

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 in the 'People Control Panel'. The page is divided into several sections:

- Default password policy options:**
 - Minimum password length: 8
 - Require strong password
 - Maximum password age: 5 days
 - Notify user 1 days before expiration.
- Accounts lockout:**
 - How many attempts the user is allowed until account is locked: 3
 - How long they are locked out for (minutes): 3
 - Send notification to People Administrators when an account is locked out

On the right side, there are two utility sections:

- Utilities:**
 - Add a new user
 - Export users
 - Add/update from CSV file
- Configuration:**
 - General configuration
 - Configure user profile fields
 - Configure Skills

A 'Save' button is located at the bottom left of the configuration area.

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](#)