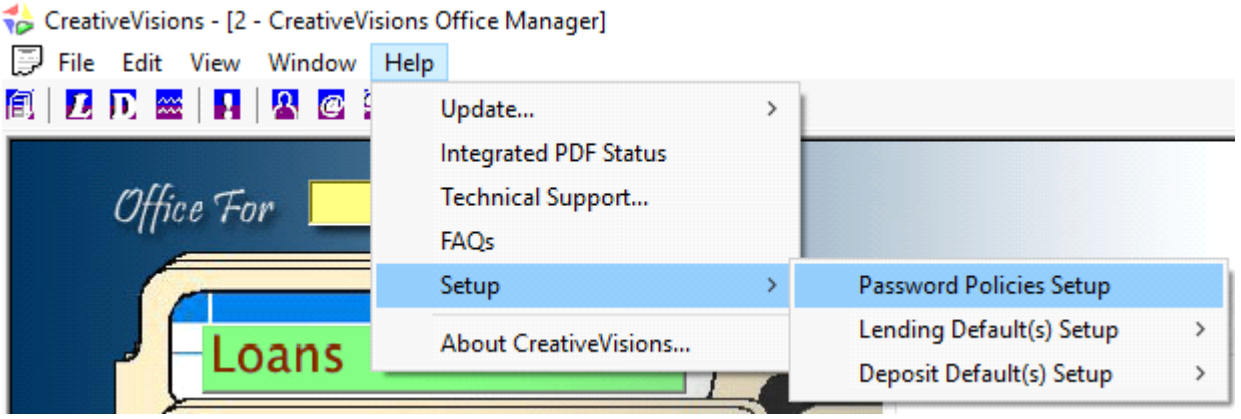
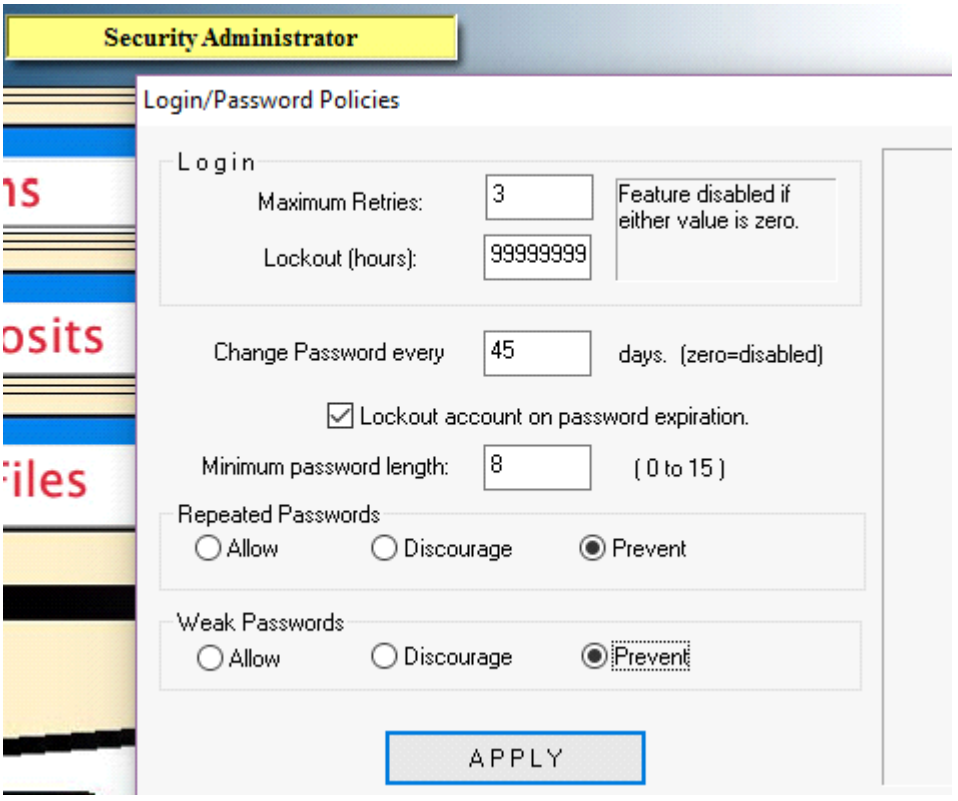
Enabling password policies in CreativeVisions

Tuesday, November 15, 2016 8:47 AM

From the toolbar menu; go to >Help >Setup >Password Policies Setup.

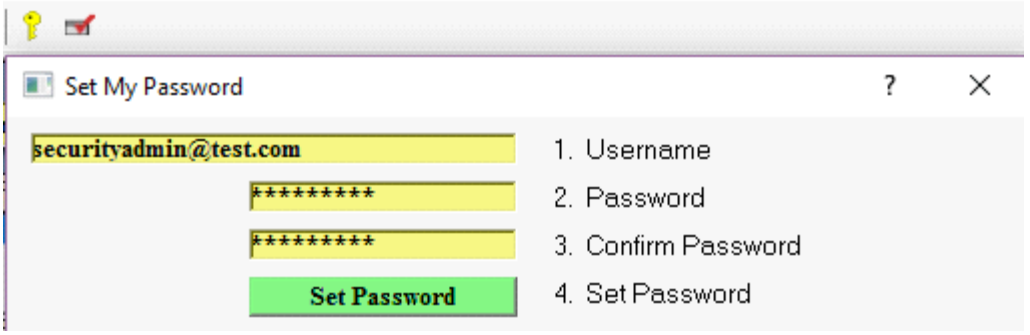


If your login does not have administrative rights, then the policies would appear as grayed out. Only a System Administrator will have the rights to make changes on password policies.



IMPORTANT NOTE: If all your values are currently set to "0", then your password policies have not yet been turned on and are disabled. BEFORE enabling password policies, each end user should FIRST re-generate their password according to the standards that will be applied. That way all user's do not get locked out of the system. For example, if you will be enforcing a password length, and if only strong passwords will be allowed; then end users should change their password to the required length, and include an uppercase letter, lowercase letter, digit and punctuation.

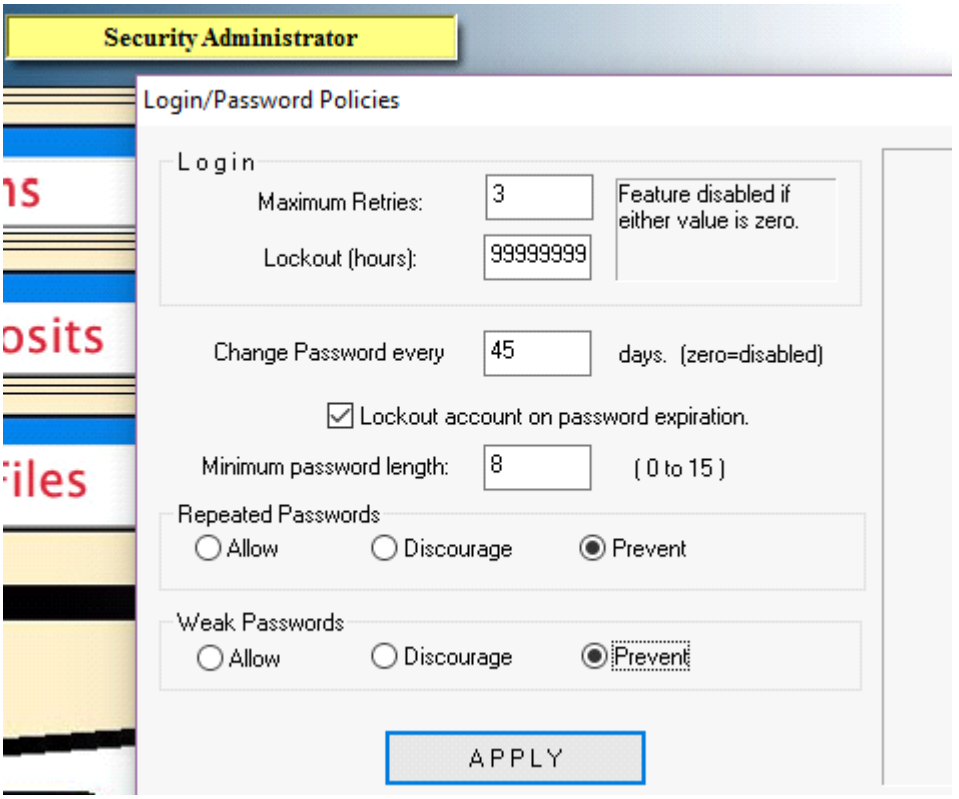
End users can change their existing passwords by clicking on the key icon on the toolbar. They must type and enter their new password **and press the tab key off each field** on #2. and #3. And then click on "Set Password".



Entering a number in the Maximum Retries field, will only allow an incorrect password to be attempted that corresponding number of times.

The number of lockout hours entered is used in conjunction with maximum retries. If the number of retries has been reached, then the system will prevent any more login attempts on the account, until the corresponding number of hours has passed.

Upon reaching the corresponding number of days when a password must change, end users will receive a warning message up to 4 days before expiration to alert them it is time to change the password.



If the “Lockout account on password expiration” option is enabled, then users will be prevented from logging into the account if the password was not reset before expiration. If the “Lockout account on password expiration” option is not enabled, then users will simply receive a warning message to reset their password upon every login attempt made, after expiration was reached.

If "Discourage" is checked on either Repeated or Weak passwords, then end user's will only receive a warning message. Otherwise if "Prevent" is checked, the system will require the passwords meet the standard and will not accept otherwise.

Enabling the use of strong passwords will require end users to set passwords consisting of at least one of each of the following: an uppercase letter, lowercase letter, digit and punctuation.

Note: If needed, administrators have the ability to re-enable an account which has been locked out.