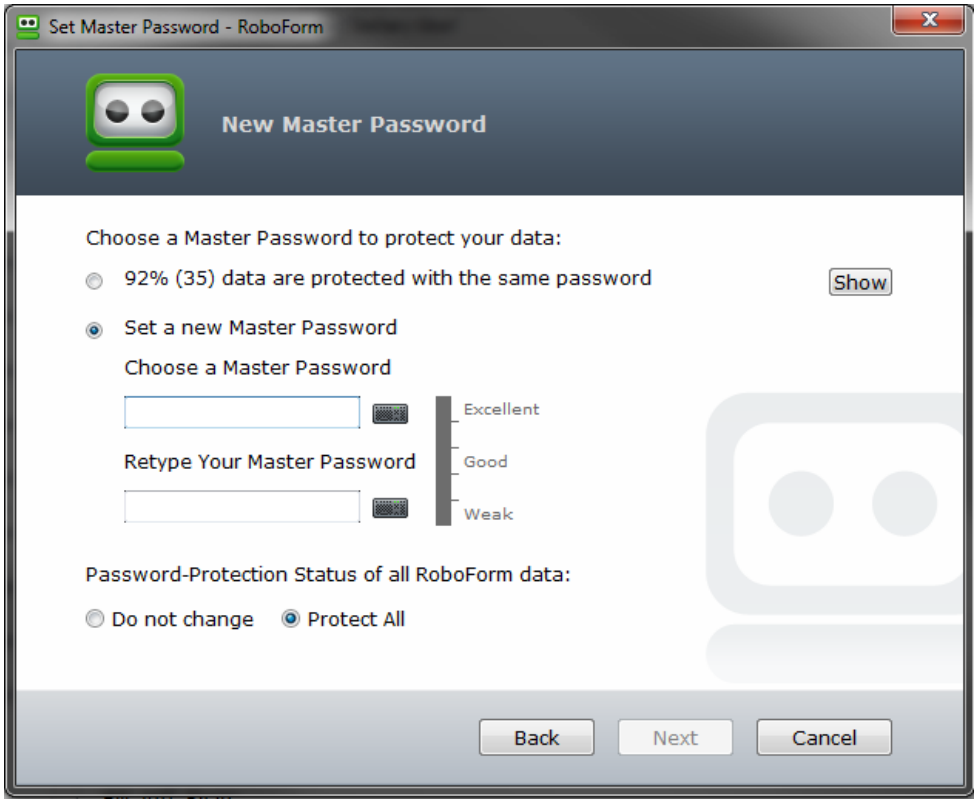
Implementing Dual Master Password Functionality in RoboForm

The Dual Master Password function of RoboForm allows Passcards to be shared in a protected format

1. For a user to capitalize on Dual Master Password (Henceforth referred to as “DMP”) functionality, they must first set their own personal Master Password to a DMP-enabled one.
    a. To do this, click the RoboForm Icon in the System Tray, then select Options.
    b. Click on the “Set Master Password, Mass protect/unprotect” button, then “Next”
    c. On this screen, set your password with a backlash in the middle. For example, the password ”Pass\word123” is an acceptable DMP type.
    d. Ensure that you select “Protect All” under “Password-Protection Status of all RoboForm Data”



2. Next, the Administrator has a few steps to take to configure the RoboForm Enterprise Managed Console for DMP
    a. Open “Services” and Stop the RFConsole service
    b. Open Group Policy Manager, and in the RoboForm Enterprise GPO, ensure that "DualPassEncryptionKeyScheme" is Enabled

c. On the server, open RoboForm and click Options. Navigate to the User Data tab. Ensure that this folder is the same as the “Path to Files” from the Company tab in the Console interface.
d. Change the Master Password of the RoboForm on the server to a DMP-enabled one by following the same steps as above
    i. Doing this will re-encrypt the Console’s passcards with the new DMP-enabled encryption
e. In the Console web interface, go to Companies, and update the Server Master Password for your Company to match the Dual Master Password which you just set the Server’s Passcards to.
f. Open “Services” and Start the RFConsole service

3. Congratulations! You should now be able to push Passcards out in an encrypted manner.
    a. When these Passcards are pushed out, users will be prompted to enter the first part of their DMP-enabled Master Password to use the Passcard.
        i. In our example, this will be “Pass”, and will be unique to each user.