Renew Security Assertion Markup Language (SAML) Certificate for Secure Access (Annual Action Required)

Contents

Introduction

Problem

Solution

Azure SAML Certificate Settings

Related Information

Introduction

This document describes the process of SAML Certificate renewal process for Secure Access.

Problem

You must update your Identity provider (IdP) with the new Secure Access Security Assertion Markup Language (SAML) certificate before the expiration date (Annually Expired June time frame). Updating this certificate is essential to avoid SAML user authentication failures and loss of Internet access for these users, unless your IDP has already been configured to monitor the Secure Access SAML metadata URL provided below.

Solution

Step 1: Verify If your SAML IDP request signature validation, If this option is disabled, no further actions is required. you can skip the rest of the process and continue using the SAML services normally.

Step 2: If SAML IDP request signature validation, download the new certificate from the **Secure Access Documentation Page** **-> Security Notices -> Security Advisories, Responses and Notices -> (Secure Access Notification - SAML Authentication Certificate Expiring).**

Step 3: Login to your SAML IDP, and replace the current SAML Certificate.

Azure SAML Certificate Settings

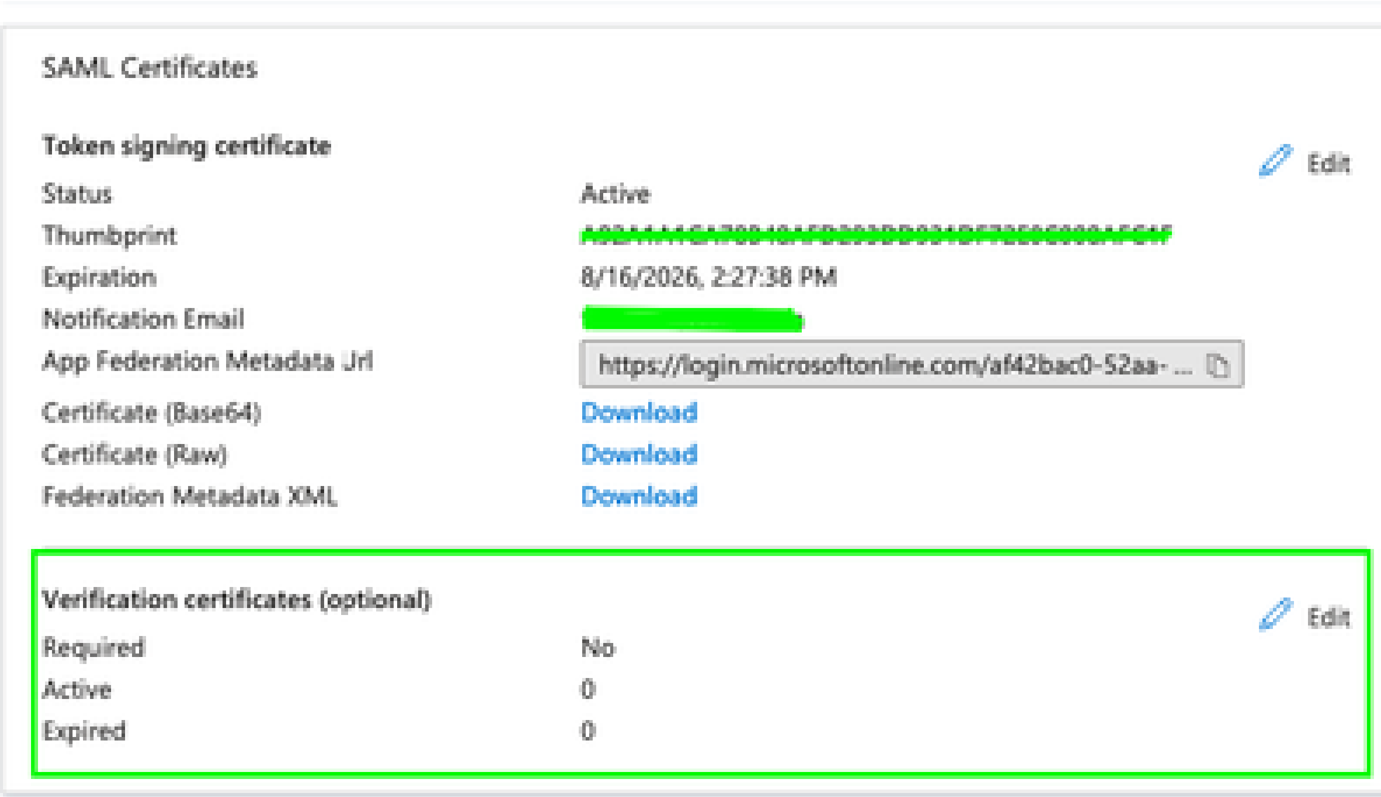
This is an Example of replacing Azure SAML IDP Certificate..

Step 1: Login to Azure Portal.

Step 2: Find your SAML SSO Profile and Click on Edit.

Step 3: Verify you have Certificate signing request validation under (Single Sign On) settings.

A. Validation is Disabled (No Actions Required):



SAML Certificates

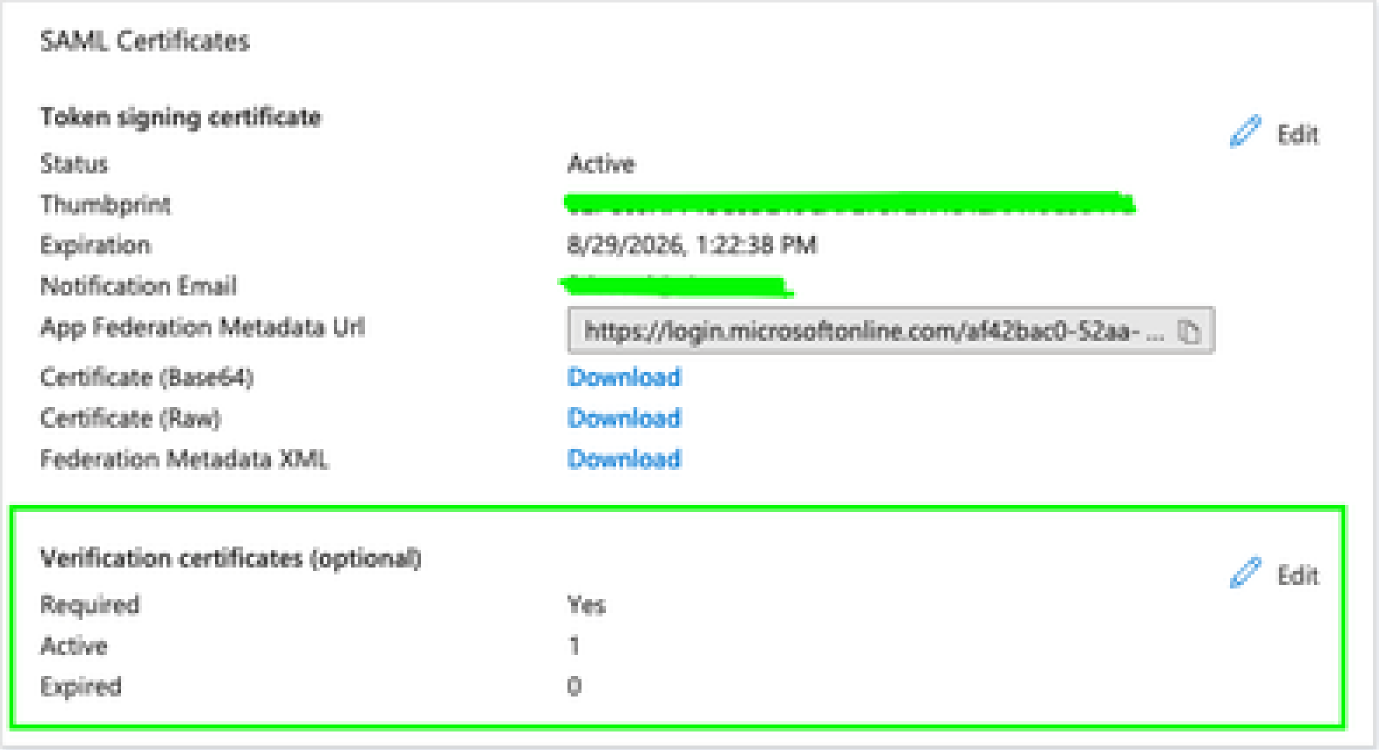
Token signing certificate

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)

Required	No
Active	0
Expired	0

B. Validation is Enabled (replacing certificate is required)



SAML Certificates

Token signing certificate

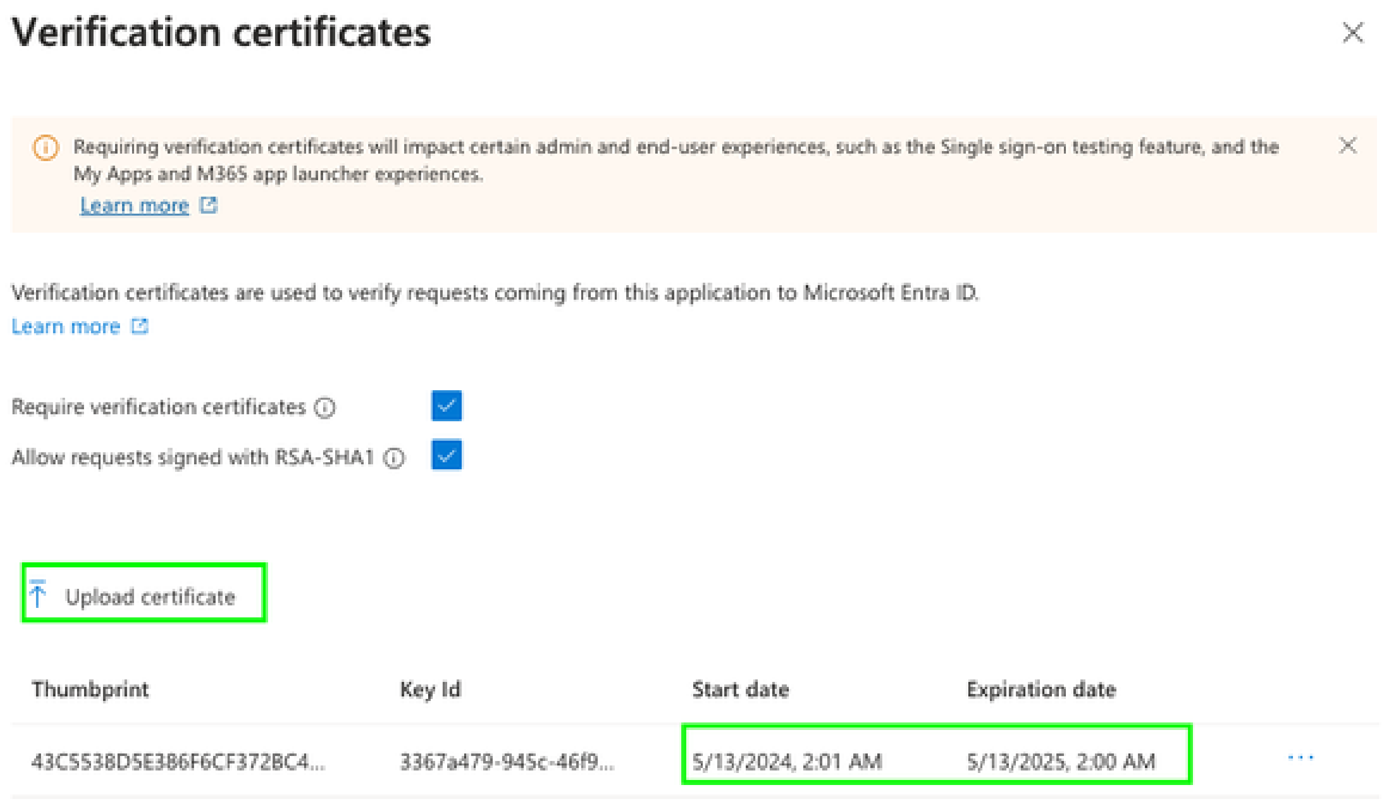
Status	Active
Thumbprint	[redacted]
Expiration	8/29/2026, 1:22:38 PM
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline.com/af42bac0-52aa- ...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	Yes
Active	1
Expired	0

Step 4: Edit the Verification certificate option.

Step 5: Upload the new SAML Certificate which can be found in the announcement referenced in (**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 ☑

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

Related Information

- [Secure Access Documentation]
- [Technical Support & Documentation - Cisco Systems]