QORTARA CLOUD GOVERNANCE

Getting Started

````
# Getting Started

Register your first agent, enforce a policy, and run a compliance scan in under 10 minutes.

## Prerequisites

- An Azure Marketplace purchase or direct Qortara Governance account.
- A tenant ID from your provisioning flow.
- An API key or session token for your environment.
- An agent workload that can call the Qortara policy evaluation API before tool execution.

## 1. Authenticate

Use your issued API credential in the `Authorization` header.

```bash
curl https://api.qortara.com/v1/agents \
  -H "Authorization: Bearer $QORTARA_API_KEY"
```

## 2. Register An Agent

Create an agent record so policy decisions and compliance evidence can be tied to a stable identity.

```json
{
  "name": "customer-support-agent",
  "framework": "langchain",
  "environment": "production"
}
```

## 3. Create A Policy

Start with a narrow runtime policy, then expand once you can see decisions in the audit stream.
````

```yaml
name: production-data-egress
effect: deny
when:
  tool.category: external_write
  data.classification: restricted
```

4. Evaluate A Tool Call

Call policy evaluation before the agent executes a sensitive tool action.

```bash
curl https://api.qortara.com/v1/policy/evaluate \
  -H "Authorization: Bearer $QORTARA_API_KEY" \
  -H "Content-Type: application/json" \
  -d @request.json
```

5. Run A Compliance Scan

Run a scan to package decisions, policy versions, and evidence references for review.

```bash
curl https://api.qortara.com/v1/compliance/scans \
  -H "Authorization: Bearer $QORTARA_API_KEY"
```

Next Steps

- Read Policy Enforcement to understand runtime decisions.
- Read Compliance Evidence before sharing artifacts with an auditor.
- Read Integrations to route governance events into existing security workflows.

Product: Qortara Cloud Governance
Source owner: Qortara
Last reviewed: 2026-04-10
Verified against: Qortara pre-launch docs