FDM을 통해 Snort 2에서 Snort 3으로 업그레이드

목차

소개

이 문서에서는 FDM(Firepower Device Manager)에서 snort 2에서 Snort 3 버전으로 업그레이드하는 방법에 대해 설명합니다.

사전 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FTD(Firepower Threat Defense)
- Firepower 장치 관리자(FDM)
- Snort.

요구 사항

다음과 같은 요구 사항이 있는지 확인합니다.

- firepower 장치 관리자에 액세스합니다.
- FDM에 대한 관리 권한
- snort 3을 사용하려면 FTD 버전이 6.7 이상이어야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD 7.2.7

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

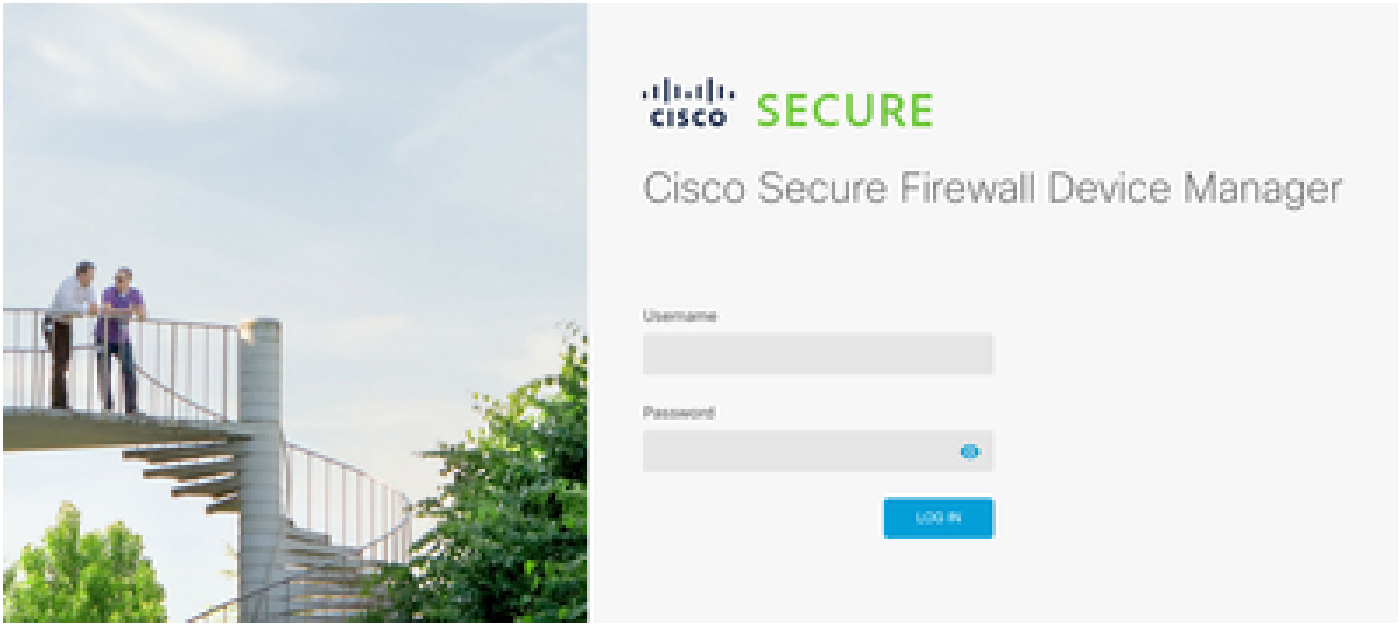
Snort 3 기능은 FDM(Firepower 장치 관리자)용 6.7 릴리스에 추가되었습니다. Snort 3.0은 다음과 같은 과제를 해결하도록 설계되었습니다.

- 메모리 및 CPU 사용량 감소
- HTTP 검사 효율성 향상
- 더 빠른 컨피그레이션 로드 및 Snort 재시작
- 프로그래밍 기능이 향상되어 기능을 더 빨리 추가할 수 있습니다.

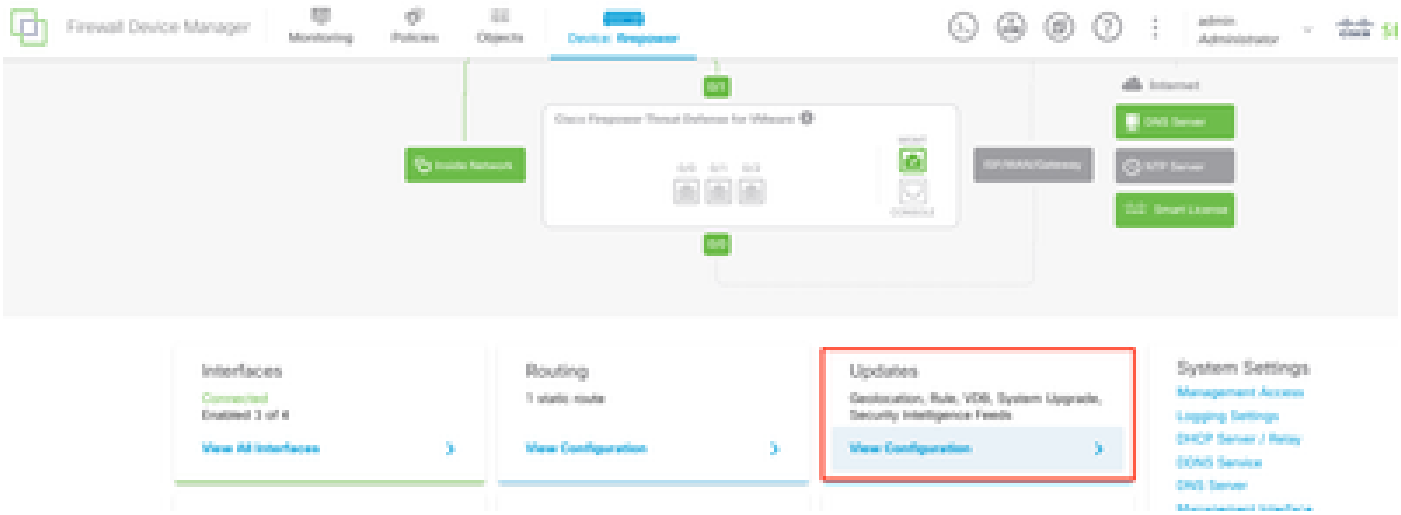
구성

설정

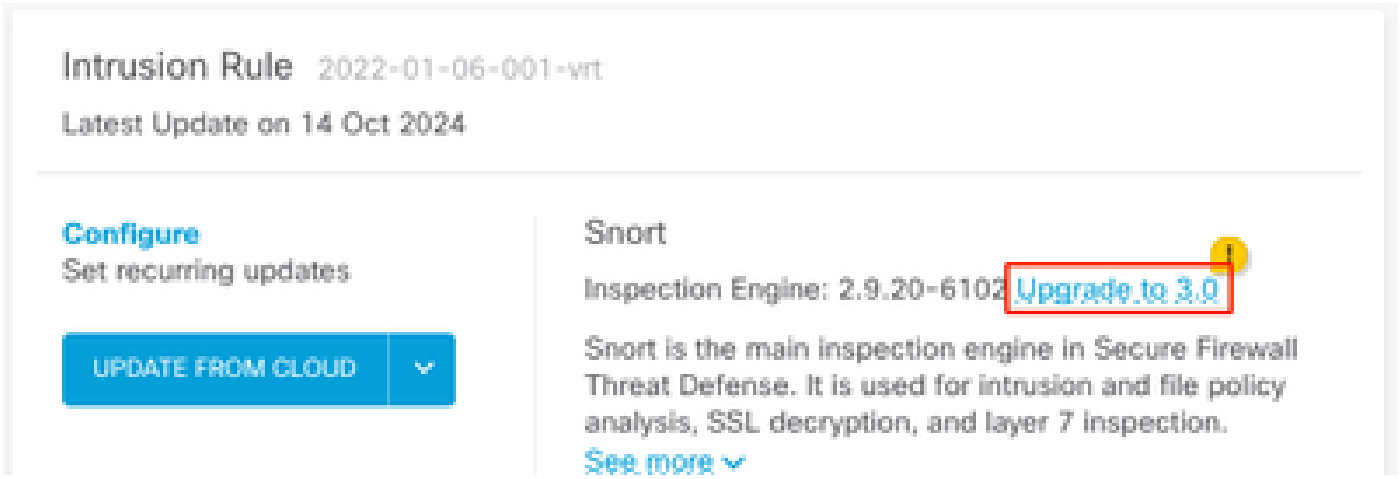
1. Firepower 장치 관리자에 로그인합니다.



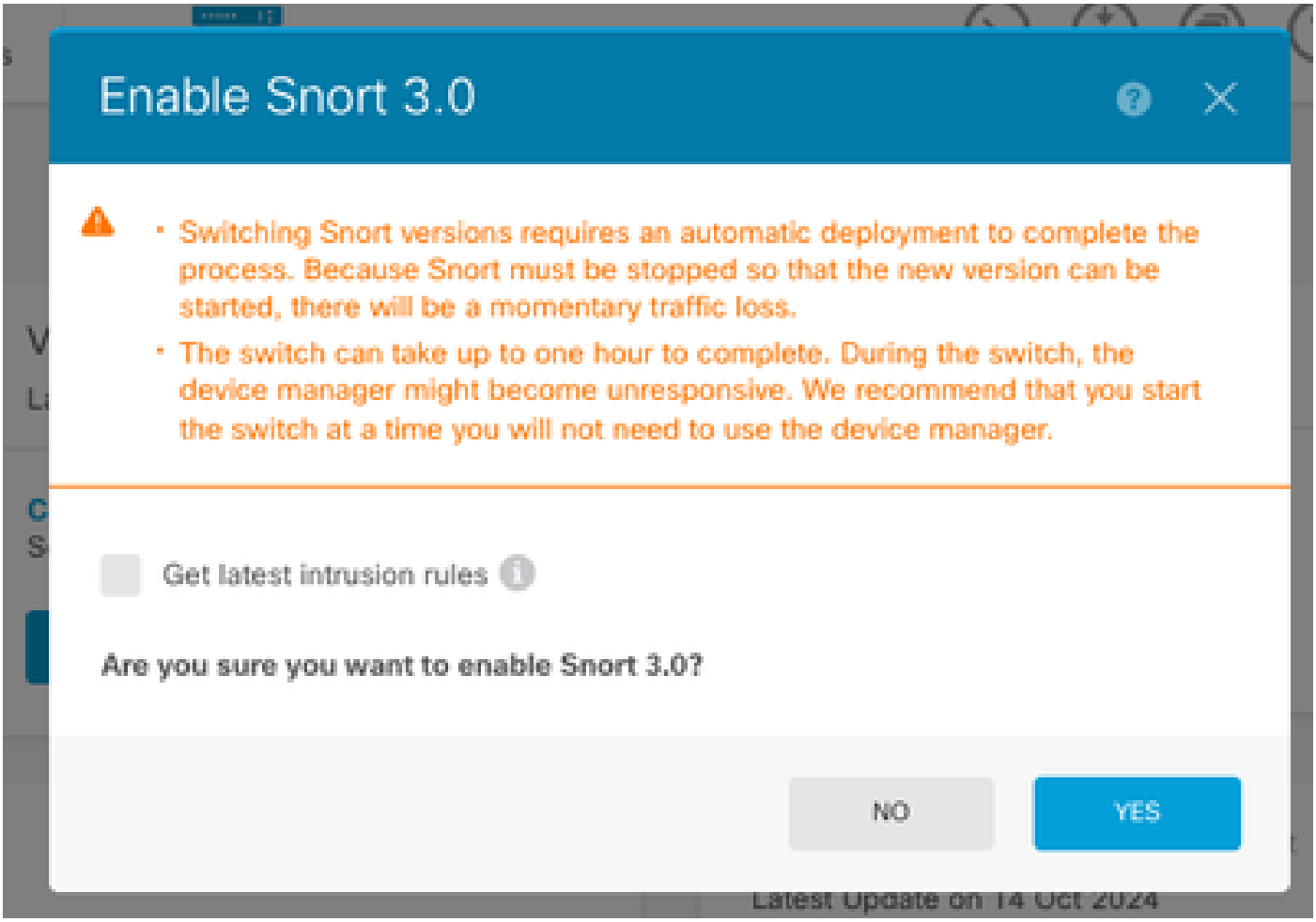
2. 장치 > 갱신 > 구성 보기로 이동합니다.

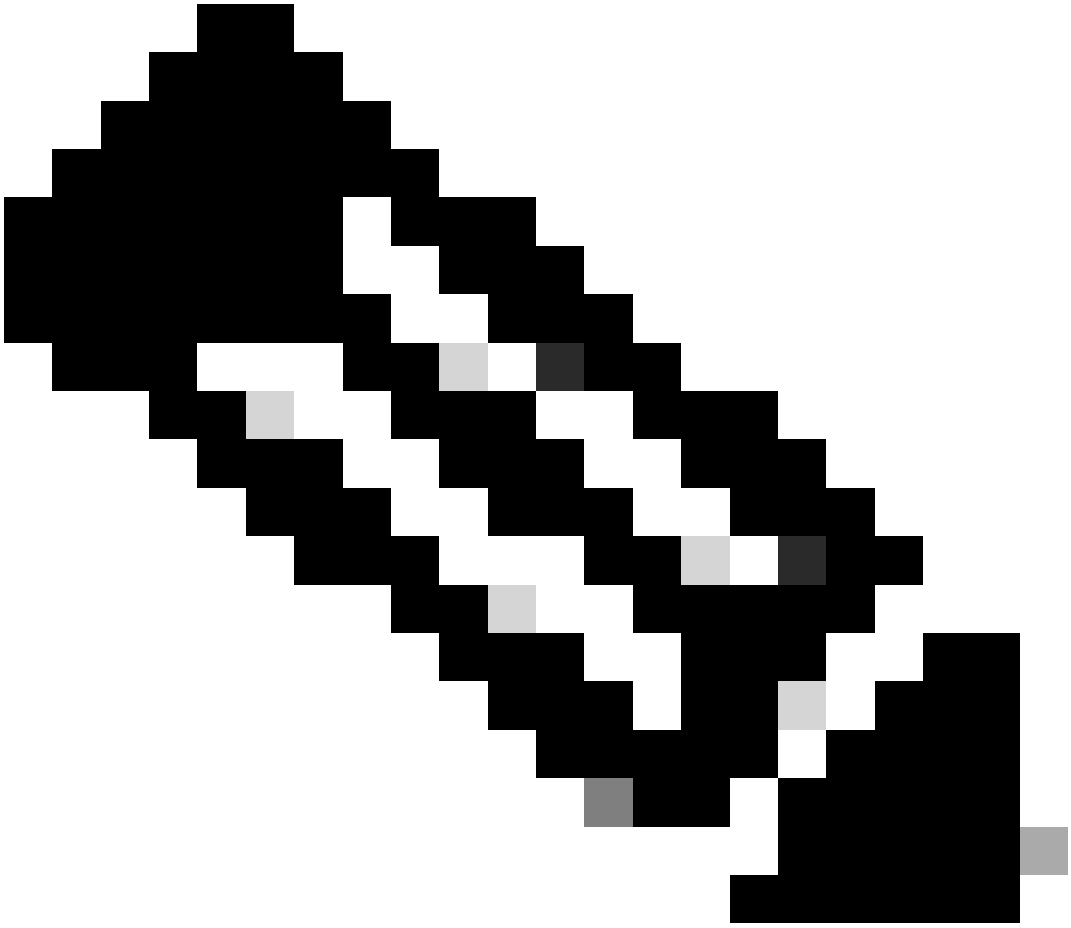


3. intrusion rules(침입 규칙) 섹션에서 upgrade to snort 3을 클릭합니다.

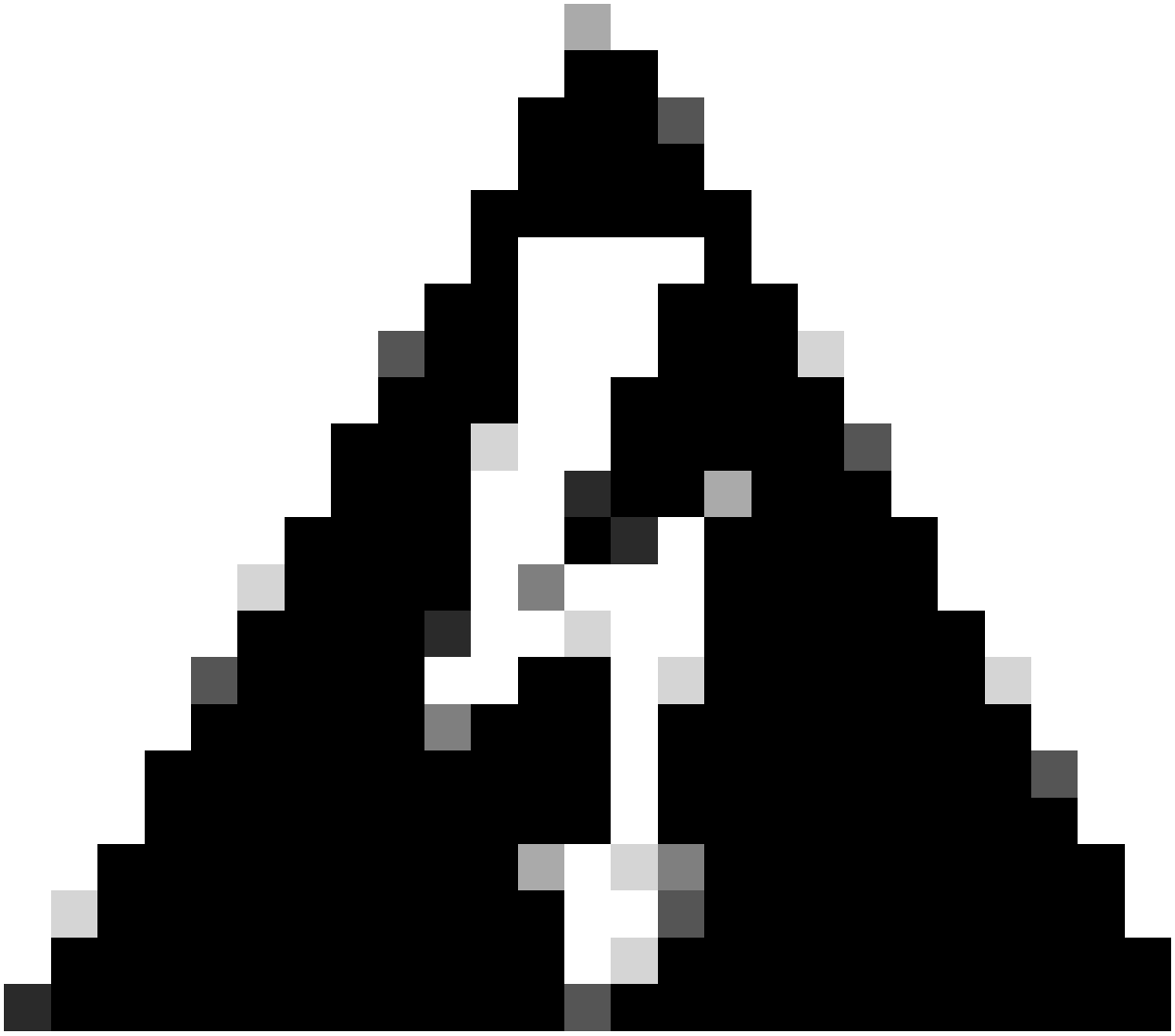


4. 선택 사항을 확인하는 경고 메시지에서 최신 침입 규칙 패키지를 가져오는 옵션을 선택한 다음 Yes를 클릭합니다.


Enable Snort 3.0
Switching Snort versions requires an automatic deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be a momentary traffic loss.
The switch can take up to one hour to complete. During the switch, the device manager might become unresponsive. We recommend that you start the switch at a time you will not need to use the device manager.
Get latest intrusion rules
Are you sure you want to enable Snort 3.0?
NO
YES
Latest Update on 14 Oct 2024

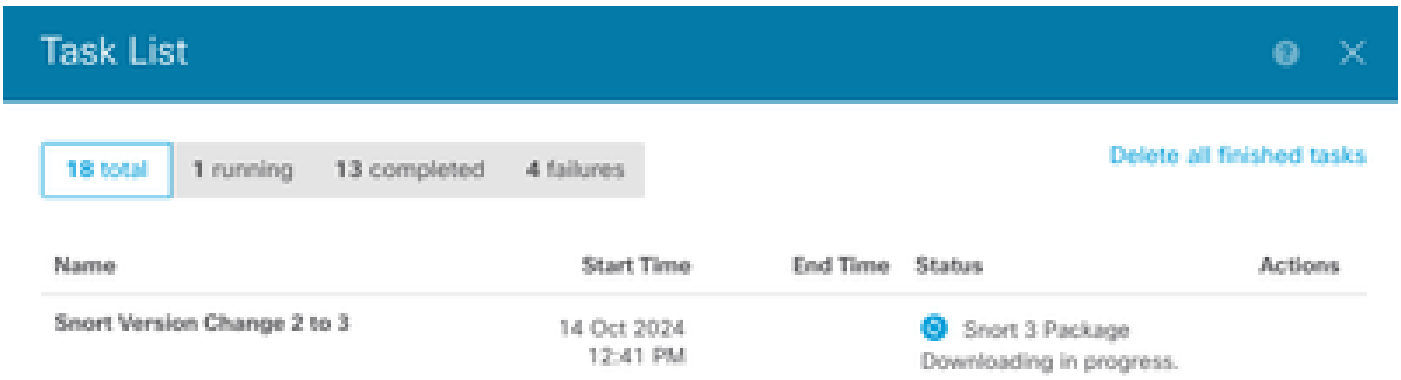


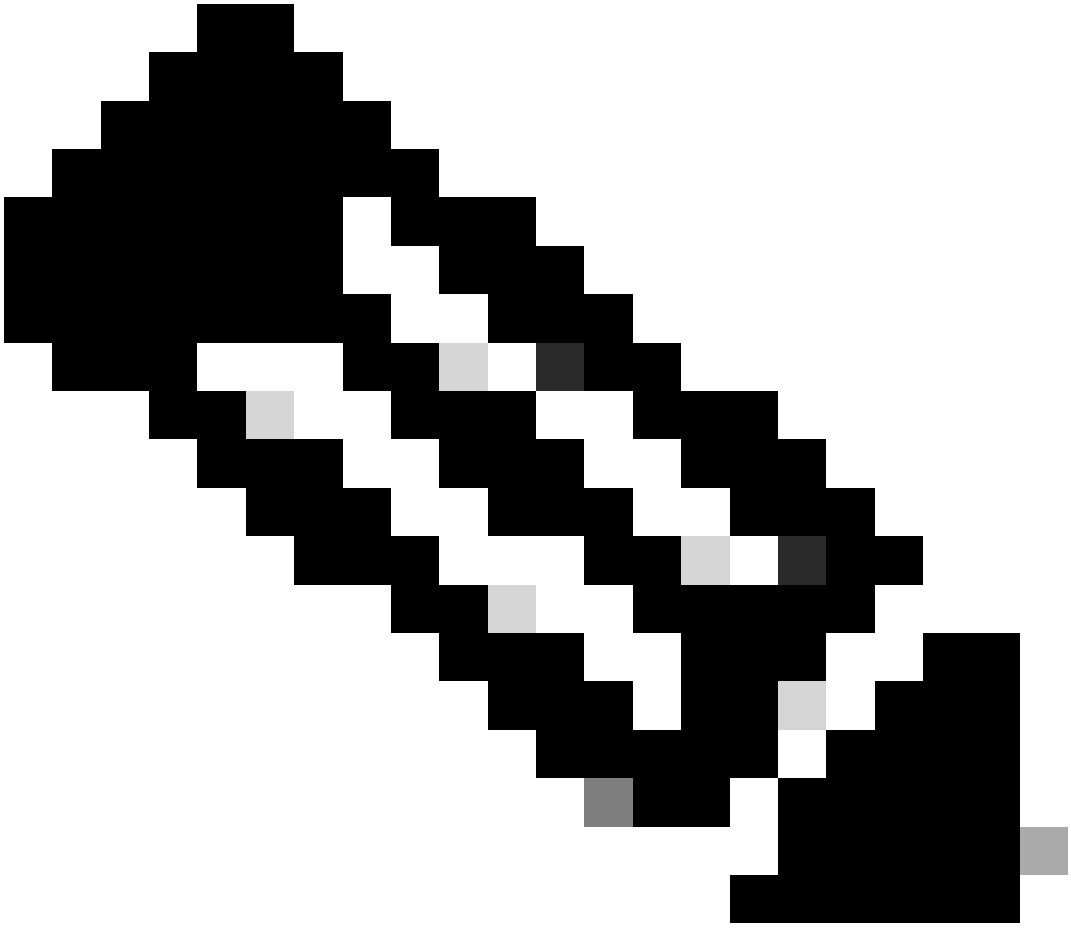
참고: 시스템에서는 활성 Snort 버전에만 패키지를 다운로드하므로 전환할 Snort 버전에 대한 최신 패키지가 설치되어 있지 않을 수 있습니다. 버전을 전환하는 작업이 완료될 때까지 기다려야 침입 정책을 수정할 수 있습니다.



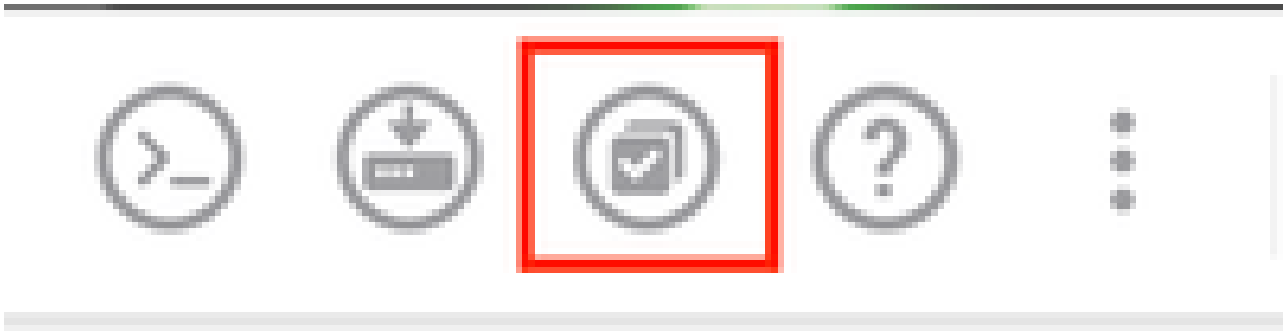
경고: Snort 버전으로 전환하면 일시적으로 트래픽이 손실됩니다.

5. 태스크 목록에서 업그레이드가 시작되었음을 확인해야 합니다.



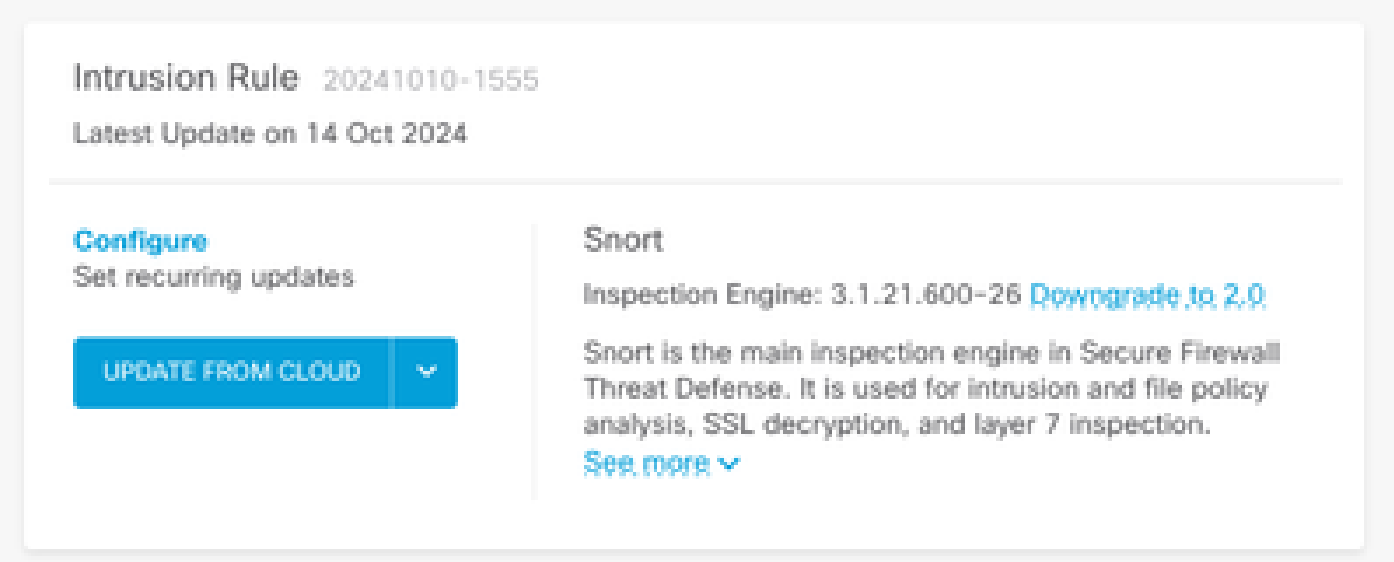


참고: 작업 목록은 구축 아이콘 옆의 탐색 모음에 있습니다.

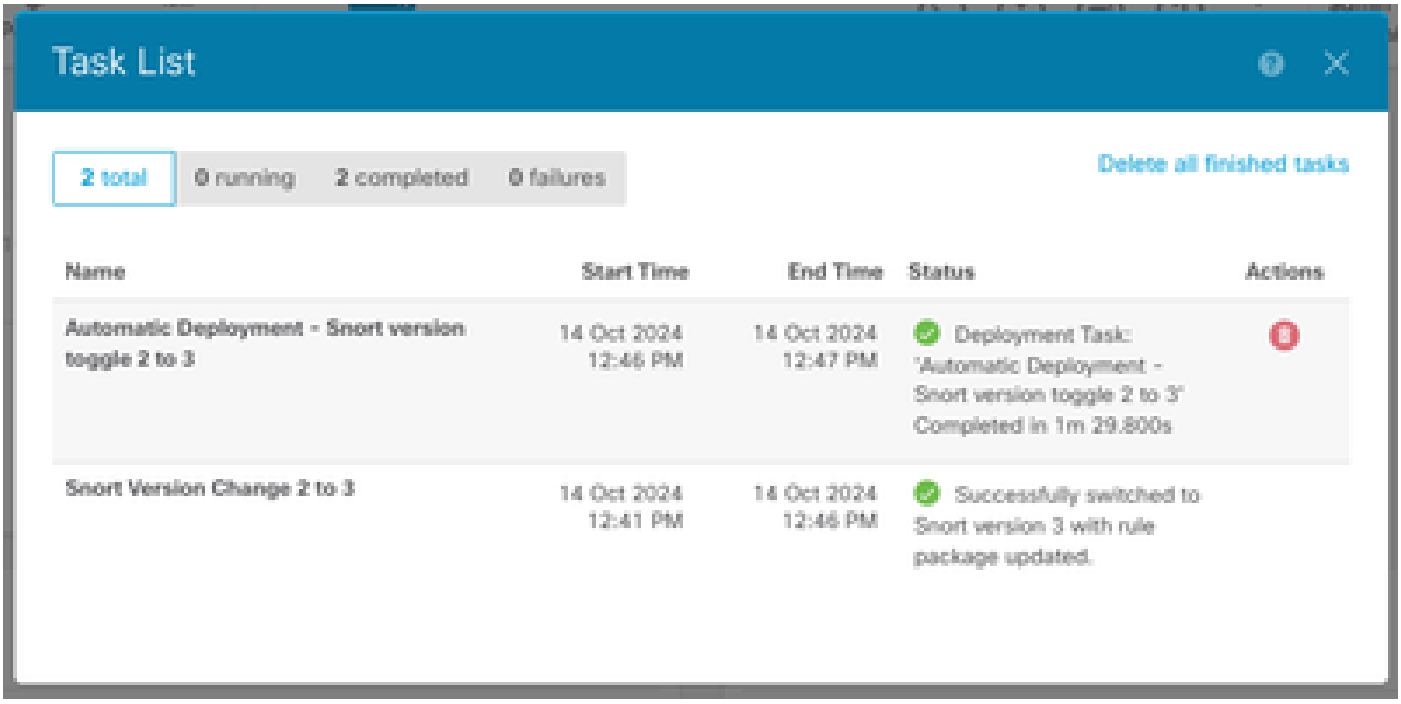


다음을 확인합니다.

Inspection Engine(검사 엔진) 섹션에는 현재 버전의 Snort 3이 표시됩니다.



마지막으로, 작업 목록에서 snort 3에 대한 변경 사항이 성공적으로 완료 및 구축되었는지 확인합니다.



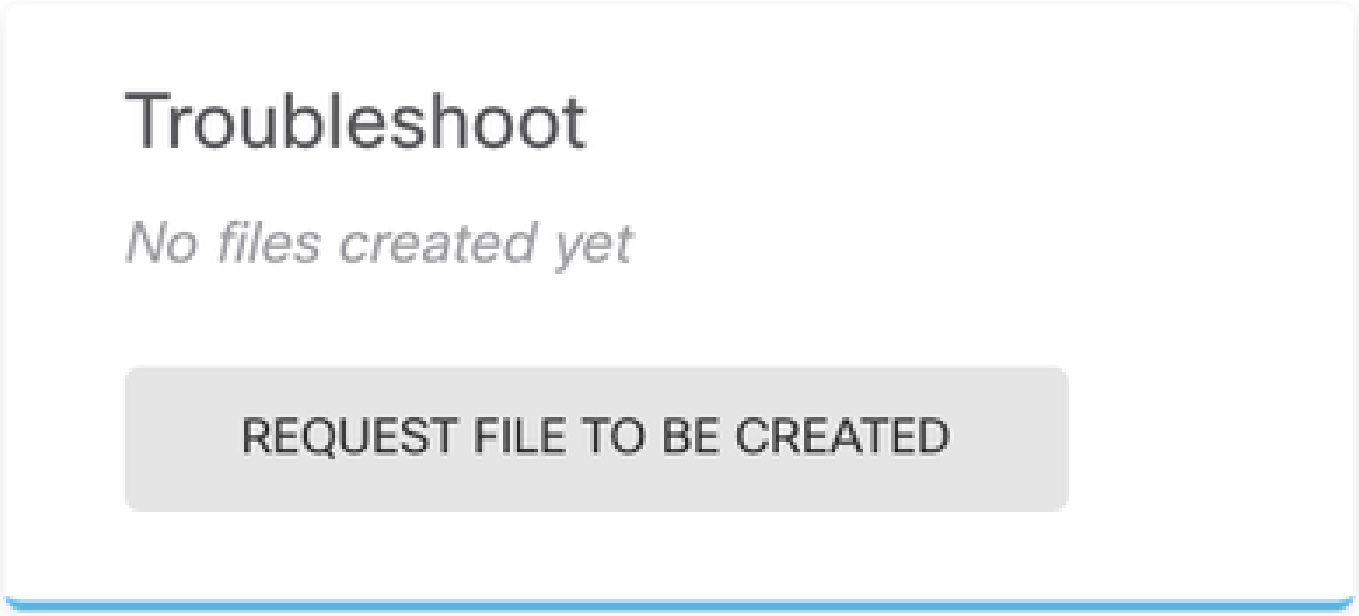
문제 해결

업그레이드하는 동안 문제가 발생하면 다음 단계를 고려하십시오.

- FTD 버전이 Snort 3과 호환되는지 확인합니다.

자세한 내용은 Cisco Secure Firewall Threat Defense 호환성 가이드를 참조하십시오

- [장치] 탭으로 이동한 다음 [파일 생성 요청]을 클릭하여 FDM에서 문제 해결 파일을 수집합니다. 수집된 후에는 TAC에서 케이스를 열고 케이스에 파일을 업로드하여 추가 지원을 받습니다.



관련 정보

- Snort 3 도입
- Snort 문서
- Cisco Secure Firewall Device Manager 컨피그레이션 가이드, 버전 7.2

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.