samegoal

User Authentication

There are three main ways to configure user authentication in SameGoal. Considerations

- Application email/password
- OpenID Connect Identity Provider
- LDAP/Active Directory

Application email/password

By default, users authenticate using an email address and password stored within SameGoal.

OpenID Connect identity provider

Single sign on (SSO) can be configured using a third party. Common providers include Google, Microsoft Azure, Duo and ClassLink. An application password is not stored in SameGoal. Configure

LDAP/Active Directory

LDAP (Active Directory, eDirectory, etc.) allows users to log in to SameGoal using the same username and password they use for other district applications (e.g. email). When SameGoal is configured for LDAP authentication and a user logs in, username and password are sent directly to your district LDAP server. The user's LDAP password is not stored in SameGoal. The server then sends back only a Yes/No answer as to whether authentication succeeded. Configure

Considerations

We recommend using single sign on or LDAP/Active Directory when its available at the district due to ease of use. Additionally, if a staff member is terminated in a centralized authentication system, they will immediately no longer be able to log in to SameGoal (even if their account is not yet deleted).

Additional implications to be aware of:

- **Password Reset** - When using single sign on with an OpenID Connect identity provider or LDAP/Active Directory, the user's password is not stored within SameGoal. Therefore, password resets must be directed to your district's IT team.
- **Third-Party Providers** - When using single sign on with an OpenID Connect identity provider or LDAP/Active Directory, this authentication method is applied to all users by default. To opt a third-party/non-district user to use an application email/password instead, visit the user's **Basics** tab, check **User not in authentication server**, and click the **Update user** button.