멀티 클라우드 방어계정 관리

계정(멀티 클라우드 방어 테넌트)

계정 정보는 관리자가 다음 기능을 생성하고 편집하는 데 사용됩니다.

Administration(관리**)** > **Management(**관리**)** > **Account(**어카운트**)**로 이동합니다.

CDO의 사용자 역할

Cisco Defense Orchestrator(CDO)에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. CDO 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 사용자는 한 테넌트에 대해서는 읽기 전용 역할을, 다른 테넌트에서는 슈퍼 관리자 역할을 가질 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다.

멀티 클라우드 방어의 역할

역할은 멀티 클라우드 방어 포털을 통해 멀티 클라우드 방어 테넌트에 액세스할 때 사용자가 수행할 수 있는 작업에서 중요한 역할을 합니다. 역할은 사용자에게 권한 집합을 부여하는 권한입니다.

다음 세 가지 역할을 사용할 수 있습니다.

- 슈퍼 관리자(admin_super)
- 편집 전용 관리자(admin_rw)
- 읽기 전용 관리자(admin_read-only)

두 가지 권한 정의는 다음과 같습니다.

- 수정 - 읽기, 쓰기, 편집 및 삭제
- 읽기 - 읽기 전용

다음 표에는 각 역할과 관련된 각 설정에 대한 권한이 요약되어 있습니다.

설정	슈퍼 관리자 **(admin_super)**	편집 전용**(admin_rw)**	읽기 전용 **(admin_read-only)**
관리			
사용자	수정	수정(슈퍼 관리자 제외)	읽기
MFA 활성/비활성	수정	수정(슈퍼 관리자 제외)	읽기
MFA 재설정	수정	수정(슈퍼 관리자 제외)	읽기
API 키	수정	수정	읽기
역할	읽기	읽기	읽기
계정 / 애플리케이션 태그	수정	수정	읽기
계정 - 이메일 도메인	수정	읽기	읽기
시스템	읽기	읽기	읽기
미터링	읽기	읽기	읽기
알림 프로파일			
서비스	수정	수정	읽기
알림	수정	수정	읽기

멀티 클라우드 방어 테넌트 내 사용자 1명만 슈퍼 관리자 역할을 할당할 수 있습니다. 이 사용자는 계정의 소유자로 간주되며 AWS 계정 또는 Linux 루트 계정의 소유자와 동의어입니다. 다른 모든 사용자에게는 읽기/쓰기 관리자 또는 읽기 전용 관리자 역할이 할당되어야 합니다.

슈퍼 관리자 역할은 멀티 클라우드 방어에 의해 할당되며 멀티 클라우드 방어 테넌트 생성 시 생성된 첫 번째 사용자에게 부여됩니다. 슈퍼 관리자 사용자를 변경해야 하는 경우 멀티 클라우드 방어 지원팀에 문의하십시오.