

Security & Compliance

How Oracle Health Dashboard protects your credentials, your data and your license. Designed for demanding corporate environments and audits.

On-premise

No telemetry

Encryption at rest

CHAPTER

01 - Design principles

Security is not an add-on: it guides every product decision.

- › **Least privilege** : operates with a read-only Oracle user.
- › **On-premise** : runs entirely on your infrastructure; **no telemetry** or external calls.
- › **Encryption at rest** for credentials and secrets.
- › **No licensed Oracle packs** : base views only (compliance).
- › **Defense in depth** : authentication, brute-force protection, cookie hardening.

CHAPTER

02 - Database access

The dashboard never modifies your databases or uses licensed features.

- › Requires only **CREATE SESSION** + **SELECT_CATALOG_ROLE** (read-only).
- › Uses **base views** exclusively (V\$ / DBA_): **no** Diagnostic or Tuning Pack.
- › Connects in **thin** mode: no Oracle Client to patch or maintain.

› Queries are static and parameterized: **no SQL injection surface** .

! “Base views only” is also a **compliance** control: it avoids accidental use of features that require additional Oracle licenses.

CHAPTER

03 - Credential protection

Your database passwords are stored encrypted and bound to the machine.

ASPECT	IMPLEMENTATION
Encryption	Fernet (AES-128-CBC + HMAC-SHA256)
Key	Derived from the Machine ID via PBKDF2
Scope	Copying profiles.json to another machine does not decrypt anything
Alert secrets	SMTP password and Telegram token also encrypted

▲ **Honest threat model: this is machine-bound encryption.** Anyone who can run the app on that same machine can decrypt (the app must, to connect). It protects against file theft, not against a local administrator.

CHAPTER

04 - Cryptographic licensing

Asymmetric signing: the binary can only verify licenses, never generate them.

Licenses are signed with **Ed25519** (public-key cryptography). The executable embeds **only the public key**; the private key lives exclusively in the vendor generator and is never distributed.

› Extracting or decompiling the binary **cannot** forge licenses.

› 100% **offline** verification: no activation server.

› License bound to a stable **Machine ID** , derived from hardware identifiers.

- › **Annual subscription** : the expiry and database limit are signed into the key itself.
- › Grace period and expiry robust against clock tampering (signed date watermark).

CHAPTER

05 - Authentication & session

Protected access when the dashboard is network-reachable.

CONTROL	DETAIL
Password hashing	PBKDF2-HMAC-SHA256 , 200,000 iterations, random salt
Brute-force protection	5 failed attempts → temporary per-IP lockout
Session cookie	HttpOnly + SameSite=Lax (+ Secure with TLS)
Session signing	Key derived from an internal secret + Machine ID

CHAPTER

06 - Network security

Minimally exposed by default. Network access is an explicit decision.

- › Listens only on **127.0.0.1** by default, in all modes.
- › Network exposure requires an explicit opt-in (**OHD_BIND_HOST=0.0.0.0**).
- › For multi-user access: a reverse proxy with **HTTPS** (IIS/ARR, nginx, Caddy).
- › The health endpoint (**/api/health**) exposes no sensitive data.

✕ Audit recommendation: never publish over plain HTTP on an open network. Use TLS terminated at a proxy, or local access via RDP.

CHAPTER

07 - Data & privacy

Your data never leaves your infrastructure.

- › **No telemetry** : the product sends no usage data to any server.
- › All state (config, history, logs) is stored **locally** .
- › History stores aggregated metrics, not the contents of your tables.
- › Alerts (email/Telegram) are sent only to the recipients you configure.

CHAPTER

08 - Supply chain

Reproducible builds and controlled dependencies.

- › Dependencies **pinned** to known versions (requirements.txt).
- › **XSS** prevention: all data coming from Oracle is escaped before rendering.
- › Docker image based on **python:3.12-slim** , running as a non-root user.
- › The license private key is excluded from every artifact (.gitignore / .dockerignore).