People: Admin overview

Requirements

This user guide is for anyone on Claromentis 8.2+

Introduction

In this article, you will be given an overview of the admin area of the People application where you will be able to manage/edit users within your intranet.

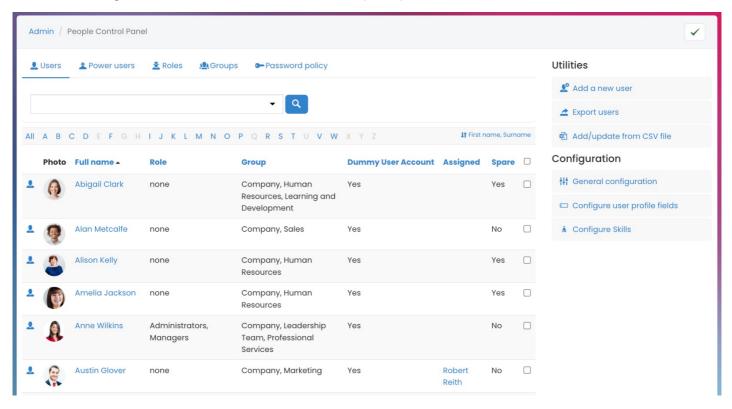The information below is outlined in the video.

The admin side & people permissions

Head to **Admin > People**.

The first area you will enter upon accessing the back end of the People application is the **People Control Panel**. From here, you will be presented with various tabs found at the top of the page.
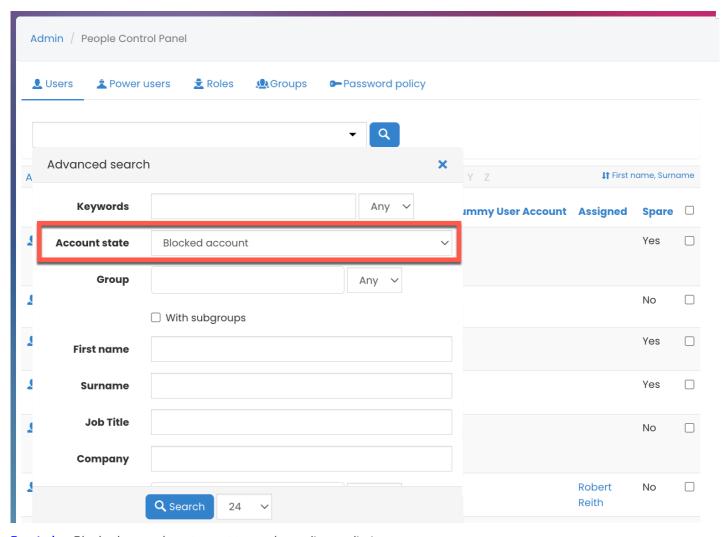
Users

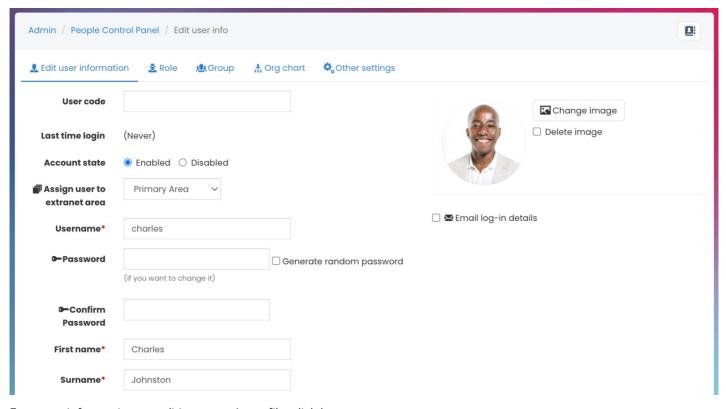**Users** is the area you will be able to view a list of all current (active) users.

As an admin, you will have additional filtering options including to also search for **Account state** (i.e. Blocked or Frozen status). This will be a useful tool if you are having to find users who are not visible from the front-end or if you

are having to reinstate Blocked users to Active status.

Reminder: Blocked users do not count toward your license limit.

When selecting a user from the list, you will be taken to an edit field where you can make changes to the user's profile.
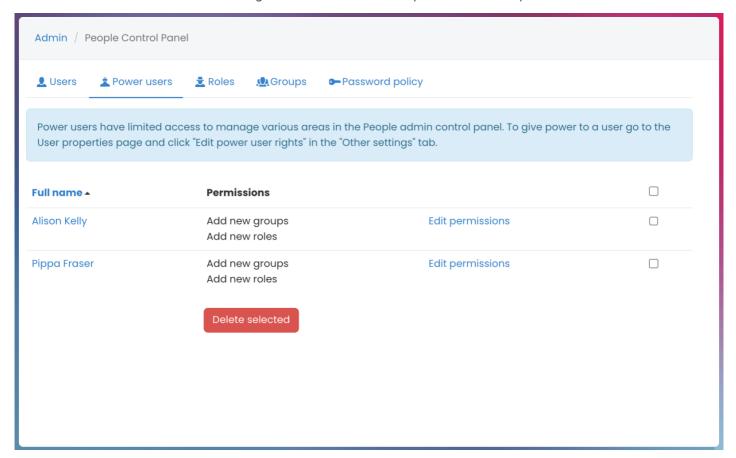

For more information on editing a user's profile, click here.

Power Users

Power Users is a feature that will give certain users access to the People Admin Panel but on a more restrictive level.

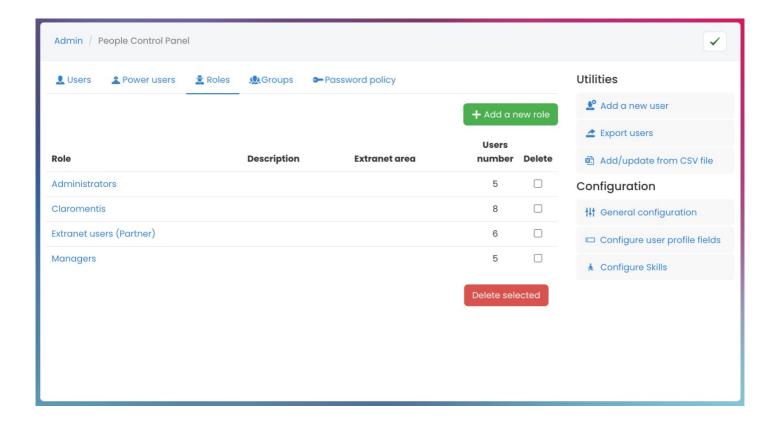Power users have limited access to manage various areas in the People admin control panel.

For more information on power users and how to assign power users, click here.

Roles

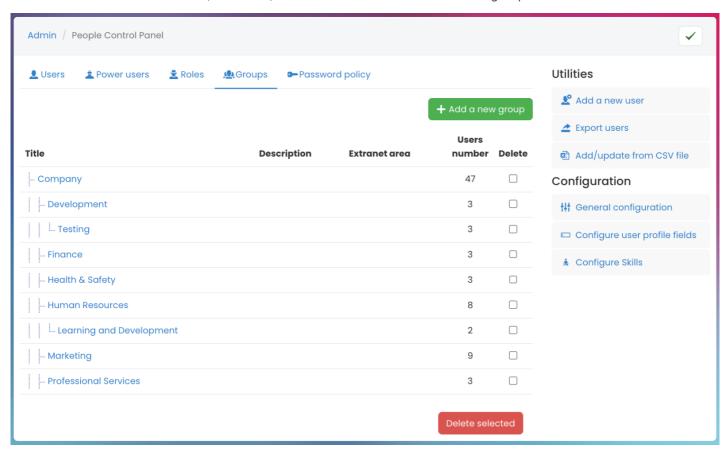The **Roles** section is where can see the roles that currently exist.

From here you can add and delete Roles, as well as, view the number of users within that Role.

Groups

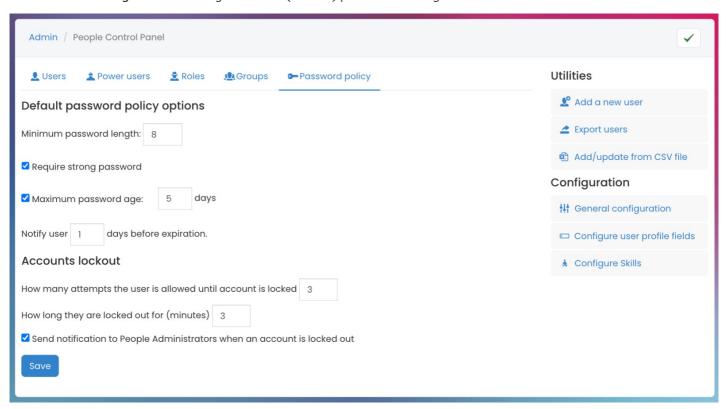Similarly to Roles, **Groups** will provide the group structure placed in your system.

You can also add and delete roles, as well as, view the number of users within that group.

For more information on Roles & Groups, click here.

Password Policy

The **Password Policy** area is where you can set (default) password settings for all users.

You have the following default password policy options:

- **Minimum password length:** Set the least number of characters that will be accepted as a password
- **Require strong password:** A checkbox option where users will have to make a password that meets complexity requirements to lower the overall risk of a security breach
- **Maximum password age:** A checkbox option to set the maximum password age meaning the number of days the password is valid
- **Notify user X days before expiration:** Set the number of days for users to get a notification before the password expires

You are also able to configure the following when accounts have been locked:

- Set the number of attempts users have until their account is locked.
- How long (in minutes) users will be kicked out of their accounts after being locked out.
- A checkbox option to send a notification to People admin when an account is locked out.