Record access policies

10 declared fields for Record access policy. Required fields include Name, Target table, Operation, Decision.

https://docs.qintoravacloud.com/forms/acl_rule/

About this form

Use this reference to identify built-in form labels, data types, and validation. Specialized workspaces can render a subset of these fields or provide workflow-specific controls. Your role, record state and tenant configuration can change what you see.

Registry key

`acl_rule`

Record label

Record access policy

Field definitions

Field	Type or reference	Built-in rules	Choices and constraints
Name `name`	text	Required Default list field	—
Target table `targetTableId`	reference schema_table	Required Default list field	Use an authoritative table such as work_items, task, ci or a business table. Views, partitions and projection aliases are rejected.
Target field (empty: entire record) `targetFieldId`	reference schema_field	Optional by default	Optional field on the selected table. Read masks this field; create/update guards changes. System identity and credential fields cannot be selected. Lookup display fields `label`
Operation `operation`	select	Required Default list field	`read`, `create`, `update`, `delete`
Decision `effect`	select	Required Default list field	`allow`, `deny`
Role (empty: all roles) `roleId`	reference roles	Optional by default	—

Field	Type or reference	Built-in rules	Choices and constraints
User (empty: all users) `subjectUserId`	reference users	Optional by default	—
Active `active`	boolean	Default list field	—
Change reason `reason`	textarea	Required	—
Expected version `version`	number	Optional by default	Current policy version. Saving checks this value to prevent overwriting another administrator’s change.

Verification evidence

The disposable audit exercised 9 applicable validation assertions on this definition. The authenticated collection read returned HTTP 200. See the verification matrix for scope.

Collection read results by built-in role

These statuses were observed over HTTP with one role per disposable MFA account. A successful list response can be empty and does not establish individual record, field, or write access.

Role	HTTP status
Asset Manager	403
Change Manager	403
CMDB Manager	403
Contract manager	403
Customer service agent	403
Customer service customer	403
Customer service manager	403
Datacenter Customer	403
Datacenter Fulfiller	403
Datacenter Manager	403
Datacenter Vendor	403
EH&S auditor	403

Role	HTTP status
EH&S manager	403
Executive Reader	403
Field service dispatcher	403
Field service technician	403
HR case agent	403
HR knowledge manager	403
HR lifecycle manager	403
HR profile manager	403
Employee Relations investigator	403
HR service catalog administrator	403
Inventory Counter	403
ITIL Fulfiller	403
Knowledge Manager	403
Business Manager	403
Platform Administrator	200
Service Desk Agent	403
Vendor manager	403
Third-party risk manager	403
Employee with no workspace role	403

Edit and verify

1. Open the list from the appropriate workspace and select an existing record or a permitted create action. Confirm the intended tenant and record number.
2. Use the visible controls for the current record type and state. For reference fields, select a returned record from the lookup. Fill visible required fields and use the dedicated workflow action when the record has approval or completion gates.
3. After saving, reopen the record and compare its persisted values, state and activity to the intended change. Check the downstream linked record when the action creates one.

Troubleshoot

- Missing field or control: compare the role, module, record state, form conditions and tenant overrides.
- Lookup returns no result: check that the referenced record is active, in scope and compatible with the current field.
- Save is rejected: keep the exact validation message and compare the field key, choice, constraints and required related records.
- See Edit and troubleshoot records and Configuration Studio.