



Password Policy Control

Scenario:

The purpose of a password policy is to prevent unauthorized access to sensitive information and protect against security breaches. A strong password policy can help ensure that users are using strong, unique passwords that are difficult for hackers to crack, and can reduce the risk of password-related security incidents

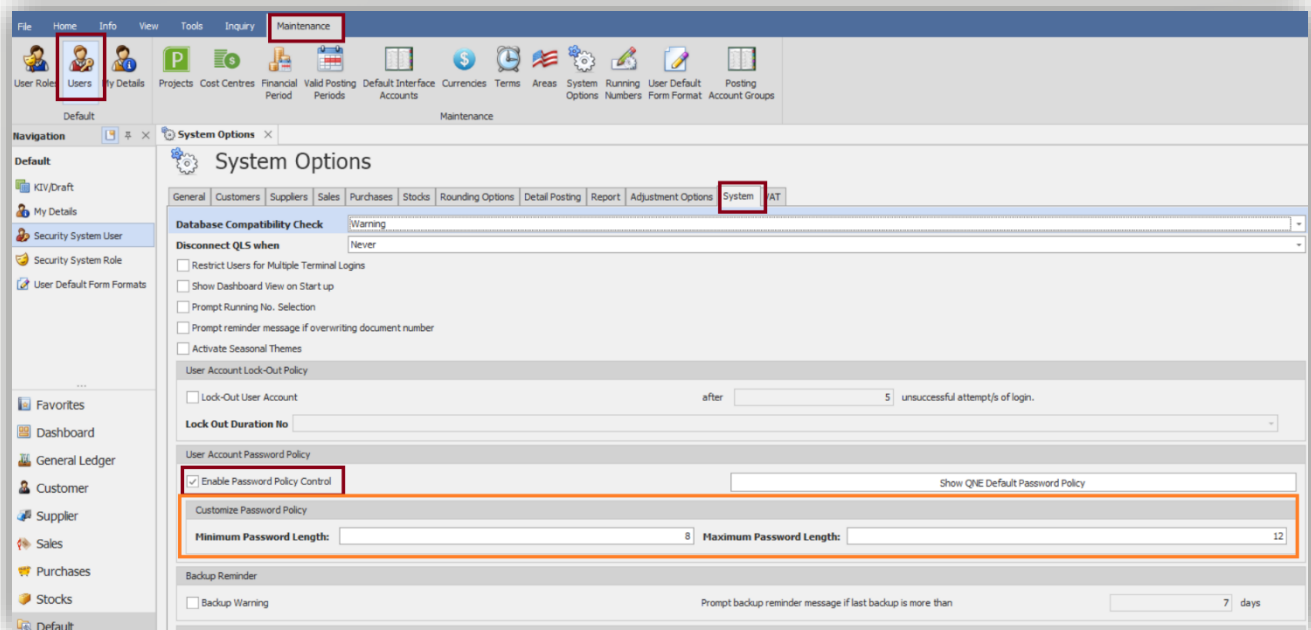
You can now set password policy in your QNE Software. Below are the criteria for the password policy

- Minimum 8 alphanumeric characters, maximum 12 characters (Default)
- Must contain at least 1 upper case
- Must contain at least 1 lower case
- Must contain at least 1 number
- Must contain at least 1 special charact e.g., * \$

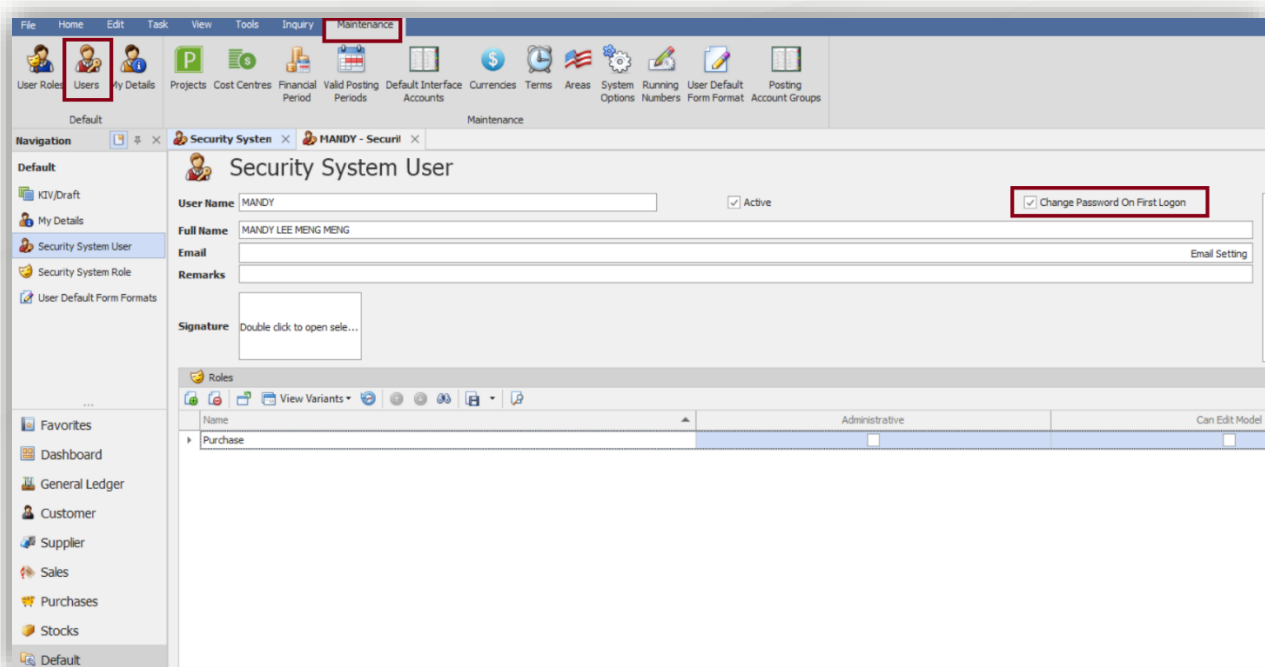
In QNE Software, you can setup the minimum and maximum length as well

Solution:

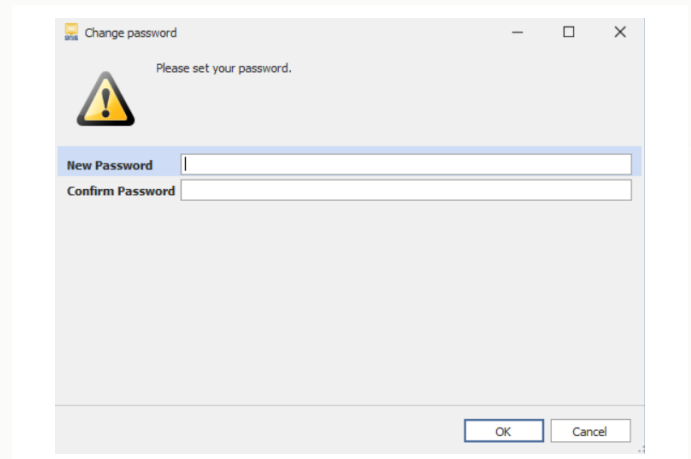
1. Maintenance > System Option > System, enable Password Policy Control
Aware that you can change the Minimum & Maximum Password Length in the setting as well



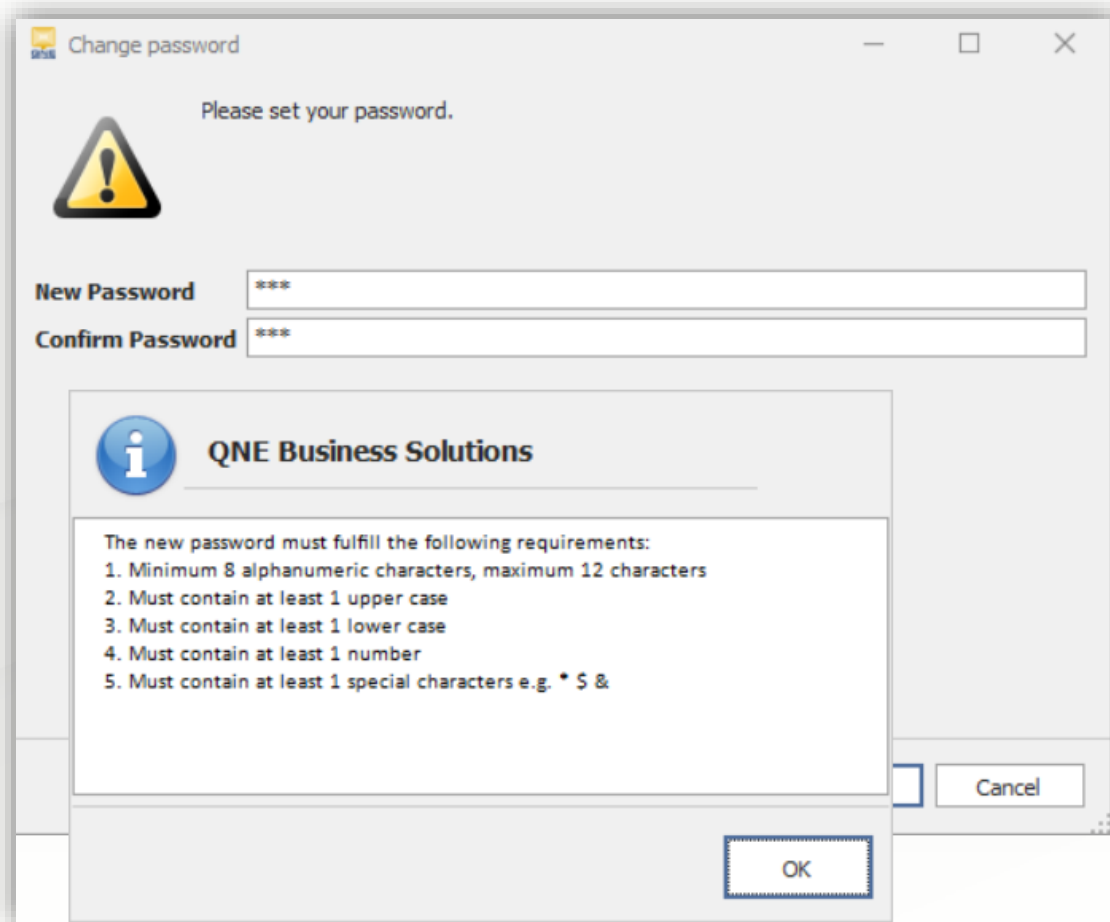
2. When you create a new user, tick "Change password on first login"



3. When user login to the system, system prompts to setup password, user has to fulfill password policy criteria.



4. If user update the password without follow the password policy criteria, system does not allow to login and prompts message as below. So user has to follow the requirement in order to setup the password.





For the user who already setup password before intend to apply password policy control, you need to reset the password for each user.

Go to Maintenance > User > Select the user > Edit > Reset Password

Name	Administrative	Can Edit Model
Purchase	<input type="checkbox"/>	<input type="checkbox"/>



For some of the users who like to change password every [90] days kindly refer this article

<https://support.qne.com.my/support/solutions/articles/81000410403-how-to-change-password-after-x-days->