Troubleshoot by symptom

Follow a reproducible path from the symptom to the responsible configuration or workflow.

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

First checks

Capture the tenant, role, page path, record number, action, exact error and timestamp with timezone. Check whether the issue affects a single record, role, tenant or all users. Reproduce with the smallest safe read or test action. Compare with an authorized expected case and redact tokens, cookies and sensitive record contents.

Symptom	Investigation
Login, MFA or session error	Sign in and recover access and identity administration.
Module, record or field missing	Diagnose record and field access.
Save, lookup or attachment blocked	Resolve save, lookup, and attachment failures.
Approval or state cannot advance	Open the product guide and check the current state, expected role, open dependencies and receipt for the last action.
Duplicate, stale or missing CIs	Model and reconcile CIs and configure discovery.
Customer or field work stalled	Customer service and field service.
Notification or event missing	Trace delivery.
API returning an error	API authentication and query guide.
Applied configuration has the wrong effect	Edit configuration in Configuration Studio.

Workspace or portal stays on the opening screen

1. Confirm you opened the intended tenant. If you were sent to sign-in or MFA, complete it and reopen the original page. If you were sent from the Agent workspace to the portal, check workspace access.
2. In the browser's Network panel, reload the page and check the page request, then `/app.js` for the workspace or `/portal.js` for the portal. A page response of `200` can arrive before JavaScript

and data finish loading. A script that returns an HTML page, redirects to sign-in, or is blocked can leave the opening screen in place.

3. Check the first failed application request and the first browser console error. If protected requests return `401`, reestablish the session. If they return `429`, wait for the server's retry interval. For an isolated `403`, check the user and route permissions before changing them. Compare `/api/health` to the failing operation to see whether the problem affects the service or a particular route.
4. If the issue appeared after a release, compare the browser entry files and server build to the artifact from that release. Reproduce using a clean browser session, with a matching synthetic role and representative data. Record whether the opening screen cleared, the destination loaded, and the intended control was usable. Test the actual workflow separately.

Escalate with actionable evidence

Include the intended and actual behavior, scope, reproducible steps, original record or run identifier, response status, last known good time, and any configuration or deployment change around the failure. Verify the recovery by repeating the affected task and confirming persistence and downstream effects.