Identity provider · Microsoft Entra ID

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

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

Provider configuration

Issuer template

`https://login.microsoftonline.com/{tenantId}/v2.0`

Discovery template

`https://login.microsoftonline.com/{tenantId}/v2.0/.well-known/openid-configuration`

Scopes

`openid profile email`

Default claim

`oid`

Default user field

`ssoIdentifier`

Setup

1. In Microsoft Entra admin center, register a Web application.
2. Add the exact redirect URI shown below under Authentication > Web.
3. Create a client secret under Certificates & secrets and copy its value before leaving the page.
4. Enter the Directory (tenant) ID, Application (client) ID, and client secret value.

Field guidance

tenantId

Directory (tenant) ID. Use a tenant GUID for a single-tenant integration.

clientId

Application (client) ID from the app registration Overview page.

clientSecret

Client secret value, not its secret ID.

idpUserClaim

Prefer the immutable tenant object ID (oid), mapped to the user SSO identifier. Set that identifier on the user record and assign the user to this provider.

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