AMP for Endpoints 포털에서 간단한 맞춤형 탐지 목록 구성

목차

소개

이 문서에서는 AMP(Advanced Malware Protection) for Endpoints 커넥터를 설치한 디바이스에서 파일이 허용되지 않도록 특정 파일을 탐지, 차단, 격리하는 Simple Custom Detection(단순 맞춤형 탐지) 목록을 생성하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- AMP 포털 액세스
- 관리자 권한이 있는 계정
- 파일 크기는 20MB 이하여야 합니다.

사용되는 구성 요소

이 문서의 정보는 Cisco AMP for Endpoints 콘솔 버전 5.4.20190709을 기반으로 합니다.

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.

워크플로

Simple Custom Detection(단순 맞춤형 탐지) 목록 옵션은 다음 워크플로를 사용합니다.

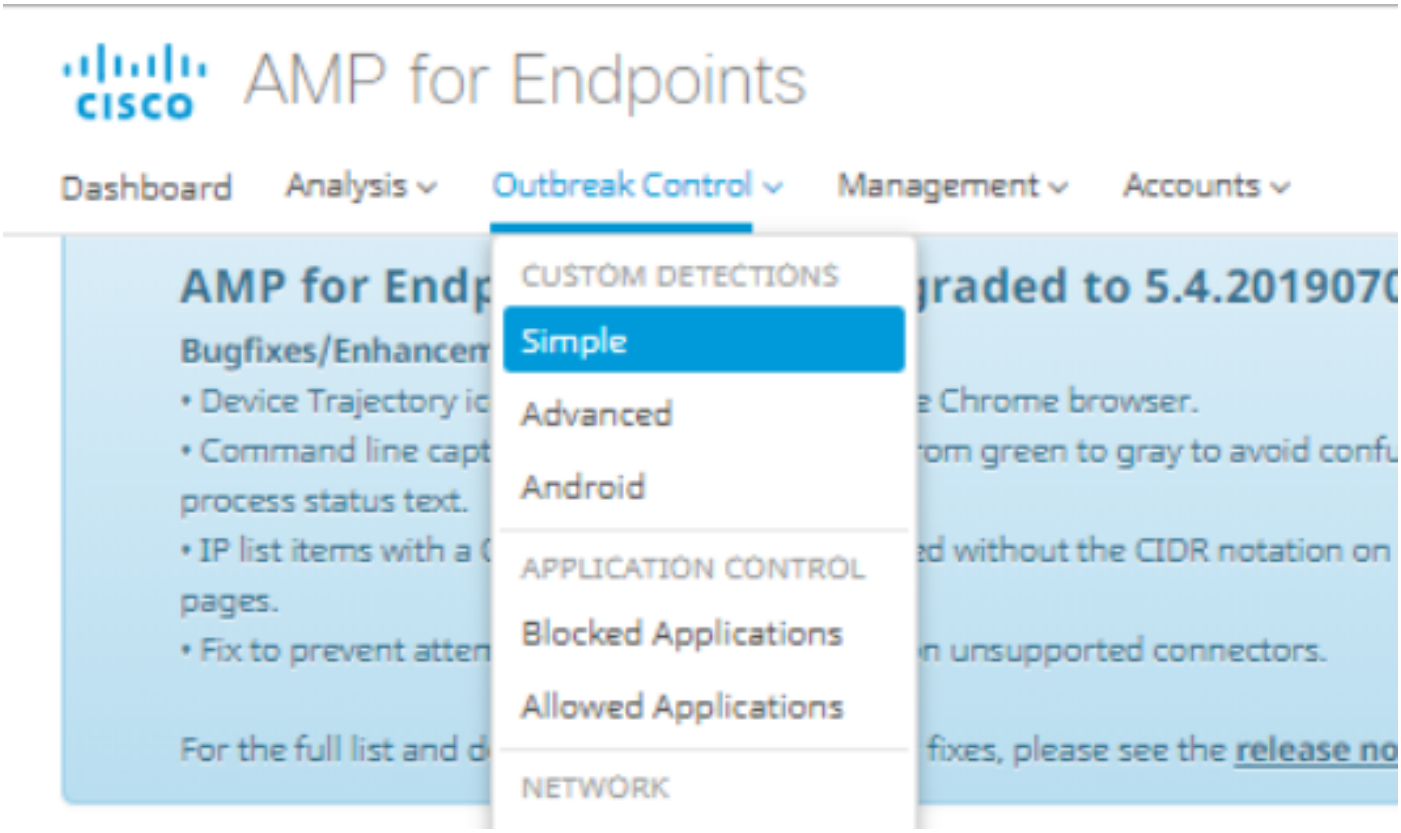
- AMP 포털에서 생성된 Simple Custom Detection(단순 맞춤형 탐지) 목록.
- 이전에 생성한 정책에 적용된 단순 맞춤형 탐지 목록.

- 디바이스에 설치되고 정책에 적용된 AMP Connector.

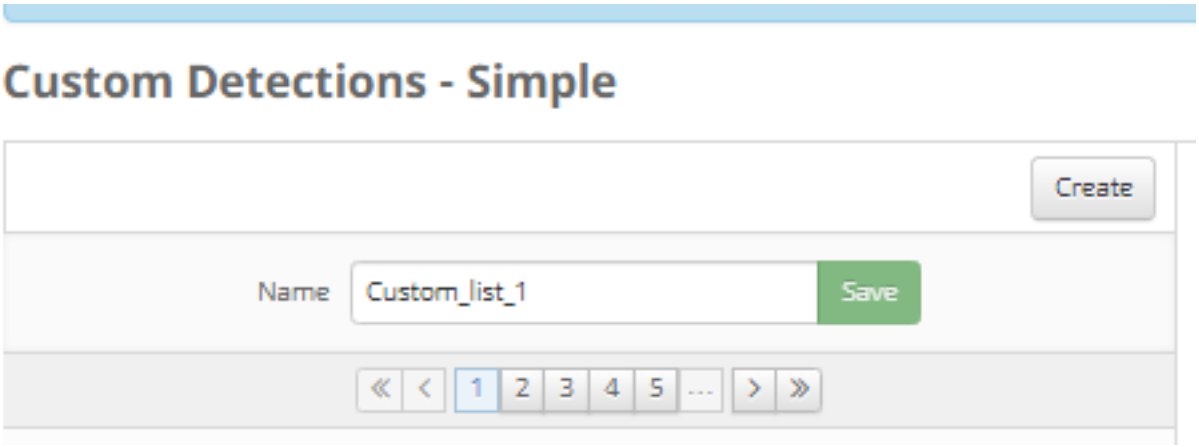
구성

Simple Custom Detection(단순 맞춤형 탐지) 목록을 생성하려면 다음 단계를 수행합니다.

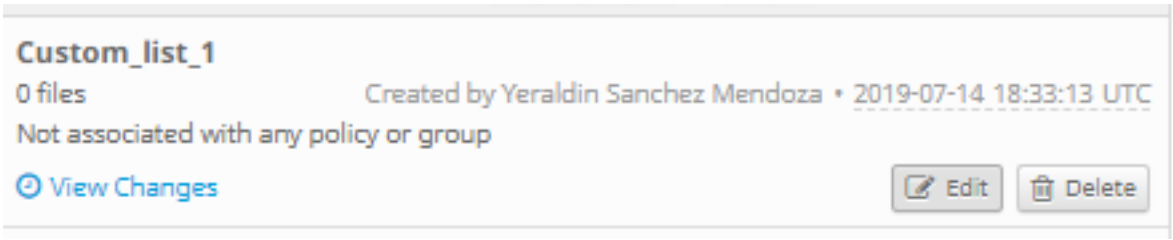
1단계. AMP Portal에서 이미지에 표시된 대로 **Outbreak Control > Simple** 옵션으로 이동합니다.



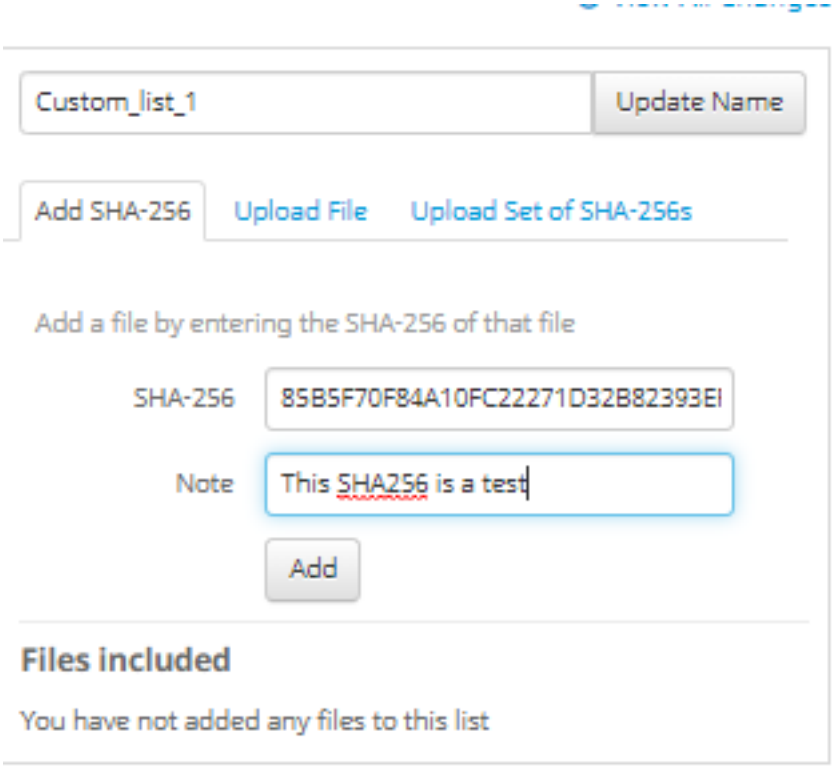
2단계. Custom Detections - Simple(맞춤형 탐지 - 단순) 옵션에서 **Create(생성)** 버튼을 클릭하여 새 목록을 추가하고, 이미지에 표시된 대로 Simple Custom Detection(단순 맞춤형 탐지) 목록을 식별할 이름을 선택하고 저장합니다.



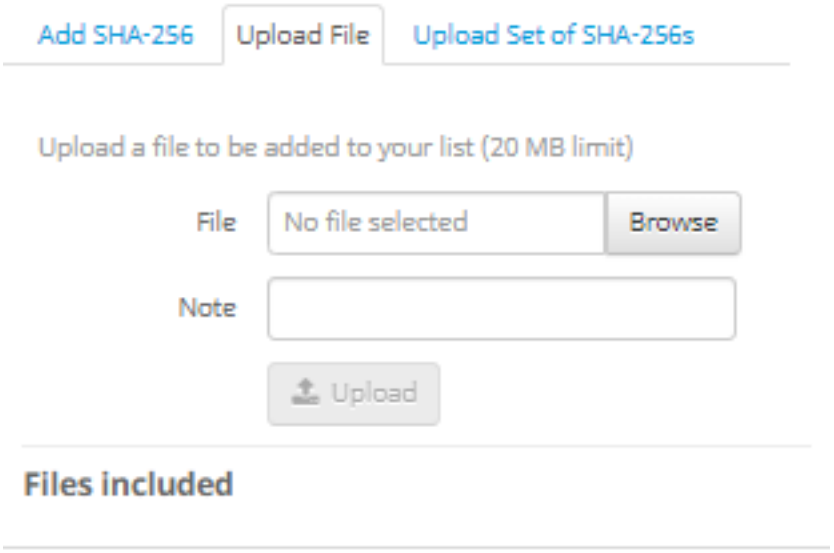
3단계. 목록이 생성되면 **편집** 버튼을 클릭하여 이미지에 표시된 대로 차단할 파일 목록을 추가합니다.



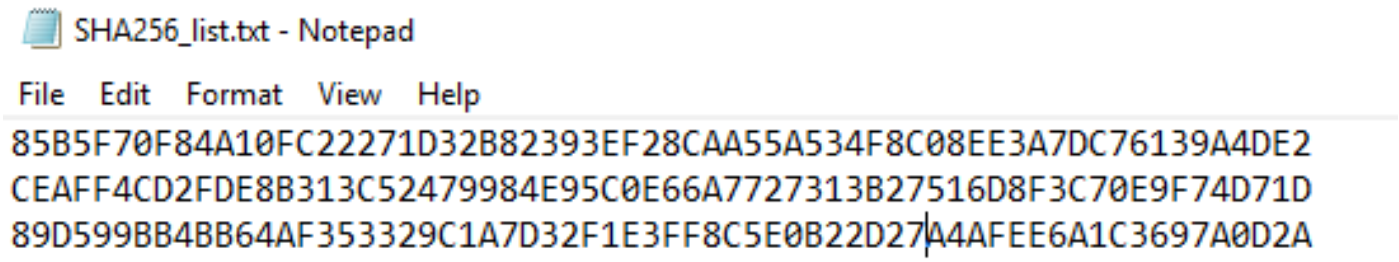
4단계. Add SHA-256(SHA-256 추가) 옵션에서, 이미지에 표시된 대로, 차단할 특정 파일에서 이전에 수집한 SHA-256 코드를 붙여넣습니다.

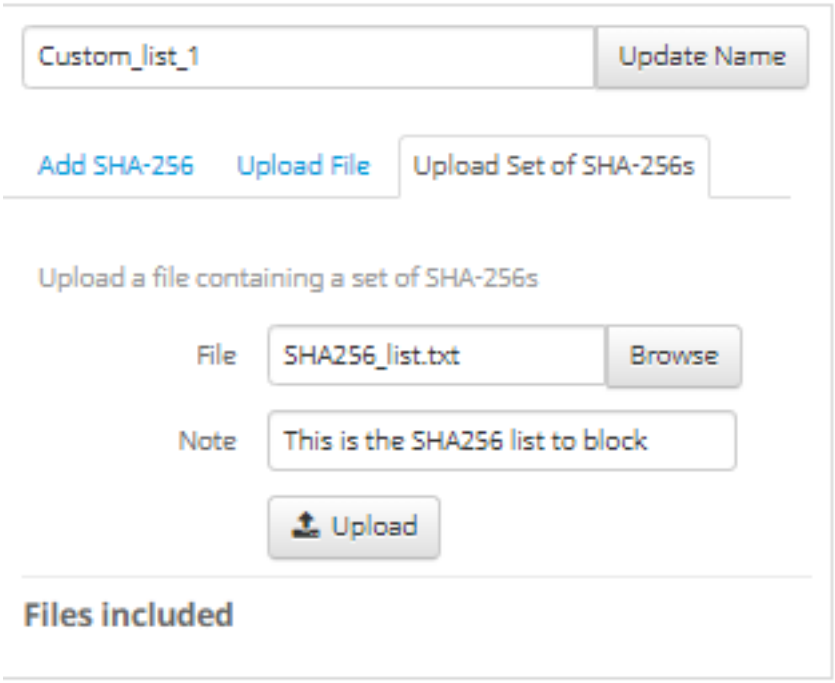


5단계. Upload File(파일 업로드) 옵션에서 차단할 특정 파일을 찾습니다. 파일이 업로드되면 이 파일의 SHA-256이 목록에 추가됩니다(이미지에 표시됨).

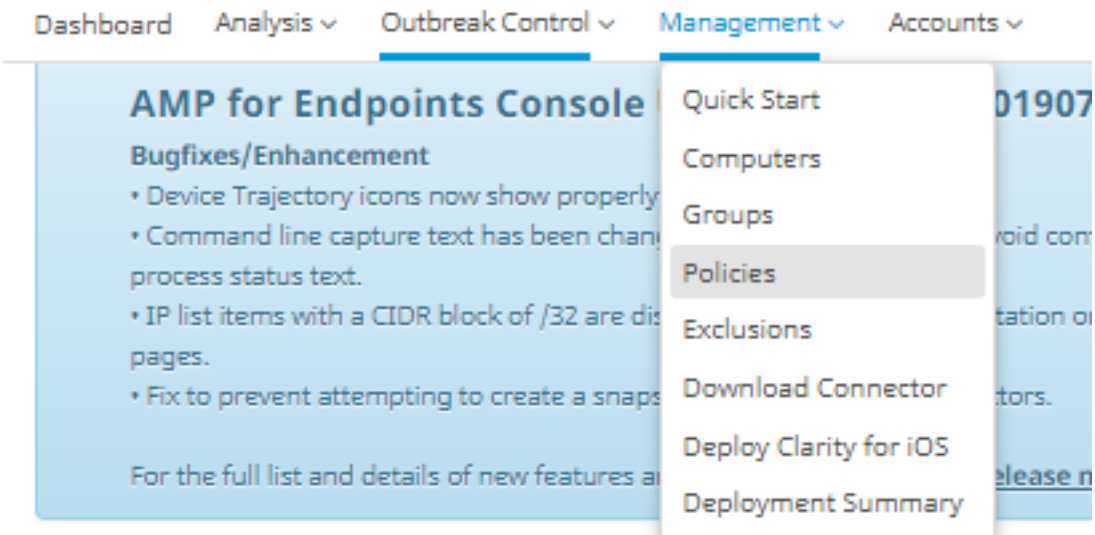


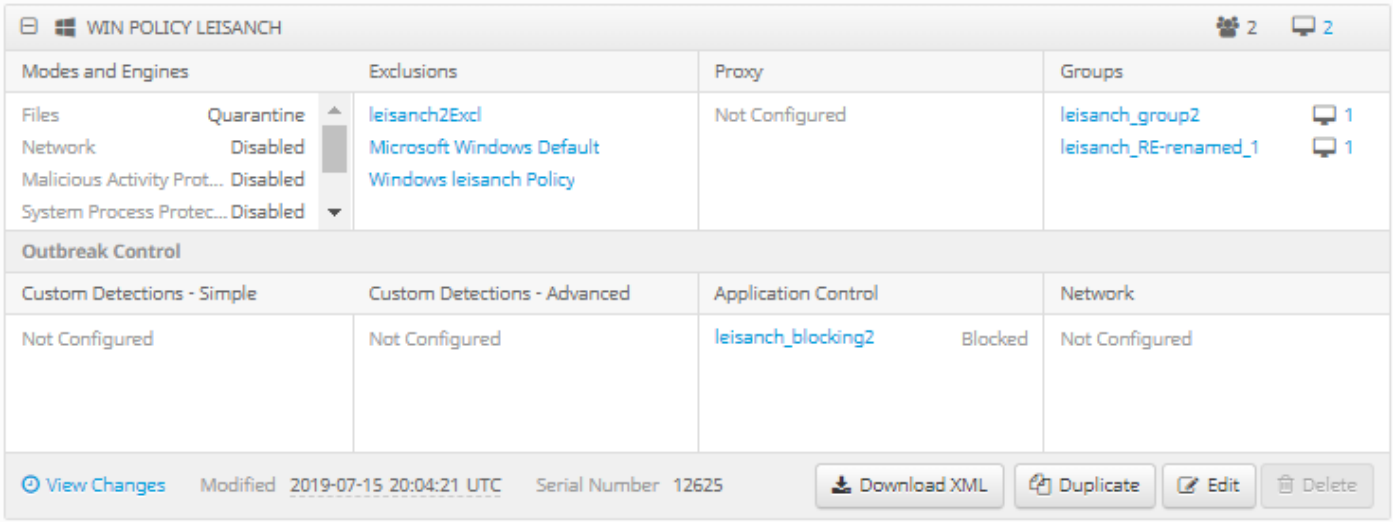
6단계. Upload Set of SHA-256s(SHA-256s 업로드 세트) 옵션을 사용하면 이미지에 표시된 것처럼 이전에 취득한 여러 SHA-256 코드 목록이 있는 파일을 추가할 수 있습니다.



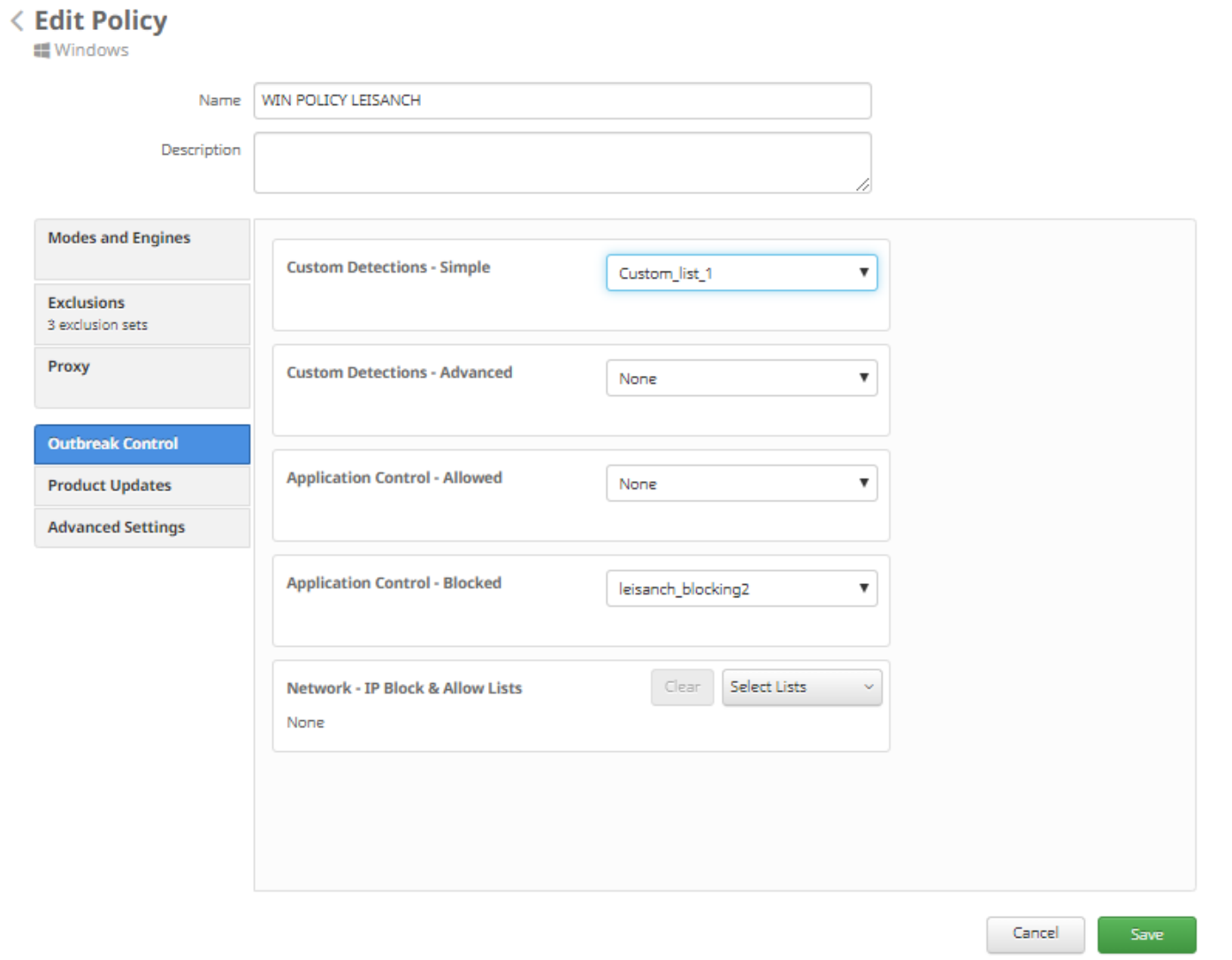


7단계. Simple Custom Detection(단순 맞춤형 탐지) 목록이 생성되면 **Management(관리) >** Policies(정책)로 이동하고 이미지에 표시된 대로 이전에 생성한 목록을 적용할 정책을 선택합니다.





8단계. Edit(**수정**) 버튼을 클릭하고 Outbreak Control(아웃브레이크 제어) **> Custom Detections - Simple(맞춤형 탐지 - 단순)으로 이동하여** 드롭다운 메뉴에서 이전에 생성한 목록을 선택하고 이미지에 표시된 대로 변경 사항을 저장합니다.



모든 단계를 수행하고 커넥터가 마지막 정책 변경 사항에 동기화되면 Simple Custom Detection(단순 맞춤형 탐지)이 적용됩니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

경고:파일이 Simple Custom Detection(단순 맞춤형 탐지) 목록에 추가된 경우 캐시 시간이 만료되어야 탐지가 적용됩니다.

참고: Simple Custom Detection(단순 맞춤형 탐지)을 추가하면 캐시될 수 있습니다.파일이 캐시되는 시간은 다음 목록에 표시된 것과 같이 파일의 속성에 따라 달라집니다.
·파일 정리:7일
·알 수 없는 파일:1시간
·악성 파일:1시간