

Authenticating a group of SAML users

- **Product:** Rosetta
- **Product Version:** 6.0

Question

How to authenticate SAML users who are not registered in Rosetta?

Use case: I have a group of users in SAML IDP that I would like to assign access rights for delivery, but I would rather not create individual Rosetta user for each SAML user.

Answer

There are two ways to authenticate SAML users:

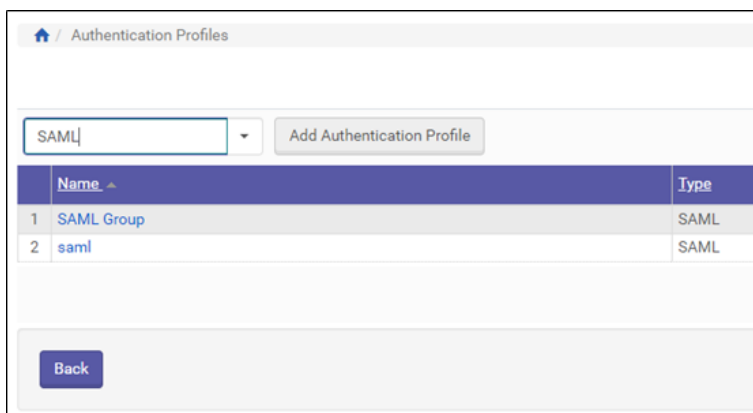
1. For each SAML user create a matching Rosetta user
2. Create a generic Rosetta user to authenticate a group of SAML users

For applying option #2, follow these steps:

1. Set up a SAML authentication Profile:

Assuming there is an existing 'saml' profile, create a new 'SAML Group' authentication profile:

- a. Go to Administration > Users: Authentication Profiles
- b. Choose type SAML and click 'Add Authentication Profile'



- c. Populate the relevant SAML IdP (for more information, see pages 170-171 in the [configuration guide](#))
- d. One of the user-related details that are returned by the IDP should be used as a matching point in Rosetta.

The IDP returns an assertion with two parts:

- a **subject** part that includes a NameID (or NameIdentifier) element
- an **attribute** part that includes a list of user-related attributes (title, cn, etc.)

You need to decide which of the user-related details will be used as a match point.

For example, the IdP can return the following assertion:

```
<saml:Assertion>
<saml:Subject>
<saml:NameID SPNameQualifier="https://eu.alma.exlibrisgroup.com/mng/
login"Format="urn:oasis:names:tc:SAML:2.0:nameidformat:uri">
73b393827e543cc2d8abe6f0c3df889f835b7e43</saml:NameID>
</saml:Subject>
<saml:AttributeStatement>
<saml:Attribute Name="title"NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue xsi:type="xs:string">Technical Support Team Leader</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="cn"NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue xsi:type="xs:string">Becky Orange </saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
```

d1. Under 'User ID location' choose Attribute

d2. Attribute Name is "title"

The screenshot shows the 'Authentication Profile Details' configuration interface. It includes fields for 'IDP issuer', 'IDP login URL', and 'IDP logout URL'. Under the 'User ID location' section, the dropdown is set to 'Attribute' and the 'Attribute Name' field contains 'title'. Similarly, the 'User Group location' dropdown is set to 'Attribute' with 'title' in the 'Attribute Name' field. The 'Certificate upload method' is set to 'Free Text'. A 'Generate Metadata File' button is located at the bottom left. A note at the bottom right states 'Certificate file already exists'.

2. Create the generic Rosetta user:

- Mark the 'Shared' checkbox
- Click 'Additional Identifiers' to open it
- Choose the "SAML Group" Authentication profile and enter the attribute value.

In our example, the title value that is shared among a group of SAML users is 'Technical Support Team Leader'.

All SAML users with title='Technical Support Team Leader' will be authenticated in Rosetta as this generic user.

- Under 'User Authentication' choose type 'Internal with External authentication'
- Save

Authentication Profile	Value	
SAML Group	Technical Support Team Leader	Delete
SAML Group	Technical Implementation Consultant	Delete
SAML Group	Technical Support Analyst	Delete

* Authentication Profile: * Value:

User Authentication

Type

Internal - Refers to a user type whereby the user information is managed wholly within the Rosetta.

External - Refers to a user type whereby user information is managed in third party IAM system or directory server, and that data is used by the Rosetta.

Internal with External Authentication - The same as internal with the exception that the authentication is managed externally.

* Password: * Verify Password:

Note

In other situations, the User ID attribute does not need to be configured in Rosetta Authentication profile at all and the users can be matched solely on User group attribute. The IdP must rerun assertion including the User group value in the attribute indicated in Rosetta Authentication profile User group location and the group value has to be added as Additional identifier to the generic Rosetta user.

3. Update General Parameters:
 - a. Go to Administration > General: General Parameters
 - b. Select Module: Authentication
 - c. On 'default_authentication_mode' put the predefined Authentication Profile Name
 - d. Update

Name	Description	Type	Module	Value
authentication_lock_duration	The duration for which a user attempting to log in to the system with an incorrect password is locked out of the system.	number	authentication	30000
authentication_max_failure	If a user attempts to log in with an incorrect password more than the number of times specified here, the user is locked out of the system for the duration specified by the authentication_lock_duration parameter.	number	authentication	3
default_authentication_mode	Specifies the default authentication method.	string	authentication	SAML Group
display_self_registration	When false, the patron self-registration is not displayed in the local authentication login form.	boolean	authentication	true
enable_remote_reports_user	Enable remote access by remote_reports user.	boolean	authentication	false
login_default_institution	The institution that appears as the default on the login page.	string	authentication	IN200
remote_access_key	Access key for remote_reports user.	string	authentication	h5yVz8M5A7lgOPMh8HNAx70R3MgA1Zu7eLrKXe7to=
remote_management	Show remote dashboards.	boolean	authentication	false
rsz_authentication	Requires authentication for RSI server access.	boolean	authentication	false

Note

After changing the 'default_authentication_mode' parameter, the authentication will be with "SAML Group" profile. Back office users will need to change their login url in order to authenticate by 'saml' profile:
<https://<<hostname>>:<<port>>/mng?auth=saml>

4. You can create access rights according to the new user created

MID	53665	Metadata Type	policy.accessrights
Created by	admin1	Creation Date	15-07-2019 11:41:00
Updated by	admin1	Update Date	15-07-2019 11:41:02

Copyright Template	<input type="text"/>
* Description	SAML GROUP TEST
When view is restricted show the following message	<input type="text"/>

Group 1	User Name equal SAML Group 1
---------	------------------------------

Additional Information

[Rosetta Configuration Guide](#), Chapter 9: pages 170-171

[Authenticating Users with SAML](#)

-
- **Article last edited:** 17-JUL-2019