Configure and verify federation and SCIM

Test provider metadata, assigned identities, SAML or OIDC sign-in, and scoped provisioning.

https://docs.qintoravacloud.com/guides/federation-scim/

Verify the configuration before activation

Open **Administration → Federation & provisioning**. Confirm provider protocol, HTTPS metadata, expected issuer and audience, callback or ACS, and tenant identity assignment. For OIDC use a signed stable claim and the provider's supported authorization-code flow with PKCE. For SAML verify metadata, signed assertion requirements and the canonical service-provider endpoints shown by Qintorava.

Test real access

1. Save the configured provider, run its metadata test and verify ready status.
2. Assign one controlled test identity. Verify its stable claim value and target user field. Sign in through the provider and confirm the intended tenant and role.
3. Test an unassigned or inactive test identity. Verify that the provider cannot grant access outside the configured tenant and assignment.
4. For SCIM, use the dedicated scoped client and test a synthetic user with expected create/read/update/deactivate operations. Confirm resulting roles and account lifecycle through authorized reads. Protect and rotate the credential under the organization's provider process.

Troubleshoot

For a missing provider button, check enabled state, successful validation of the current configuration, and published credentials. For a rejected callback, compare issuer, audience, exact callback URL, state and assignment before editing mappings. A successful discovery-document request establishes metadata reachability. A real sign-in and denied-account test establish the end-to-end access behavior for that configured provider.