# Password Policy

Last Modified on 16/04/2019 6:26 pm AEST

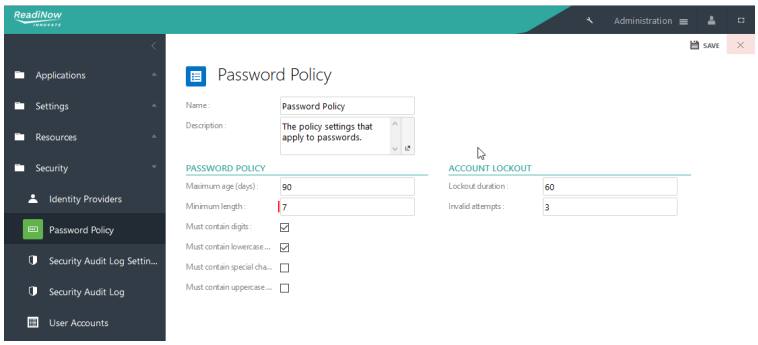
The Password Policy enables Administrators to set limits and restrictions on the types of passwords their users can create. You can use this feature to create a more secure system.

# Configuring the password policy

To configure the password policy:

1. Select Application Menu. The menu appears with available applications.
2. Select **Administration**. The application displays at the landing page.
3. In the Left Navigation Area, select **Security**. The Security expands to display list.
4. Select **Password Policy**. The existing Password Policy displays.
5. Select **Edit** and configure the following fields as required:
    - Maximum age (days): type the maximum password age in days
    - Minimum length: type the minimum password length
    - Must contain digits: select the checkbox if a digit is required for the password
    - Must contain lowercase characters: select the checkbox if a lowercase character is required for the passwords
    - Must contain special characters: select the checkbox if a special character is required for the passwords
    - Must contain uppercase characters: select the checkbox if a uppercase character is required for the passwords
    - Lockout duration: type the number of minutes a locked account remains locked
    - Invalid attempts: type the number of invalid logons before accounts are locked
6. Select **Save** to save changes.

*Screenshot: Configure the Password Policy*




# Changing your password

There are two scenarios where the password may need to be reset:

- A user is logged in, but wants to change the password
- A user has forgotten the username or password and can't log in

## Changing your password when logged in

See Changing the Password.

## Resetting the password from the login page

See Forgot your username or password