ERP integration · WORKDAY

Provider REST API integration with an explicit request/response mapping. A provider-specific API schema or approved adapter is required; selecting a product does not configure its API.

https://docs.qintoravacloud.com/integrations/erp-integration/workday/

Prerequisites

- Protected HTTPS provider API
- Secret Manager credential
- Provider-approved purchase-order payload and response reference mapping

Configuration steps

1. Configure a protected read-only test path
2. Map purchase-order fields to the provider schema
3. Run the real authenticated API test
4. Submit an approved test order and reconcile its returned provider reference

Provider fields

Field	Type	Requirement and options
Authentication scheme `authScheme`	select	Required `bearer_token`, `api_key`, `basic`, `oauth2_client_credentials`
Protected read-only API test path `testPath`	text	Required
Purchase-order API path `submissionPath`	text	Required
Provider reference response path `referencePath`	text	Required Dot-separated JSON path, for example data.orderNumber.

Field	Type	Requirement and options
Read-only order lookup `reconciliationPath`	text	Optional Optional HTTPS same-origin GET path. Include {orderId} in the path or query; it is replaced with the original idempotency key.
Response request key `reconciliationKeyPath`	text	Optional Dot-separated path to the original request ID in the response. It must match exactly to confirm the delivery.
Provider request JSON mapping `requestTemplate`	textarea	Required JSON values can reference {{order.number}}, {{order.quantity}}, {{order.unitCost}}, {{order.currency}}, {{model.modelNumber}} and other saved order/model fields.
API-key header name `apiKeyHeader`	text	Optional
OAuth token URL `tokenUrl`	url	Optional
OAuth scopes `scope`	text	Optional

Verify and troubleshoot

Test with the narrowest supported non-production scope. Confirm that the connection test reaches the expected provider and that the preview or receipt matches the intended scope. Check identity, credential references, network access and provider permissions before retrying. Record the failure stage and redact sensitive payloads when escalating.