Product security

Encryption in transit and at rest, agent identity and enrolment, sessions, step-up authentication, audit log and signed reports.

Scope

This document summarises the product's security controls as recorded in the public sources of the dossier. Each capability is labelled with its status.

Encryption in transit

Status: Available

- The channel between each agent and the console uses **TLS with mutual authentication**: agent and console authenticate with X.509 certificates before operating.
- The agent always initiates the connection toward the console and maintains a periodic signed heartbeat. No inbound ports are opened on managed servers for this channel and no central SSH keys are held.

Encryption at rest

Status: Available

- Backups are encrypted in stream with **AES-256-GCM** before reaching their destination.
- Hypervisor credentials held by the agent are stored encrypted with **AES-256-GCM**, never in cleartext.
- Key Custody Protocol envelopes are derived with **Argon2id** and encrypted with **AES-256-GCM**.
- Sensitive changes recorded in the log are stored encrypted at rest.
- In the government form, backup encryption cannot be disabled.

The complete algorithm inventory is set out in the algorithms and modules document of this library.

Agent identity

Status: Available

- Each agent has its **own certificate**, issued at enrolment.
- Enrolment is performed with a **single-use token**, of brief validity, bound to the organisation and to a label. When used, the token is consumed and cannot be used a second time.
- At enrolment the server fingerprint is also recorded, which binds the licence to that machine and allows detecting duplications.

- Agent certificates have limited validity, are renewed automatically before expiry and can be revoked; revocation propagates through the agent's own channel.
- For bulk registrations there is a reusable and revocable fleet key, as an alternative to the individual token.

User sessions and authentication

Status: Available

- The console has native sign-in on its own domain and, according to the product form, federated sign-in and institutional providers configured by the institution.
- Sessions have configurable maximum duration and inactivity timeout, and sign-out invalidates the session on the server.
- Sign-in is protected against repeated attempts through rate limiting.
- Users may register **WebAuthn access keys** (passkeys). User verification is mandatory in that flow and the system detects cloning of a key.
- Console roles apply deny-by-default: operator, approver, auditor and read-only, with concrete actions assigned to each role.

Step-up authentication on anomalous context

Status: Available

On anomalous context — for example, a new network address, a new device or an unusual time — the console requires step-up re-authentication before sensitive actions, such as destroying recipes, deciding recertifications or activating governed debug surfaces. Without that valid re-authentication, the sensitive action is denied and the denial is recorded.

Audit log

Status: Available

- Every relevant act is recorded: enrolments, sign-ins, deployments, convergences, approvals, recovery decisions, licence changes, recertifications and authorisation denials, with actor, organisation, moment and outcome.
- Log chains link each entry with the fingerprint of the previous one; altering or deleting an intermediate entry breaks the chain and is detected on verification.
- In the government form, the log is local and exportable to the institution's security event management system.
- Custody documents incorporate a **document forensic mark**, whose existence and purpose — attributing leaks of custody documents — are public. Its format is not disclosed.

Signed reports

Status: Available

Reports the product delivers — validation, audit, backup and recovery — are digitally signed with **Ed25519** through an internal platform module, without depending on an external service. A report without a registered and verified signature is not considered delivered. The third-party verification procedure is set out in the signed reports and public verification document.

Additional declared controls

Status: Available

- Image scanning on recipe admission, with a fail-closed criterion: a quarantined image blocks application.
- In backup verification, restored content is subjected to antivirus analysis; a compromised backup is marked and isolated, and is never deleted automatically.
- Separation of duties in critical operations, including disaster recovery and key custody.