5. If a user uses wrong passwords several times, he would not be able to log in even with a correct password afterwards.

Cause: To prevent unauthorized access to the CAP Systems, 3 consecutive unsuccessful attempts (using wrong passwords) to log in will lock the corresponding user account automatically (excluding Discoverer). All further attempts, even with the correct password, will not be entertained.

Solution: When a user account is locked, the system administrator should follow these steps to release it:-

a. Log in the CAP System using the responsibility of the System Administrator.

b. Go to Security > User > Define.

c. Remove the "Effective End Date" of the relevant user record.

d. Reset the password to anything desirable. The original password can be re-used, or a new one can be used.

e. Inform the user the new password.

Please note the followings:-

a. When the user logs in again, the System will prompt him to change his password immediately.

b. If the user uses an incorrect password, the account will be locked immediately (instead of allowing 3 consecutive unsuccessful attempts).

c. When an account is locked (when the password is <old password>) and the user has successfully re-set it to a new password (<new password>), and then the account is locked again after 3 consecutive unsuccessful attempts to log in, the System Administrator will not be able to re-set the password to either the <old password> or the <new password>.