

User Authentication with SAML

User Authentication with SAML

SAML enables Rosetta to exchange authentication and authorization information, allowing a user to sign in or out of an external system and be automatically signed in or out of Rosetta, or vice versa. Rosetta supports the SAML 2.0 Web Browser SSO profile.

Note

When consortium members log in with SAML, a list of institutions for which they have permissions is displayed from which they can select the one to which they want to log in.

For a more information concerning SAML-based SSO for Rosetta, see <http://developers.exlibrisgroup.com/rosetta/integrations/saml>

To configure the SAML authentication profile:

The screenshot shows a web form for configuring a SAML authentication profile. It is divided into two main sections: 'General Information' and 'Authentication Profile Details'.
General Information: Includes fields for 'Created Date' (05/07/2017), 'Updated Date' (05/07/2017), 'Created By' (John Smith), and 'Updated By' (John Smith). There are also fields for '* Name' and 'Description'. The 'Type' is set to 'SAML'.
Authentication Profile Details: Features a 'Metadata File Upload Method' with radio buttons for 'HTTP' (selected) and 'File'. Below this is a 'URL' field and a 'Populate Profile' button. Required fields include '* IdP issuer', '* IdP login URL', and '* IdP logout URL'. There are dropdown menus for 'User ID location' (set to 'NameID') and 'User Group location' (set to 'Attribute'), with an adjacent 'Attribute Name' field. A 'Certificate upload method' dropdown is set to 'Free Text'. An 'ADFS' checkbox is present and unchecked. At the bottom, there is a 'Rosetta Certificate Version' field showing 'Signed certificate | Expiration date: 05 January 2021' and a 'Generate Metadata File' button. 'Cancel' and 'Save' buttons are at the bottom right.

Authentication Profile Details

1. From the Rosetta Administration module, click **Users > Authentication Profiles > Add Authentication Profile**. The following page is displayed:

2. Enter a name and description for the profile.
3. You can populate the profile information from metadata. To use a metadata link, select **HTTP** and provide the location of the link in the URL field. To use a metadata upload, select **File** and select the file. For more information about this file, see <https://developers.exlibrisgroup.com...egrations/saml>.
4. Click **Populate Profile** to populate the profile information.
5. If you do not populate the profile from metadata, enter the settings for the **IdP issuer**, **IdP Login URL**, **IDP Logout URL**, and **User ID Location**.
6. For **User Group Location**, select **Attribute** and for **Attribute Name**, enter the name of the attribute in the SAML XML file that contains the user group list.
7. In Certificate upload method, select the type of certificate to upload. Alma accepts certificate file uploads and free-text certificate entry. If you select **Free Text**, enter the text of the certificate. If you select **File**, select the file.
8. Select **ADFS** if the IdP enables Active Directory Federation Services.
9. Select the Rosetta certificate version that you want to use, and click **Generate Metadata File** to generate the Rosetta metadata file that you are required to provide to the IdP.
10. Click **Save**.