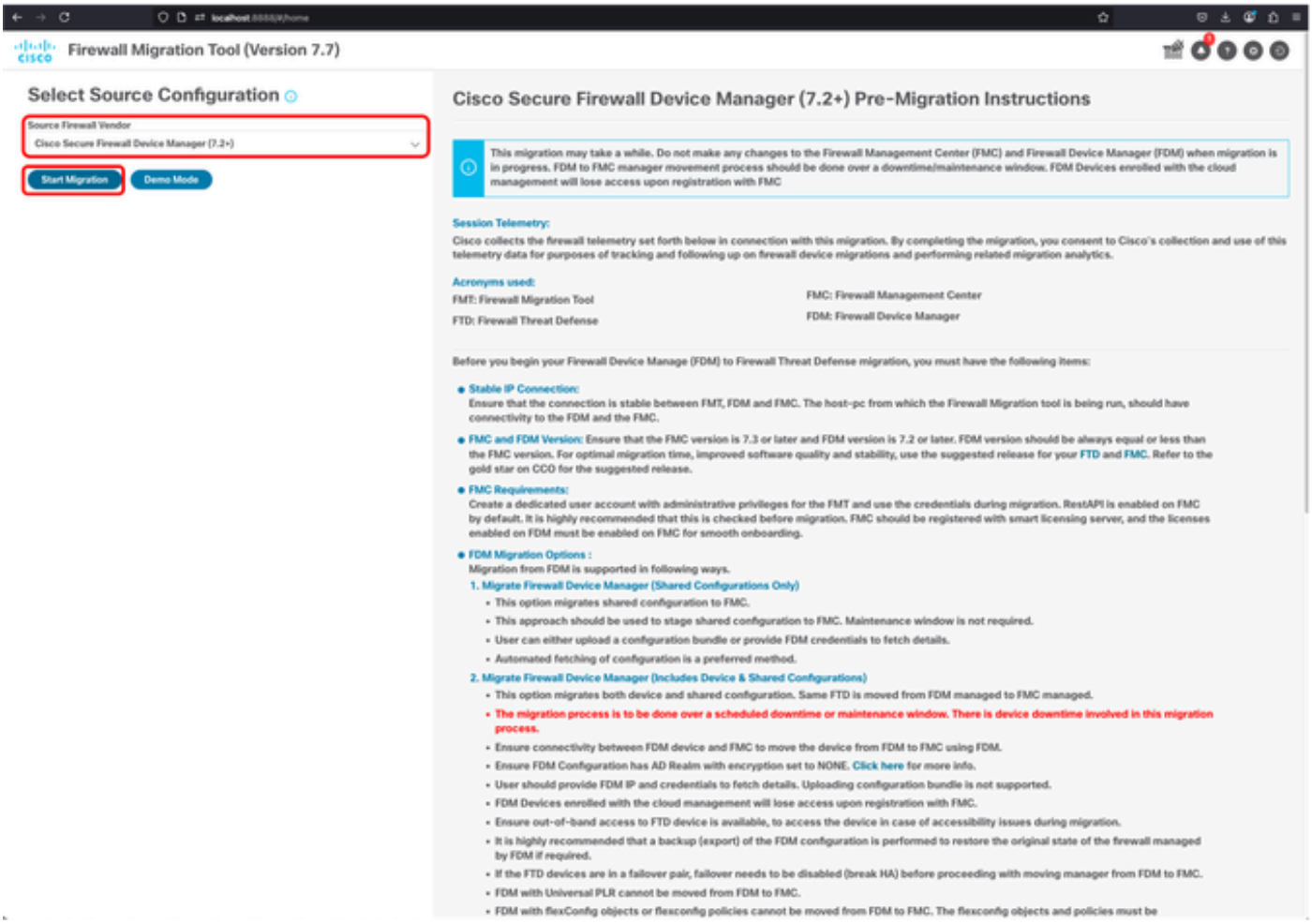
20. 모든 것이 정상인 경우 200 OK 응답을 받으며 configuration.zip 파일이 저장될 대상 폴더를 묻는 팝업 창이 표시됩니다. 이제 이 .zip 파일을 Firewall Migration Tool에 업로드할 수 있습니다.



Postman - Config.zip 파일 다운로드 요청 - 저장

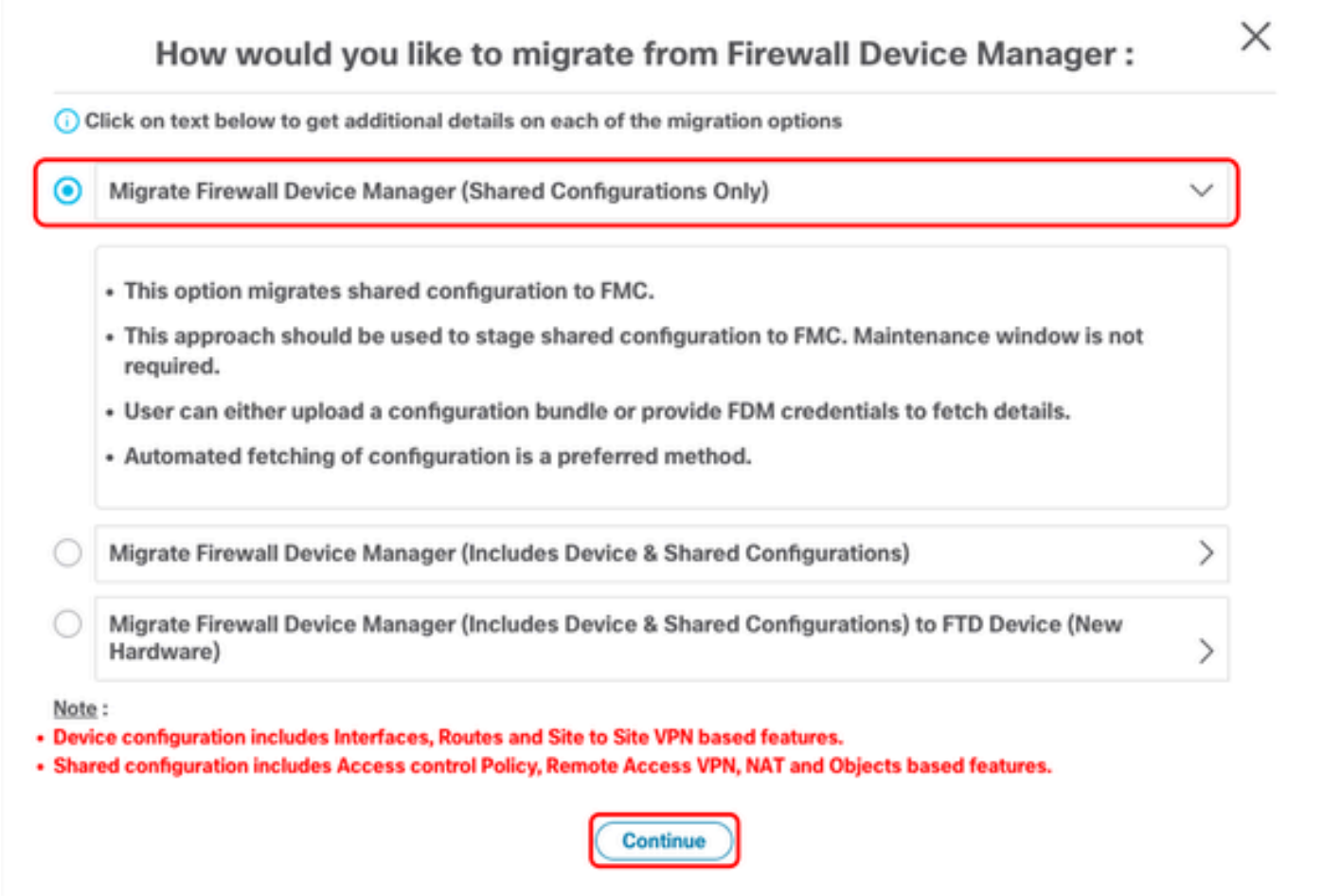
방화벽 마이그레이션 툴

21. Firewall Migration Tool을 열고 Select Source Configuration(소스 컨피그레이션 선택) 드롭다운 메뉴에서 Cisco Secure Firewall Device Manager(7.2+)를 선택하고 Start Migration(마이그레이션 시작)을 클릭합니다.



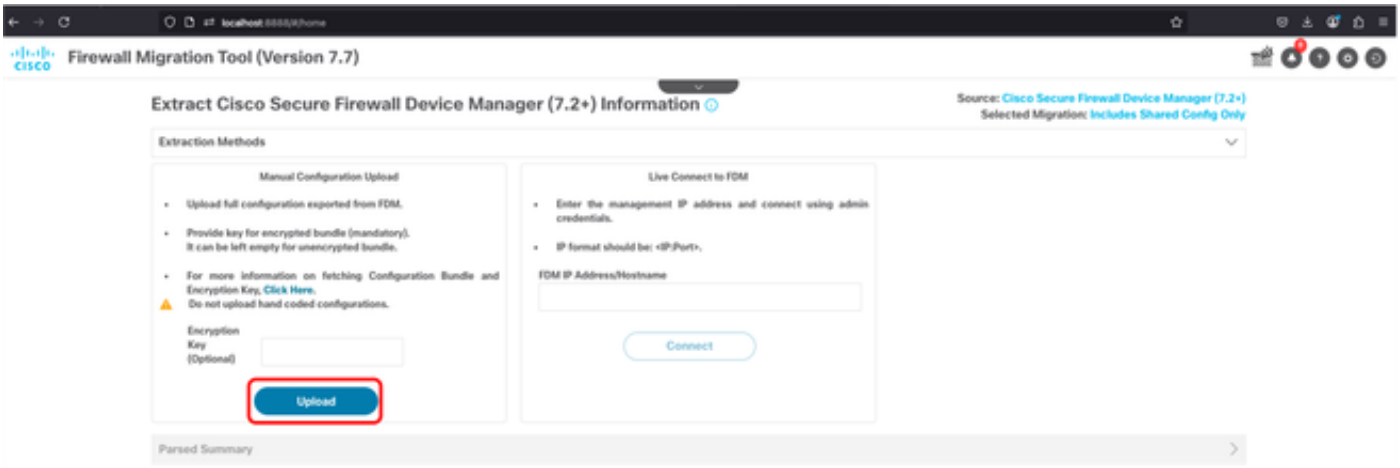
FMT - FDM 선택

22. 첫 번째 라디오 버튼, Migrate Firewall Device Manager (Shared Configurations Only)(방화벽 디바이스 관리자 마이그레이션(공유 컨피그레이션만 해당)를 선택하고 Continue(계속)를 클릭합니다.



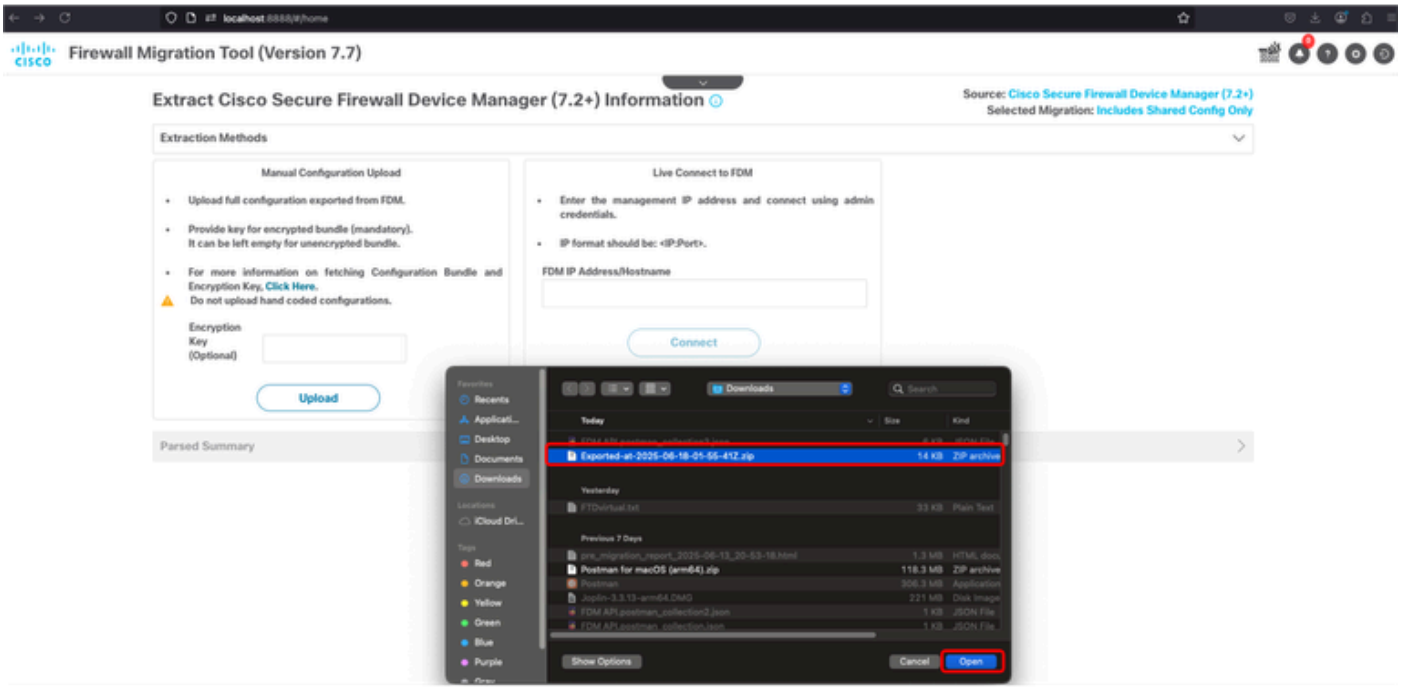
FMT - FDM 마이그레이션 공유 구성만

23. 왼쪽 패널(수동 구성 업로드)에서 업로드를 클릭합니다.



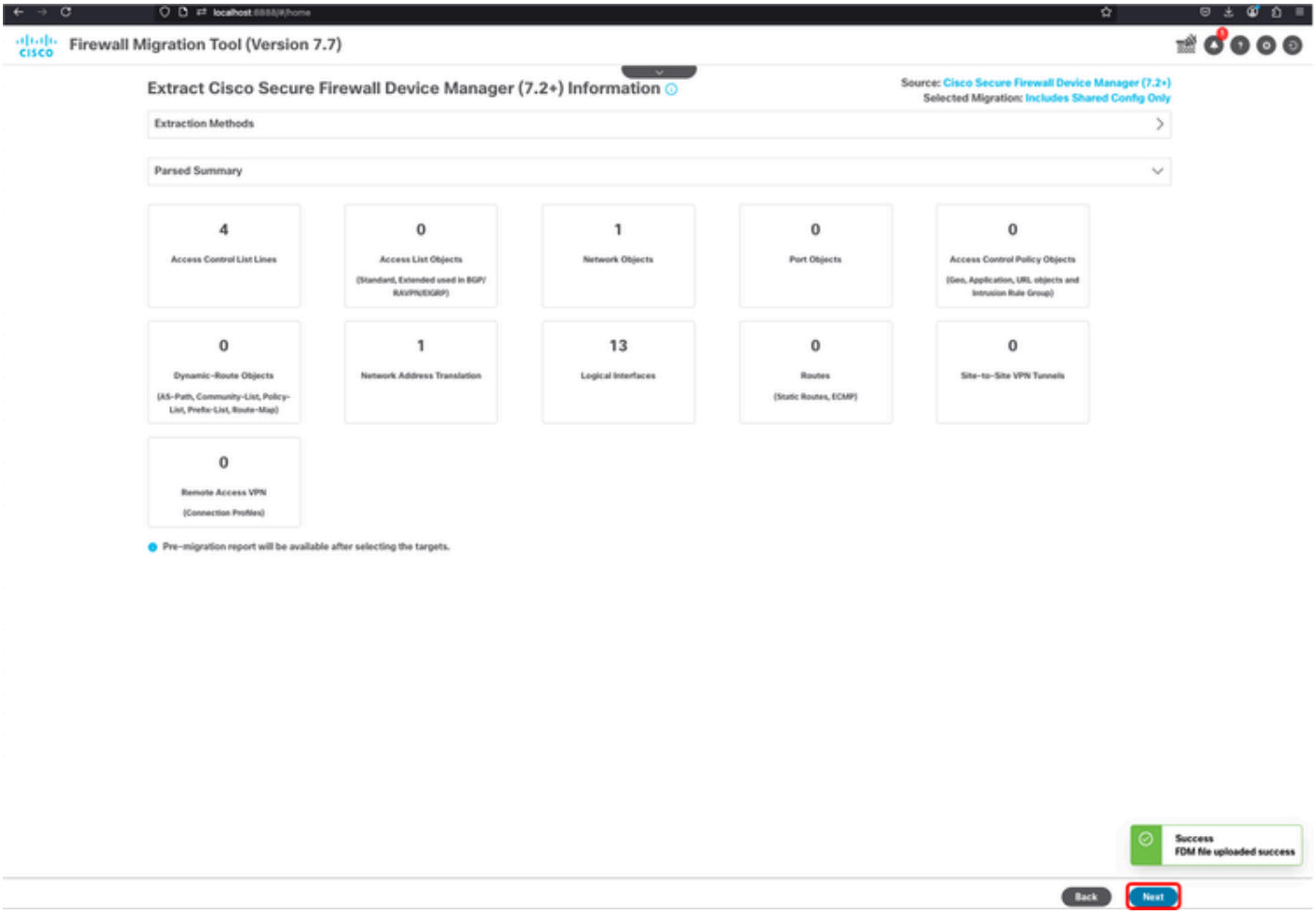
FMT - Config.zip 파일 업로드

24. 이전에 저장한 폴더에서 내보낸 zip 구성 파일을 선택하고 열기를 누릅니다.



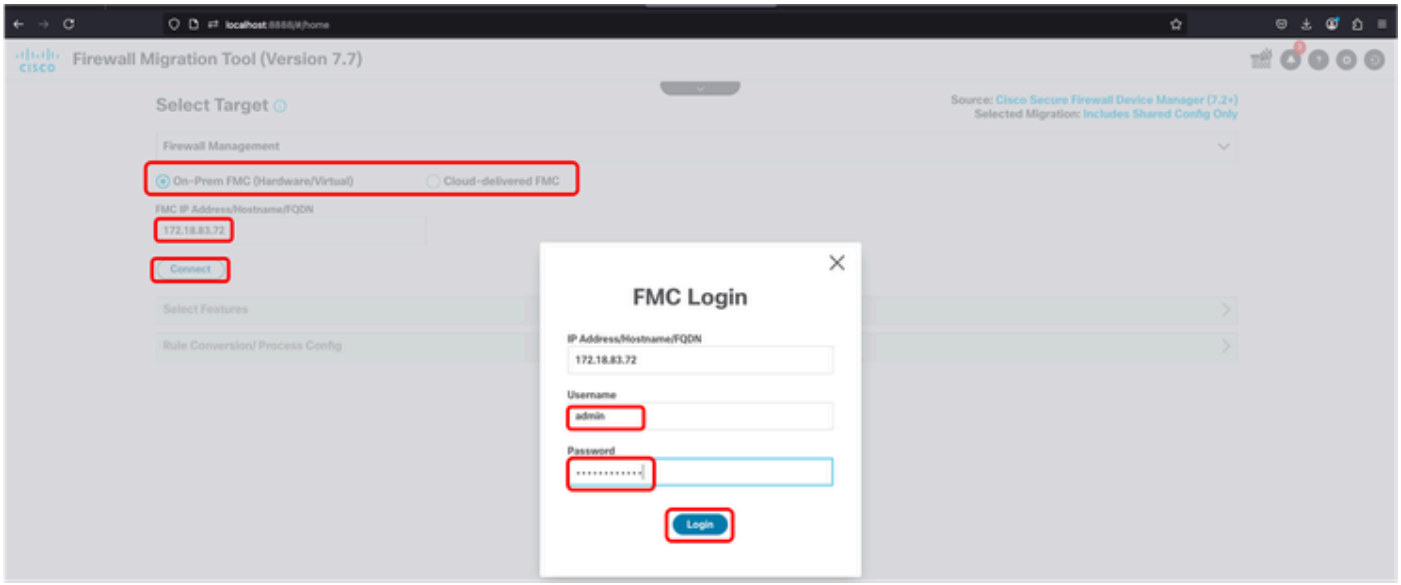
FMT - Config.zip 파일 선택

25. 모든 작업이 예상대로 진행되면 구문 분석된 요약이 표시됩니다. 또한 오른쪽 아래 모서리에는 FDM 파일이 성공적으로 업로드되었음을 알리는 팝업이 표시됩니다. Next(다음)를 클릭합니다.



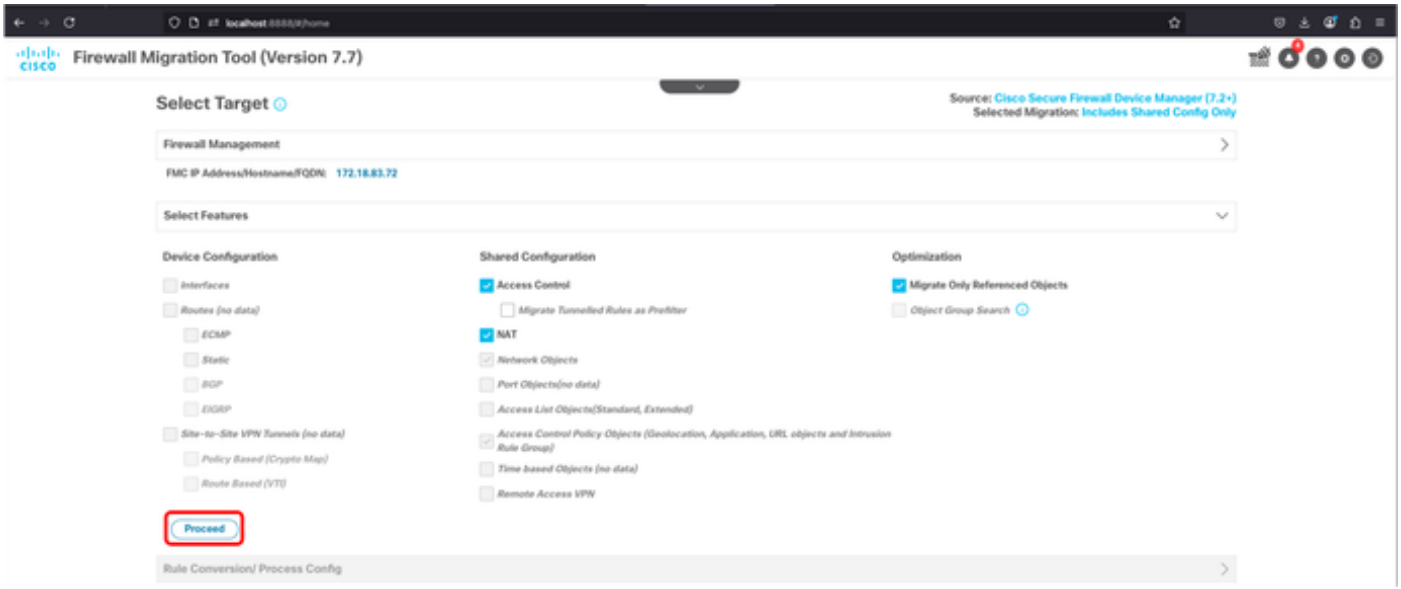
FMT - 구문 분석 요약

26. 사용자 환경에 더 적합한 옵션을 선택합니다(온프레미스 FMC 또는 Cd-FMC). 이 시나리오에서는 온프레미스 FMC가 사용됩니다. FMC IP 주소를 입력하고 Connect(연결)를 클릭합니다. 새 팝업이 나타나고 FMC 자격 증명을 요청합니다. 이 정보를 입력한 후 Login(로그인)을 클릭합니다.



FMT - FMC 대상 로그인

27. 다음 화면에는 대상 FMC와 마이그레이션할 기능이 표시됩니다. Proceed(진행)를 클릭합니다.

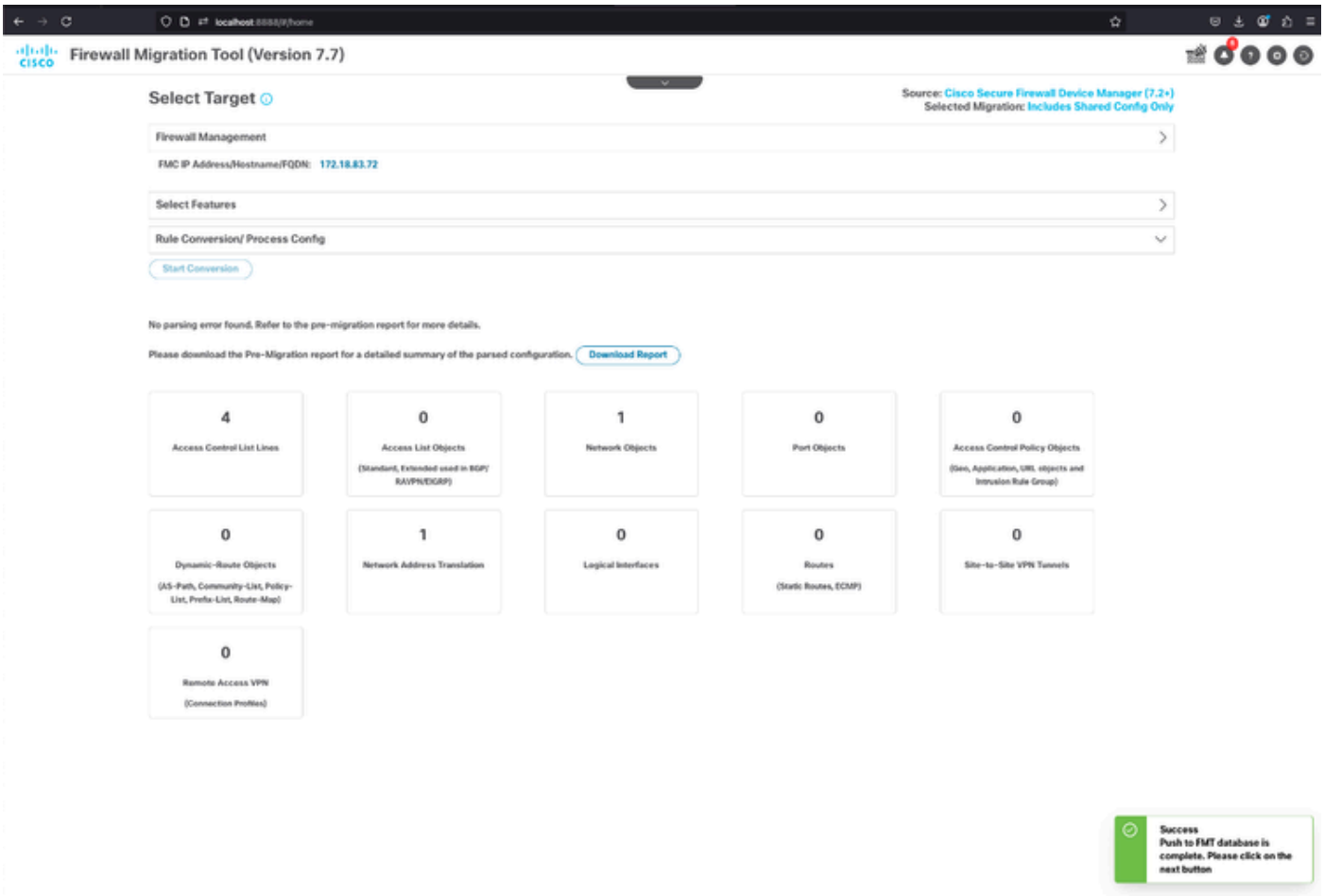


FMT - FMC 대상 - 기능 선택

28. FMC 대상이 확인되면 변환 시작 버튼을 누릅니다.

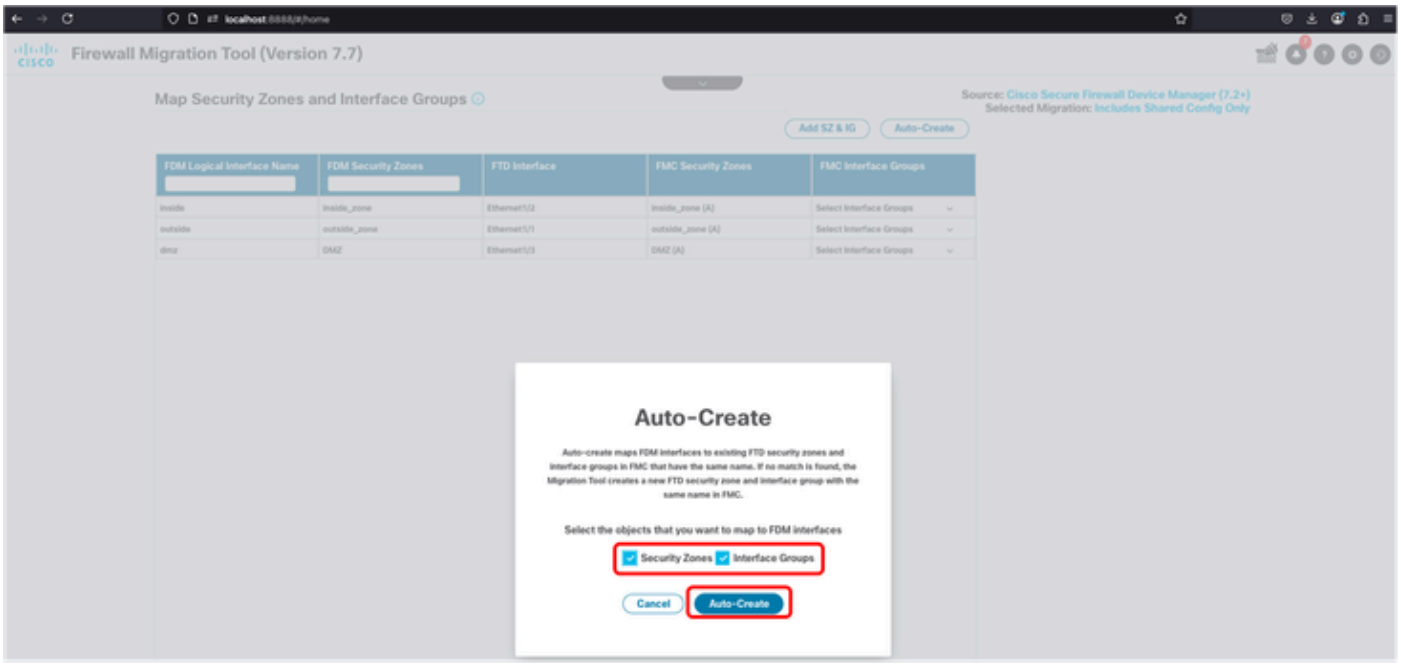
FMT - 컨피그레이션 변환 시작

29. 모든 작업이 예상대로 진행되면 오른쪽 아래 모서리에 팝업이 표시되어 FMT 데이터베이스 밀어넣기가 완료되었음을 알립니다. Next(다음)를 클릭합니다.



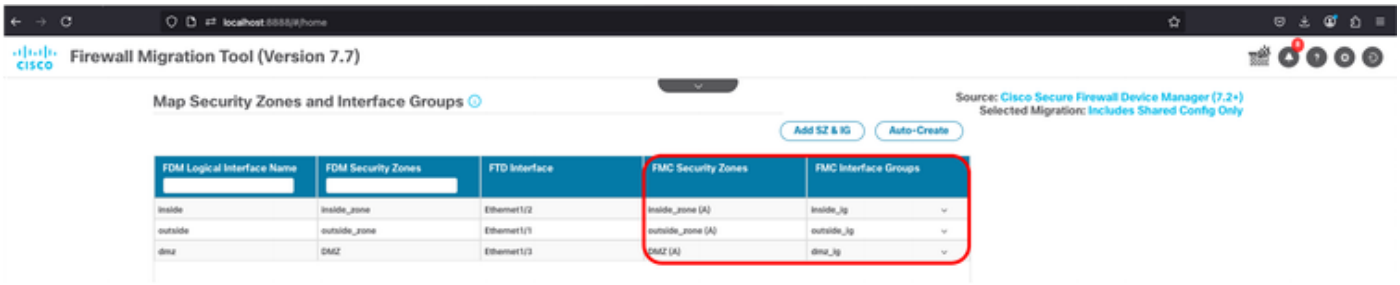
FMT - 데이터베이스 밀어넣기를 완료했습니다.

30. 다음 화면에서 보안 영역 및 인터페이스 그룹을 수동으로 생성하거나 자동 생성을 선택해야 합니다. 이 시나리오에서는 자동 생성이 사용됩니다.



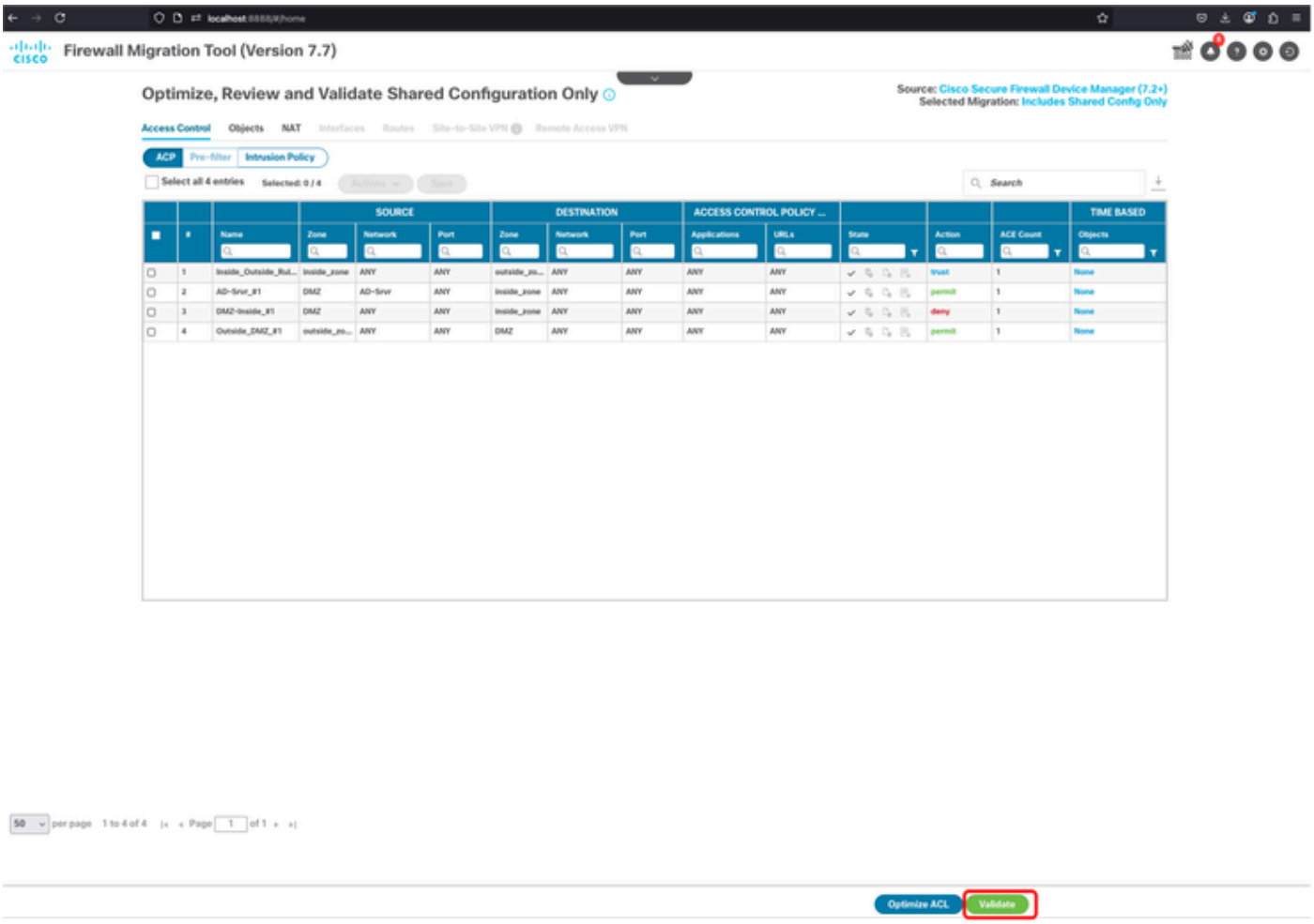
FMT - 보안 영역 및 인터페이스 그룹 자동 생성

31. 완료되면 테이블에 4번째 열과 5번째 열, 보안 영역 및 인터페이스 그룹이 각각 표시됩니다.



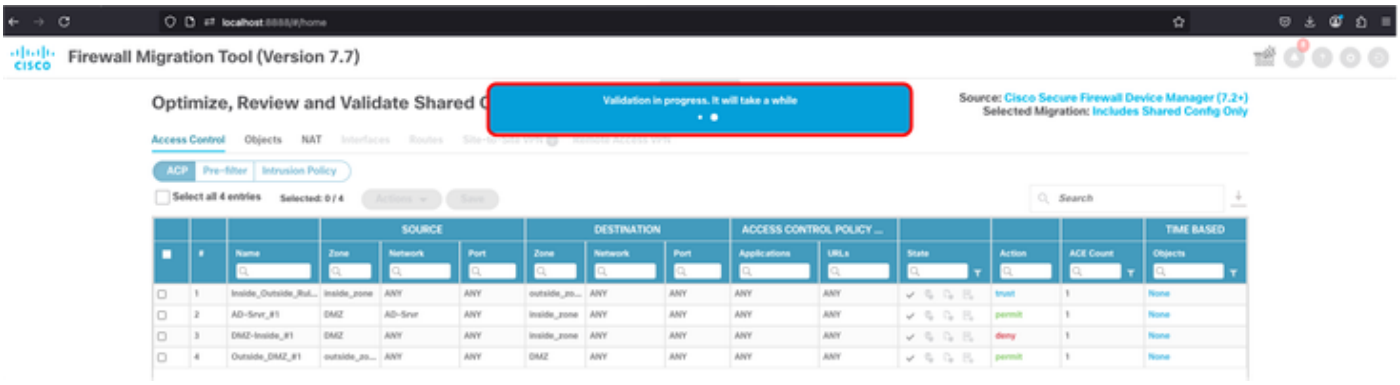
FMT - 보안 영역 및 인터페이스 그룹을 성공적으로 생성했습니다.

32. 다음 화면에서 ACL을 최적화하거나 ACP, 객체 및 NAT를 검증할 수 있습니다. 완료되면 Validate(검증) 버튼을 클릭합니다.



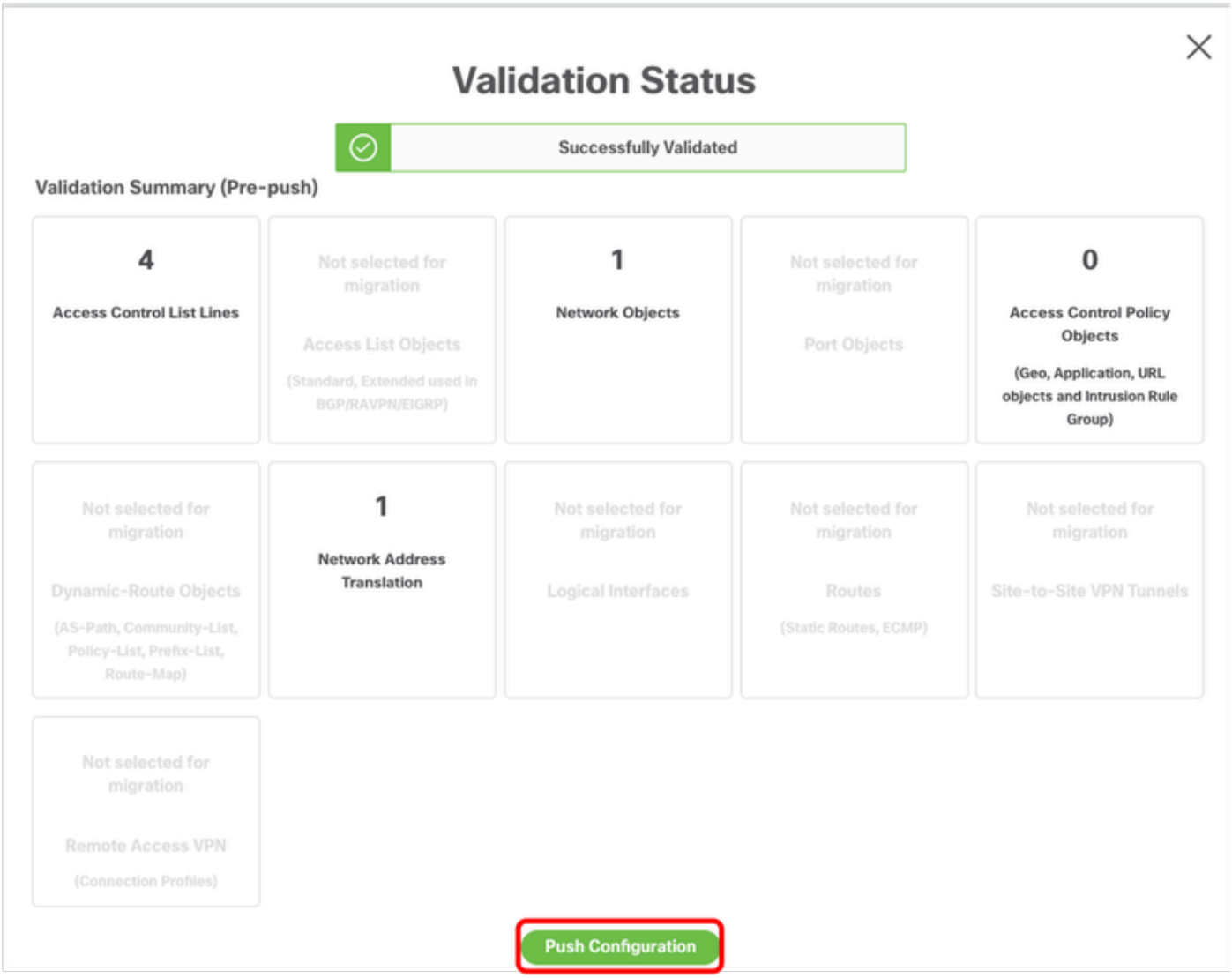
FMT - ACL 최적화 - 마이그레이션 검증

33. 검증이 완료되려면 몇 분 정도 걸립니다.



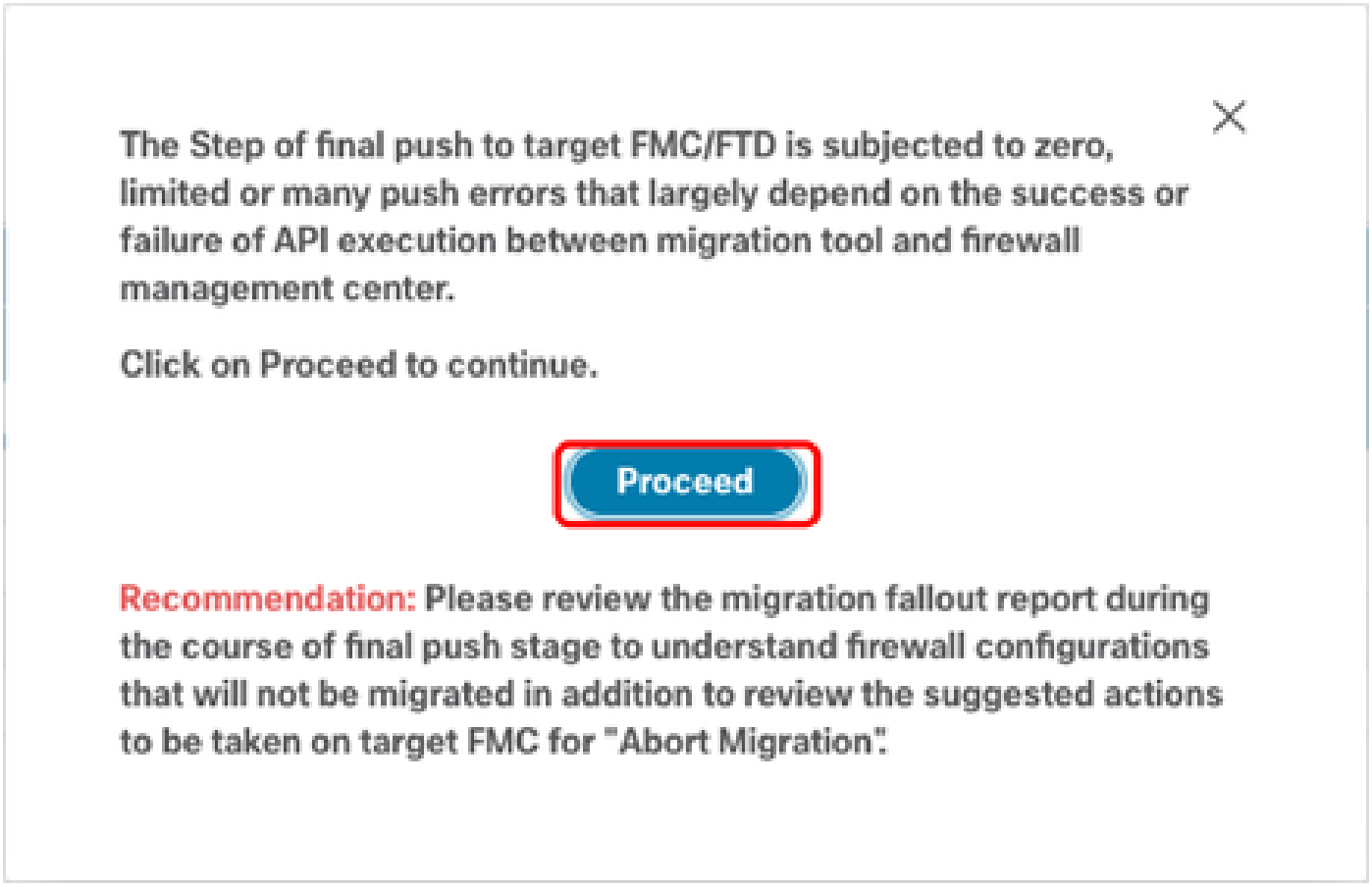
FMT - 검증 진행 중

34. 완료되면 FMT는 구성이 성공적으로 검증되었음을 알려주고 다음 단계는 구성 밀어넣기 단추를 누릅니다.



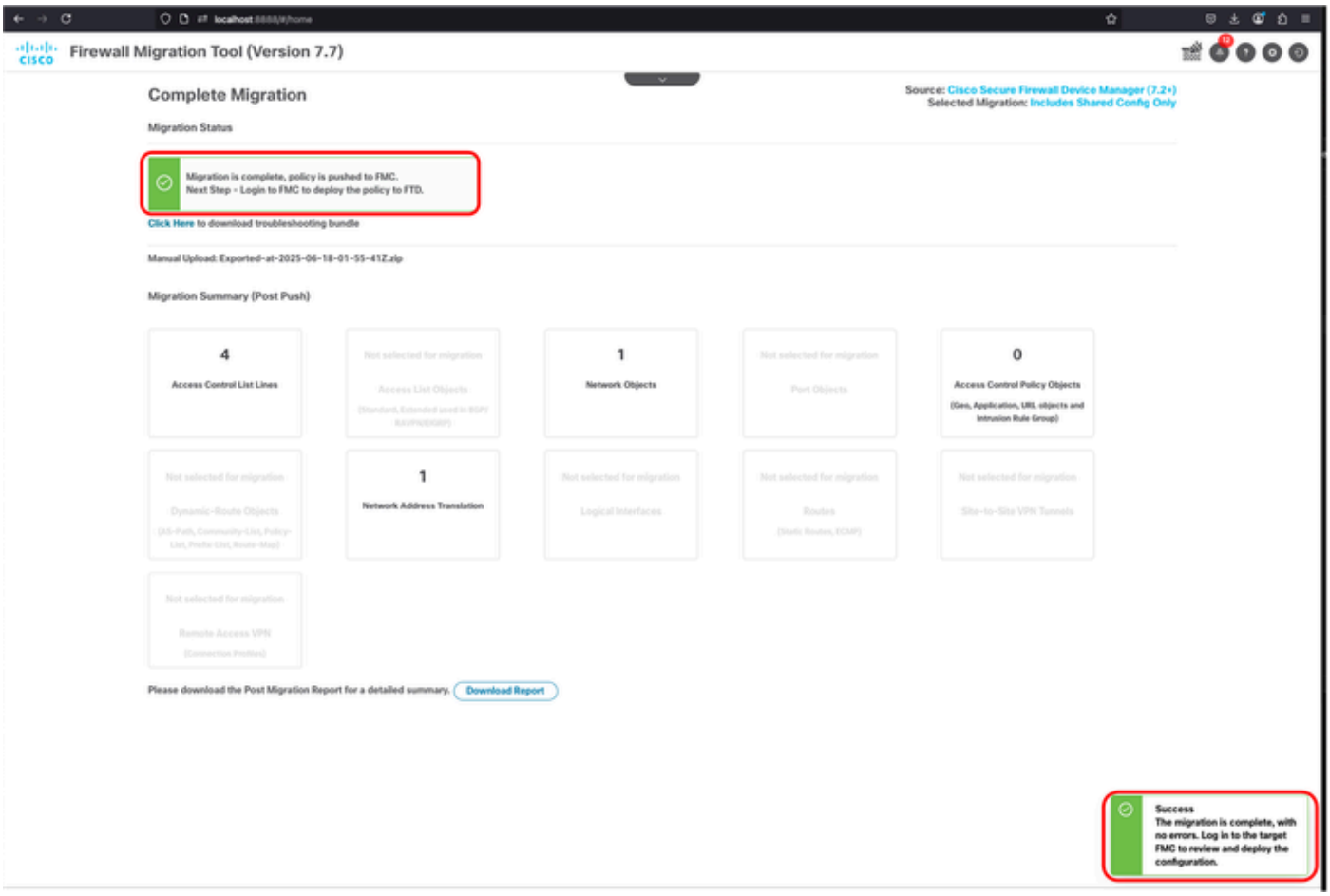
FMT - 검증 성공 - FMC로 컨피그레이션 푸시

35. 마지막으로 진행 버튼을 클릭합니다.



FMT - 컨피그레이션 푸시로 진행

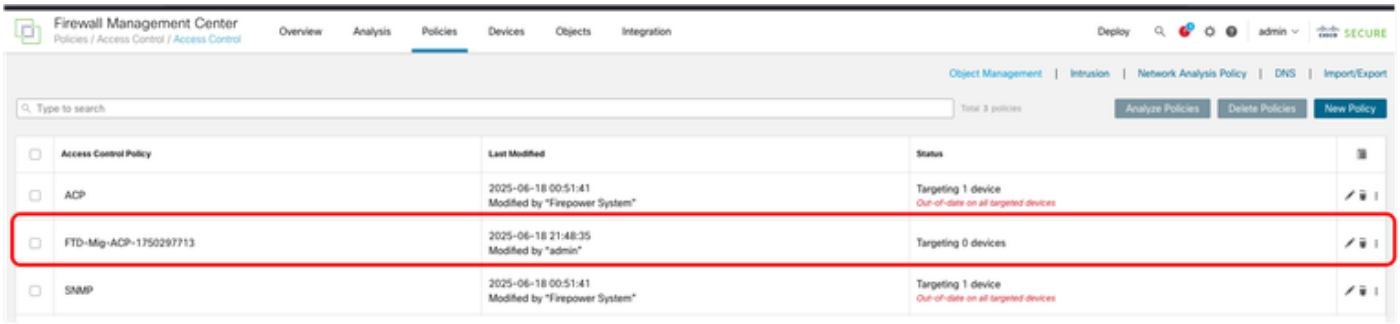
36. 모든 사항이 예상대로 진행되면 마이그레이션 성공 알림이 표시됩니다. FMT에서는 FMC에 로그인하고 마이그레이션된 정책을 FTD에 구축하도록 요청합니다.



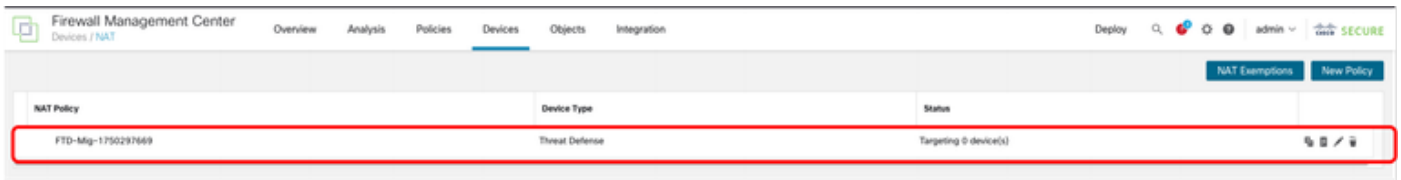
FMT - 마이그레이션 성공 알림

FMC 확인

37. FMC에 로그인하면 ACP 및 NAT 정책이 FTD-Mig로 표시됩니다. 이제 새 FTD로 구축을 진행할 수 있습니다.



FMC - ACP 마이그레이션됨



FMC - 마이그레이션된 NAT 정책

관련 정보

- FMT - FMC로의 FDM 마이그레이션 가이드
- FMT 릴리스 정보

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.