How accounts work

Lix has one source of truth for authentication: Keycloak (identity.lix.systems). Most services are bound to Keycloak for authentication via OAuth2, although it supports SAML as well.

GitHub vs Local accounts

GitHub accounts are used at Lix for two reasons:

- Ease of login and onboarding
- Ban/allow list management

We don't really care if people have the same username or other information on Lix as they have on GitHub. We don't care about whether people have first/last names on our Keycloak or if they are using pseudonyms.

Allow/ban listing

There is an allow-list and a ban list maintained at: https://git.lix.systems/lix-project/access-control (private repo, available only to Lix core team). To add people to a list, use `./add.sh list.txt gh-username`. Once a list change is pushed, it can take up to five minutes for the change to take effect, as this is currently running on a 5m cron job.

In short, the process for adding a user to the ban or allow list is:

1. Make sure you have the latest version of the repo (i.e. `git pull`) and the github `gh` command is installed.
2. Run `./add.sh <relevant-list-file> <github username>`.
3. Commit and push the change.
4. The ACL change will apply automatically within five minutes.

Be warned -- the allow-list method of access control is temporary / established for the beta period.

Our allow/ban listing is done by GitHub ID, using keycloak-allowban-plugin, a custom Keycloak plugin that reads text files with allow/ban lists. The GitHub ID is put into a user profile attribute, which prevents ban-evasion via account unlinking since it will stick across unlinking.

Known weirdness with the allow/ban list plugin

If a user tries to log in via GitHub and they are not allowed by the plugin, the account is created anyway, it is simply not usable. This is a known issue; putting the plugin in the registration flow caused half-registered users, so it is only in the post-gh-login flow and the normal login flow (to catch unlinked banned accounts).

Local accounts

The Lix core team should have local accounts (linking to GitHub is OK), strongly preferably with 2FA. Other people can be given local accounts if they are trustworthy and prefer to have local accounts (since the usual ban process doesn't work on them; though it is not hard to ban them, just disable the account).

Note that GitHub backed accounts can be turned *mostly* into local accounts by the user simply setting up local auth and unlinking the GitHub account (though the GitHub ID will intentionally persist in properties so this doesn't degrade our bans story).

We would *prefer* for everyone to use WebAuthn for local accounts, but this is often not possible and passwords are OK as long as they're just put in a password manager.

To create a local account, get the following info:

- Username
- Email (which will appear publicly on Gerrit and must be deliverable)
- WebAuthn ok?

Then create an account on https://identity.lix.systems/admin with the provided details. On the account's page, go to Credentials, select Credential Reset, then if WebAuthn is ok for the person, set "WebAuthn Register Passwordless" in the actions (otherwise just password reset) and send it.

Removing last names for people

Due to Keycloak being a silly little thing, we need to use "declarative user profiles" to allow not setting last names. For now, Lix core team members with necessary access will have to remove them manually on request.

This would be fixed by updating Keycloak to 24 on lix.systems and setting up declarative user profiles: https://git.lix.systems/lix-project/web-services/issues/64

How to ban someone

If a user has violated our community norms and needs to have their access to our infrastructure removed, follow the following steps:

1. Add them to the banned users list on https://git.lix.systems/lix-project/access-control and push the changes.
2. Go to https://identity.lix.systems/admin and disable their account for good measure.
3. Ban them from Matrix: FIXME
4. (if you really don't like what's going on) invalidate all sessions:
    1. `ssh root@git.lix.systems -- mysql -D forgejo -e 'delete from session;'`
    2. `ssh -p 2022 youruser@gerrit.lix.systems gerrit flush-caches --cache web_sessions`

3. FIXME: bookstack

Revision #5
Created 2024-04-02 06:32:35 UTC by jade
Updated 2024-04-02 22:45:27 UTC by ktemkin