Identity provider · Google Workspace

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

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

Provider configuration

Issuer template

`https://accounts.google.com`

Discovery template

`https://accounts.google.com/.well-known/openid-configuration`

Scopes

`openid profile email`

Default claim

`email`

Default user field

`See provider setup`

Setup

1. In Google Cloud Console, configure the OAuth consent screen for the organization.
2. Create an OAuth 2.0 Client ID with application type Web application.
3. Add the exact redirect URI shown below to Authorized redirect URIs.
4. Copy the client ID and secret; optionally restrict sign-in to Workspace domains.

Field guidance

clientId

OAuth Web client ID ending in apps.googleusercontent.com.

clientSecret

OAuth client secret from Google Cloud Console.

allowedDomains

Workspace domains such as qintorava.com. Leave blank only when consumer accounts are allowed.

idpUserClaim

Use email for standard Google OpenID Connect mapping.

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