Background information:

Our application has user accounts and groups of users (e.g. Administrators).

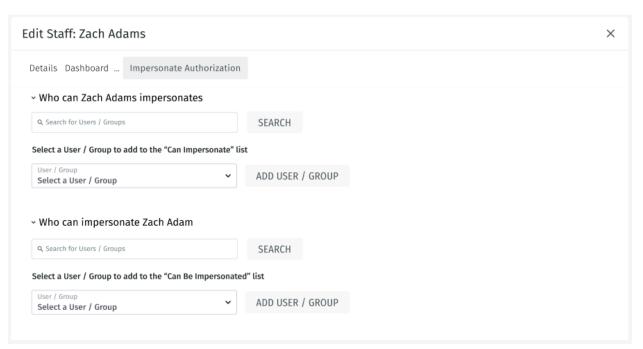
It also has a functionality that lets some users impersonate others, to perform actions on their behalf.

We want to have tight control over who can impersonate who. To do that we have developed a configuration screen on each user account where administrators can specify who this user is allowed to impersonate (specific users or members of groups). We can also see and manage who is allowed to impersonate this user.

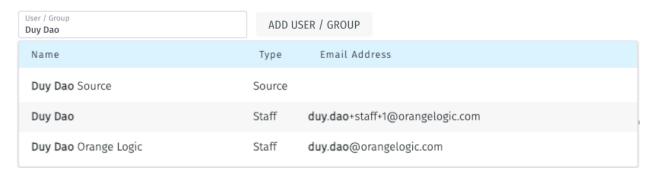
See below screenshots of these screens. What problems do you see and what are your recommendations to improve clarity and usability?

Workflow:

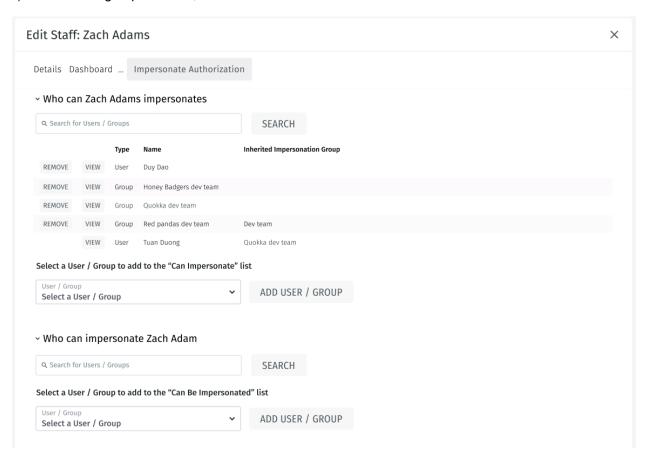
1) Enter the 'Impersonate Authorization' tab of Zach Adams' account \rightarrow No user or group is set yet.



2) Set up the list of users and groups that Zach Adams can impersonate by typing to search for a user/ group \rightarrow Select a user/ group \rightarrow Click on the 'ADD USER / GROUP' button to add the selected user/ group.



3) After a user / group is added, we'll show the list as follows.



4) You can use the search bar to search for users / groups added in a list. Enter a search term and hit Enter or click on the 'SEARCH' button to search.

