Sign in and recover access

Use local credentials or your organization identity, complete MFA, and recover access when a factor is unavailable.

https://docs.qintoravacloud.com/guides/sign-in/

Before you begin

Use the URL supplied by your administrator. For the demo, open Qintorava Cloud. Accounts, MFA enrollment, roles, and enabled sign-in methods belong to the tenant. Open the portal for self-service and the Agent workspace for assigned operational duties.

Sign in

1. Enter your username or email and password. Select **Sign in with local credentials**. If an organization sign-in button appears, select the provider approved for your account.
2. Complete the next step shown by the platform. Local accounts can be required to enroll a factor. On the verification screen use the authenticator code, a stored recovery code, or **Verify with a passkey** when the browser and enrollment support it.
3. For enrollment, use the authenticator instructions shown by the tenant and finish verification before leaving the page. Store recovery codes in your approved credential manager. If the platform sends you to a required password change, complete that page and sign back in as directed.
4. Verify that the intended portal or workspace opens and that the expected organization and navigation are available.

Recover access

Use a recovery code if available. If every factor and recovery code is unavailable, open Recover account and use the supervised recovery flow. The administrator follows the tenant's identity verification and approval process. Complete enrollment again when the approved recovery instructions direct you to do so. Verify access from a fresh browser session.

Troubleshoot sign-in

Symptom	What to check
Organization sign-in button is missing	Ask your administrator to confirm whether a provider is active and available on this tenant. Local login is the provider shown by the current demo.

Symptom	What to check
Authenticator code is rejected	Use the entry for this tenant, check automatic device time, and wait for the next code if the current one is expiring. Use the current browser tab if verification is tied to the sign-in attempt.
Passkey prompt cancels or times out	Retry on your enrolled device or use your authenticator or recovery code. Check whether the browser supports the required passkey operation.
You return to sign-in repeatedly	Reopen the tenant URL in the same browser profile, check cookie policy for that origin, and complete all required factors. Record the redirect path and time if it repeats.
Portal opens but Agent workspace redirects	Verify that the account has workspace access and the intended tenant membership.

See Session and identity administration.