Configure identity, MFA, and user lifecycle

Verify sign-in configuration and session security with tenant-scoped test accounts.

https://docs.qintoravacloud.com/guides/identity/

Configure identity

Open **Find a workspace → Administration** and select **Identity providers**, **Federation & provisioning**, or **User directory integrations** for the task. Verify the tenant and keep an approved recovery account available while changing federation. Use the tenant-provided callback or ACS information and the identity provider's approved credentials.

1. Confirm the provider protocol, issuer/entity ID, callback/ACS URL, audience and claim mapping. Use protected credential storage.
2. Test with a scoped identity and check that the expected tenant, group and role are applied. Confirm MFA enforcement and any required fresh verification on sensitive operations.
3. For provisioning, preview or test a limited user/group scope and verify external identity matching. Check deactivation and reactivation behavior before broad rollout.
4. Record the working configuration and access checks. If sign-in fails after activation, restore the prior reviewed configuration through the approved recovery account and validate sign-in again.

Investigate sessions and recovery

Use **Account security** to inspect your sessions. Administrative session review and revocation require authorized access and fresh verification where shown. For supervised recovery, verify identity through the configured process, record the reason and required approval, then confirm reenrollment and audit evidence. See Sign in and recover access.