

MULTI-STORE CDM · HITL FINANCIAL GATES · EXCEPTION CENTER

AI E-commerce Operations & Autonomous Retail Management Platform

Dockerized AIECOM for multi-store CDM ingest (Shopify / Woo / Custom / Magento), policy RAG, MCP order & inventory agents, HITL refund/PO/price gates, Exception Center, forecast / warehouse / SQL / eval, ERP-carrier-EDI stubs, learning loops, and cost hard-stop — governed commerce ops AI, not a checkout chatbot.

M0–M10
MILESTONES CLOSED

PASS
PHASE 1 / MVP / 3

1.0.0
API VERSION

PASS
M10 CLOSEOUT SMOKE

Built by **Abdul Basit** · AI Automation Engineer

BUSINESS IMPACT

Fewer silent automation fails · safer money paths · audit-ready retail ops
Stores→CDM→agents→HITL→exceptions · unauthorized actions 0 · approval compliance 100% · silent financial failures 0 · Phase gates Met

OVERVIEW

Commerce platforms ingest into a shared CDM. FastAPI owns RAG, MCP allowlists, HITL, Exception Center, forecast/warehouse/content/pricing/SQL/eval, learning, retention, and the ops dashboard. n8n runs thin HTTP wrappers with a global DLQ. **Shopify/ERP remain systems of record**; Magento/ERP/carrier/EDI depth is fixture/API-first. Live production cutover is formally waived (**W-01**) for sandbox acceptance.

TYPE

AI commerce operations platform (not a single n8n Zap)

ROLE

AI Automation Engineer / Commerce Ops AI Engineer

DELIVERY

API 1.0.0 · Milestone M10 · Closeout 2026-09-12 · Milestones doc v1.11

STACK

FastAPI · n8n · Postgres · Redis · Qdrant · MinIO · store fixtures · notify stubs · Compose aiecom

PORTS

API **8001** · n8n **5679** · Auth: X-API-Key + X-RoLe

BUYERS

Retail / multi-store ops teams needing gated, grounded automation

THE PROBLEM

- Multi-store chaos — no shared CDM
- Silent fails — webhook errors look OK
- Ungoverned AI — refunds/POs without HITL
- Stock lag — reorder without audit
- Exception fog — no queue / resume
- No closeout — hard to prove gates

THE SOLUTION

- FastAPI AIECOM — CDM, agents, HITL
- Thin n8n — ingest / notify / DLQ
- MCP ACL — audited tool denies
- HITL gates — refund / PO / price
- Exception Center — SLA + resume
- Cost hard-stop — daily budget enforce

WHO IT SERVES

- Teams needing gated commerce AI
- Ops needing exception queues
- Works without live vendor keys
- Lead: **\$6.1 delay** → HITL → DLQ
- Secondary: Magento · forecast · SQL

CAPABILITY SURFACES

SURFACE	FOCUS	SURFACE	FOCUS
Ingest / CDM	Shopify · Woo · Custom · Magento · idempotent DLQ	Agents / MCP	Order Ops · inventory · CX · supplier
HITL / EXC	Refund · PO · price · assign/resolve/resume	Ops UI	/ops/ui/ · cost · metrics · tenant KPIs
P1 depth	Forecast · WH score · content · SQL · eval	P2 depth	ERP · carrier · EDI · learning · K8s docs

Demo lead: shipping-delay investigate → notify → exception/HITL. **Secondary:** Magento fixture ingest · MCP deny · cost hard-stop. **Closeout:** m10_closeout_smoke.py PASS · ACCEPTANCE Signed (sandbox).

Architecture rule: FastAPI owns AI / AuthZ / HITL / CDM · n8n stays thin · financial writes require approval · poison/fail → DLQ (never silent) · Shopify/ERP remain SoR · env-only secrets.

LAYERED ARCHITECTURE & CAPABILITIES

Architecture, journeys, agents, and safety proofs

Principle: FastAPI owns agents, HITL, RAG, MCP, and CDM; **n8n owns thin side effects** — no god-workflow. Data plane and governance are first-class layers (see page 5 diagram).

Stores (Shopify / Woo / Custom REST / Magento)
→ FastAPI ingest (normalize + idempotent upsert) + MinIO raw payloads
→ Postgres CDM · Qdrant policy/product RAG · Redis kill-switch / rate limits
→ Agents/MCP allowlists · HITL (refund/PO/price) · Exception Center
→ P1: forecast / warehouse / content / SQL / eval
→ P2: ERP sync · carrier rate-shop · EDI 855 · learning export · K8s docs
→ Ops UI /cost /metrics · n8n DLQ · m10 closeout smoke

COMPONENT	ROLE IN THE SYSTEM
Ingest adapters	Platform envelopes → CDM; POST /ingest/fixtures/{platform} ; poison → DLQ
Ops UI + API	/ops/ui/ ; Auth X-API-Key + X-Role ; leadership tenant summary
MCP server	Per-agent allowlists; analyst cannot update_order_status ; denies audited
HITL / Approvals	REFUND_HITL_USD / PO_HITL_USD ; price apply blocked without approval
Cost / kill-switch	COST_HARD_STOP denies LLM/MCP writes over budget; admin kill-switch

INTELLIGENCE

- Policy/product RAG + citations / no-answer
- Order Ops investigate (delay / OOS / payment)
- Forecast with assumptions + uncertainty
- Text-to-SQL allowlisted SELECT only
- Eval scorecards + human_corrections export

INTEGRATIONS

Shopify / Woo / Custom	M2 fixtures
Magento	M9 adapter demo
ERP inventory	/integrations/erp/*
Carrier / EDI	Rate shop · 855 stub
K8s / live prod	Docs / W-01

SAFETY & OPS

- HITL before money moves
- Poison ingest → DLQ (silent_success=false)
- Kill switch + retention job
- Learning PII redaction
- Append-oriented audit_events

LEAD DEMO PATH (\$6.1–\$6.3)

- \$6.1 delay investigate + stub notify
- \$6.2 inventory scan → reorder → PO HITL
- \$6.3 low-confidence → exception (no financial guess)
- Magento order_created fixture ingest
- Ops UI open exceptions + /cost/summary

SECURITY PROOF POINTS

Missing API key → **401**. Analyst MCP write denied + audited. Refund/PO/price without approval blocked. Force-fail notify / poison ingest never silent. UAT: unauthorized **0** · approval **100%** · silent financial failures **0**.

RELIABILITY · M0-M10 · PHASE GATES

Reliability, full milestone unlock, Phase gates, closeout

RELIABILITY AND COMMERCE SAFETY

AREA	WHAT SHIPPED
Auth	X-API-Key + X-RoLe (ops / finance / admin / service...)
MCP	Per-agent allowlists · audited denies
HITL	Approve before refund / PO / price apply
DLQ	Poison ingest · force-fail notify paths
Cost	Soft alerts + COST_HARD_STOP hard deny
Retention	/admin/retention/run · pending approvals untouched
Audit	Agent runs · approvals · tool denies · integrations

PHASE GATES + CLOSEOUT

• Phase 1 (M4) — multi-store CDM; RAG; MCP; confidence escalate; injection privilege escalation → 0	
• MVP / Phase 2 (M7) — \$6.1–\$6.3; five P0 n8n; HITL; Exception UI; unauthorized → 0 ; silent fails → 0	
• Phase 3 (M10) — P1 forecast/SQL/eval; P2 Magento/ERP/learning/K8s; docs+KT; sandbox Met; live W-01	
m10_closeout_smoke.py	PASS (health 1.0.0 · MCP deny · poison non-silent)
API version	1.0.0
Closeout date	2026-09-12
Evidence chain	docs/m2 → m4 → m7 → m8 → m9 → m10

MILESTONES M0-M10 (ALL COMPLETE) — WHAT UNLOCKED

ID	THEME	WHAT UNLOCKED
M0	Kickoff & architecture	Stack, principles, commerce non-goals (Shopify/ERP remain SoR)
M1–M2	Skeleton → CDM ingest	Compose, RBAC, kill-switch, Shopify/Woo/custom adapters, DLQ
M3–M4	RAG → Phase 1	Citations, inventory risk/reorder HITL, MCP Order Ops, Phase 1 Met
M5–M6	Returns → n8n demos	Refund HITL, CX/supplier, P0 workflows, \$6.1–\$6.3 smoke
M7	Exception UI / MVP	Ops dashboard, cost/OBS, MVP_GATE Signed
M8–M9	P1 → P2 polish	Forecast/WH/SQL/eval; Magento/ERP/carrier/EDI; learning; hard-stop
M10	Docs / UAT / KT	OPS-05 finals, ACCEPTANCE Signed, Phase 3 Met, API 1.0.0

CDM / INGEST

Idempotent upsert · MinIO payload refs · Magento extension · fixture ingest paths for UAT.

AGENTS + HITL

- MCP tool allowlists
- Low-confidence escalate
- Refund / PO / price gated

OPS + RECOVERY

- Exception assign/resolve/resume
- pg_dump backup smoke (runbook)
- Cutover checklist + KT pack

Concrete reliability: no-key → 401 · MCP overreach denied · financial writes need HITL · poison → DLQ · unauthorized / silent financial fails at UAT: **0**.

Delivery truth: M0–M10 complete · Phase 1/MVP/3 Met · m10 smoke PASS · API 1.0.0 · cite live 1.0.0 version.

OUTCOMES · TECH · DEPTH · HONEST SCOPE

Stack, UAT, n8n catalog, residual risks

TECH STACK + REPRODUCE

FastAPI 1.0.0 · n8n · Postgres · Redis · Qdrant · MinIO · Compose aiecom

docker compose up -d --build · python docs/m10/samples/m10_closeout_smoke.py

Surfaces: /ops/ui/ · /health · /docs · n8n:5679 · Auth: X-API-Key + X-Role

SCOPE HONESTY

- No fabricated client logos or reviews
- Fixture/API-first stores without live credentials
- Waivers: live cutover (W-01), live Magento/ERP/carrier/EDI
- Not a Shopify replacement — full AIECOM M0–M10

M10 CLOSEOUT EVIDENCE INDEX

DOC	PURPOSE
UAT.md / ACCEPTANCE.md	Golden paths Met · PRD Complete/Waived · Signed sandbox
CUTOVER.md / RUNBOOK.md / KT.md	Deploy checklist · day-2 ops · KT agenda
API.md / SECURITY.md / DEMO.md	OPS-05 finals
m10_closeout_smoke.py + uat_results.json	Health 1.0.0 · MCP deny · Magento · eval/cost baseline

DASHBOARD

Exceptions	Open / resolve / SLA
Cost	Summary · hard-stop
Tenant KPIs	Leadership strip

P1 / P2

Forecast / WH / SQL	M8
Content / pricing	M8
Magento / ERP	M9
K8s guide	Docs

N8N CATALOG

- commerce_ingest / order_*
- inventory / returns / notify
- supplier_monitoring / followup
- approval_callback / error_global

N8N (THIN CALLERS)

Ingest · order exception · inventory · returns · supplier · notify · approval callback · global error — env API key only; no secrets in workflow JSON.

RESIDUAL RISKS (HONEST)

Live store/ERP sandboxes · prod TLS/secret rotation · LLM quality · wet-ink acceptance — tracked as M10/M9 waivers; **none reopen Phase gates**.

SAMPLE JOURNEYS + GATES

\$6.1 Delay investigate	\$6.2 Reorder HITL	\$6.3 Low-confidence EXC	Returns HV refund HITL
Magento Fixture ingest	MCP Unauthorized deny	Poison DLQ non-silent	Closeout Smoke PASS

ONE-LINER

AIECOM — Dockerized FastAPI + n8n commerce ops: multi-store CDM, MCP agents with HITL, Exception Center, forecast/warehouse/SQL/eval, Magento/ERP stubs, learning + cost hard-stop — M0–M10 complete at API 1.0.0.

Upwork CTA: paste UPWORK_UPLOAD.md · gallery: architecture PNG → before/after PNG → this PDF (visuals on page 5) · optional Loom from LOOM_SCRIPT.md .

SYSTEM VISUALS

Architecture & before / after

