

Kenta / Administration

Manage your profile, security and signed-in sessions

Review your canonical shared account or existing native account, manage sessions and choose presentation preferences without changing organization authority.

Current · Revision 10 · Reviewed Oct 26, 2026

► Applicability

Before you begin

- Use your own authorized account and complete the authentication required for the current Kenta session.
 - Save unsaved project, billing or support work before signing out, switching accounts or ending the session you are currently using.
 - Use the account's native authentication controls only when they are available; managed-provider accounts must follow their configured provider's supported path.
-

Your account and your working organization are separate

On a configured shared Aurona deployment, the account menu uses your canonical Aurona identity. My account, Preferences, Security, Sessions and Organizations and access open the configured Aurona Account workspace. Names, email and verification status come from the shared identity service; a similar email in another system does not link identities or grant access.

On an existing native deployment, account settings remain in Kenta. A permitted display-name change affects only your own native identity's presentation. Neither mode grants organization, project, review, billing or support-staff authority.

Switch organization selects an existing authorized membership. It does not switch the signed-in person. In a managed product, Use another account first ends this application session and opens a fresh sign-in. Other application sessions are retained. Save work before ending a session.

Shared preferences and product display settings have different scopes

In Aurona Account, Preferences saves interface language, an IANA time zone, date format and number format to your canonical person. A saved version applies on subsequent shared-account, managed Kenta and managed Materials page loads, including another host with an older language cookie. Before the first save, the effective interface language can follow the host language selection.

Shared formatting changes presentation, not original dates, engineering units, exports, currency precision or contractual values. Calendar-only dates keep their calendar day. Kenta display preferences separately control density, reduced motion and contrast; native Kenta preferences are not automatically copied into the shared person.

A save uses a version check and a retry-safe operation. If another update wins first, keep your draft, reload the current preferences and review before saving again. A failed response is not proof that a change was never committed.

Follow the account’s actual authentication mode

Shared-account Security describes the actual sign-in provider and this session's verification state. Name, email, password and multi-factor changes remain with that provider. Use a verified management link when configured; otherwise contact your organization's identity administrator. Opening this workspace does not configure or contact an unconfigured provider.

Shared Sessions lists this person's recorded Aurona application sessions. End session affects the selected session; Sign out of all Aurona sessions is a separate confirmed action that follows the configured provider sign-out path when available. Product-only sign-out does not request identity-provider logout.

Existing native account controls continue to use Kenta's password, authenticator, recovery and session services. Their recorded timestamps do not identify physical devices, browser locations or all external-provider sessions. Recovery codes are credentials and must stay out of cases and diagnostics.

Inputs and terminology

Inputs and terminology

Term	Meaning
Display name	The provider-managed canonical name on shared deployments, or an editable native profile name where permitted. It is separate from email and access grants.

Term	Meaning
Current session	The authenticated application session used by the account request. Ending it requires a new sign-in for that application.
Organization selection	The current working context among organizations your account can already access; selection does not create membership.
Personal preferences	Shared Aurna settings cover language, an IANA time zone, date and number presentation. Kenta display settings cover density, motion and contrast. Existing native account preferences retain their original scope.

Procedure

1. Review a configured shared Aurna account

From managed Kenta or Materials, open the Account menu and choose My account. Confirm the canonical name, email and actual Email verification status. Provider-managed profile fields are read-only here.

Open Preferences, choose the intended interface language, Time zone, Date format and Number format, then Save preferences. Wait for the saved confirmation and reload to apply a changed interface language. Kenta display preferences remain a separate product setting.

Open Security for provider management guidance and Sessions to inspect your own Aurna application sessions. Review the target and confirmation before ending a session or all Aurna sessions.

Open Organizations and access to inspect authorized memberships, search a long list and select Switch organization where available. Product, project, billing and review permissions remain separate. Organization administration is shown only for authorized administrators.

2. Open an existing native Kenta profile

On an existing native deployment, open the Account menu and choose My account. The Profile section shows your own native personal information.

Confirm the displayed name and email before making a change. Review the current organization separately; its membership and permissions are not profile fields. A requested organization that is unavailable does not become an access grant; your own personal account may still be accessible.

3. Change an editable native display name

If the profile allows editing, enter the intended Display name and select Save profile. The server checks your current session and the expected previously saved name.

Wait for the saved confirmation and verify the returned profile. A conflicting change requires reloading and reviewing the current value before saving again. If editing is managed by an external provider, use the displayed provider guidance.

4. **Review native Kenta security and sessions**

Open Security and sessions and inspect the actual authenticator state. Use Review and end your sessions or the Sessions section to inspect your own listed native sessions.

Use the supported authenticator setup or replacement flow only when required. Replacement requires your current password and an unused recovery code and revokes existing sessions and prior recovery codes. Complete verification with a current six-digit code, then store newly issued recovery codes privately; select I have saved these codes only after you have retained them.

In Sessions, select End session or End current session for the intended record and review its confirmation. Ending the current session signs you out. Sign out all sessions is a separate action and requires confirmation; save unsaved work first.

5. **Choose native presentation and working context**

On an existing native deployment, open Preferences and review Application language, Time zone, Date format, Number format, Display density, Motion preference and Contrast preference. Use a valid IANA time zone and inspect the example before Save preferences.

These are versioned personal account preferences. They do not alter original source data, engineering units, permissions or exact contractual values. A change made elsewhere requires reloading the current preferences before saving again.

Review Organization notification preferences separately: they apply only to your current organization. Email delivery is disabled; recording a requested email frequency does not send or enable email.

Use Organizations and access or Switch organization to choose an existing authorized membership. Review the switch confirmation; a pending invitation is not active membership.

Verify the result

The correct shared or native workspace shows your own identity and authorized organization context. Saved preferences survive reload. A confirmed session change affects its stated session scope; an unavailable provider or preference store remains explicitly unavailable.

What happens next

Profile editing does not change email verification, passwords, project roles, finance grants, support enrollment or another person's sessions.

Signing out or switching accounts can discard unsaved browser work after confirmation. Keep recovery codes and authenticator setup material out of support cases, screenshots and clipboard diagnostics.

Session listings are bounded to the available current native records and recent security activity is a limited metadata history. They are not a complete device inventory or an external-provider audit.

Replacing a native authenticator revokes existing sessions and recovery codes. Complete the new verification before leaving setup, and retain the new recovery codes securely. This is distinct from changing a display name or presentation preference.

Shared-account organization membership, product entitlement and mapped source membership are independently checked. A pending invitation or matching email never substitutes for active access. Switching an organization does not migrate identities or rewrite other product sessions.

Troubleshooting

The profile changed before my save completed

Review the conflict message and the current saved profile. Another permitted update may have changed the expected name. Reload the profile, review the returned value and re-enter the intended change if it is still needed. Do not repeatedly submit an outdated expected value.

Name or session editing is unavailable

Check whether this account uses a managed sign-in provider and whether the native session still satisfies required authentication. Follow the configured provider's account controls or sign in again through the existing supported flow. Contact the configured administrator for access problems; do not create another identity to bypass the restriction.

A session is no longer available

The session may already have expired or been revoked. The workspace does not establish device identity or location. Refresh your own session list. If you ended the current session, authenticate again normally. Report an unexplained authentication problem through a case without sharing credentials or recovery codes.

