Identity provider · Ping Identity / PingOne

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

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

Provider configuration

Issuer template

`https://auth.pingone.com/{environmentId}/as`

Discovery template

`https://auth.pingone.com/{environmentId}/as/.well-known/openid-configuration`

Scopes

`openid profile email`

Default claim

`email`

Default user field

`See provider setup`

Setup

1. Create an OIDC Web Application in PingOne.
2. Add the exact callback shown below as a Redirect URI and enable Authorization Code.
3. Assign the application to the required populations or groups.
4. Copy the environment ID, client ID, and client secret.

Field guidance

environmentId

PingOne Environment ID from environment properties.

clientId

Client ID from the application Configuration tab.

clientSecret

Client secret from the application Configuration 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