Nikxius

DESIGN-PARTNER EVALUATION · PROPOSED

What the boundary trusts

Security and trust model · Review before granting access

The protected agent is untrusted input to an enrolled operation. The trusted computing base includes the Node and configuration, PostgreSQL and privileged administrators, the configured IdP/JWKS source, Kubernetes API, and customer-controlled admission and credential environment. A compromised Node or cluster administrator is outside the prevention claim.

Identity and credentials

Material	Holder and boundary
Workload JWT	Agent; can propose/inspect its operations. It grants no Kubernetes mutation permission or human role.
Human JWT	Reviewer/sponsor; issuer, audience, registered role, MFA and freshness checked. Synthetic local claims are not real MFA.
Kubernetes token	Node only; mounted read-protected file, reloaded per request, pinned API origin/CA.
Database login	Node uses restricted non-superuser/non-BYPASSRLS role. Separate migration credential is removed after setup.
Evidence key	Optional customer-controlled Ed25519 key file; separate authenticated public-key distribution.

Customer IdP token acquisition is integrated externally. The browser's token handoff is not a full SSO redirect/PKCE client. Identity mappings load at startup; reviewed changes require restart. Task-grant revocation is durable and does not require restart.

Least privilege must include bypass review

Scope the Node to the named resource and required reads/watch/patch. Kubernetes RBAC cannot restrict a patch to one image field; trusted adapter code supplies that restriction. Native admission constraints may add protection and must be tested with the actual controller/admission composition.

The agent must not read Secrets, mint the Node's token, exec into privileged pods, assume another role, invoke an equivalent CI writer or use host access to escape the boundary. The local tests probe named routes. They do not prove that every customer bypass path is absent.

Failure, revocation and break-glass

Missing mandatory authority, policy, approval or durable admission prevents new protected dispatch. That does not recall a request already admitted or stop every delayed sender. Native UID/version/field tests remain necessary. A missing response stays UNKNOWN; no timer converts it to failure.

A Node restart preserves durable operation state in PostgreSQL and ends browser sessions. An old database restore can forget native effects; reconcile the restore gap before reopening writes. Missing native history may leave an outcome unresolved indefinitely.

Customer emergency access remains separately governed. Record the operator, reason, time and native evidence when using it. Never use break-glass to rewrite the original operation as successful, cancelled or nonexistent. The Runtime has no “mark successful” or “reset unknown” endpoint.

Data, evidence and operational responsibility

Operation inputs, identities, decisions, attempts and projected observations stay in the customer’s Node/database. There is no required Nikxius-hosted telemetry or model-provider dependency in this path. Support access and export sharing require explicit scope. Customer infrastructure provides encryption at rest, backups, network controls and retention decisions; their configuration is not established by local tests.

Exports contain supported lifecycle records and stated limits. A signature establishes integrity and attribution under the configured key; it does not establish business correctness, uncompromised execution or independent Kubernetes truth. No automated destructive retention job is supplied; unresolved attempts and consumed identities must not be purged to clear a queue.

No SOC 2, ISO 27001, external penetration test, production SLA, incident-response staffing or customer production acceptance is claimed. Security review is part of the nonproduction evaluation; production needs separate admission.

Source: `docs/security/THREAT_MODEL.md`, `CREDENTIAL_MODEL.md`, `TRUST_BOUNDARIES.md`, `FAILURE_SEMANTICS.md`; `docs/runtime/DEPLOYMENT.md` and `RECOVERY.md`.