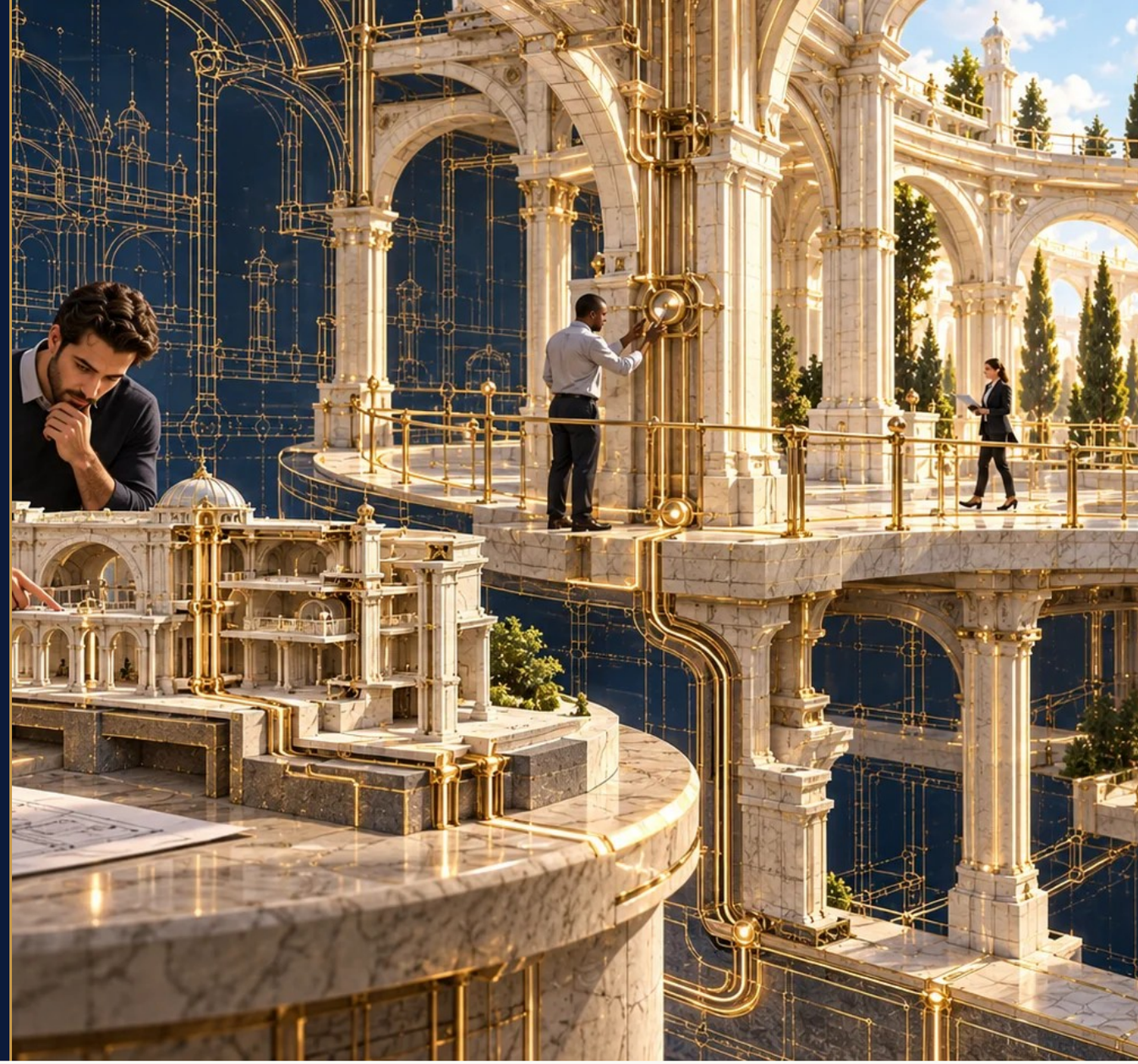
OPENAI ARCHITECTURE PRIMER

Permissions and Access

Roles, project boundaries, and credential permissions

A visual guide to how people and workloads receive only the OpenAI platform access their tasks require.

FIRST-PARTY DOCUMENTATION / INDEPENDENT LUMINITY SYNTHESIS



Access is evaluated in layers

Scope, assigned roles, and credential permissions answer different parts of the authorization question.

FOUR CONTROL IDEAS

01 Two scopes

Organization roles may apply across projects. Project roles stay within one project boundary.

02 Roles combine by union

Direct and group-assigned organization and project roles add together; a narrower role does not subtract a broader grant.

03 Keys add a second check

For a project API key request, the key and the user’s project role must both include the requested permission.

04 Changes take time

Allow up to 30 minutes for role changes and group synchronization to propagate before verifying access.

THE ACCESS QUESTION

Three decisions

01 Where?

Choose organization-wide or one project.

02 Who?

Assign a user or group; use a service account for a workload.

03 What?

Grant the smallest role and credential permission set needed for the task.

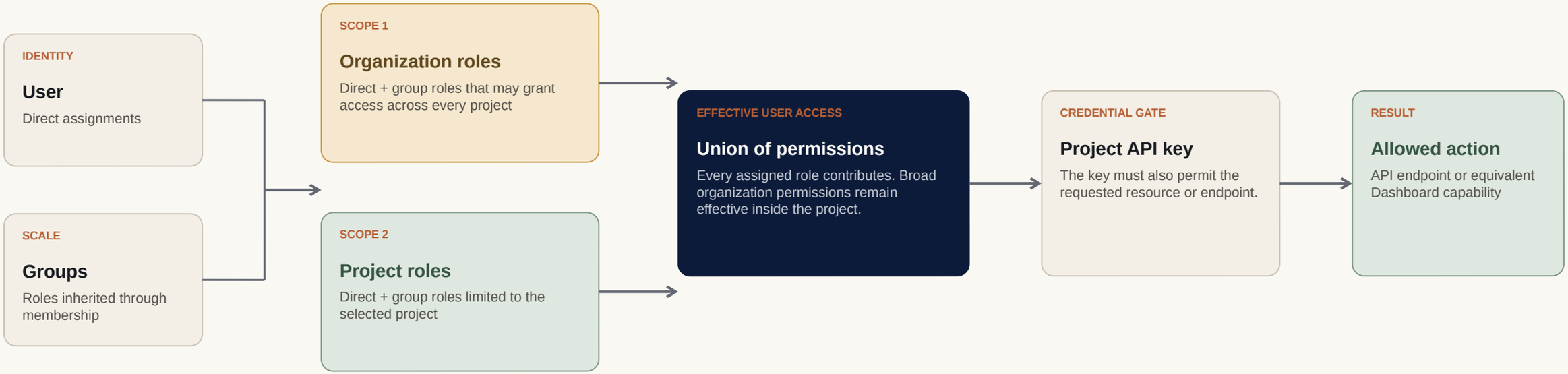
© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/rbac · verified Oct 26, 2026

OpenAI Select Partner

How effective access is calculated

The same permission model governs API calls and corresponding Dashboard actions.



DESIGN IMPLICATION A restricted key cannot grant more than the user's project role. A narrow project role cannot cancel a broad organization-level grant.

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/rbac · verified Oct 26, 2026

OpenAI Select Partner

Projects are the operating boundary

Projects contain resources and settings; people and workloads enter through different access paths.

OPENAI ORGANIZATION

ADMINISTRATIVE SCOPE

Organization owner

Creates projects, sees every project, and manages organization-level administration.

ASSIGNMENT SCALE

Groups

Reusable collections of users; may be synchronized from an identity provider through SCIM.

PROJECT

HUMAN ADMIN

Project owner

Adds members, manages settings, limits, keys, and service accounts.

HUMAN OPERATOR

Project member

Uses project resources and creates project-scoped personal keys within granted permissions.

WORKLOAD IDENTITY

Service account

Project-unique system identity. Its secret is shown once; restrict its key after creation.

RESOURCE BOUNDARY

Scoped resources

Files, assistants, storage, and threads stay inside the project and cannot be moved between projects.

OPERATING CONTROLS

Project controls

Model access, rate limits, spend settings, usage, and API-key permissions.

EXCEPTION The Default project has special membership behavior; fine-tuned models in the Default project are accessible from other projects.

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/rbac · verified Oct 26, 2026

OpenAI Select Partner

A least-privilege operating pattern

Begin with the task, contain it in a project, and verify the resulting access before rollout.

01 Define the task
Name the exact actions and resources required.

02 Choose project
Separate experiments, staging, and production.

03 Assign groups
Map teams to narrowly scoped custom roles.

04 Issue credential
Restrict personal or service-account key permissions.

05 Verify + review
Test as a non-owner; remove unused roles and keys.

FOUR CHECKS BEFORE RELEASE

01 Scope
No organization role grants more than the project design intends.

02 Identity
Human work uses user access; application work uses a project service account.

03 Credential
Keys stay server-side and expose only required endpoint permissions.

04 Evidence
A non-owner test confirms both API and Dashboard behavior after propagation.

LUMINITY SYNTHESIS

Least privilege is a lifecycle: design the boundary, grant the minimum, verify effective access, then review and remove stale access.

© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/rbac · verified Oct 26, 2026

OpenAI Select Partner