

Synapse-Apex — Administrator Guide

For administrators responsible for deploying, configuring and running Synapse-Apex. For day-to-day bid work, see the [User Guide](#).

1. Deployment

Prerequisites

- Docker and Docker Compose.
- (Optional) An Anthropic API key to enable AI features.

First run

```
cp .env.example .env
# edit .env – at minimum set a strong JWT_SECRET; optionally ANTHROPIC_API_KEY
docker compose up -d --build
```

Open **http://localhost:3000**.

On first boot the backend creates the database schema and **seeds** reference data: the administrator account, compliance frameworks, resource types, effort rules, licence costs, and the default workflow template.

Key environment variables (.env)

Variable	Purpose
JWT_SECRET	Signing secret for auth tokens — set a long random value
ADMIN_EMAIL / ADMIN_INITIAL_PASSWORD	The seeded administrator (created once, on first boot)
ANTHROPIC_API_KEY	Enables AI extraction/generation. Leave blank to run AI-disabled
ANTHROPIC_MODEL	Generation model (default <code>claude-opus-4-8</code>)
UPLOAD_MAX_MB	Max upload size

DEFAULT_CURRENCY	Currency label (default GBP)
------------------	------------------------------

Note (this version): the schema is created on startup rather than via migrations. If you change the data model between versions, reset the volumes with `docker compose down -v` (destroys data) before `up`. Alembic migrations are the planned follow-up (see `DECISIONS.md`).

Default login

`ADMIN_EMAIL` / `ADMIN_INITIAL_PASSWORD` from `.env` (defaults `admin@synapse.local` / `ChangeMe123!`). You are forced to change the password on first login.

2. Administration area

Open **Administration** from the sidebar. Tabs available to administrators:

Users

- **Create user:** email, name, a temporary password and one or more roles. The user must change the password at first login.
- **Roles** are toggled per user by clicking the role chips (greyed = not held).
- **Deactivate** performs a soft delete — the account can no longer sign in, but its history remains in the audit trail.
- Safeguards: you cannot delete your own account, and you cannot remove/deactivate the **last** administrator.

Roles: **Administrator**, **Bid Manager**, **Contributor**, **Finance**, **Approver**, **Read-Only**. All access is enforced server-side; the UI only hides what a role cannot use.

Security (MFA & AI Integration)

- **Enforce MFA** toggles organisation-wide MFA. When enforced, any user without MFA is required to enrol (scan QR + confirm a code) at their next login before reaching the app. When optional, users may still enrol voluntarily.
- **AI Integration (Assistant)** — an on/off switch for the **Assistant**, an *additional* advisory tool. It does **not** replace the existing AI extraction/generation. When enabled, Bid Managers may switch on a per-bid Assistant that advises the team, self-checks its output for hallucinations, and proposes response enhancements for human approval. When disabled, no bid can use the Assistant. If no `ANTHROPIC_API_KEY` is configured, the toggle still works but the Assistant returns clearly-labelled placeholders (and its self-check cannot run) until a key is added.

Frameworks

- **Add, amend** (edit name/description inline), **toggle active on/off**, and **delete** compliance frameworks. Frameworks are data — capability responses and bid responses align to whichever frameworks are selected. Toggling a framework **off** hides it from bid selection (and from the Assistant's framework-alignment) without deleting it or affecting bids that already use it. Seeded set: ISO 27001, ISO 9001, Cyber Essentials Plus, NIST CSF, SOC 2, GDPR/DPA 2018.
- When AI is active, the per-bid Assistant can suggest how to **better align a response to a framework** (see the User Guide -> Assistant).

Resources (also available to Finance)

- **Resource types**: add, amend and delete the roles used to cost delivery. Each carries a **cost rate** and **sell rate**.
- **Rate basis toggle**: switch the whole table between **Hourly** and **Daily** rates. Editing a rate keeps the other basis in sync ($\times/\div$ 8). Deleting a resource soft-removes it from selection.
- **Export CSV** for offline editing; import is available via the API.
- **Licence costs**: add, amend (inline edit of name, vendor, unit, unit cost, billing) and delete the software/licence lines that feed the cost engine. Units are per endpoint / per user / per site / flat; billing is monthly / annual / one-off.

Effort rules

The rules that convert endpoint counts into resource hours (e.g. "per 100 workstations -> 32h Service Desk Analyst/month", "per site -> 8h + 16h one-off Network Engineer", fixed roles). These are **data, not code** — amend them to match your delivery model. Each rule targets a resource type and produces recurring and/or one-off hours.

Access: effort rules can be **added, amended and deleted by Administrators, Bid Managers and Finance**. Each rule has a trigger (`per_endpoint`, `per_site` or `fixed`), an endpoint type (for `per_endpoint`), a "per quantity", a target resource type, and recurring / one-off hours. All changes are recorded in the audit log against the acting login.

Workflow

Displays the default workflow template — stages and milestone offsets (working days before submission). New bids are instantiated from this template. Stages and milestones are stored as editable data.

Audit

The **global** audit log across the whole system: logins and MFA events, user and role changes, framework/resource/rule changes, bid state changes, approvals, exports and AI runs. Per-bid trails are also available inside each bid's **Activity** tab.

3. How the modules fit together

1. **Capability library** (sidebar -> Capability library): upload service and technical architecture documents; the system extracts capabilities and drafts framework-aligned "win" responses. Approve capabilities to make them reusable — only **approved** capabilities ground bid responses.
2. **Bid response engine**: per bid, upload the tender -> review requirements -> generate grounded responses.
3. **Cost engine**: endpoint counts + effort rules + rate catalogue -> cost sheet (plus user-entered non-people costs).
4. **Pricing**: contingencies + margin -> priced scenarios with AI justification.
5. **Resource catalogue**: the master rates/licences that the cost engine consumes (Administration -> Resources).
6. **Package**: assemble -> approve -> export.
7. **Answer Library** (sidebar -> Answer Library): a searchable catalogue of tender questions and responses that **fills itself** — approved responses are harvested automatically, and won/lost outcomes are stamped onto entries. Users search and reuse proven answers (and insert them straight into new responses), which is the single biggest lever for winning more tenders: reuse what already won, faster. - **Harvest approved** (Administrators / Bid Managers) back-fills the Library from all existing approved responses in one click — run it once after upgrading to v2. - Curators (Bid Manager, Contributor) add/edit answers, tag/categorise, mark **master** answers, and archive weak ones. All Library actions (create, edit, master, archive, reuse) are audited. - Search is keyword + filter (category, client, outcome, framework) in this MVP; semantic/AI-ranked search is a planned enhancement (see the blueprint in docs/ANSWER_LIBRARY_BLUEPRINT.md).

Because rates, effort rules, frameworks and workflow are all **data**, you can tailor the system to your organisation without code changes.

4. AI configuration

- Set `ANTHROPIC_API_KEY` to enable AI. The default model is `claude-opus-4-8`.
- **After editing `.env`, recreate the containers** so the key is picked up — `docker compose up -d --force-recreate backend worker` (a plain restart does not re-read `.env`). Confirm with `docker compose exec backend printenv ANTHROPIC_API_KEY`.
- **AI status indicator**: the dashboard header shows a live status pill — **green "AI connected & working"**, grey "AI not configured", or red "AI error" (hover for the reason and model; click to re-check). It calls `GET /api/ai/status`, which makes a minimal live call to verify the key, model and connectivity. If it shows red with "Invalid API key" or "Cannot reach the Anthropic API", fix the key / network and re-check.
- **If you change `requirements.txt` or upgrade the app, rebuild the image**: `docker compose build backend worker && docker compose up -d`.

- With no key, all AI steps **degrade gracefully** to clearly labelled placeholders so the workflow remains fully usable.
- AI is used for: capability extraction & response drafting, tender requirement extraction, bid response generation, and pricing justification. Word limits set on requirements are passed to the model as hard limits.
- Token usage is recorded against each AI call for cost visibility.
- **Governance:** all AI output is a draft requiring human review; the system never submits anything externally.

5. Operations

Backups

```
# Database
docker compose exec postgres pg_dump -U apex apex > backup_$(date +%F).sql
# Uploaded documents
docker run --rm -v synapse-apex_uploads:/data -v "$PWD":/backup alpine \
  tar czf /backup/uploads_$(date +%F).tgz -C /data .
```

Logs & health

- Backend health: `GET /api/health` (also used by the container healthcheck).
- Structured logs are emitted by the backend and worker containers (`docker compose logs -f backend worker`).

Tests

```
docker compose run --rm backend pytest -q
```

Covers the exact-decimal cost/pricing maths and the working-day back-scheduler.

Scaling background work

Document parsing and AI generation run on the Celery **worker** container via Redis. Run more workers by scaling the service: `docker compose up -d --scale worker=3`.

6. Security notes

- Passwords are bcrypt-hashed; accounts lock for 15 minutes after 5 failed attempts.
- Access tokens are short-lived (15 min); refresh tokens rotate.

- RBAC is enforced on every endpoint server-side.
- The audit log is append-only. Keep `JWT_SECRET` secret and rotate it if leaked (rotating invalidates existing sessions).
- Restrict who holds the **Administrator** and **Finance** roles — they control users, system data and commercial rates.