# XDR 장치 인사이트 및 Umbrella 통합 문제 해결

## 목차



## 소개

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

## 사전 요구 사항

### 요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다.

- XDR
- Umbrella
- 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.

Umbrella는 현재 위협에 대비한 공격자 인프라를 자동으로 찾아내고 악의적인 요청이 조직의 네트워크 또는 엔드포인트에 도달하기 전에 미리 차단합니다. 통합을 통해 악성코드 감염을 더 일찍 차

단하고, 이미 감염된 디바이스를 더 빨리 식별하며, 데이터 유출을 방지할 수 있습니다. 이 통합으로 모든 위치와 사용자의 인터넷 활동에 대한 완벽한 가시성을 확보할 수 있으며, 두 번 클릭 응답을 통해 신속하게 도메인을 차단할 수 있습니다. 여러 Umbrella 기능이 지원되며 Umbrella 플랫폼에서 생성된 API 키를 통해 연결됩니다.

구성에 대해 자세히 알아보려면 통합 모듈 세부 정보를 검토하십시오.

# 문제 해결

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

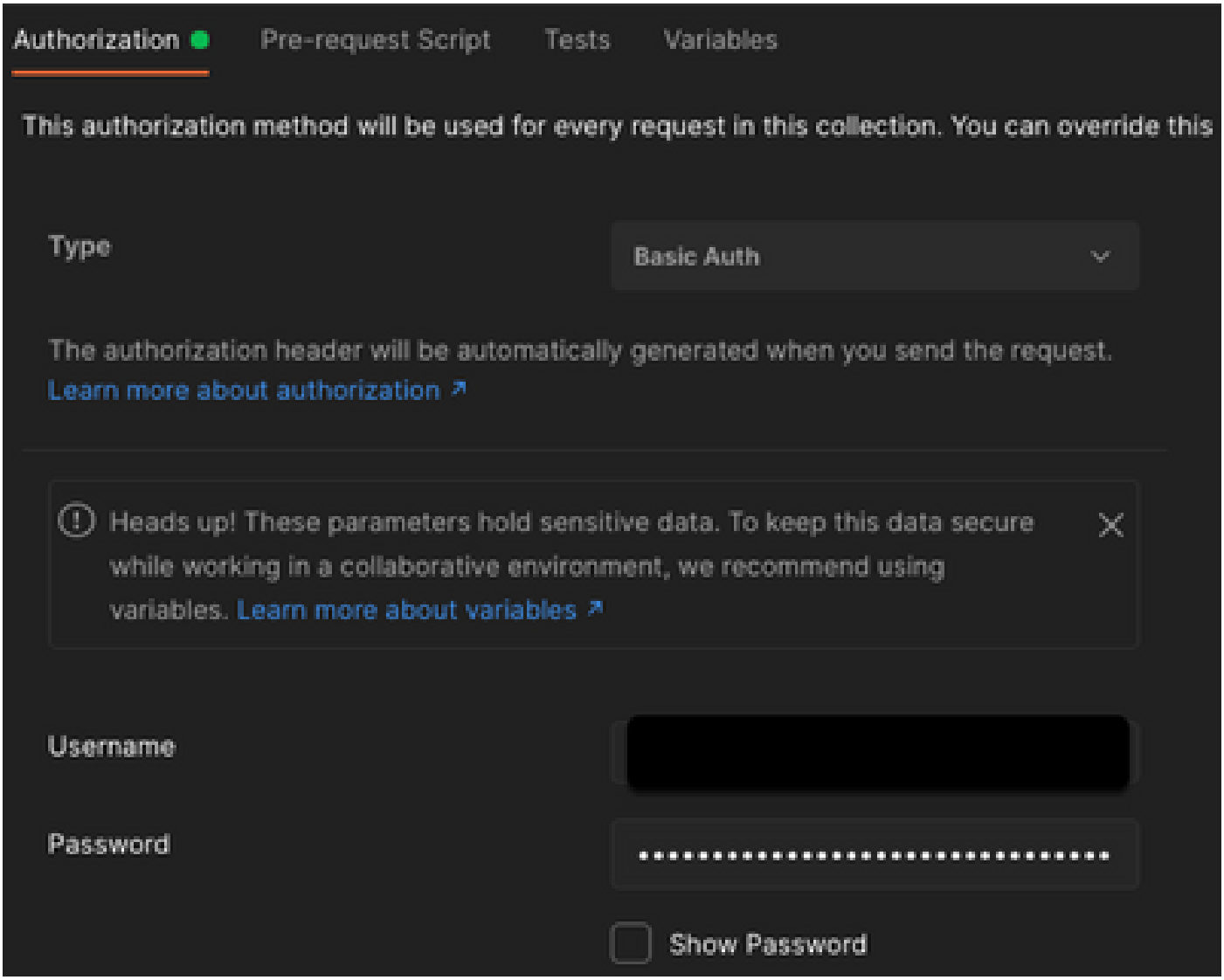
## XDR Device Insights 및 Umbrella를 사용한 연결 테스트

1단계. 이미지에 표시된 대로 Basic Authas를 권한 부여 방법으로 선택할 수 있습니다.

---

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

---



2단계. 이 API 호출을 사용하여 테로밍 컴퓨터를 가져올 수 있습니다(기본 페이지 제한은 100개 항목).

```
https://management.api.umbrella.com/v1/organizations/
```

```
        /roamingcomputers
```

3단계. 첫 번째 호출에 대한 응답으로 총 개체 수가 반환됩니다. 제한 및 페이지 매개 변수를 사용하여 다음 페이지를 가져올 수 있습니다.

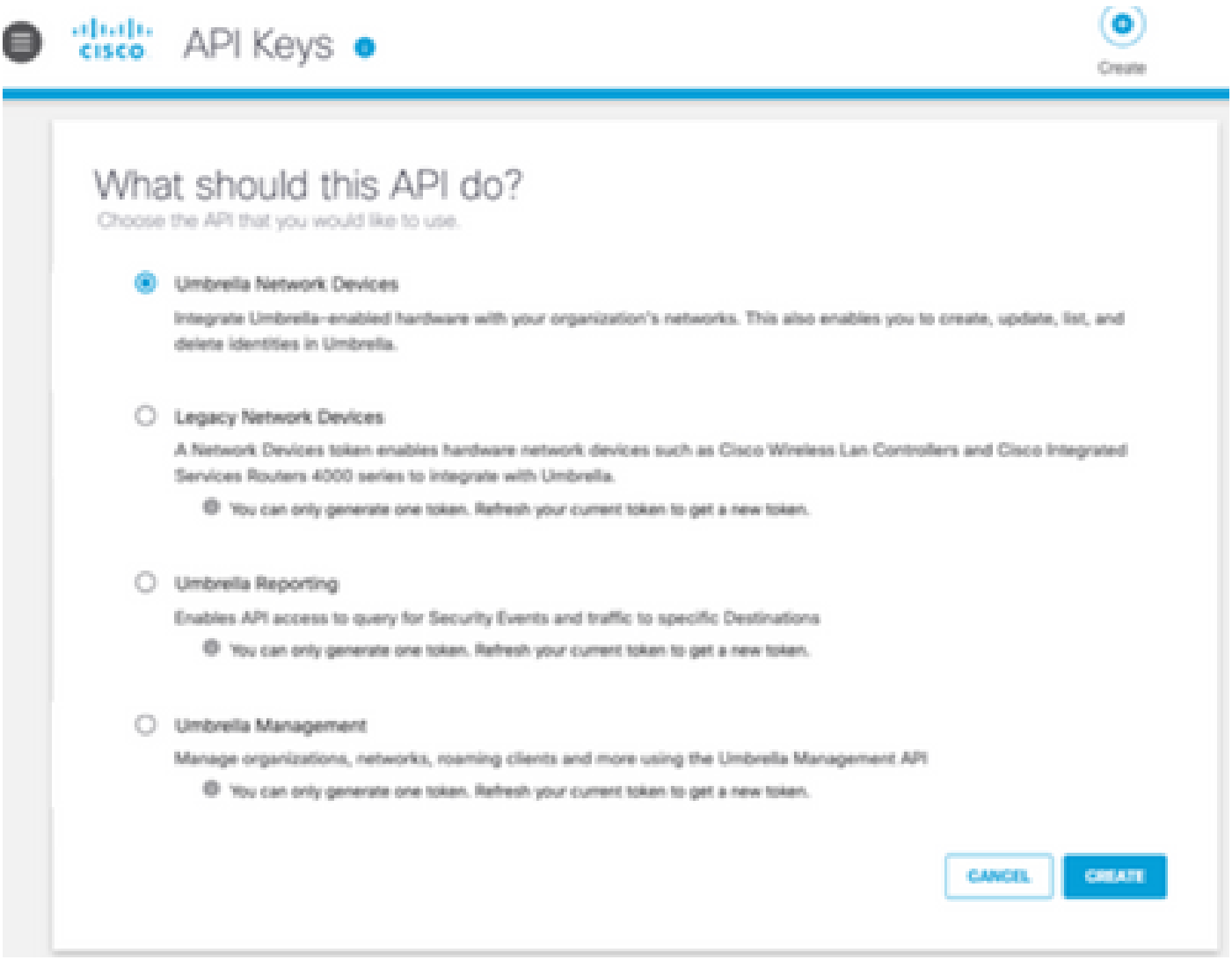
```
https://management.api.umbrella.com/v1/organizations/
```

```
        /roamingcomputers?limit=5&page=2
```

## 잘못된 키

XDR Device Insights는 XDR과 동일한 키를 사용하지 않으므로 그림과 같이 Umbrella API 키로 구성된 키가 올바른지 확인하고 확인해야 합니다.

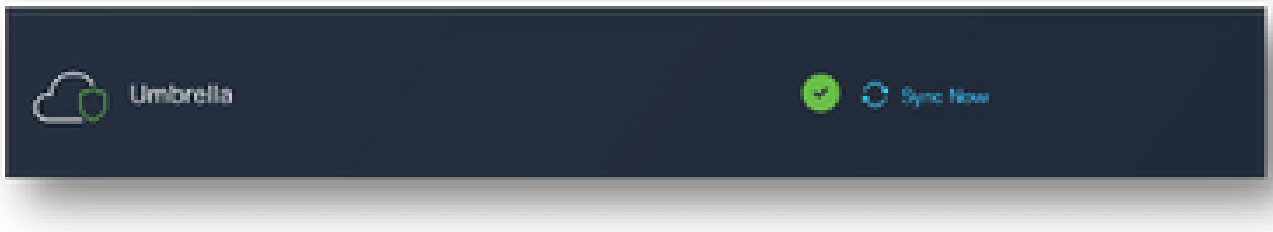
- Umbrella Network Devices(Umbrella 네트워크 디바이스): 어떤 DNS 정책을 학습하는 데 사용되는 API
- Umbrella Management: 엔드포인트를 학습하는 데 사용되는 API




## 다음을 확인합니다.

Umbrella가 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 클릭합니다




Device Insights 및 Umbrella 통합과 관련하여 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.