Access Methods

Agiloft provides a number of methods to configure user access. The system provides integration with common authentication standards, including Google OAuth and SAML, as well as other Single Sign-On (SSO) providers. In addition, administrators can configure hotlinks and access URLs, and set up two-factor authentication (2FA). To begin configuring system access, navigate to **Setup > Access**.

- User Access: Provides an overview of how users can access the system, as well as how you can create custom login pages and password reset pages.
- LDAP Access: Provides an overview of integrating Lightweight Directory Access Protocol (LDAP) with Agiloft to synchronize users, authenticate logins, and provide single sign-on support.
- Single Sign-on: Details different methods for using single sign-on with Agiloft, which is a method of simplifying user access by authenticating against a single identity source.
- Two-Factor Authentication: Describes how two-factor authentication works with Agiloft, which requires users to verify their identity using a code sent to their mobile device.
- Hyperlinks: Provides an overview of using hyperlinks to access the system, in addition to performing other actions.
- Exit and Login URLs: Details how to customize Exit and Login URLs, which determine where the user is taken when they log out or are timed out of the system, respectively.
- Groups: Provides an overview of how groups work in the system, as well as how to set group permissions with the Group Permissions wizard and the Table Permissions wizard.
- Teams: Provides an overview of how teams work in the system, as well as how to use the Teams wizard.

You can also control access by imposing IP address restrictions on your system. For more information, see Security.