**MCPX‑KendoBridge — Config & Feature Flag Reference (DB‑Sourced, Non‑Secret)**

**Document:** docs/config\_reference.docx  
**Project Code:** MCPX‑KendoBridge  
**Version:** 1.0.0 (Draft)  
**Last Updated:** 2025‑09‑26  
**Document Owner:** DoSE (Accountable) — DocFactory (Responsible) — DBA/SecLead (Consulted)

**Purpose.** Provide a **single source of truth** for **non‑secret** configuration and feature flags for MCPX‑KendoBridge, including **types**, **defaults**, **safe ranges**, **validation**, **change procedures**, and **audit hooks**. All dynamic values are stored in SQL Server tables AppConfig and FeatureFlag and surfaced **only** through stored procedures: sp\_Config\_GetValue, sp\_Config\_GetAll, sp\_Feature\_IsEnabled, sp\_Lookup\_Get. **Secrets are never stored in DB**; they live in **GitHub Environments** or vendor portals.

**DB COMPLIANCE:** **Add‑only** schema/migrations; **Stored‑procedure‑only** DAL; **No‑Hard‑Coding** in code/tests/ui. **RTM validates on Prod DB (read‑only)**.

**Table of Contents**

1. Key Principles & Trust Boundaries
2. Configuration Tables & SP Contracts
3. Key Catalog (Type, Default, Range, Impact)
4. Feature Flags (Behavior & Safety)
5. Change Procedures (Ops & Migration Patterns)
6. Validation & Monitoring
7. Environment Matrix (Alpha → Beta → RTM → Prod)
8. Secrets Map (Out‑of‑Scope to DB)
9. Assumptions
10. Next Steps

**1) Key Principles & Trust Boundaries**

* **DB as source of truth** for **non‑secret** runtime config; app reads via **SPs**; caching is short‑TTL.
* **Ingress & SSE** behavior must respect **DB‑driven** timeouts and keep‑alive intervals.
* **Origin allow‑list** is **data‑driven**; requests outside the list are rejected with a **403 envelope**.

**2) Configuration Tables & SP Contracts**

* **Tables:** AppConfig([Key] PK, [Value], [UpdatedAt]), FeatureFlag([Name] PK, [Enabled], [UpdatedAt]).
* **SPs:**
  + sp\_Config\_GetValue(@Key) → NVARCHAR(MAX)
  + sp\_Config\_GetAll() → [Key],[Value]
  + sp\_Feature\_IsEnabled(@Name) → BIT
  + sp\_Lookup\_Get(@Type,@Key) (extensible)
* **Grants:** App principal has **EXECUTE** on SPs only; no table rights. (Include the grant snippet from DB scripts in Evidence.)

**3) Key Catalog (Type, Default, Range, Impact)**

| **Key** | **Type** | **Default (seed)** | **Safe Range / Format** | **Source** | **Reads via** | **Affects** | **Notes** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Mcp:ChildCommand | string | npx | executable name/path | AppConfig | sp\_Config\_GetValue | Child spawn | Non‑secret |
| Mcp:ChildArgs | string | -y @progress/kendo-react-mcp@latest | quoted arg string | AppConfig | sp\_Config\_GetValue | Child spawn | Non‑secret |
| Mcp:ChildCwd | string | `` (empty) | abs/rel path | AppConfig | sp\_Config\_GetValue | Child spawn | Non‑secret |
| Security:AllowedOrigins | csv string | https://chat.openai.com,https://platform.openai.com | Comma‑sep origins (scheme+host[:port]) | AppConfig | sp\_Config\_GetValue | Access control | 403 on mismatch |
| Network:SseKeepAliveSeconds | int | 15 | **5–120** | AppConfig | sp\_Config\_GetValue | Streaming | Heartbeat cadence |
| Network:RequestTimeoutSeconds | int | 120 | **30–600** | AppConfig | sp\_Config\_GetValue | Transport | End‑to‑end timeout |

**Extensibility (add‑only):** New keys MUST be **non‑secret**, documented here (type, purpose, safe range), and added by **add‑only** migration. No removals/renames—use superseded notes.

**4) Feature Flags (Behavior & Safety)**

| **Flag** | **Type** | **Default** | **Source** | **Reads via** | **Behavior** | **Safety Notes** |
| --- | --- | --- | --- | --- | --- | --- |
| EnableLegacyHttpSse | bool | false | FeatureFlag | sp\_Feature\_IsEnabled | Enables legacy /messages + /sse | Off by default; 403 feature\_disabled when off |

* Flags are **non‑secret** and **DB‑driven**; changes are auditable via UpdatedAt and Evidence Pack snapshots.

**5) Change Procedures (Ops & Migration Patterns)**

**Ops (UI or admin script)**

* Update a key/flag via an **approved ops interface** that calls **SPs** (never inline SQL).
* Export /config/effective (non‑secret) before/after; attach to Evidence.

**Add‑only migration (idempotent MERGE)**

-- Example: update allow-list safely

MERGE dbo.AppConfig AS T

USING (VALUES (N'Security:AllowedOrigins', N'https://chat.openai.com,https://platform.openai.com,https://mygpt.example')) AS S([Key],[Value])

ON T.[Key]=S.[Key]

WHEN MATCHED AND ISNULL(T.[Value],N'')<>S.[Value] THEN

UPDATE SET T.[Value]=S.[Value], T.[UpdatedAt]=SYSUTCDATETIME()

WHEN NOT MATCHED THEN

INSERT([Key],[Value],[UpdatedAt]) VALUES(S.[Key],S.[Value],SYSUTCDATETIME());

**Do not** store or reference **secrets** here; see §8.

**6) Validation & Monitoring**

* **Validation on boot:** App fails readiness if required keys are missing or malformed (type/format checks).
* **Monitoring:** Alert on anomalous **keep‑alive** cadence (SSE TTFB/heartbeats), abnormal timeouts, or spikes in origin\_forbidden.
* **Evidence:** Include /config/effective snapshots for each release (≥ 1 year).

**7) Environment Matrix (Alpha → Beta → RTM → Prod)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Env** | **DB** | **Secrets Source** | **Notes** |
| **Alpha** | Alpha DB | GitHub Environment **alpha** | Functional bring‑up |
| **Beta** | Beta DB | GitHub Environment **beta** | Hardening + perf smoke |
| **RTM** | **Prod DB (read‑only)** | GitHub Environment **rtm** (RO conn) | Parity guard; no writes |
| **Prod** | Prod DB | GitHub Environment **prod** | GA + 24‑h checks |
| RTM parity check compares /config/effective with expected prod values. Promotion blocks on drift. |  |  |  |

**8) Secrets Map (Out‑of‑Scope to DB)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Secret** | **Where configured** | **Used by** | **Notes** |
| SQL connection string(s) | GitHub Environments (per env) | API | **Never** in DB or docs |
| TELERIK\_LICENSE / \_PATH | GitHub Environments | UI CI build only | **Never** in DB or images |

**Policy:** Secrets are **never** stored in DB, code, or logs. Rotation is handled via runbook.

**9) Assumptions**

* Ingress supports SSE without buffering; timeouts/keep‑alive are honored.
* App has only **EXECUTE** on SPs; **no** table rights.
* **Add‑only** evolution; RTM is read‑only to Prod DB.

**10) Next Steps**

* Add any newly approved keys here before deployment; ship an **add‑only migration** with seeds.
* Ensure /config/effective always excludes secrets and demonstrates non‑secret parity across envs in Evidence.
* Keep this reference linked from the PR template and Compliance doc.

**Footer (optional):**  
*MCPX‑KendoBridge • Config & Feature Flag Reference • v1.0.0 (Draft) • 2025‑09‑26 • Technijian Internal*