



User & Admin Guide

A dockerized platform to scrape, track, and manage UK public and private sector tender opportunities for Cyber Security Services (MDR, SOC, Incident Response, Vulnerability Management, CTI, and more).

1. Getting Started

Prerequisites

- Docker Desktop (or Docker Engine + Docker Compose v2) installed and running.
- Ports 8080 (web), 8000 (API), and 5432 (database) free on your machine.

Launch the application

From the project root, copy the environment template and start the stack:

```
cp .env.example .env
docker compose up --build -d
docker compose logs -f backend
```

Then open the dashboard in your browser:

Service	Address
Web Dashboard	http://localhost:8080
API documentation	http://localhost:8000/docs
Health check	http://localhost:8000/health

2. First-Run Setup & Logging In

Bid Sentinel does not ship with a default account. The **first time** you open the dashboard, the login screen detects that no users exist and instead shows a **Create administrator account** form.

Create your administrator

- 1 Enter your full name, email address, and a password (minimum 8 characters), then confirm the password.
- 2 Click **Create admin account**. You are signed in automatically as an administrator.

- 3 The setup form locks itself permanently once this first account exists — afterwards the screen shows the normal **Sign in** form.
- Your session is stored securely in the browser using a JWT token, so you stay logged in across page refreshes and browser restarts (persistent session).
 - Click **Sign out** in the top-right corner to end your session.
 - Additional users (admin or standard) can be created later by an administrator — see section 9.

3. Using the Dashboard

The dashboard shows a customisable **Performance overview** at the top, followed by the full table of cyber-security opportunities.

Light & dark mode. A sun/moon button in the header (and on the sign-in screen) switches between light and dark themes. Your choice is remembered on that browser; first-time visitors follow their operating system's preference automatically.

Performance overview (analytics)

A strip of KPI cards and charts summarises bid performance and updates instantly as you change a bid status or outcome. Use the toggles to pivot the data:

- **KPI cards** — Total tracked, Open now, Bidding, Pipeline value, Closing in 14 days, **Win rate**, and **Value won**. Once an opportunity's outcome is **Lost** it drops out of the **Bidding** count and its amount is removed from **Pipeline value**, so those cards always reflect the live pipeline.
- **Measure** toggle — switch every chart between opportunity **Count** and total **Value (£)**.
- **Date** toggle — base the time chart on Published or Closing dates.
- **Range** toggle — 90 days, 12 months, or All time.
- **Pivot by** — break the data down by Portal, Keyword, Buyer, Bid status, or Outcome.
- Charts: bid pipeline by status, opportunities over time, the configurable pivot breakdown, and demand by service line. Use **Hide** to collapse the whole panel.

Table columns

Column	Description
Opportunity Name	Title, buyer, matched keyword, and detected certifications
Fit	Capability fit % (see Capability fit & certifications below)
Published	Date the notice was published
Closing	Submission deadline, with a 'days left' countdown
Value (£)	Contract value (numeric) or raw text for ranges/POA
Duration	Contract length or start/end dates
Bid Status	Interactive dropdown: Pending / Bid / No Bid
Outcome	Result dropdown: Awaiting / Won / Lost (drives win rate)
Link	Opens the original notice on the source portal

Searching, filtering and sorting

- **Search box** — filter by opportunity title or buyer name.
- **Status filter** — show only Pending, Bid, or No Bid opportunities.
- **Portal filter** — show opportunities from a single source portal only.
- **Sort** — order the table by Published date, Closing date, Value, or Title, using the Asc/Dsc toggle to switch direction.

Capability fit & certifications

Bid Sentinel scores how well each opportunity matches your services. In **Settings** → **Capability profile & fit**, build a profile of the services you offer in two ways: **add terms manually**, and/or **upload a service-overview document** (PDF, DOCX or TXT) to **generate terms from its content** — then tick the ones to keep (use Select all / Clear to help). Generation is local keyword extraction by default, or AI when the AI enhancement is enabled.

- **Fit %** on each row is the share of your capability terms the opportunity mentions. Hover it to see exactly which terms matched, and sort the table by **Fit %** to surface the best matches first.
- **Certifications** required/mentioned in a notice (Cyber Essentials Plus, ISO 27001, CHECK, SC/DV clearance, and more) are detected automatically and shown as amber chips under the opportunity name.
- After changing your profile, click **Recompute fit & certs** to re-score existing opportunities (new ones are scored automatically).

This is deterministic and explainable: it matches the exact terms in your lists, so widen coverage by adding terms. Nothing is sent to any external service.

AI enhancement (optional)

For richer results you can switch on the optional AI enhancement in **Settings** → **AI enhancement** (administrators only). When on, a low-cost Claude model produces a concise **AI summary** (shown at the top of the expanded view), a reasoned **Fit %**, and more accurate certifications, clearances and technical requirements. It requires an API key to be configured; if none is set the toggle is disabled and Bid Sentinel stays fully deterministic and offline. After switching it on, click **Recompute** to apply it to existing opportunities (new ones are analysed automatically).

A slow-blinking status dot in the dashboard header shows the AI Assistant at a glance: **green** when it is active (enabled and a key configured), **red** when it is off.

Recording decisions and outcomes

Each row has two colour-coded dropdowns. The **Bid Status** column (Pending / Bid / No Bid) records your decision to pursue an opportunity. The **Outcome** column (Awaiting / Won / Lost / **No Bid** / **Disregarded**) records the result once a bid concludes — this feeds the Win rate and Value won figures. Setting the **Bid Status** to **No Bid** automatically defaults the **Outcome** to **No Bid** (you can still change it afterwards). Setting an outcome to **Disregarded** marks an opportunity to hide; tick **Hide disregarded** in the toolbar to remove them from the view and the analytics. Both save instantly; if a save fails the dropdown reverts.

Adding an opportunity manually

To track an opportunity Bid Sentinel didn't scrape, click **+ Add opportunity** in the toolbar. Enter at least a **Title** (buyer, value, dates, duration, URL and description are optional) and click **Add opportunity**. It is analysed for certifications, fit and technical requirements just like a scraped one (paste the details into the

Description to get the most out of this), and is labelled **Manual entry** — you can filter to these via the portal filter. A URL is optional; leave it blank and the Link column simply shows “Manual”.

Editing or deleting an opportunity

Expand any opportunity (the arrow beside its name) to reveal **Edit** and **Delete** buttons. **Edit** opens the same form pre-filled so you can correct any detail — certifications, fit and technical requirements are re-analysed when you save. **Delete** removes the opportunity entirely; use this to clear entries that were scraped in error. Deleting shows an **Undo** button in the notice bar — click it to restore the opportunity if you removed it by mistake (see “Undo a deletion” below). Both actions are recorded in the audit trail.

Bulk-deleting unwanted opportunities

Admins see a **checkbox** on each row. Tick several (or use the header checkbox to select every row in the current view), then click **Delete selected** in the toolbar. The chosen opportunities are removed and — crucially — **blocked from being scraped back in**: each one's link and reference are added to a suppression list the scraper checks on every run, so they will not reappear. Use the search and filters first to narrow the view, then select-all to clear a whole category quickly. The action is confirmed before it runs and is recorded in the audit trail.

Undo a deletion

Deleted something by mistake? After any delete — single or bulk — an **Undo** button appears next to the confirmation message. Click it to restore the opportunities and, for bulk deletes, automatically lift the scrape block that was applied. Undo stays available for **14 days** after a deletion (comments are not restored). If the same notice has already been re-scraped in the meantime, that one is skipped.

Tuning out irrelevant types

Some scrapes surface opportunities that are not really Cyber Security — for example catering, grounds maintenance or printer supplies pulled in by a broad CPV code. Each row has a **Tune out** button (admins). Click it and confirm a word or phrase that characterises the type you want gone (a sensible suggestion is pre-filled). Bid Sentinel then removes the matching opportunities immediately and suppresses that type on all future scrapes.

Guardrail: anything Cyber Security related is **always kept**, no matter what you tune out — a term only hides opportunities that also have no cyber-security signal, so you can never accidentally lose a relevant bid. Manage or remove tune-out terms under **Settings** → **Tune-out list** (removing a term lets that type back in on the next scrape). Tune-out changes are recorded in the audit trail.

Expanding an opportunity

Click the **arrow** beside any opportunity name to expand it. The detail view shows three panes:

- **Certifications, accreditations & security clearances** required or mentioned in the notice (clearances such as SC/DV are listed separately).
- **Top technical requirements** — the most relevant requirement sentences scraped from the opportunity description.
- **Comments** — add notes for your team; each comment shows its author and timestamp, and can be deleted by its author or an administrator.

4. Exporting Data

Use the toolbar buttons above the table to export the **currently filtered view**:

- **Export CSV** — downloads a spreadsheet-ready file (opens in Excel / Google Sheets).
- **Export PDF** — downloads a formatted, landscape PDF report of the table.

Tip: apply a search term or status filter first to export just that subset.

Management summary report

Admins and analysts see a **Management PDF** button in the toolbar (and on the Intelligence page). It downloads a concise, board-ready summary of the pipeline: how many opportunities are **tracked, open and being bid on**, the total **pipeline value** and **value won**, a breakdown by bid status, the opportunities currently being bid on, and your **capability** and **certification / clearance gaps**. Pipeline value and the being-bid-on count exclude anything marked **Lost**, so the figures match the dashboard. Where email is configured, an **Email summary** button sends it to your own account address.

Email me this

If outgoing email is configured, **Email CSV / Email PDF** buttons appear alongside the exports (and an **Email me** button on the Intelligence report). These send the report to **your own account email address** — the one you signed in with. If you don't see the buttons, email hasn't been set up on the server (see the Email setup guide).

5. Settings — Bid Portals

Open **Settings** from the top-right of the dashboard. The Settings page is organised into **tabs** — Users & roles, AI enhancement, Capability & fit, Bid Portals, Keywords, CPV codes, Tune-out list, Schedule, and Audit trail (the Users and Audit tabs are visible to administrators only). Click a tab to open that section; only that section is shown, so there is no long page to scroll.

On the **Bid Portals** tab you'll find every portal Bid Sentinel can check. **All portals are selected by default and have an active scraper** — switch any toggle off to exclude it from future scans (admins only). Find a Tender and Contracts Finder use official data APIs (robust); the others use a best-effort web scraper that runs every cycle but may need tuning per site (and credentials for portals that require a login) to return results reliably.

Adding your own portal: use the **Add a portal** form at the bottom of the panel (name, URL, and optional scope). It is registered immediately, marked **Custom**, and can be enabled, scheduled, and later given a scraper. Custom portals can be deleted; built-in ones can only be disabled with the toggle.

Portal	Scope
Find a Tender Service (FTS) [API]	Above-threshold UK public sector procurement
Contracts Finder [API]	Below-threshold England + wider public sector
Sell2Wales	Welsh public bodies
Public Contracts Scotland	Scottish public sector tenders
eTendersNI	Northern Ireland eProcurement
ProContract (Due North)	Regional councils and local authorities
Delta eSourcing	Various contracting authorities
In-Tend	Public sector localized portal instances
Achilles	Utilities, transport and infrastructure

CCS / Government Commercial Agency	Central government frameworks
Digital Marketplace (G-Cloud)	Cloud and digital services frameworks

6. Settings — Keywords

The **Keywords** panel shows the built-in cyber-security terms Bid Sentinel always searches (MDR, SOC, Incident Response, Vulnerability Management, CTI, and more). These cannot be removed.

Adding your own keywords is **optional**. Type a term (for example “Penetration Testing” or “ISO 27001”) and click **Add**; it is then included in every subsequent scan alongside the built-in list. Remove a custom keyword at any time with the × button.

CPV codes

The **CPV codes** tab lets you add Common Procurement Vocabulary codes (the standard EU/UK classification for what a contract is about) to **narrow** the scrape. Enter a **code** (for example 72500000) and an optional **description** (for example “Computer-related services”) and click **Add**.

CPV codes work as a **combined filter with your keywords, not an alternative to them**. When one or more CPV codes are **active**, an opportunity is only kept if it matches a **keyword** AND one of your active **CPV codes** (in its classification or its text). This removes notices that happen to carry a matching CPV code but are not actually about cyber security. If no CPV codes are active, keyword matching alone applies, exactly as before.

Each code has an **Active** toggle. Switch a code off to stop it applying to the scrape without deleting it — handy for temporarily widening or narrowing coverage. The header shows how many of your codes are currently active. Use **Remove** to delete a code permanently.

CPV matching mode. A toggle at the top of the tab controls how strictly CPV codes are applied:

- **Lenient (recommended, default)** — CPV codes only narrow notices that actually publish a CPV classification. Notices from sources that don't expose CPV codes (most HTML portals) are judged on keywords alone, so you don't lose relevant opportunities just because a portal omits CPV data.
- **Strict** — every opportunity must match one of your CPV codes. Anything without a matching CPV code — including notices that publish no CPV data at all — is excluded. Use this only when you want the tightest possible targeting.

If you added CPV codes and noticed fewer opportunities than expected, keep the mode on **Lenient** (or switch a code off). The check-digit suffix is optional — 72500000 and 72500000-0 are treated the same. Remove a code at any time with the **Remove** button. Adding or removing CPV codes is an admin action and is recorded in the audit trail.

Tune-out list

The **Tune-out list** tab manages the negative terms that hide irrelevant opportunity types (see “Tuning out irrelevant types” above). It lists every tuned-out term; each can be removed to let that type back in on the next scrape. You can also add a term here directly. A built-in **guardrail** means a term only ever hides opportunities that have **no** cyber-security signal, so Cyber Security related opportunities are never suppressed.

7. Settings — Scheduling Scrapes

The **Scrape Schedule** panel lets you run Bid Sentinel automatically on **multiple days and times**. To create a schedule:

- 1 Select one or more **days** (Mon–Sun).
- 2 Add one or more **times** with the time pickers (use '+ Add time' for more).
- 3 Click **Add to schedule**. A slot is created for every day × time combination.

Example: choosing Mon & Wed at 09:00 and 17:00 creates four slots. Each slot can be paused/resumed or deleted individually. The panel shows the **next scheduled run** and the timezone in use (default Europe/London). If no slots are set, Bid Sentinel falls back to a regular interval scan.

8. The Scraper Engine

A background worker automatically scans your **enabled portals** on the **schedule you define** (or a regular interval if none is set), keeping only opportunities that match the built-in and custom keyword list — and, when you have set CPV codes, that ALSO match one of those codes. Duplicate notices are detected by URL and reference ID and never inserted twice.

Only live opportunities are brought in. At scrape time the engine ignores **contract award notices** and **closed, cancelled or withdrawn** tenders, and will not import an opportunity whose **closing date has already passed** — so nothing that is already closed is ever added. (Opportunities that publish no closing date are kept, since there is no date to judge them on.)

This filtering applies only when **importing new** opportunities. An opportunity that was scraped while it was open **stays in your table after its closing date passes** — it is never removed automatically — so your history and any bids you tracked against it are preserved. Remove old entries yourself with Delete or the multi-select bulk delete whenever you choose.

Tracked keywords

The built-in list is broad and cyber-specific — e.g. Cyber Security, Information Security, Managed Detection and Response, MDR, SOC, Security Operations Centre, Incident Response, Vulnerability Management / Assessment, Cyber Threat Intelligence (CTI), Penetration Testing, Digital Forensics, MSSP, SIEM, ISO 27001 and more. Add organisation-specific terms on the Keywords tab to widen coverage further.

Running it on demand (admins only)

Administrators see a **Run Scraper** button in the toolbar. Click it to fetch new opportunities immediately. The status message is a full **diagnostic summary**: how many candidates each portal returned, how many were newly inserted, and a breakdown of why the rest were skipped — already tracked, closed/expired, CPV-filtered, tuned-out or suppressed — plus whether the CPV filter is running in lenient or strict mode. If a portal shows **0** candidates or an error, that portal returned nothing (some HTML portals need per-site tuning or a login); if lots were CPV-filtered, switch the CPV mode to Lenient or disable some CPV codes.

9. User Administration (Admins)

Open **Settings** and use the **Users & roles** panel (visible to administrators only) to manage accounts with role-based access control:

- **Add a new user** — enter a full name, email, password (min 8 characters) and a role, then click **Add user**.

- **Change a role** — switch any user between Standard and Admin from the role dropdown.
- **Enable / disable** — click the status pill to suspend or restore access without deleting the account.
- **Reset password** — set a new password for any user inline.
- **Delete** — remove an account. You cannot delete or change the role of your own account (a safeguard against locking yourself out).

Roles

Role	Capabilities
Admin	Everything: manage users, portals, keywords, schedule, run scraper
Analyst	Read-only, plus the Intelligence tab and its PDF report
Standard	View tenders, search/filter/sort, set bid status & outcome, export

Audit trail

The **Audit trail** panel in Settings (administrators only) records application activity — logins and every change — with the actor, action, timestamp, result, and IP address. Use **Refresh** to load the latest entries; the most recent appear first.

10. Analyst Intelligence

Users with the **Analyst** (or Admin) role see an **Intelligence** link in the dashboard header. The Intelligence tab mines the opportunity assessments to surface gaps and sales angles:

- **Capability gaps** — in-demand services appearing across opportunities that your capability profile doesn't cover, ranked by frequency and value.
- **Certification & clearance gaps** — how often each is required versus whether you hold it (from the **Accreditations you hold** list in Settings → Capability & fit). Flags certs that block you.
- **Buyer intelligence** — a profile per client organisation (volume, value, average fit, win/loss, most-requested services) and which are prime targets.
- **Win/loss** and **demand trends** — where you win or lose, and how demand is moving over time.
- **Sales angles** — a concise, data-driven pitch for each target buyer; tick **AI angles** for an AI-written version (requires the AI enhancement).

Click **Export PDF report** to download a branded, printable Intelligence Report covering all of the above for sharing with the wider team.

11. Troubleshooting

Symptom	Resolution
Cannot reach dashboard	Check 'docker compose ps'; ensure containers are 'Up'.
Login fails	Verify ADMIN_EMAIL/PASSWORD in .env; data persists across restarts.
Table is empty	Click 'Run Scraper' (admin) or wait for the scheduled run.
Reset everything	Run 'docker compose down -v' then 'up --build -d'.

Bid Sentinel — UK Cyber Security Tender Platform. User Guide. Always respect the terms of use and rate limits of the source portals when scraping.