Verify an external integration from connection to receipt

Distinguish configured, reachable, authorized and fully verified provider behavior.

https://docs.qintoravacloud.com/guides/provider-verification/

Define the result you need

Integration	Minimum end-to-end evidence
OIDC, SAML or SCIM	A real approved tenant, successful assigned identity, rejected unassigned identity, and matching provisioned user and access evidence.
Directory import	Complete scoped read, matching preview, applied receipt and intended account changes.
Cloud inventory and cost	Verified provider identity, authorized scope, complete response and reconciled inventory or billing evidence.
Discovery	Read-only connection, preview, scheduled run and persisted class, source and relationship evidence.
ERP	Authenticated protected test, approved sandbox order and provider reference, then reconciled outcome or receipt.
Software deployment	Eligible target, approved deployment, provider terminal status and verified installation.
Notification channels	Authorized test recipient, provider message ID and final status or inbound callback where applicable.
Teams	Configured tenant, app permissions and authorized test action with an observed provider result.
Knowledge and AI	Approved retrieval scope, authorized and denied evidence tests, and the observed provider or fallback receipt.
Attachments	Authorized upload, real scan result, checksum-matched retrieval and denied access check.
Agent interoperability	Approved peer or client, exact protocol contract, scoped identity, matching challenge and receipt.

Run a disposable acceptance test

1. Find the integration profile in its product collection and write down the intended operation and expected final result. Choose one test account, recipient or resource. Verify the tenant and endpoint in the connection before creating a test record.

2. Run the connection test and verify the provider identity and scope. Where available, run a read-only preview and compare returned counts, identifiers and pagination. Record the connection or run ID.
3. Create one disposable transaction only when the provider and tenant are approved for test writes. Follow the product's approval action. Record the original correlation or idempotency key before submitting. Compare the initial response with the provider's terminal status and the saved Qintorava record.
4. Test one denied operation, such as an out-of-scope resource or unassigned identity. Confirm the provider and Qintorava have no unintended record or receipt. When a failure is ambiguous, query by the original key before resubmitting. Close or reverse the disposable transaction through the product's approved action.

Record and recover

Record the provider, environment, credential alias, allowed scope, test method, request ID, and final verified result. Keep credentials and customer payloads out of the receipt. If the provider is unavailable or unconfigured, record that condition and verify the failure behavior with the smallest supported check. If a request may have caused an external effect, reconcile by its original identifier before repeating it.

The demo health check reported Teams unconfigured. The public provider list contained no active SSO provider, and the signed-in workspace showed no SAML or SCIM connections. The displayed cloud demo connections showed failed latest billing syncs, and the Vertex AI usage telemetry view reported stale data. A tenant needs approved sandbox accounts, endpoints, recipients and credentials to establish current provider outcomes. See the verification matrix.