Configuring User Authentication for Primo VE

Introduction

Primo supports a number of authentication schemes, which are defined using Alma’s integration profiles. An institution may choose to use more than one of the following authentication schemes:

- LDAP
- SAML based authentication such as Shibboleth
- CAS
- OAuth based authentication with Facebook, Google, Twitter or using email
- Alma internal users

For information on configuring external authentication systems, see Integrations with External Systems. After you have configured the integration profile in Alma, you must use the User Authentication page to specify which authentication systems are relevant to end users in Primo VE. For information about the Ex Libris Identity Service, see https://developers.exlibrisgroup.com/alma/integrations/user-management/authentication/exl_identity_service.

Login Pages

The User Authentication page (Discovery > Authentication > User Authentication) allows you to configure authentication profiles and the help links and labels that display on the Login pages for Primo VE.
If multiple profiles are defined and activated, the system will display the Parallel Login page, which allows users to select the type of authentication to use to sign in to Primo VE. You can display up to five links on the Parallel Login page.

After users select an authentication method, they will receive the appropriate login page for the selected authentication method.

Configuring the Login Links

The Profiles tab on the User Authentication page allows you to enable a maximum of five login links, which allow users to select a type of authentication to use to log on to the system.
To enable the login links:

1. Open the User Authentication page (Configuration Menu > Discovery > Authentication > User Authentication) and select the Profiles tab (which is the default tab).

Profiles Tab

2. In the Authentication Profiles section, activate the types of authentication that you want to provide to users. If multiple authentication types are enabled, the system will display the Parallel Login page to users.

3. To configure the help links on the Login page, see Configuring the Help Links.

4. In the Authentication Settings section, specify the following options:
   - **Single Sign Out Upon Timeout** – When selected, a single sign-out request is sent to the authentication system (CAS and SAML) when Primo VE times out. Otherwise, the system logs the user out of Primo VE and remains open to other campus applications.
   - **Enable Silent Login** – When enabled for CAS and SAML authentication methods, users who have already signed in to other campus applications will be automatically signed in to Primo VE when they open a Primo VE session in a new window or tab with the same browser. Otherwise, users must sign in to Primo VE.

   **Note**
   
   If you have configured multiple authentication profiles, Primo will attempt to apply the silent login with the first eligible profile only.

5. Select **Save**.
Configuring the Help Links

The Profiles tab on the User Authentication page allows you to configure up to four help links. For each help link, you can specify a label and a URL for the help page.

To configure the help links:

1. On the User Authentication page (Configuration Menu > Discovery > Authentication > User Authentication), select the Profiles tab (which is the default tab).

2. Select Edit next to the login link for which you want to add a help page.

3. Specify the label and URL for the help page.

4. Select Save.
Configuring the Labels

The Labels tab on the User Authentication page allows you to configure various labels on the login pages.

To configure the labels:

1. Open the User Authentication page (Configuration Menu > Discovery > Authentication > User Authentication) and select the Labels tab.

   ![Image of User Authentication page]

   **Labels Tab**

2. Use the following table to configure the fields associated with each label:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>login.login</td>
<td>The label for the Login button.</td>
</tr>
<tr>
<td>login.cancel</td>
<td>The label for the Cancel button.</td>
</tr>
<tr>
<td>login.password</td>
<td>The label for the Password field.</td>
</tr>
<tr>
<td>parallel.login.link1 - parallel.login.link5</td>
<td>The labels for up to five parallel login links on the Parallel Login page.</td>
</tr>
<tr>
<td>login.error.message</td>
<td>The error message that display when users are unable to sign in.</td>
</tr>
<tr>
<td>login.title</td>
<td>The label for the title of the sign-in page.</td>
</tr>
<tr>
<td>login.userid</td>
<td>The label for the User ID field.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>login.dual.title</td>
<td>The label for the title of the Parallel Login page.</td>
</tr>
<tr>
<td>parallel.login.description1 -</td>
<td>The descriptions for each of the links on the Parallel Login page.</td>
</tr>
<tr>
<td>parallel.login.description5</td>
<td></td>
</tr>
</tbody>
</table>

3. **Select** Save.