

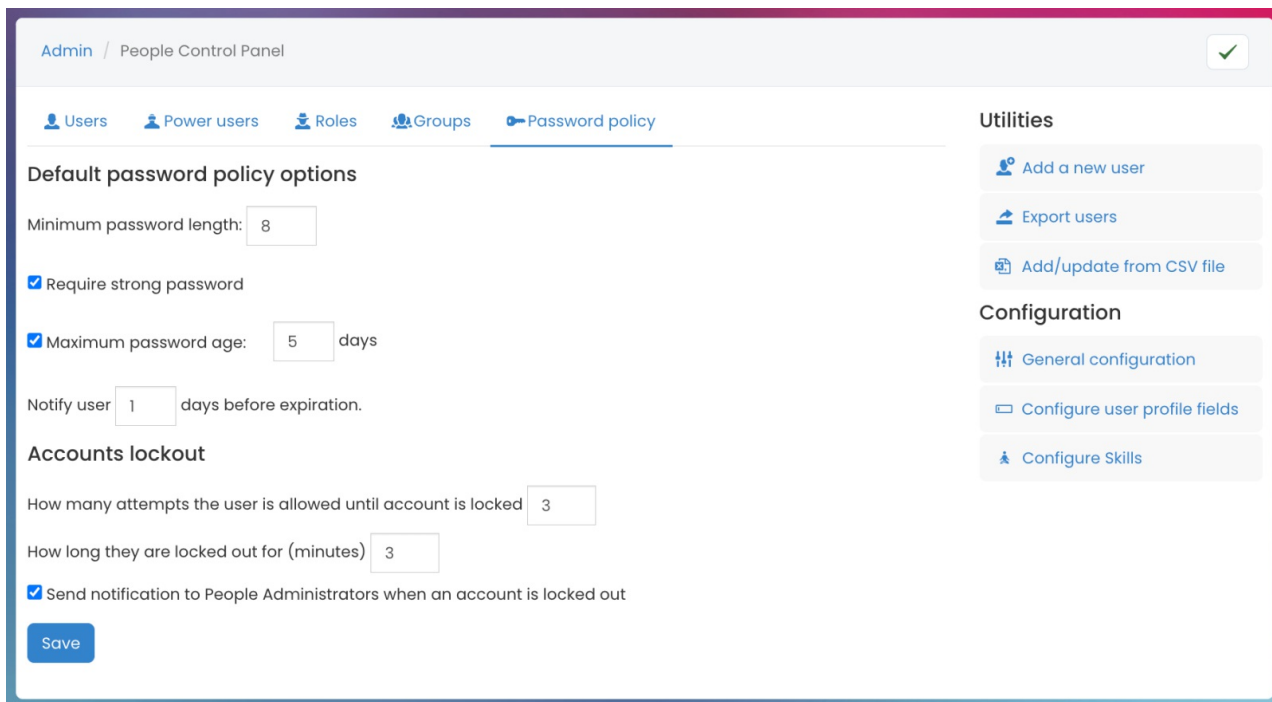
Password Policy

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.



The screenshot shows the 'Password policy' configuration page within the 'People Control Panel'. The page has a top navigation bar with 'Admin / People Control Panel' and a green checkmark icon. Below the navigation bar are tabs for 'Users', 'Power users', 'Roles', 'Groups', and 'Password policy'. The 'Password policy' tab is selected. The main content area is divided into two sections: 'Default password policy options' and 'Accounts lockout'. The 'Default password policy options' section includes a 'Minimum password length' input field set to 8, a 'Require strong password' checkbox checked, a 'Maximum password age' input field set to 5 days, and a 'Notify user' input field set to 1 days before expiration. The 'Accounts lockout' section includes a 'How many attempts the user is allowed until account is locked' input field set to 3, a 'How long they are locked out for (minutes)' input field set to 3, and a 'Send notification to People Administrators when an account is locked out' checkbox checked. A 'Save' button is located at the bottom left of the form. On the right side of the page, there are two utility sections: 'Utilities' with links for 'Add a new user', 'Export users', and 'Add/update from CSV file'; and 'Configuration' with links for 'General configuration', 'Configure user profile fields', and 'Configure Skills'.

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.