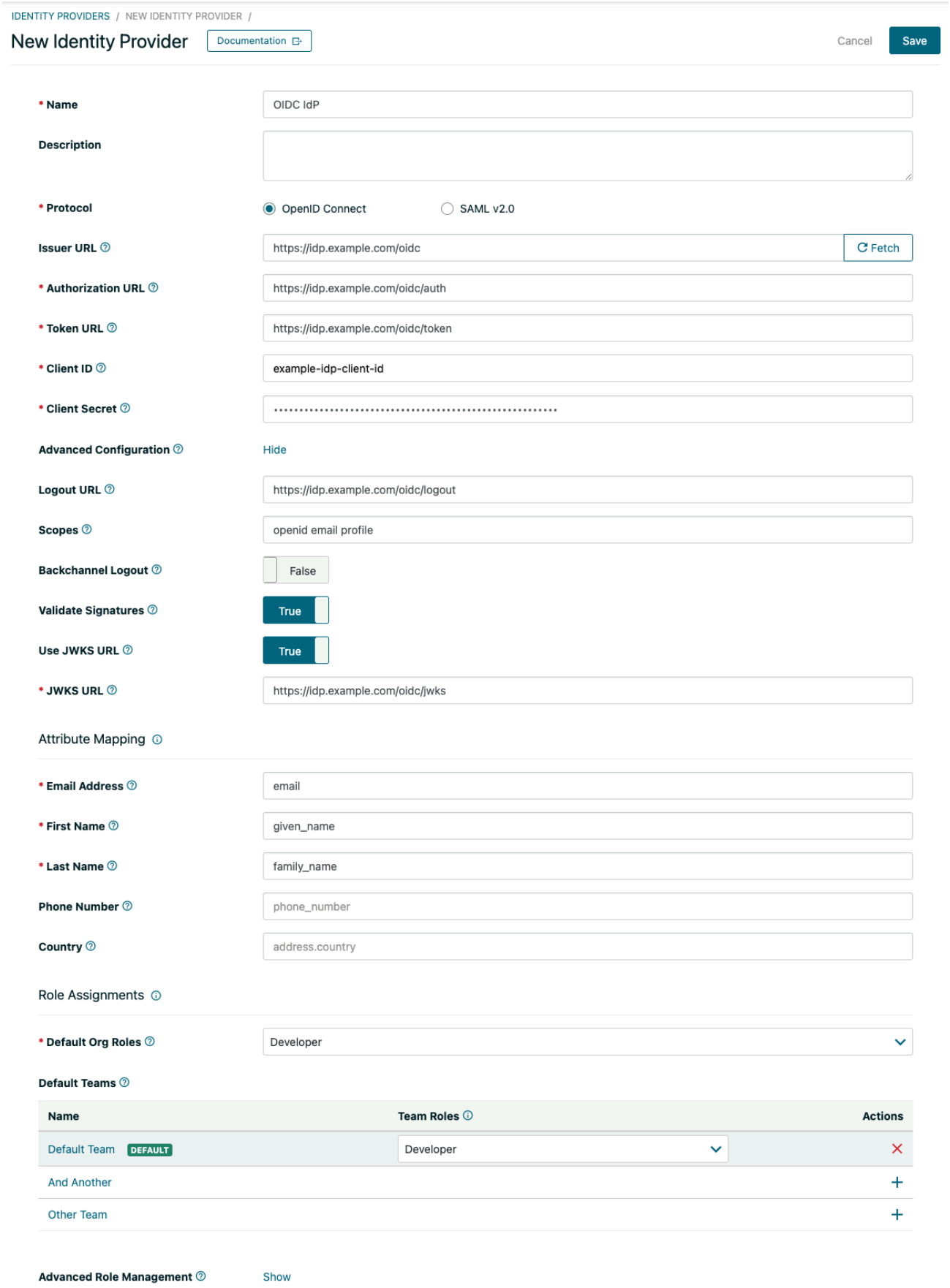
Configuring an OpenID Connect (OIDC) IdP

Sequence	Completed task to configure and enable an IdP		
1	-	-	Add a domain and
		-	Verify domain ownership
			Configure an OIDC or SAML v2.0 IdP
		Step 1 tasks (add and verify a domain, or configure an IdP) can be completed in any order	
2	-	Confirm the association of an IdP to the domain	
3	-	Enable the IdP configuration for all domain users	
4	-	(*Optional*) Add a subdomain	

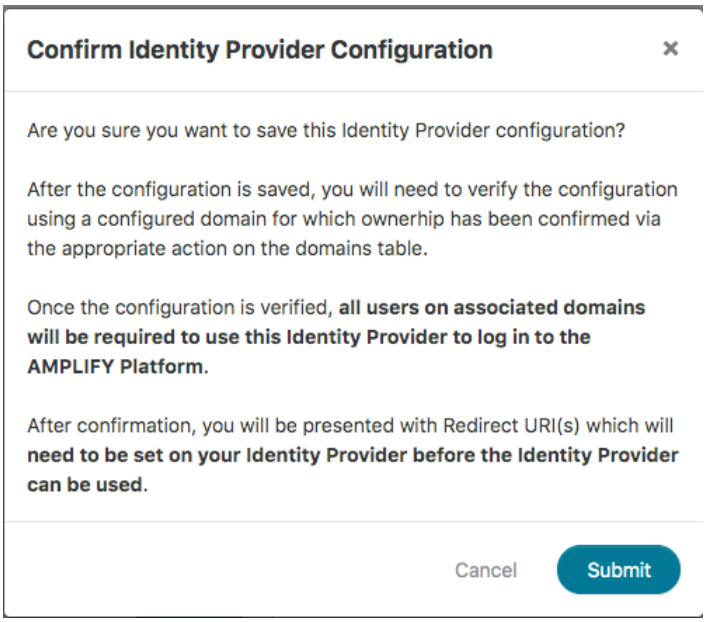
This section includes details on configuring an OpenID Connect (OIDC) Identity Provider.

To create a new Identity Provider

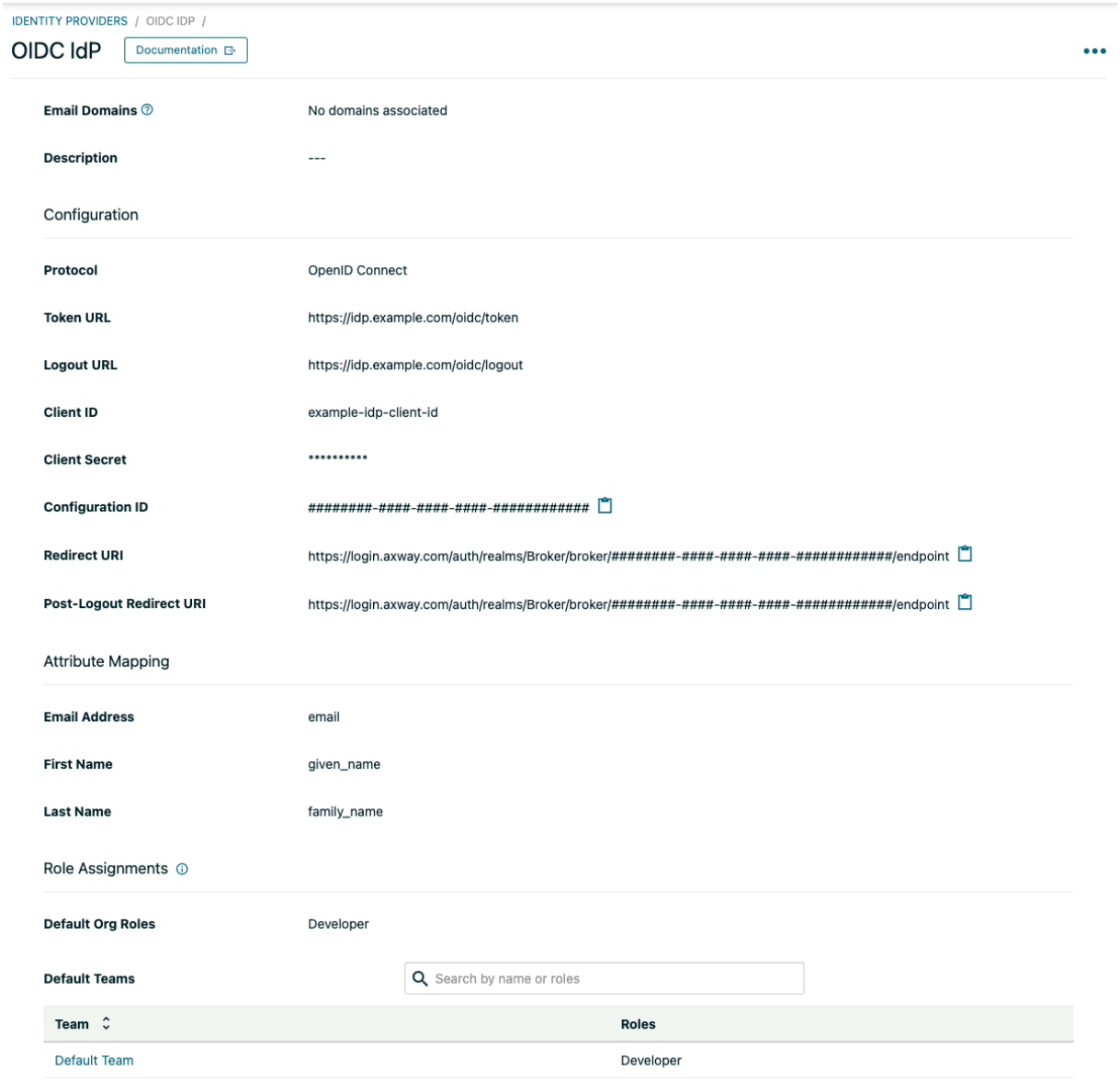
1. From the *Identity Providers* page, click **+ Identity Provider**. The **New Identity Provider** form will be presented.
2. Select **OpenID Connect**. A blank form is presented.
3. Enter the **Issuer URL** and then click **Fetch** to retrieve and populate the OIDC provider configuration values exposed by the issuer. The values can also be manually entered.
4. Enter the **Client ID** and **Client Secret** fields from the values that are configured for your OIDC Identity Provider's AMPLIFY Platform client.
5. Complete the **Advanced** configuration settings (**Logout URL** and **Backchannel Logout**) if they are applicable to your Identity Provider.
6. Confirm the provider configuration values for **Authorization URL**, **Token URL**, and **Attribute Mapping**.
7. Complete the *Role Assignments* section. Refer to Role Assignments for details.
8. The following is an example of a completed OIDC form (before clicking **Save**).



9. Click **Save**. A confirmation dialog appears with a message that, once the Identity Provider configuration is verified, all users on that domain will be required to log into the AMPLIFY Platform with their Identity Provider credentials.



10. To complete the configuration, you must add values configured in the AMPLIFY Platform *Identity Providers* detail page to your Identity Provider.
    - Copy the **Redirect URI** and optionally the **Post-Logout Redirect URI** into the OIDC configuration manually or by clicking the clipboard icon.



- Click **Save** in the OIDC page.

When a new Identity Provider is being configured, the organization administrator can edit any field. After an OIDC Identity Provider is pending or verified, the organization administrator is not permitted to edit the **Authorization URL**, **Token URL**, and **Client ID** fields.