Identity provider · Auth0

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

https://docs.qintoravacloud.com/integrations/identity-provider/auth0/

Provider configuration

Issuer template

`https://{tenantDomain}/`

Discovery template

`https://{tenantDomain}/.well-known/openid-configuration`

Scopes

`openid profile email`

Default claim

`email`

Default user field

`See provider setup`

Setup

1. Create a Regular Web Application in Auth0.
2. Add the exact callback shown below to Allowed Callback URLs.
3. Add the application origin to Allowed Web Origins and the signed-out URL to Allowed Logout URLs.
4. Copy the domain, client ID, and client secret.

Field guidance

tenantDomain

Auth0 tenant or custom domain, for example tenant.us.auth0.com.

clientId

Client ID from the application Settings page.

clientSecret

Client secret from the application Settings page.

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