Identity provider · Okta Workforce Identity

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

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

Provider configuration

Issuer template

`https://{oktaDomain}`

Discovery template

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

Scopes

`openid profile email`

Default claim

`email`

Default user field

`See provider setup`

Setup

1. In Okta Admin Console, create an OIDC Web Application integration.
2. Set the sign-in redirect URI to the exact callback shown below.
3. Assign the people or groups who may access Qintorava Cloud.
4. Enter the Okta organization domain, client ID and secret. The organization issuer supports workforce sign-in. If you licensed a custom authorization server, replace both issuer and discovery URL with its canonical values.

Field guidance

oktaDomain

Okta domain such as company.okta.com, without https://.

authorizationServerId

Use default unless a custom authorization server was created.

clientId

Client ID from the application General tab.

clientSecret

Client secret from the application General tab.

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