장치 인사이트 및 보안 엔드포인트 통합 문제 해결

목차

소개

이 문서에서는 통합을 구성하고 Device Insights 및 Secure Endpoint 통합을 트러블슈팅하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

SecureX Device Insights는 조직 내 장치에 대한 통합 보기를 제공하며 Secure Endpoint와 같은 통합 데이터 소스의 인벤토리를 통합합니다.

Device Insights를 사용하면 모든 소스의 정보가 통합되고 SecureX 내의 디바이스 인사이트에 표시

되므로 더 간단하게 모든 디바이스 정보를 전체적으로 볼 수 있으며 데이터 소스 포트폴리오 전체에서 디바이스를 더 효율적으로 조사할 수 있습니다.

활성화되면 디바이스 인사이트는 SecureX와 통합된 모듈에서 인벤토리 및 디바이스 데이터를 자동으로 가져올 준비가 되었습니다. 따라서 이미 SecureX에 통합된 모듈이 있는 경우 이 기능을 사용하기 위해 모듈을 삭제하거나 다시 추가할 필요가 없습니다.

컨피그레이션에 대해 자세히 알아보려면 Cisco SecureX 컨피그레이션 모듈에서 자세한 내용을 검토하십시오.

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

Secure Endpoint Module 추가

- 모듈을 활성화하는 사용자는 제품을 통합할 수 있는 관리자 권한이 있어야 합니다.

  참고: 새 소스를 통합할 경우 인벤토리에 보고하는 디바이스를 보려면 수동으로 동기화하거나 자동 동기화가 수행될 때까지 기다려야 합니다.

연결 확인

API 연결을 허용하려면 사용자 환경에서 다음 FQDN이 허용되어야 합니다.

- api.amp.cisco.com
- api.apjc.amp.cisco.com
- api.eu.amp.cisco.com

연결을 테스트할 사용자 Postman

https://<AMP API 지역별 FQDN>/v1/computers

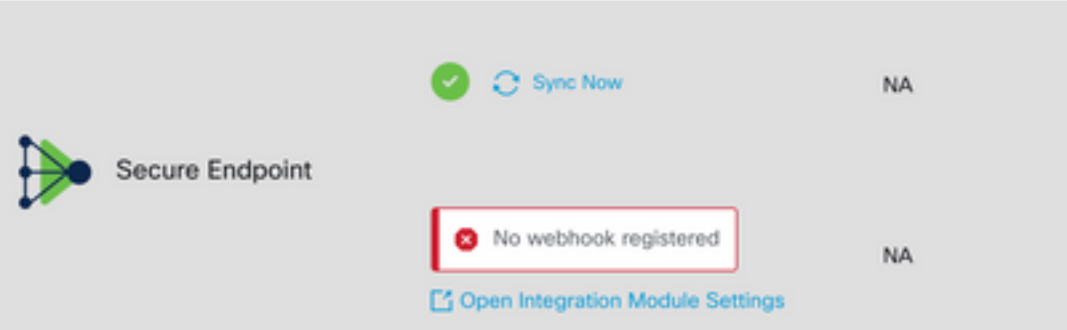
https://< AMP API 지역별 FQDN>/v1/computers/< 커넥터 GUID>

참고: 보안 엔드포인트는 기본 인증을 권한 부여 방법으로 사용합니다.

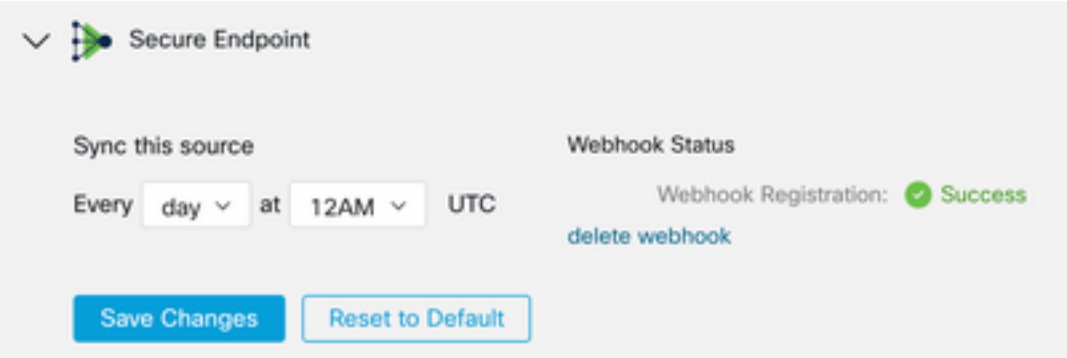
디바이스 번호 불일치

- Device Insights는 지난 90일의 정보를 저장하지만 Secure Endpoint는 30일의 정보를 저장합니다. 디바이스 수가 일치하지 않으면 관련된 컴퓨터의 마지막 표시에서 90일을 초과하지 않는지 확인합니다.
- Secure Endpoint 콘솔에 두 콘솔 모두에서 불일치를 유발하는 중복 커넥터가 없는지 확인합니다.

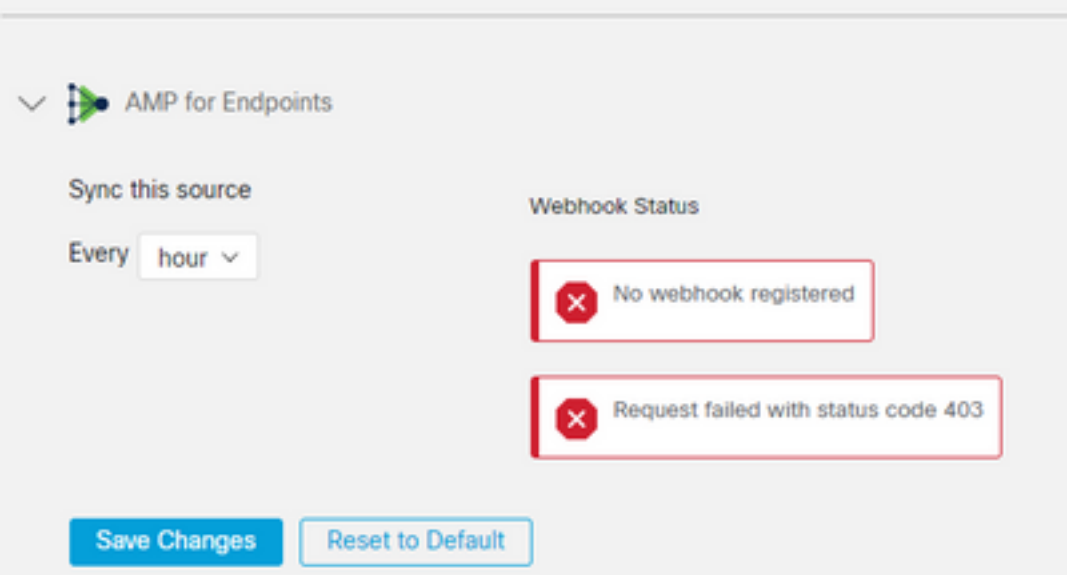
시나리오 1. 등록된 Webhook 없음



Source Setting(소스 설정)으로 이동한 다음 Register Webhook(Webhook 등록) 버튼을 클릭합니다. 요청이 수행되면 Webhook 상태가 이미지에 표시된 것처럼 표시됩니다.



시나리오 2. HTTP 오류.



400 - 잘못된 요청

401 - 무단

403 - 금지

404 - 메서드가 허용되지 않음

HTTP 오류의 경우 구성된 API 자격 증명을 검토하고, 수집된 정보가 SecureX의 모듈 컨피그레이션에 붙여넣은 정보와 일치하는지 확인합니다.

브라우저 문제

Device Insights에 잘못된 데이터가 표시되면 다른 브라우저 또는 개인 창에서 테스트하여 잘못되었거나 오래된 브라우저 캐시를 삭제합니다.

다중 조직 문제

Secure Endpoint 통합 모듈은 Enable 버튼을 사용합니다. 따라서 현재 하나의 Secure Endpoint 콘솔에만 Secure Endpoint를 연결할 수 있지만, 해당 조직의 관리자라면 하나의 SecureX 아래에 여러 Secure Endpoint 모듈을 연결할 수 있습니다. 다시 말해, 여러 Secure Endpoint 조직에서 Admin인 경우 하나의 SecureX 대시보드 아래에서 API 모듈을 통해 이러한 모든 조직을 연결할 수 있습니다. Secure Endpoint 콘솔이 다른 SecureX 조직에 아직 통합되지 않았는지 확인합니다.

SecureX 포털은 여러 개의 Secure Endpoint 인스턴스를 통합할 수 있지만 Secure Endpoint는 하나의 SecureX 인스턴스에만 통합할 수 있습니다.

HAR 로그

Device Insights 및 Secure Endpoint 통합과 관련하여 문제가 지속되는 경우 브라우저에서 HAR 로그를 수집하는 방법을 SecureX Console에서 HAR 로그 수집을 참조하고 TAC 지원에 문의하여 자세한 분석을 수행하세요.

관련 정보

- SecureX 로그인(설명서)
- 기술 지원 및 문서 – Cisco Systems

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.