Update Secure Access SAML VPN Authentication Certificate (Service Provider Certificate)(보안 액세스 SAML VPN 인증 인증서 업데이트(서비스 공급자 인증서))

목차

소개

배경 정보

사전 요구 사항

- 요구 사항

Cisco Secure Access 대시보드

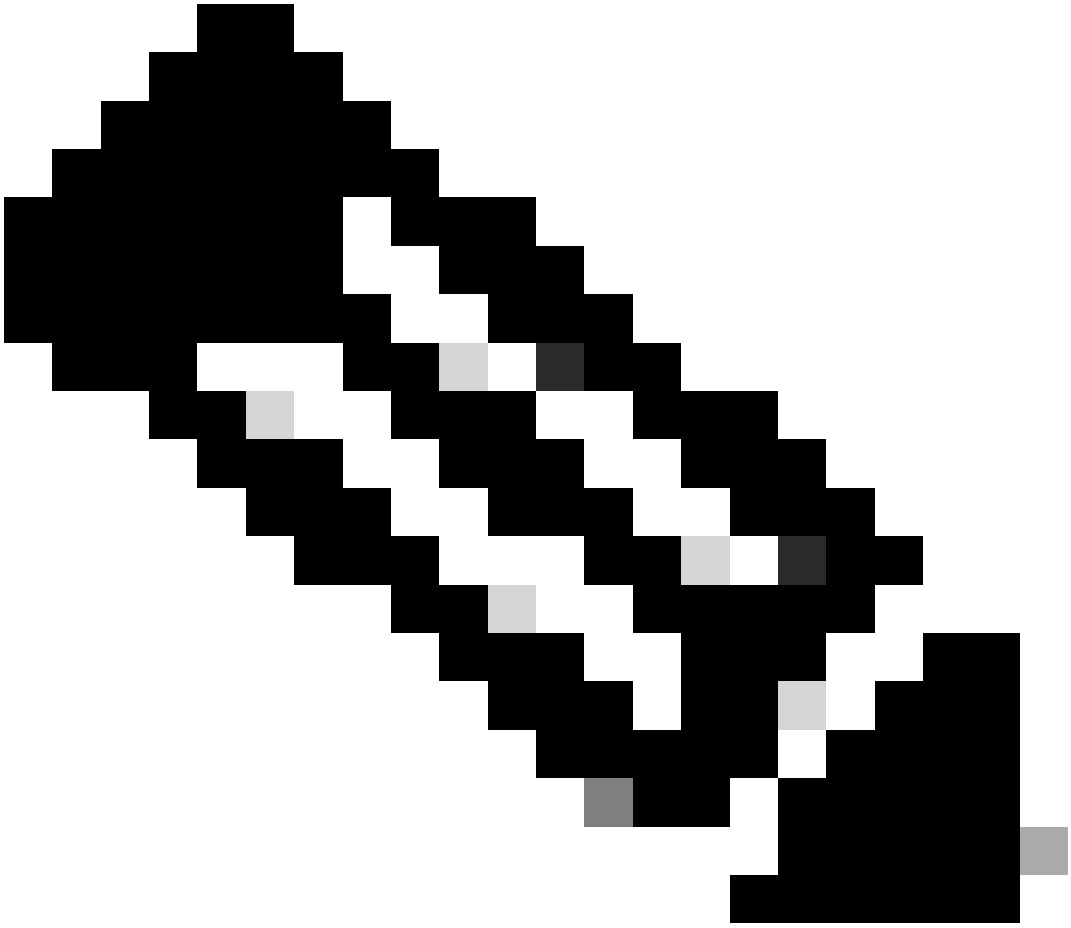
Microsoft Entra ID(Microsoft Azure)

소개

이 문서에서는 IdP(Identity Provider) 인증서를 새 Secure Access Service Provider Certificate로 업데이트하는 데 필요한 단계를 설명합니다.

배경 정보

VPN(Virtual Private Network) 인증에 사용되는 Cisco SAML(Secure Access Security Assertion Markup Language) 인증서는 곧 만료되며, 이 인증서의 유효성을 검사할 경우 VPN 사용자를 인증하는 데 사용되는 현재 IdP로 업데이트할 수 있습니다.
이에 대한 자세한 내용은 Secure Access Announcements 섹션에서 확인할 수 있습니다.



참고: 대부분의 IdP는 기본적으로 이 SAML 인증서를 확인하지 않으며 이는 요구 사항이 아니므로 IdP에서 추가 작업이 필요하지 않습니다. IdP에서 보안 액세스 인증서를 검증하는 경우 IdP 컨피그레이션에서 보안 액세스 인증서 업데이트를 계속 진행합니다.

이 문서에서는 구성된 IdP가 인증서 검증을 수행하는지 확인하는 단계를 다룹니다. Entra ID(Azure AD), PingIdentity, Cisco DUO, OKTA입니다.

사전 요구 사항

요구 사항

- Cisco Secure Access Dashboard 액세스
- IdP 대시보드 액세스

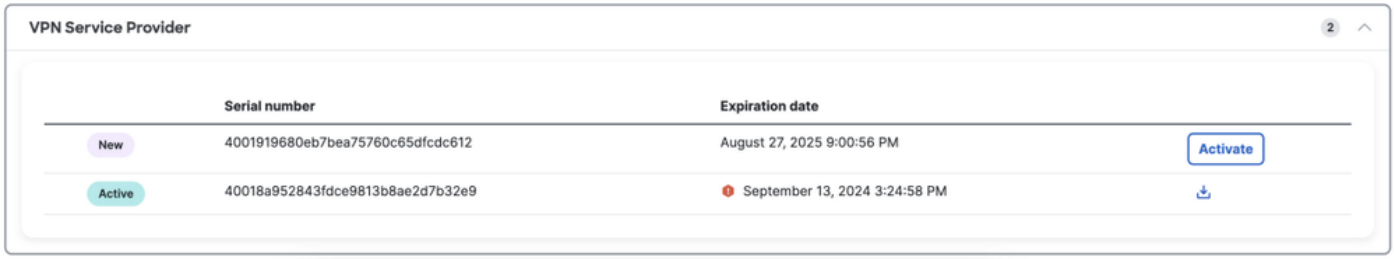
Cisco Secure Access 대시보드

참고: 새 보안 액세스 인증서를 활성화하는 다음 단계를 수행한 후 IdP가 이 인증서 검증을 수행하는 경우 새 인증서로 IdP를 업데이트하십시오. 그렇지 않으면 원격 액세스 사용자에 대한 VPN 인증이 실패할 수 있습니다.

IdP가 이 인증서 검증을 수행하는지 확인하는 경우 Secure Access에서 새 인증서를 활성화하고 근무 외 시간에 IdP에 업로드하는 것이 좋습니다.

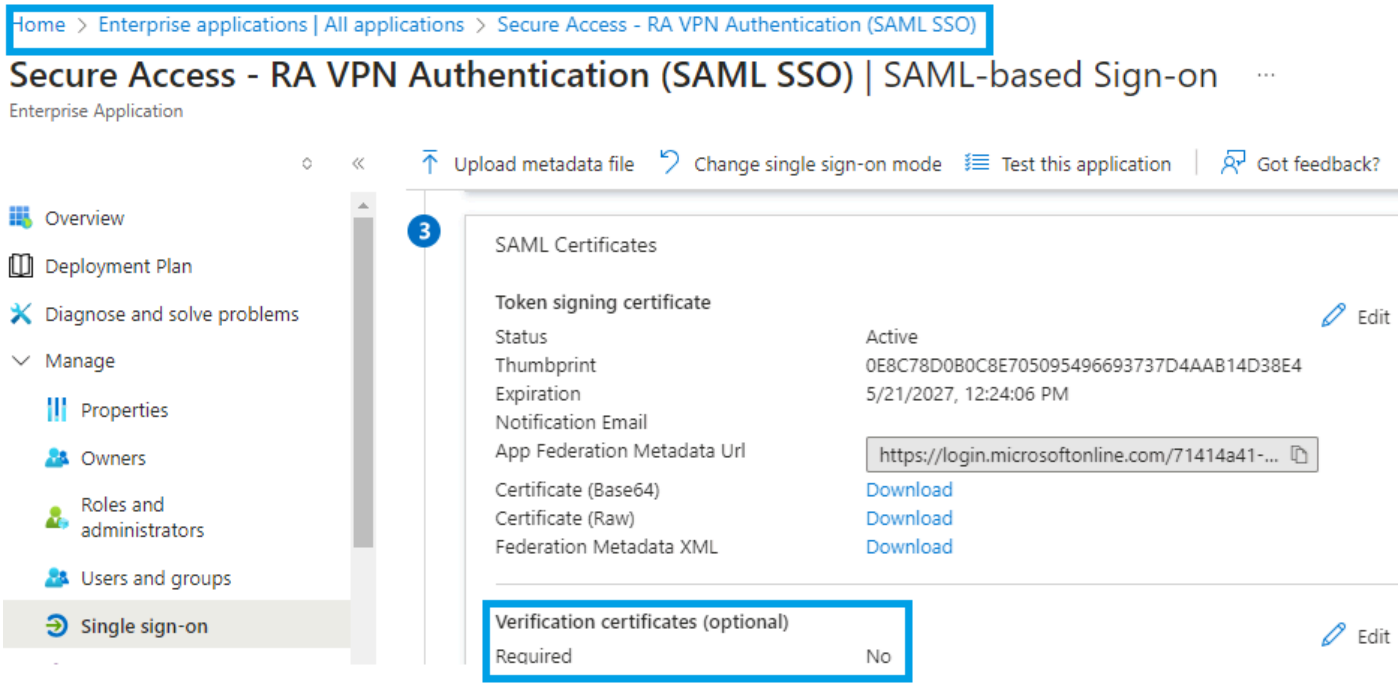
Secure Access Dashboard(보안 액세스 대시보드)에서 필요한 유일한 작업은 Secure(보안) > Certificates(인증서) > SAML Authentication(SAML 인증) > Service Provider certificates(서비스 공급자 인증서)로 이동한 다음, "New(새로 만들기)" 인증서에서 "Activate(활성화)"를 클릭합니다.

Activate(활성화)를 클릭하면 New Secure Access(새 보안 액세스) 인증서를 다운로드하여 인증서 검증을 수행하는 경우 IdP에서 가져올 수 있습니다.

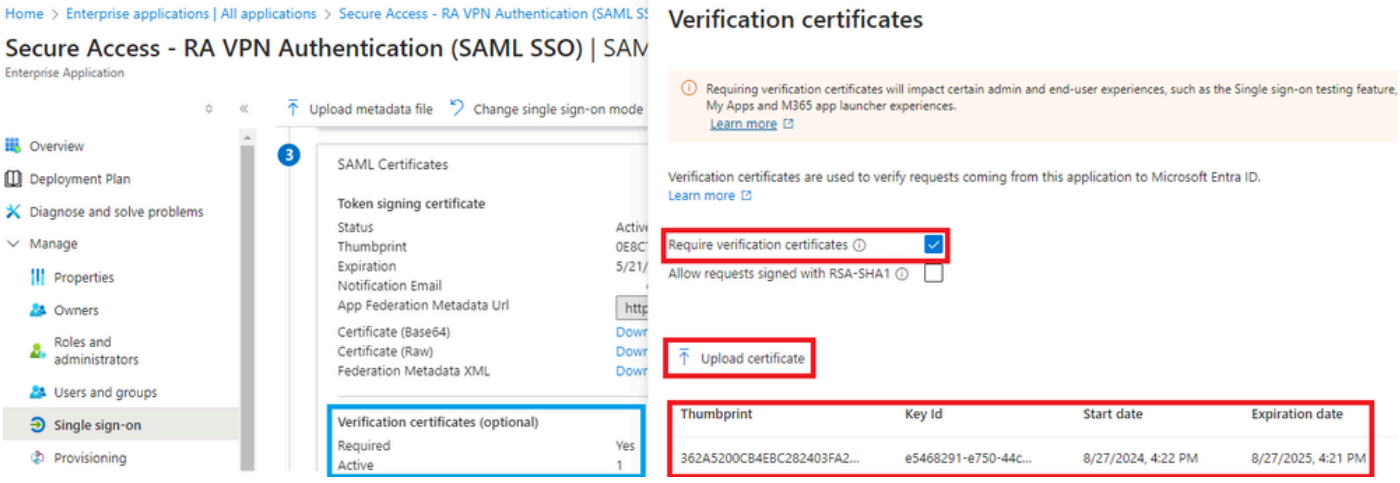


Microsoft Entra ID(Microsoft Azure)

기본적으로 인증서 유효성 검사를 수행하지 않는 ID(Azure AD)입니다.

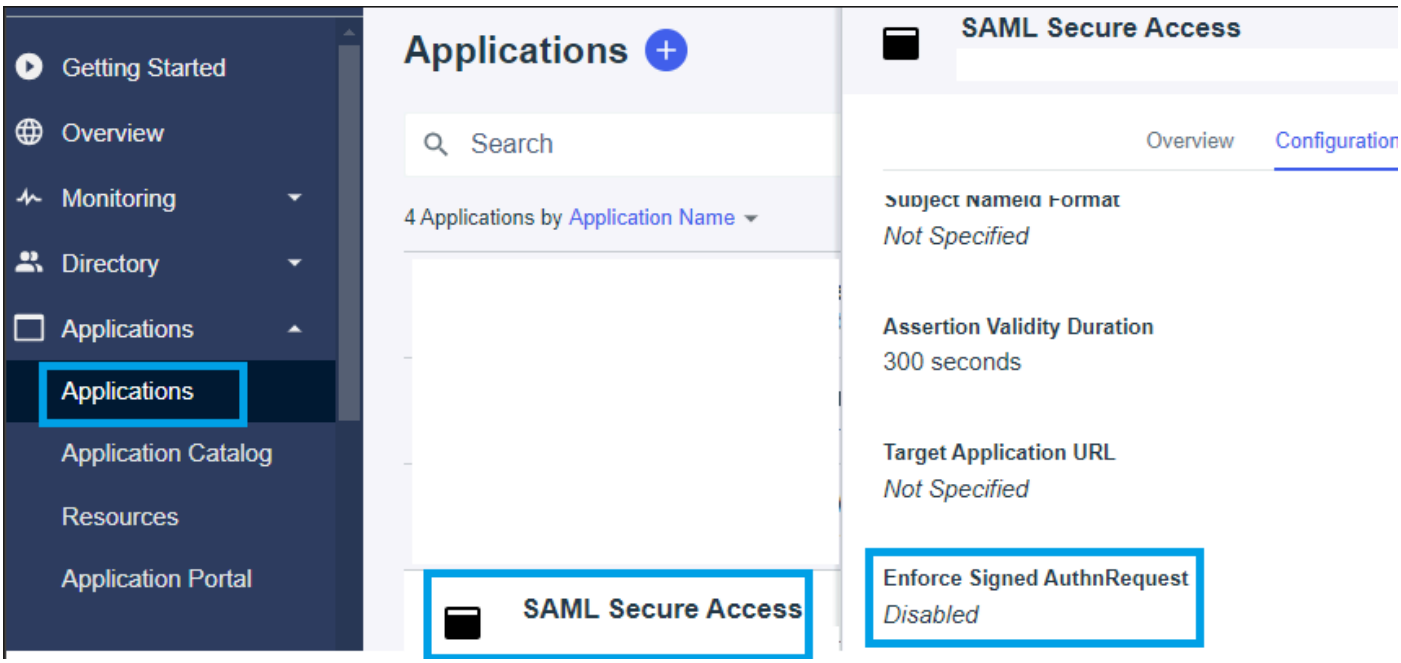


IdP Entra ID 값 "Verification Certificate (optional)(확인 인증서(선택 사항))"가 "Required = yes(필수 = 예)"로 설정된 경우 Edit(편집) 및 "Upload certificate(인증서 업로드)"를 클릭하여 새 Secure Access SAML VPN 인증서를 업로드합니다.

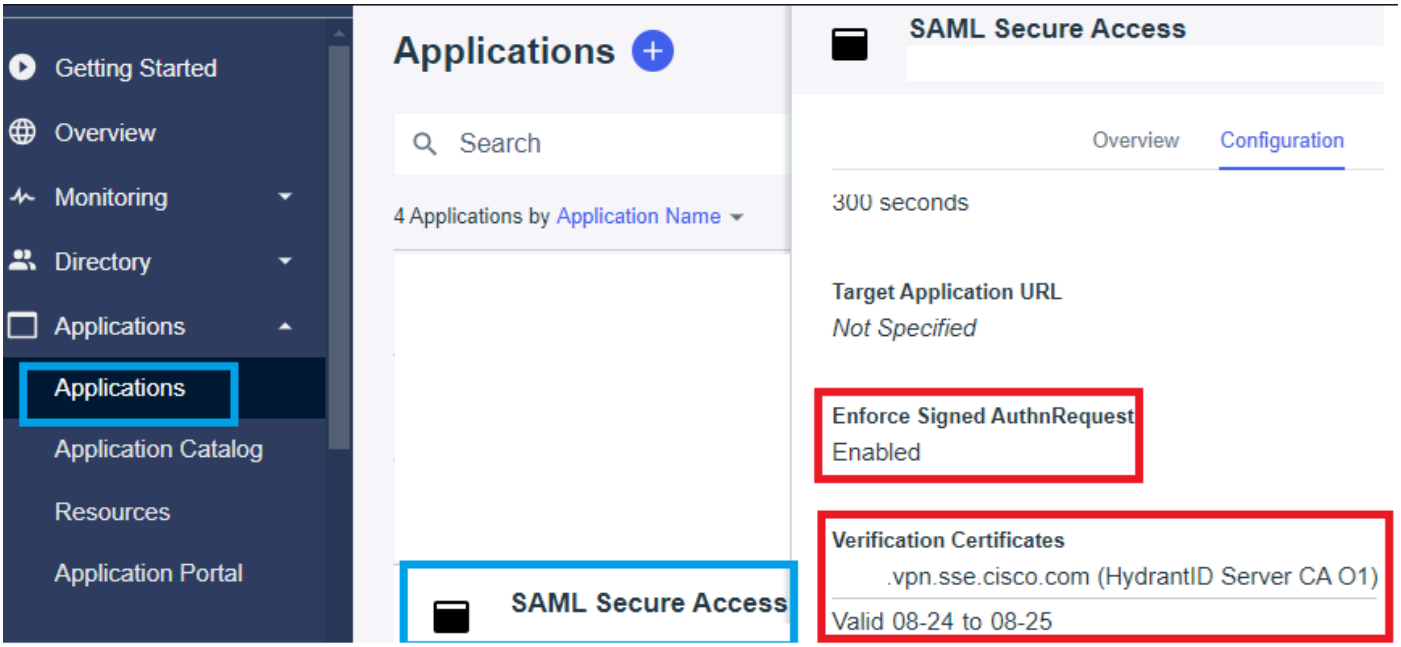


PingID

PingIdentity는 기본적으로 인증서 검증을 수행하지 않습니다.



IdP Pingidentity에서 Enforce Signed AuthnRequest 값이 "Enabled(활성화됨)"로 설정된 경우 Edit(편집)를 클릭하고 새 Secure Access SAML VPN Certificate(보안 액세스 SAML VPN 인증서)를 업로드합니다.



Cisco 듀오

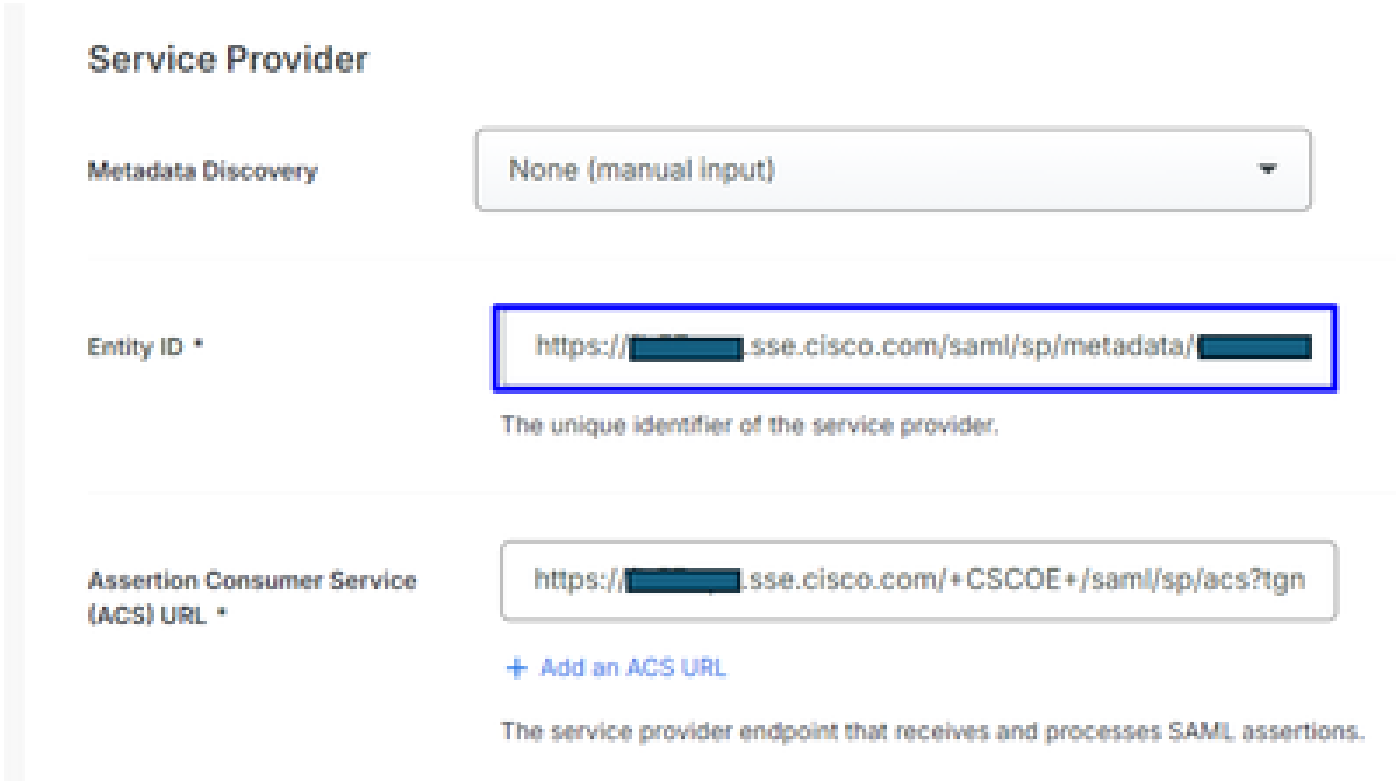
Cisco DUO는 기본적으로 서명 요청 검증을 수행하지만, Assertion Encryption이 활성화되어 있지 않으면 DUO 자체에 대해 수행할 작업이 필요하지 않습니다.

요청 서명을 위해 DUO는 관리자가 제공한 메타데이터 엔티티 ID 링크를 사용하여 새 인증서를 다운로드할 수 있습니다.

서명 응답 및 어설션 작업

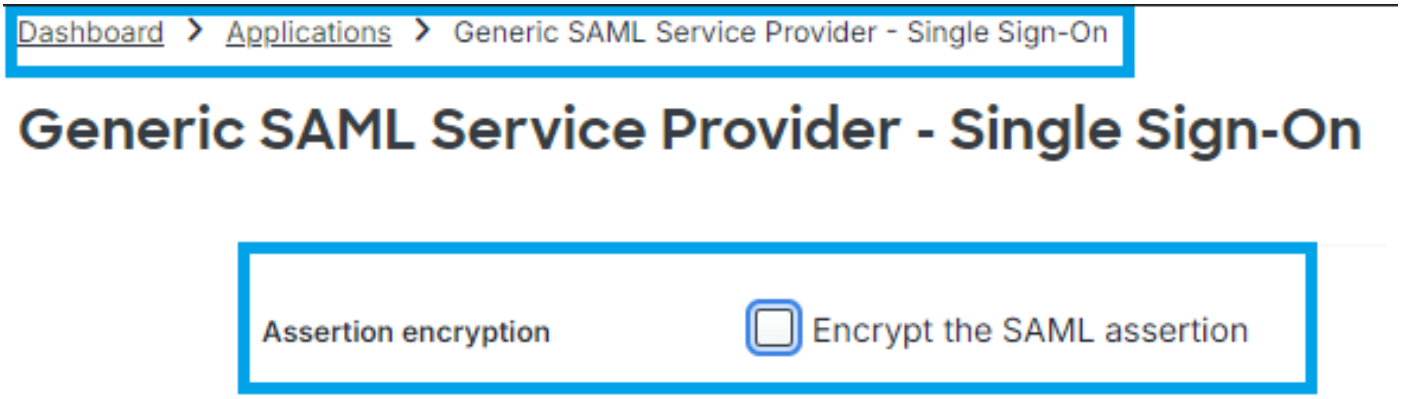
엔터티 ID 설정

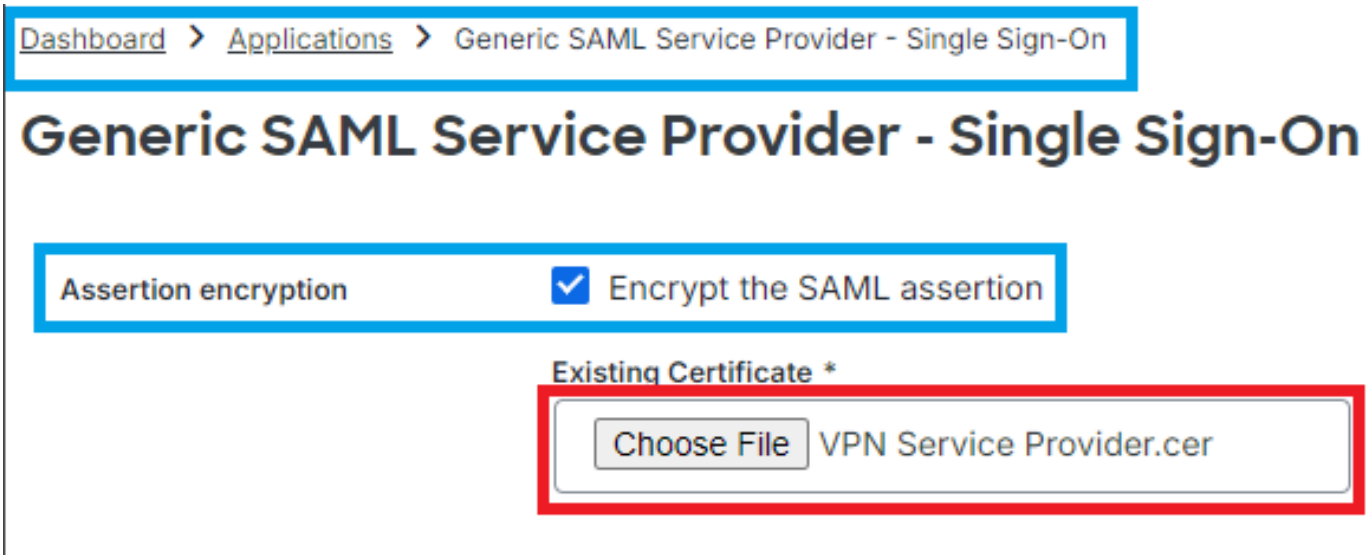
이 단계에서 필요한 작업은 없습니다. DUO는 Entity ID Link(https://<entry-id>.vpn.sse.cisco.com/saml/sp/metadata/<profile_name>)에서 새 인증서를 가져올 수 있습니다.



어설션 암호화

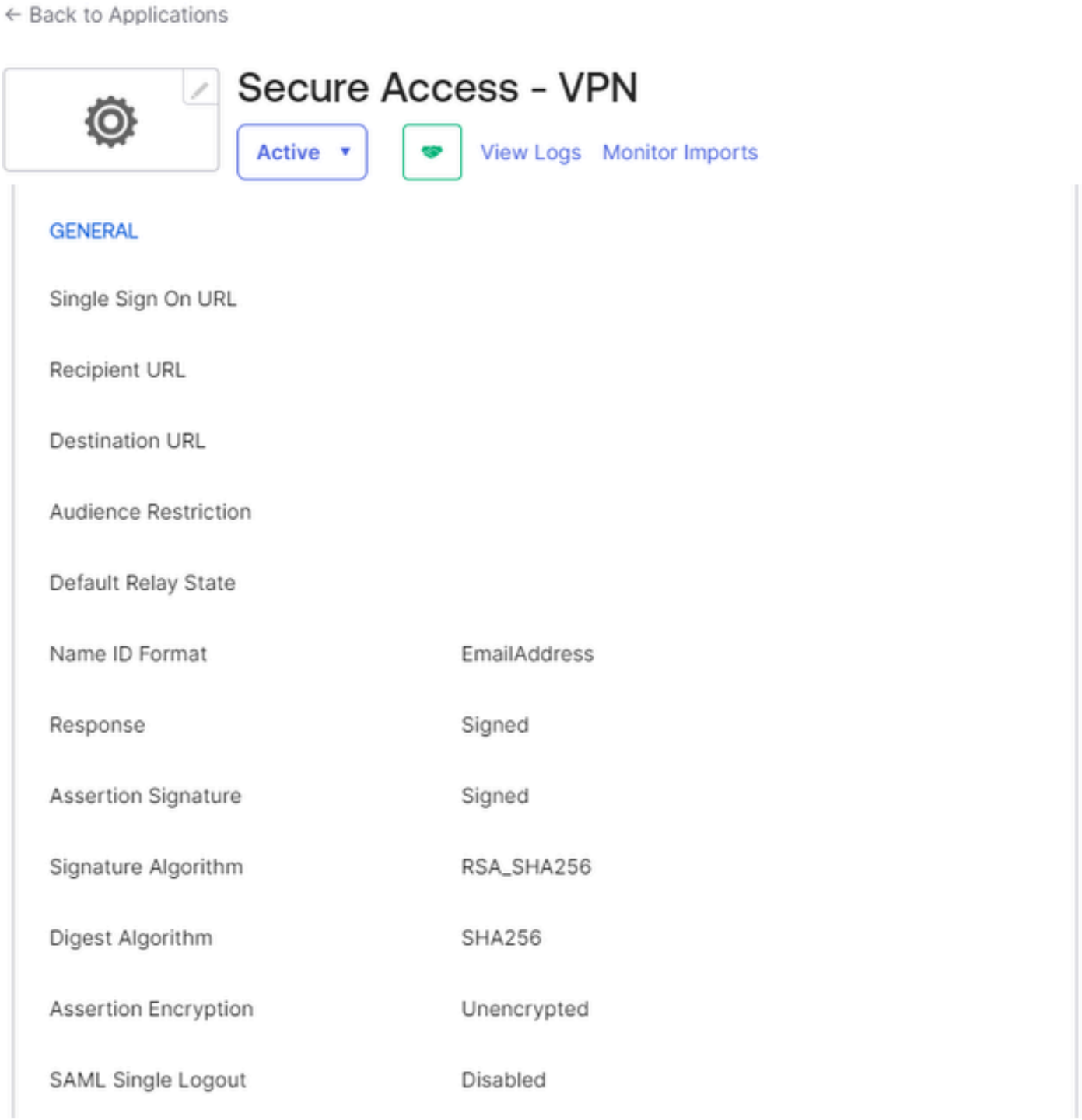
IdP Cisco DUO에서 "Assertion encryption" 값에 "Encrypt the SAML Assertion(SAML 어설션 암호화)"이 표시된 경우 "choose File(파일 선택)"을 클릭하고 새 Secure Access SAML VPN 인증서를 업로드합니다.



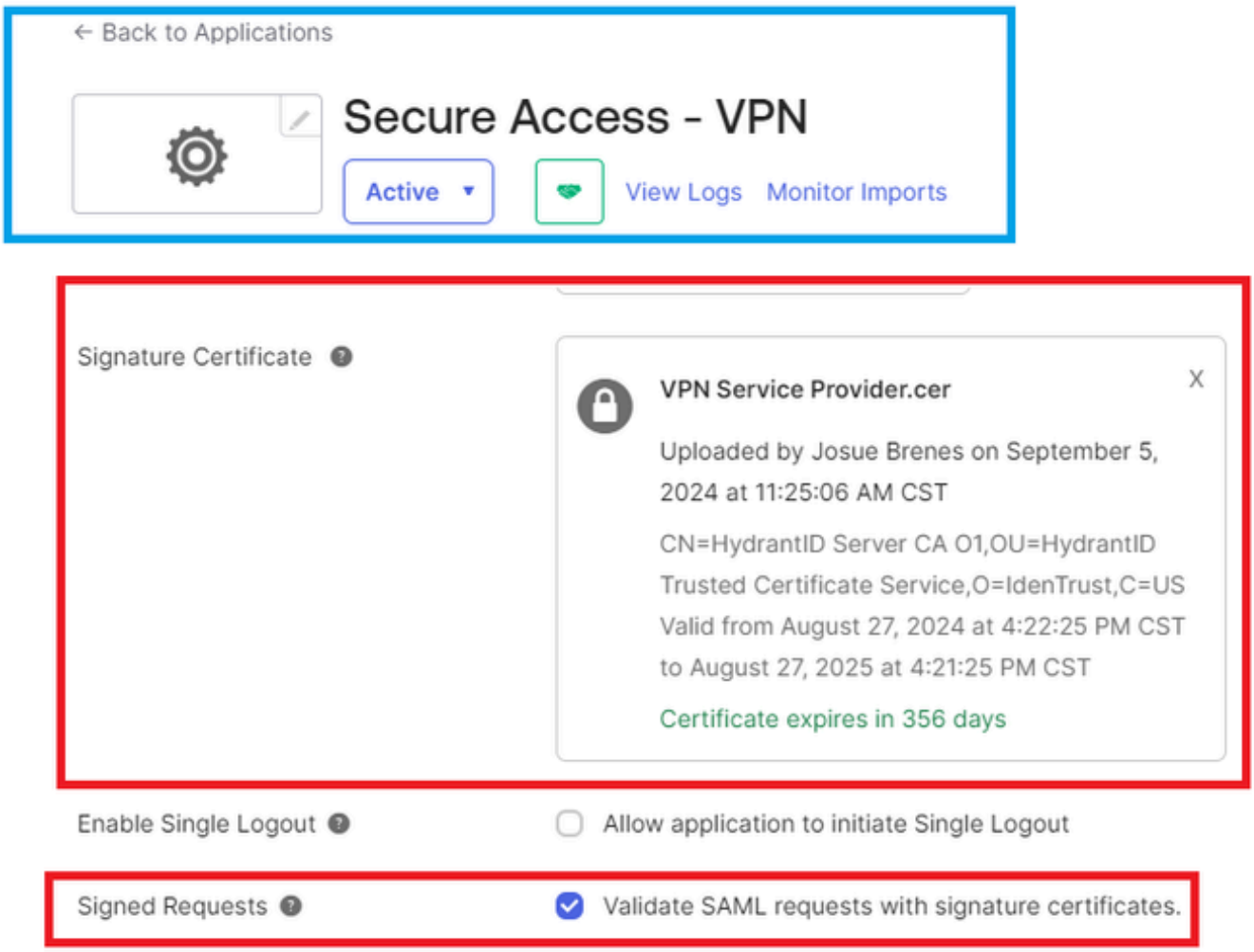


옥타

OKTA는 기본적으로 인증서 검증을 수행하지 않습니다. General(일반) > SAML Settings(SAML 설정)에는 "Signature Certificate(서명 인증서)"라는 옵션이 없습니다.



IdP OKTA에서 General(일반) > SAML Settings(SAML 설정) 아래에 "Signature Certificate Assertion encryption(서명 인증서 어설션 암호화)"이라는 값이 있으면 OKTA가 인증서 검증을 수행하고 있음을 의미합니다. "Edit SAML Settings(SAML 설정 수정)"를 클릭하고 Signature Certificate(서명 인증서)를 클릭한 다음 새 Secure Access SAML VPN Certificate(새 보안 액세스 SAML VPN 인증서)를 업로드합니다.



관련 정보

- Secure Access Help Center(사용 설명서)
- 기술 지원 및 문서 – Cisco Systems
- 보안 액세스 커뮤니티 페이지
- VPN용 새 보안 액세스 SAML 인증 인증서

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.