Governance Studio
by Adapted Media Pty Ltd

GOOGLE CLOUD AGENT IDENTITY AUTH MANAGER CENTRALISES TOOL CREDENTIALS

OPERATIONAL SIGNAL

DOMAIN: ADMIN — Administration I **CONFIDENCE LEVEL:** HIGH
INSTITUTIONAL DIMENSIONS: Authority I Attribution I Visibility I Escalation I Continuity

Signal ID	Platform	Source	Audience	Signal Date
SIG-ADMIN-018	Google Cloud Agent Identity	Link	Admin I Security I Technology	2026-08-22

CAPABILITY SHIFT

Google Cloud has moved Agent Identity auth manager and the Agent Identity APIs to General Availability. The service provides a centralized credentials vault and authentication broker for outbound tool authentication using 3-legged OAuth, 2-legged OAuth and API keys. Google also states that the Agent Identity APIs replace the legacy IAM Connectors API for managing auth providers and agent identities.

ORGANISATIONAL CONSEQUENCE

For teams building agents on Google Cloud, credential handling can now be consolidated around dedicated Agent Identity services instead of the legacy connector API. The governance question is who may create or change auth providers and agent identities, how credential access is controlled, and whether operational records make those changes visible across projects.

WHAT TO WATCH

- Projects still calling the legacy iamconnectors.googleapis.com API for auth-provider or agent-identity management
- Changes to agentidentity.googleapis.com and agentidentitycredentials.googleapis.com configuration or access patterns
- Credential-broker errors or permission changes as teams adopt the generally available services

WHY THIS MATTERS NOW

General Availability establishes Agent Identity auth manager as a production service and confirms the Agent Identity APIs as the replacement for legacy IAM Connectors management.

WHAT TO REVIEW

- Projects that manage agent identities or auth providers through the legacy IAM Connectors API
- Who can create, change or use OAuth and API-key credentials in Agent Identity auth manager
- Logging for changes to Agent Identity providers, identities and credential access
- Migration sequencing where automation depends on iamconnectors.googleapis.com

GOVERNANCE CONTEXT

Centralising agent credentials can simplify control but concentrates authority in a shared identity layer. Organisations need administrative ownership and visibility over who can configure the broker and which agent identities can obtain credentials.

Scope Boundary: This artefact translates observed platform capability changes into operational considerations. It does not constitute policy, legal advice, or enforcement guidance.