

Kenta / Administration

Manage membership, roles and controlled access withdrawal

Keep organization membership, project access, technical review, billing and support authority separately governed.

Current · Revision 6 · Reviewed Oct 26, 2026

► Applicability

Before you begin

- The specific native organization-administration, project-management or delegated capability required for the operation.
-

Keep shared membership and product authority separate

On a configured shared deployment, Account → Organizations and access lists the canonical person's authorized AURONA memberships. The current organization is a working context, not another identity. A long list can be searched locally without exposing organizations outside that authorized list.

Switch organization uses an existing active membership. Managed Kenta and Materials also require the product entitlement, reviewed source mapping and current native authority before changing product context. A rejected switch retains the selected organization and work context.

The shared Organization administration link appears only with central administration authority. Kenta source-specific identity controls, project grants and billing remain independently authorized in their existing workspaces. The native member and withdrawal tasks below apply only where those Kenta controls are available; central membership does not grant them automatically.

Inputs and terminology

Inputs and terminology

Term	Meaning
Organization membership	Belonging to an organization; it does not automatically create a new project, technical-review or financial grant.
Shared-record access	An explicit, bounded grant to named records and chosen source versions rather than the whole project.

Procedure

1. Inspect the member's actual scope

Open Organization settings → Members & invitations. Inspect the member record, active access, project memberships and retained grants.

Review explicit project, reviewer and financial authority independently; do not infer identity from an email match alone.

2. Prepare a controlled invitation or grant

Use the permitted invitation or project-access action. Choose the intended member, role, scope and expiry, then review the exact records and source versions.

A prepared native invitation does not send email automatically. Share its one-time private link only through an authorized channel.

3. Review lifecycle impact before withdrawal

Inspect the impact of revocation, member removal or session withdrawal. Record the required reason and any independent approval.

Refresh the resulting member state. Existing history remains attributable; re-invitation does not silently restore previous financial or project grants.

Verify the result

The intended authority is explicitly granted, expired or withdrawn with retained audit history and current session checks.

What happens next

Identity administration, organization retention/deletion and temporary project support remain separate capabilities. A deletion-request approval is not execution or physical byte erasure.

Troubleshooting

An administration control is denied

Inspect whether your role is native organization administrator, delegated identity administrator, project manager or billing-only. Request the specific required authority; do not broaden a project grant to bypass an organization control.