samegoal

LDAP/Active Directory Integration

Your district can configure SameGoal to authenticate users against a central district server via Lightweight Directory Access Protocol (LDAP). Many districts use LDAP to manage user authentication across a variety of district applications.

SameGoal supports standard configurations of Active Directory and eDirectory. Additional LDAP implementations may work but are not officially supported. To perform authentication against a locally hosted LDAP server, SameGoal servers located in the SameGoal IP range must be able to open TCP connections to your LDAP server from outside your local network.

Steps *To configure LDAP:*

1. Create and install an SSL certificate (self-signed is acceptable) on your LDAP server.
    - LDAPS (port 636) is required.
    - LDAP is not allowed (not secure).
2. Setup a publicly routable IP address which port forwards to the private IP address of your LDAP server.
3. Limit traffic to connections from the SameGoal IP range.
4. Log into SameGoal as an admin user and go to **Settings** > **District Information**.
5. Click **add Active Directory/LDAP Information**.
6. Enter in your LDAP URL.
    - Your LDAP URL must be well-formed (e.g. **ldaps://w.x.y.z/** or **ldaps://ad.district.k12.oh.us/**) and publicly routable.
7. Email your LDAP URL and LDAP Domain to tier2help@samegoal.com. The SameGoal technical team will confirm our servers can perform authentication.
    - Your LDAP Domain should be the domain you wish users to authenticate within for SameGoal.

Tip Only one of the authentication methods should be configured/enabled, so if you're enabling LDAP, ensure OIDC and ClassLink are not configured.