



Usage for Shared Accounts

It's okay to have an account associated with a group email. You should never login using the shared account. For example, the Joint Use department has an account called JUGroup. It is associated with an email address (aldenju@aldensys.com). No one from the Joint-Use group should ever login to Alden ONE as JUGroup.

Reasons to NOT Login with Shared Accounts:

- For security and compliance.
- If the system has a password, it should never be shared across users.
- When someone leaves your company, a shared account password must be updated to prevent misuse from prior employees.
- Shared accounts create inability to have true audit history (who did what, when several users are using the same logins).
- Multi-Factor Authentication will become required on all accounts. MFA will require a single authenticator application on a user's device. If multiple people are using the same login, they will have to ask for the MFA code each time.

Acceptable Use of Shared Accounts:

- Within Alden ONE, automation can be used to auto-assign workflows to a shared account.
 - Each user should have their own login where they can access and view conversations that are assigned to the shared account.
 - By each user having their own login, they can reassign any conversation to themselves as needed.
 - Having a conversation assigned to a shared account doesn't prevent others within the company from working on a conversation.