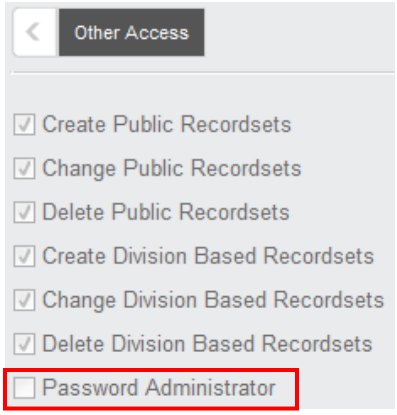
AwareManager JXT now offers password administration features that allow you to maintain tighter control over the passwords used by your Contacts.

Establishing a Password Administrator

It is very important that you first identify in your organization who will serve as password administrator(s). They will be responsible for setting up any rules regarding acceptable passwords and serving as the point people for users who require password assistance moving forward.



Password Administrator access is set up via Permissions:

1. Go to **Administration→Permissions**.
2. Under the Other Access tab you will see a **Password Administrator** checkbox.
3. For any Permission group you want to serve as password administrators, select this option.

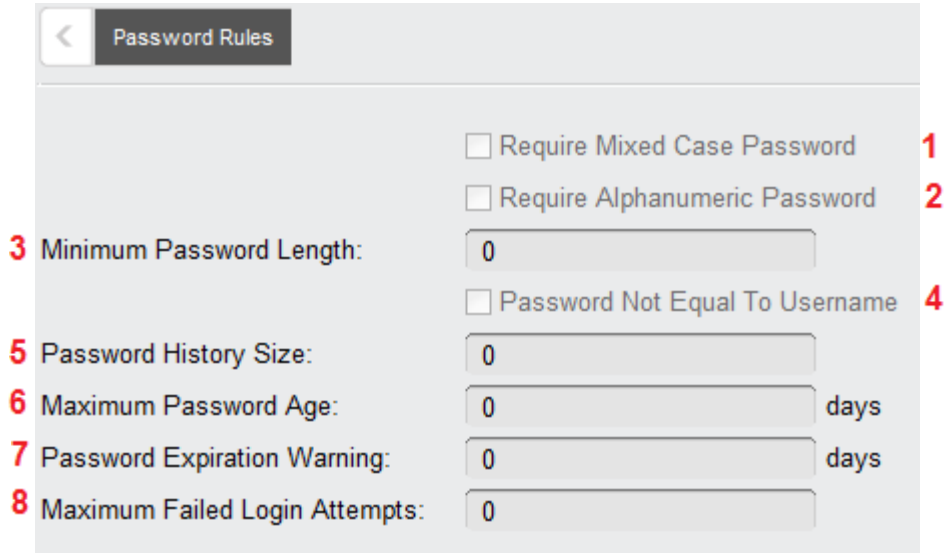
Note: If you only want a subset of the Contacts belonging to the current Permission group to serve as password administrators, you should do the following:

1. Select the original Permission record and duplicate it.
2. Leave all values the same and additionally select **Password Administrator.** They should also have access to Contact Preferences, if this is not already granted.
3. Save the record with a new **Code**.
4. Return to the original Permission record from **Step 1.**
5. In View mode, press the **Contacts** button to jump to the list of Contacts currently linked to this Permission.
6. Highlight those contacts you want to serve as password administrators.
7. From the Contact List, change their **Permission** to the new record created in **Step 3.**

The password administrators will have access to the various features related to password management, including both password rules and password operations.

Password Rules

The rules which define the types of passwords that are acceptable can be found under Contact Preferences (right-click on **Contacts** and select **Preferences**).

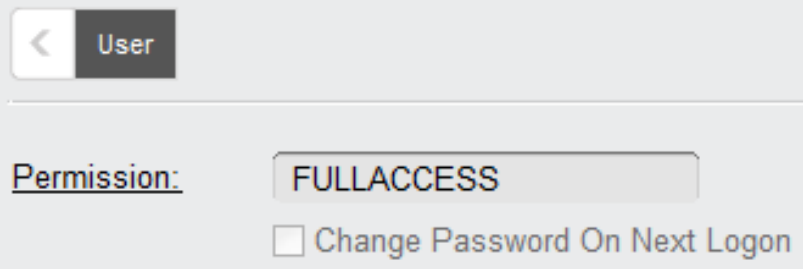


1. **Require Mixed Case Password** – requires that any password entered must contain a combination of upper and lowercase characters
2. **Require Alphanumeric Password** – requires that any password entered must contain a combination of alphabetic and numeric characters
3. **Minimum Password Length** – specifies the minimum length allowed for a password. If this value is set to 0, there is no minimum length.
4. **Password Not Equal To Username** – requires that a user's password cannot be the same as their Contact *Code*
5. **Password History Size** – specifies the number of unique passwords a user must set for him or herself before they can reuse a password. If this value is set to 0, it means there are currently no restrictions on how often a password can be reused.
    - **For example:** if this value is set to 3, the user can't reuse their first password until they've reset it a second and third time; on the fourth time they may reuse the original.
6. **Maximum Password Age** – specifies the number of days a user's password will be valid before they must change it. This counter goes in effect for each individual user from the day they last reset it. If this value is set to 0, it means there is currently no maximum password age.
7. **Password Expiration Warning** – specifies the number of days in advance of the expiration date the users will begin receiving expiration notifications immediately after login. They will be prompted to change their password with each notification with the option to hold off. This notice will appear each time they log in from the number of days out specified until 1 day out; at 0 days remaining the user will be forced to change their password after login. If this value is set to 0, it means the users will not receive any advance warning.

8. **Maximum Failed Login Attempts** – specifies the number of incorrect login attempts that are allowed per user name before their account is locked out. At that point a password administrator must unlock the account for the user. If this value is set to 0, no maximum is enforced.

Contact Updates

The **Contacts** capsule has also been altered to account for the new password restrictions. All changes pertain to the **User** tab.

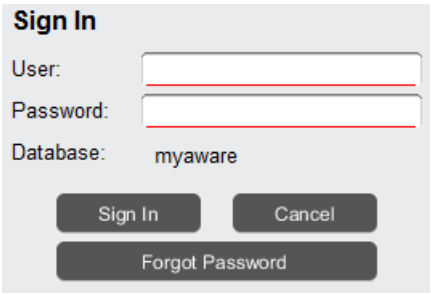


1. Password fields have been removed from this tab; passwords cannot be viewed within the program anymore
2. **Change Password On Next Logon** – If this is selected for a user, after their next successful login to the system they will immediately be prompted to change their password. This new password will have to conform to any new password rules established. After the user changes their password, this checkbox will automatically become unchecked.

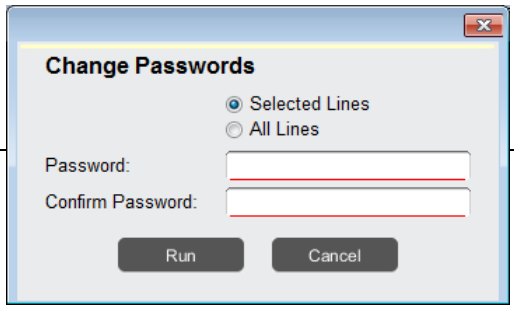
Note: Password Rules are not retroactive, meaning any user whose password was set before these rules were in place will not automatically be forced to change it. You should instead select the *Change Password On Next Logon* checkbox for all users so that the next time they logon they are forced to choose a new password that conforms with the rules.

Password Operations

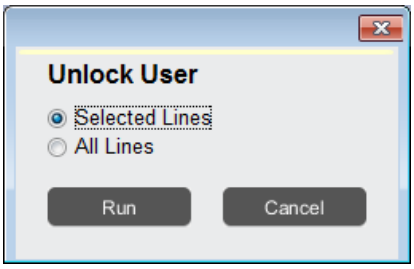
Following are the operations which pertain to password administration:



- **Forgot Password**: This option, available from the login screen, requires that you first enter your login in the *User* field. Pressing this button will then prompt you to confirm you want your password reset. If you press **Yes**, the system will reset the password for the login specified and email it to the address on file for that login.
- **Change Password** (User Settings): This operation is still available for individual users to manually change their password. From **User Settings** select **Operations > Change Password** to enter and confirm your new password. The system will check that the new password conforms to any password rules in place.
- **Change Passwords** (Contacts)**:** This operation is visible under the **Operations** menu of the **Contacts** capsule, but is only accessible by those Contacts who are selected as Password Administrators. You



can select one or more contacts in the Contact List and run this operation to reset all of their passwords to the same value. If the new password does not conform to the password rules in place, you will see an error report detailing the problem and no passwords will be updated. In this case you will have to re-run the operation until a new password is accepted.



- **Unlock User:** This operation is visible under the **Operations** menu of the **Contacts** capsule, but is only accessible by those Contacts who are selected as Password Administrators. Select one or more users who have been locked out of the system (due to exceeding the *Maximum Failed Login Attempts*) and run this on their Contact records to unlock them. The number of failed login attempts stored for them will be reset to 0 at this point.
- **Show User Information:** This report is visible under the **Operations** menu of the **Contacts** capsule, but is only accessible by those Contacts who are selected as Password Administrators. Select one or more users to run this report on. For each user the report will indicate the following:
    - *Contact* – Code
    - *Password Changed Date* – Last day the user's password was changed.
    - *Current Failed Logon Attempts* – Number of consecutive times the user unsuccessfully tried to log in to the program.
    - *Account Locked* – Indicates whether their account is currently locked; in this case you must run the **Unlock User** operation on those users for them to be able to log in again.

AwareManager jxt

User Information
DIG Property Group
50 Congress Street
Boston, Massachusetts 02109

Contact	Password Changed Date	Current Failed Logon Attempts	Account Locked
BAIN.MATTHEW	April 9, 2013	0	No
BARLEY.BILL	April 9, 2013	0	No
BEAVER.JIM	April 9, 2013	0	No