Gen-Core AI

TESSARA

Administrator Manual

Configuration, identity, operations and controlled change

Release baseline
Tessara v1.3.0

Audience
Tessara platform administrators, security administrators and service operators

Published
September 2026

Document owner
Gen-Core AI

This manual describes the capabilities and controls present in the Tessara v1.3.0 application baseline. Availability of some actions depends on permissions and deployment configuration.

Gen-Core AI

Contents

DOCUMENT USE	Use the User Manual for daily work, the Administrator Manual for platform configuration and identity operations, and the Feature List for release scope and capability review.

Gen-Core AI

Document control

Field	Value
Product	Tessara
Release baseline	v1.3.0
Document status	Initial controlled issue
Purpose	Controlled operational guidance for configuring and maintaining Tessara v1.3.0 without breaking business traceability or production security.
Owner	Gen-Core AI
Review trigger	Material workflow, permission, navigation or release change

1. Administrator responsibilities

Administration is an operational control surface. Administrators manage configuration, identities, appearance, governance and release operations; they should not silently rewrite business records to bypass the application lifecycle.

- Use least privilege and separate routine administration from assurance and delivery decisions.
- Protect identity, backup, release and audit operations with explicit ownership.
- Test configuration changes in the Mac test environment before production use.
- Preserve customer, assessment, project and audit history during upgrades.
- Record change reason, evidence and rollback path for material changes.

2. Deployment and authentication modes

Environment	Expected approach
Mac test/development	Local Docker deployment used for functional acceptance. Authentication mode may be development and must not be treated as the production security baseline.
Linux production	Reverse-proxied HTTPS deployment with Keycloak authentication. Production packages can enforce temporary password replacement and TOTP MFA.
Portable project-suite integration	The Gen-Core Project Suite package is designed for integration with other Gen-Core platforms through namespaced routes, additive schema changes and host-provided identity context. Integration must be tested per host platform.

Gen-Core AI

SECURITY BOUNDARY	Do not disable or reconfigure MFA, Keycloak, session controls or the protected superadministrator merely to simplify an application upgrade. Authentication changes require their own approved change.

3. User lifecycle and access operations

Open Administration → Users. The protected account is tessara.superadmin.local. Some actions are disabled for protected identities.

Action	Administrator outcome
Create user	Creates an identity with user details, role, scope and enabled state.
Validate	Checks enabled state, MFA configuration, email verification and required actions.
Edit	Maintains profile, role, scope and enabled state.
Enable / Disable	Controls sign-in without deleting the identity.
Reset password	Sets a temporary password of at least 10 characters; change is required at next login.
Reset MFA	Removes current enrolment; enrolment is required at next login where MFA is enforced.
Revoke sessions	Logs the user out of current sessions.
Delete	Removes an eligible identity; protected-user and dependency rules apply.

Recommended user procedure

1. **Authorise.** Confirm requester, role, scope, manager and environment.
2. **Create.** Use a unique username and minimum necessary access.
3. **Validate.** Confirm required actions, email and MFA position.
4. **Communicate securely.** Send temporary access details through an approved channel.
5. **Review.** Periodically disable dormant users and revoke sessions after material access change.
6. **Offboard.** Disable first, revoke sessions, preserve audit evidence, then delete only when policy permits.

4. Catalogues and assurance configuration

Administration area	Managed content
Products & Services	Code, name, type—Assessment, Assurance, Implementation, Remediation, Advisory or Managed Service—description and active state.
Standards & Regulations	Code, name, authority, version, jurisdiction, description and active state.
Assessment Templates	Stages and scoring approach.

Administration area	Managed content
Workflow Configuration	Stages and enforced gates.
Report Templates	Output format and approval expectations.
Dictionaries	Controlled lists used by the platform.
Knowledge	Source authority, summary, implementation guidance, official URL, licence note and tags; maintained from the Knowledge area.

Catalogue change control

- Use stable codes and meaningful versions.
- Archive superseded entries instead of repurposing their identity.
- Validate licensing and source authority before loading standards content.
- Assess the effect on engagement creation, assessment snapshots and reports before activation.
- Use audit history to confirm actor, action, record type and time.

5. Project and workflow configuration

Administration → Project Management stores configurable phases, health values and stage-gate settings. The v1.3.0 operational baseline uses phases Mobilise, Design, Implement, Validate and Close; health values On Track, At Risk, Off Track and Complete.

Control	Administration expectation
Requirement governance	Retain Delivery Execution and Project Control classifications; do not create tasks without an approved driver.
Board stages	Preserve coherent stages across list and Kanban views; validate column deletion and card migration.
Task controls	Maintain accepted task types, priority values, acceptance status, notification fields and colour defaults.
Programme controls	Validate project assignment, cross-project dependency types and resource overallocation reporting.
Lifecycle gates	Do not relax stage gates without a documented operational decision.

6. Notifications and integrations

Area	Configurable items / checks
Notifications	Days, channel, recipient and enabled state. Supported channels include in-application, email, Microsoft Teams and webhook.
Integrations	Enabled state, connection status, endpoint and authentication. Supported authentication choices include OAuth2, API key, client certificate and HMAC-SHA256.
Task notification	Date/time, recipient and message are stored on the action item. Test that enabled notifications include a scheduled time.

Area	Configurable items / checks
Secrets	Credentials belong in protected runtime configuration, not descriptions, labels or exported configuration records.

7. Branding and themes

1. **Prepare the logo.** Use a wide transparent PNG no larger than 1.5 MB.
2. **Preview.** Administration → Branding → choose the PNG. The preview updates before save.
3. **Complete identity.** Set organisation, platform name, support email and footer.
4. **Save and verify.** Confirm navigation and generated-content branding. When a logo is active it replaces the sidebar wordmark.
5. **Maintain themes.** Activate a supplied theme or create/edit a custom theme using the labelled colour controls. Active-theme and built-in protections apply to deletion.

8. Data, AI and feature governance

Area	Governance expectation
Data Management	Use controlled XLSX/CSV exchange, validation preview and backup before bulk mutation.
AI Governance	Set provider/model and retain human-review and evidence-citation requirements. AI output must not overwrite deterministic scores or authorised decisions.
Feature Management	Activate features only after environment-specific acceptance; record dependencies and rollback.
Dictionaries	Use controlled values where dropdowns improve consistency; avoid near-duplicate spellings.

9. Observability, backups and releases

Area	Baseline control
Observability	Health checks enabled; critical support contact maintained.
Backup & Recovery	Daily schedule, 35-day retention, encryption and off-host copy are the supplied configuration defaults; align to policy.
Release Management	Checks and approval required. Preserve current application and PostgreSQL data before upgrade.
Installer safety	Use disposable-database migration validation before live change; stop if validation fails.
Rollback	Restore both application and database from the same protected pre-upgrade point.

Data-preserving upgrade sequence

1. **Confirm scope.** Verify current and target version, platform, package checksum and change approval.

2. **Check prerequisites.** Ensure Docker Desktop is running on Mac; verify disk, ports and dependent services.
3. **Back up.** Create protected application and PostgreSQL backups.
4. **Preflight.** Apply migration and validation to a disposable copy of the current database.
5. **Upgrade.** Apply only after preflight passes.
6. **Validate.** Check release version, core routes, record counts, authentication, key workflows and audit.
7. **Retain evidence.** Keep backup location and diagnostic logs until acceptance and retention policy permit disposal.

10. Security and audit

Control	What to verify
Security mode	Matches environment: development only for controlled test use; production for deployed service.
Realm	Correct Keycloak realm and client configuration for the deployment.
Superadministrator	tessara.superadmin.local remains protected and tightly controlled.
MFA	Required actions and TOTP enrolment operate in production.
Sessions	Revocation works after password, MFA or access changes.
Audit	Administrative changes show actor, action, record type, record identifier and timestamp.
Proxy/TLS	Production FQDN routes only intended paths; HTTPS and security headers validate.

11. Operational checklists

Daily / event-driven

- Review health checks and critical alerts.
- Confirm scheduled backups completed.
- Review failed sign-in, user-lockout or integration events where available.
- Respond to evidence expiry and notification failures through the responsible business owner.

Monthly / release-driven

- Review enabled users, roles, scopes and dormant accounts.
- Test backup restoration in an isolated environment.
- Review active standards, products, workflows and integrations.
- Review programme resource conflicts and project reporting exceptions.
- Export or review audit evidence according to policy.
- Revalidate production MFA and logout behavior after release change.

12. Troubleshooting and recovery

Symptom	Safe response

Symptom	Safe response
Docker Desktop not running	Start Docker Desktop, wait for docker info to succeed, then rerun the Mac installer.
Migration/preflight fails	Do not alter live data. Retain diagnostics, correct the package or data rule, and rerun the disposable validation.
User cannot sign in	Validate user, enabled state, required actions, MFA and session state; avoid bypassing production authentication.
Configuration not visible	Confirm active state, permissions, spelling/code, save confirmation and browser refresh.
Task creation blocked	Create and approve/baseline the matching project work driver.
Programme project unavailable	It is probably assigned to another programme; remove it there before reassignment.
Board column deletion blocked	Keep at least one column and choose a destination for cards in a populated column.
Recovery required	Stop application mutation, identify the correct matched application/database backup, restore in a controlled window and validate before reopening service.