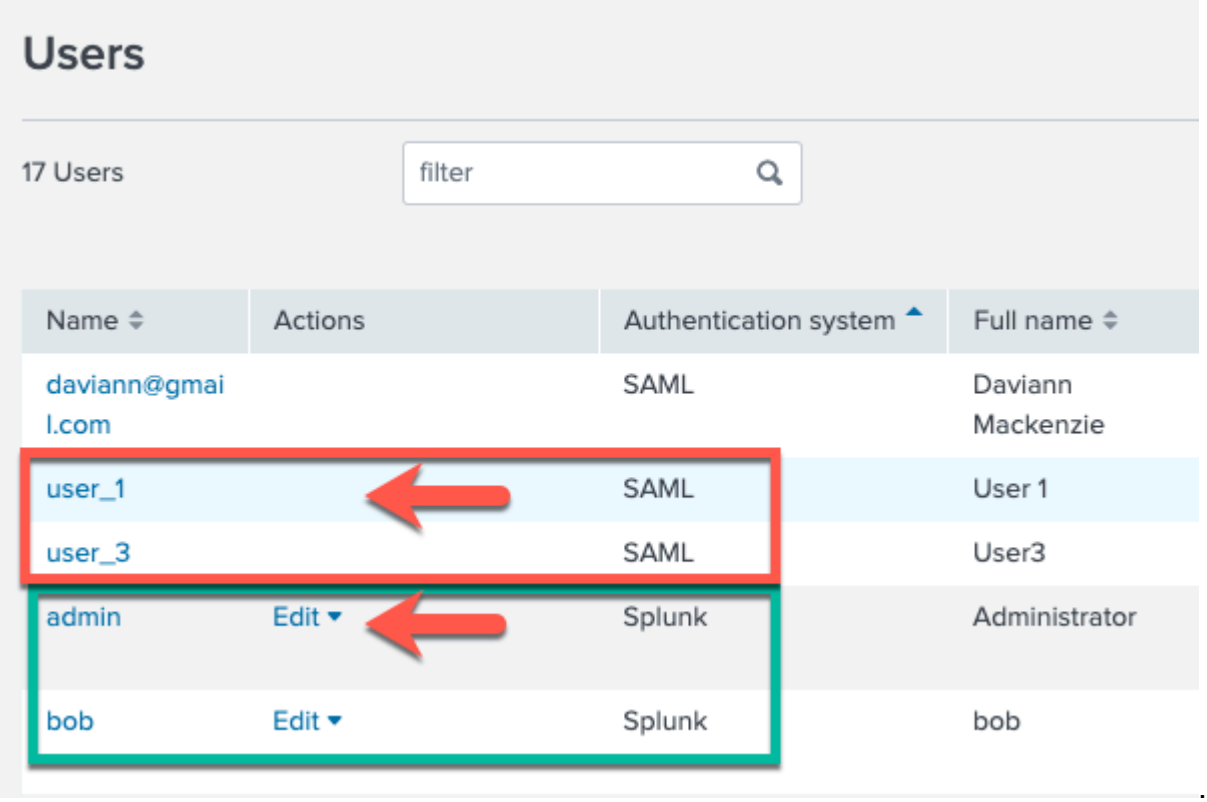
Splunk UI를 통해 SAML 사용자를 관리할 수 없습니다.

적용 가능성

Splunk Cloud Splunk Enterprise

설명

관리자는 Users UI를 통해 로컬에서 생성된 어카운트를 사용하여 SAML 사용자를 관리할 수 없습니다

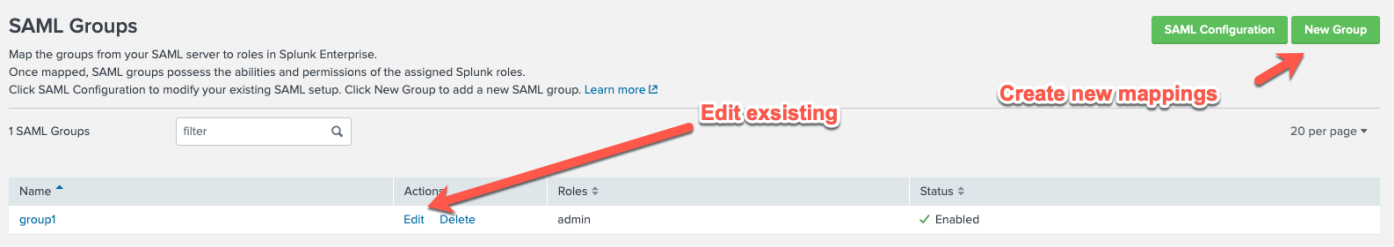


해결

SAML 통합을 통해 프로비저닝되는 사용자는 다음 두 가지 메커니즘만 사용하여 관리할 수 있습니다.

1. IdP(Identity Provider): IdP는 로그인 중에 사용자 로그인과 연결된 "역할"을 Splunk 인스턴스에 전송합니다. 사용자에 대해 역할을 추가하거나 제거해야 하는 경우 IdP를 통해 또는 IdP가 사용자를 검색하는 경우 LDAP를 통해 이 작업을 수행합니다.

2. SAML 그룹(매핑) https://<Splunk instance>/en-GB/manager/launcher/saml
이 인터페이스에서 IdP의 사용자 역할을 Splunk 역할에 매핑할 수 있습니다



역할 매핑 수정 또는 제거 설명서에서는 이러한 옵션에 대해 설명합니다

SAML 사용자를 제거하려면 연결된 역할(Splunk의 그룹 매핑에 사용됨)을 제거하여 IdP/LDAP 레벨에서 먼저 이 작업을 수행해야 합니다. 이렇게 하면 Splunk 인스턴스에서 사용자를 제거할 수 있습니다.

Splunk Cloud를 사용 중인 경우 이 문서에서 Splunk의 오래된 SAML 사용자를 제거하는 방법을 살펴보십시오

온프레미스 Splunk 인스턴스를 사용 중인 경우 이 커뮤니티 솔루션 Remove Old SAML Users(이전 SAML 사용자 제거)를 검토하십시오

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.