SAML SSO – Verify and Replace 2025 Self-Signed Certificate

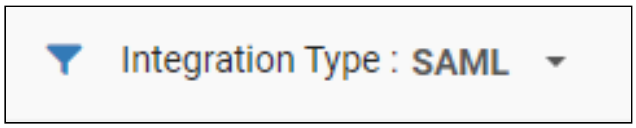
- **Product:** Alma, Primo VE, Leganto, Esploro, Rapido

The current self-signed SAML service provider certificate will expire in December 2025. If your institution uses this certificate, we recommend consulting with your IT department to determine whether a replacement is needed for Alma, Primo VE, or other applications. If so, the replacement should be coordinated with your identity provider administrators as detailed below.

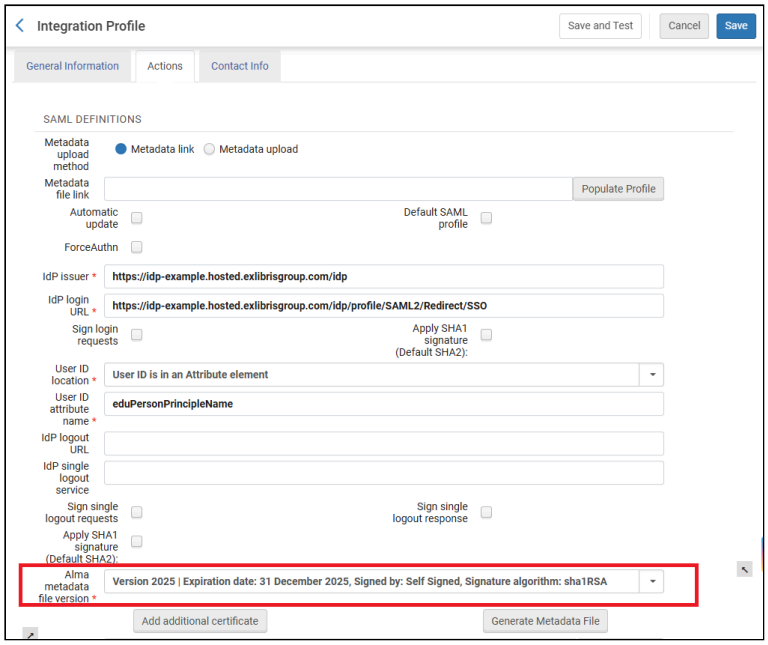
Instructions to Determine if you are Using the 2025 Self-signed Service Provider SAML Certificate

To determine if your Alma/Primo VE/Leganto/Esploro/Rapido application is using the 2025 self-signed service provider SAML certificate, which expires on December 31, 2025, follow these instructions:

1. Log in to the staff management module of your Alma/Primo VE/Leganto/Esploro/Rapido.
2. Go to the Integration Profile List screen (**Configuration > General > External Systems > Integration Profiles**).
3. From the filter 'Integration Type' drop-down options, choose **SAML**.



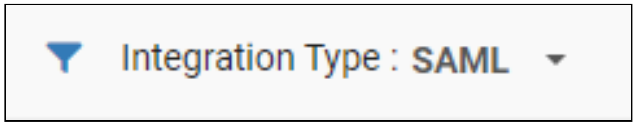
4. Locate the relevant Integration Profile and select **Edit** from the row actions.
5. In the Integration Profile screen, navigate to the **Actions** tab.
6. Verify if the 2025 self-signed SAML certificate is selected. Refer to the screenshot below as an example:



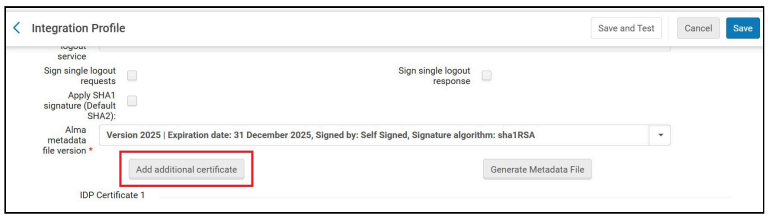
Instructions to Replace the 2025 Self-signed Service Provider SAML Certificate

To replace the 2025 self-signed service provider SAML certificate, which expires on December 31, 2025, follow these instructions:

1. Log in to the staff management module of your Alma/Primo VE/Leganto/Esploro/Rapido.
2. Go to the Integration Profile List screen (**Configuration > General > External Systems > Integration Profiles**).
3. From the filter 'Integration Type' drop-down options, choose **SAML**.



4. Locate the relevant Integration Profile and select **Edit** from the row actions.
5. In the Integration Profile screen, navigate to the **Actions** tab.
6. Click the **Add additional certificate** button.



7. In the New Alma metadata file version drop-down menu, select the Version 2030 certificate as shown in the following screenshot:

Note

UK Access Management Federation members should refer to the special instructions at the end of this document.

---

8. Click the **Save** button to save the changes.
9. Copy and modify the URL format below to construct the SAML Service Provider metadata URL using the new 2030 certificate:
   https://application_server_name/view/saml/metadata?VERSION=VERSION_2030
   Examples:
   Alma: https://myinstitutionID.alma.exlibrisgroup.com/view/saml/metadata?VERSION=VERSION_2030
   Primo VE (hosted server name): https://myinstitutionID.primo.exlibrisgroup.com/view/saml/metadata?VERSION=VERSION_2030
   Primo VE (custom server name): https://primo.library.myinstitution.edu/view/saml/metadata?VERSION=VERSION_2030

Note

A small number of institutions' SAML identity providers require signed login or logout requests. If your IdP has this requirement, please submit a support case so that we can assist you with the certificate replacement process. This procedure involves an additional step and a different method for providing the new SP metadata file.

---

10. Send the metadata file URL(s) to your SAML identity provider (IdP) administrators, and ask them to update the IdP configurations using the metadata files.
11. Once the IdP configurations are updated, test to ensure login is working.
12. After confirming that login is working, follow steps 1 to 5 to open the integration profile again.
13. Click the **Delete old certificate** button to remove the 2025 version certificate.
14. Click the **Save** button.
15. Test again to ensure that login is still working.

Note

If your institution uses the **Alma generic server name** for SAML login with **Alma or Primo VE**, and is a member of a SAML federation—such as the **InCommon Federation (U.S.)** or the **UK Access Management Federation** — we will be replacing the certificate for you. Therefore, please open a support ticket so we can coordinate with you to replace

---

the expiring certificate.

We are scheduled to update the federation service provider entries that use Alma generic server names during the week of **December 14, 2025**.

For your reference, here are some example SAML service provider entity IDs using Alma generic server names:

- https://na01.alma.exlibrisgroup.com/mng/login
- https://eu.alma.exlibrisgroup.com/mng/login
- https://sandbox01-na.alma.exlibrisgroup.com/mng/login
- https://sandbox02-eu.primo.exlibrisgroup.com/mng/login

If your institution uses custom host names and is a member of a SAML federation, our support team has already completed the certificate replacement process to the extent possible. To verify, please follow the instructions in the first section of this document, and check the certificate selection in your integration profile:
• If the 2030 certificate is selected, no further action is needed.
• If the 2025 certificate is still selected, please open a support ticket so we can assist you.
• If both the 2025 and 2030 certificates are selected (as shown in step 7 of the certificate replacement instructions), it means we've update the federation settings but could not confirm that your IdP has retrieved the 2030 certificate from the federation. In this case, please proceed to step 9 and coordinate with your IdP administrators to complete the certificate replacement process.

Special Instructions for UK Access Management Federation members: The UK federation now requires a 3072-bit certificate. To meet this requirement, we have added a new certificate that expires in 2028. If your institution uses custom host names, our support team has already completed the certificate replacement process. However, if you are using Alma or Primo generic server names and do not open a support case before we update the federation entries during the week of December 14, 2025, you may experience login issues. To resolve this, follow the above "Instructions to Replace the 2025 Self-signed Service Provider SAML Certificate" steps from 1 through 5. Then, in the "Alma metadata file version" drop-down menu, select "Version 20280811" to replace the "Version 2025" certificate, and click "Save" to confirm the changes.

- **Article last edited:** 30-Jul-2025