



## 환영합니다.

---

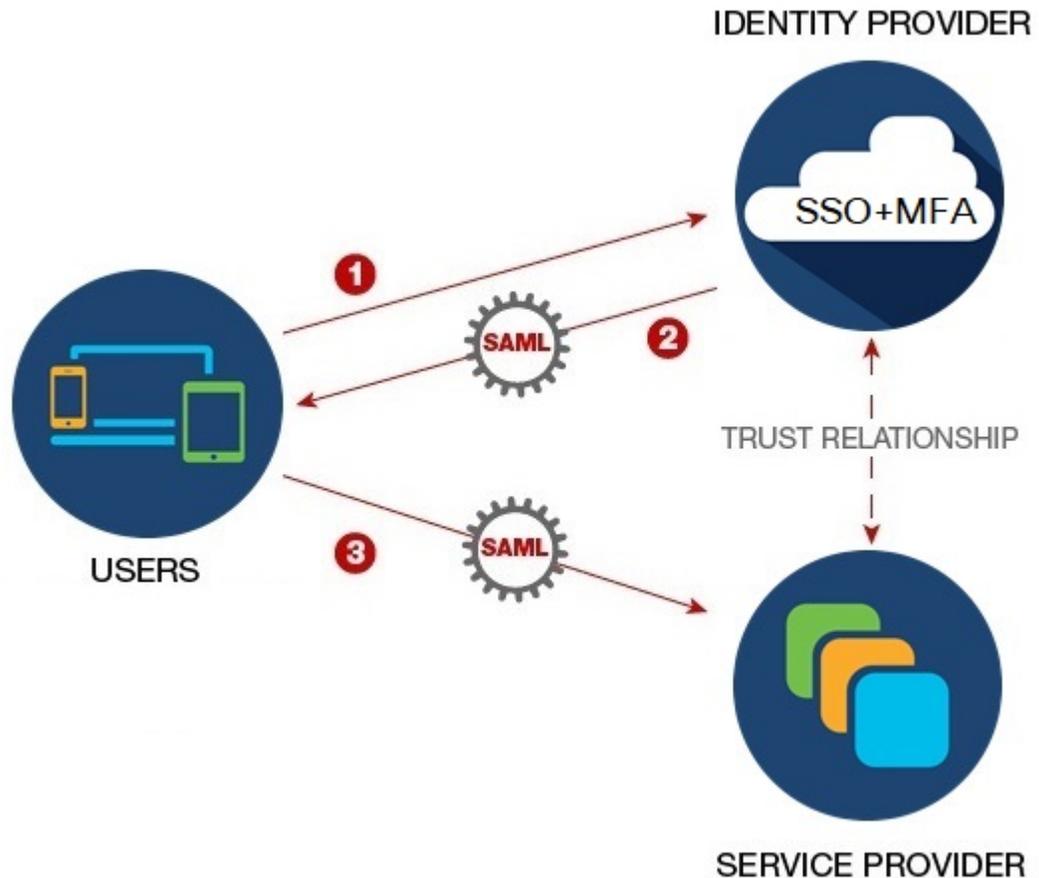
- [개요, 1 페이지](#)
- [운영 방식, 2 페이지](#)

## 개요

Cisco SecureX 로그인을 사용하면 모든 디바이스에서 하나의 자격증명 집합으로 모든 Cisco Security 제품에 쉽게 액세스할 수 있습니다. 사용자 이름과 비밀번호를 사용하여 로그인하면 모든 Cisco Security 제품이 맞춤형 대시보드에 앱으로 표시됩니다.

- 앱을 클릭하면 Cisco Security 제품 전반에서 원활한 워크플로를 위해 자동으로 로그인됩니다. 더 이상 여러 비밀번호를 기억하고 복잡하게 사용할 필요가 없습니다.
- Duo MFA(Multi-Factor Authentication) 통합은 적응형, 계층화된, 간소화된 인증을 의미합니다. 푸시 알림 한 번, 탭 한 번으로 즉시 액세스

## 운영 방식



SAML(Security Assertion Markup Language)은 ID 제공자(IdP)와 SP(통신 사업자) 간에 인증 및 권한 데이터를 교환하기 위한 XML 기반의 개방형 표준입니다. SP와 IdP 간 교환을 하면 사용자의 ID와 권한을 확인합니다. 이렇게 하면 단일 자격 증명 집합을 사용하여 다른 애플리케이션에 로그인할 수 있게 됩니다. 각 애플리케이션 모두에 대해 별도의 SSO(Single Sign-On, 단일 인증)를 관리하는 것보다 사용자당 SSO(Single Sign-On, 단일 인증)를 관리하는 것이 더 쉽습니다.

1. 사용자는 Duo의 MFA와 통합된 Cisco SecureX 로그인인 SSO IdP에 로그인합니다.
2. IdP와 SP 사이에 신뢰 관계가 있습니다. IdP는 SP에 신뢰할 수 있는 사용자 관련 정보가 포함된 SAML 속성 어설션을 전달할 수 있습니다.
3. 사용자가 다른 애플리케이션을 실행하면, SP가 IdP에서 사용자 권한 부여 및 인증을 요청합니다. IdP에 대한 SSO가 성공했기 때문에, 사용자는 이제 추가 자격 증명을 기억하고 입력할 필요 없이 다른 모든 애플리케이션에 액세스할 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.