QSENTIA CONNECT

Connect for brokers and family offices.

A practical guide for approved partners who want to ingest QSentia model outputs, evidence, telemetry, and signed updates through a controlled API layer.

Model-output API

Pull entitled models and latest signal packages into research systems, OMS workflows, dashboards, or internal risk tooling.

Evidence before allocation

Backtests, trade/order logs, drawdowns, live paper returns, and broker status support due diligence before capital is approved.

Signed webhooks

Receive model updates through HMAC-signed webhooks after your endpoint has passed test delivery.

Operational controls

Every key is scoped by customer, model entitlement, environment, and rate limit.

Usage and billing records

API calls and webhook deliveries create audit and usage records for partner review.

Capital stays gated

Live allocation is separate from Connect ingestion and happens only after diligence, approvals, and operating checks.

Web guide · qsentia.com/connect/user-guide
Apply for access · qsentia.com/connect/onboarding

From first review to production ingestion.

The Connect workflow is deliberately staged so an investment team can evaluate model evidence while the technical team validates secure delivery before production use.

1. **Review model evidence**
   Use the marketplace and model pages to review public evidence, live paper status, backtest metrics, and sample logs.

2. **Submit Connect application**
   Provide organization details, integration type, target models, expected API volume, and receiving workflow.

3. **Approval and scope**
   QSentia approves the partner, creates the customer record, sets model entitlements, and assigns request limits.

4. **Receive API key**
   Store the sandbox or production key in a secret manager. Do not place it in browser code, notebooks, or spreadsheets.

5. **Pull and validate outputs**
   Call the models endpoint, fetch latest signals, reconcile timestamps, and record the QSentia model id in your internal systems.

6. **Register webhooks**
   Add HTTPS endpoints, verify signatures, send test events, and enable scheduled delivery only after test logs are clean.

7. **Operate and audit**
   Monitor usage rows, webhook deliveries, billing status, and model entitlement changes in the Connect portal.

RECOMMENDED ACCEPTANCE TEST

- ✓ The partner can list entitled models and see only approved model ids.
- ✓ The latest-signal endpoint returns a current timestamp, evidence id, signal payload, and broker-status context.
- ✓ The receiving webhook verifies the QSentia signature and records the event id idempotently.
- ✓ Usage events and webhook deliveries are visible in the Connect portal after the test run.

Minimum endpoints for a partner integration.

Approved partners use a bearer API key. Production systems should fail closed when rate limits are exhausted or signatures cannot be verified.

METHOD	ENDPOINT	PURPOSE
GET	`/api/connect/v1/models`	List entitled models, broker status, latest signal time, and live return context.
GET	`/api/connect/v1/models/{model_id}/latest-signal`	Fetch the latest signal package for one entitled model.
GET	`/api/connect/v1/webhooks`	Review registered endpoints and delivery state.
POST	`/api/connect/v1/webhooks`	Register a receiving endpoint for signed delivery.
POST	`/api/connect/v1/webhooks/test`	Queue and dispatch a test event.

Example API request

```
# Environment
BASE=https://www.qsentia.com
MODEL=btc-futures-sentiment-daily

# List entitled models
curl -s "$BASE/api/connect/v1/models" \
  -H "Authorization: Bearer qs_sandbox_your_key"

# Fetch the latest signal for one model
curl -s "$BASE/api/connect/v1/models/$MODEL/latest-signal" \
  -H "Authorization: Bearer qs_sandbox_your_key"
```

Webhook verification

`X-QSentia-Event-Id`	Unique delivery identifier — record it idempotently.
`X-QSentia-Event-Type`	The kind of model update being delivered.
`X-QSentia-Timestamp`	Delivery time, included in the signed payload.
`X-QSentia-Signature`	HMAC signature to verify before processing.

Verify before processing. Compute HMAC-SHA256 over `timestamp + "." + raw request body` and compare it to the delivered signature before acting on any event.

How partners should run Connect safely.

Connect is not intended to bypass investment diligence. It gives partners a controlled way to ingest model output while preserving security, entitlement, monitoring, and audit records.

Security

Bearer keys are scoped and revocable. Webhook secrets are stored server-side and shown once to the partner.

Rate limits

Requests are constrained per minute and per day. Partners should monitor limit headers and back off before exhaustion.

Usage records

API calls and webhook deliveries write audit and usage rows for operational and commercial review.

Capital workflow

Evidence and Shadow Mode come first. Actual capital enters selected models only after gated approval and account setup.

PARTNER LAUNCH CHECKLIST

- ✓ Integration owner and technical owner are named.
- ✓ Target model ids and environment are approved by QSentia.
- ✓ API key is stored in a secret manager and rotated when ownership changes.
- ✓ Webhook receiver uses HTTPS and validates QSentia HMAC signatures.
- ✓ Test webhook event is accepted, logged, and idempotently handled.
- ✓ Usage logs and billing-meter rows are reviewed before production delivery is enabled.
- ✓ Internal investment workflow records model id, signal timestamp, evidence id, and downstream action.

Q SENTIA

Need onboarding help?

inquiries@qsentia.com
qsentia.com/connect/onboarding