

Use the shared Aurona sign-in and understand identity readiness

Complete existing password/MFA or configured provider authentication without treating sign-in as a product-access grant.

Current · Revision 6 · Reviewed Oct 26, 2026

► Applicability

Recognize shared and existing native sign-in

Configured shared deployments use the canonical Aurona identity and a separately scoped session for each application. Existing native Kenta sign-in continues without automatic identity migration. A configured central account link does not itself establish a production identity-provider connection.

In a managed product, Use another account ends the current application session and requests fresh authentication. Sign out of this application preserves other application sessions and does not request provider logout. Sign out of all Aurona sessions is separately confirmed in the shared Sessions workspace.

Shared account profile and preferences do not replace product, project, billing or review authorization. An organization switch is validated before changing the application context; a denied target leaves the previous context selected.

Procedure

1. Open the shared account entry

Use Aurona sign-in. Kenta's compatible legacy sign-in links lead to the same account entry and preserve permitted local return destinations.

Complete the existing password and enrolled MFA flow, or the managed provider flow when that product is actually configured to require it.

2. Confirm product and organization access

After authentication, select an assigned application and the authorized organization. A valid session alone does not create a Kenta entitlement or project grant.

Use normal account sign-out controls for your own sessions; do not use administrative revocation merely to close a browser session.

3. Inspect SSO setup accurately

Administrators can inspect Identity & security for issuer/client configuration, domain checks, recovery review and actual provider sign-in evidence.

A saved draft or simulated check does not enable enforcement. Credentials belong in protected deployment configuration; the customer tenant and real provider setup must exist first.

Verify the result

An authenticated identity reaches only assigned applications and permitted records; unconfigured identity integration remains pending.

What happens next

No automatic identity linking or shared parent-domain cookie is implied. The current integration boundary uses OIDC; SAML support is not claimed.

Troubleshooting

MFA or a return link fails

Check the correct account, enrolled authenticator and exact permitted local destination. A used code cannot be replayed. Use the account's supported recovery path or contact your configured administrator; never paste passwords, codes or bearer links into a case.

SSO remains unverified

Check real issuer/client, redirect and domain setup and the recorded live verification evidence. Complete the external provider setup and authorized verification. Do not relabel a simulated result as live.

