# EntraID로 빈 흰색 화면이 표시되는 보안 액세스 브라우저 기반 SAML 인증 문제 해결

## 목차

## 문제

Cisco Secure Client가 설치되지 않은 디바이스에서 브라우저 기반 SAML 인증을 강제하도록 Cisco Secure Access를 구성할 때 인증 프로세스가 EntraID 인증 페이지를 표시하는 대신 빈 흰색 화면으로 리디렉션됩니다. 이 문제는 특히 Microsoft Edge 일반(비 InPrivate) 모드 및 Google Chrome 브라우저에서 발생합니다. Edge InPrivate 모드를 사용하는 경우 인증이 올바르게 작동합니다. SAML 인증 프로파일에 Decryption(해독) 및 SSO Authentication(SSO 인증)이 모두 활성화되어 있습니다.

구성된 정책 구조에는 다음이 포함됩니다.

- 사후 인증 사용자에 대한 정책을 허용합니다. (출처: 모든 사용자, 대상: 모두)
- SAML 인증 프로파일을 사용하여 SAML 인증 정책을 허용합니다. (출처: 엔드포인트 IP, 대상: 0.0.0.0 TCP 80,443)
- SAML 인증 프로파일을 사용하여 SAML 인증 헬퍼 정책을 허용합니다. (출처: 엔드포인트 IP, 대상: 모두)
- 차단 정책. (출처: 엔드포인트 IP, 대상: 모두)

## 환경

- Cisco Secure Access(인터넷 액세스 모듈)
- IdP(ID 제공자)로서의 ID
- Cisco Secure Client가 없는 디바이스에 대한 브라우저 기반 SAML 인증
- 암호 해독 및 SSO 인증이 활성화된 SAML 인증 프로파일
- Microsoft Edge 및 Google Chrome 브라우저

# 해결

특정 EntraID 관련 도메인을 SAML 인증 프로파일 컨피그레이션의 암호 해독 제외 목록에 추가하여 문제를 해결합니다. 이렇게 하면 SSL/TLS 해독 프로세스가 EntraID 인증 흐름을 방해하지 않습니다.

## 1단계: 암호 해독 제외 목록에 EntraID 도메인 추가

SAML 인증 프로파일에 대한 암호 해독 제외 목록에서 다음 4개의 EntraID 도메인을 구성합니다.

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

## 2단계: SAML 정책에 컨피그레이션 적용

암호 해독 제외 설정이 다음 모두에 적용되는지 확인합니다.

- Allow SAML authentication(SAML 인증 허용) 정책. (출처: 엔드포인트 IP, 대상: 0.0.0.0 TCP 80,443)
- Allow SAML authentication helper(SAML 인증 헬퍼 허용) 정책. (출처: 엔드포인트 IP, 대상: 모두)

## 3단계: 해결 확인

암호 해독 제외 컨피그레이션을 적용한 후 인증 흐름을 테스트합니다.

- Microsoft Edge(일반 모드): EntraID 인증 페이지로 리디렉션할 수 있습니다.
- Google Chrome: EntraID 인증 페이지로 리디렉션할 수 있습니다.

- 두 브라우저 모두 EntraID 인증 입력 화면을 일관되게 표시할 수 있습니다.

## 원인

빈 흰색 화면은 SAML 인증 프로파일에 대해 암호 해독이 활성화된 경우 Cisco Secure Access의 SSL/TLS 암호 해독 프로세스가 EntraID 인증 플로우를 방해하기 때문에 발생합니다. 암호 해독 프로세스는 브라우저와 EntraID 인증 서버 간의 보안 통신을 중단하여 인증 페이지가 제대로 로드되지 않도록 합니다. InPrivate 모드는 해독 간섭을 우회하여 SSL/TLS 세션을 다르게 처리하기 때문에 작동합니다. EntraID 도메인을 암호 해독 제외 목록에 추가하면 암호 해독 없이 인증 트래픽이 통과할 수 있으므로 보안 인증 흐름의 무결성이 유지됩니다.

## 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.