

Account & access / Account and access guidance

Manage security and sessions

Use the account service's actual authenticator, recovery and sign-out controls.

Current · Revision 3 · Reviewed Oct 29, 2026

► Applicability

Before you begin

Complete required authentication and open the account/security area available to your application. Controls depend on your actual session and permissions. This guide does not assert that a customer OIDC/SSO provider is configured.

Protect authentication material

Use the authenticator setup flow only when it is required or explicitly initiated through the account service. Save recovery codes securely when first shown. A recovery code is single-use and does not replace knowledge of the password. Never place codes, secrets or reset links in public documentation or feedback.

End sessions deliberately

Use Sign out to end the current supported session. Sign out of all sessions is the distinct account action for broader revocation. Replacing an authenticator is also a security-sensitive flow: the native account interface requires the current password and an unused recovery code and states that all sessions are signed out before setup is required again. Read the displayed consequence before submitting.

When a control is unavailable

Use only controls actually shown for the current identity system and role. Contact the existing support/access process if credentials or codes are unavailable; do not assume a documentation link resets security or enables an external provider.

Open Aurona account (<https://auronainc.com/account>)