**Document: 03 – Actors & Use Cases**

**Project:** MCPX-KendoBridge Admin Portal  
**Document ID:** TJ-MCPX-DOC-03  
**Version:** 1.0.0  
**Status:** Draft  
**Date:** 2025-09-27  
**Owner:** Doc-Factory (Technijian)  
**Confidentiality:** Technijian Internal

**Document Control**

| **Version** | **Date** | **Author** | **Change Summary** | **Status** |
| --- | --- | --- | --- | --- |
| 0.1.0 | 2025-09-27 | Doc-Factory | Initial draft created from SDLC baseline | Draft |
| 1.0.0 | 2025-09-27 | Doc-Factory | First complete version for review/approval | Draft |

**Approvals**

| **Role/Team** | **Name** | **Signature/Date** | **Comment** |
| --- | --- | --- | --- |
| Director of Software Eng. |  |  |  |
| Systems Architect |  |  |  |
| Security/Compliance |  |  |  |
| DBA |  |  |  |
| QA Lead |  |  |  |

**1. Purpose**

Define the **actors** and **use cases** for the MCPX-KendoBridge Admin Portal, establishing clear responsibilities, access boundaries (RBAC), and end-to-end interaction flows that align with the Technijian SDLC, Azure SSO (Entra ID), and the Figma → **KendoReact (Fluent 2)** implementation.

**2. Scope**

Covers **admin-only** operations: authentication/authorization, health & readiness, configuration/feature flags/lookups (DB SP–backed), evidence visibility, job launch + **SSE** progress streaming, audit trails, and environment-aware operations (Alpha → Beta → RTM → Prod). End-user/tenant-facing experiences are **out of scope** for this document.

**3. Actors**

| **Actor ID** | **Actor Name** | **Description / Responsibility** |
| --- | --- | --- |
| A1 | **Portal Admin** | Human admin assigned via **AAD app role** and/or **group**. Full control over config, flags, jobs, and allow-lists. |
| A2 | **Portal Viewer** | Human read-only user (AAD role/group). Can view dashboards, effective config, and evidence; **no** mutations. |
| A3 | **Identity Provider (AAD)** | Azure AD (Entra ID) handling SSO (MSAL PKCE) and issuing JWTs with app roles/claims. |
| A4 | **Admin API** | .NET 8 service exposing JSON + **SSE**; enforces authZ, rate limits, error envelope; talks to DB via SPs only. |
| A5 | **DB (SQL Server 2022)** | Persists config/feature flags/lookups/audit; accessed via **stored procedures only**. |
| A6 | **Jobs/Workers** | Long-running tasks initiated by Admin API; emit streaming progress events (**SSE**) + heartbeats. |
| A7 | **Observability Stack** | Central logging/metrics/alerts; provides SLI/SLO dashboards and error budgets. |
| A8 | **GitHub Actions (CI/CD)** | CI checks (build/tests/a11y/CodeQL/etc.) and CD promotions with approvals and evidence bundling. |
| A9 | **Microsoft Graph** | Directory read/write for user/group listing and (if enabled) access assignments. |
| A10 | **CORS Clients (Web App)** | Browser SPA (React + **KendoReact Fluent 2**). Must originate from allow-listed Origins per environment. |

**4. Roles & RBAC**

| **Role** | **AAD Construct** | **Permissions (high-level)** |
| --- | --- | --- |
| **Portal.Admin** | App Role / Security Group | Full CRUD on config/flags/lookups; launch jobs; manage CORS allow-list; view evidence/audit |
| **Portal.Viewer** | App Role / Security Group | Read-only access to dashboard, effective config, evidence; **no** mutations |

**Principle:** Server-enforced RBAC; UI hides unauthorized actions for UX, but **never** trusts client-side checks.

**5. Use Case Catalogue (MoSCoW Priorities)**

| **UC ID** | **Name** | **Primary Actor** | **Brief Description** | **Priority** |
| --- | --- | --- | --- | --- |
| UC-01 | Sign in with Azure SSO | Portal Admin | Admin signs in via AAD (MSAL PKCE), role claims issued, session established. | **M** |
| UC-02 | View Dashboard (Health/Ready) | Portal Admin | See service status, versions, uptime, queue depth, p50/p95, error rate. | **M** |
| UC-03 | View Effective Config | Portal Viewer | Read non-secret effective configuration (merged per env). | **M** |
| UC-04 | Manage App Config Keys | Portal Admin | Create/update config keys via SPs; audit trail captured. | **M** |
| UC-05 | Toggle Feature Flags | Portal Admin | Enable/disable flags; target by env/role if supported. | **M** |
| UC-06 | Manage Lookups | Portal Admin | CRUD lookup values safely (add-only schema rules apply). | **S** |
| UC-07 | Launch Job & Stream Progress (SSE) | Portal Admin | Start long-running task and observe live progress/heartbeats. | **M** |
| UC-08 | Review Audit Trail | Portal Admin | Filterable view of who/what/when for mutations and key reads. | **S** |
| UC-09 | Manage CORS Allow-List | Portal Admin | View/edit allowed Origins per env with approval workflow. | **S** |
| UC-10 | Access Control – Assign/Remove Users | Portal Admin | Add/remove users to AAD group or app role via Graph (if enabled). | **S** |
| UC-11 | Evidence Pack – View/Download | Portal Viewer | Access release evidence attached by CI/CD. | **S** |
| UC-12 | RTM⇄Prod Config Parity Check | Portal Admin | Compare RTM intended Prod settings; surface drift before promote. | **S** |
| UC-13 | Rate-Limit & Error Handling | Admin API | Server enforces policies; UI surfaces standardized error envelope. | **M** |

Legend: **M** = Must; **S** = Should; **C** = Could; **W** = Won’t (this release)

**6. Detailed Use Cases**

**UC-01 — Sign in with Azure SSO**

**Primary Actor:** Portal Admin  
**Supporting:** Identity Provider (AAD), Admin API  
**Preconditions:** App registration configured; user assigned to Portal.Admin or Portal.Viewer.  
**Trigger:** User navigates to portal URL.  
**Main Flow:**

1. Web app initiates **MSAL PKCE** auth; user signs in on AAD.
2. AAD issues **ID token** + **access token** with app role claims.
3. Web app stores tokens (session) and calls Admin API with Authorization: Bearer.
4. API validates JWT (issuer/audience/signature/exp) and role claims.
5. UI routes to **/dashboard** with environment indicator.

**Alternative Flows:**

* 1A. **Unauthorized role** → API returns 403 with error envelope; UI shows “no access” and support link.
* 1B. **Token expired** → Silent renew; if fails, force re-auth.

**Postconditions:** Authenticated session with role; telemetry event logged.  
**NFRs:** Login round-trip ≤ 2.0s p95; no refresh tokens stored in localStorage; secure cookie or session storage.

**UC-02 — View Dashboard (Health/Ready)**

**Primary Actor:** Portal Admin (or Viewer)  
**Preconditions:** UC-01 successful.  
**Main Flow:**

1. UI calls /healthz and /ready (JSON).
2. API collects component status (API, DB, Jobs, external deps) and returns metrics (uptime, p50/p95, error rate, queue depth, version).
3. UI renders KendoReact **Cards/Charts** with environment badge.

**Postconditions:** Latest status visible; SLI widgets updated.  
**NFRs:** /healthz p95 ≤ 150 ms; dashboard initial load ≤ 1.5s p95.

**UC-03 — View Effective Config**

**Primary Actor:** Portal Viewer  
**Preconditions:** UC-01 successful.  
**Main Flow:**

1. UI requests GET /config/effective (non-secret).
2. API aggregates DB values and returns merged view with requestId.
3. UI renders Kendo **Grid** with filters/export.

**NFRs:** p95 ≤ 300 ms; supports paging/filtering server-side.

**UC-04 — Manage App Config Keys**

**Primary Actor:** Portal Admin  
**Preconditions:** UC-01 successful; RBAC = Admin.  
**Main Flow:**

1. Admin selects **Add/Update**.
2. UI posts to /config/keys → API executes SP (sp\_Config\_\*) with validation.
3. Change is persisted; **Audit** entry recorded (who/what/when/before→after).
4. UI shows success toast and reflects new value.

**Alt:** Validation error → 400 with envelope; UI shows inline errors.  
**NFRs:** All mutations audit-logged; idempotency key honored to avoid duplicates.

**UC-05 — Toggle Feature Flags**

**Primary Actor:** Portal Admin  
**Flow:** Similar to UC-04 using sp\_Feature\_\*; optional targeting (env/role).  
**NFRs:** Flag read p95 ≤ 5 ms at API (cached); write operations audited.

**UC-06 — Manage Lookups**

**Primary Actor:** Portal Admin  
**Flow:** CRUD via sp\_Lookup\_\* adhering to **add-only schema** (soft-delete/deprecate patterns).  
**NFRs:** Referential integrity validated at SP boundary.

**UC-07 — Launch Job & Stream Progress (SSE)**

**Primary Actor:** Portal Admin  
**Preconditions:** UC-01; RBAC = Admin.  
**Main Flow:**

1. UI POST /jobs with payload + Idempotency-Key.
2. API enqueues **Job** and responds with Job ID.
3. UI opens **SSE** to /jobs/{id}/events with Accept: text/event-stream.
4. Worker emits progress events and **heartbeats** at defined interval.
5. UI updates progress and final state (completed|failed).

**Alt:** Network drop → client retries SSE with backoff; server resumes from last known event ID (if supported).  
**NFRs:** **TTFB ≤ 200 ms** for first SSE event; heartbeat every ≤ 10s; rate-limit protects server.

**UC-08 — Review Audit Trail**

**Primary Actor:** Portal Admin  
**Flow:** Filter by actor, date range, entity; export CSV/PDF; evidence links maintained.  
**NFRs:** Query p95 ≤ 500 ms for 10k entries; PII minimized.

**UC-09 — Manage CORS Allow-List**

**Primary Actor:** Portal Admin  
**Flow:** View/edit Origins per environment; approval workflow (2-person rule optional).  
**NFRs:** Changes effective on next config refresh; all edits audited.

**UC-10 — Access Control – Assign/Remove Users**

**Primary Actor:** Portal Admin  
**Preconditions:** Admin consent granted for Graph write (if enabled).  
**Main Flow:**

1. Search user via **Microsoft Graph**; see role/group status.
2. Add/remove user to **Portal.Admin** or **Portal.Viewer** group/app role.
3. UI confirms; audit entry written.

**Alt:** If write denied, generate a **Change Request** artifact with approver routing.  
**NFRs:** Propagation note displayed; re-login required for new privileges.

**UC-11 — Evidence Pack – View/Download**

**Primary Actor:** Portal Viewer  
**Flow:** Browse releases; download evidence artifacts (build/test reports, CodeQL, SBOM, OpenAPI diff, approvals).  
**NFRs:** Artifacts retained ≥ 1 year; checksums/attestations presented.

**UC-12 — RTM⇄Prod Config Parity Check**

**Primary Actor:** Portal Admin  
**Flow:** Compare RTM intended-Prod settings; flag drift; block promotion if critical deltas present.  
**NFRs:** Deterministic comparison; exportable diff.

**UC-13 — Rate-Limit & Error Handling**

**Primary Actor:** Admin API  
**Flow:** API enforces per-principal/IP/session policy; on breach returns **429** with Retry-After. All errors use standard envelope { code, message, details?, requestId }.  
**NFRs:** Global safeguards prevent noisy neighbors; envelope logged with correlation IDs.

**7. Use Case Diagram (PlantUML)**

@startuml

left to right direction

actor "Portal Admin" as Admin

actor "Portal Viewer" as Viewer

rectangle "MCPX-KendoBridge Admin Portal" {

(UC-01 Sign in with Azure SSO) as UC01

(UC-02 View Dashboard) as UC02

(UC-03 View Effective Config) as UC03

(UC-04 Manage App Config) as UC04

(UC-05 Toggle Feature Flags) as UC05

(UC-06 Manage Lookups) as UC06

(UC-07 Launch Job & Stream (SSE)) as UC07

(UC-08 Review Audit Trail) as UC08

(UC-09 Manage CORS Allow-List) as UC09

(UC-10 Assign/Remove Users) as UC10

(UC-11 Evidence Pack) as UC11

(UC-12 RTM⇄Prod Parity) as UC12

(UC-13 Rate-Limit & Errors) as UC13

}

Admin --> UC01

Admin --> UC02

Admin --> UC03

Admin --> UC04

Admin --> UC05

Admin --> UC06

Admin --> UC07

Admin --> UC08

Admin --> UC09

Admin --> UC10

Admin --> UC11

Admin --> UC12

Viewer --> UC01

Viewer --> UC02

Viewer --> UC03

Viewer --> UC11

UC01 ..> UC13 : uses

@enduml

**8. Traceability**

| **Use Case** | **Key Endpoints (OpenAPI 3.1)** | **DB SPs (indicative)** | **Evidence / Tests** |
| --- | --- | --- | --- |
| UC-01 | /auth/\* (OIDC/MSAL client), token validation | — | Login E2E, role claim checks |
| UC-02 | GET /healthz, GET /ready | sp\_Health\_\* (if used) | Smoke tests; SLI dashboards |
| UC-03 | GET /config/effective | sp\_Config\_GetAll | Contract tests; a11y Grid checks |
| UC-04 | POST/PUT /config/keys | sp\_Config\_SetValue, sp\_Config\_Audit | Unit/integration + audit snapshot |
| UC-05 | POST/PUT /flags | sp\_Feature\_Set, sp\_Feature\_Audit | Feature toggle tests per env |
| UC-06 | \*/lookups/\* | sp\_Lookup\_\* | Referential tests |
| UC-07 | POST /jobs, GET /jobs/{id}/events (SSE) | sp\_Jobs\_\* (if queued in DB) | SSE TTFB/perf tests; resiliency/retry |
| UC-08 | GET /audit | sp\_Audit\_Query | Export & retention tests |
| UC-09 | GET/PUT /security/cors | sp\_Security\_Origins\_\* | Two-person change flow |
| UC-10 | POST /access/\* (Graph proxy) | — (directory ops via Graph) | Role assignment tests / dry-run |
| UC-11 | GET /evidence/\* | — | Artifact checksums/attestations validated |
| UC-12 | GET /config/parity?from=RTM&to=Prod | sp\_Config\_Diff | Promotion gate test |
| UC-13 | — (global) | — | 429 policy tests; error envelope contracts |

**9. Assumptions & Dependencies**

* App roles/groups exist in AAD; CI injects environment variables/URIs.
* SQL access is via **stored procedures only**; schema follows **add-only** rule.
* CORS is allow-listed per environment; origins maintained by UC-09.
* Figma Make is the design SoT; **KendoReact (Fluent 2)** is the delivery component set; ThemeBuilder tokens applied.

**10. Acceptance Criteria (Document Level)**

* Actor definitions, RBAC, and **13** use cases are complete with flows, alt paths, NFRs, and traceability.
* Use-case diagram present; IDs stable and referenced in backlog items.
* All mutating use cases specify **audit logging** and **error envelope** behavior.
* SSE behavior (TTFB, heartbeat cadence, retry guidance) captured for UC-07.

**End of Document — TJ-MCPX-DOC-03 v1.0.0**