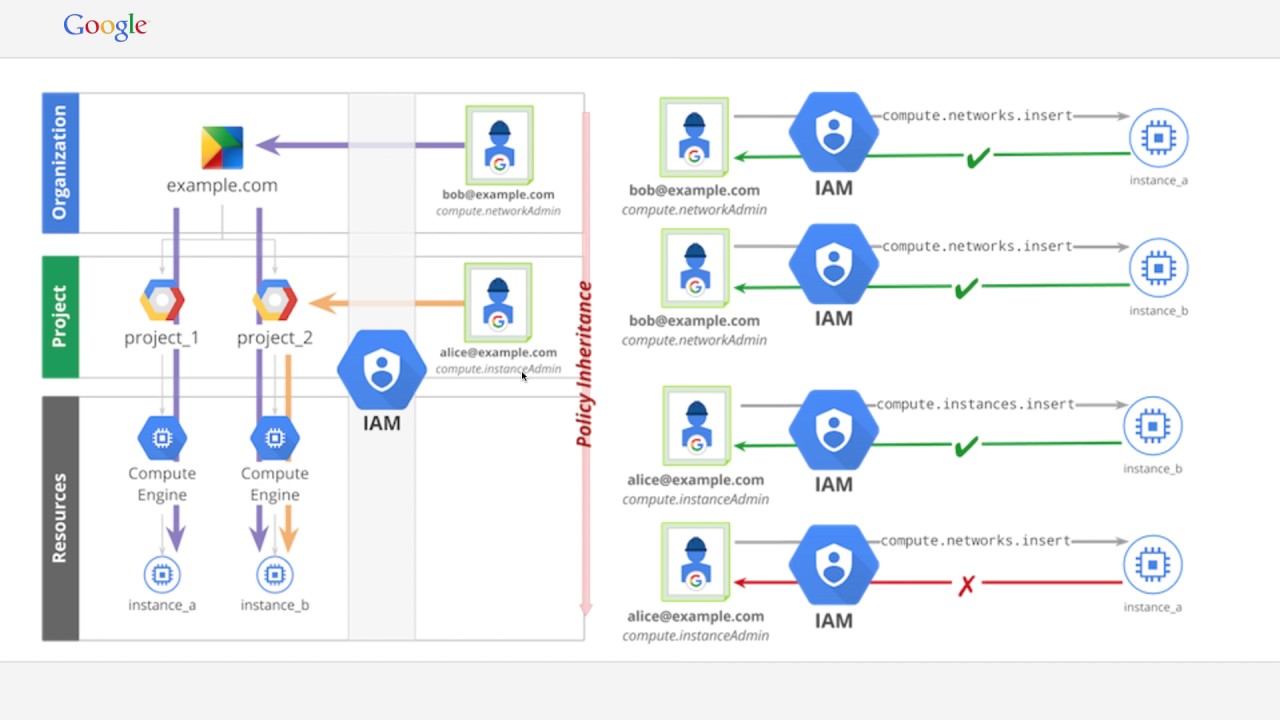
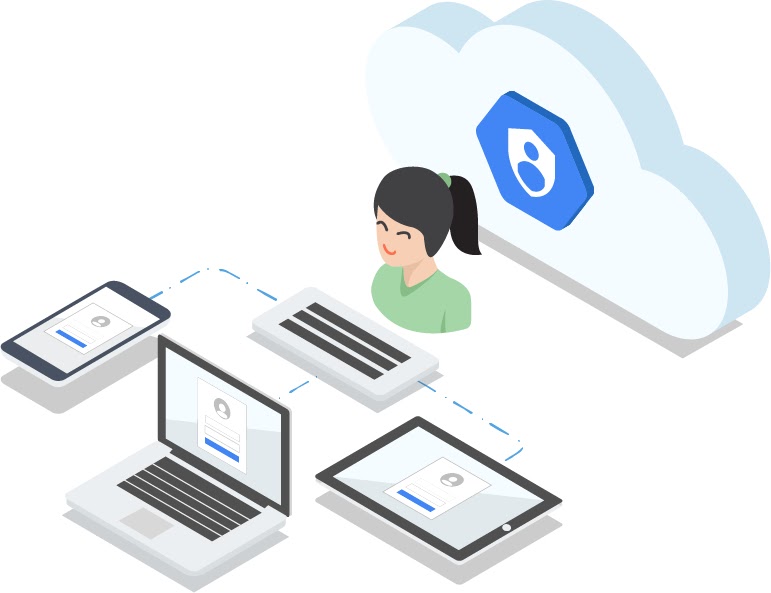
**GOOGLE CLOUD IAM**

IAM Cloud

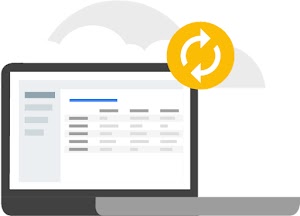
**Cloud Identity and Access Management** (**IAM**) lets administrators authorize who can take action on specific resources, giving you full control and visibility to manage Google **Cloud** resources centrally.





Enterprise-grade access control

Cloud 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, Cloud 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. Cloud 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

Cloud 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](https://cloud.google.com/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

Cloud 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. Cloud IAM lets you focus on business policies around your resources and makes compliance easy.



Enterprise identity made easy

Leverage [Cloud Identity](https://cloud.google.com/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](https://cloud.google.com/resource-manager).