Identity provider · Microsoft AD FS

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

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

Provider configuration

Issuer template
: Use your provider metadata

Discovery template
: Use your provider metadata

Scopes
: `openid profile email`

Default claim
: `sub`

Default user field
: `ssoIdentifier`

Setup

1. Create a confidential OIDC web application (or a signed SAML application when using SAML).
2. Enable Authorization Code with PKCE S256 for OIDC; copy the canonical issuer and discovery URL from your tenant.
3. Register the exact Qintorava callback URI shown after saving. Assign only the intended users in your IdP.
4. Map a signed stable claim to the user SSO identifier, explicitly assign the user, validate metadata and then perform a real sign-in.

Field guidance

issuer
: Exact issuer identifier from your tenant metadata. Provider region and tenant URLs vary.

discoveryUrl
: Canonical public HTTPS discovery document for this tenant. No credentials in the URL.

idpUserClaim
: Use a stable signed subject claim. Populate the same value in the selected user field before assignment.

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