

MaxAudit Verifier – Self-Assessment Toolkit

Version: 1.0

Issued by: SAC, Take Back Your Data (TBYD)

License: MaxOneOpen License v2.2 – Structurally Enforced

1. Purpose

The Verifier module enables MaxOne system operators to independently assess their compliance status. It uses the same cryptographic audit core as the Dongle but is optimized for CI/CD environments, internal monitoring, and development workflows.

2. Execution Modes

- Manual: Local execution on operator's infrastructure
- CI/CD: Pipeline-integrated validation during build/test stages
- Continuous: Background monitoring with real-time alerts (optional)

3. Integration Primitives

- Docker container with reproducible build (signed)
- CLI interface with YAML/JSON output
- Integration hooks for GitLab CI, GitHub Actions, Jenkins, etc.
- Static binary for offline environments

4. Output Artifacts

- Console display of audit result
- JSON result file for automated evaluation
- Optional export of signed audit protocol for regulatory readiness
- Integration-ready status hook (e.g. exit code mapping)

5. Profiles & Fork Awareness

The Verifier supports profile-based validation to account for system-specific architecture forks. Each profile defines expected modules, configuration bounds, and deviation thresholds.

- Default Profile: Standard MaxOne reference instance
- Custom Profiles: Defined by system operators, signed and hash-anchored
- Fork-aware mode: Integrates with Fork Registry for structural compatibility

6. Security & Transparency

- Fully auditable source code (public)
- Verifier binaries signed with SAC release key
- No data retention, no telemetry
- No privileged system access required

7. Self-Healing & Advisory Layer (optional)

An optional advisory engine can be enabled to automatically identify likely causes of deviations and suggest corrections. This layer is non-binding and runs in isolated mode, separate from the audit logic.

8. Operator Responsibilities

- Regular execution is recommended (e.g. weekly or per deployment)
- Operators are responsible for responding to yellow or red audit results
- Local records may be required for legal audit trails