Cisco Security Cloud 어카운트

Cisco XDR 통합을 활성화하는 데 필요한 계정

Management Center를 Cisco Security Cloud과 통합하고 분석 및 위협 조사를 위해 Cisco XDR에 이벤트를 전송하려면 지역 클라우드 에 다음 계정 중 하나가 있어야 합니다.

- Cisco Security Cloud 로그인 계정.
- Secure Endpoint 계정
- Secure Malware Analytics 계정
- Cisco 보안 계정.

중요 사용자나 사용자의 조직이 대상 지역 클라우드에서 상기 계정 중 하나를 이미 이용하고 있다면, 기존 계정을 사용하십시오. 새 계정을 생성하지 마십시오. 계정과 연결된 데이터는 해당 계정에만 사용할 수 있습니다.

계정이 없다면 Cisco XDR 통합 활성화를 위한 계정 얻기, 2 페이지의 내용을 참조하십시오.

직접 통합을 위해서는 관리 센터 및 매니지드 디바이스를 등록하는 CDO 테넌트가 필요합니다. 아직 CDO 테넌트가 없는 경우 테넌트를 요청합니다. 자세한 내용은 CDO 테넌트 요청을 참조하십시오.

Cisco XDR 통합 활성화를 위한 계정 얻기

시작하기 전에

사용할 지역 클라우드에서 사용자가 사용자의 조직이 이미 계정을 만들었다면, 새 계정을 만들지 마십시오. 기존 계정을 사용하여 Cisco XDR에 방화벽 이벤트 데이터 전송을 활성화합니다. 조직에 이미 해당 클라우드에 대해 지원되는 계정이 있는지 확인합니다. 지원되는 계정 유형에 대해서는 Cisco XDR 통합을 활성화하는 데 필요한 계정, 1 페이지의 내용을 참조하십시오. 조직 내 누군가가 해당 지역 클라우드의 계정을 이미 만들었다면 해당 계정 관리자에게 대신 계정을 추가해달라고 요청해야 합니다. 자세한 내용은 사용자 CDO 계정에 대한 액세스 관리, 2 페이지를 참조하십시오.

프로시저

단계 **1** 사용할 지역 클라우드를 결정합니다. 자세한 내용은 지역 클라우드 선택 지침 및 제한 사항를 참고하십시오.

단계 **2** 보안 클라우드 로그인 어카운트가 없지만 하나를 만들려면 선택한 지역 클라우드로 이동합니다.

지역 클라우드 및 해당 URL의 목록은 지역 클라우드의 내용을 참조하십시오.

단계 **3** **Sign Up Now(**지금 등록하기**)**를 클릭합니다.

보안 클라우드 로그인 계정을 생성하는 방법에 대한 자세한 내용은 새 Cisco Security Cloud 로그인 계정 생성을 참조하십시오.

클라우드 계정에 대한 액세스 관리

사용자 계정 관리는 보유한 클라우드 계정의 유형에 따라 달라집니다.

참고 Secure Malware Analytics 또는 Secure Endpoint 계정을 사용하여 클라우드에 액세스하는 경우 해당 제품에 대한 설명서를 참조하십시오.

사용자 CDO 계정에 대한 액세스 관리

Cisco Security Cloud에 액세스하기 위해 CDO 계정을 사용하는 경우 이 절차를 사용하여 사용자를 관리합니다.

시작하기 전에

이 작업을 수행하려면 CDO에 슈퍼 관리자 권한이 있어야 합니다.

프로시저

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 내비게이션 바에서 **Settings(**설정**)** > **User Management(**사용자 관리**)**를 클릭합니다.

CDO의 사용자 관리에 대한 자세한 내용은 CDO 온라인 도움말을 참조하십시오.