Splunk Integration

Splunk Integration

The Splunk integration forwards Qortara governance events into Splunk HTTP Event Collector (HEC) as structured JSON, so policy decisions, compliance results, and audit records land in the same place your team already runs searches, dashboards, and alerts.

This integration is delivered by Qortara Cloud Governance, the hosted platform, which is in pre-launch. The webhook delivery system that pushes events to HEC is part of that hosted platform and has not launched yet. Treat this guide as a reference for how the integration is designed to work rather than as a description of a running service. The HEC configuration steps, SPL searches, CIM mappings, and event schema below are accurate reference material and are safe to review and prepare against now; the live event flow becomes available when Qortara Cloud Governance launches.

How it works

Qortara Cloud Governance is designed to emit a governance event whenever something worth recording happens: a policy is evaluated, a compliance scan completes, a budget cap is crossed, and so on. When you register a Splunk HEC endpoint as a webhook destination, the platform is designed to deliver each event to that endpoint over HTTPS as a single JSON document in Splunk's HEC envelope.

You configure two things: a HEC token and index in Splunk, and a webhook destination in Qortara that points at your HEC URL. After that, events are designed to arrive in your chosen index with the `qortara:governance` sourcetype, ready for the searches in this guide.

Step 1: Configure HTTP Event Collector in Splunk

These steps run in Splunk and do not depend on Qortara being live; you can complete them now to be ready.

1. In Splunk Web, go to **Settings** then **Data Inputs** then **HTTP Event Collector**.
2. Confirm HEC is enabled under **Global Settings**. Keep **Enable SSL** on. Qortara is designed to refuse delivery to non-HTTPS endpoints.
3. Choose **New Token**.
4. Name the token (for example, `qortara-governance`).

5. Set the destination index. A dedicated index such as `qortara` is recommended so you can tune retention separately from other data.
6. Review and submit. Copy the generated token value; you will paste it into Qortara.

Your HEC endpoint URL follows Splunk's standard form:

```bash
# Splunk Cloud
https://http-inputs-<your-stack>.splunkcloud.com:443/services/collector/event

# Splunk Enterprise (self-managed)
https://<your-splunk-host>:8088/services/collector/event
```

You can verify the token works with a manual test event before Qortara is involved:

```bash
curl -k "https://<your-splunk-host>:8088/services/collector/event" \
  -H "Authorization: Splunk <your-hec-token>" \
  -d '{"event": "qortara hec test", "sourcetype": "qortara:governance"}'
```

A successful call returns `{"text":"Success","code":0}` and the test event appears in your index.

Step 2: Register the webhook in Qortara

When Qortara Cloud Governance is available, you register the Splunk HEC endpoint as a webhook destination from the Qortara portal:

1. Open **Webhooks** in the portal and add a destination.
2. Set the URL to your HEC event endpoint (the `/services/collector/event` URL from Step 1).
3. Add an `Authorization` header with the value `Splunk <your-hec-token>`.
4. Optionally filter which event types are forwarded. High-volume tenants often forward only the event types they search on.
5. Save and send a test delivery to confirm the event reaches Splunk.

The webhook is designed to use at-least-once delivery. See [Troubleshooting](#troubleshooting) for deduplication guidance.

Event types forwarded

Qortara Cloud Governance is designed to forward the following event types. Volume figures are planning estimates, not guarantees.

| Event type | Description | Typical volume |

| --- | --- | --- |
`policy_evaluation`	Every policy decision (allow / deny / needs_review).	100 to 10,000 per day per agent
`audit_event`	Cryptographically signed audit record.	1:1 with policy_evaluation
`compliance_scan_result`	Framework scan results (SOC 2, GDPR, EU AI Act, NIST AI RMF).	1 to 100 per day per tenant
`trust_federation_lookup`	Cross-organization attestation queries.	Variable
`saga_verification`	Action-outcome reconciliation results.	1:1 with sensitive actions
`budget_cap_alert`	Triggered at 50 / 80 / 100 percent of a budget cap.	Event-driven
`rate_limit_exceeded`	Per-tenant rate limit violations.	Event-driven
`tenant_lifecycle`	Signup, upgrade, downgrade, and suspension events.	Low volume

Sample event payload

Every event is designed to use this envelope. With `KV_MODE = json` (see field extractions below), Splunk extracts `event_type`, `tenant_id`, `agent_id`, and `decision` as fields automatically.

```json
{
  "event": {
    "event_type": "policy_evaluation",
    "event_id": "evt_abc123...",
    "timestamp": "2026-04-09T17:23:45.123Z",
    "tenant_id": "qor:your-tenant-id",
    "schema_version": "1.0",
    "data": {
      "agent_id": "agent_xyz789",
      "policy_id": "pol_456def",
      "policy_name": "data-access-restriction",
      "decision": "deny",
      "reason": "Agent lacks permission to access resource type 'customer_pii'",
      "resource": "customers/12345",
      "action": "read",
      "evaluation_duration_ms": 12,
      "framework_context": ["soc2", "gdpr"]
    },
    "merkle_hash": "a1b2c3d4..."
  },
  "sourcetype": "qortara:governance",
  "time": 1712687025.123
}
```

Field extractions (optional)

Qortara sends well-structured JSON that Splunk parses automatically. Add these extractions for cleaner timestamp handling and CIM compatibility.

Recommended `props.conf`:

```ini
[qortara:governance]
KV_MODE = json
TIME_PREFIX = "timestamp":"
TIME_FORMAT = %Y-%m-%dT%H:%M:%S.%3NZ
SHOULD_LINEMERGE = false
TRUNCATE = 0
```

CIM (Common Information Model) compatibility

Mapping Qortara events into Splunk's CIM data models lets them participate in Splunk Enterprise Security data models (such as Alerts, Authentication, and Change) automatically. Add these aliases:

```ini
[qortara:governance]
FIELDALIAS-cim-action = decision AS action
FIELDALIAS-cim-user = agent_id AS user
FIELDALIAS-cim-src = policy_id AS src
FIELDALIAS-cim-dest = resource AS dest
FIELDALIAS-cim-signature = policy_name AS signature
EVAL-vendor = "Qortara"
EVAL-product = "Qortara Cloud Governance"
```

Example Splunk searches

Once events are flowing, these searches give you immediate value. They assume the `qortara` index and the `qortara:governance` sourcetype.

1. Policy denials in the last hour:

```spl
index=qortara sourcetype="qortara:governance" event_type="policy_evaluation"
decision=deny
| stats count by agent_id, policy_name
| sort -count
```

2. Compliance scan failures by framework:

```spl
index=qortara sourcetype="qortara:governance" event_type="compliance_scan_result"
status=failed
| stats count by framework, check_id
| sort framework
```

3. Budget cap approaching trend:

```spl
index=qortara sourcetype="qortara:governance" event_type="budget_cap_alert"
| timechart span=1h count by threshold_percent
```

4. Top 10 agents by policy evaluation volume:

```spl
index=qortara sourcetype="qortara:governance" event_type="policy_evaluation"
| stats count by agent_id
| sort -count
| head 10
```

5. Saga verification mismatches:

```spl
index=qortara sourcetype="qortara:governance" event_type="saga_verification"
result=mismatch
| table _time, agent_id, action, expected_outcome, actual_outcome
```

6. Rate limit violations by tenant:

```spl
index=qortara sourcetype="qortara:governance" event_type="rate_limit_exceeded"
| stats count by tenant_id, endpoint
| sort -count
```

7. Trust federation cross-org lookups:

```spl
index=qortara sourcetype="qortara:governance" event_type="trust_federation_lookup"
| stats count by source_org, target_org
```

```

8. Policy decision rate by type (dashboard panel):

```spl
index=qortara sourcetype="qortara:governance" event_type="policy_evaluation"
| timechart span=5m count by decision
```

9. Audit log integrity (should be 100 percent signed):

```spl
index=qortara sourcetype="qortara:governance" event_type="audit_event"
| stats count AS total, count(eval(merkle_hash!="")) AS signed
| eval integrity_pct = round(signed/total*100, 2)
```

10. Tenant lifecycle events (last 7 days):

```spl
index=qortara sourcetype="qortara:governance" event_type="tenant_lifecycle"
earliest=-7d
| stats count by lifecycle_event
```

11. Slowest policy evaluations (latency investigation):

```spl
index=qortara sourcetype="qortara:governance" event_type="policy_evaluation"
| sort -evaluation_duration_ms
| head 20
| table _time, agent_id, policy_name, evaluation_duration_ms
```

12. Correlation: policy denials preceding incident alerts:

```spl
(index=qortara sourcetype="qortara:governance" event_type="policy_evaluation"
decision=deny) OR (index=security sourcetype="incident" severity=high)
| transaction agent_id maxspan=5m
| where eventcount > 1
| table _time, agent_id, decision, policy_name, incident_type
```

Recommended dashboards

A starting set of panels for a governance overview:
```

- Policy decision rate by type over time (search 8).
- Denials by agent and policy for the current window (search 1).
- Compliance scan failures by framework (search 2).
- Audit log integrity percentage (search 9).
- Budget cap alert trend (search 3).
- Slowest policy evaluations for latency triage (search 11).

Cost and volume planning

Estimate your Splunk ingest volume before committing. These are planning estimates for a fully running deployment, not commitments.

Qortara tier	Daily events	Daily volume
Developer (4 or fewer agents)	1,000 to 5,000	about 0.5 to 2.5 MB per day
Professional (5 to 25 agents)	25,000 to 150,000	about 12 to 75 MB per day
Enterprise (100 or more agents)	1M to 10M	about 500 MB to 5 GB per day

For high-volume deployments, filter event types in the webhook configuration and consider a dedicated Splunk index with tighter retention.

Security considerations

- Store HEC tokens in your team's secret manager. Never commit them to source control.
- TLS is required. Qortara is designed to refuse delivery to non-HTTPS endpoints.
- Every event includes a `merkle_hash` field for tamper verification.
- Events leave Qortara's hosting region and cross the public internet to reach your HEC endpoint. Account for that in your network and data-handling reviews.

Troubleshooting

Events not appearing in Splunk

1. Check the Qortara portal under **Webhooks** then **Delivery history** for HTTP status codes.
2. Verify the HEC token is still valid in Splunk Web.
3. Check the `_internal` index for HEC errors.
4. Contact support@qortara.com with your tenant ID.

Duplicate events

The webhook is designed to use at-least-once delivery, so you may occasionally receive a duplicate. Deduplicate on the unique `event_id` field:

```spl
```

```
index=qortara sourcetype="qortara:governance" | dedup event_id
```

Reference links

- Splunk HEC setup: docs.splunk.com
- Planned Splunkbase listing: [splunkbase.splunk.com/qortara]
(https://splunkbase.splunk.com/qortara)
- Integration support: support@qortara.com
- Integration requests and partnerships: [support@qortara.com]
(mailto:support@qortara.com)

Product: Qortara Cloud Governance
Source owner: Qortara
Last reviewed: 2026-06-10
Verified against: Awaiting app-dev integration validation