Overview

Provider keys (Provider Vault)

Some tools can only carry an API key (Cursor, Copilot, Gemini CLI, Codex CLI). For these, the Gateway injects **your organization's** provider key server-side — developers never see or hold it.

Supported providers

- **OpenAI** and **Anthropic** — standard API keys.
- **Azure OpenAI** — key + your Azure resource endpoint; the Gateway routes to your own Azure deployment.
- **Google Gemini** — standard API key.

How keys are stored

Keys are encrypted at rest (AES-256-GCM) with strict database-role separation; they are decrypted only in memory, per request, and never logged or returned by any API. The console shows only the last 4 characters.

Model allow-lists

Each key can be restricted to specific models. With multiple keys for one provider, the requested model selects the matching key.

Connection modes

Per tool, you choose: **subscription** (the developer's own account passes through — Claude Code's default) or **managed key** (vault injection). Tools whose mechanism cannot carry a subscription credential are locked to managed mode. The Activity row records which mode actually served each request.

Revision #1
Created 2026-08-01 13:06:27 UTC by Sentilai Docs
Updated 2026-08-01 13:06:27 UTC by Sentilai Docs