Configuring User Authentication

Introduction

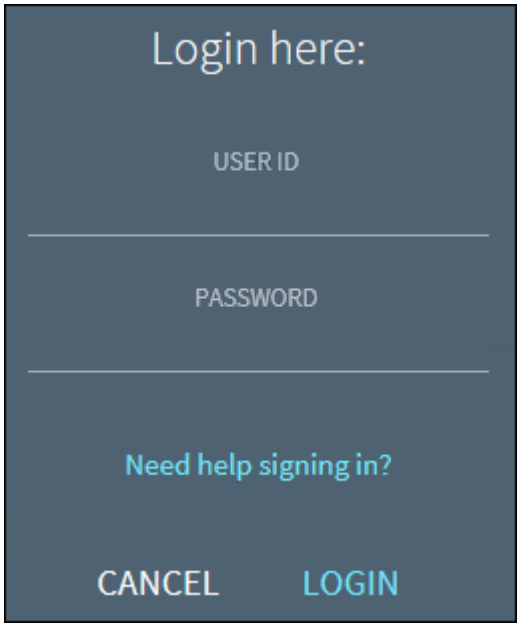
Rapido supports several authentication schemes, which are defined using Rapido's integration profiles. An institution may choose to use more than one of the following authentication schemes:

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

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

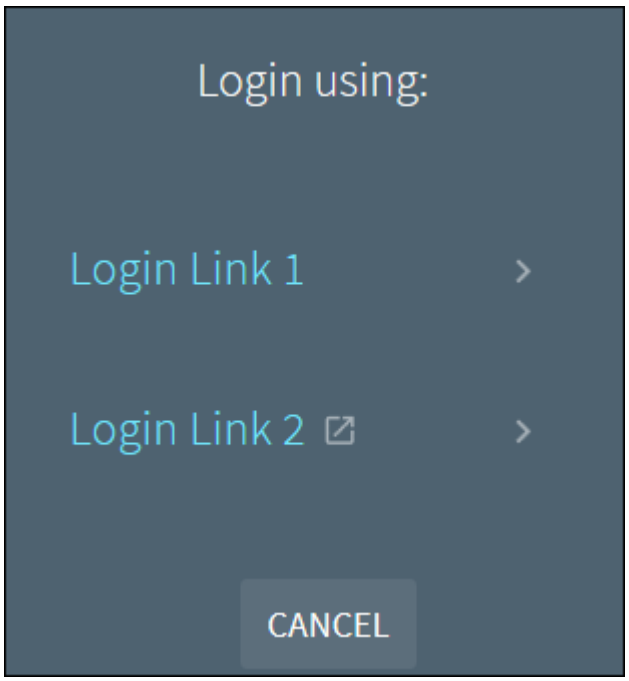
Login Pages

The User Authentication page (**Discovery > Authentication > User Authentication**) enables you to configure authentication profiles and the help links and labels that appear on the Login pages for Rapido.



Login Page

If multiple profiles are defined and activated, the system shows the Parallel Login page, which enables users to select the type of authentication to use to sign in to Rapido. You can show up to five links on the Parallel Login page.



Parallel Login Page

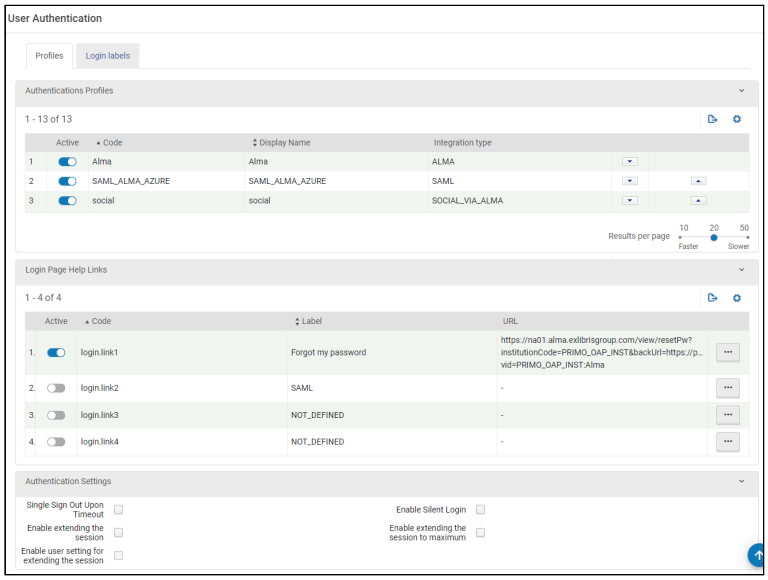
After users select an authentication method, they receive the appropriate login page for the selected authentication method.

Configuring the Login Links

The **Profiles** tab on the User Authentication page enables you to enable a maximum of five login links, which enables users to select a type of authentication to use to log in to the system.

To enable the login links:

1. Open the User Authentication page (**Configuration > 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 authentications that you want to provide to users. If multiple authentication types are enabled, the system shows the Parallel Login page to users.
3. 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 Rapido times out. Otherwise, the system logs the user out of Rapido 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 are automatically signed in to Rapido when they open a Rapido session in a new window or tab with the same browser. Otherwise, users must sign in to Rapido.

      Note

      - Currently, this option is not supported if you are using an Azure IDP.
      - If you have configured multiple authentication profiles, Primo attempts to apply the silent login with the first eligible profile only.

    - **Enable extending the session** — When selected, users receive a message 60 seconds before timeout, and it will allow them to extend the session for another session period. If the users do not want to continue their session, they are signed out, the screen is refreshed, and the UI redirects to the configured URL for timeouts. By default, this field is disabled.
    - **Enable extending the session to maximum** — When selected, users receive a message 60 seconds before timeout, and it enables them to extend the session to the maximum period (which is seven days and is not configurable). During this period, users who decide to continue with the maximum session are automatically signed in when using the same device. If the users do not want to continue their session, they are signed out, the screen is refreshed, and the UI redirects to the configured URL for timeouts. By default, this field is disabled.

      Note

      If both the **Enable extending the session** and **Enable extending the session to maximum** parameters are enabled, **enable extending the session to maximum** has precedence.

    - **Enable user setting for extending the session** — When selected, this parameter adds the **Automatically extend my session** option to the **My Library Card > Personal Details and Settings** tab, which enables the users to extend their sessions automatically without being prompted to extend the session. By default, this field is disabled.
4. Select **Save**.

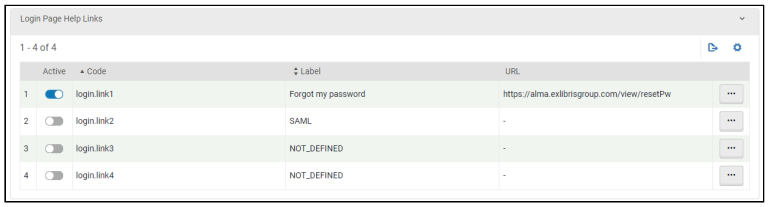
Configuring the Help Links

The **Profiles** tab on the User Authentication page enables 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:

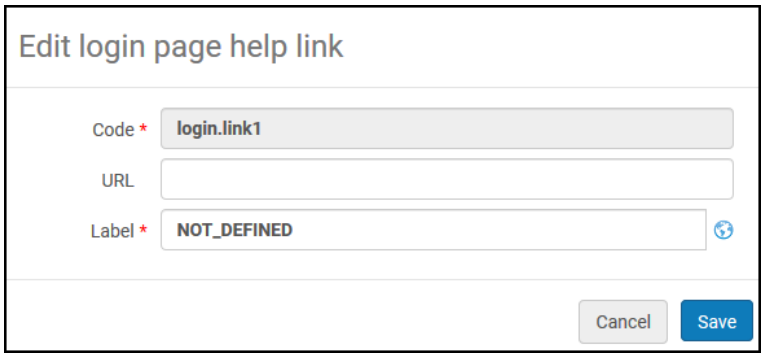
1. On the User Authentication page (**Configuration > Discovery > Authentication > User Authentication**), select the

Profiles tab (which is the default tab).



Profiles Tab

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



Define Help Link Page

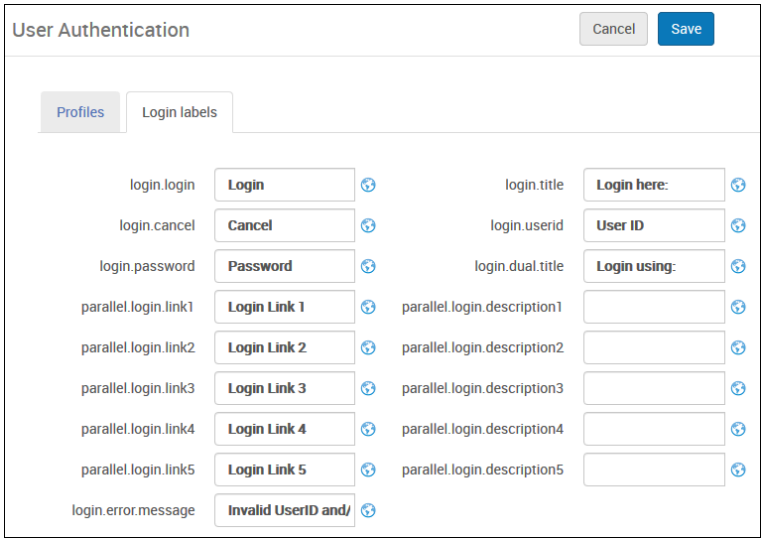
3. Specify the label and URL for the help page.
4. Select **Save**.

Configuring the Labels

The **Login labels** tab on the User Authentication page enables you to configure various labels on the login pages.

To configure the labels:

1. Open the User Authentication page (**Configuration > Discovery > Authentication > User Authentication**) and select the **Login labels** tab.



Labels Tab

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

Define Labels on the Login and Parallel Login Pages

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

3. Select **Save**.