Brown and GitHub's SAML Auth

Tom DuVally - 2020-10-14 - Comments (0) - Technical Systems

When your GitHub Organization was created, we recommended and implemented Shibboleth (SAML) as the authentication. We are now recommending to **not** use SAML. This document explains some of the reasons why.

SAML Auth and Orgs

When SAML auth is enabled for an Organization, GitHub assumes that all the auth'd users have the same rights, and will allow any of those users to join the Org. Repository access and rights are still controlled by their owners, but the Org membership can not be. Members automatically also have repo creation access inside an Org, which may be problematic.

The reason is that GitHub does not examine account information coming from Shibboleth. Shibboleth provides the info, but GitHub only relies on it's own user authorization system. The advantage of Shibboleth is that we can link a Brown user to their GitHub account, and it can provide some level of trust for the account (authentication), but the downside of not having control over Org Membership may outweigh that advantage.

Using GitHub Auth

Relying on GitHub's user auth will require Org Owners validate each GitHub user for membership, rather than relying on Shib. GitHub's usernames are globally unique and will likely NOT match Brown usernames.

We strongly recommend enforcing GitHub 2 Factor Auth for non-SAML Orgs. Removing SAML will **not** impact members, but enforcing 2FA *will remove* any user who does not already have 2FA enabled on their account. For this reason, we recommend notifying users some time before enforcing 2FA so they have time to enable it. Otherwise they will be **removed** and need to be re-invited.