AMP for Endpoint Console에서 엔드포인트에서 디버그 활성화

목차

소개

이 문서에서는 Cisco Secure Endpoint Console에서 엔드포인트에서 디버그를 활성화하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

시작하기 전에 다음을 확인하십시오.

- Cisco Secure Endpoint for Endpoints 콘솔에 대한 관리 액세스
- 디버깅할 엔드포인트가 Cisco Secure Endpoint에 이미 등록되어 있습니다

사용되는 구성 요소

문서에서 사용되는 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Secure Endpoint Console 버전 5.4.20240718
- Cisco Secure Endpoint Connector 6.3.7 이상
- Microsoft Windows 운영 체제

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

생성된 진단 데이터는 추가 분석을 위해 Cisco TAC(Technical Assistance Center)에 제공될 수 있습니다.

진단 데이터에는 다음과 같은 정보가 포함됩니다.

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

문제

이 시나리오 중 하나를 수행하는 동안 Cisco Secure Endpoint Console에서 엔드포인트에서 디버그를 활성화해야 합니다.

시나리오 1: 디바이스를 재부팅하는 경우 IP 트레이 인터페이스에서 디버그 모드를 활성화하십시오. 그렇지 않으면 재부팅해도 해결되지 않습니다. 부팅 디버그 로그가 필요한 경우 Secure Endpoint 콘솔의 정책 컨피그레이션에서 디버그 모드를 활성화할 수 있습니다.

시나리오 2: 디바이스에서 Cisco Secure Endpoint Connector의 성능 문제가 발생하는 경우 디버그 모드를 활성화하면 분석을 위해 세부 로그를 수집하는 데 도움이 될 수 있습니다.

시나리오 3: Secure Endpoint Connector로 특정 문제를 해결할 때 자세한 로그를 통해 문제의 근본 원인을 파악할 수 있습니다.

구성

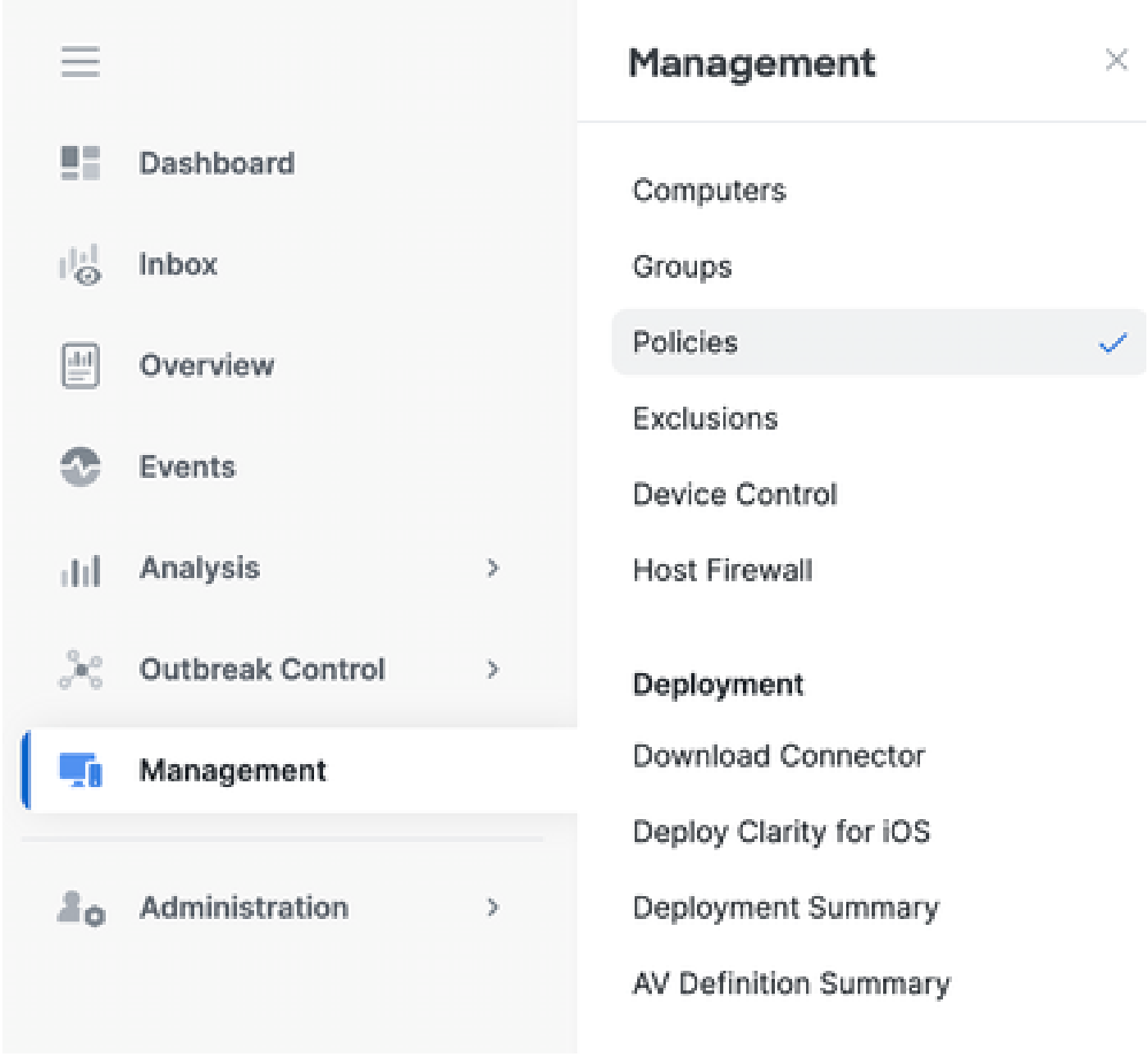
Secure Endpoint Console(보안 엔드포인트 콘솔)을 통해 지정된 엔드포인트에서 성공적으로 디버그 모드를 활성화하려면 다음 단계를 완료합니다.

1단계: 디버깅으로 이동할 엔드포인트 식별

1. Cisco Secure Endpoint Console에 로그인합니다. 기본 대시보드에서 Management 섹션으로 이동합니다.
2. Management(관리) > Computers(컴퓨터)로 이동합니다.
3. 디버그 모드가 필요한 엔드포인트를 식별하고 기록합니다.

2단계: 기존 정책 복제

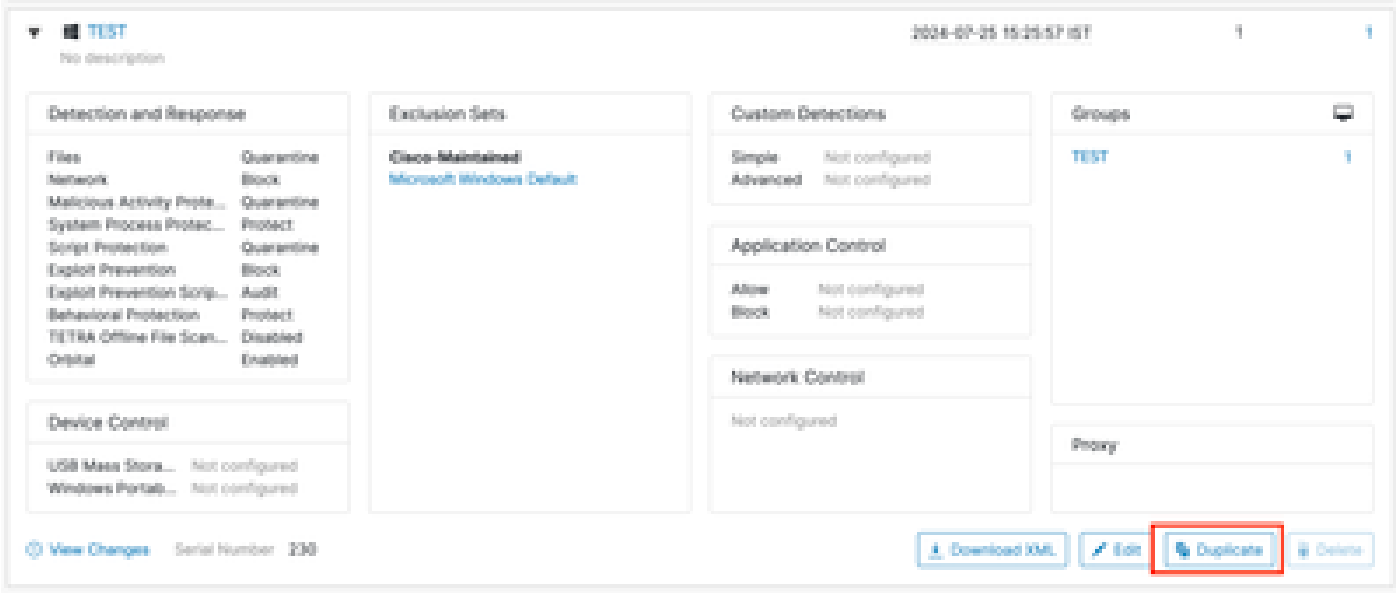
1. Management > Policies로 이동합니다.



2. 식별된 엔드포인트에 현재 적용된 정책을 찾습니다.

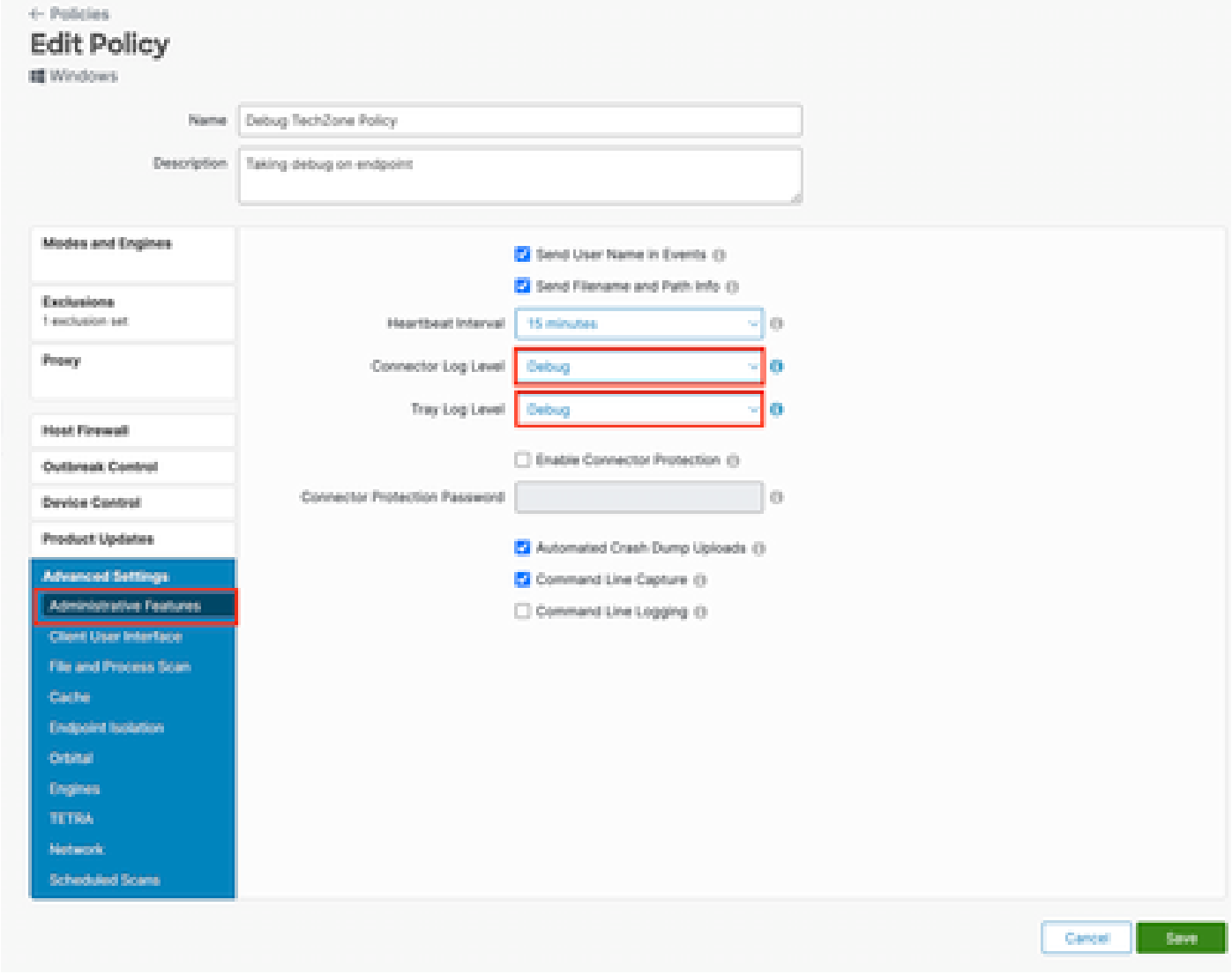
3. 정책을 눌러 정책 창을 확장합니다.

4. 기존 정책의 사본을 생성하려면 복제를 클릭합니다.



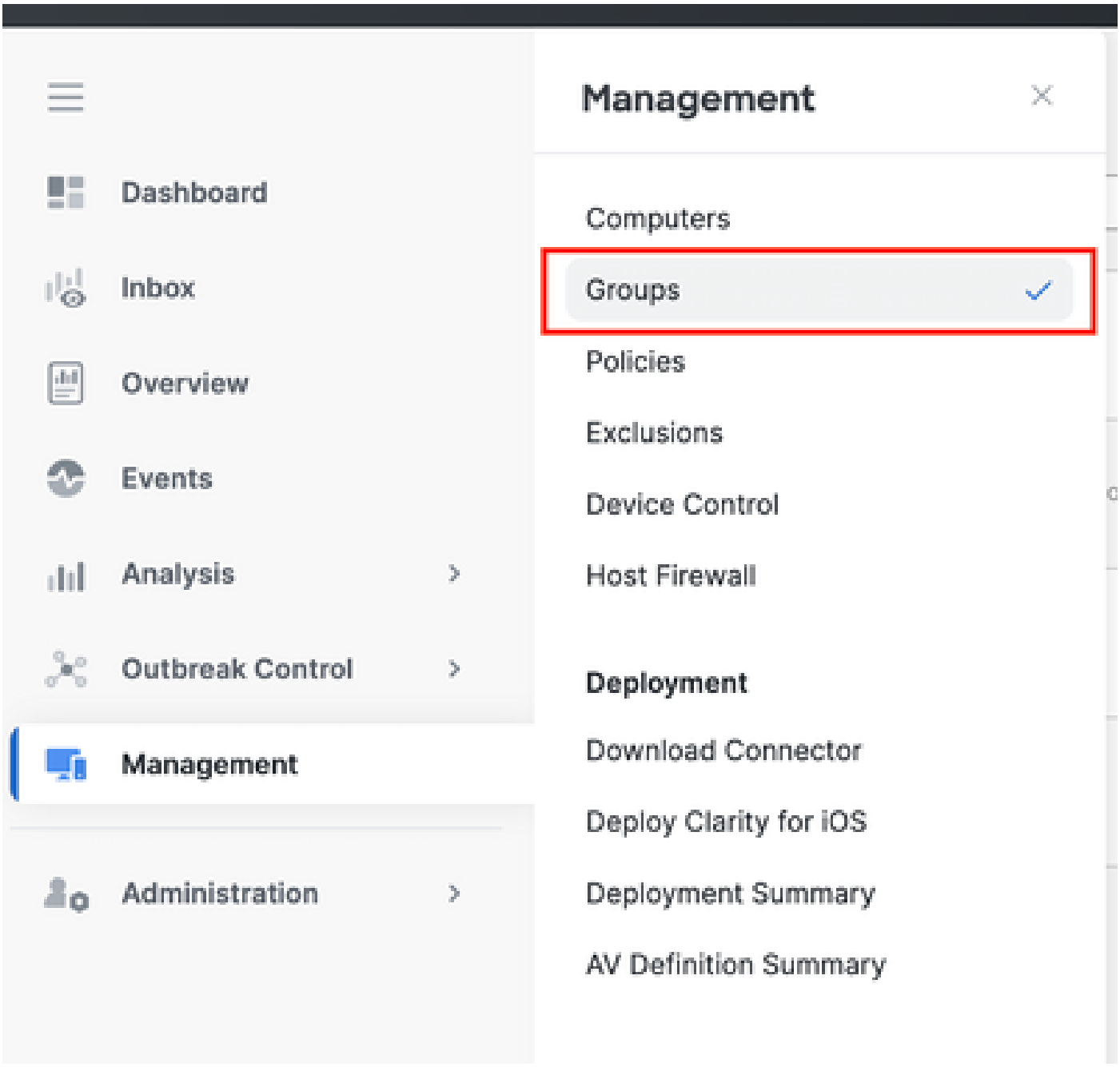
3단계: 이 정책을 디버깅할 로그 레벨 구성

1. 중복된 정책 창을 선택하고 확장합니다.
2. Edit(편집)를 클릭하고 정책의 이름을 변경합니다(예: Debug TechZone Policy).
3. Advanced Settings(고급 설정)를 클릭합니다.
4. 사이드바에서 Administrative Features를 선택합니다.
5. Connector Log Level(커넥터 로그 레벨)과 Tray Log Level(트레이 로그 레벨)을 모두 Debug(디버그)로 설정합니다.
6. Save(저장)를 클릭하여 변경 사항을 저장합니다.



4단계: 새 그룹 생성 및 해당 새 정책 링크

1. Management(관리) > Groups(그룹)로 이동합니다.

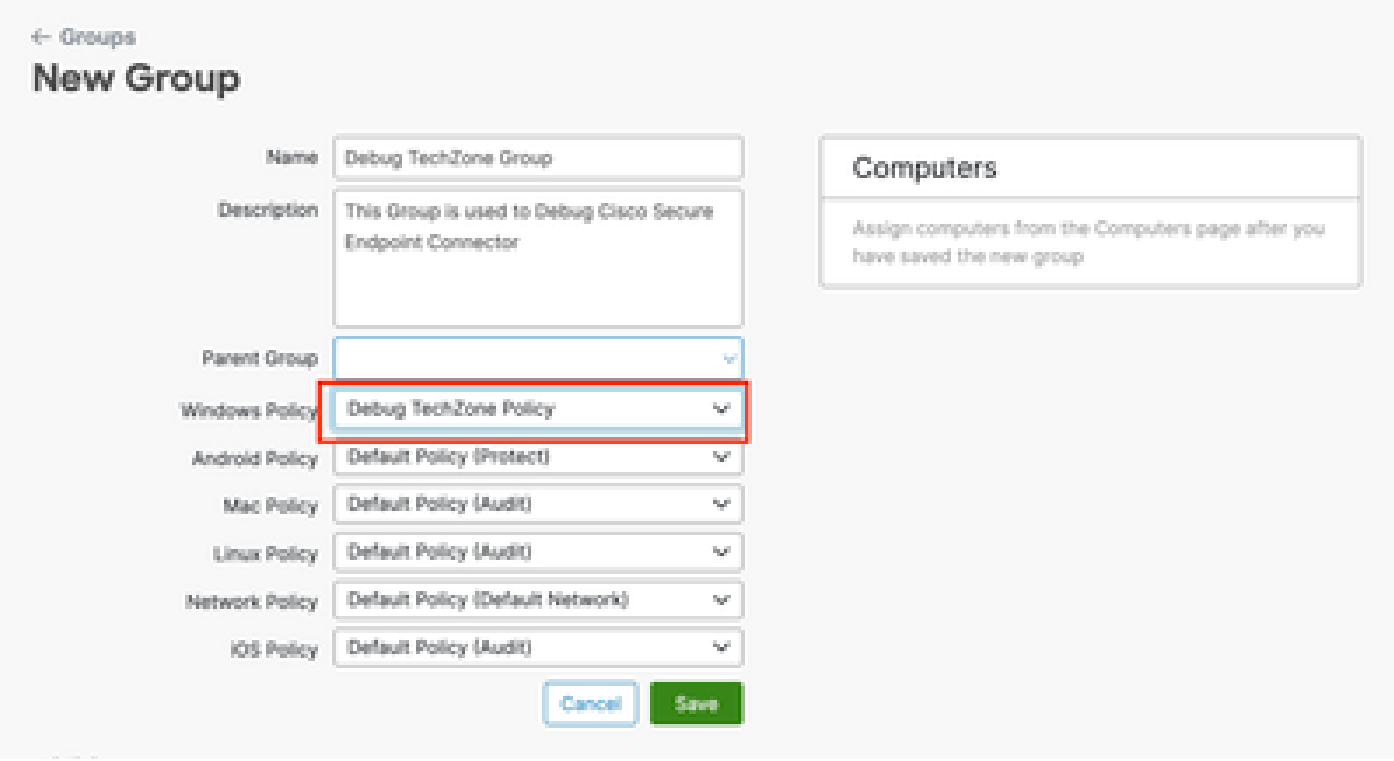


2. 화면 오른쪽 상단에 있는 그룹 생성을 클릭합니다.

3. 그룹의 이름을 입력합니다(예: Debug TechZone Group).

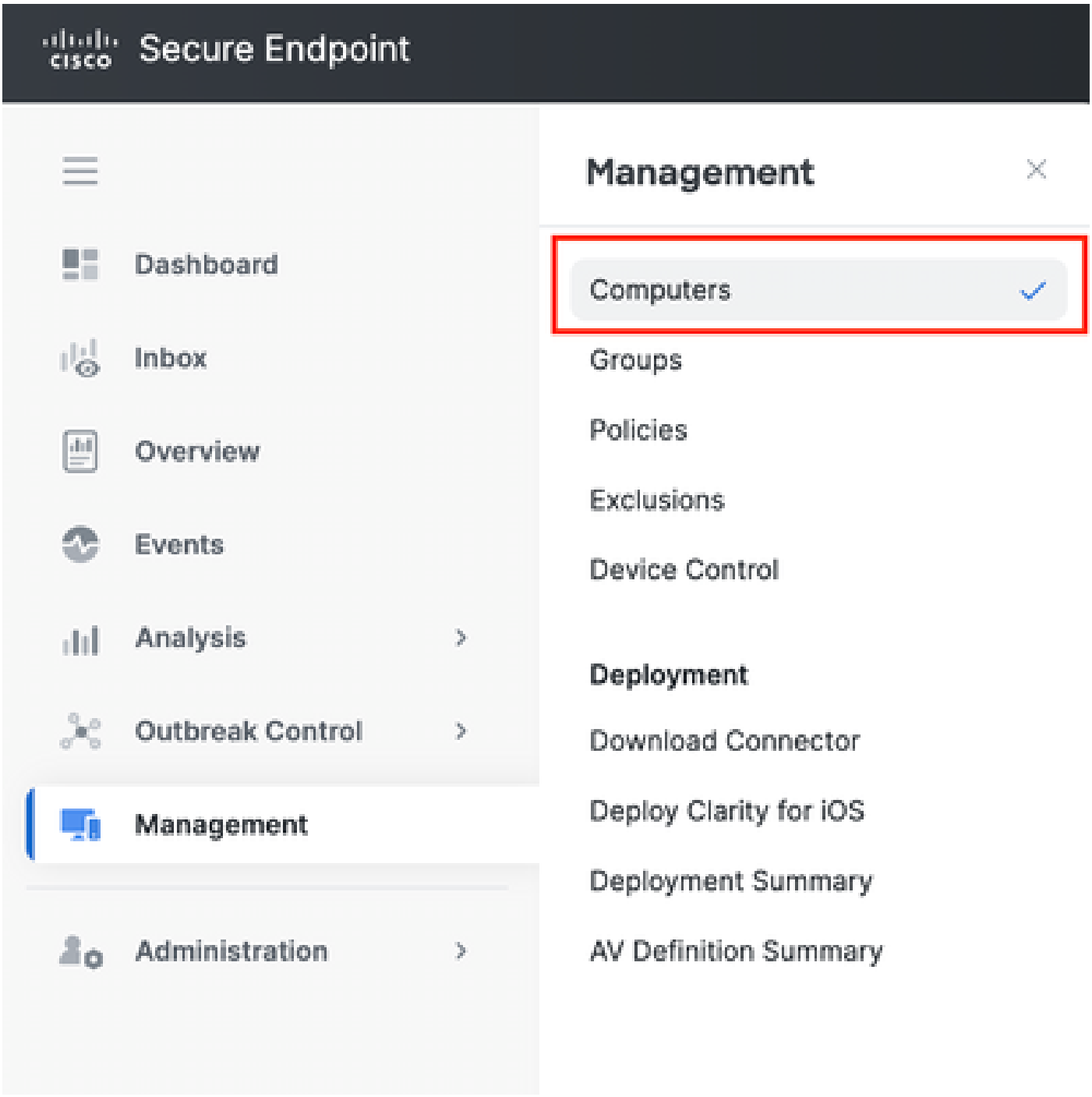
4. 정책을 기본값에서 새로 생성된 디버그 정책으로 변경합니다.

5. 저장을 클릭합니다.



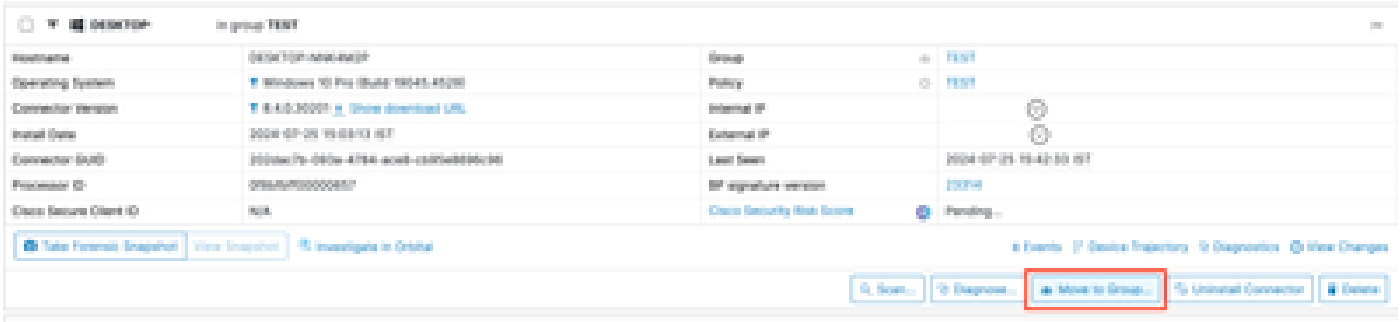
5단계: 식별된 엔드포인트를 이 새 그룹으로 이동

1. 관리 > 컴퓨터로 다시 이동합니다.



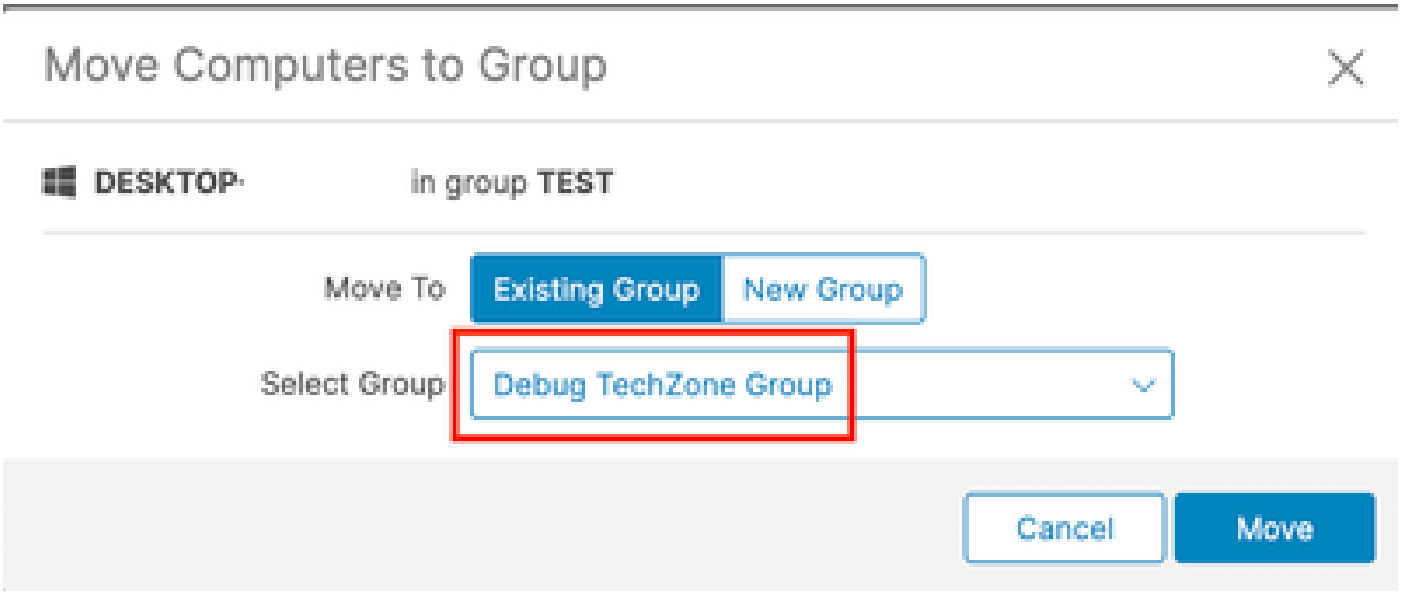
2. 목록에서 식별된 끝점을 선택합니다.

3. 그룹으로 이동을 클릭합니다.



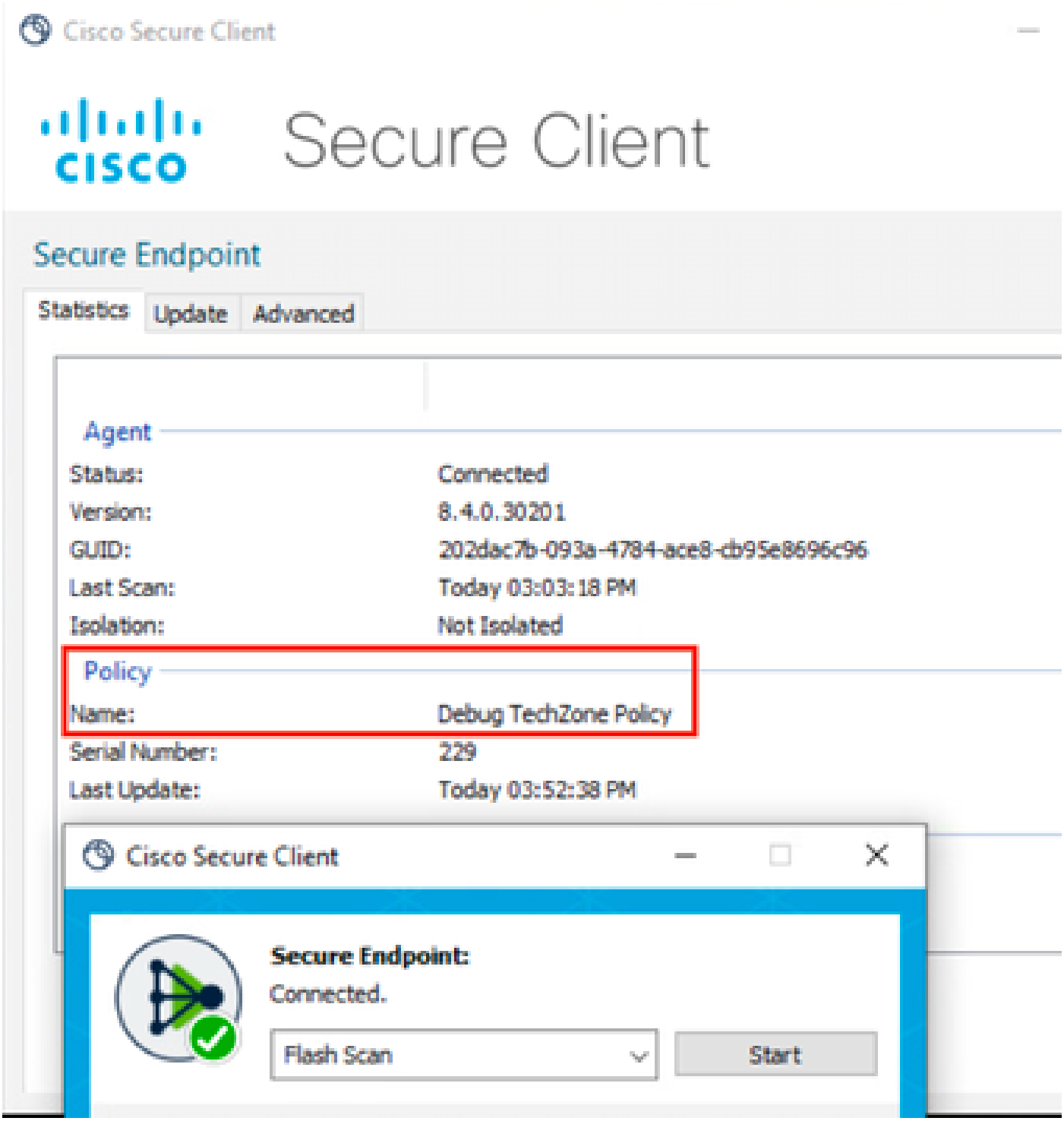
4. 그룹 선택 드롭다운 메뉴에서 새로 생성된 그룹을 선택합니다.

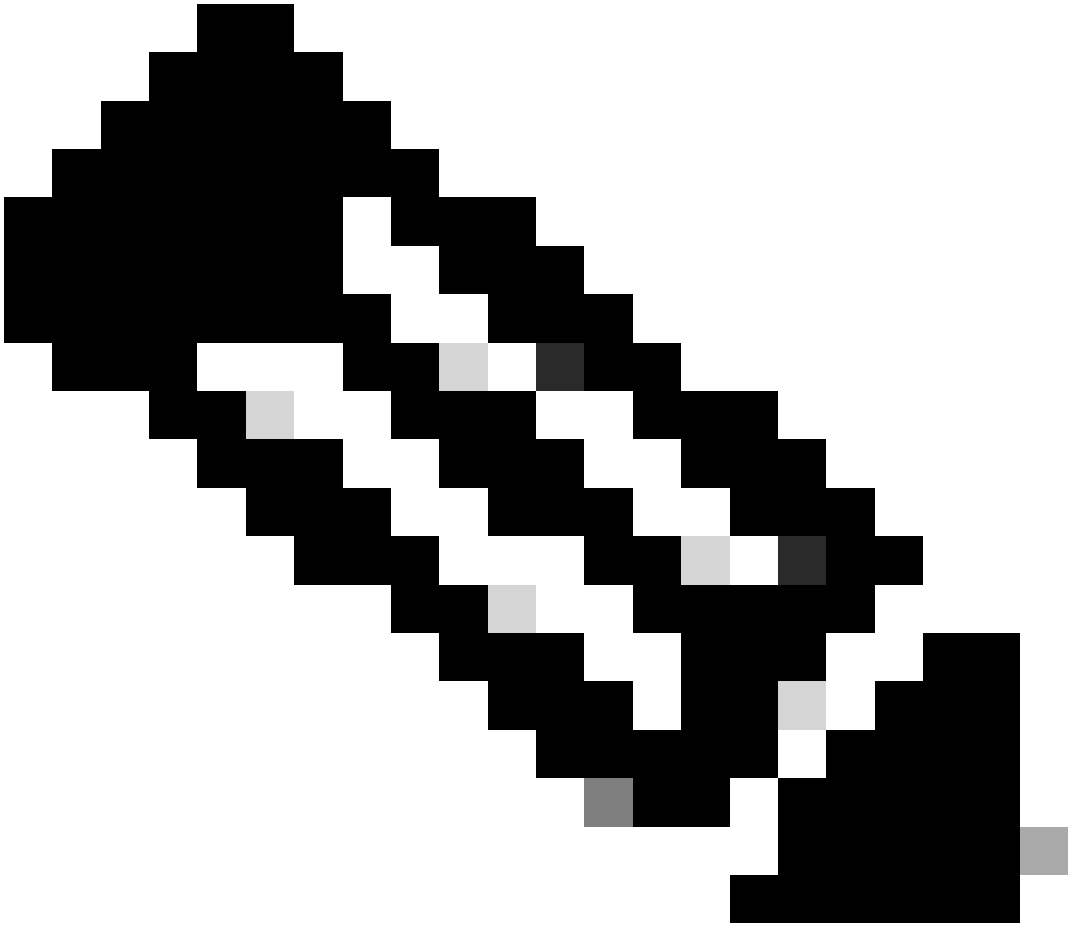
5. 선택한 끝점을 새 그룹으로 이동하려면 이동을 클릭합니다.



6단계: 컴퓨터의 페이지 및 커넥터 UI에서 엔드포인트 확인

1. 엔드포인트가 Computers(컴퓨터) 페이지의 새 그룹 아래에 나열되어 있는지 확인합니다.
2. 엔드포인트에서 Secure Endpoint connector UI를 엽니다.
3. 메뉴 모음에서 보안 엔드포인트 아이콘을 확인하여 새 디버그 정책이 적용되었는지 확인합니다.


Cisco Secure Client
Secure Client
Secure Endpoint
Statistics
Update
Advanced
Agent
Status: Connected
Version: 8.4.0.30201
GUID: 202dac7b-093a-4784-ace8-cb95e8696c96
Last Scan: Today 03:03:18 PM
Isolation: Not Isolated
Policy
Name: Debug TechZone Policy
Serial Number: 229
Last Update: Today 03:52:38 PM
Cisco Secure Client
Secure Endpoint:
Connected.
Flash Scan
Start



참고: 디버그 모드는 Cisco 기술 지원 엔지니어가 이 데이터를 요청하는 경우에만 활성화할 수 있습니다. 디버그 모드를 길게 사용하면 디스크 공간을 빠르게 채울 수 있으며 과도한 파일 크기로 인해 커넥터 로그 및 트레이 로그 데이터가 지원 진단 파일에 수집되지 않을 수 있습니다.

자세한 내용은 Cisco 지원에 문의하십시오.

Cisco 전 세계 지원 문의처

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.