

보안 액세스를 위한 SAML(Security Assertion Markup Language) 인증서 갱신(연간 조치 필요)

목차

- [소개](#)
 - [문제](#)
 - [솔루션](#)
 - [Azure SAML 인증서 설정](#)
 - [관련 정보](#)
-

소개

이 문서에서는 보안 액세스를 위한 SAML 인증서 갱신 프로세스의 프로세스를 설명합니다.

문제

만료 날짜(매년 6월 만료 기간) 전에 새 SAML(Security Assertion Markup Language) 인증서로 IdP(Identity Provider)를 업데이트해야 합니다. 아래에 제공된 Secure Access SAML 메타데이터 URL을 모니터링하도록 IDP가 이미 구성되어 있지 않은 경우 이러한 사용자의 SAML 사용자 인증 실패와 인터넷 액세스 손실을 방지하려면 이 인증서를 업데이트하는 것이 중요합니다.

솔루션

1단계: SAML IDP 요청 서명 검증이 비활성화되었는지 확인합니다. 이 옵션을 비활성화하면 추가 작업이 필요하지 않습니다. 프로세스의 나머지를 건너뛰고 SAML 서비스를 정상적으로 계속 사용할 수 있습니다.

2단계: SAML IDP가 서명 검증을 요청하는 경우 [Secure Access Documentation Page](#) -> Security Notices -> Security Advisories, Responses and Notices -> (Secure Access Notification - SAML Authentication Certificate Expiring)에서 새 인증서를 다운로드합니다.

3단계: SAML IDP에 로그인하고 현재 SAML 인증서를 교체합니다.

Azure SAML 인증서 설정

다음은 Azure SAML IDP 인증서를 대체하는 예입니다.

1단계: [Azure](#) 포털에 [로그인합니다](#).

2단계: SAML SSO 프로필을 찾은 다음 Edit(수정)를 클릭합니다.

3단계: (Single Sign On) 설정에서 Certificate Signing Request Validation(인증서 서명 요청 검증)이 있는지 확인합니다.

A. 검증이 비활성화되어 있습니다(조치가 필요하지 않음).

The screenshot shows the 'SAML Certificates' configuration page. Under the 'Token signing certificate' section, the 'Status' is 'Active', 'Expiration' is '8/16/2026, 2:27:38 PM', and 'Notification Email' is redacted. Below this, the 'Verification certificates (optional)' section is highlighted with a red box. It shows 'Required' is 'No', 'Active' is '0', and 'Expired' is '0'. There are 'Download' links for 'Certificate (Base64)', 'Certificate (Raw)', and 'Federation Metadata XML'. An 'Edit' link is visible for both the token signing certificate and the verification certificates section.

B. 유효성 검사가 활성화되었습니다(인증서 교체 필요).

The screenshot shows the 'SAML Certificates' configuration page. Under the 'Token signing certificate' section, the 'Status' is 'Active', 'Expiration' is '8/29/2026, 1:22:38 PM', and 'Notification Email' is redacted. Below this, the 'Verification certificates (optional)' section is highlighted with a red box. It shows 'Required' is 'Yes', 'Active' is '1', and 'Expired' is '0'. There are 'Download' links for 'Certificate (Base64)', 'Certificate (Raw)', and 'Federation Metadata XML'. An 'Edit' link is visible for both the token signing certificate and the verification certificates section.

4단계: Verification certificate(확인 인증서) 옵션을 수정합니다.

5단계: ([Secure Access Documentation 페이지](#))에서 참조한 공지에서 찾을 수 있는 새 SAML 인증을 업로드합니다.

Verification certificates



ⓘ Requiring verification certificates will impact certain admin and end-user experiences, such as the Single sign-on testing feature, and the My Apps and M365 app launcher experiences. [Learn more](#)

Verification certificates are used to verify requests coming from this application to Microsoft Entra ID.

[Learn more](#)

Require verification certificates

Allow requests signed with RSA-SHA1

[Upload certificate](#)

Thumbprint	Key Id	Start date	Expiration date	
43C5538D5E386F6CF372BC4...	3367a479-945c-46f9...	5/13/2024, 2:01 AM	5/13/2025, 2:00 AM	...

관련 정보

- [Secure Access 설명서](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.