Identity and Access Management (IAM)

Fine-grained access control and visibility for centrally managing cloud resources.

Enterprise-grade access control

Identity and Access Management (IAM) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage Google Cloud resources centrally. For enterprises with complex organizational structures, hundreds of workgroups, and many projects, IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes.

Simplicity first

We recognize that an organization's internal structure and policies can get complex fast. Projects, workgroups, and managing who has authorization to do what all change dynamically. IAM is designed with simplicity in mind: a clean, universal interface lets you manage access control across all Google Cloud resources consistently. So you learn it once, then apply everywhere.

The right roles

IAM provides tools to manage resource permissions with minimum fuss and high automation. Map job functions within your company to groups and roles. Users get access only to what they need to get the job done, and admins can easily grant default permissions to entire groups of users.

Smart access control

Permissions management can be a time-consuming task. Recommender helps admins remove unwanted access to Google Cloud resources by using machine learning to make smart access control recommendations. With Recommender, security teams can automatically detect overly permissive access and rightsize them based on similar users in the organization and their access patterns.

Get granular with context-aware access

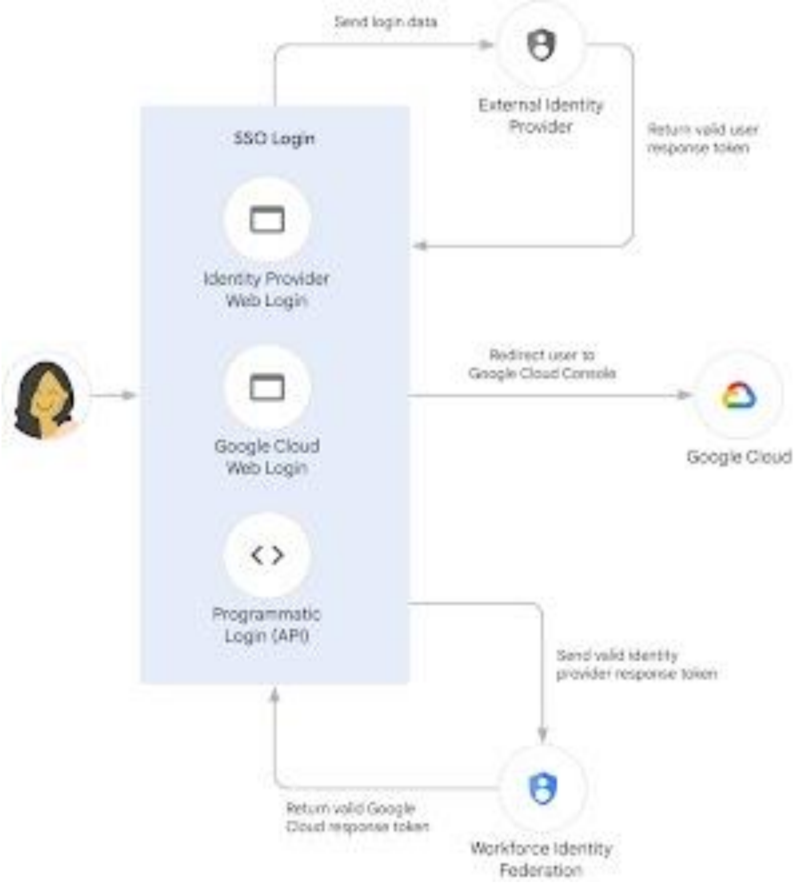
IAM enables you to grant access to cloud resources at fine-grained levels, well beyond project-level access. Create more granular access control policies to resources based on attributes like device security status, IP address, resource type, and date/time. These policies help ensure that the appropriate security controls are in place when granting access to cloud resources.

Streamline compliance with a built-in audit trail

A full audit trail history of permissions authorization, removal, and delegation gets surfaced automatically for your admins. IAM lets you focus on business policies around your resources and makes compliance easy.

Enterprise identity made easy

Leverage Cloud Identity, Google Cloud's built-in managed identity to easily create or sync user accounts across applications and projects. It's easy to provision and manage users and groups, set up single sign-on, and configure two-factor authentication (2FA) directly from the Google Admin Console. You also get access to the Google Cloud Organization, which enables you to centrally manage projects via Resource Manager.


Send login data
External Identity Provider
Return valid user response token
SSO Login
Identity Provider Web Login
Google Cloud Web Login
Programmatic Login (API)
Redirect user to Google Cloud Console
Google Cloud
Send valid identity provider response token
Return valid Google Cloud response token
Workforce Identity Federation

Workforce Identity Federation

Workforce Identity Federation lets you use an external identity provider (IdP) to authenticate and authorize a workforce—a group of users, such as employees, partners, and contractors—using IAM, so that the users can access Google Cloud services. Workforce Identity Federation uses an identity federation approach instead of directory synchronization, eliminating the need to maintain separate identities across multiple platforms.

Features

Single access control interface

IAM provides a simple and consistent access control interface for all Google Cloud services. Learn one access control interface and apply that knowledge to all Google Cloud resources.

Fine-grained control

Grant access to users at a resource level of granularity, rather than just project level. For example, you can create an IAM access control policy that grants the Subscriber role to a user for a particular Pub/Sub topic.

Automated access control recommendations

Remove unwanted access to Google Cloud resources with smart access control recommendations. Using Recommender, you can automatically detect overly permissive access and rightsize them based on similar users in the organization and their access patterns.

Context-aware access

Control access to resources based on contextual attributes like device security status, IP address, resource type, and date/time.

Flexible roles

Prior to IAM, you could only grant Owner, Editor, or Viewer roles to users. A wide range of services and resources now surface additional IAM roles out of the box. For example, the Pub/Sub service exposes Publisher and Subscriber roles in addition to the Owner, Editor, and Viewer roles.

Web, programmatic, and command-line access

Create and manage IAM policies using the Google Cloud Console, the IAM methods, and the gcloud command line tool.

Built-in audit trail

To ease compliance processes for your organization, a full audit trail is made available to admins without any additional effort.

Support for Cloud Identity

IAM supports standard Google Accounts. Create IAM policies granting permission to a Google group, a Google-hosted domain, a service account, or specific Google Account holders using Cloud Identity. Centrally manage users and groups through the Google Admin Console.

Free of charge

IAM is offered at no additional charge for all Google Cloud customers. You will be charged only for use of other Google Cloud services. For information on the pricing of other Google Cloud services, see the Google Cloud Pricing Calculator.