Cisco Cloud Sign-On을 사용한 Secure Access Migration Single Sign-On 인증 컨피그레이션

목차

문제

Umbrella에서 보안 클라우드 제어로 마이그레이션하는 동안 관리 SSO(Single Sign-On) 동작이 예기치 않게 변경되었습니다. 이전에 구성한 Microsoft Centera ID를 인증 및 MFA에 사용하는 대신 관리자는 DUO를 통한 Cisco Cloud Sign-On을 사용하여 인증해야 했습니다. 이로 인해 관리자는 새 비밀번호를 설정하고 다단계 인증을 위해 DUO에 등록하라는 프롬프트를 받게 됩니다.

환경

- 기술: 보안 액세스(이전 Umbrella)
- 마이그레이션: 보안 클라우드 제어를 위한 우산
- 인증: ID 공급자로 구성된 Microsoft Azure AD(Enterprise ID)
- Multi-Factor Authentication: Microsoft 365 MFA가 이전에 구성됨
- 새 인증 방법: DUO를 통한 Cisco 클라우드 로그인

해결

Microsoft Entra ID에서 Cisco Cloud 로그인으로 인증 마이그레이션은 Secure Access 마이그레이션 프로세스 중에 발생하는 필수 단계입니다. SAML UI 인증을 올바르게 구성하려면 다음 단계를 수행해야 합니다.

1단계: 보안 액세스 마이그레이션 완료

Secure Access에서 SAML UI 인증을 구성하기 전에 전체 Secure Access 마이그레이션을 완료합니다. 이렇게 하면 모든 구성 요소가 제대로 마이그레이션되고 인증 컨피그레이션을 수행할 준비가

됩니다.

2단계: 보안 클라우드 제어를 통해 SAML 인증 구성

이제 SAML UI 인증 컨피그레이션이 Secure Access 내에서 직접 관리되지 않고 SCC(Security Cloud Control) 인터페이스를 통해 관리됩니다. Security Cloud Control(보안 클라우드 제어) > Authentication Settings(인증 설정)로 이동하여 ID 제공자 컨피그레이션 옵션에 액세스합니다.

3단계: ID 공급자 컨피그레이션 검토

Security Cloud Control 페이지에서 ID 제공자 컨피그레이션을 검토하고 검증합니다. 새 환경에 대해 Microsoft Entra ID 통합이 올바르게 구성되었는지 확인합니다.

원인

인증 동작 변경은 Umbrella에서 Secure Access로의 필수 마이그레이션 프로세스의 일부입니다. 이 마이그레이션 과정에서 SAML 인증이 Microsoft Entra ID에서 Cisco Cloud Sign-On으로 자동 전환되므로 다단계 인증에 DUO가 필요합니다. 이는 인증 설정이 개별 제품 인터페이스 내에서가 아니라 보안 클라우드 제어를 통해 중앙에서 관리되는 새로운 Secure Access 플랫폼의 필수 아키텍처 변경입니다.

관련 콘텐츠

- ID 제공자 통합
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.