XDR 장치 인사이트 및 DUO 통합 문제 해결

목차

소개

이 문서에서는 통합을 구성하고 XDR Device Insights 및 Cisco DUO 통합을 트러블슈팅하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다.

- XDR
- DUO
- API에 대한 기본 지식
- Postman API 툴

사용되는 구성 요소

이 문서의 정보는 이러한 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- XDR

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

XDR Device Insights는 조직 내 장치에 대한 통합 보기를 제공하며 통합된 데이터 소스의 인벤토리를 통합합니다.

Duo는 인력을 보호하고 기업 네트워크 경계를 넘어 액세스 보안을 강화하여 모든 장치 및 위치에서 모든 인증 시도의 데이터를 보호합니다. Duo를 사용하면 스냅에서 ID를 확인하고, 관리되는 장치와

관리되지 않는 장치의 상태를 모니터링하고, 비즈니스에 맞는 적응형 보안 정책을 설정하고, 장치 에이전트 없이 안전한 원격 액세스를 제공하며, 안전하고 사용하기 편리한 Single Sign-On을 빠르고 쉽게 제공할 수 있습니다.

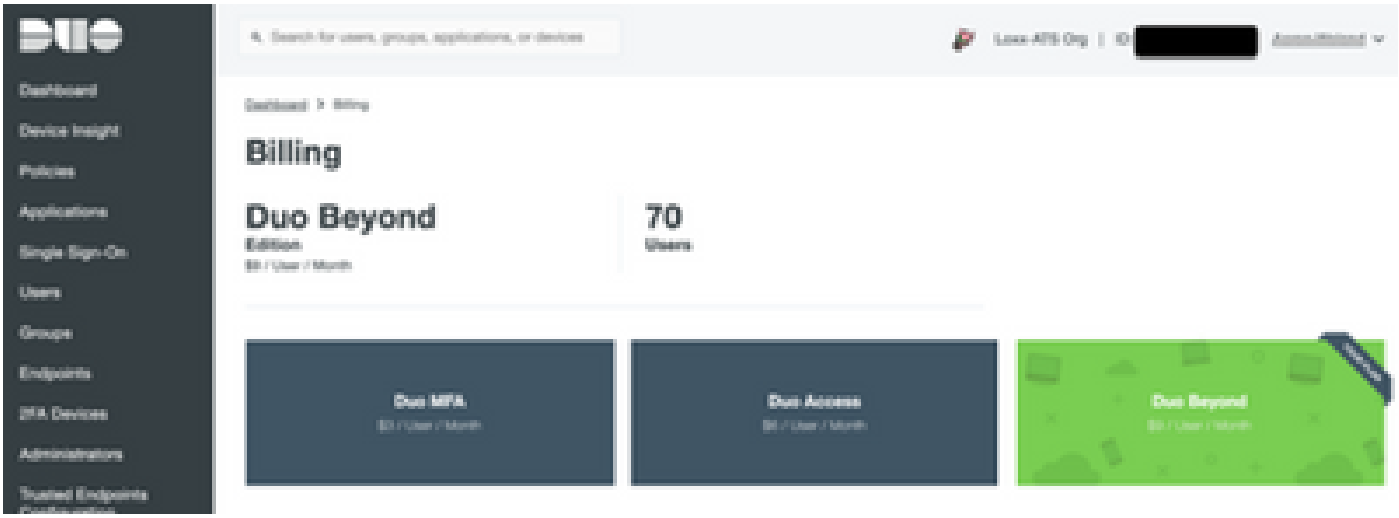
구성에 대해 자세히 알아보려면 통합 모듈 세부 정보를 검토하십시오.

문제 해결

XDR 및 DUO 통합의 일반적인 문제를 해결하려면 API의 연결 및 성능을 확인할 수 있습니다.

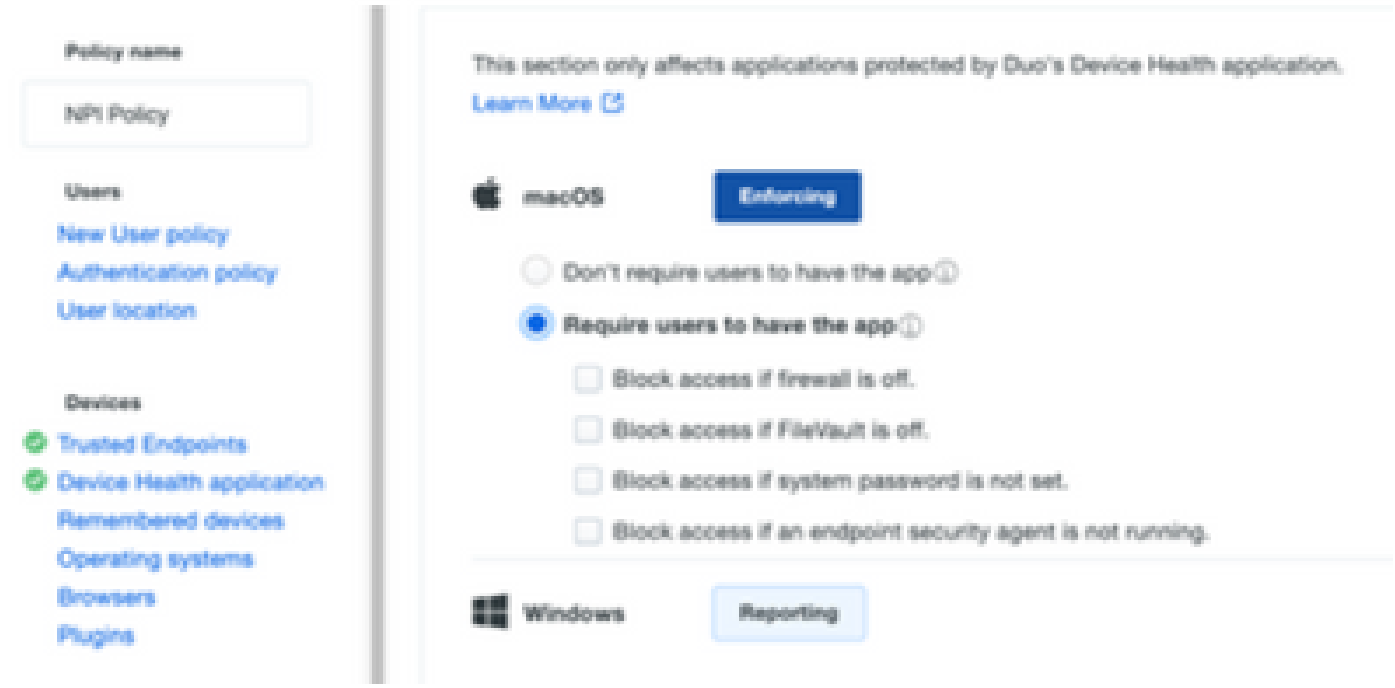
라이센스 레벨 검토

- Duo Admin(듀오 관리자) 패널에서 라이센스 확인
- 이미지에 표시된 대로 Duo Access, Duo Beyond(또는 최신 하이엔드 라이센스, MFA 전용 또는 무료)에 대해 Duo 라이센스가 부여됨

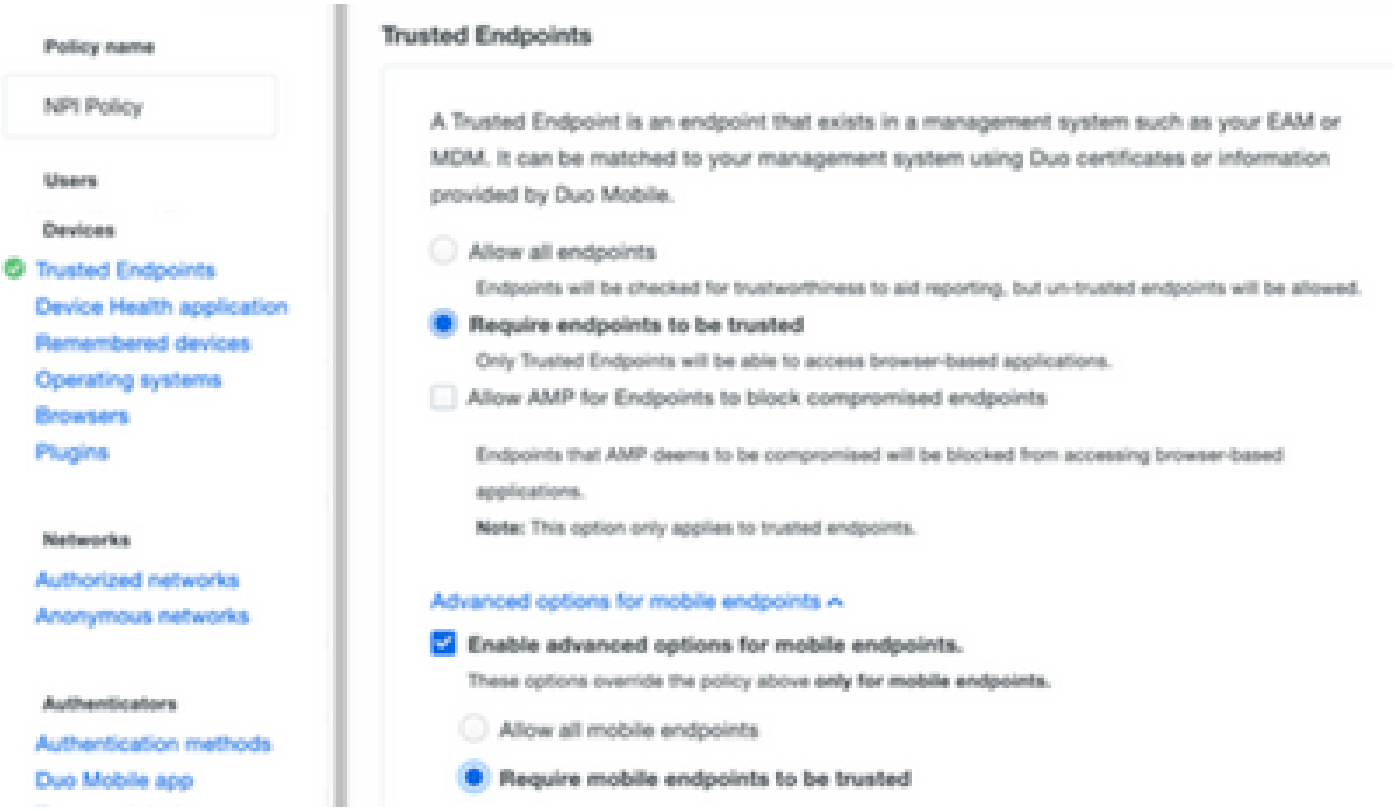


Duo의 데이터 없음

- 이미지에 표시된 대로 인증 정책에서 Duo Health Agent 데이터를 사용하는지 확인합니다



- 이미지에 표시된 대로 인증 정책에서 신뢰할 수 있는 엔드포인트를 사용하는지 확인합니다



XDR Device Insights 및 DUO를 사용한 연결 테스트

Postman Tool을 사용하여 연결을 테스트하는 동안 더 많은 시각적 출력을 얻을 수 있습니다.

참고: Postman은 Cisco에서 개발한 툴이 아닙니다. Postman 툴 기능에 대한 문의 사항은 Postman 지원에 문의하십시오.

- 오류 코드 40301 "액세스 금지"는 이미지에 표시된 대로 올바른 레벨의 라이센스가 없음을 의미합니다

- 인증 방법으로 No Auth를 선택할 수 있습니다
- 이 API 호출을 사용하여 디바이스 목록을 가져올 수 있으며(API는 페이지당 지원되는 최대 항목 수를 반환함), DUO API 페이지 매김에 대한 설명서를 찾을 수 있습니다

```
https://
```

```
/admin/v1/endpoints
```

- 첫 번째 호출에 대한 응답으로 총 개체 수가 반환됩니다(오프셋 및 제한 매개 변수를 사용하여 다음 페이지를 가져올 수 있음).

```
https://
```

```
/admin/v1/endpoints?limit=5&offset=5
```

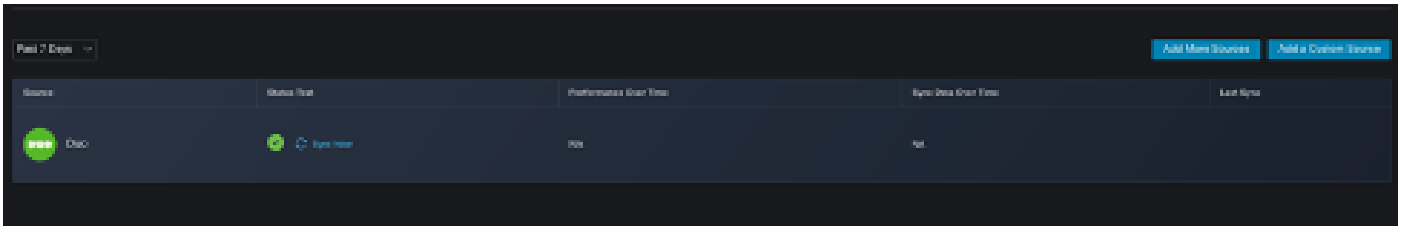
```
"metadata": {
    "total_objects": 64
},
```

```
"metadata": {
    "next_offset": 5,
    "total_objects": 64
},
```


다음을 확인합니다.

DUO가 XDR Device Insights에 소스로 추가되면 성공적인 REST API 연결 상태를 확인할 수 있습니다.

- 녹색 상태의 REST API 연결을 볼 수 있습니다
- 이미지에 표시된 것처럼 초기 전체 동기화를 트리거하려면 SYNC NOW를 누릅니다



XDR Device Insights 및 DUO 통합으로 문제가 지속되는 경우 브라우저에서 HAR 로그를 수집하고 TAC 지원에 문의하여 더 심층적인 분석을 수행하십시오.

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.