Google to require MCP or CLI access for AI agents on Workspace from February 2027



Google announced agent identities, human approval and prompt injection screening across Workspace and Google Cloud. AI agents must use Workspace MCP servers or the CLI, with enforcement from 1 February 2027.

- Under the Workspace AI Tools Addendum, AI agents must connect via Workspace MCP servers or the CLI; technical enforcement starts 1 February 2027.
- Conventional applications can keep using existing REST APIs.
- External agents need dedicated OAuth client IDs, least-privilege scopes and quotas; quota-related billing begins 1 April 2027.
- Sensitive actions such as sending email or changing Drive sharing require user confirmation.
- The addendum bars permanent storage of raw Workspace data, model training use and API

> scraping, and caps Google Technical Information retention at 30 days.

Google has announced a set of controls for autonomous AI agents that access enterprise data and cloud infrastructure through Google Workspace and Google Cloud. It also made its Workspace Model Context Protocol (MCP) servers and command-line interface (CLI) generally available.

What changes

Under the new Workspace AI Tools Addendum, AI agents must connect through the Workspace MCP servers or the CLI. Technical enforcement begins on 1 February 2027. Conventional applications can continue to use existing REST APIs. The MCP servers cover Gmail, Drive, Docs, Sheets, Slides, Calendar, Chat and Tasks, and requests are checked against organizational permissions, DLP policies and classification labels.

External agents must use dedicated OAuth client IDs so administrators can tell them apart from ordinary applications. Least-privilege scopes and quotas apply, and quota-related billing starts on 1 April 2027. In Google Cloud, agents receive individual identities through Agent Registry, and Agent Gateway screens requests for prompt injection using Model Armor.

Data handling and oversight

The addendum prohibits permanent storage of raw Workspace data, its use for model training, and unauthorized API scraping. Google Technical Information, such as vector embeddings and memory indexes, is limited to 30 days of retention. Providers must delete user data and related technical information when an integration is disconnected or revoked.

Administrators can audit agent activity and revoke access in the admin console. Google advises reviewing connected apps and agents, configuring DLP and monitoring OAuth logs, while developers should migrate integrations and add user confirmation and prompt injection protection before the deadline.

What to do now

1. Inventory AI agents and third-party AI tools connected to Workspace and Google Cloud, and identify owners.
2. Check which integrations still use REST APIs for agent behavior and plan migration to MCP or CLI before 1 February 2027.
3. Review DLP policies and classification labels so agent requests are properly governed.
4. Monitor OAuth activity logs and remove grants that are unused or over-scoped.
5. Assess AI tool providers against the addendum's retention, deletion and no-training terms, including PDPL obligations.
6. Require human confirmation for sensitive agent actions such as external sharing and IAM changes.