Authenticate and query records

Use documented API operations, bounded record filters, and read-only GraphQL for authorized access.

https://docs.qintoravacloud.com/guides/api-and-queries/

Establish the request context

Use the base URL and sign-in or integration mechanism configured for your tenant. A Cloud Load Balancer response, Google IAM token, and an application session each describe different checks. Protected platform routes require the application authorization expected by that operation. Keep session cookies, provider secrets, MFA codes and recovery codes out of examples and logs.

Query a record list

The gateway API reference describes published methods, parameters and responses. Use read endpoints for discovery and follow the published mutation requirements when writing. A session-backed browser integration should handle login redirects, 401 and 403 explicitly.

```
GET /api/work-items?type=incident&limit=25&sort=-createdAt
GET /api/foundation/locations?limit=10&fields=name,city
```

Shared list responses include items, total, limit, offset and hasMore for supported collection endpoints. Use declared fields, sort keys and operators. The shared query contract uses a bounded limit of 1–200 and a literal text query of up to 200 characters. Offset pages reflect separate reads. Keep a stable sort and reconcile changes if records may move between pages.

For an advanced filter, JSON-encode the filter in the query parameter. Example intent:

```
{"all":[{"field":"priority","operator":"in","value":["high","critical"]},
        {"field":"title","operator":"contains","value":"database"}]}
```

GraphQL and errors

Use the governed GraphQL read explorer or the documented endpoint for a bounded read. It uses record, tenant and field authorization. Review the response errors and run a simpler projection to isolate a restricted or unknown field.

Status	Check
400 or 422	Request body, allowed fields, query operator, enum values, or workflow validation.
401	Application session or required verification.
403	Role, tenant, field/record access, or same-origin requirements for the operation.
404	Path, gateway availability and authorized visibility of the record.
409	Current state, expected version, conflicting update or exhausted capacity.
429 or 503	Backoff guidance, provider health and application capacity. Verify prior mutation outcome before retrying.