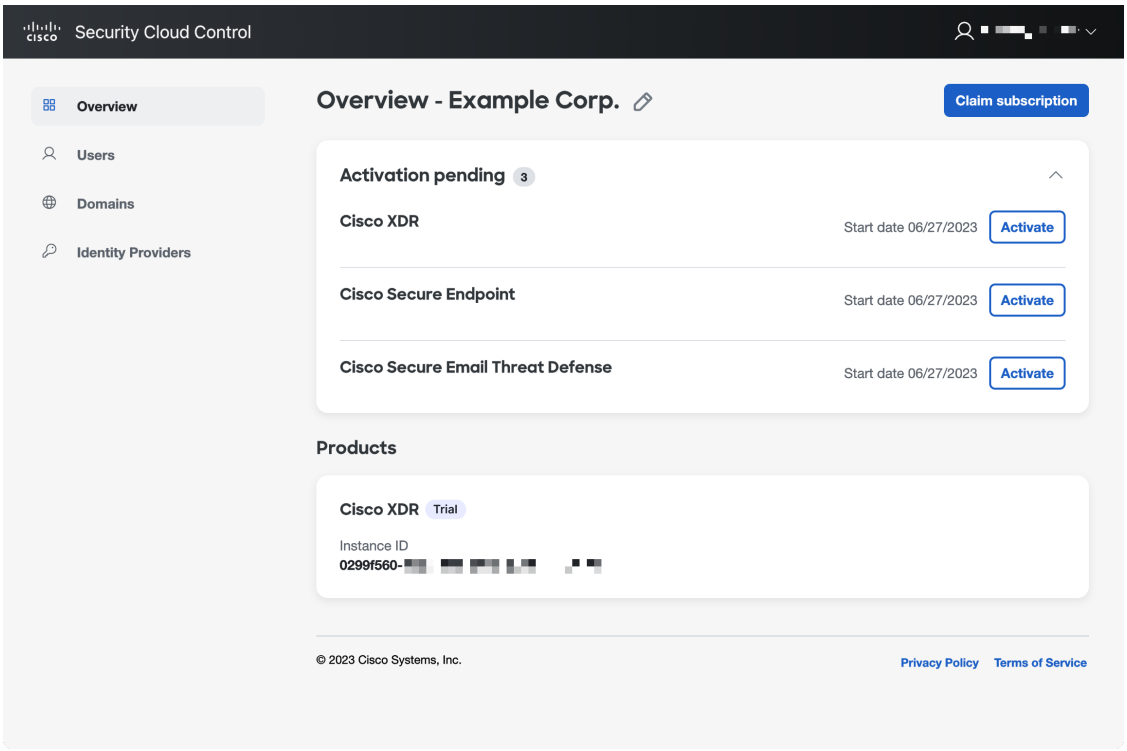
개요

Cisco Security Cloud 제어 개요

Security Cloud Control은 Cisco Security Cloud 전체에서 Cisco Secure 제품 인스턴스, 사용자 ID 및 사용자 액세스 관리의 중앙 집중식 관리를 제공하는 웹 애플리케이션입니다. Security Cloud Control 관리자는 새로운 Security Cloud 엔터프라이즈를 생성하고, 엔터프라이즈의 사용자를 관리하고, 도메인을 클레임하고, 조직의 SSO ID 제공자를 통합하는 등의 작업을 수행할 수 있습니다.

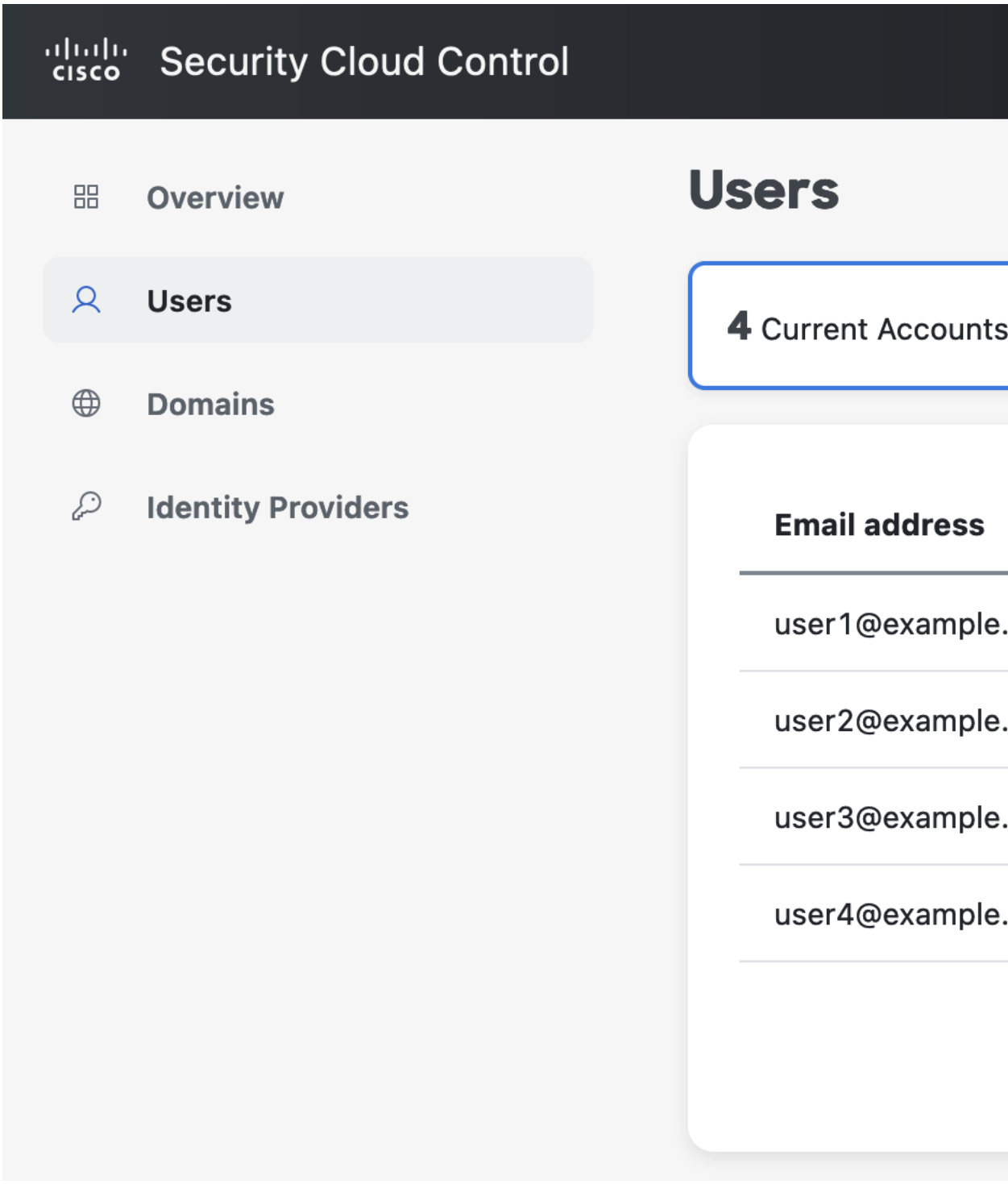
Overview(개요**)** 탭

Overview(개요**)** 탭에는 현재 활성화된 Cisco 제품 인스턴스와 활성화 보류 중인 인스턴스가 나열됩니다. 여기에서 보안 클라우드에 구독을 신청하거나 외부 제품을 연결할 수도 있습니다. 자세한 내용은 제품 및 구독 관리를 참조하십시오.



Users(사용자) 탭

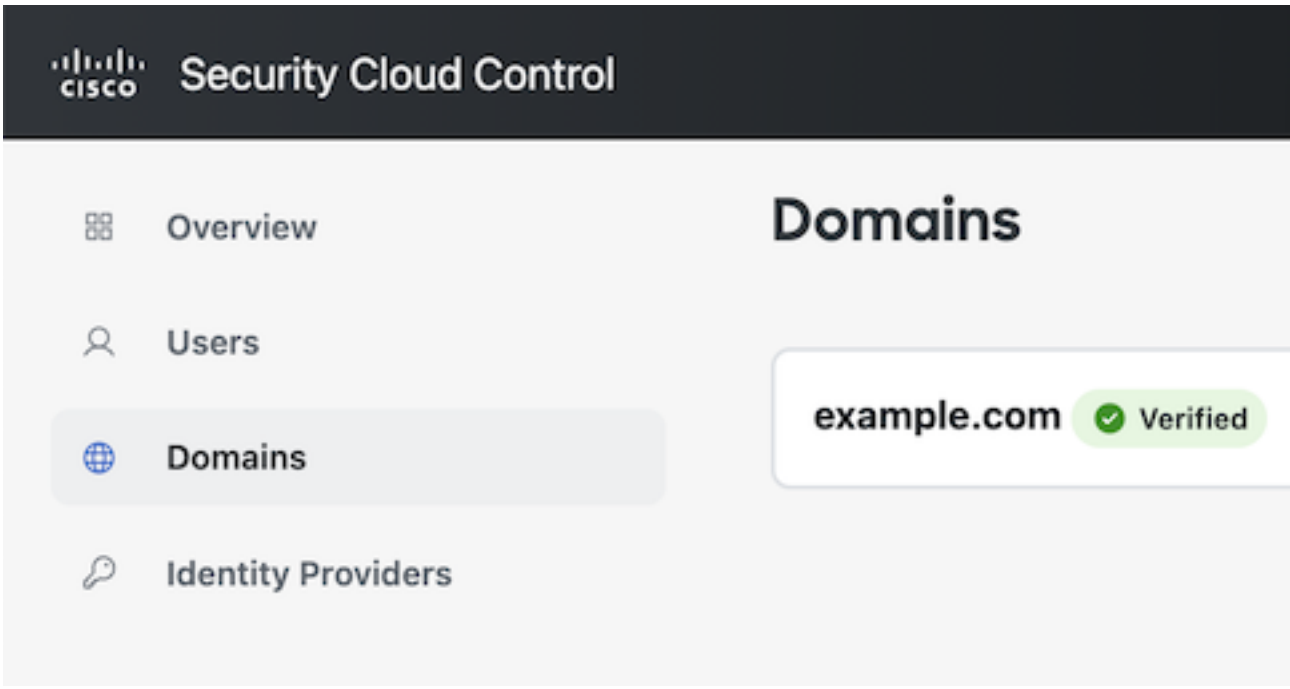
Users(사용자) 탭은 관리자가 엔터프라이즈에 초대한 사용자를 나열합니다. 관리자는 사용자 비밀번호와 MFA 설정(클레임되고 확인된 도메인의 사용자의 경우)을 재설정하고 사용자 계정을 비활성화할 수도 있습니다. 자세한 내용은 사용자 관리를 참조하십시오.



Domains(도메인**)** 탭

Domains(도메인**)** 탭에는 엔터프라이즈에 대해 클레임되고 확인된 이메일 도메인이 나열되어 있습니다. ID 제공자를 Security Cloud Sign On과 통합하려면 도메인을 확인해야 합니다. 또한 이를 통해 관

리자는 클레임된 도메인에 있는 사용자의 비밀번호 또는 MFA 설정을 재설정할 수 있습니다. 자세한 내용은 도메인 관리를 참조하십시오.



Identity Providers(ID 제공자) 탭

Identity Providers(ID 제공자) 탭에는 현재 엔터프라이즈에 대해 SAML(Secure Assertion Markup Language)을 사용하여 Security Cloud Sign On과 통합되는 모든 ID 제공자가 나열됩니다. 이를 통해 엔터프라이즈 사용자는 ID 제공자의 SSO 인증서를 사용해 Cisco Secure 제품에 액세스할 수 있습니다. 자세한 내용은 ID 제공자 통합 가이드의 내용을 참조하십시오.

Security Cloud Control 로그인

보안 클라우드 제어에 로그인하려면 Cisco Security Cloud Sign On 계정이 필요합니다. 계정이 없는 경우 계정을 만들고 Duo MFA 또는 Google Authenticator로 다단계 인증을 구성합니다. 보안 클라우드 로그인 계정으로 보안 클라우드 제어에 처음 로그인할 때 엔터프라이즈에서 단독 사용자로 보안 클라우드 로그인 계정을 사용하여 새 엔터프라이즈가 생성됩니다.

보안 로그인 계정과 연결된 엔터프라이즈가 하나뿐인 경우 로그인할 때 해당 엔터프라이즈가 항상 선택됩니다. 여러 엔터프라이즈를 생성한 경우 로그인한 후 마지막으로 선택한 엔터프라이즈가 선택됩니다.

단계 **1** 보안 클라우드 제어를 엽니다.

단계 **2** 계정을 생성할 때 설정한 보안 클라우드 로그인 자격 증명 및 MFA 옵션을 사용하여 로그인합니다.

보안 클라우드 제어 계정에 처음 로그인하는 경우, 새 엔터프라이즈가 기본 이름으로 생성됩니다. 연필 아이콘을 클릭하여 엔터프라이즈 이름을 변경할 수 있습니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.