

DOCUMENTATION

HEAL UI Security

HEAL Software Inc.

HEAL uses two Keycloak-managed controls to protect the UI from unauthorized access. Session timeout, and login session validation.

Session timeout

If the browser stays idle for the set time, the HEAL session ends on its own. The user has to log in again to continue. This protects unattended workstations on shared desks.

Login session validation

If a user logs in from more than one browser or device, HEAL keeps one session valid and ends the others. Any actions from the ended sessions are logged out. This blocks a stolen session token from being reused on another machine.

> **Heads up.** By default, Keycloak does not limit concurrent user sessions. To turn on single-session enforcement, deploy an `EventListenerProvider` in Keycloak.

How the controls work

1. **User logs in.** Keycloak issues a session token.
2. **HEAL UI checks the token** on every request.
3. **Idle timer runs.** If it goes past the SSO Session Idle limit, the token is invalidated.
4. **A new login from a second device** ends the older session.
5. **The old session is rejected** on its next request, forcing a new login.

Configure (admin)

1. Open the Keycloak Administration Console.

2. Go to Realm Settings > Tokens.

3. Set SSO Session Idle to your preferred idle timeout. For example, 30 minutes.

4. Deploy the EventListenerProvider to enforce one active session per user.

5. Save and test by logging in from two browsers.

Next

HEAL Confidential. All Rights Reserved 2026

- Forgot Password . self-service password reset.
- Accessing HEAL UI . first login walkthrough.

HEAL Confidential. All Rights Reserved 2026