AMP for Endpoints 및 Threat Grid를 WSA와 통합

목차

소개

이 문서에서는 AMP(Advanced Malware Protection) for endpoints 및 TG(Threat Grid)를 WSA(Web Security Appliance)와 통합하는 단계에 대해 설명합니다.

기고자: Uriel Montero, Yeraldin Sanchez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 엔드포인트용 AMP 액세스
- TG 프리미엄 액세스
- 파일 분석 및 파일 평판 기능 키가 포함된 WSA

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- AMP 퍼블릭 클라우드 콘솔
- WSA GUI
- TG 콘솔

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

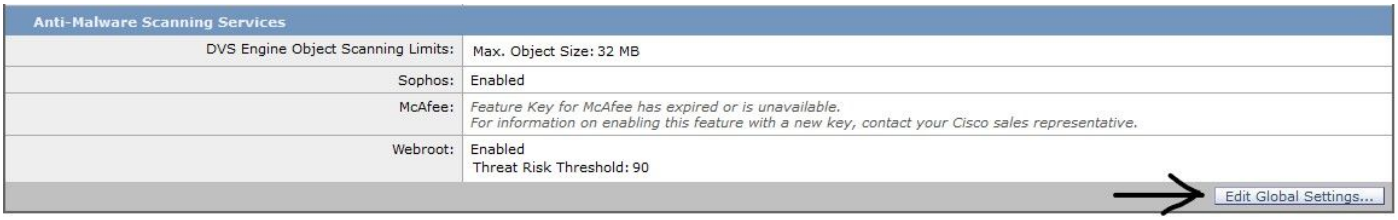
구성

WSA 콘솔에 로그인합니다.

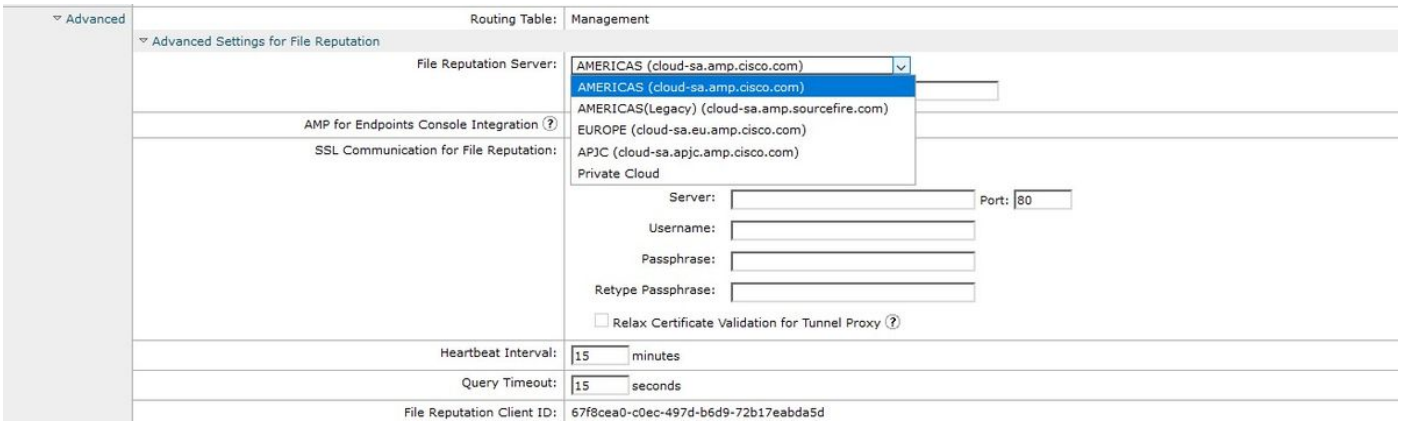
로그인한 후 **Security Services(보안 서비스) > Anti-Malware and Reputation(악성코드 차단 및 평판)으로 이동하여** 이 섹션에서 AMP 및 TG를 통합하는 옵션을 찾을 수 있습니다.

AMP 통합

Anti-Malware Scanning Services(안티멀웨어 스캐닝 서비스) 섹션에서 이미지에 표시된 대로 **Edit Global Settings(전역 설정 편집)**를 클릭합니다.

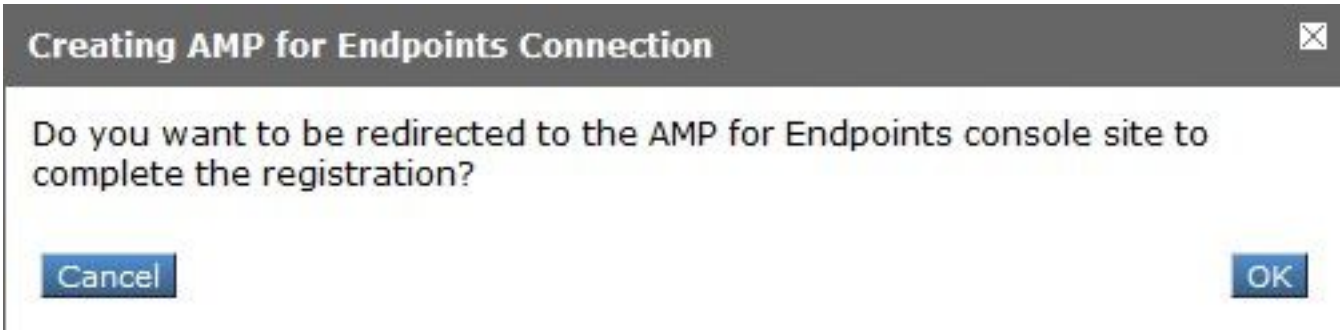


Advanced(**고급) > Advanced Settings for File Reputation(파일 평판**에 대한 고급 설정) 섹션을 검색하여 확장한 다음 일련의 클라우드 서버 옵션이 표시되면 해당 위치에서 가장 가까운 옵션을 선택합니다.

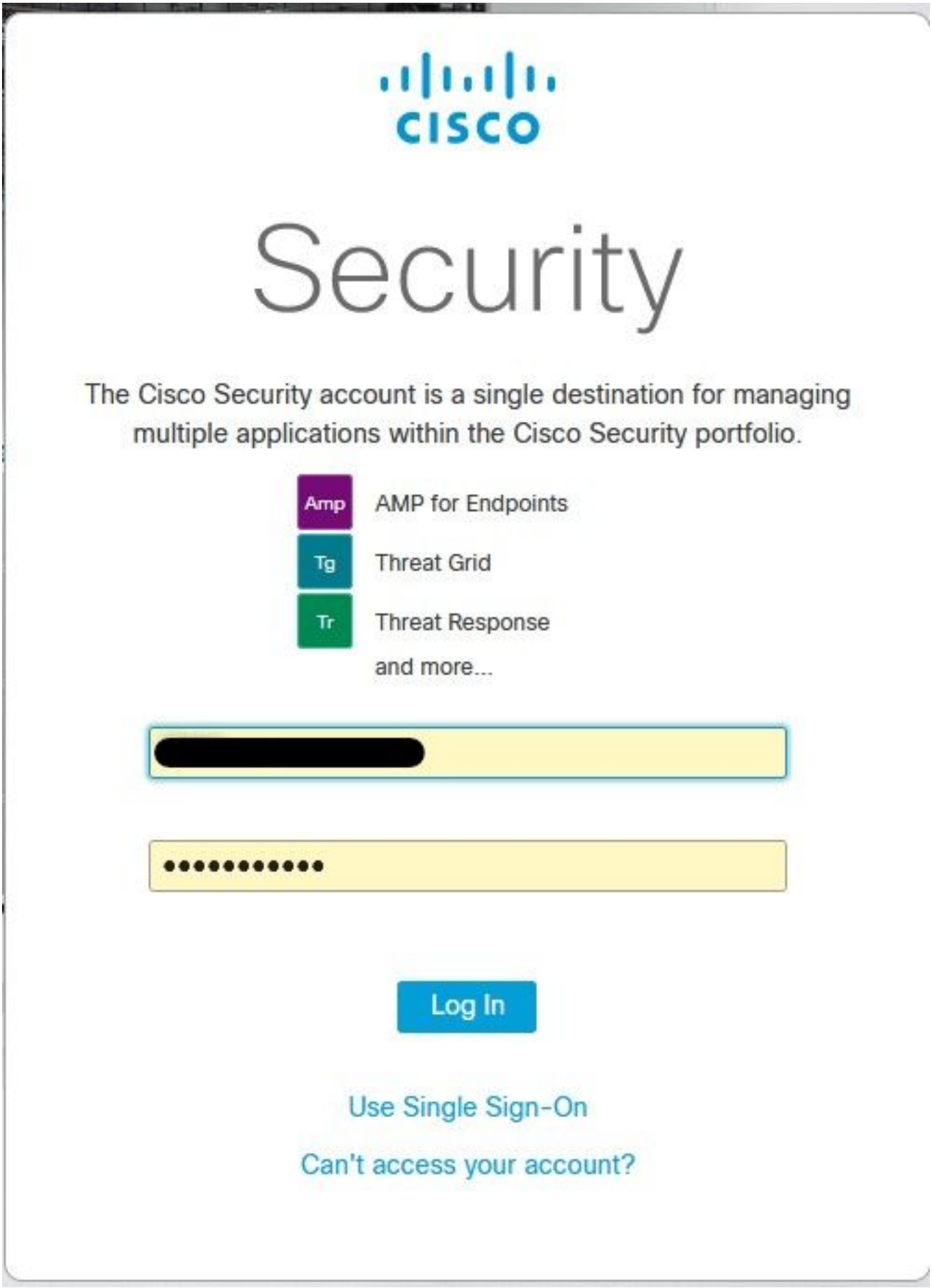


클라우드를 선택한 후 Register Appliance **with AMP for Endpoints** 버튼**을** 클릭합니다.

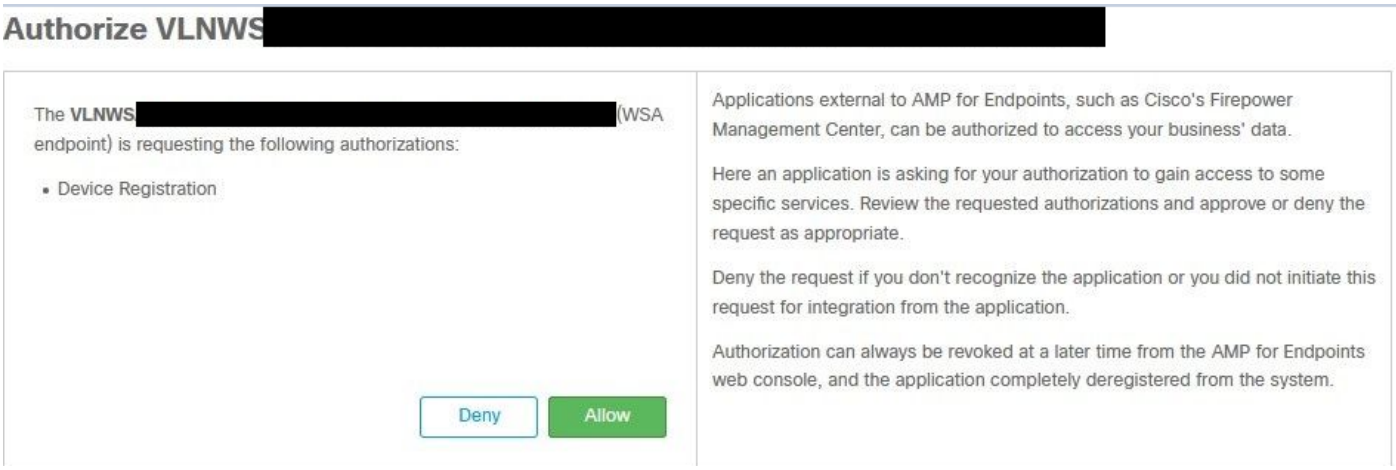
AMP 콘솔로 리디렉션하는 팝업 창이 나타나면 이미지에 표시된 대로 **Ok 버튼**을 클릭합니다.



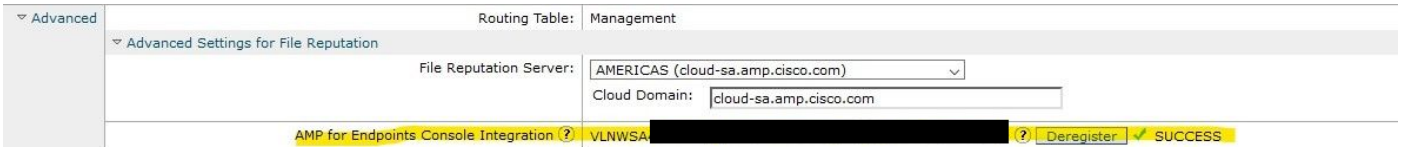
유효한 AMP 자격 증명을 인그레스(ingress)하고 이미지에 표시된 대로 **Log in(로그인)**을 클릭해야 합니다.



Device Registration(디바이스 등록)을 수락하고 클라이언트 ID를 기록해 둡니다. 이 ID는 나중에 콘솔에서 WSA를 찾을 수 있도록 도와줍니다.



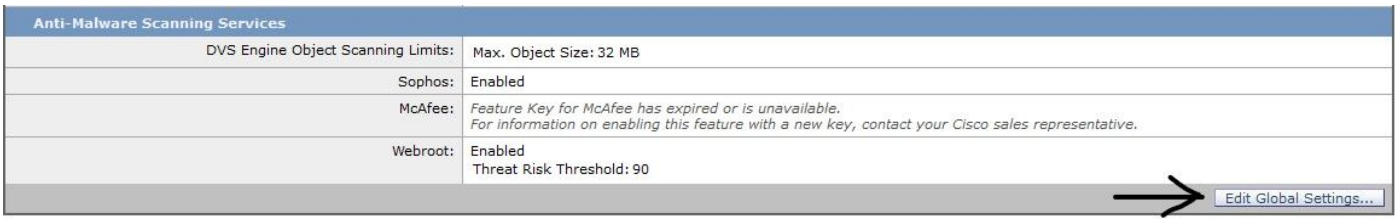
WSA 콘솔로 돌아가면 이미지에 표시된 대로 Amp for Endpoints Console Integration 섹션에 확인 메시지가 나타납니다.



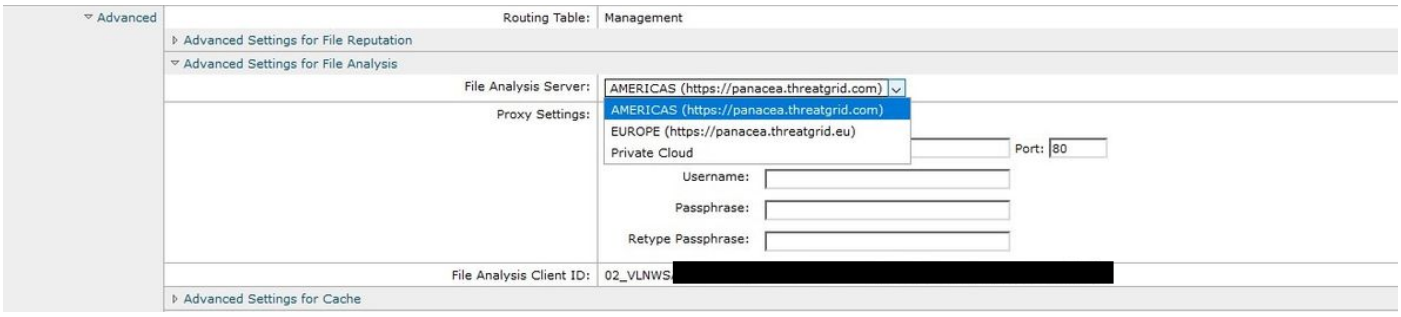
참고: Submit and Commit 변경 사항(프롬프트가 표시되면)을 클릭하여 프로세스를 다시 수행해야 합니다.

Threat Grid 통합

Security **Services(보안 서비스) > Anti-Malware and Reputation(안티멀웨어 및 평판)**으로 이동한 다음 Anti-Malware Protection Services(안티멀웨어 보호 서비스)에서 이미지에 표시된 대로 **Edit Global Settings(전역** 설정 편집) 버튼을 클릭합니다.

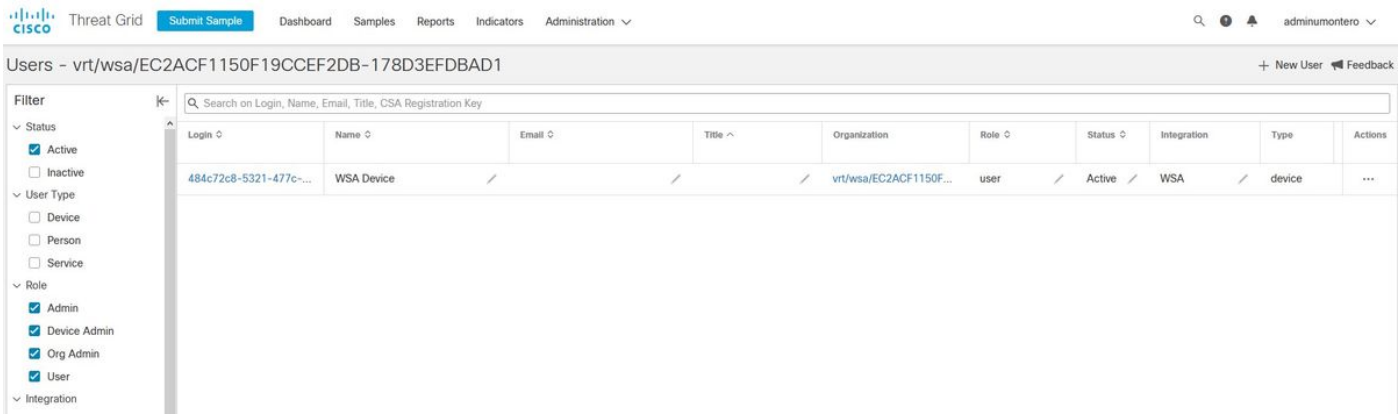


Advanced(**고급) > Advanced Settings for File Analysis(파일 분석 고급 설정**) 섹션을 검색하고 확장한 다음 이미지에 표시된 대로 위치에 가장 가까운 옵션을 선택합니다.



Submit and **Commit**(제출 및 **커밋)**을 클릭합니다.

TG 포털 측에서 어플라이언스가 AMP/TG와 성공적으로 통합되면 Users(사용자) 탭에서 WSA 디바이스를 검색합니다.



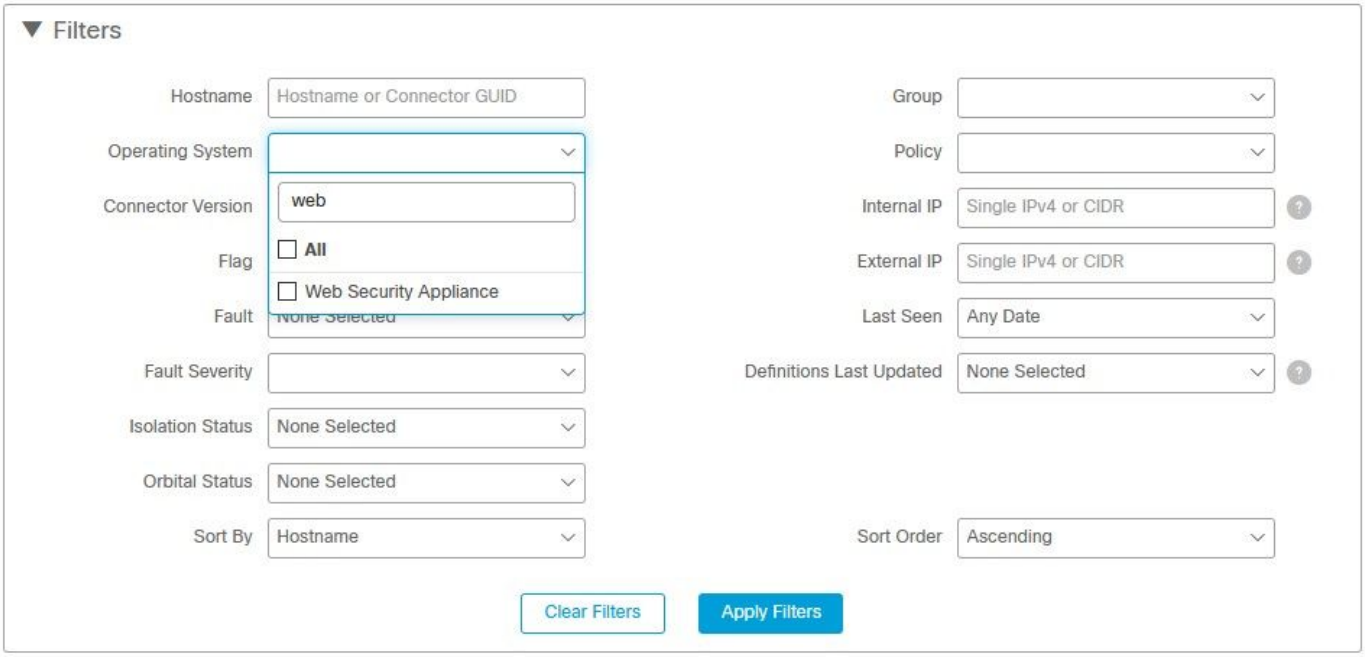
로그인을 클릭하면 해당 어플라이언스의 정보에 액세스할 수 있습니다.

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

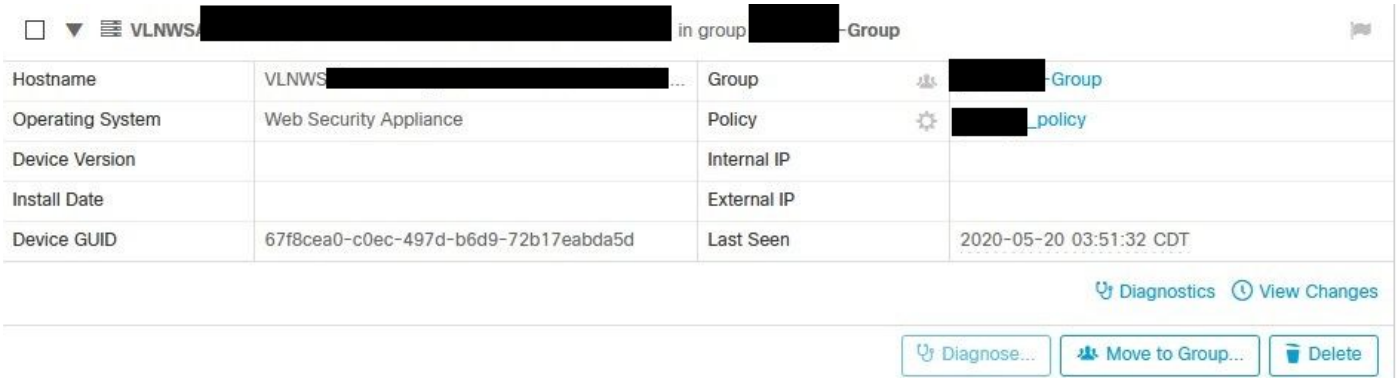
AMP와 WSA의 통합이 성공했는지 확인하기 위해 AMP 콘솔에 로그인하고 WSA 디바이스를 검색할 수 있습니다.

Management(**관리**) > **Computers(컴퓨터)**로 이동하고 필터 섹션에서 **Web Security Appliance**를 검색하고 필터를 적용합니다.

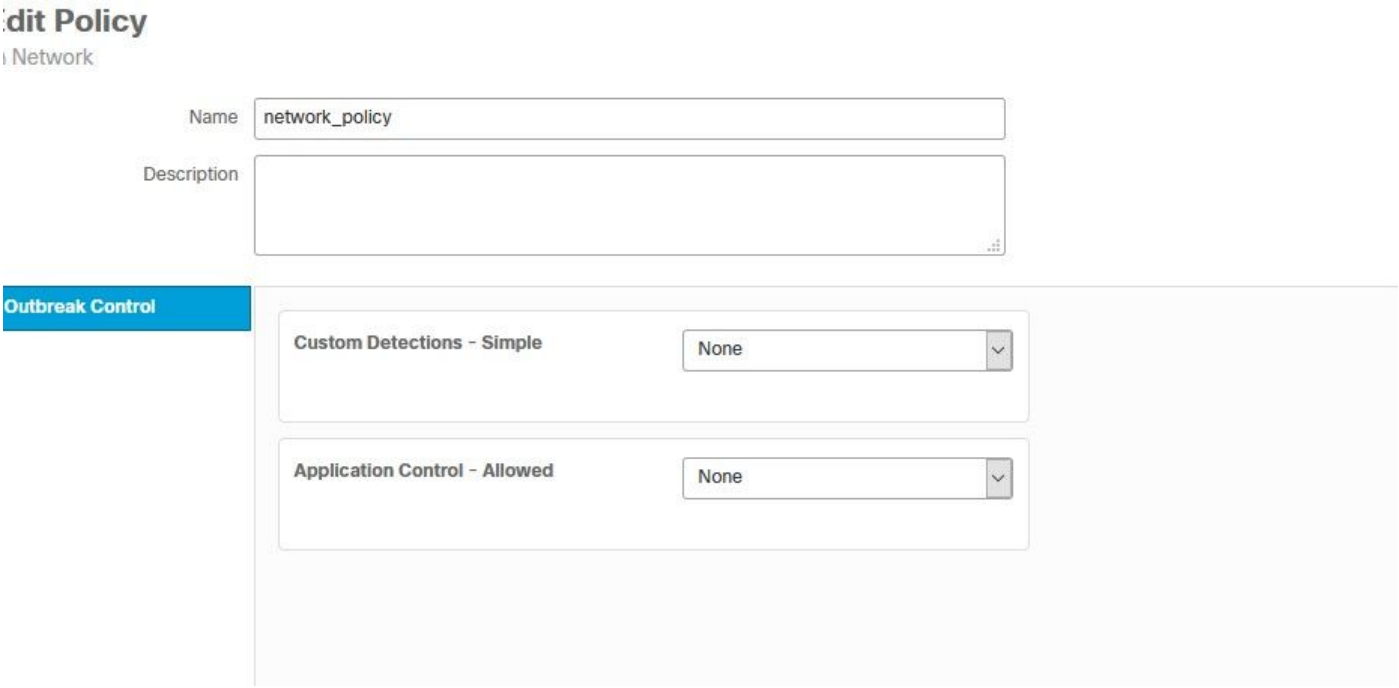


여러 WSA 디바이스가 등록된 경우 파일 분석 클라이언트 ID로 식별할 수 있습니다.

디바이스를 확장하면 해당 디바이스가 속한 그룹, 적용된 정책 및 디바이스 GUID를 사용하여 디바이스 전파 흔적을 볼 수 있습니다.

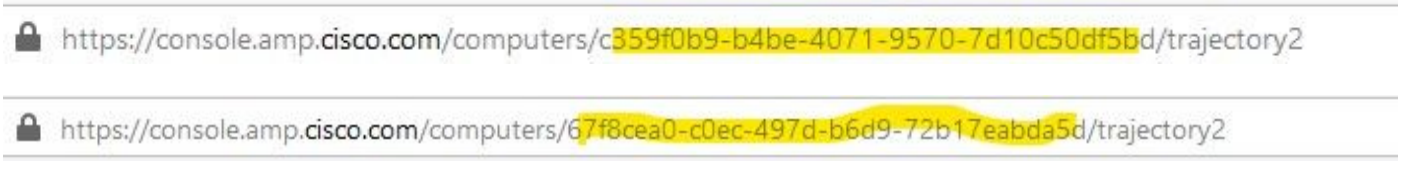


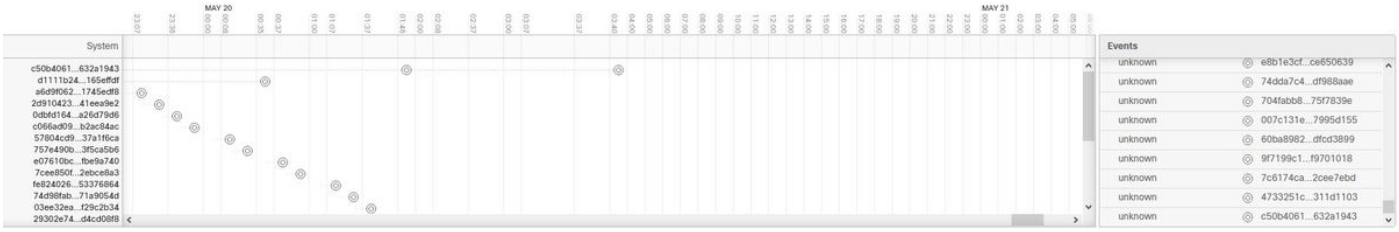
정책 섹션에서 디바이스에 적용되는 Simple Custom Detections(단순 맞춤형 탐지) 및 Application Control(애플리케이션 제어) - Allowed(허용됨)를 구성할 수 있습니다.



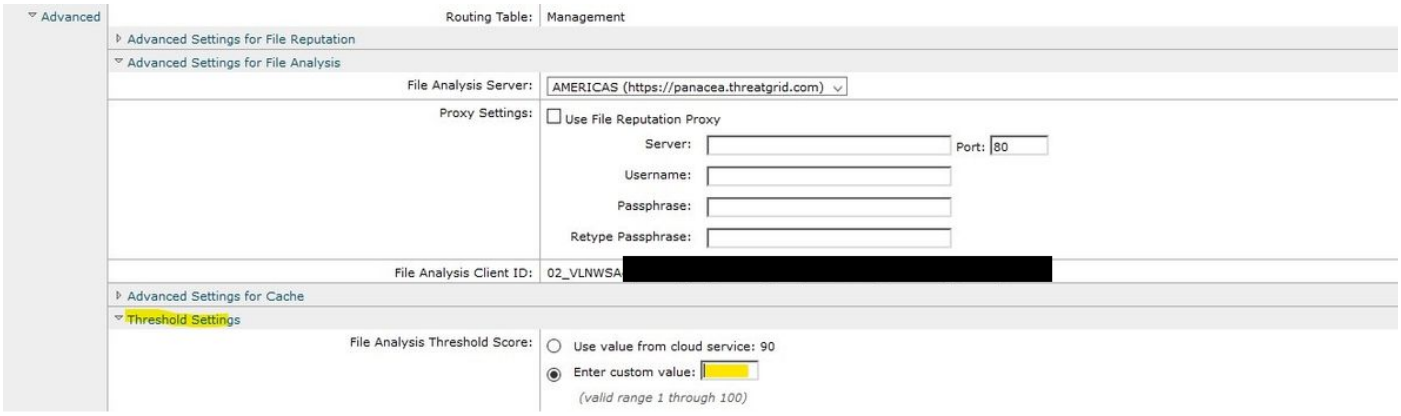
WSA의 Device Trajectory 섹션을 보려면 다른 컴퓨터의 Device Trajectory를 열고 Device GUID를 사용해야 합니다.

변경 사항은 이미지에 표시된 대로 URL에 적용됩니다.





Threat Grid의 경우 임계값이 90입니다. 파일이 해당 번호 아래에 점수를 받으면 해당 파일이 악성으로 찌르지 않지만 WSA에서 맞춤형 임계값을 구성할 수 있습니다.



문제 해결

WSA가 AMP 페이지로 리디렉션되지 않음

- 방화벽에서 AMP에 필요한 주소를 허용하는지 확인하고 여기를 클릭합니다.
- 적절한 AMP 클라우드를 선택했는지 확인합니다(레거시 클라우드 선택 금지).

WSA는 지정된 SHA를 차단하지 않습니다.

- WSA가 올바른 그룹에 있는지 확인합니다.
- WSA에서 올바른 정책을 사용하고 있는지 확인합니다.
- SHA가 클라우드에서 깨끗하지 않은지 확인하십시오. 그렇지 않으면 WSA에서 이를 차단할 수 없습니다.

WSA가 내 TG 조직에 표시되지 않음

- 적절한 TG 클라우드(미주 또는 유럽)를 선택했는지 확인합니다.
- 방화벽에서 TG에 필요한 주소를 허용하는지 확인합니다.
- 파일 분석 클라이언트 ID를 기록해 둡니다.
- Users(사용자) 섹션에서 검색합니다.
- 찾을 수 없는 경우 Cisco 지원에 연락하여 조직 간에 이동하는 데 도움을 주십시오.