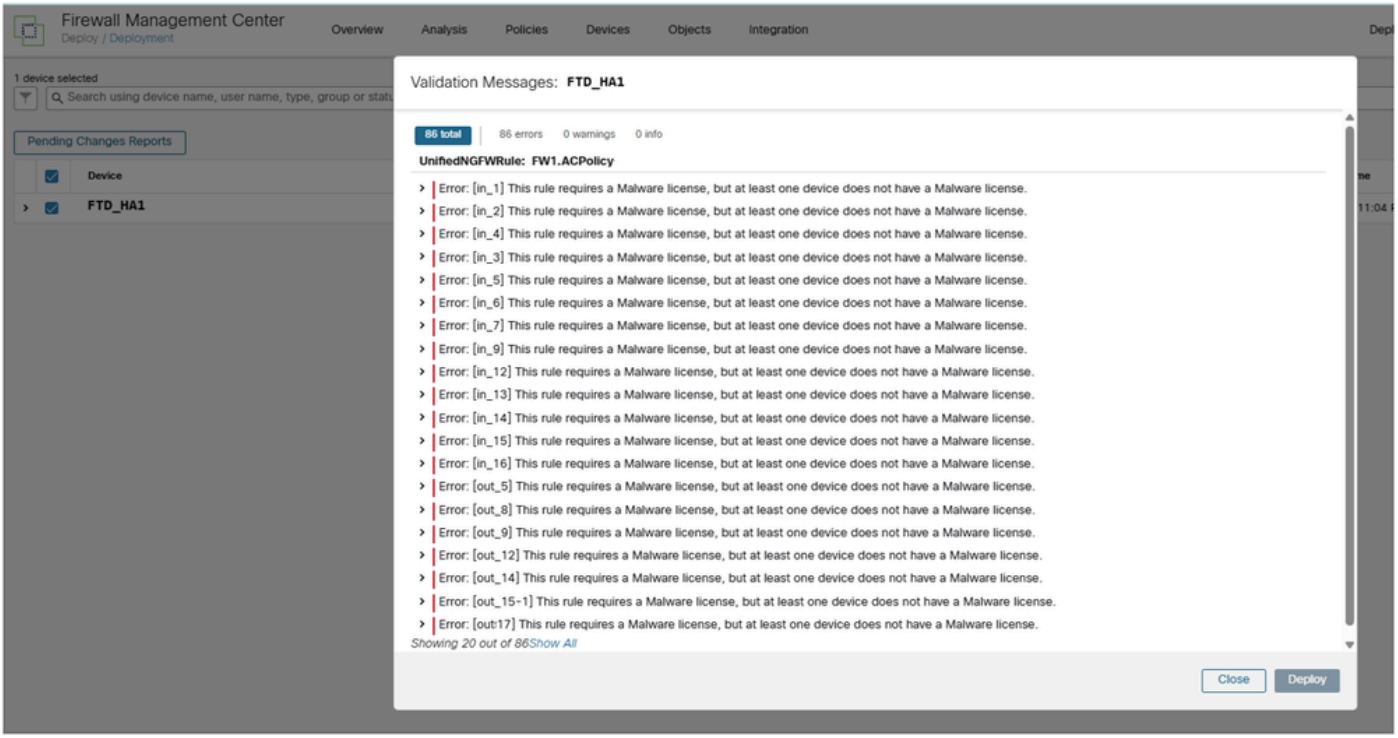
FTD 정책 구축의 악성코드 라이센스 오류 트러블슈팅

목차

문제

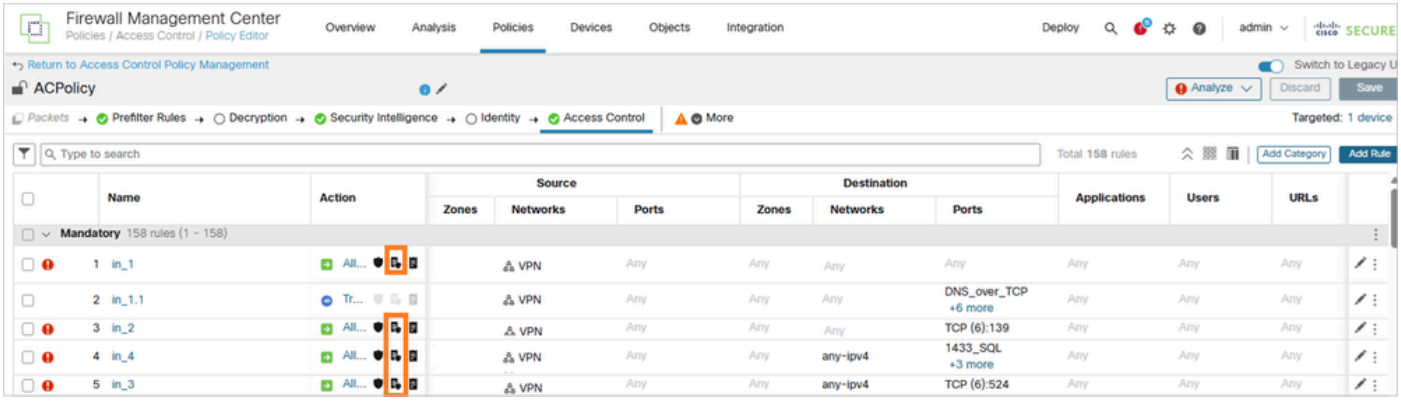
Cisco FMC(Secure Firewall Management Center)에서 정책을 변경하려고 하면 "이 규칙에는 악성코드 라이센스가 필요하지만 하나 이상의 디바이스에 악성코드 라이센스가 없습니다."라는 오류 메시지가 나타납니다. 이 오류는 정책 배포 및 컨피그레이션 변경 사항이 영향을 받는 방화벽 디바이스에 적용되지 않도록 합니다.



환경

- FMC 7.4.2. 기타 소프트웨어 버전도 영향을 받습니다.
- FTD(Firewall Threat Defense)를 실행하는 FPR1140. 다른 플랫폼도 영향을 받습니다.

- FTD는 하나 이상의 규칙에서 파일 정책이 활성화된 ACP(Access Control Policy)를 사용합니다.



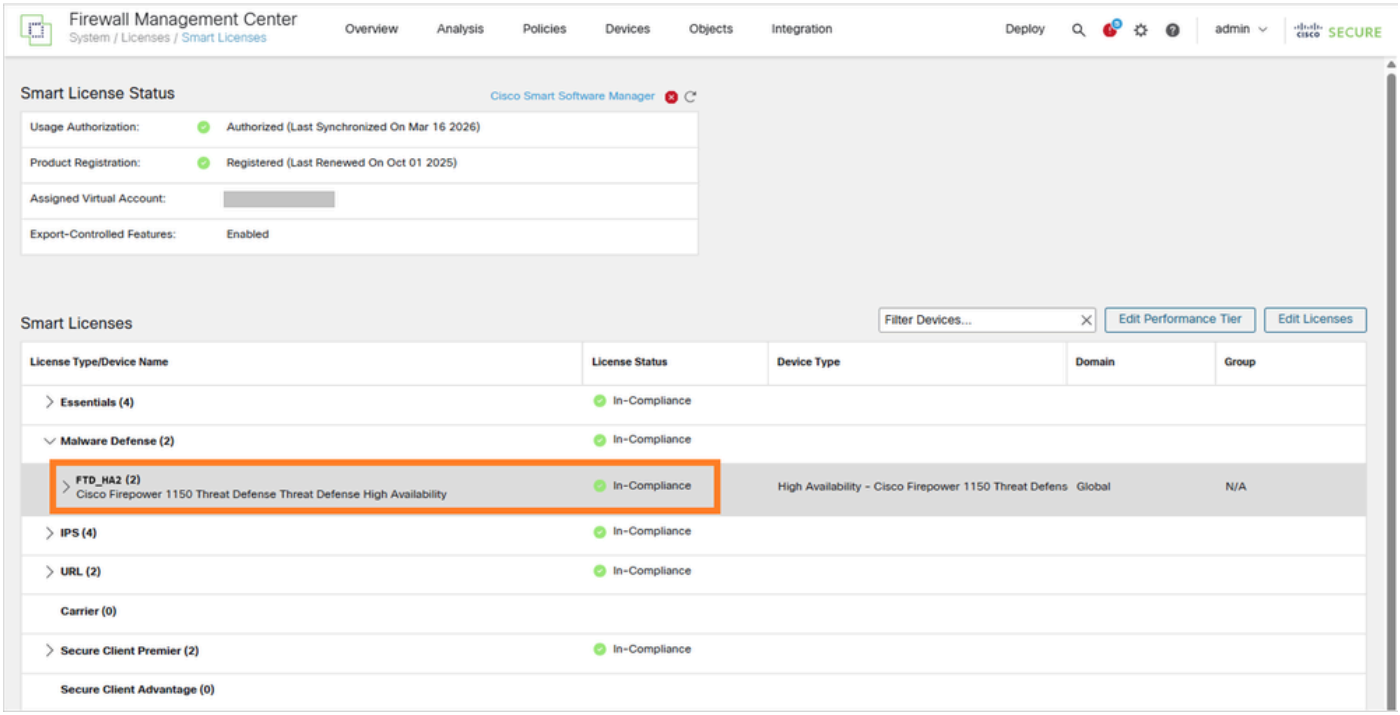
해결

이 악성코드 라이센스 오류 해결에는 영향을 받는 디바이스에 필요한 악성코드 라이센스를 가져와 설치하는 작업이 포함됩니다. 다음 단계를 사용하여 문제를 해결합니다.

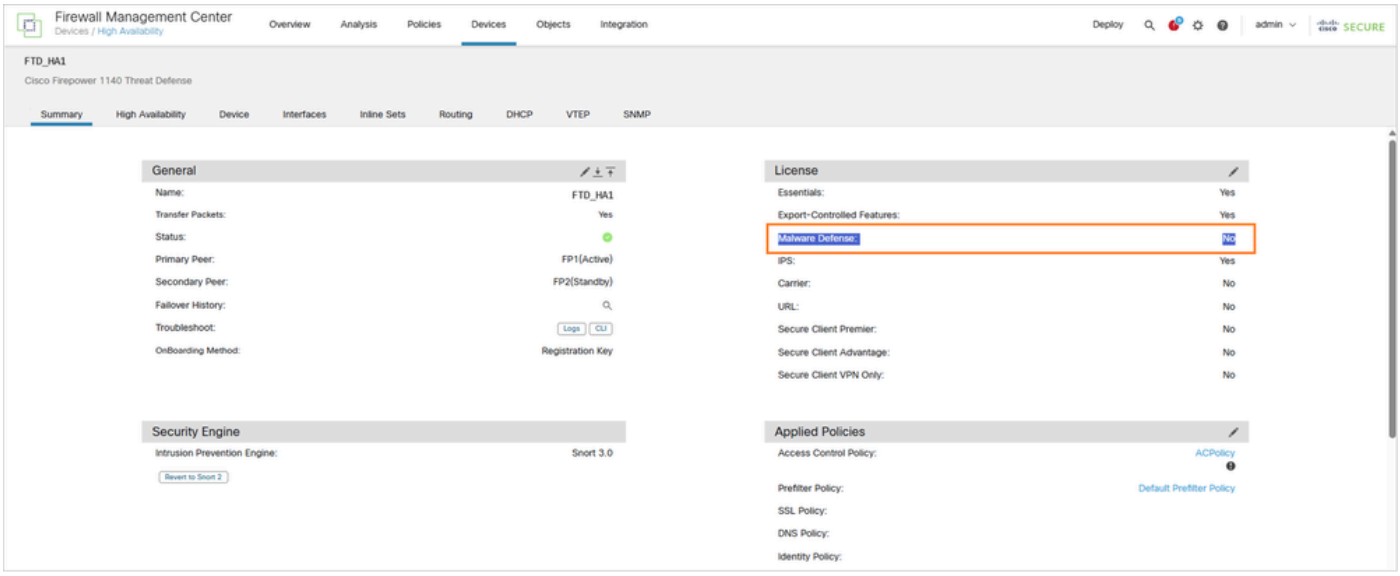
1단계. 라이센싱 격차 파악

영향을 받는 방화벽 디바이스에 AMP(Advanced Malware Protection)를 사용하도록 구성된 파일 정책이 있지만 해당 Malware Defense 라이센스가 없는지 확인합니다. 이는 디바이스 컨피그레이션을 확인하고 사용 가능한 라이센스와 비교하여 확인할 수 있습니다.

이 경우 FTD_HA2 쌍에만 악성코드 라이센스가 있습니다. FTD_HA1 쌍에는 다음 항목이 없습니다.



FTD_HA1 방화벽 쌍에 Malware 라이센스가 No(아니요)로 설정되어 있습니다.



2단계. 필요한 라이센스 받기

Cisco 영업 담당자 또는 공인 파트너와 협력하여 해당 장치에 필요한 악성코드 라이센스를 확보합니다. 라이센스는 특정 방화벽 모델 및 구축 요건에 적합해야 합니다.

3단계. 악성코드 라이센스 설치

라이센스를 얻은 후에는 표준 Cisco 라이센싱 프로세스를 통해 해당 디바이스에 설치합니다. 여기에는 일반적으로 관리 컨피그레이션에 따라 FMC를 통해 라이센스를 적용하거나 디바이스에서 직접 라이센스를 적용하는 것이 포함됩니다.

4단계. 라이센스 설치 확인

라이센스를 설치한 후 Malware Defense 기능이 이제 제대로 활성화되었는지, 라이센스 오류가 제거되었는지 확인합니다.

5단계. 정책 배포 테스트

정책 변경 내용을 다시 배포하여 라이선스 문제가 해결되었으며 정책 작업이 정상적으로 진행될 수 있는지 확인하십시오.

원인

이 오류는 파일 정책이 AMP 기능을 사용하도록 구성되어 있지만 해당 Malware Defense 라이센스가 해당 방화벽 디바이스에 설치되어 있지 않거나 활성화되지 않은 라이센스 검증 불일치로 인해 발생합니다. FMC는 정책이 기술적으로 구성된 경우에도 라이센스 준수를 시행하고 필요한 라이센스가 누락된 경우 정책 구축을 방지합니다.

이러한 검증을 통해 올바른 라이센스 기능만 디바이스에 구축되어 Cisco의 라이센스 요구 사항을 준수하고 라이센스 없는 기능의 사용을 방지할 수 있습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

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.