Identity provider · Other OpenID Connect provider

Set up federation, map the signed identity, and verify a real test sign-in.

https://docs.qintoravacloud.com/integrations/identity-provider/other/

Provider configuration

Issuer template
: Use your provider metadata

Discovery template
: Use your provider metadata

Scopes
: `openid profile email`

Default claim
: `email`

Default user field
: `See provider setup`

Setup

1. Register Qintorava Cloud as an OpenID Connect confidential web client.
2. Enable Authorization Code flow and add the exact callback shown below.
3. Enter the issuer and discovery document URLs supplied by the provider.
4. Choose a stable ID token claim and the matching Qintorava user field.

Field guidance

issuer
: Exact issuer identifier returned by the discovery document.

discoveryUrl
: HTTPS OpenID Provider Configuration URL.

clientId
: Confidential web client identifier.

clientSecret
: Confidential web client secret.

Verify sign-in

Test metadata and then sign in with an explicitly assigned test user. Confirm the tenant and effective permissions. Test an unassigned account and confirm access is denied. The live demo currently advertises local sign-in.

Federation and SCIM runbook · Provider documentation