

Erneuern des SAML-Zertifikats (Security Assertion Markup Language) für sicheren Zugriff (jährliche Aktion erforderlich)

Inhalt

[Einleitung](#)

[Problem](#)

[Lösung](#)

[Azure SAML-Zertifikateinstellungen](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird der Prozess zur Verlängerung von SAML-Zertifikaten für sicheren Zugriff beschrieben.

Problem

Sie müssen Ihren Identitätsanbieter (IdP) vor dem Ablaufdatum (jährliches Ablaufdatum: Juni) mit dem neuen SAML-Zertifikat (Secure Access Security Assertion Markup Language) aktualisieren. Die Aktualisierung dieses Zertifikats ist wichtig, um Fehler bei der SAML-Benutzerauthentifizierung und den Verlust des Internetzugriffs für diese Benutzer zu vermeiden, es sei denn, Ihr IDP wurde bereits für die Überwachung der unten angegebenen SAML-Metadaten-URL für sicheren Zugriff konfiguriert.

Lösung

Schritt 1: Überprüfen Sie, ob die Validierung der Signatur Ihrer SAML-IDP-Anforderung aktiviert ist. Wenn diese Option deaktiviert ist, sind keine weiteren Aktionen erforderlich. Sie können den restlichen Prozess überspringen und die SAML-Dienste normal weiter verwenden.

Schritt 2: Wenn die Signaturvalidierung für SAML IDP-Anfragen erfolgt, laden Sie das neue Zertifikat von der [Secure Access Documentation Page](#) -> Security Notices -> Security Advisories, Responses and Notices -> (Secure Access Notification - SAML Authentication Certificate Expiring) herunter.

Schritt 3: Melden Sie sich bei Ihrem SAML IDP an, und ersetzen Sie das aktuelle SAML-Zertifikat.

Azure SAML-Zertifikateinstellungen

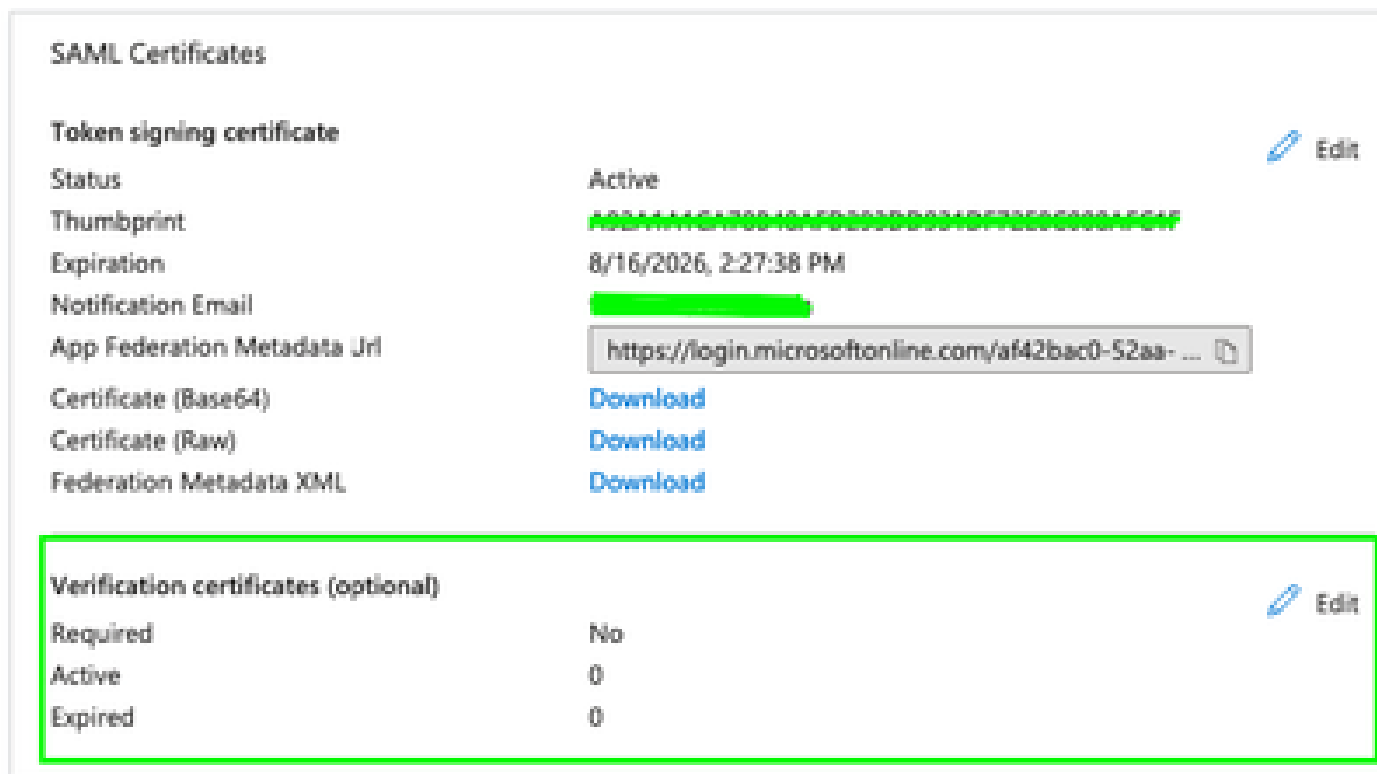
Dies ist ein Beispiel für das Ersetzen des Azure SAML IDP-Zertifikats.

Schritt 1: Melden Sie sich beim [Azure-Portal an](#).

Schritt 2: Suchen Sie Ihr SAML SSO-Profil und klicken Sie auf Bearbeiten.

Schritt 3: Überprüfen der Validierung von Zertifikatsanforderungen unter den Einstellungen für einmaliges Anmelden

A. Validierung ist deaktiviert (keine Aktionen erforderlich):



The screenshot displays the 'SAML Certificates' configuration page in the Azure portal. It is divided into two main sections: 'Token signing certificate' and 'Verification certificates (optional)'. The 'Token signing certificate' section shows a single active certificate with details such as its thumbprint, expiration date (8/16/2026), and notification email. Below these details are links to download the certificate in Base64, Raw, and Federation Metadata XML formats. The 'Verification certificates (optional)' section, highlighted with a red border, shows that certificate validation is not required, with zero active and zero expired certificates. An 'Edit' button is present for both sections.

SAML Certificates	
Token signing certificate Edit	
Status	Active
Thumbprint	[REDACTED]
Expiration	8/16/2026, 2:27:38 PM
Notification Email	[REDACTED]
App Federation Metadata Url	https://login.microsoftonline.com/af42bac0-52aa- ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download
Verification certificates (optional) Edit	
Required	No
Active	0
Expired	0

B. Validierung ist aktiviert (Ersetzen des Zertifikats ist erforderlich)

SAML Certificates

Token signing certificate Edit

Status: Active

Thumbprint: [REDACTED]

Expiration: 8/29/2026, 1:22:38 PM

Notification Email: [REDACTED]

App Federation Metadata Url: <https://login.microsoftonline.com/af42bac0-52aa-...>

Certificate (Base64): [Download](#)

Certificate (Raw): [Download](#)

Federation Metadata XML: [Download](#)

Verification certificates (optional) Edit

Required: Yes

Active: 1

Expired: 0

Schritt 4: Bearbeiten der Option für das Verifizierungszertifikat

Schritt 5: Laden Sie das neue SAML-Zertifikat hoch, das Sie in der Ankündigung finden, auf die in verwiesen wird ([Secure Access Documentation Page](#)).

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	...

Zugehörige Informationen

- [Dokumentation für sicheren Zugriff](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.