

Manifesto Auto - Sales OS rooftop install

Agency runbook. No prices. HITL never auto-sends.

Commercial runbook for Manifesto Agency installing this CRM on a dealership. Not marketing copy.

1. One rooftop = one stack

Piece	Rule
Vercel project	One project per rooftop (or per dealer group with tenant isolation). Scope manifesto-atlas.
Neon	Dedicated database. Never Manifesto Headshot, never the public website Neon, never another dealer.
This repo	manifestoauto-crm is the Sales OS kernel (ADR-004).
Brand site	manifestoauto.com stays marketing lime. This app is dealership SaaS blue.

2. Brand

Set NEXT_PUBLIC_* (or edit config/brand.ts):

- PRODUCT_NAME, SHORT_NAME, COMPANY_NAME, SUPPORT_EMAIL, LOGO_TEXT
- PRIMARY_COLOR default #0A5CFF · ACCENT_COLOR default #3B82F6
- POWERED_BY=false for a silent fork

Export tokens: GET /api/brand/tokens (JSON or ?format=css).

3. Auth

- Better Auth email/password.
- Production **requires** BETTER_AUTH_SECRET (openssl rand -base64 32).
- NEXT_PUBLIC_APP_URL / BETTER_AUTH_URL = the rooftop origin.
- CRM_REQUIRE_AUTH=true in production. Seed demos may open the floor.

4. Automotive Intelligence (directory)

Rooftop CRM holds **this store's** units and leads. The cited **model/brand directory** (DuckDB on Rig1) is the Automotive Intelligence layer - Sales OS light (Resources + refuse ranks), AgentOS full (generations, trims, market_series). Spec: ENTITY_CATALOG.md. Do not point CRM Neon at the encyclopedia. Do not invent city volumes or APR.

5. Intelligence (cloud vs local)

All model calls go through lib/llm-gateway.ts. Floor drafts still HITL.

Env	Effect
LLM_PROVIDER=rules (or no keys)	No network. Rules coach only. Air-gap demo.

Env	Effect
LLM_PROVIDER=omniroute	Free/cheap OpenAI-compatible router. OMNIRoute_BASE_URL default http://127.0.0.1:20129/v1, model auto/best-free. Local path. HITL drafts only - never scrape, never auto-send.
LLM_PROVIDER=local	OpenAI-compatible on-network. Default http://127.0.0.1:11434/v1 (Ollama). Also LM Studio, vLLM, llama.cpp.
LLM_PROVIDER=cloud	xAI if XAI_API_KEY, else OpenAI if OPENAI_API_KEY, else LLM_BASE_URL + LLM_API_KEY.
LLM_PII_MODE=redact	Default. Strip email/phone/SSN before cloud. Local may passthrough (store-internal).
LLM_PII_MODE=local_only	Never call cloud even if cloud keys exist. If local is down -> rules fallback.

Dealership IT that must keep customer text off the public internet: LLM_PROVIDER=local and LLM_PII_MODE=local_only.

Settings -> Intelligence is **read-only** (install-time). GET /api/health exposes llm and photo without keys.

6. Listing Studio photos

Lot stills stay on the unit. **Photos** inside Listing Studio is the Shoturo-class offer. It queues a **named scene + light** job (kind: listing_photo). A human approves before any public gallery use. Catalog / OEM stills live in Automotive Intelligence (Lance + DuckDB on Rig1) and must not replace this VIN.

Do **not** use a Gemini / Imagen API key as the listing renderer - those models redraw the car. Empty plates are an offline Rig1 job. Live listing pixels are **matte + plate composite** (POST {PHOTO_BASE_URL}/v1/listing-composite).

GET /api/health sets features.listingPhotoCompositor=true only when PHOTO_BASE_URL is set **and** GET {PHOTO_BASE_URL}/health returns { ok: true, service: "listing-compositor" }. Langflow on this Mac (127.0.0.1:7860) is **not** the compositor.

Env	Effect
PHOTO_PROVIDER=rules	Default. Intent + optional crop-export when Blob/R2 is on.
PHOTO_PROVIDER=local	On-network compositor (PHOTO_BASE_URL, default http://127.0.0.1:7865).
PHOTO_PROVIDER=cloud	Compositor at PHOTO_BASE_URL only. Gemini/Imagen/diffusion hosts are blocked. LLM_PII_MODE=local_only (or PHOTO_PII_MODE) falls back to rules. Do not set this in production.
PHOTO_API_KEY	Optional Bearer for the compositor. Never exposed on health/catalog.

Local / Rig1 process (matte + named plate, not BiRefNet, not Gemini):

```
npm run compositor # 127.0.0.1:7865
npm run compositor:status # fail-closed probe
# PHOTO_PROVIDER=local
# PHOTO_BASE_URL=http://127.0.0.1:7865
```

Rig1 bind for Tailscale/LAN: PHOTO_COMPOSITOR_HOST=0.0.0.0 npm run compositor. Point CRM at that host. Production stays PHOTO_PROVIDER=rules until that URL answers.

Integrity always blocks damage fill, rust removal, odometer change, plate swap, VIN hide. Allowed: background, lighting, crop, shadow.

7. Isolation checklist

- [] Neon project is this CRM only (docs/DATA_PLANE.md)
- [] Automotive Intelligence (Lance + DuckDB, if installed) is Rig1 Auto-only - not this Neon
- [] No Headshot / Ghost / Cal env copied in
- [] Webhook secret set for public ingest
- [] ALLOW_SEED_RESET=false in production
- [] Live voice dial **off** (VOICE_LIVE_DIAL_ENABLED unset)

8. Smoke

```
curl -s "$ORIGIN/api/health" | jq '.ok, .llm, .photo, .features.listingPhotoDesk'
curl -s "$ORIGIN/api/agents" | jq '.autoSend, .agents[].id'
```

Then: login -> pipeline has seed or imported leads -> /approvals HITL queue -> Listing Studio copy / photos never publish.

9. Entitlements

Unlock only what was sold:

- NEXT_PUBLIC_ENTITLEMENT_SALES_OS=true
- AgentOS / Academy false until those packages are on the SOW

Packages are **Academy** -> **Sales OS** -> **AgentOS**. White-label is a layer, not a fourth SKU.

10. Agents

GET /api/agents is the catalog for MCP / ops. autoSend and liveDial are always false.

11. Provision a rooftop (not the hosted demo)

Metro Auto (metro-auto) is the hosted production demo. Do not treat it as a paying rooftop. Do not invent a contract value or live dealer inventory.

A real store is a second tenant. The master admin must already exist (npm run seed:admin). Then:

```
TENANT_SLUG=acme-motors TENANT_NAME="Acme Motors" TENANT_TIMEZONE=America/New_York \
npm run provision:rooftop
```

That creates tenants if missing, attaches SEED_ADMIN_EMAIL as tenant admin, writes HITL-safe defaults (autoSend=false, autoPublish=false, quietHoursEnforce=false), and optionally a white-label overlay (layer, not a SKU). It never deletes Metro Auto demo data. Price / entitlements stay env-driven - this command does not write USD.

Do **not** set CRM_TENANT_ID / CRM_TENANT_SLUG unless you intend to switch the install default off Metro Auto.

Dealer-site ingest (contact required; HITL draft only):

```
curl -s -X POST "$ORIGIN/api/webhooks/lead" \
-H 'content-type: application/json' \
```

```
-H "x-crm-secret: $CRM_WEBHOOK_SECRET" \  
-H "x-crm-tenant: acme-motors" \  
-d '{"firstName":"Taylor","lastName":"Reed","email":"t@example.com","vehicleInterest":"2024  
Camry","source":"dealer-site","draftFirstResponse":true}'
```

The dealer website still has to POST. This path is not a paid rooftop until a SOW, entitlements, and their site are wired.

12. Floor walk after install

- Home and Settings: Sales OS walk (8 steps). **Send walk lead** posts POST /api/leads/walk and queues a HITL first-response only.
- Settings: quiet-hours enforce toggle holds first-response as draft in the quiet window. Nothing auto-sends either way.
- Settings: download /sales-os-install.pdf (this runbook).
- AgentOS Cron: On/Off + Run now. Jobs queue drafts. Open /approvals?status=pending.
- If LLM_PROVIDER=omniroute (or local), first-response may polish the rules template. Critique still runs. autoSend stays false.