

Duo SAML 통합으로 보안 액세스 RAVPN 인증에 실패했습니다.

목차

문제

Duo를 IDP(Identity Provider)로 사용하여 Cisco RAVPN(Secure Access Remote Access VPN)에 연결하려고 할 때 Active Directory가 백그라운드로 통합되면 사용자는 Duo 포털 수준에서 인증에 성공하더라도 인증 실패가 발생합니다.

구체적인 증상은 다음과 같습니다.

- Duo 포털은 인증에 대한 성공 메시지를 표시합니다.
- Cisco SecureClient는 Duo 성공 직후 "인증 실패" 오류 메시지를 표시합니다.
- Duo 로그는 "액세스 권한 부여" 상태를 표시합니다.
- Cisco Secure Access 포털 로그에 "AAA 실패" 상태가 표시됩니다.

이렇게 하면 외부 ID 공급자가 성공적인 인증을 확인하지만 VPN 클라이언트가 Secure Access 인프라 내의 인증 유효성 검사 실패로 인해 연결을 설정할 수 없는 연결이 끊어집니다.

환경

- Cisco Secure Access RAVPN 구축
- Duo Security as SAML Identity Provider
- Duo와 Active Directory 통합
- VPN 연결을 위한 Cisco SecureClient
- SAML 기반 인증 흐름

해결

Duo와 Cisco Secure Access 간의 사용자 특성 매핑을 수정하여 인증 실패를 해결했습니다. 다음 섹션에 설명된 단계를 수행하여 문제를 파악하고 해결했습니다.

1단계: 활동 검색 확인

1.- Cisco Secure Access Dashboard에 로그인합니다. Monitor(모니터) > Remote Access Logs(원격 액세스 로그)를 클릭합니다.

2.- 권한 부여 확인 실패 메시지 아래의 사용자 이름 필드를 확인합니다.

3.- Connect(연결) > User and Groups(사용자 및 그룹)에서 UPN 값과 일치시킵니다.

Cisco Secure Access는 권한 부여 확인을 위해 User Principal Name 값을 확인합니다.

Duo에서 전달되는 사용자 계정 이름이 User and Groups(사용자 및 그룹)에서 해당 사용자의 사용자 계정 이름 값과 일치하지 않습니다.

조사 결과:

- 사용자 이메일 주소: user@gmail.com
- 사용자 계정 이름(UPN 사용자 이름)

2단계: Duo 컨피그레이션 조정

올바른 사용자 특성 매핑을 보장하기 위해 Duo SAML 컨피그레이션을 수정하는 과정이 포함되어 있습니다.

- Duo Admin(듀오 관리) 패널에 액세스합니다.
- Cisco Secure Access용 SAML 애플리케이션 컨피그레이션으로 이동합니다.
- 사용자 특성 매핑을 수정하여 User and Groups(사용자 및 그룹)에서 해당 사용자의 User

Principal Name(사용자 계정 이름) 값과 일치해야 하는 이메일 주소를 전송합니다.

- 컨피그레이션 변경 사항을 저장합니다.

4단계: 확인

Duo 컨피그레이션을 조정한 후 인증 흐름을 테스트하고 성공적으로 검증했습니다. 사용자는 인증 실패 없이 원격 액세스 VPN을 사용하여 연결할 수 있었습니다.

원인

인증 실패의 근본 원인은 Duo SAML 어설션과 Cisco Secure Access 기대 간의 사용자 특성 매핑 불일치입니다. Duo는 SAML 어설션에서 UPN(User Principal Name)으로 사용자 이름을 전송하도록 구성된 반면 Cisco Secure Access는 사용자 이메일 주소를 예상하도록 구성되었습니다. 이 불일치로 인해 Duo IDP 수준에서 인증에 성공했지만 Secure Access 수준에서 인증이 실패했으며, 그 결과 Secure Access에 "AAA 실패"가 로그인되었고 Duo 로그는 "액세스 허용"으로 나타났습니다.

관련 콘텐츠

- [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.