Disable Keycloak account management for users

Theresa Henze - 2026-10-27 - How To ...

To disable Keycloak account management for users, the “account” and “account-console” system applications must be disabled.

> **Warning**: The Bare.ID profile requires the “account” system application. If the Bare.ID profile is used, only disable the “account-console” system application. The steps are described in the article Bare.ID User Profile.

- To do this, sign in to Bare.ID with an administrator account and select the instance for which you want to disable Keycloak account management for users on the welcome page.
- Click on “Applications” in the left-hand navigation bar.
- Activate the “Show system applications” checkbox above the list of connected applications to display the system applications in the list of connected applications.



- Click on the “account” entry to open it.
- Deactivate the “Connection activated” option to deactivate the connection.



- Confirm the change by clicking on the “Save” button.
- Navigate back to the list of connected applications.
- Check the “Show system applications” checkbox to the right above the checkbox to display the system applications in the list of connected applications.
- Open the “account-console” connection by clicking on the corresponding entry in the list.
- Deactivate the “Connection activated” option to deactivate the connection.
- Confirm the change by clicking the “Save” button.

The Keycloak account management for users is no longer accessible.

Application visibility in account management

If account management remains enabled, each application can still be controlled individually in the application configuration.

- Use **Always enable in account application** when an application should always be shown in the user’s account management view after the user has access to it. If this option is disabled, the user can have access in the backend while the application is not displayed in the account management interface.

- Use the application visibility option to hide applications that should not appear in the user-facing application overview. This is useful for technical applications such as SCIM clients that do not provide a direct user action.

  Note: These visibility settings affect the account management display only. They do not replace the application’s access or role configuration.