SAML certificate expiration April 2024

Documentation

SAML certificate expiry

Information about verifying the signature certificate in your SAML configuration.

LumApps will replace the private certificate we use to sign SAML requests on Thursday, April 4th, 2024 at 10 am CET.

If you have activated the option to require the verification of the certificate signature in your Identity Provider, temporarily disable this option so that users can still log in to your LumApps platform with no issue.

Important: If the option to require the verification of the certificate signature is turned on after we update our certificate, users can no longer log in using the SAML login method.

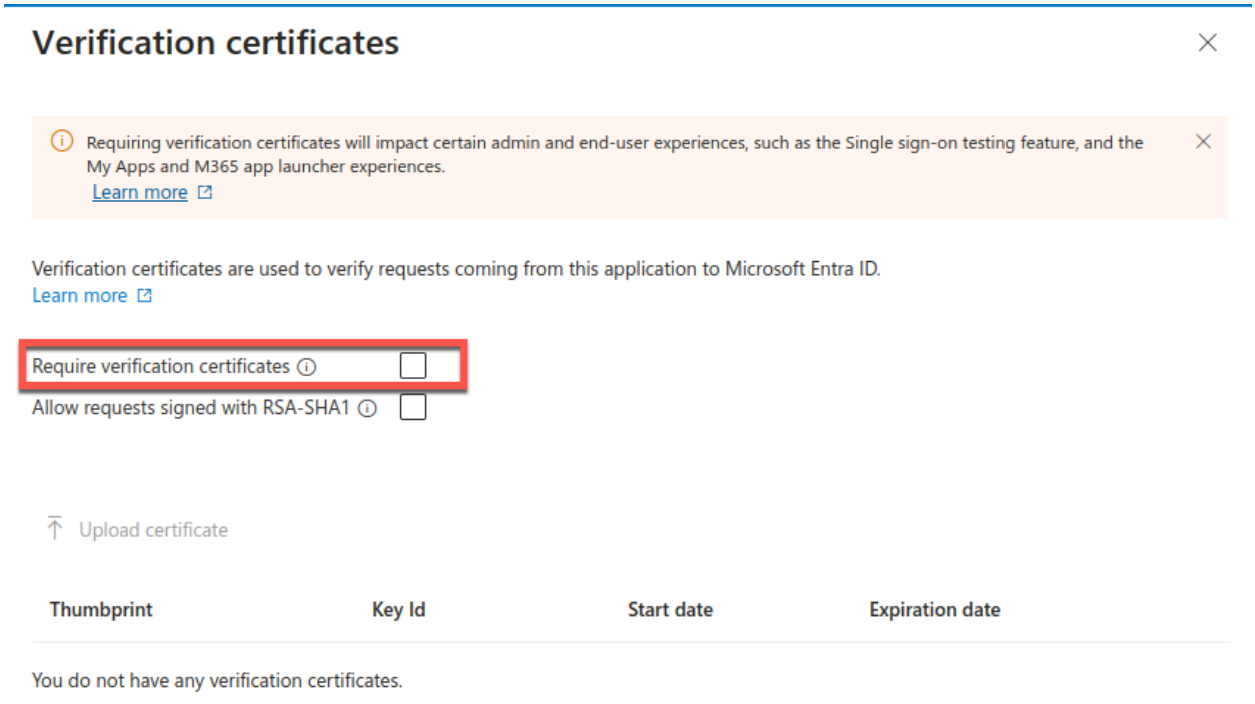
The following pages detail **how to remove certificate requirements in your provider**.

Remove certificate requirement for sign in - Microsoft Entra

Follow the steps on this page to enable login without requiring the certificate signature verification.

For more information about SAML signing certificates used in Microsoft Entra applications, refer to the Microsoft documentation: SAML Request Signature Verification and Tutorial: Manage certificates for federated single sign-on pages.

1. Go to your Azure AD administrator portal.
2. In the **Azure services** section, select **Enterprise applications**.
3. Search for and select your LumApps SAML application from the list.
4. In the side-menu, go to **Single Sign-on**.
5. Go to section 3 **SAML Certificates→ Verification certificates (optional)**.
6. Click **Edit**.
   Result: A side panel opens.
7. Ensure **Require verification certificates** is DISABLED.



Remove certificate requirement for sign in - Okta

Follow the steps on this page to enable login without requiring the certificate signature verification.

For more information, refer to the Okta documentation: Manage signing certificates.

1. Go to your Okta administration back office.
2. In the side-menu, go to **Applications→Applications**.
3. Search for and click the application you created for SAML login to LumApps.
4. Go to the **General** tab.
   Result: From this tab, you can verify if **SAML Signed Request** is enabled. If the setting is enabled, this indicates your application is using a signing certificate.
5. Click **Edit**.
6. Click **Next**.
7. Click **Show Advanced Settings**.
8. Ensure the **Signed Requests** check-box is NOT selected.
9. Save the configuration.