FMC에서 문제 해결 Syslog를 전송하고 볼 디바이스 구성

목차

소개

이 문서에서는 진단 syslog 메시지를 FMC에 전송하고 Unified Event Viewer에서 볼 수 있도록 관리되는 디바이스를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.
· Syslog 메시지
•FMC(Firepower Management Center)
•FTD(Firepower Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
· 이 문서는 모든 Firepower 플랫폼에 적용됩니다.
· 소프트웨어 버전 7.6.0을 실행하는 FTD(Secure Firewall Threat Defense Virtual)
· 소프트웨어 버전 7.6.0을 실행하는 FMC(Secure Firewall Management Center Virtual)
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.

기능 개요

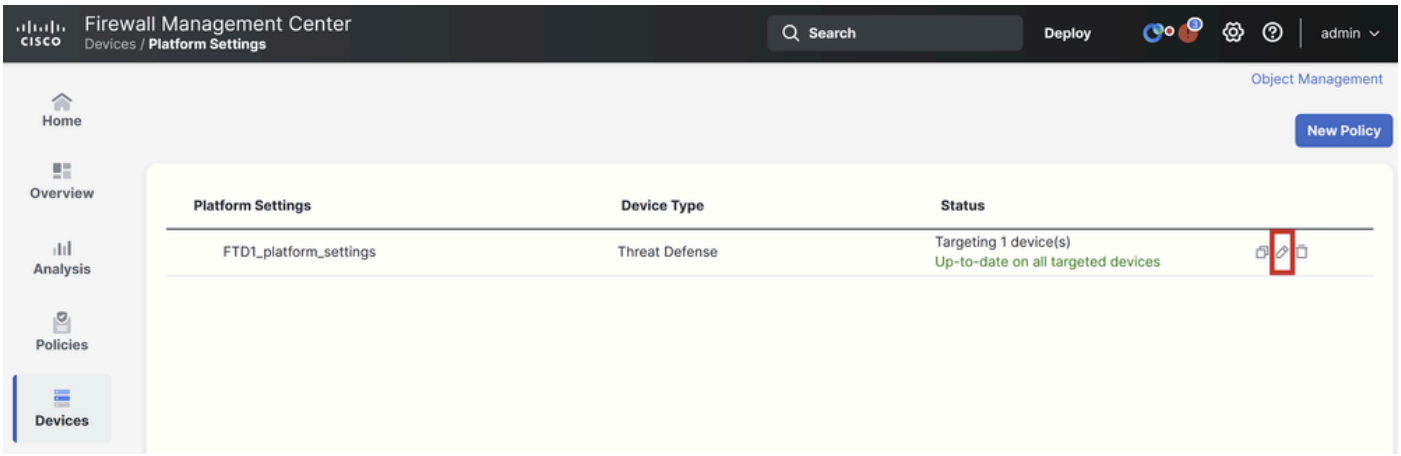
Secure Firewall 7.6의 Unified Event Viewer 테이블에 새로운 Troubleshoot 이벤트 유형이 추가됩니다. 플랫폼 설정 syslog 로깅 컨피그레이션이 확장되었으며 VPN 로그만 전송하는 대신 LINA에서 생성한 진단 syslog 메시지를 FMC로 전송할 수 있습니다. 이 기능은 FMC 7.6.0과 호환되는 소프트웨어 버전을 실행하는 모든 FTD에서 구성할 수 있습니다. cdFMC에는 분석 도구가 없으므로

cdFMC는 지원되지 않습니다.

- All Logs(모든 로그) 옵션은 이벤트 볼륨으로 인한 긴급, 경고 및 위기 로그 레벨로 제한됩니다 .
- 이 트러블슈팅 로그는 디바이스에서 FMC로 전송된 모든 syslog를 표시합니다(VPN 또는 기타).
- 문제 해결 로그는 FMC로 이동하며 Unified Event View(통합 이벤트 보기) 및 Devices(디바이스) > Troubleshoot(문제 해결) > Troubleshooting Logs(문제 해결 로그) 아래에 표시됩니다.

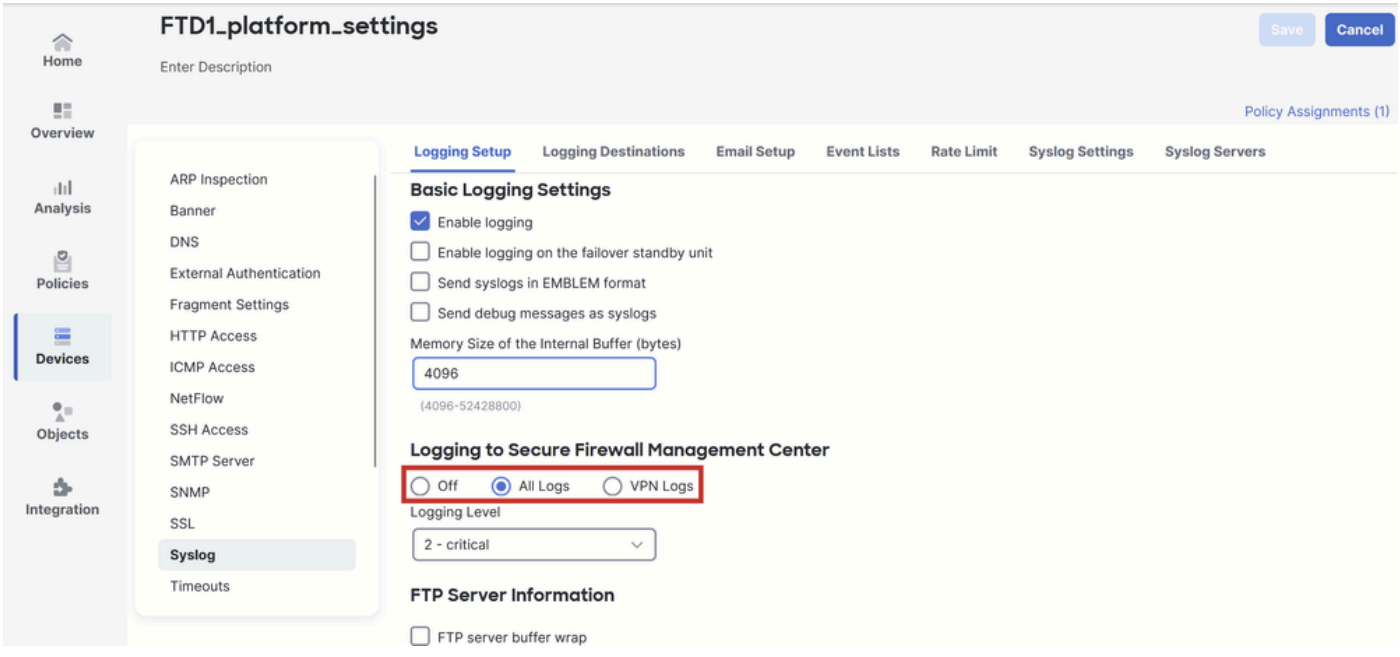
구성

FMC Devices(FMC 디바이스) > Platform Settings(플랫폼 설정)로 이동하고 정책의 오른쪽 상단 모서리에 있는 Edit(수정) 아이콘을 클릭합니다.



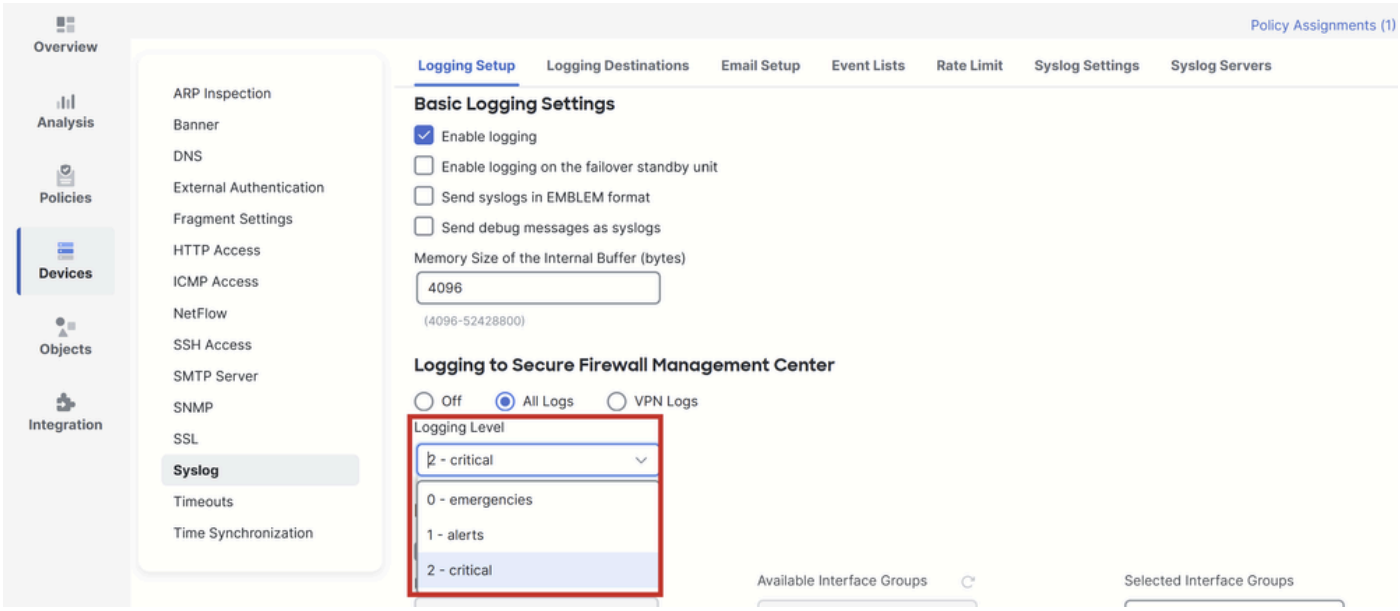
플랫폼 설정 정책

Syslog > Logging Setup으로 이동합니다. Logging to Secure Firewall Management Center(Secure Firewall Management Center에 로깅)에서 세 가지 옵션을 볼 수 있습니다.



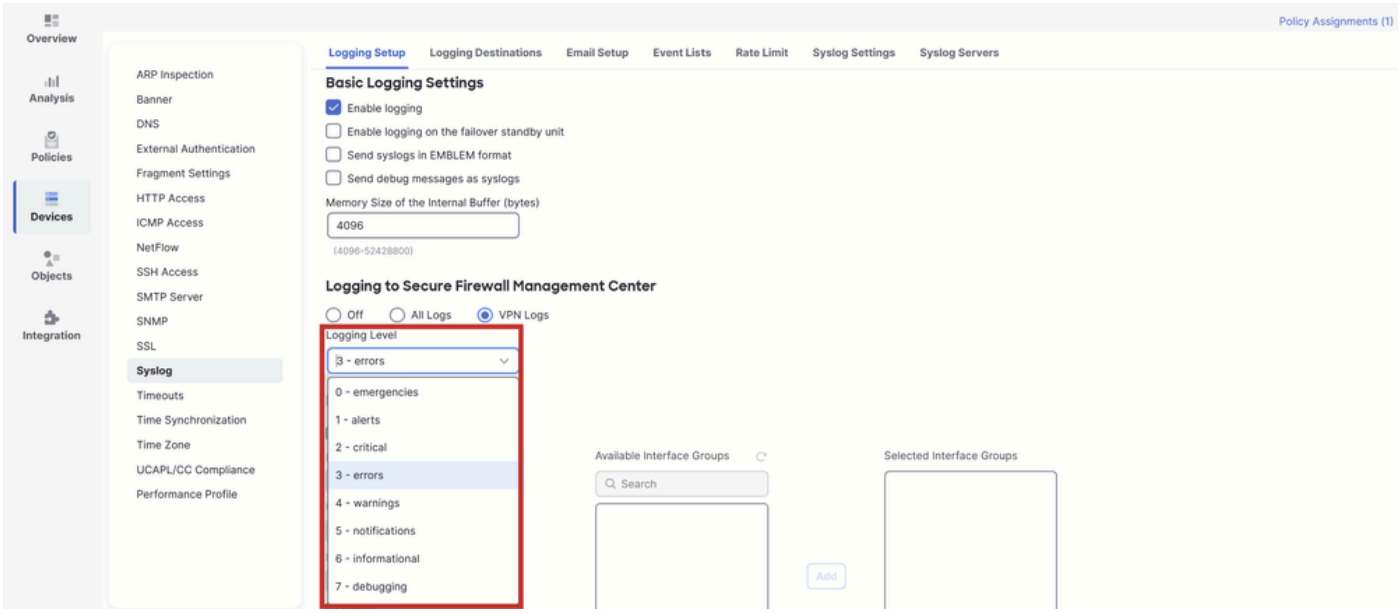
3가지 로깅 옵션

All Logs(모든 로그)를 선택하는 경우 사용 가능한 세 가지 로깅 레벨 중 하나를 선택할 수 있습니다. 긴급 상황, 경고, 위험 상황 등 모든 진단 syslog 메시지를 FMC(VPN 포함)로 전송합니다.

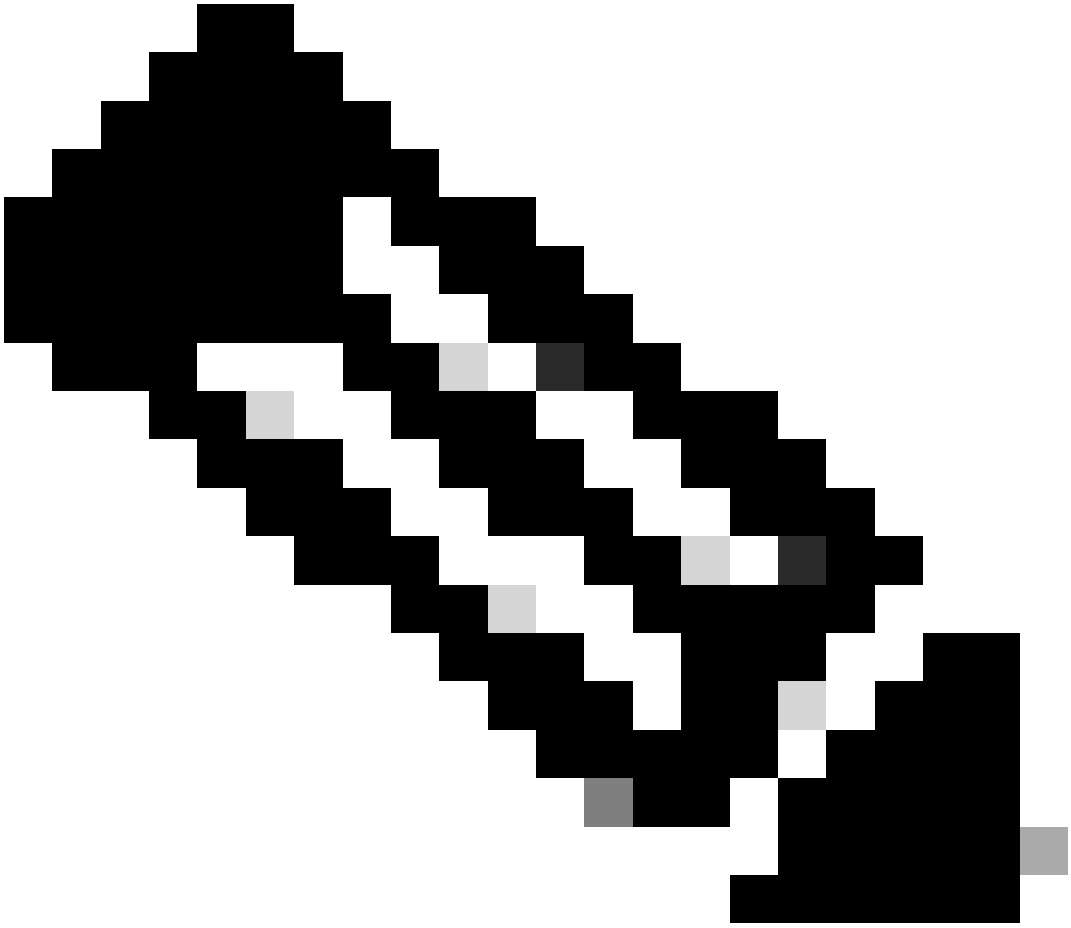


사용 가능한 로깅 레벨

VPN Logs(VPN 로그)를 선택하는 경우 모든 로깅 레벨이 사용 가능하며 그 중 하나를 선택할 수 있습니다.

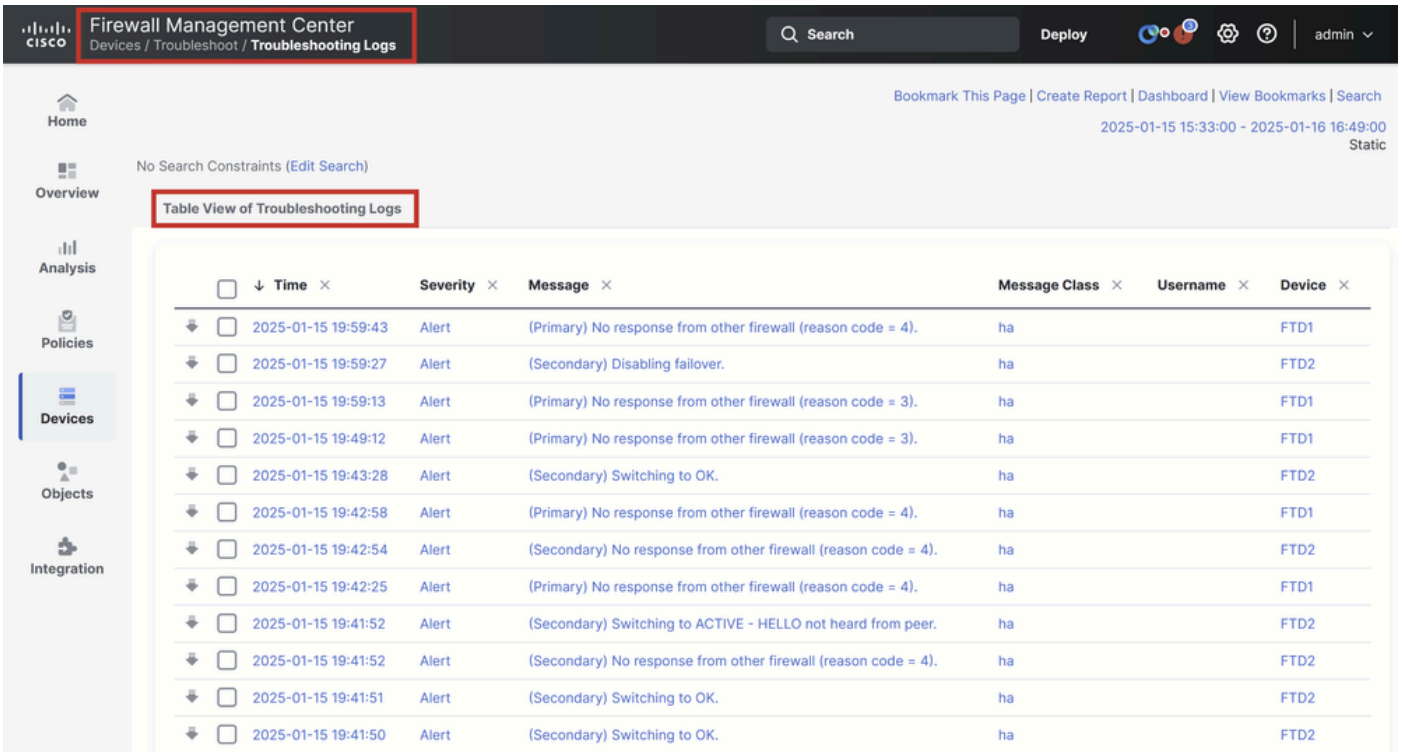


사용 가능한 로깅 레벨



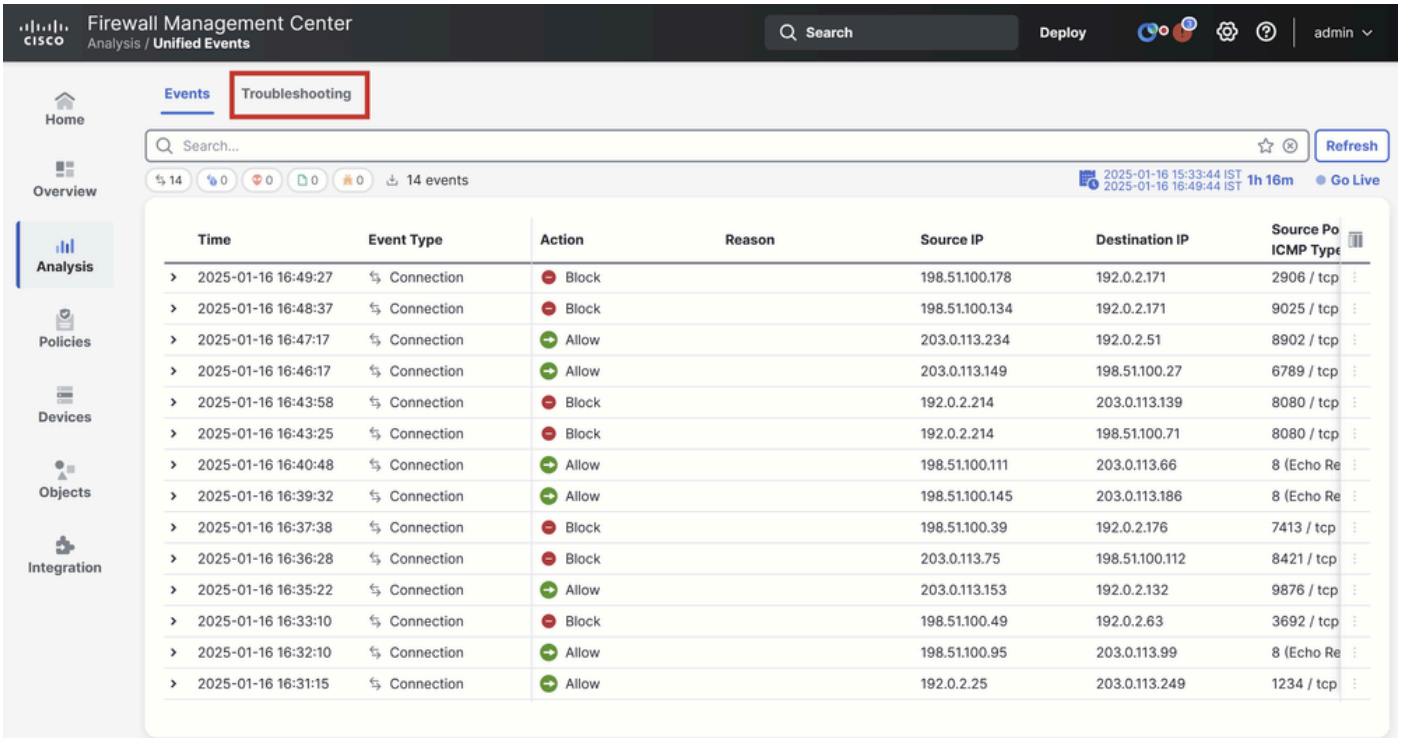
참고: Site-to-Site 또는 원격 액세스 VPN을 사용하여 디바이스를 구성하면 기본적으로 VPN syslog를 관리 센터에 전송할 수 있습니다. VPN 로그 이외의 모든 syslog를 FMC로 보내도록 All Logs(모든 로그)로 변경할 수 있습니다.

이러한 로그는 Devices(디바이스) > Troubleshoot(문제 해결) > Troubleshooting Logs(문제 해결 로그)에서 액세스할 수 있습니다.



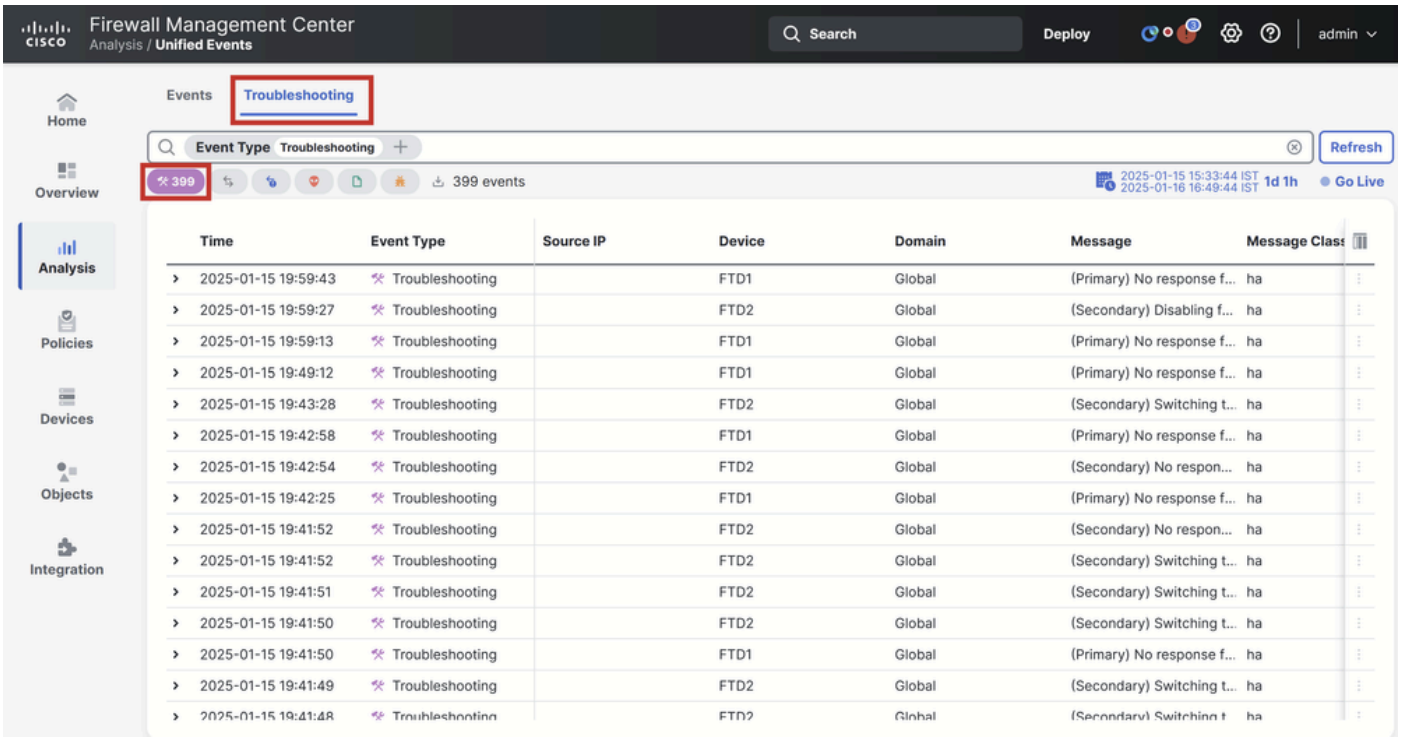
문제 해결 로그의 표 보기

이제 Unified Event Viewer 페이지에서 새 문제 해결 보기 탭을 사용할 수 있습니다. 이러한 이벤트를 보려면 Analysis > Unified Events > Troubleshooting으로 이동합니다.



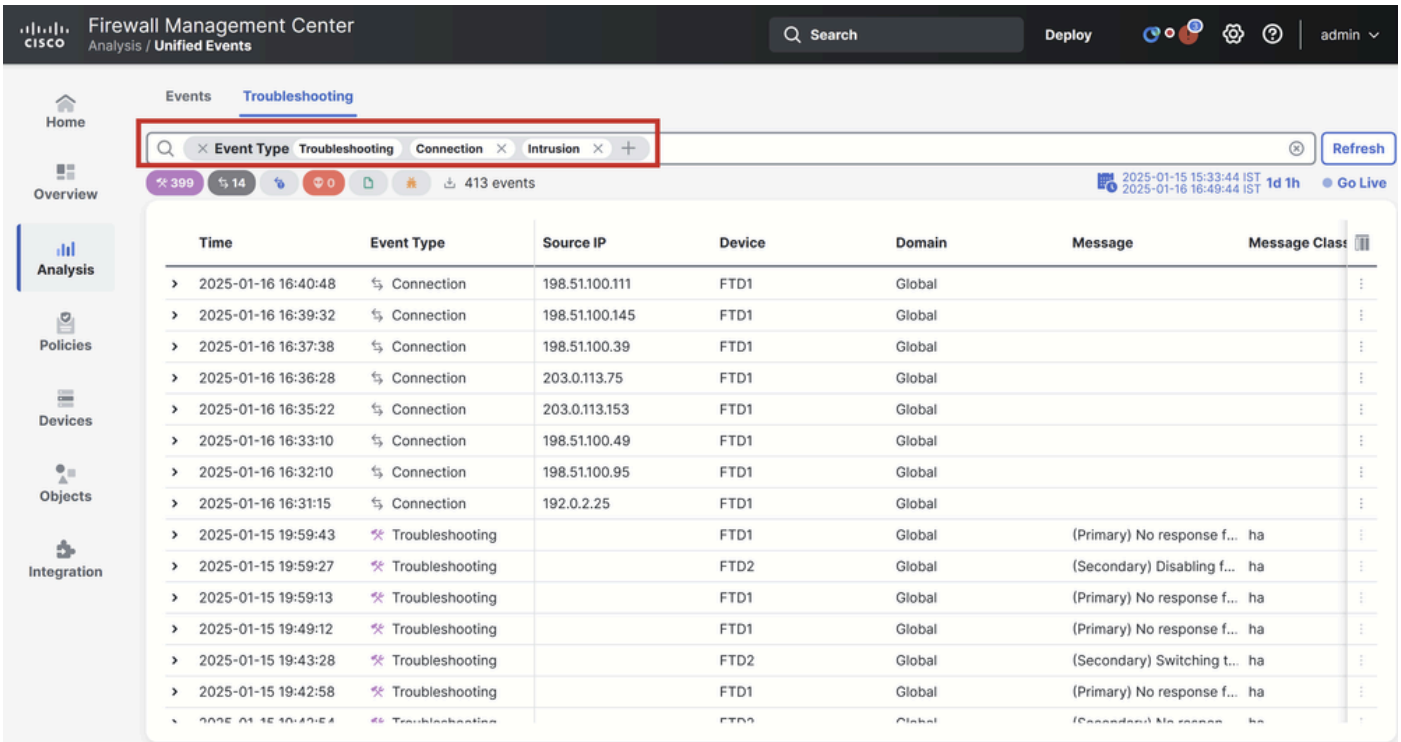
문제 해결 보기

이 탭으로 전환하면 테이블에 새 이벤트 유형이 표시됩니다. 다른 유형과 마찬가지로 Troubleshooting 뷰의 중심이므로 뷰에서 추가하거나 제거할 수 없습니다.



문제 해결 이벤트 유형

다른 이벤트 유형은 이 트러블슈팅 보기에서 계속 추가 및 제거할 수 있습니다. 이렇게 하면 진단 로그를 다른 이벤트 데이터와 함께 볼 수 있습니다.



기타 이벤트 유형

구성 확인

FMC GUI에서 컨피그레이션을 완료하면 FTD CLI에서 show running-config logging 및 show logging 명령을 CLISH 또는 LINA 모드로 실행하여 확인할 수 있습니다.

```
FTD1# show running-config logging
logging enable
logging timestamp
logging list MANAGER_ALL_SYSLOG_EVENT_LIST level critical
logging buffered errors
logging FMC MANAGER_ALL_SYSLOG_EVENT_LIST
logging device-id hostname
logging permit-hostdown
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
```

FTD CLI 명령

```
FTD1# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Timezone: disabled
    Logging Format: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level errors, 45 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: hostname "FTD1"
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_ALL_SYSLOG_EVENT_LIST, 45 messages logged
```

FTD CLI 명령

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.