Using Social Networks for User Authentication

Note
If you are working with Primo VE and not Primo, see Configuring User Authentication for Primo VE.

Alma environments support the use of the following social networks to perform user authentication: Google and Facebook. The following steps describe the interaction between the user, Primo, Alma, and the social network to provide authentication and authorization:

1. The user invokes the sign-in option in Primo.

2. Primo displays the Primo login page, which also contains a link to the social login page.

3. The user clicks the link to the social login page, according to the integration profile configured in Alma (see Social Login).

Note
If you have configured both Google and Facebook in Alma, the user selects a preferred social network from the Social Network Login page. Otherwise, the user is redirected automatically to the only configured social network.

4. Authentication is handled by Alma and the social network:
   1. If the user has not signed in to the social network, the social network displays a sign-in page for the user to sign in. Otherwise, no additional sign-in is necessary.
   2. After the user signs in, the social network sends a token to Alma.
   3. If the user is not recognized by Alma and self-registration is configured in Alma (see Social Login), Alma prompts the user to perform self-registration. If self-registration is not configured in Alma, the user is sent an error message.

5. If the user has been authenticated, Primo logs the user in.

For information on configuring social logins in Alma and the social networks, see the following pages, respectively:

- Social Login
- Social Logins in the Developer Network

Configuring a Social Login Profile

Authentication using a social network via Alma does not require much configuration because the relevant information is
defined for the Primo institution and displayed automatically for you in the login profile.

It is assumed that social authentication will be used in parallel with another authentication method to allow users to select a social network option from the parallel login page, which will display when the user attempts to sign in.

To configure Primo to use social authentication:


   **Note**

   Social authentication is available with the new Primo UI only.

2. Select your institution from the **Owner** drop-down list.

   **Note**

   The source of your Primo institution must be Alma in order to configure Alma user authentication.

3. Create a new login profile. The Login Profile page opens. For more information on creating login profiles, see The Primo Authentication Manager.

4. Select **SOCIAL_VIA_ALMA** from the Select Authentication Method drop-down list.

   The Social via Alma authentication parameters appear on the page.

   ![Social Login Profile Page](http://example.com/login-profile-page)

5. Use the following table to configure the Alma authentication fields:
### Alma Configuration Fields

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOCIAL_ALMA_LOGIN_URL</td>
<td>(Required) The IDP login URL. This is the URL Primo uses when it sends the authentication request to Alma.</td>
</tr>
<tr>
<td>ALMA_INSTITUTION</td>
<td>(Required) The Alma institution code, which is defined in the Alma Institution Code mapping table.</td>
</tr>
<tr>
<td>JWT_SIGNATURE_SECRET</td>
<td>(Required) Used for the handshake between Primo and Alma. Any value can be used here as long as it matches the entry defined for Alma's customer parameter jwt_signature_secret (Administration &gt; User Management Configuration &gt; Configuration Menu &gt; General &gt; Other Settings in Alma; see Configuring Other Settings).</td>
</tr>
</tbody>
</table>

6. Select **ALMA** (see Alma Information Request Fields) from the Select User Information Method drop-down list.

7. Select **Save** to save your Social via Alma profile and to return to the Login Profiles page.