DLP 정책 포함 및 제외 구성

목차

소개

이 문서에서는 DLP 정책에서 포함 및 제외 옵션을 사용하여 데이터 유출 방지 규칙을 특정 ID에 맞춤화하는 방법에 대해 설명합니다.

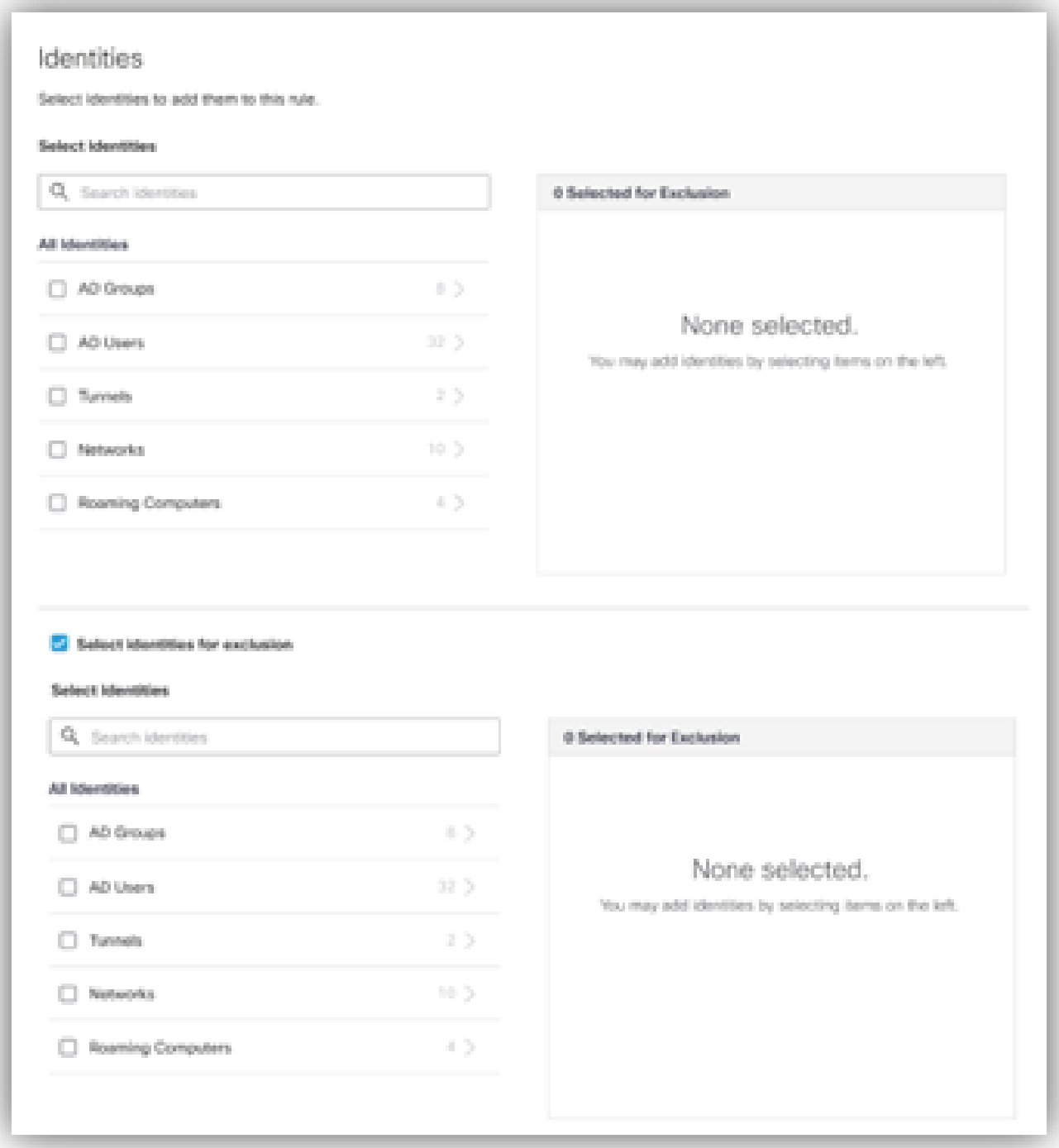
개요

DLP 정책의 포함 및 제외 옵션을 사용하면 데이터 유출 방지 규칙에서 지원하는 ID를 정확하게 정의할 수 있습니다. 특정 사용자 또는 그룹을 포함하거나 제외하여 정책 시행을 보다 세부적으로 제어할 수 있습니다.

DLP 정책 포함 및 제외 옵션 활용

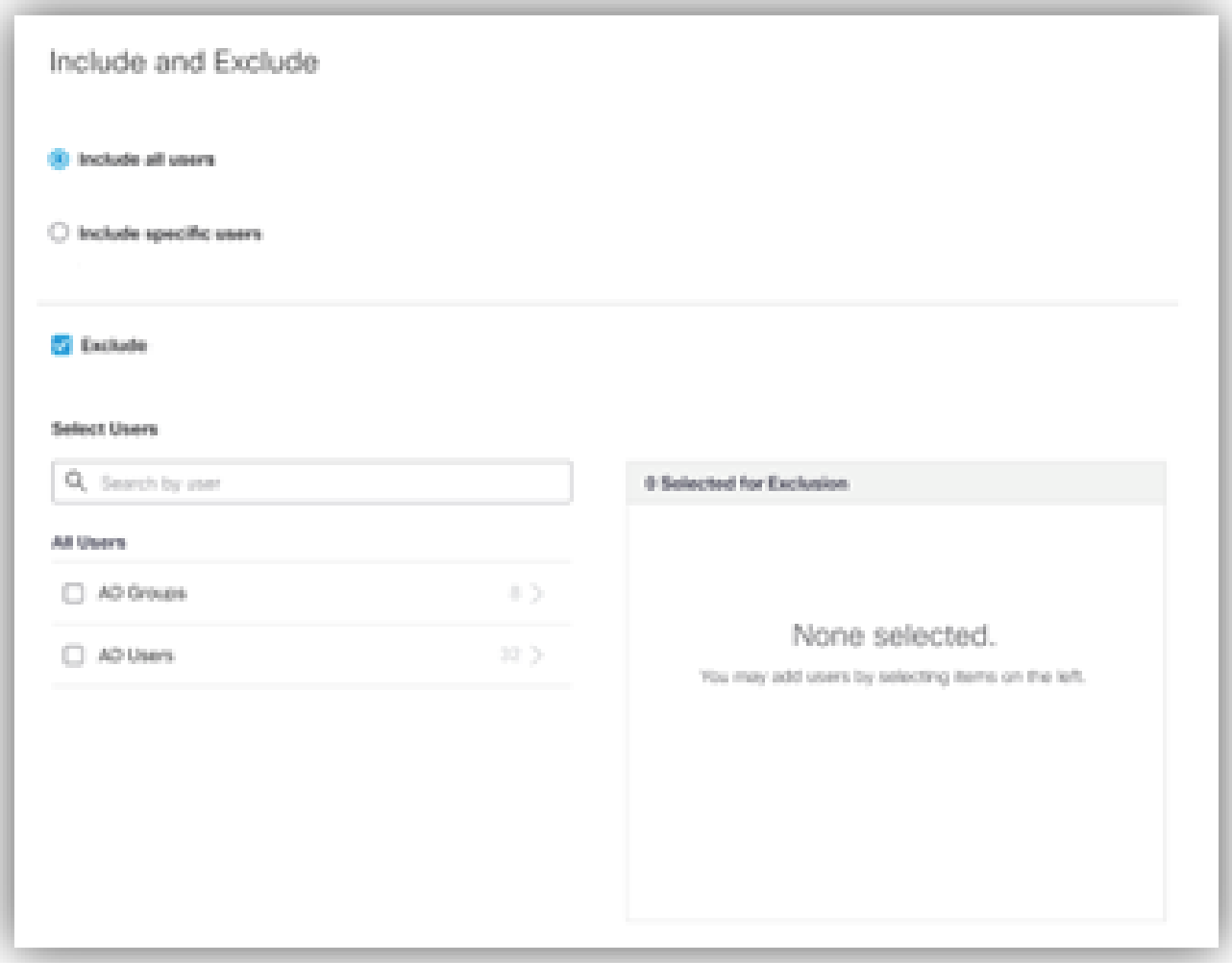
실시간 DLP 규칙

- Umbrella 또는 Secure Access 대시보드에서 Real-Time DLP 규칙을 생성하거나 수정합니다.
- Destinationsection으로 이동합니다.
  - 이제 동일한 목록에서 ID(사용자 또는 그룹)를 포함하거나 제외할 수 있습니다.
- 이렇게 하면 지정된 ID에만 DLP 작업을 적용하거나 필요에 따라 특정 ID를 제외할 수 있습니다.



SaaS API DLP 규칙

- SaaS API DLP 규칙 컨피그레이션에서 Include and Excludesection으로 이동합니다.
  - 여기에서 어떤 AD(Active Directory) 사용자와 AD 그룹을 동시에 포함하거나 제외할지를 지정할 수 있습니다.
- 이렇게 하면 선택한 ID에 DLP 정책을 적용하거나 특정 사용자 또는 그룹에 정책이 적용되지 않도록 할 수 있습니다.



추가 정보 찾기

단계별 지침은 Umbrella 및 Secure Access 설명서를 참조하십시오.

우산:

- 데이터 손실 방지 정책에 실시간 규칙 추가
- 데이터 손실 방지 정책에 SaaS API 규칙 추가

보안 액세스:

- 데이터 손실 방지 정책에 실시간 규칙 추가
- 데이터 손실 방지 정책에 SaaS API 규칙 추가

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.