# OpenID Connect

To configure an OpenID Connect type of integration profile, you must have the following role:

- General System Administrator

Rapido integration supports the OpenID Connect standard for user authentication. See the Developer Network for more information.

When a Rapido user attempts to log in, user authentication can be processed using systems that support the OpenID Connect standard such as Auth0 and Azure. This works in a manner similar to the social login process in Rapido.

---

**Note**

Multiple OpenID Connect integration profiles can be defined in Rapido. This enables you to define different user authentication for different groups of users, for example, for students and faculty staff.

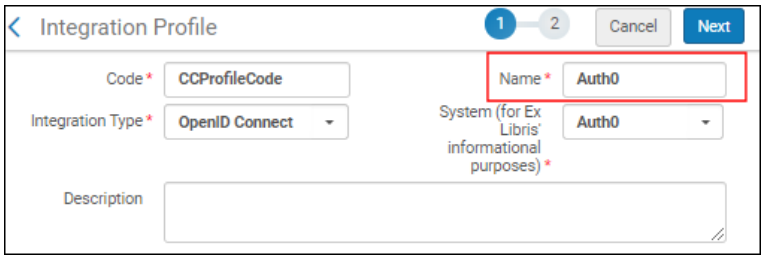
---

# Creating an OpenID Connect Integration Profile

If you want to use this method of authentication, you need to create and configure an OpenID Connect integration profile.

**To create an OpenID Connect integration profile:**

1. Open the Integration Profile List page (**Configuration > General > External Systems > Integration Profiles**).
2. Select **Add Integration Profile**.
3. From the Integration Type dropdown, select **OpenID Connect**.
4. From the System dropdown, select the option that represents the OpenID Connect authentication system that you are using.
5. Enter a code and name for this integration profile. This name is used in the label for the login option in Rapido:




6. Select **Next.**
7. Select **Active** if you want to begin using this integration profile after saving it. Select **Inactive** if you want to enabled the profile at a later time.
8. Enter the following information provided by the OpenID Connect authentication system:
    - App ID
    - App Secret
    - Well-known URL — Select to automatically fill in all the below fields with the default OIDC information. This saves you time and helps ensure that all the fields are defined correctly. If you select not to use the well-known URL, fill in the below fields manually.
    - Authorization endpoint
    - Token endpoint
    - Scopes — select a space-delimited list of scopes. The minimum scope for the authentication process is 'openid'.
    - Matching Claims — Claim code containing the user ID. For most OpenID providers that would be 'sub', the subject identifier. If you elect a different claim code, the "UserInfo endpoint" field opens where you can call the UserInfo endpoint with the access token to retrieve the additional claims. Rapido locates the user using the configured claim in either the id_token or in the output of the UserInfo request.
    - Select **Force Authentication** if you want to force authentication when Rapido authenticates users using OIDC. This helps ensure that the user is properly authenticated with the correct institution.
    - **Base64 encode the state parameter** — Select this to encode the relay state parameter in base64 (instead of URL-encode). This might be needed for integration with AWS.
    - **Logout URL** — Add a Logout URL to which the system will redirect after logging out. This logs out the user from other systems that are connected to the same OpenID provider.
9. Select **Save**.