API REST

API REST

> *Dernière mise à jour : 2026-05-10*

34 endpoints, tous prefixés `/api`. Auth par cookie de session (HTTP-only). Validation Zod systématique.

Auth

Méthode	Path	Auth	Description
POST	`/api/auth/register`	Non	Crée user (username, email, password). Hash argon2id. Statut `pending`. Notif admin email
POST	`/api/auth/login`	Non	Login → session 7j. Rate-limit 5 tentatives / 15 min
POST	`/api/auth/logout`	Oui	Invalide la session
GET	`/api/confirm-user/:token`	Non	Email confirmation one-time → role `user`

Games

Méthode	Path	Auth	Description
GET	`/api/games`	Confirmed	Liste tous jeux + metadata BGG
GET	`/api/games/:id`	Confirmed	Détail jeu (rules_language, hasCardDatabase, etc.)

Méthode	Path	Auth	Description
GET	`/api/games/:id/pdf`	Confirmed	Stream PDF (`Content-Type: application/pdf`)
GET	`/api/games/:id/page-image/:page`	Confirmed	PNG 300 DPI page N (rendu via `pdftoppm`)
GET	`/api/games/search?q=`	Confirmed	Recherche fulltext (LIKE)
POST	`/api/games/ingest`	Confirmed + canAddGames	Multipart : PDF + metadata. Si `scheduled_start_at` : queue scheduled, sinon démarrage immédiat
DELETE	`/api/games/:id`	Admin	Supprime jeu, questions, purge collection Qdrant
DELETE	`/api/games/:id/scheduled`	Confirmed + canAddGames	Annule ingestion scheduled. 409 si pas en `scheduled`

Ask (RAG)

Méthode	Path	Auth	Description
POST	`/api/ask/retrieve`	Confirmed	Retrieval seul (chunks sans génération) — pour évaluation
POST	`/api/ask/stream`	Confirmed	RAG streaming SSE (question → retrieval → Claude). Body : `{ game_id, question, extensions, history, cardMentions, stickyCardMentions }`
GET	`/api/ask/:questionId`	Confirmed	Récupère la réponse persistée (fallback SSE après crash connexion)
PUT	`/api/ask/:questionId/feedback`	Confirmed	Vote pouce ↑↓ + comment

Cards

Méthode	Path	Auth	Description
GET	`/api/cards/search?gameId=&q=&limit=`	Confirmed	Autocomplete par collection (BM25 ou full-text)

Méthode	Path	Auth	Description
GET	`/api/cards/image/:pointId?w=&gameId=`	Confirmed	Proxy image cachée (sharp resize, fallback CDN)

Decks

Méthode	Path	Auth	Description
POST	`/api/decks/parse`	Confirmed	Parse decklist texte → pointIds Qdrant. Whitelist `flesh-and-blood-cards`. Rate-limit 10/min

BGG

Méthode	Path	Auth	Description
GET	`/api/bgg/hot`	Confirmed	Top 20 jeux BGG (cache 6h)
GET	`/api/bgg/search?q=`	Confirmed	Recherche BGG XML API
GET	`/api/bgg/game/:bggId`	Confirmed	Détail jeu BGG
GET	`/api/bgg/game/:bggId/expansions`	Confirmed	Extensions d'un jeu BGG

Lorcana

Méthode	Path	Auth	Description
GET	`/api/lorcana-symbols/:symbolId`	Confirmed	SVG symboles spécialisés Lorcana

Admin

Méthode	Path	Auth	Description
GET	`/api/admin/health`	Admin	Health Qdrant, TEI, reranker, Claude SSH, SMTP + stats

Méthode	Path	Auth	Description
GET	`/api/admin/users`	Admin	Liste users (id, username, role, canAddGames)
DELETE	`/api/admin/users/:id`	Admin	Supprime user + questions, réassigne ses jeux à l'admin
POST	`/api/admin/users/:id/set-can-add-games`	Admin	Toggle `canAddGames`
POST	`/api/admin/confirm-user/:userId`	Admin	Force confirmation user pending → role `user`
GET	`/api/admin/feedback?gameId=&vote=&from=&to=&page=`	Admin	Pagine feedbacks filtrés
GET	`/api/admin/feedback/:id`	Admin	Détail feedback + diagnostics complets
POST	`/api/admin/feedback/export`	Admin	Export CSV feedbacks filtrés
POST	`/api/admin/games/:id/sync-cards`	Admin	Force sync collection Qdrant vs source
GET	`/api/admin/cards/list`	Admin	Liste collections + counts
POST	`/api/admin/send-test-email`	Admin	Test SMTP
POST	`/api/admin/send-password-reset/:userId`	Admin	Force reset email

Health

Méthode	Path	Auth	Description
GET	`/api/health`	Non	`{ status: 'ok', timestamp }` (Docker healthcheck)

Patterns globaux

- **UUID v4** partout (`game_id`, `question_id`, `user_id`)
- **Rate-limit ask** : 20 questions/min/user
- **Rate-limit deck parse** : 10/min/user
- **Rate-limit login** : 5 tentatives → 15 min cooldown / IP
- **Limites taille** : question ≤500 chars, comment ≤1000 chars, decklist ≤50 000 chars
- **SSE events** : `meta` (1er, porte questionId), `phase`, `context`, `token`, `done`, `error`, `quota_pause`, `heartbeat` (8s)

Pas d'OpenAPI/Swagger — le tableau ci-dessus est la source de vérité.

Revision #1
Created 2026-05-10 15:19:56 UTC by thymon
Updated 2026-05-10 15:19:56 UTC by thymon