**Document: 09 – Test Strategy**

**Project:** MCPX-KendoBridge Admin Portal  
**Document ID:** TJ-MCPX-DOC-09  
**Version:** 1.1.0  
**Status:** Draft  
**Date:** 2025-09-27  
**Owner:** QA Lead (Technijian)  
**Confidentiality:** Technijian Internal

**Document Control**

| **Version** | **Date** | **Author** | **Change Summary** | **Status** |
| --- | --- | --- | --- | --- |
| 1.0.0 | 2025-09-26 | QA Lead | Initial strategy | Draft |
| 1.1.0 | 2025-09-27 | QA Lead | Align to MSAL PKCE, KendoReact Fluent 2, **JSON vs SSE**, CORS allow-list, parity, single k6 path | Draft |

**Approvals**

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

**1. Purpose**

Define **how** we verify MCPX-KendoBridge meets functional and non-functional expectations before each promotion (**Alpha → Beta → RTM → Prod**) and how evidence is captured for audits.

**2. Scope**

* **Admin Web** (React + **KendoReact Fluent 2**)
* **Admin API** (.NET 8; JSON default, **SSE** when negotiated)
* **DB** (SQL Server 2022; **SP-only**, **add-only** schema)
* **Azure SSO** (MSAL PKCE) and optional **Microsoft Graph**
* **CORS allow-list**, **rate limiting**, **error envelope**, **Config Parity** (RTM↔Prod)

**3. Test Taxonomy**

| **Layer** | **Goals** | **Tools** |
| --- | --- | --- |
| **Unit** | Smallest testable units; pure logic, validators, mappers | xUnit/NUnit (API), Vitest/Jest (Web) |
| **Component** | KendoReact components render/props/ARIA | React Testing Library |
| **Contract** | OpenAPI schemas, status codes, error envelope | Dredd/Prism or REST Assured + OpenAPI validator |
| **Integration** | API↔DB (SP calls), API↔MCP (STDIO), Web↔API happy/negative paths | .NET integration tests; Playwright for Web |
| **Security** | AuthZ (roles), CORS, rate-limit, secret scan | Playwright + API client; repo scanners in CI |
| **E2E (Gherkin)** | User-visible flows, SSE behavior, origin policy | Cucumber/Playwright; existing tests/gherkin/\*.feature |
| **Performance (Smoke)** | SSE **TTFB ≤ 200ms**, heartbeat cadence | **k6**: tests/perf/k6\_sse\_ttfb.js |
| **Accessibility** | WCAG 2.2 AA (zero critical) | axe (CI), manual keyboard paths |
| **Parity** | RTM↔Prod config **0 critical diffs** | Parity job + report verification |

**4. Environments & Data**

* **Alpha**: ephemeral DB seeded by migrations + fixtures.
* **Beta/RTM**: stable data; parity check enabled in **RTM**.
* **Prod**: read-only checks only; no destructive tests.

**Test Data**

* Config/Flags/Lookups seeded via **SPs**; fixtures versioned.
* **Secrets** mocked (Key Vault/ENV).
* **Microsoft Graph**: mock or tenant sandbox; toggle tests by feature flag.

**5. Entry & Exit Criteria**

**Entry (per stage)**

* CI green (build, unit, contract, scanners).
* Test data applied; endpoints reachable.

**Exit**

* **Alpha → Beta**: unit/component/integration/E2E pass; axe zero critical.
* **Beta → RTM**: above + perf smoke within SLO; CodeQL/Dependency Review no high/critical (or waivers).
* **RTM → Prod**: above + **Config Parity = 0 critical**; approvals logged.

**6. Test Suites & Key Cases**

**6.1 Authentication & RBAC (MSAL PKCE)**

* **TS-AUTH-01** Login redirect to AAD; successful callback routes to /dashboard.
* **TS-AUTH-02** Invalid/expired token ⇒ **401** envelope with requestId.
* **TS-AUTH-03** **Portal.Viewer** cannot mutate (config/flags/lookups/jobs) ⇒ **403**.
* **TS-AUTH-04** Token renewal path (silent or re-auth) maintains route intent.

**6.2 CORS & Security Headers**

* **TS-CORS-01** Allowed origin succeeds (preflight + request).
* **TS-CORS-02** Disallowed origin ⇒ **403** origin\_forbidden.
* **TS-SEC-01** TLS required; HSTS present.
* **TS-SEC-02** CSP baseline blocks inline/eval (if enabled).

**6.3 Error Envelope & Legacy Endpoints**

* **TS-ERR-01** All errors use { code, message, details?, requestId }.
* **TS-LEG-01** /messages & /sse **OFF** by default ⇒ **403** feature\_disabled.
* **TS-LEG-02** When flag ON, endpoints function and are audited.

**6.4 Config / Flags / Lookups**

* **TS-CONF-01** GET /config/effective returns **non-secrets** only.
* **TS-CONF-02** Add/Update key via endpoint triggers **SP** and writes **audit** (who/what/when/before→after).
* **TS-FLAG-01** Toggle flag updates evaluation; audit written.
* **TS-LOOK-01** Add/Update/Deprecate lookup respects **add-only** rule.

**6.5 Jobs & SSE**

* **TS-JOB-01** POST /jobs returns ID; idempotency prevents duplicates.
* **TS-JOB-02** GET /jobs/{id}/events streams **SSE** with first event **TTFB ≤ 200ms**.
* **TS-JOB-03** **Heartbeat ≤ 10s** when no progress events.
* **TS-JOB-04** Network drop ⇒ client reconnects (optional Last-Event-ID).
* **TS-JOB-05** Terminal completed|failed status with duration; error envelope on fail.

**6.6 Health/Ready & Parity**

* **TS-HLT-01** /healthz includes component states; p95 ≤ 150ms.
* **TS-RDY-01** /ready true only when dependencies healthy.
* **TS-PRTY-01** RTM parity report against **expected Prod** ⇒ **0 critical** before Prod.

**6.7 Evidence & Audit**

* **TS-EVD-01** Release includes Evidence Pack items (OpenAPI diff, CodeQL, SBOM, axe, perf smoke, parity, approvals).
* **TS-AUD-01** All admin mutations produce audit entries retrievable via API/UI.

**6.8 Accessibility (WCAG 2.2 AA)**

* **TS-A11Y-01** Keyboard navigation for all routes; visible focus.
* **TS-A11Y-02** Roles/labels/ARIA states correct; toasts use live region.
* **TS-A11Y-03** Color contrast via tokens ≥ 4.5:1.

**6.9 Rate Limiting**

* **TS-RL-01** Exceed JSON quota ⇒ **429** with Retry-After.
* **TS-RL-02** Exceed SSE stream limits (per principal/IP) ⇒ **429**; logs show throttle reason.

**7. Automation Plan**

**7.1 CI (per PR / main)**

* Build + unit (API/Web), component tests.
* OpenAPI lint/diff (non-breaking or waived).
* Contract tests against ephemeral service.
* Secret scanning, Dependency Review, **CodeQL**.
* **axe** run on critical routes.

**7.2 Nightly**

* Playwright E2E (auth, RBAC, config/flags/lookups, jobs SSE).
* **k6** perf smoke: tests/perf/k6\_sse\_ttfb.js (TTFB/heartbeat).
* Parity dry-run (in RTM branch).

**7.3 Pre-Deploy (stage job)**

* Re-run contract/E2E quick set.
* Publish Evidence Pack artifacts.

**8. Tooling & Harness**

* **Playwright**: browser E2E + API requests; env selectable.
* **k6**: SSE smoke; thresholds declared (TTFB ≤ 200ms; heartbeat gap ≤ 10s).
* **Prism/Dredd** (or equivalent): OpenAPI contract conformance.
* **Test doubles**: MCP child process stub; Graph stub when write disabled.
* **Data reset**: migrations + SP fixtures; idempotent seeding.

**9. Defect Workflow & Reporting**

* Issues filed with repro, logs (requestId), screenshots, environment, commit SHA.
* Severity ties to SLOs (e.g., SSE heartbeat gap breach = **High**).
* Daily QA report during hardening; dashboard of pass/fail trends, perf, a11y.

**10. Traceability (sample)**

| **UC / FR / NFR** | **Suite** | **Case IDs** |
| --- | --- | --- |
| UC-01 Auth, FR-AUTH-01..03 | E2E/Contract | TS-AUTH-01..04 |
| UC-02 Dashboard, NFR Perf | E2E/Perf | TS-HLT-01, k6 thresholds |
| UC-07 Jobs/SSE | E2E/Perf | TS-JOB-01..05 |
| UC-09 CORS | Security | TS-CORS-01..02 |
| UC-12 Parity | Parity | TS-PRTY-01 |
| NFR A11y | Accessibility | TS-A11Y-01..03 |
| NFR Rate-limit | Security | TS-RL-01..02 |

**11. Acceptance Criteria (Strategy)**

* Suites implemented and runnable via CI; environment-parametrized.
* Evidence Pack contains test outputs and checksums for every release.
* Parity gate enforced before Prod; SSE SLOs met.

**12. Open Issues**

* Decide final rate-limit thresholds (align with NFR policy).
* Confirm Graph write mode for Access page tests.
* Finalize which parity keys are **critical** vs **minor**.

**End of Document — TJ-MCPX-DOC-09 v1.1.0**