Cisco Secure Endpoint Connector for Mac 진단 데이터 수집

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[배경 정보](#)
[지원 도구를 사용하여 진단 파일 생성](#)
[macOS Finder를 사용하여 지원 툴 실행](#)
[macOS 터미널을 사용하여 지원 툴 실행](#)
[문제 해결](#)
[디버그 모드 사용](#)
[단일 하트비트 디버그 모드 활성화](#)
[디버그 모드 비활성화](#)

소개

이 문서에서는 Cisco Secure Endpoint Mac Connector에서 사용 가능한 지원 툴 애플리케이션을 통해 진단 파일을 생성하는 데 사용되는 프로세스와 성능 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 보안 엔드포인트 Mac 커넥터
- 맥OS

사용되는 구성 요소

이 문서의 정보는 Secure Endpoint Mac 커넥터를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

보안 엔드포인트 Mac 커넥터는 Mac에 설치된 커넥터에 대한 진단 정보를 생성하기 위해 사용되는 지원 도구라는 애플리케이션을 패키지화합니다. 진단 데이터에는 다음과 같은 Mac에 대한 정보가

포함됩니다.

- 리소스 사용률(디스크, CPU 및 메모리)
- 커넥터별 로그
- 커넥터 컨피그레이션 정보

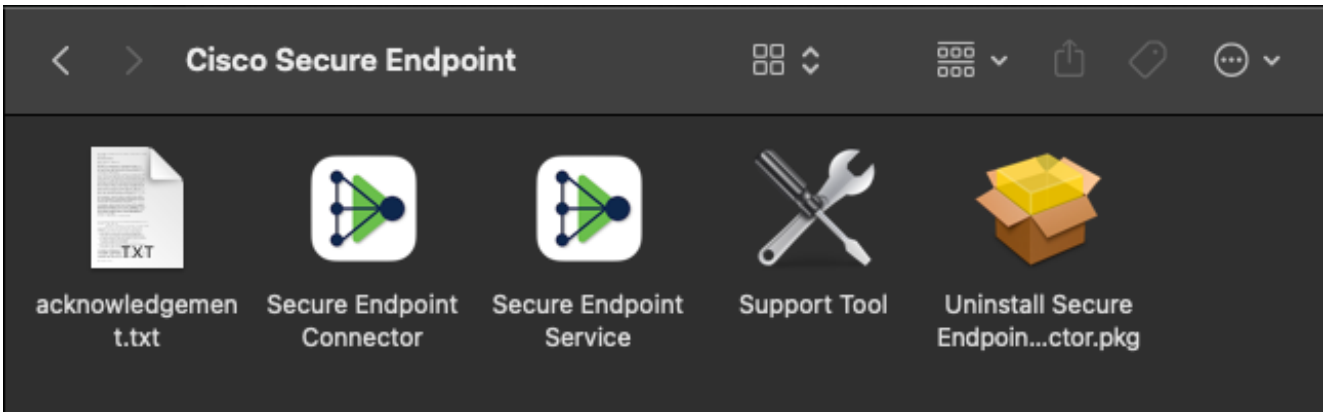
지원 도구를 사용하여 진단 파일 생성

이 섹션에서는 진단 파일을 생성하기 위해 GUI 또는 CLI에서 Support Tool 애플리케이션을 시작하는 방법에 대해 설명합니다.

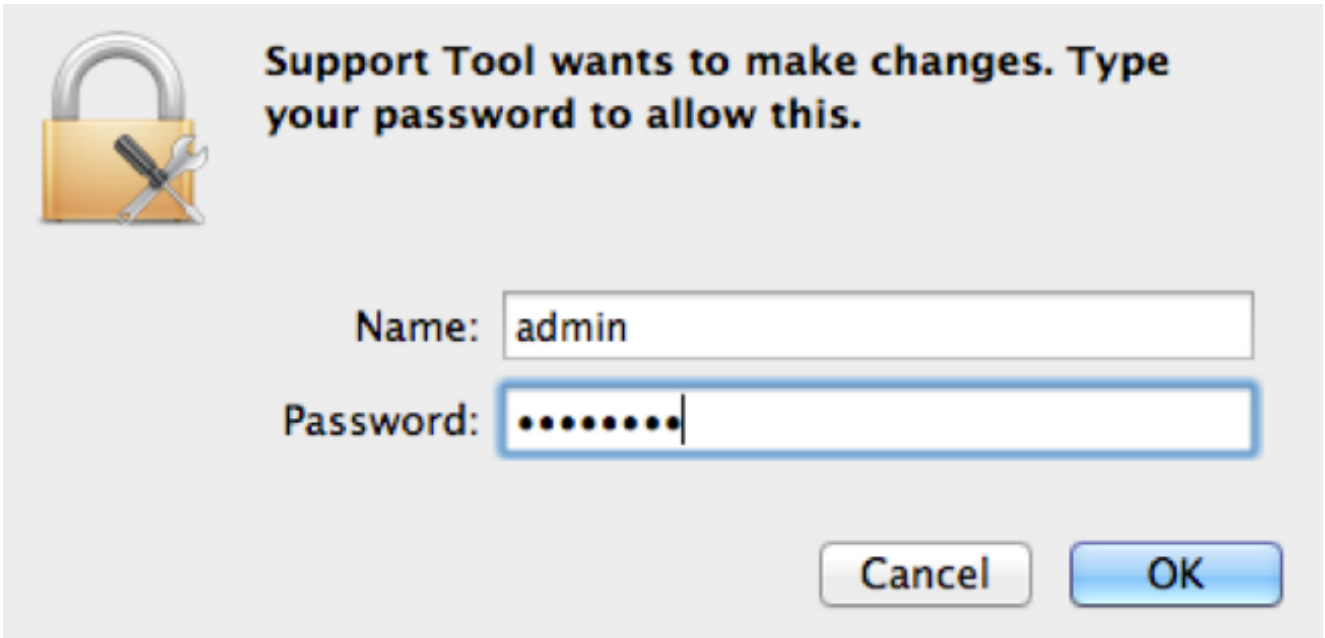
macOS Finder를 사용하여 지원 툴 실행

macOS Finder를 사용하여 Secure Endpoint Mac 커넥터 지원 도구를 실행하려면 다음 단계를 완료하십시오.

1. Applications(애플리케이션) 폴더에서 Cisco Secure Endpoint(Cisco 보안 엔드포인트) 디렉토리로 이동하고 Support Tool Launcher(지원 툴 시작 관리자)를 찾습니다.



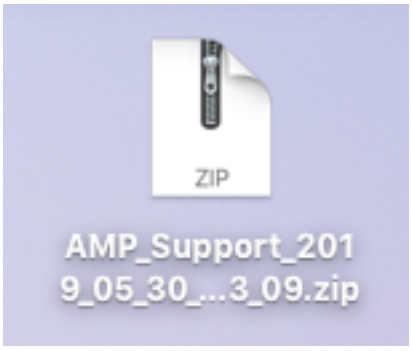
2. Support Tool 시작 관리자를 두 번 클릭하면 관리자 자격 증명을 묻는 메시지가 표시됩니다.



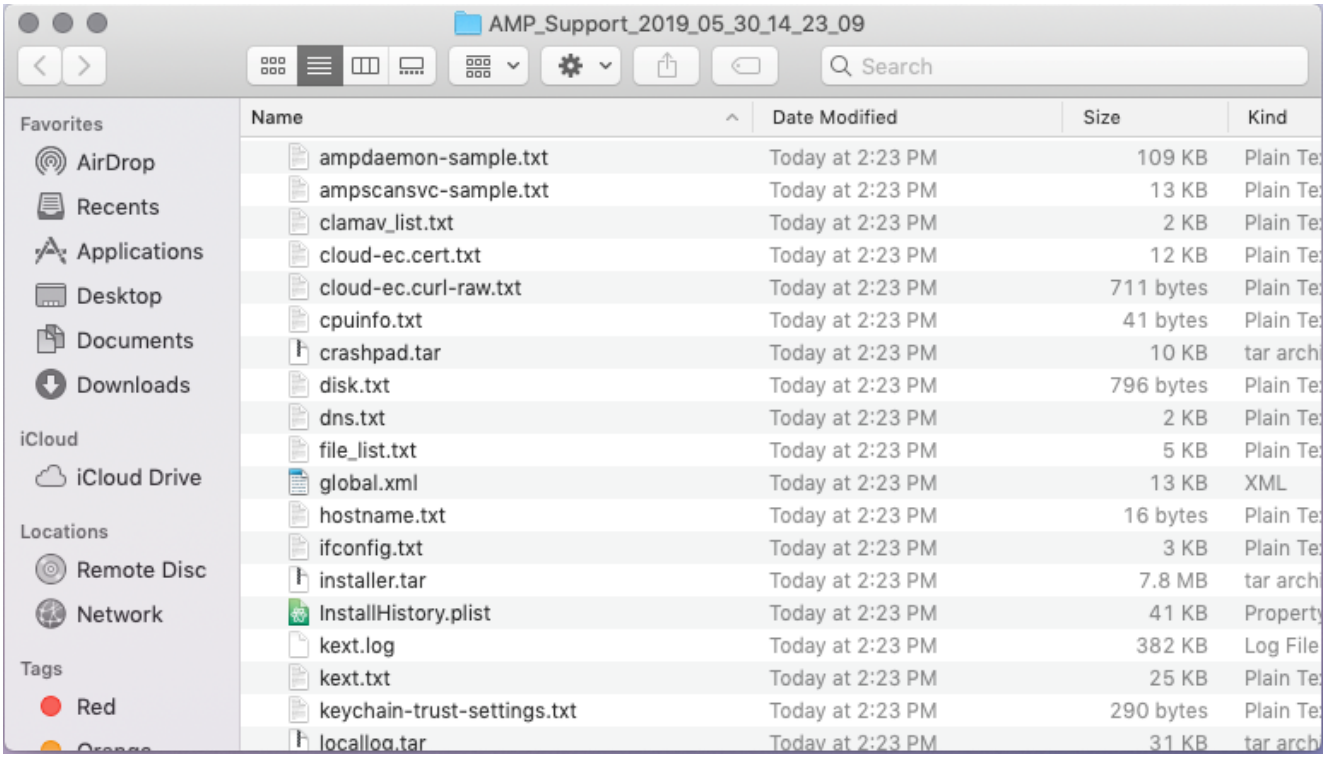
3. 자격 증명을 입력하면 Support Tool(지원 툴) 아이콘이 도크에 표시됩니다.

참고: Support Tool 애플리케이션은 백그라운드에서 실행되며 완료하는 데 다소 시간이 걸립니다(약 20-30분).

4. Support Tool 애플리케이션이 완료되면 파일이 생성되어 데스크톱에 배치됩니다.



다음은 압축되지 않은 출력의 예입니다.



5. 데이터를 분석하려면 이 파일을 Cisco 기술 지원 팀에 제공하십시오.

macOS 터미널을 사용하여 지원 툴 실행

지원 툴 시작 관리자는 다음 디렉토리에 있습니다.

```
/Library/Application Support/Cisco/AMP for Endpoints Connector/
```

Support Tool 애플리케이션을 실행하려면 다음 명령을 입력합니다.

> **참고:** 이 명령을 root로 실행해야 하므로 root로 전환하거나 sudo를 사용하여 명령의 앞에 붙여야 **합니다**.

```
root@mac# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector root@mac#
./SupportTool
```

> **참고: 이 명령은 장황하게 실행됩니다. 완료되면 진단 파일이 생성되어 바탕 화면에 배치됩니다.**

문제 해결

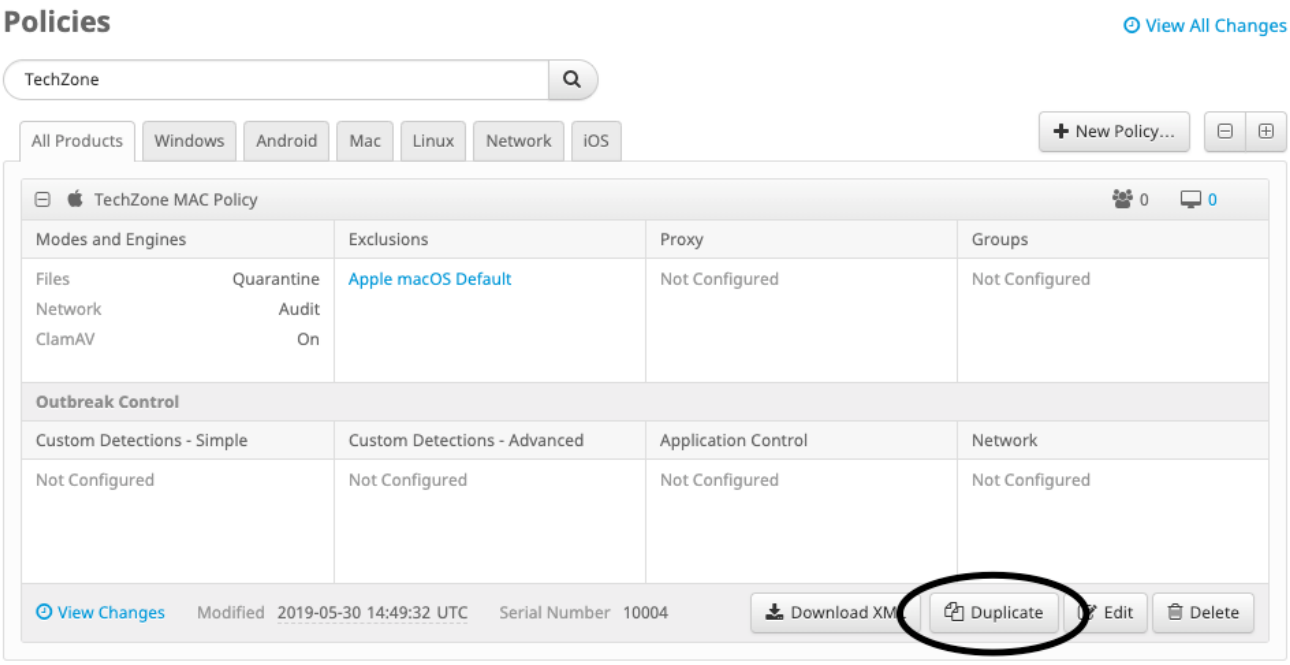
이 섹션에서는 성능 문제를 해결하기 위해 보안 엔드포인트 Mac 커넥터에서 디버그 모드를 활성화 및 비활성화하는 방법에 대해 설명합니다.

디버그 모드 사용

> **경고**: Cisco 기술 지원 엔지니어가 이 데이터를 요청하는 경우에만 디버그 모드를 활성화해야 합니다. 디버그 모드를 오랫동안 활성화하면 디스크 공간을 매우 빠르게 채울 수 있으며 과도한 파일 크기로 인해 커넥터 로그 및 트레이 로그 데이터가 지원 진단 파일에 수집되지 않을 수 있습니다.

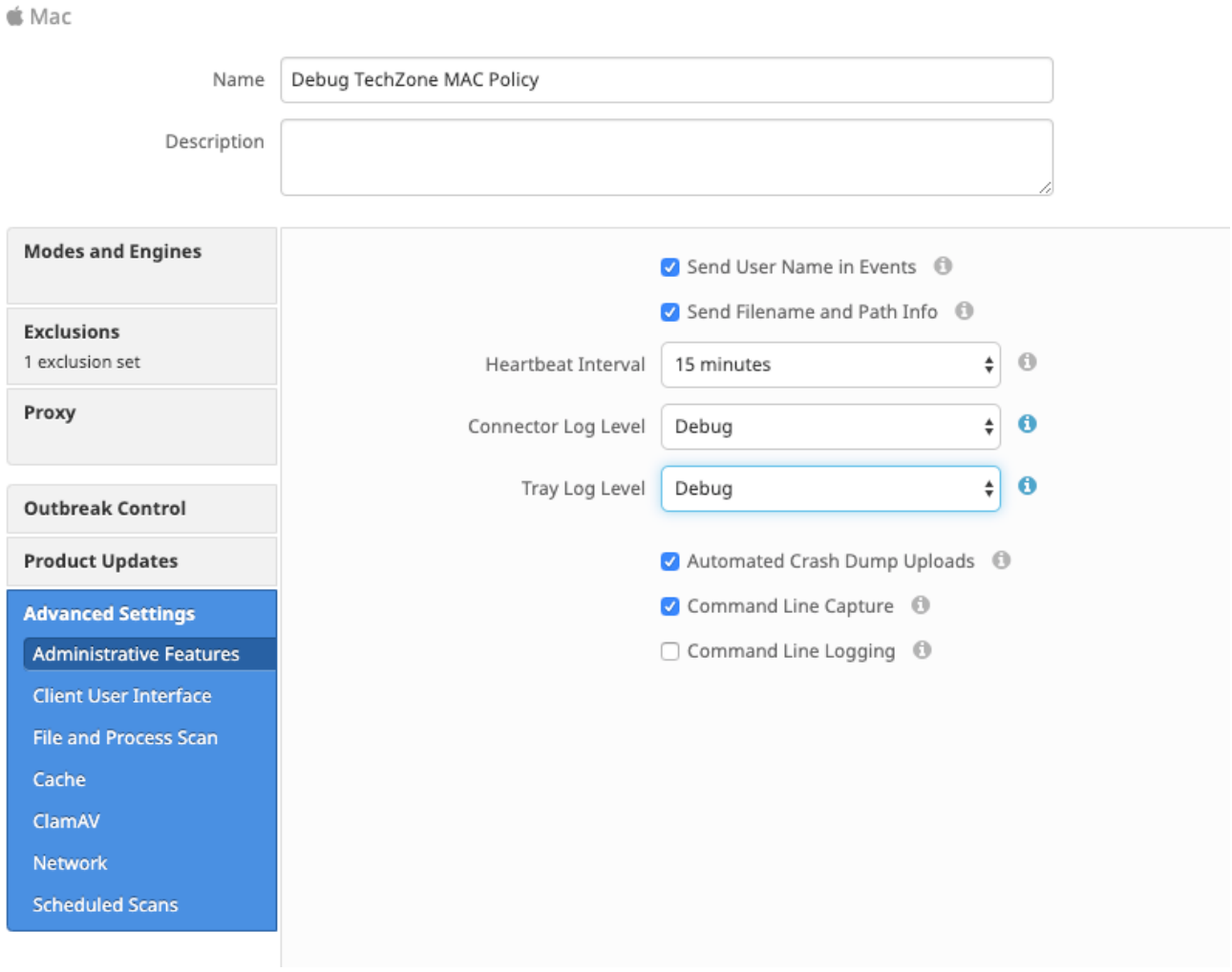
디버그 모드는 보안 엔드포인트 커넥터의 성능 문제를 해결하려는 시도에 유용합니다. 디버그 모드를 활성화하고 진단 데이터를 수집하려면 다음 단계를 완료하십시오.

1. Secure Endpoint Console에 로그인합니다.
2. **Management > Policies**로 **이동합니다**.
3. 컴퓨터에 적용된 정책을 찾고 정책 창을 확장할 정책을 클릭한 다음 **중복**. Secure Endpoint Console은 중복된 정책을 통해 업데이트됩니다.

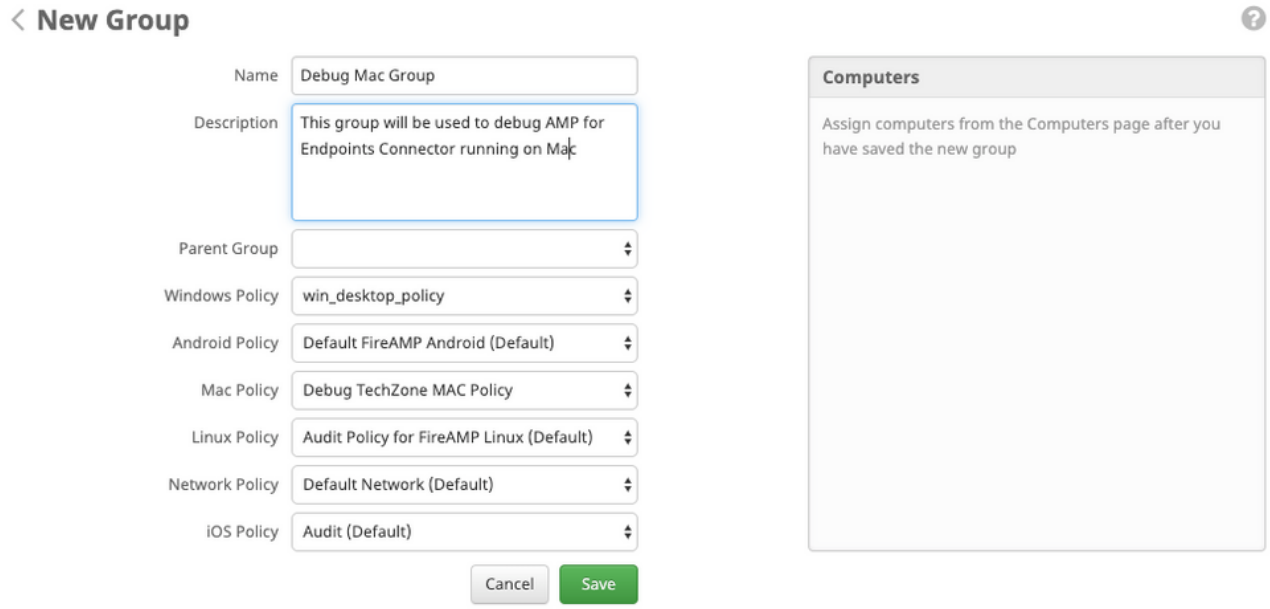


4. Duplicate policy(중복 정책) 창을 선택하고 확장한 다음 **편집** 정책의 이름을 변경합니다. 예를 들어 *디버그 TechZone MAC 정책*.

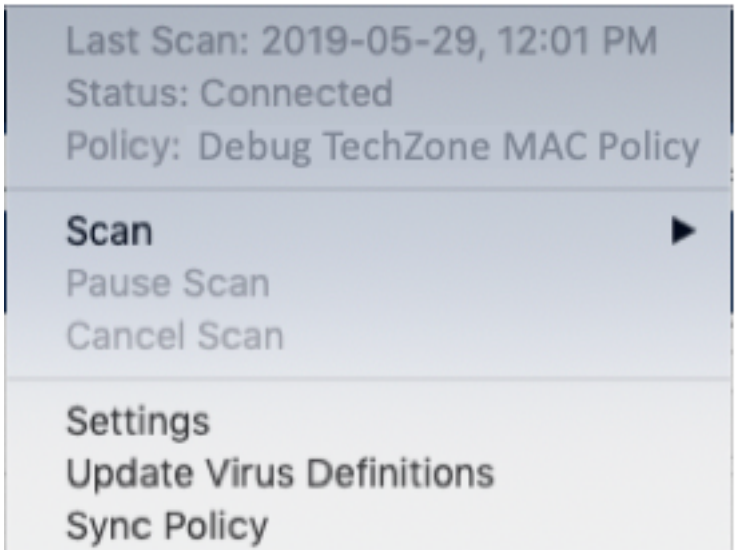
5. 클릭 **고급 설정**, 선택 **관리 기능** 사이드바에서 **디버그** connector Log Level(커넥터 로그 레벨) 및 Tray Log Level(트레이 로그 레벨) 드롭다운 메뉴 모두:



6. 다음을 클릭합니다. **저장** 버튼을 클릭하여 변경 사항을 저장합니다.
7. 탐색 **관리 > 그룹** 및 **그룹 생성** 화면 오른쪽 상단 근처에 있습니다.
8. 그룹의 이름을 입력합니다. 예를 들어 Debug TechZone *Mac Group을 사용할 수 있습니다*.



9. Mac 정책 변경 *기본 Mac 정책* 방금 생성한 중복 새 정책, 즉 **디버그 TechZone Mac 정책** 살펴보겠습니다. 클릭 **저장**.
10. 탐색 **관리 > 컴퓨터** 목록에서 컴퓨터를 확인합니다. 선택한 후 **그룹으로 이동...**.
11. 새로 만든 그룹을 **그룹 선택** 드롭다운 메뉴. 클릭 **이동** 선택한 컴퓨터를 새 그룹으로 이동합니다. 이제 Mac에 올바른 디버그 정책이 있어야 합니다. 메뉴 모음에 나타나는 보안 엔드포인트 아이콘을 선택하고 새 정책이 적용되었는지 확인할 수 있습니다.

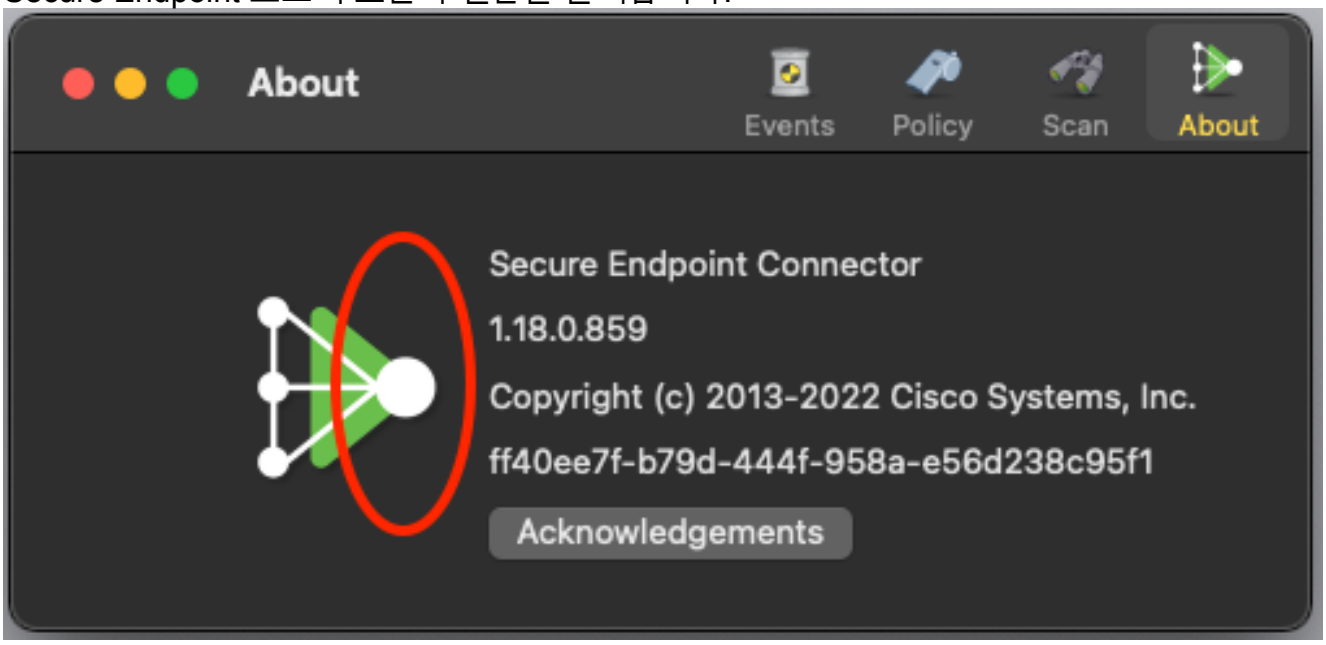


단일 하트비트 디버그 모드 활성화

이 절차는 1.0.4 커넥터 이상에서만 사용할 수 있습니다. 그러면 다음 하트비트까지 단일 커넥터를 디버그 모드로 설정할 수 있습니다. 상황에 따라, 이것은 우리의 개발자에게 충분한 정보를 제공하지만 심장 박동 길이에 따라, 전체 진단 분석을 하는 데 필요한 모든 프로세스를 포착하지 못할 위험이 있습니다. 단일 하트비트에 대해 디버그를 활성화하는 단계는 다음과 같습니다.

1. 커넥터 메뉴 모음에 액세스하고 **설정.**
2. 클릭 **대략**

3. Secure Endpoint 로고의 오른쪽 절반을 클릭합니다.



4. 올바르게 완료되면 화면 오른쪽에 다음 알림이 팝업됩니다.

다음 하트비트 이후에 디버그가 자동으로 비활성화됩니다.

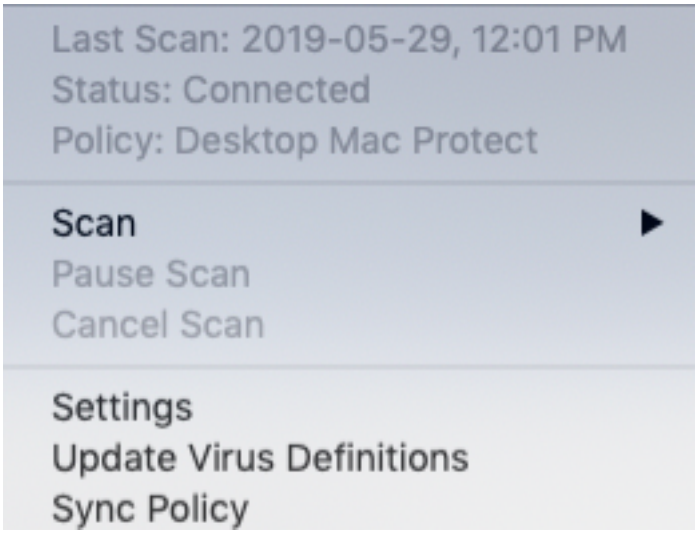
디버그 모드 비활성화

디버그 모드의 진단 데이터를 얻은 후에는 보안 엔드포인트 커넥터를 다시 일반 모드로 되돌려야 합니다. 디버그 모드를 비활성화하려면 다음 단계를 완료합니다.

1. Secure Endpoint Console에 로그인합니다.
2. **Management > Groups로 이동합니다**.

3. 디버그 모드에서 생성한 새 *그룹인* Debug TechZone Mac Group을 찾습니다.
4. Edit를 **클릭합니다**.

5. 화면의 오른쪽 위에 있는 컴퓨터 창에서 목록에서 컴퓨터를 찾습니다. 이를 선택하면 Computerspage로 이동합니다. 다시 한 번 목록에서 컴퓨터를 선택하고 그룹으로 **이동...을 클릭합니다.**.
6. 그룹 선택 드롭다운 메뉴**에서** 이전 그룹을 선택합니다. 선택한 컴퓨터를 이전 그룹으로 이동하려면 이동을 클릭합니다.
7. 메뉴 모음에서 보안 엔드포인트 아이콘을 클릭합니다. **메뉴**에서 동기화 정책을 선택합니다.
8. 이제 정책이 이전 기본값으로 반환되는지 확인합니다. 메뉴 모음에서 이것을 확인하세요. 이제 정책을 Debug TechZone *Mac* 그룹으로 변경하기 전에 사용했던 원래 정책으로 되돌렸어야 합니다.


Last Scan: 2019-05-29, 12:01 PM
Status: Connected
Policy: Desktop Mac Protect
Scan
Pause Scan
Cancel Scan
Settings
Update Virus Definitions
Sync Policy

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.