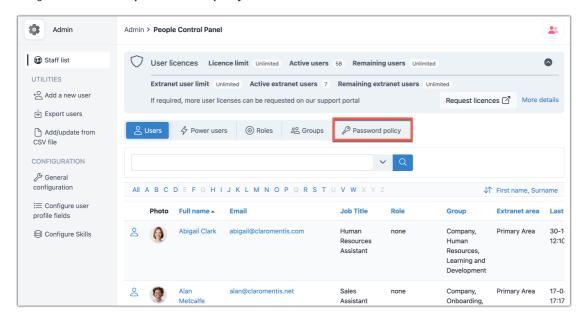


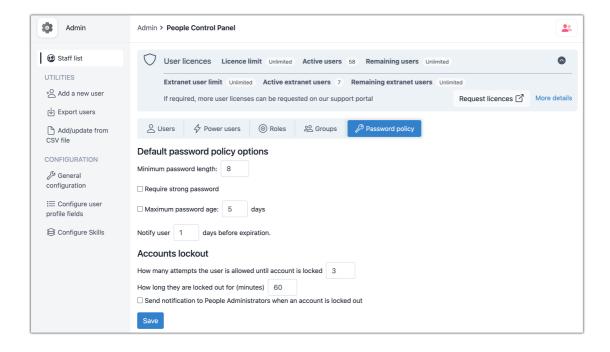
People application administrators can set a password policy that applies to all passwords created for local accounts.

(Synced or SSO accounts have their passwords controlled externally and not in Claromentis)

## **Available options**

Navigate to Admin > People > Password policy





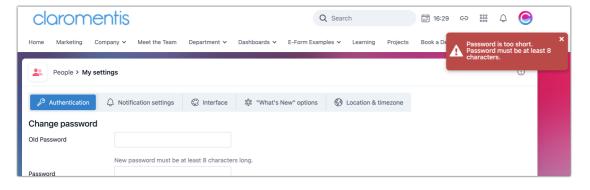
## Default password policy options

- Minimum password length: Set minimum password length (8 is the minimum value)
- Require strong password: Enable the option to require a strong password (i.e. at least one upper case letter, a numeric or a special character)
- Maximum password age: Set how long a password can be used for before the system will prompt the user to set a new one.

## **Accounts lockout**

- The number of attempts allowed: Set the number of attempts a user has to enter the correct login details
- The length (minutes) users are locked out: Set the period of time (in minutes) users are locked out for before their attempts reset, and they can try again.

If a user attempts to create a password that does not meet the password policy settings, this will be flagged on screens so they can self-rectify:



Created on 7 November 2025 by Hannah Door

Tags: intranet, people, user guide, password, password reset