




Using Open ID Connect (OIDC) in Zoho Directory

As an OpenID provider, Zoho Directory (ZD) can help you in authenticating the users and getting authorization to access users profile information securely. This is done through the OIDC authentication protocol. [Learn more about OIDC.](#)

In Zoho Directory, you can configure OpenID Connect (OIDC) for any third-party apps. The way OIDC performs vary based on the type of application you configure ZD with.

How OIDC works:

Third-party apps (Relying Party) request the Authorization Endpoint of ZD to authenticate the user and get user's authorization to access certain user information. After authenticating the user and obtaining authorization, the authorization endpoint sends an ID token and access token to the Relying Party (RP).

 The method used for this token exchange varies based on the type of RP and the authentication flow chosen. [Learn about the RP types and the recommended authentication flows for each.](#)

RP requests user information (claims) to the UserInfo Endpoint of ZD with the access token. ZD sends the consented claims to the RP.

OIDC Terminologies for better understanding:

OpenID Provider

Zoho Directory (ZD) is the OpenID Provider(OP). It helps in authenticating the user and also obtaining consent from the user for the RP to access certain user information.

Relying Party

Relying Party in the OIDC flow is the third-party app that you are trying to configure in ZD and which will request authentication and authorization of the user to ZD.

Claims

Any information about the user that ZD sends to RP is called as claims. ZD sends users' basic profile information such as name, first name, gender, email address and profile picture.

Sign-in URL

RP's URL where the users initiate the sign-in process.

Sign-out URL

RP's URL where users will be automatically logged out once they log out from Zoho Directory.

Callback URL

URL to which Zoho redirects users after authenticating them.

Client ID

Unique ID given to the RP to identify it when users try signing in.

Client Secret

Secret key given to the RP to identify it when users try signing in.

Authorization Endpoint

Endpoint where the user authenticates themselves and grants permission to access specific information about them.

Token Endpoint

Endpoint where RP exchanges the required tokens for the authorization code.

User Info Endpoint

Where RP requests the needed profile information of the user who is trying to sign-in.

Discovery endpoint

Where all the OIDC details related to Zoho Directory are displayed.

JSON Web Key (JWK) endpoint

Where RP receives a key to verify the authenticity of the tokens received.