개요

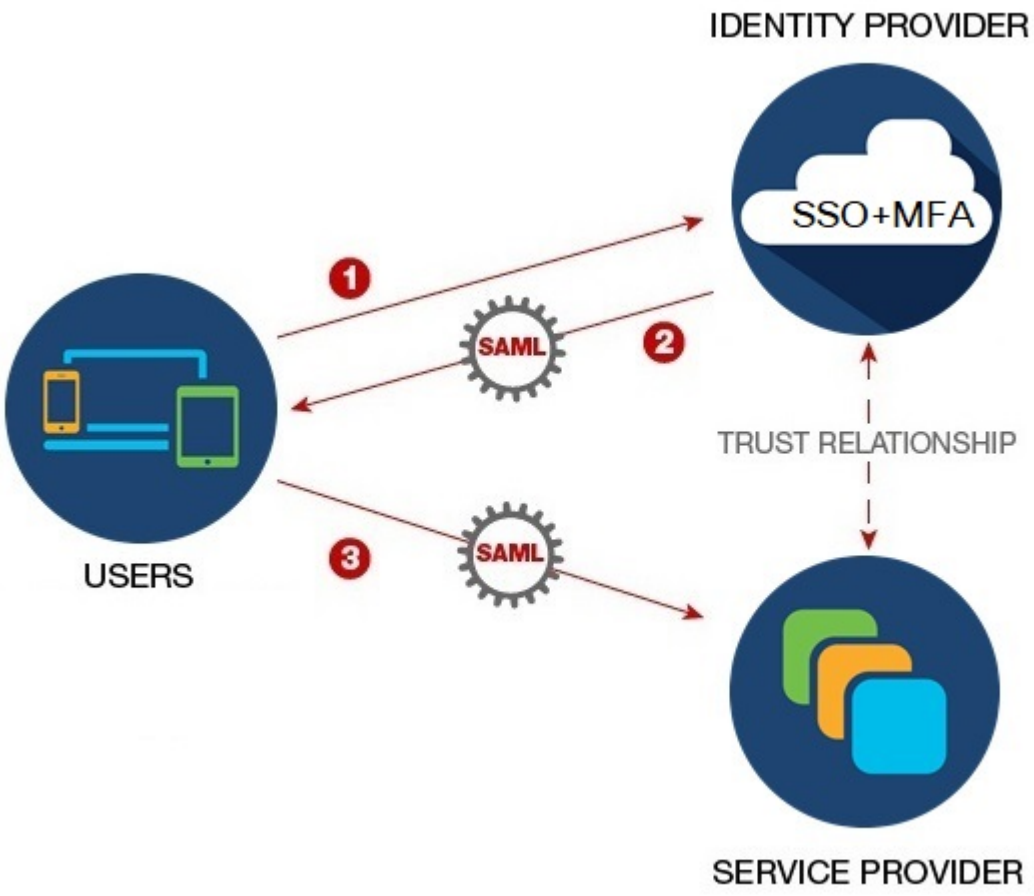
중요 **Enterprise Manager**가 사용이 중지되었습니다. 이제 보안 클라우드 제어 를 사용하여 ID 공급자 통합을 관리할 수 있습니다. 자세한 내용은 ID 공급자 통합 가이드를 참조하십시오.

모든 기존 ID 공급자 통합 데이터는 보안 클라우드 컨트롤을 통해 사용할 수 있습니다.

개요

SAML(Security Assertion Markup Language)을 사용하여 자체 또는 서드파티 IdP(ID 공급자)를 Cisco Security Cloud Sign On과(와) 통합할 수 있습니다. SAML은 ID 공급자(IdP)와 SP(통신 사업자) 간에 인증 및 권한 데이터를 교환하기 위한 XML 기반의 개방형 표준입니다. 이 경우 통신 사업자는 Security Cloud Sign On입니다. 통합되면 사용자는 SSO(Single Sign On) 자격 증명을 사용하여 Security Cloud

Sign On에 로그인할 수 있습니



다단계 인증 요구 사항

Security Cloud Sign On에는 모든 계정에 대해 Duo 다단계 인증이 필요합니다. SAML(Security Assertion Markup Language)을 사용하여 자체 ID 공급자와 을 통합하는 고객은 Duo MFA를 옵트아웃할 수 있습니다.

Duo MFA에 등록한 사용자는 선택적으로 Google Authenticator에 등록할 수 있습니다. Google Authenticator에 등록한 후에는 후속 로그인에서는 Duo MFA 챌린지가 아닌 Google Authenticator 챌린지만 표시합니다.

Cisco 고객 ID 또는 Microsoft를 통해 페더레이션된 로그인을 사용하는 경우(Security Cloud Sign On 페이지의 **Other login options(**기타 로그인 옵션**)** 아래) 동일한 정책이 적용됩니다.

기존 IdP 통합 고객

이 가이드에서 설명하는 셀프 서비스 도구로 생성되지 않은 IdP 통합이 Security Cloud Sign On인 경우, 이 도구를 사용하여 기존 구성을 업데이트할 수 없습니다. 통합에 대해 다음 설정을 수정해야 하는 경우 Cisco TAC를 사용하여 케이스를 열어야 합니다.

- SAML SSO(Single Sign On) URL 또는 엔터티 ID URI
- X.509 서명 인증서
- MFA(다단계 인증) 설정