Link to article: https://discover.claromentis.com/knowledgebase/articles/369/password-policy

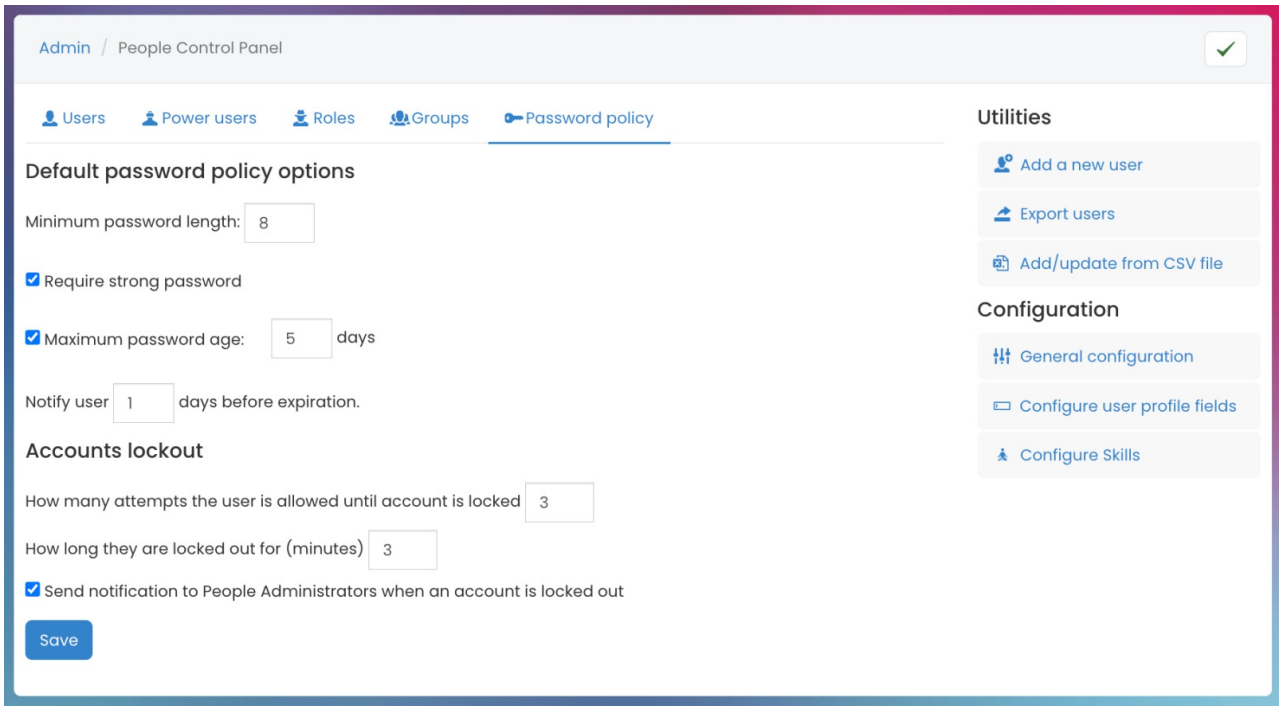
Password Policy

This guide & video aims to show the password policy on the admin side of the People application defining password reset dates and strength.

Password Policy

Navigate to **Admin > People > Password policy**

This area will allow you to configure certain settings for users' passwords.



Default password policy options

- **Minimum password length:** Set minimum password length to at least a value of 8
- **Require strong password**: Enable the option to require a strong password (i.e. at least one upper case letter, a numeric and a special character)
- **Maximum password age:** Set the number of days that a password must be used before the user can change it

Accounts lockout

- **The number of attempts allowed:** Set number of attempts allowed until the account is locked out
- **The length (minutes) users are locked out:** Set the period of time (in minutes) are locked out before users can try login again

Please note: If using Active Directory or SSO, the Password policy area is not needed.

Created on 1 February 2022 by Veronica Kim. Last modified on 1 August 2024
Tags: intranet, people, user guide, password, password reset