

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	-	<i>(Optional)</i> 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**).

New Identity Provider

[Documentation](#)

Cancel

Save

*** Name**

Description

*** Protocol** OpenID Connect SAML v2.0

Issuer URL [Fetch](#)

*** Authorization URL**

*** Token URL**

*** Client ID**

*** Client Secret**

Advanced Configuration [Hide](#)

Logout URL

Scopes

Backchannel Logout False

Validate Signatures True

Use JWKS URL True

*** JWKS URL**

Attribute Mapping

*** Email Address**

*** First Name**

*** Last Name**

Phone Number

Country

Role Assignments

*** Default Org Roles** [v](#)

Default Teams

Name	Team Roles	Actions
Default Team DEFAULT	Developer v	x
And Another		+
Other Team		+

Advanced Role Management [Show](#)

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.

Confirm Identity Provider Configuration ✕

Are you sure you want to save this Identity Provider configuration?

After the configuration is saved, you will need to verify the configuration using a configured domain for which ownership has been confirmed via the appropriate action on the domains table.

Once the configuration is verified, **all users on associated domains will be required to use this Identity Provider to log in to the AMPLIFY Platform.**

After confirmation, you will be presented with Redirect URI(s) which will **need to be set on your Identity Provider before the Identity Provider can be used.**

Cancel Submit

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.

OIDC IdP

[Documentation](#)



Email Domains ⓘ	No domains associated
Description	---
Configuration	
Protocol	OpenID Connect
Token URL	https://idp.example.com/oidc/token
Logout URL	https://idp.example.com/oidc/logout
Client ID	example-idp-client-id
Client Secret	*****
Configuration ID	#####-###-###-###-##### ⓘ
Redirect URI	https://login.axway.com/auth/realms/Broker/broker/#####-###-###-###-#####/endpoint ⓘ
Post-Logout Redirect URI	https://login.axway.com/auth/realms/Broker/broker/#####-###-###-###-#####/endpoint ⓘ
Attribute Mapping	
Email Address	email
First Name	given_name
Last Name	family_name
Role Assignments ⓘ	
Default Org Roles	Developer
Default Teams	<input type="text" value="Search by name or roles"/>
Team ⌵	Roles
Default Team	Developer

- 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.