Diagnose record and field access

Trace tenant, module, role, row, and field policy decisions before changing permissions.

https://docs.qintoravacloud.com/guides/access-policies/

Reproduce the failing action

Capture the tenant, user role, collection, record ID, field, intended operation and observed result. Confirm the user's tenant membership and enabled module. Check active role and group memberships. Compare visibility of the same object and fields using the intended role and tenant.

Simulate and fix

1. Open **Access policies & relationship queries**. Select the relevant table and operation. Use the simulator with the affected user and record where authorized.
2. Inspect applicable row and field policies, condition inputs and the effective decision. Check related records and lookup ACLs when a field is editable but its reference list is empty.
3. Make a scoped change in a test tenant. Verify an allowed case and a denied case, including list, record detail, search or export as relevant.
4. Apply through the reviewed Configuration Studio workflow or the authorized policy editor. Verify with the affected role and capture the audit receipt.

Interpret access failures

Observation	Next check
A signed-in user opening `/workspace` returns to `/portal`	Confirm whether the user is meant to have Agent workspace access. Verify the effective roles and grants before investigating the module. The employee portal is the expected surface for a user who only manages their own requests.
A protected API returns `401`	Check whether the session is present and MFA is complete. If the response includes a sign-in or MFA path, follow it and retry from the intended account.
A protected action returns `403`	Check the operation's module, record and action authorization. Test whether the user can read the record and whether the current state permits the action. Some sensitive actions require a separate recent MFA proof and return 428 when that proof is missing.
A list returns `200` with no rows	Clear unrelated filters. Confirm the test record exists, then compare company, assignment, service scope and row policy. Verify a known in-scope record is visible and a known out-of-scope record stays hidden.

Observation	Next check
A reference field is visible but offers no choices	Test the referenced collection with the same role. Compare dependent field values and related records, including whether the target is active and in scope.

Verify a role change with two accounts

1. Use a disposable record and synthetic accounts. Give the first account the intended role and give the second the nearest role that must remain restricted. Compare current memberships and effective permissions in **Groups & roles** before signing in.
2. Complete MFA for each account in a separate browser session. Open the relevant workspace or portal. Check the list, open the record, and verify the field is shown or withheld as intended.
3. Attempt the smallest representative edit with both accounts. Reopen the record after the allowed action and inspect its activity. Confirm the denied action did not change the record, a linked record, or a provider receipt.
4. Record the module, operation, test roles, record and field keys, results, and policy version. Repeat with the production grant model before rollout if it includes group membership, multiple roles or tenant overrides. The verification matrix shows the built-in single-role baseline.