How to configure User Account Lock Out Policy ?

[Version 1.0]

Jason Lee

[07 March 2023]

Amendment Record

| REV. No	Nature of Change	Prepared By	Prepared Date	Reviewed & Approved by
1.0	Creation	Jason Lee	07-Mar-2023	

SCENARIO

A user account lockout policy is a security policy that determines when and for how long a user account should be locked out after entering a wrong password.

It can help prevent malicious users or hackers from guessing and cracking the user's password by using brute force.

SOLUTION

1. Go to Maintenance > System Options > System
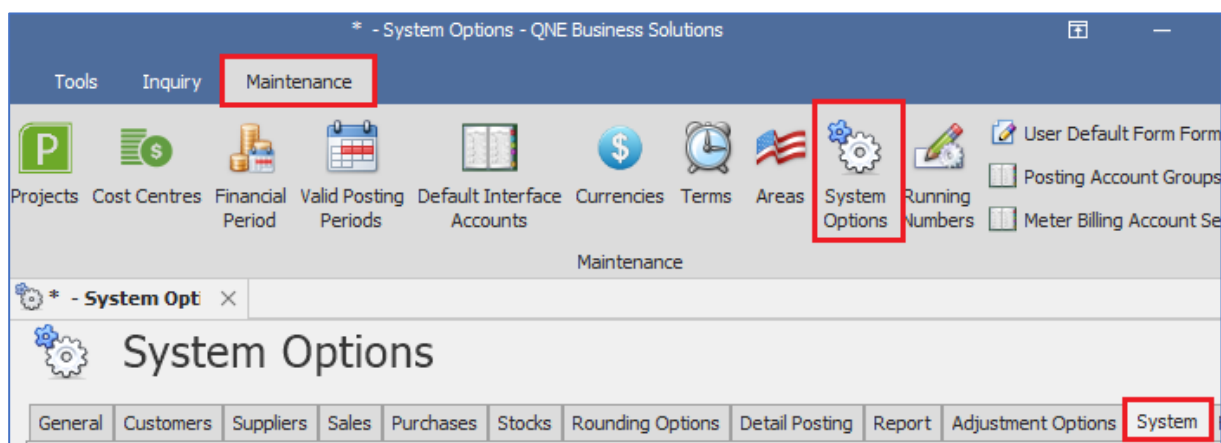
2. Under "User Account Lock-Out Policy", tick checkbox "Lock-Out User Account"
3. Key in "After x unsuccessful attempt/s of login" to define lock out an account after the user entered the wrong password x number of times.
4. Select lock out account for how long in "Lock Out Duration No"
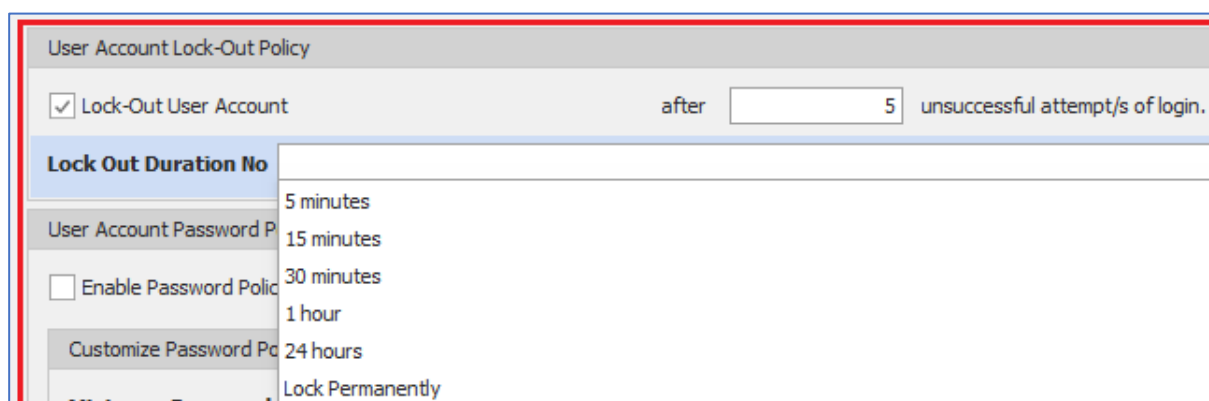
5. Click Save after configuration.

6. A "Login Failed" message will prompt when the user (User_A) enters the wrong password 3 times
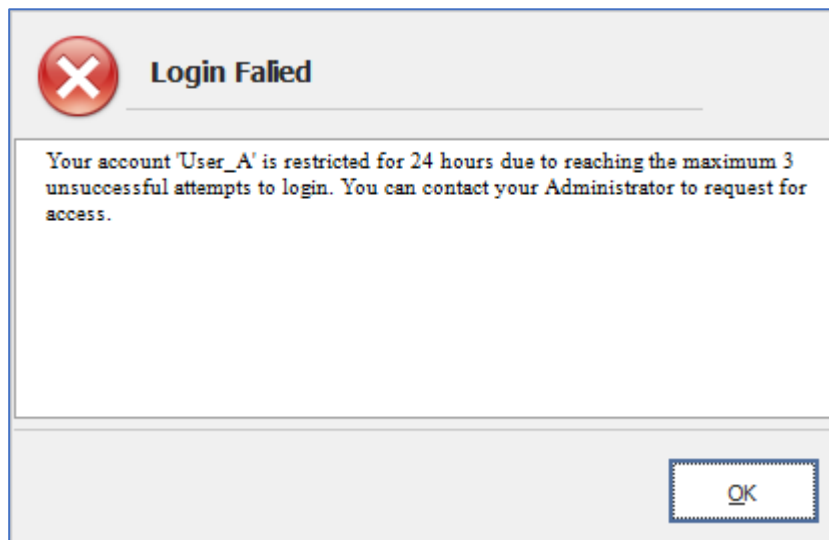
7. Based on the above example, User_A can either wait for 24 hours or contact the "Administrator" user to Unlock the User Account.
8. To unlock the locked User Account, Administrator can go to Maintenance > Users > double-click on the locked User Account.
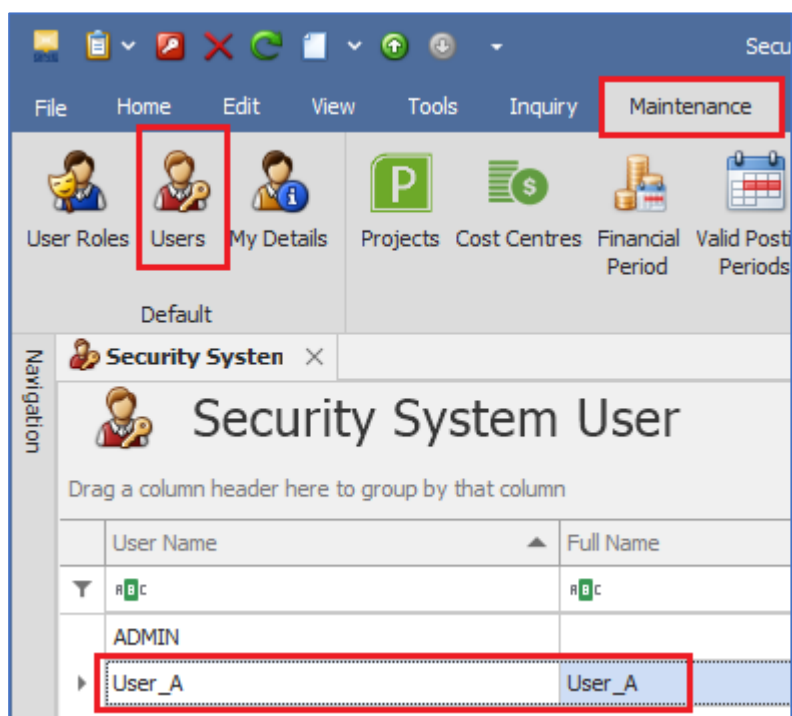
9. Go to Edit then click the "Unlock Account" button.
10. Now the "User_A" account is unlocked and able to login again.

** Learn more about How to reset user's password

** Learn more about Azure Cloud

** Learn more about QNE Hybrid Cloud Software