Google Ads API Tool Design Document

Basic Access application documentation

APPLICANT	Yang Qiang
ENTITY	Individual developer
TOOL	Google Ads API Manager
USE	Internal performance and affiliate advertising automation
REPOSITORY	github.com/yangqiang-ads/google-ads-api-manager
VERSION	1.0 - 26 August 2026

01 Executive summary

Google Ads API Manager is a planned internal Python application for an individual developer. It will orchestrate authorized Google Ads account creation, campaign generation, advertising submission, performance reporting, AI-assisted analysis, and validated automated optimization. The tool is not a public product and will not be made available to external users or clients.

Application status	Initial design and configuration stage. Development and production rollout will follow test-account validation and Google Ads API access approval.

Applicant and tool profile

Applicant	Yang Qiang
Entity type	Individual developer
Primary business location	China
Repository	https://github.com/yangqiang-ads/google-ads-api-manager
Intended audience	Repository owner only - no public or client access
Business model	Individual performance and affiliate marketing using approved offers and authorized advertising accounts. Revenue may be earned from qualifying conversions. The software itself is not sold, licensed, rented, or offered as a service.

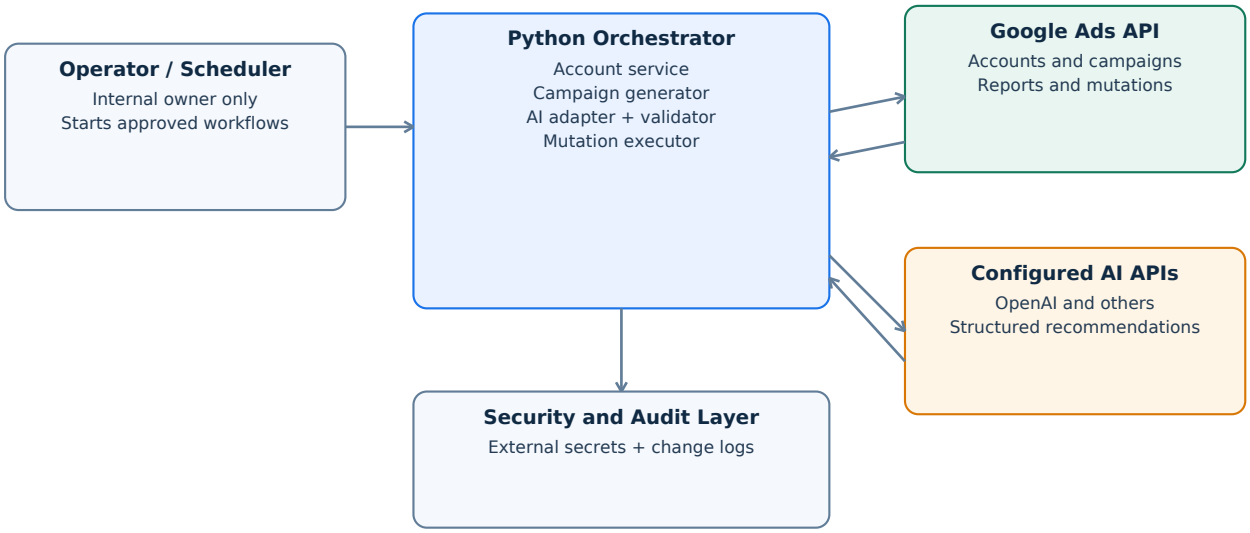
Primary objectives

- Create and configure eligible customer accounts beneath an authorized manager account.
- Generate and submit compliant campaign structures, keywords, headlines, descriptions, bids, and budgets.
- Retrieve aggregated performance data and obtain structured recommendations from configured AI APIs, including OpenAI.
- Apply only validated optimization changes and retain an audit trail of automated actions.

Important boundary	The tool will not bypass Google Ads account limits, ad review, suspensions, enforcement systems, or policy controls. Account and advertisement creation remains subject to Google eligibility and review.

02 System design and architecture

The application uses a Python orchestration layer between the internal operator, Google Ads API, and configured AI APIs. AI providers return structured proposals; they never receive Google credentials and never call Google Ads directly. The Python application remains the sole execution authority.



Component responsibilities

Account service	Creates and configures eligible customer accounts beneath the authorized MCC.	Google eligibility and manager-account permissions are enforced.
Campaign generator	Builds campaign, ad group, ad, keyword, bid, budget, and URL payloads.	Output is schema-checked and policy-checked before submission.
Reporting collector	Retrieves authorized campaign metadata and aggregated performance metrics.	Read scope is restricted to owned or explicitly authorized accounts.
AI adapter	Sends minimized non-sensitive inputs to configured AI APIs and receives structured proposals.	No Google tokens, private keys, payment data, or personal data are sent.
Validation engine	Checks permissions, formatting, policy rules, budgets, bids, thresholds, and account allowlists.	A failed check blocks execution.
Mutation executor	Applies eligible Google Ads changes with idempotency, retries, and rate-limit handling.	Every action is logged; an emergency stop disables further mutations.

03 Functional scope and Google Ads API usage

The following scope is requested for internal account management, advertising creation, reporting, and optimization. Features will be introduced incrementally after test-account validation.

Customer account creation	CustomerService.CreateCustomerClient	Create eligible customer accounts beneath the authorized manager account and record returned customer IDs.
Reporting	GoogleAdsService.Search / SearchStream	Read account, campaign, ad group, ad, keyword, status, and aggregated performance fields.
Campaign management	Campaign, budget, ad group, ad, and criterion mutate services	Create and update campaigns, budgets, ad groups, responsive search ads, keywords, bids, and statuses.
Operational controls	Status updates and read-back verification	Pause, enable, or update resources only after validation; verify the resulting state.
Monitoring	Read-only queries and error responses	Monitor serving status, policy results, operation failures, and quota or rate-limit errors.

Explicitly out of scope

- Providing the developer token, Google Ads API access, or automation service to third parties.
- User access invitation or user administration workflows.
- Billing setup, payment account manipulation, invoice access, or payment data processing.
- Customer Match uploads, personally identifiable information, or remarketing data processing.
- App Conversion Tracking and Remarketing API usage.
- Any workflow intended to evade account limits, policy review, suspension, or enforcement.

Access model All target accounts must be owned by the applicant or explicitly authorized and reachable through the authorized manager-account hierarchy. No external user interface or client login is planned.

04 AI-assisted advertising workflow and data flow

The tool may integrate multiple configured AI API providers, including OpenAI. AI is used for text generation, campaign structuring, pattern analysis, and structured optimization recommendations. The Python application validates and executes permitted actions; AI output is never treated as directly executable.

End-to-end processing sequence

1	Operator or scheduler starts an authorized workflow.	Account allowlist, task type, and limits are loaded.
2	Google Ads API returns authorized metadata and aggregated metrics.	Only fields needed for the requested analysis are retained.
3	Python minimizes and prepares AI input.	Credentials, payment data, and personal data are excluded.
4	Configured AI API returns structured content or recommendations.	Output is parsed into a defined schema; free-form execution is prohibited.
5	Validation engine checks the proposal.	Policy rules, URL allowlists, formatting, permissions, bid and budget limits, and change thresholds must pass.
6	Mutation executor submits eligible changes to Google Ads API.	Google performs its normal validation, review, and enforcement.
7	Application reads back results and writes an audit record.	Request type, resource IDs, outcome, timestamp, and error category are logged.

Data classification

Permitted operational data	Campaign names or labels, ad text, keyword text, targeting configuration, aggregated clicks, impressions, cost, and conversion metrics.	Only when necessary for generation or optimization; minimized before transmission.
Restricted secrets	Developer token, OAuth credentials, service-account private keys, refresh tokens, API keys, passwords.	Never transmitted and never committed to the public repository.
Restricted financial data	Payment methods, invoices, banking details, billing credentials.	Not collected or transmitted.
Restricted personal data	Names, emails, phone numbers, addresses, customer lists, user identifiers.	Not collected for this workflow and not transmitted.

AI provider control

Each configured AI provider is treated as an authorized processor. Provider credentials are stored separately, input fields are minimized, and provider-specific retention and security settings are reviewed before activation.

05

Security, automation safeguards, and auditability

Credential and access controls

- Google and AI credentials are stored outside source code using environment-based or managed secret storage.
- The public GitHub repository contains design documentation only and must not contain tokens, keys, account exports, or private logs.
- The application uses least-privilege Google Ads access and an explicit allowlist of permitted manager and customer accounts.
- All network requests use provider-supported encrypted transport; secrets are excluded from application logs.

Automated advertising safeguards

Schema validation	Require defined fields and valid resource relationships for every generated payload.	Reject malformed or incomplete payloads.
Policy and content rules	Check length, required fields, prohibited patterns, destination URLs, and configured brand rules.	Block submission and log the reason.
Budget and bid limits	Apply configured minimums, maximums, daily caps, and percentage-change limits.	Clamp or reject out-of-range changes.
Account permissions	Require authorized MCC path and approved customer-account allowlist.	Deny access outside the authorized hierarchy.
Idempotency and retries	Use stable operation identifiers and bounded retry with backoff.	Avoid duplicate account or campaign creation.
Rate and volume limits	Throttle jobs and respect Google API quotas and service-specific limits.	Pause the queue on quota or rate-limit errors.
Emergency stop	Provide an internal kill switch that disables all mutations while preserving read-only monitoring.	No new changes are submitted until re-enabled.
Audit logging	Record requested action, resource IDs, validation outcome, API result, timestamp, and error category.	Failed or blocked actions remain traceable.

Ad review

Automated submission does not equal approval. Newly created or modified advertising remains subject to standard Google Ads review, serving eligibility, and policy enforcement.

06 Development, testing, and operational plan

Phased implementation

1. Configuration	Google Cloud project, authentication, test manager account, secret storage, logging foundation.	Successful authenticated read-only call against a test account.
2. Read-only validation	Reporting queries, data minimization, AI analysis in non-executing mode.	Correct metrics, no sensitive data in AI payloads, stable error handling.
3. Test-account mutations	Campaign and ad creation, status updates, validation engine, limits, and audit logs.	Repeatable test results with no duplicate resources or out-of-limit changes.
4. Controlled production rollout	Small allowlisted account set with conservative job and change limits.	Stable operation, policy compliance, monitored costs, and reviewed logs.
5. Expanded internal use	Additional owned or authorized accounts and scheduled optimization.	Ongoing monitoring, incident response, and periodic control review.

Monitoring and incident response

- Monitor authentication failures, permission errors, policy results, quota errors, mutation failures, and unexpected spend changes.
- Suspend mutation jobs on repeated failures, anomalous volume, or safeguard violations.
- Rotate exposed credentials immediately and remove affected credentials from authorized configurations.
- Review automated change logs and restore prior values where supported and appropriate.

Change management

- Material changes to audience, data use, API capabilities, or external availability will be documented before deployment.
- If the Google Ads API use case changes, the applicant will submit the appropriate tool-change or permissible-use request.
- Repository documentation will remain aligned with the production design and current API application statements.

07 Compliance declarations and references

Compliance declarations

- The tool is for internal use by the individual developer and is not accessible to clients or the general public.
- All Google Ads accounts accessed by the tool will be owned by or explicitly authorized to the applicant.
- The developer token will not be shared, sublicensed, exposed through another API, or used with a third-party advertising tool.
- The tool will not process App Conversion Tracking and Remarketing API data, Customer Match data, billing data, or payment information.
- The tool will comply with Google Ads API terms, Google Ads advertising policies, and the applicable policies of configured AI API providers.
- The tool will not circumvent account creation limits, advertiser verification, ad review, suspensions, or enforcement systems.

References

Google Ads API developer token	developers.google.com/google-ads/api/docs/api-policy/developer-token
Google Ads API access levels	developers.google.com/google-ads/api/docs/api-policy/access-levels
Google Ads API policies	support.google.com/adspolicy/answer/6169371
OpenAI API data controls	developers.openai.com/api/docs/guides/your-data
Public design repository	github.com/yangqiang-ads/google-ads-api-manager

Document owner	Yang Qiang - Individual developer. This document contains no developer token, API key, OAuth secret, customer ID export, payment data, or personally identifiable information.