
Rosetta SAML Service Provider Certificate Update

- **Product:** Rosetta
 - **Product Version:** 8.2+
-

Description

The Rosetta SAML service provider certificate will expire on **January 1, 2026** and needs to be updated.

Note

To our knowledge, most SAML identity providers (IdPs) do not enforce the SAML certificate expiration checks. Even if customers fail to update the certificate before January 1, 2026, logging in to Rosetta using SAML should still be possible. However, we **recommend updating the certificate as soon as possible**.

Detailed instructions

All Rosetta customers using SAML authentication profiles need to follow the steps below:

Install the New Certificate on Each Application Server

1. Log in to the Rosetta server as the **dps** user.
2. Run **util sp** → **7 Deploy Certificate**, select **Self-Signed**, then download and install the certificate.
3. Restart the Rosetta application using **dps_stop** and **dps_start**.

SP. Service Pack Management

-
0. Exit Procedure
 1. Prepare/Update Environment
 2. Update Rosetta
 3. Update 3rd Party Products
 5. SP rollback
 6. Download Hotfix
 - 7. Deploy Certificate**

Please choose certificate type:

1. Signed
- 2. Self-Signed**
- 2

Connecting to MFT...

Connected to downloads-eu.hosted.exlibrisgroup.com.

The following certificates are available:

1. SelfSigned_01012026.crt

2. SelfSigned_31122032.crt

Please enter certificate number to download [exit]:

2

Certificate SelfSigned_31122032.crt selected.

Copying files...

Connected to downloads-eu.hosted.exlibrisgroup.com.

Updating DB...

SelfSigned_31122032.crt was deployed successfully. Restart the server to apply the changes.

Press ENTER to continue

Generate New Metadata File

- Access **Administration** → **Authentication Profile** page.
- Click **Update**, select the new certificate at the bottom of the page, and click **Generate Metadata File**.
- The metadata file will be downloaded to your PC.

Note

- If you click **Cancel**, the current service provider certificate remains active, and you can continue using it until you upload the new metadata file to your IdP.
- If you click **Save**, you must immediately upload the updated metadata file to your IdP so that SAML authentication to Rosetta continues to work.

The screenshot shows the 'Authentication Profile Details' form. The 'Rosetta Certificate Version' dropdown menu is highlighted with a red box and contains the text 'Self Signed certificate | Expiration date: 31 December 2032'. A red arrow points to the 'Generate Metadata File' button. Other fields include 'Metadata File Upload Method' (set to 'File'), 'IDP Issuer', 'IDP login URL', 'IDP logout URL', 'User ID location', 'User Group location', 'Certificate upload method', and 'ADFS'.

Upload the Metadata File to IdP

The new SAML metadata file must be uploaded to your IdP to update its configuration with the new certificate information.

Switch Rosetta Authentication Profile to Use the Updated Certificate

Once the IdP side is updated:

1. Access **Administration** → **Authentication Profile**.
2. Click **Update**, select the new certificate used to generate the metadata file, and click **Save**.

From that moment on, you should be able to log in using the updated SAML profile with the new certificate.

-
- **Article last edited:** 12-Dec-2025