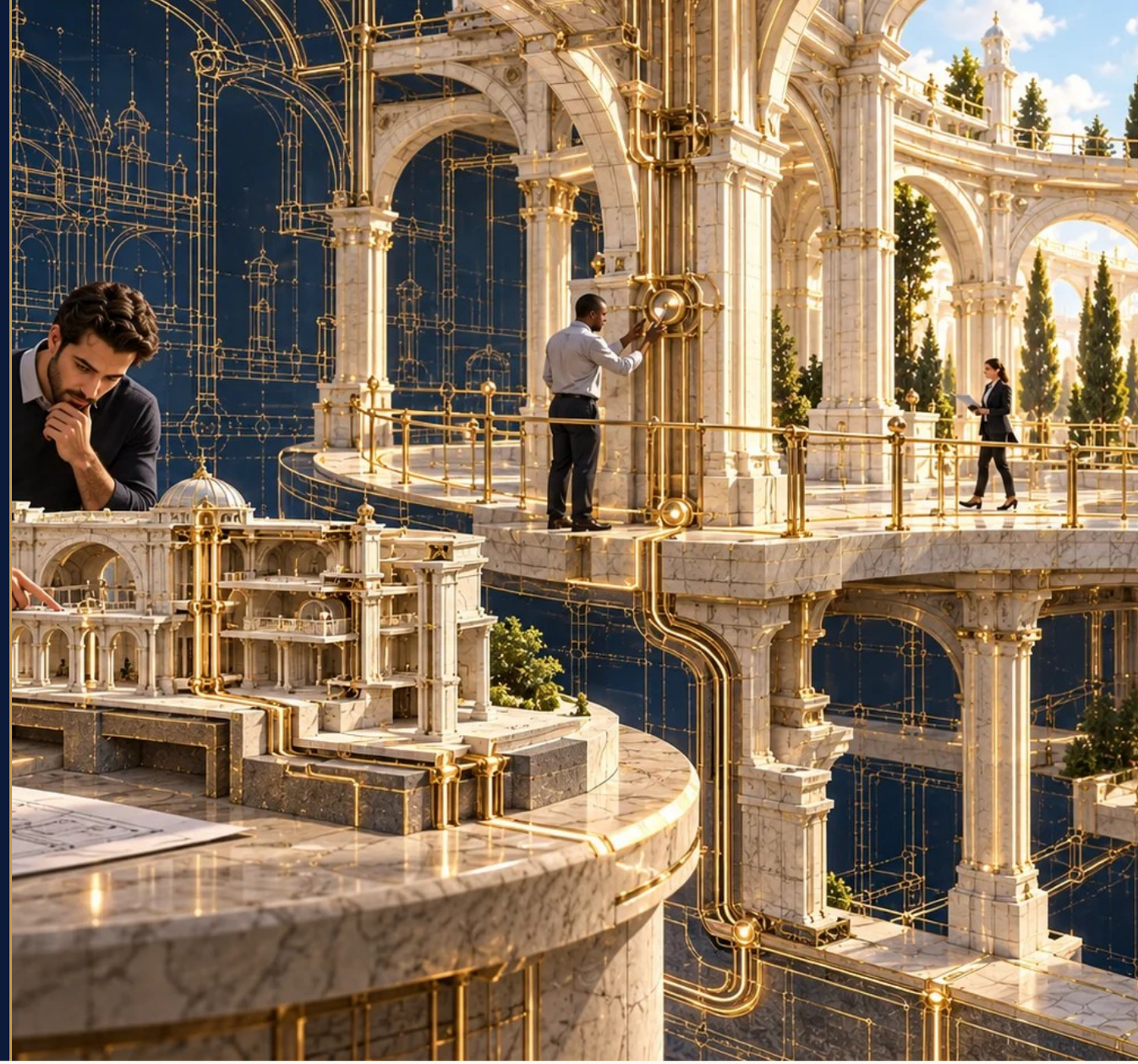
OPENAI ARCHITECTURE PRIMER

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



Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

OpenAI Permissions and Access

Source verified Nov 5, 2026

OpenAI Select Partner

Access Is Evaluated in Layers

Scope, assigned roles, and bearer credentials answer different parts of the authorization question.

AT A GLANCE

2
role scopes:
organization + project

4
assignment sources:
direct/group × org/project

2
bearer credential paths:
API key + short-lived token

30
minutes: role and group
propagation, allow up to

Effective Access
01

Organization and project roles assigned directly or through groups combine into one permission union.

Project Boundary
02

Resources, people, workload identities, credentials, and operating controls remain scoped to a project.

IN THIS SET

Three chapters

01 Effective access

How direct and group roles combine across organization and project scopes, then meet the credential gate.

02 Project boundary

How human and workload identities enter a project and which resources and controls stay inside it.

03 Least-privilege decision

How scope, actor, credential, verification, and review become one operating pattern.

Roles, permission categories, authentication paths, and project behavior can change. Recheck the live OpenAI documentation before deployment.

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

Source: https://developers.openai.com/api/docs/guides/rbac · verified Nov 5, 2026

OpenAI Select Partner

Effective Access

Assigned roles combine by union; project API key requests must also pass key and project-role checks.

01

What contributes to access?

✓ Organization roles	ALL PROJECTS
✓ Project roles	ONE PROJECT
✓ Direct and group assignments	COMBINED
! Narrow role subtracts broad grant	NO
! Role changes verify immediately	ALLOW 30 MIN

Assigned roles → **Union of permissions**

02

How an action is authorized

Scope · organization + project | **Source · direct + group** | **Gate · role + credential**

1. **Identify** — Resolve the user and group memberships
2. **Collect** — Read organization and project roles
3. **Combine** — Build the union of role permissions
4. **Authorize** — Check the requested action and credential

SCOPE
Organization roles remain effective inside projects

UNION
Every direct and group role contributes permissions

GATE
A project key and project role must both permit the API action

03

Four authorization surfaces

Organization Role — SCOPE

Applies across all projects and can widen access inside every project.

Project Role — BOUNDARY

Applies only in the selected project and joins any organization role.

API Key — CREDENTIAL

The key must permit the requested resource or endpoint; it cannot widen the role.

Allowed Action — RESULT

The same role design should produce the expected API and Dashboard access.

ACCESS RULE

- Union only adds permissions
- Key cannot widen the role
- Allow propagation before testing
- Verify as a non-owner

Luminity Digital
INTELLIGENCE, ENGINEERED. DELIVERED.

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

Source: https://developers.openai.com/api/docs/guides/rbac · verified Nov 5, 2026

OpenAI Select Partner

Projects Bound Access and Resources

People, workload identities, credentials, resources, and operating controls meet inside one project.

01

What stays within a project?

✓ Project members and roles	SCOPED
✓ Service accounts	PROJECT UNIQUE
✓ Files, assistants, storage, threads	SCOPED
! Resources move between projects	NO
! Direct Default-project service accounts	NO

Organization member → Project access path

02

How identities enter the boundary

Boundary · selected project | Actor · human or workload | Control · role + credential

1 **Create** — An organization owner creates the project

2 **Assign** — Add users or groups with project roles

3 **Issue** — Create a key, service account, or token

4 **Operate** — Use resources under project controls

HUMAN
A user joins the organization before receiving project access

WORKLOAD
A service account is unique to its project

CREDENTIAL
API keys or workload identity tokens authenticate requests

03

Four project control surfaces

Human Access — USER
Owners and members receive project roles directly or through groups.

Workload Access — SYSTEM
Use a project service account or short-lived workload identity token for system access.

Scoped Resources — RESOURCE
Files, assistants, storage, and threads remain inside the project boundary.

Operating Controls — CONTROL
Model access, rate limits, spend settings, usage, and key permissions apply at project scope.

BOUNDARY

- No cross-project resource moves
- Service accounts stay project scoped
- Default membership differs
- Fine-tuned model exception

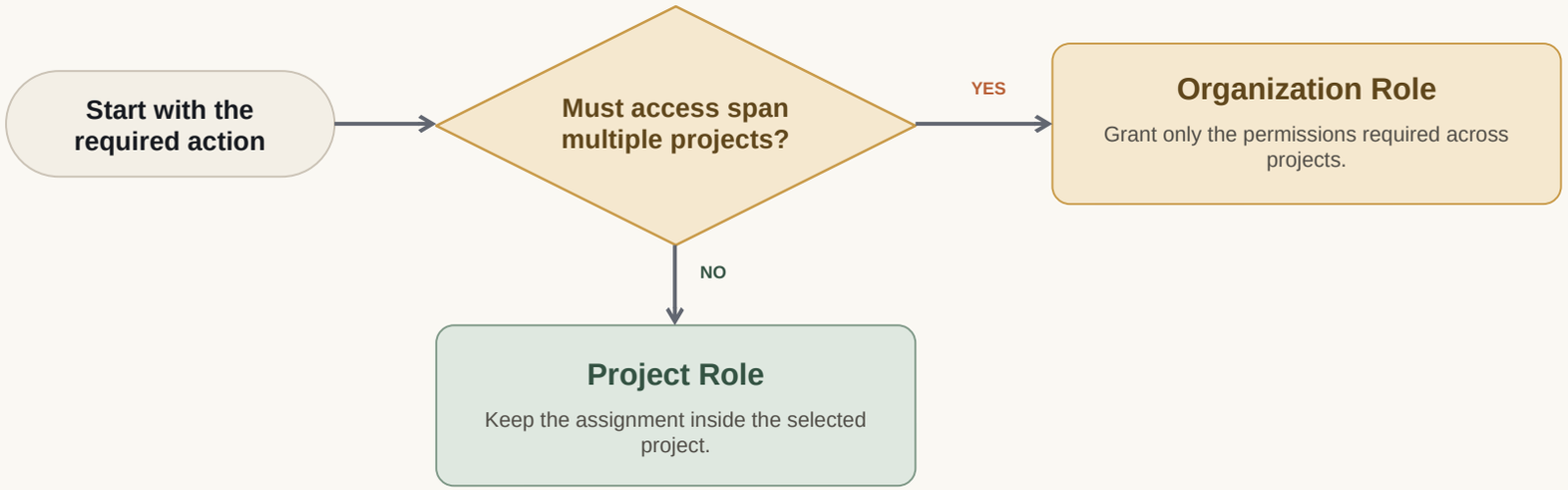
© 2026 Luminity Digital, Inc. | Independent synthesis of official OpenAI documentation.

Source: https://developers.openai.com/api/docs/guides/rbac · verified Nov 5, 2026

OpenAI Select Partner

A Least-Privilege Access Decision

Choose the narrowest role scope first, then apply identity, credential, verification, and review controls.



OVERLAYS APPLY AFTER THE ROLE SCOPE

Human Identity — ACTOR

Assign a user or group. Use a personal project key only when the user calls the API.

Workload Identity — SYSTEM

Prefer a short-lived federated token when appropriate; otherwise use a project service account.

Credential — GATE

Keep secrets server-side and restrict keys to the required resources or endpoints.

Verification and Review — EVIDENCE

Wait for propagation, test as a non-owner, then remove unused roles and keys.

ARCHITECTURE RULE

- Scope does not replace credential limits
- Broad grants remain effective
- Verify after propagation
- 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 Nov 5, 2026

OpenAI Select Partner