DATAFLOW
Financial Software Solutions

Users & Security

Dear user,

You must make sure that you have read “Navigating the System” first before reading any other Clarity guides as without a good knowledge of the navigation you will not fully benefit from the features and shortcuts that Clarity will provide for you.

Click here to read Navigating the System:
https://dataflow.co.uk/images/uploads/release_notes/Clarity_-_Navigating_the_System_.pdf

Also at the end of each guide, there may be a list of other supplements for further explanation of features within this routine.

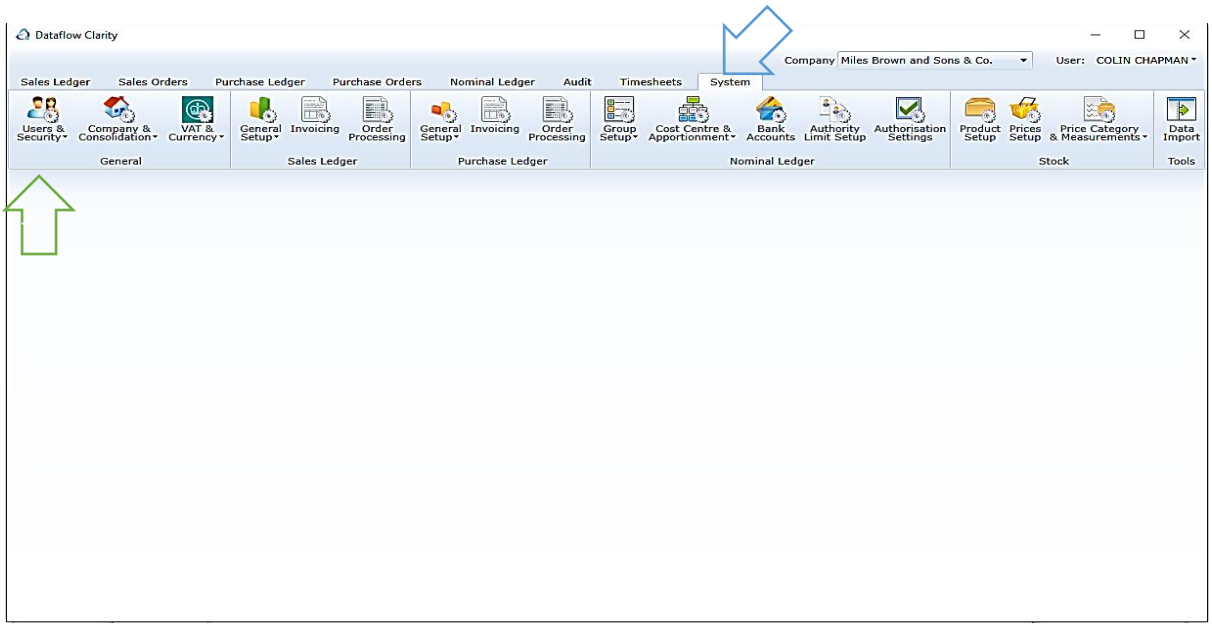
Enjoy exploring Clarity and please do not hesitate to suggest any improvement that you feel will be useful to add to this document.

Warmest regards

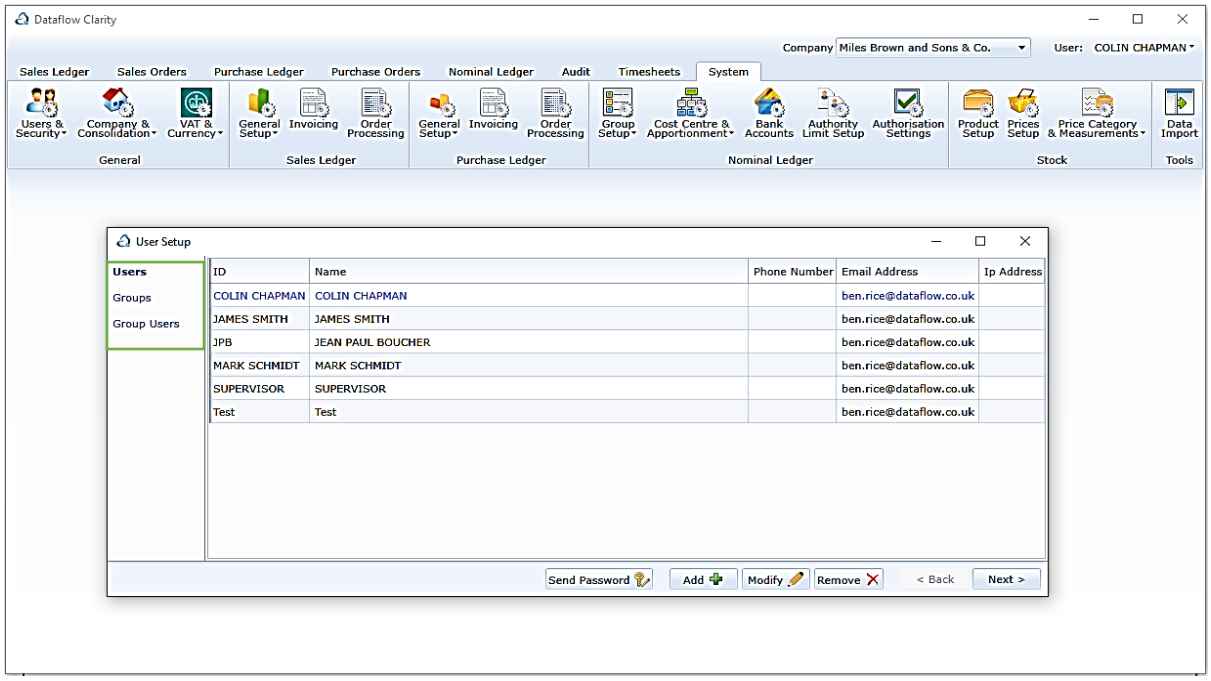
Dataflow (UK) Ltd

The *Users & Security* window is the area where you setup Clarity users, assign licensing access and manage how the system handles user passwords.

The *Users & Security* section is found in the *System* tab (blue arrow in the image below), then to *Users & Security* (green arrow).



The first option is the *Users Setup* window. The *User Setup* window is split into three sections – *Users*, *Groups* and *Group Users* (highlighted below in green).



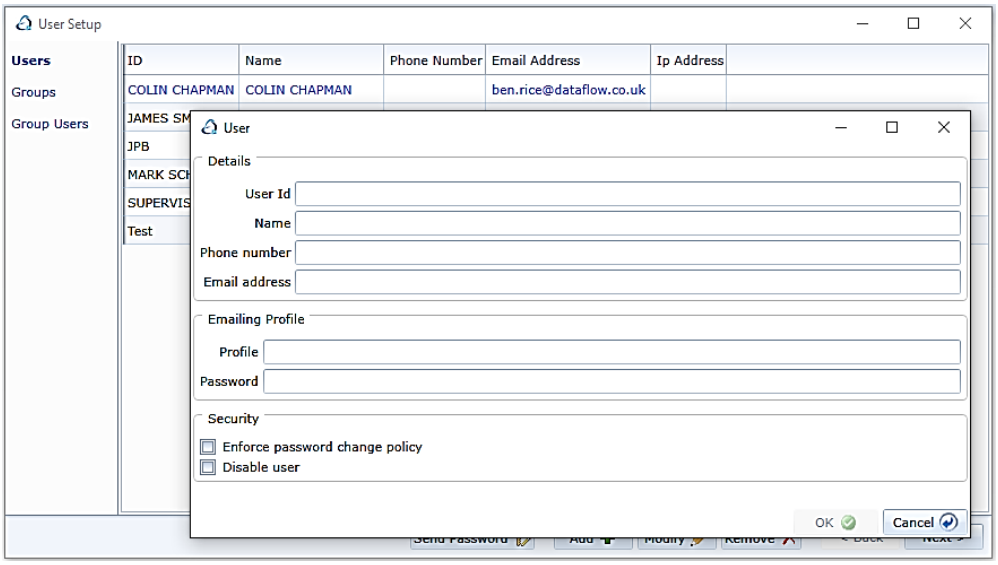
The first section is *Users*. This is where you create, modify and remove users.

To add a new user use the Add button.

To modify an existing user click on the user within the list and use the Modify button.

To remove an existing user click on the user within the list and use the Remove button.

Clicking Add to create a new user will open the following form.



The *Details* section:

The ***User ID*** field is the User ID entered when the user logs into Clarity.

The ***Name*** field is the user name.

The ***Phone number*** field is the users contact number (not mandatory).

The mail address entered into the ***Email address*** field is the email address Clarity will use when resetting passwords. Emailing Profile section will be removed and should not be used.

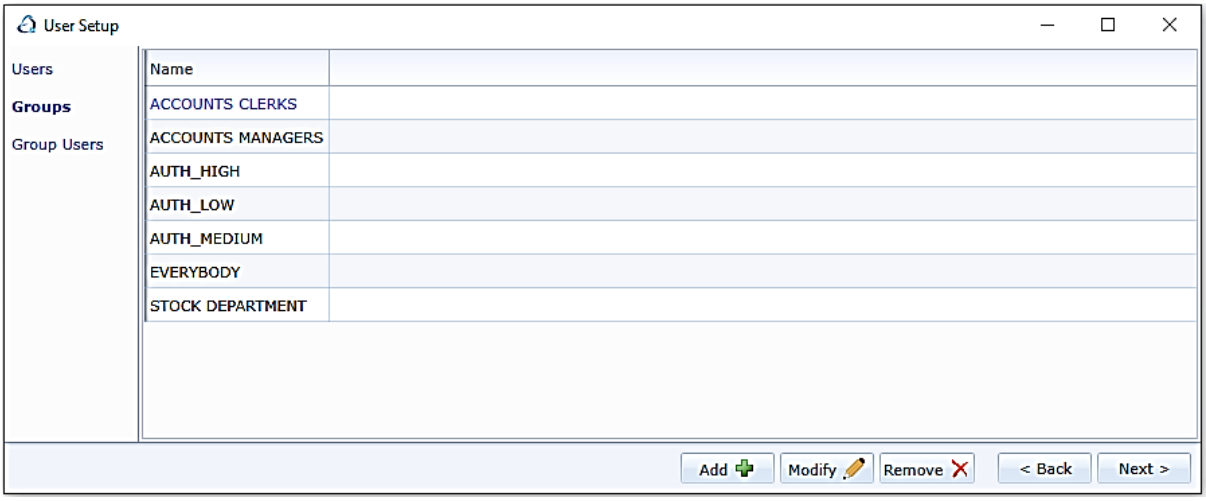
The *Security* section:

Enforce password change policy: This parameter works in conjunction with the Password change section within the Password Security window detailed further down in this guide.

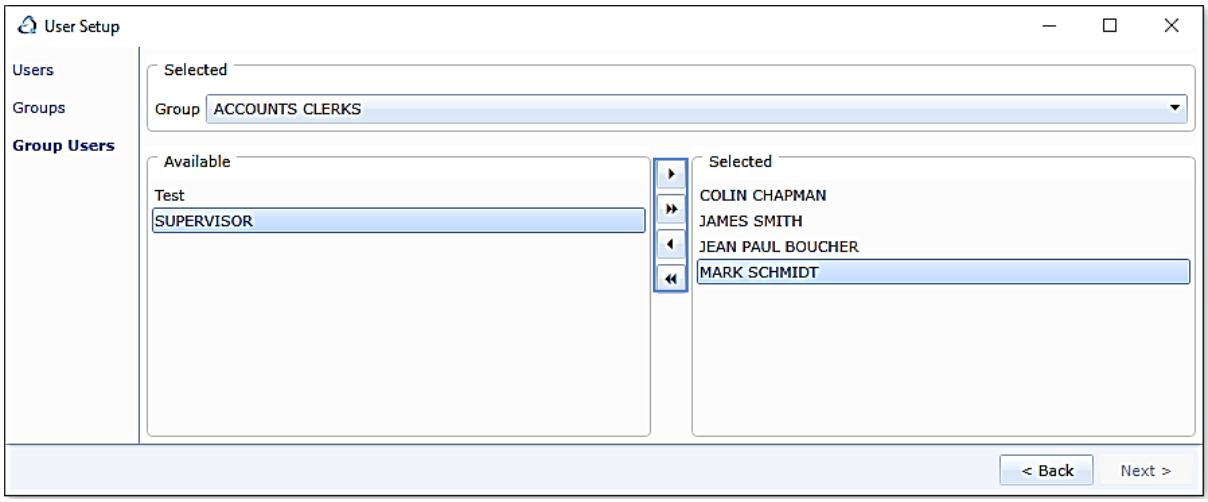
Disable user: Tick this parameter if you wish to disable this user's access. Clarity adds a user stamp to the transactions posted by that user for audit transparency. Deleting a user will remove this association so it's recommended that users are disabled to maintain this history rather than delete the user.

The next section is *Groups*. This is where you create, modify and remove user groups. Authority limitations are applied at group level rather than user level. As an example a user group can be a description given to a body of users, such as a department etc. that will adopt the same authority limits set in Clarity.

To add a new user group use the Add button.
To modify an existing user click on the user group within the list and use the Modify button.
To remove an existing user click on the user group within the list and use the Remove button.



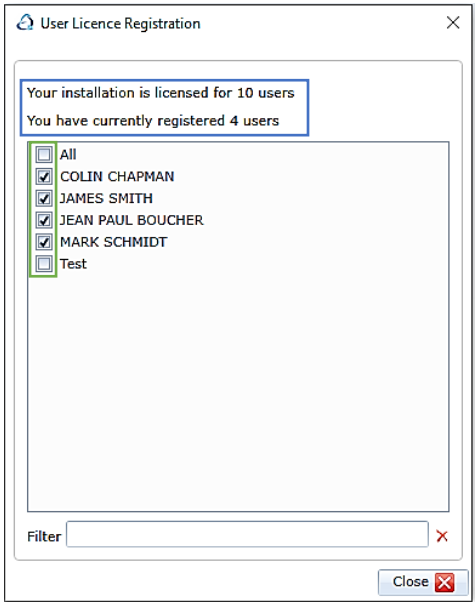
The last section in this window is *Group Users*. This is where you assign users to their corresponding user Group. Assign users by clicking on the user and then move the user across using the central arrows highlighted below in blue.



The Second menu option under *Users & Security* is the *User Licence Registration* window. Your Clarity licencing agreement will allow for a set number of Clarity users. Use the *User Licence Registration* window to assign Clarity access to the required users.

The area highlighted in blue below denotes how many users your licence allows and how many user licences you have used.
To assign user access simply tick the box next to the required username (highlighted in green below), or tick the *All* option to automatically tick all users.

Note – you may set up as many Clarity users as you wish but you will only be able to tick as many users as you are licenced for.

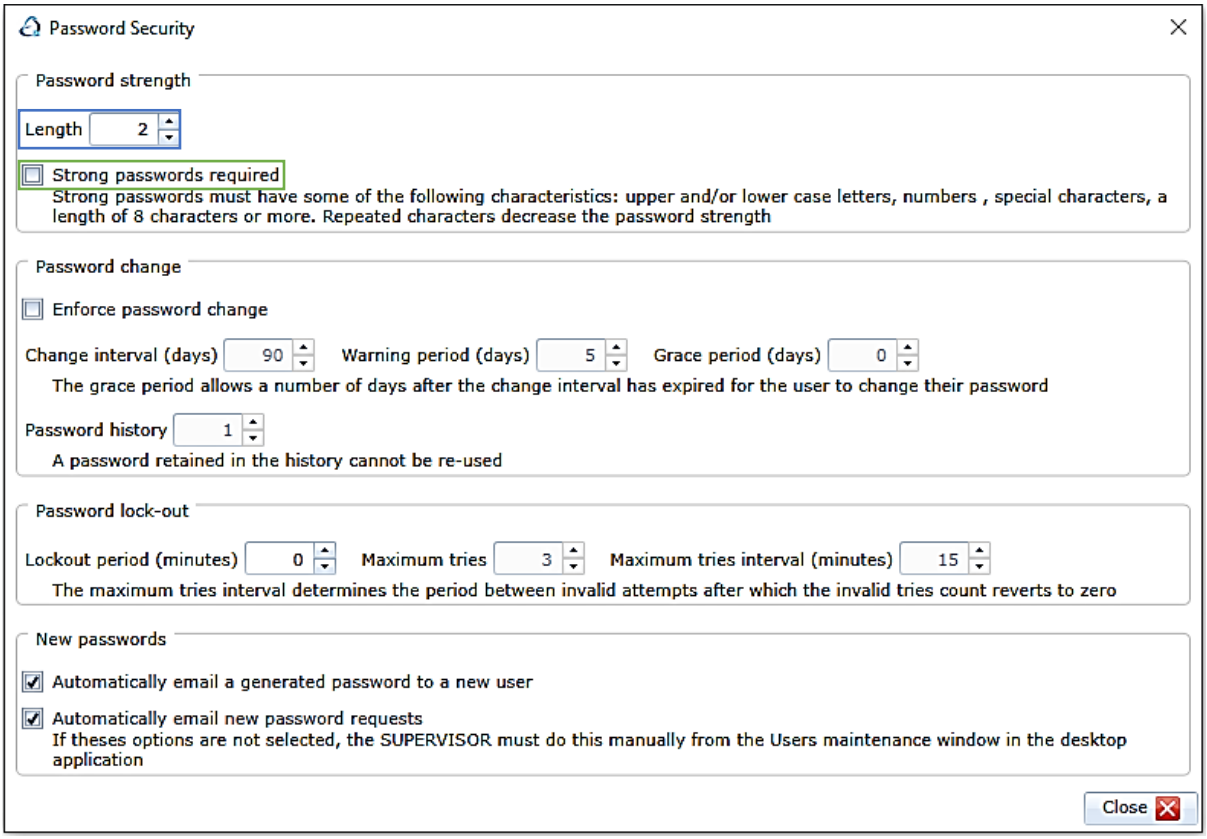


The last option under the *Users & Security* menu is the *Password Security* window. This is where you control how user passwords are handled within Clarity.

The first section is ***Password strength***

The *Length* parameter highlighted in blue below denotes the minimum password length required.

The *Strong passwords required* parameter highlighted in green should be used if you would like to set a minimum security criteria to chosen passwords. The requirements are listed below the parameter.



The second section is ***Password change***.

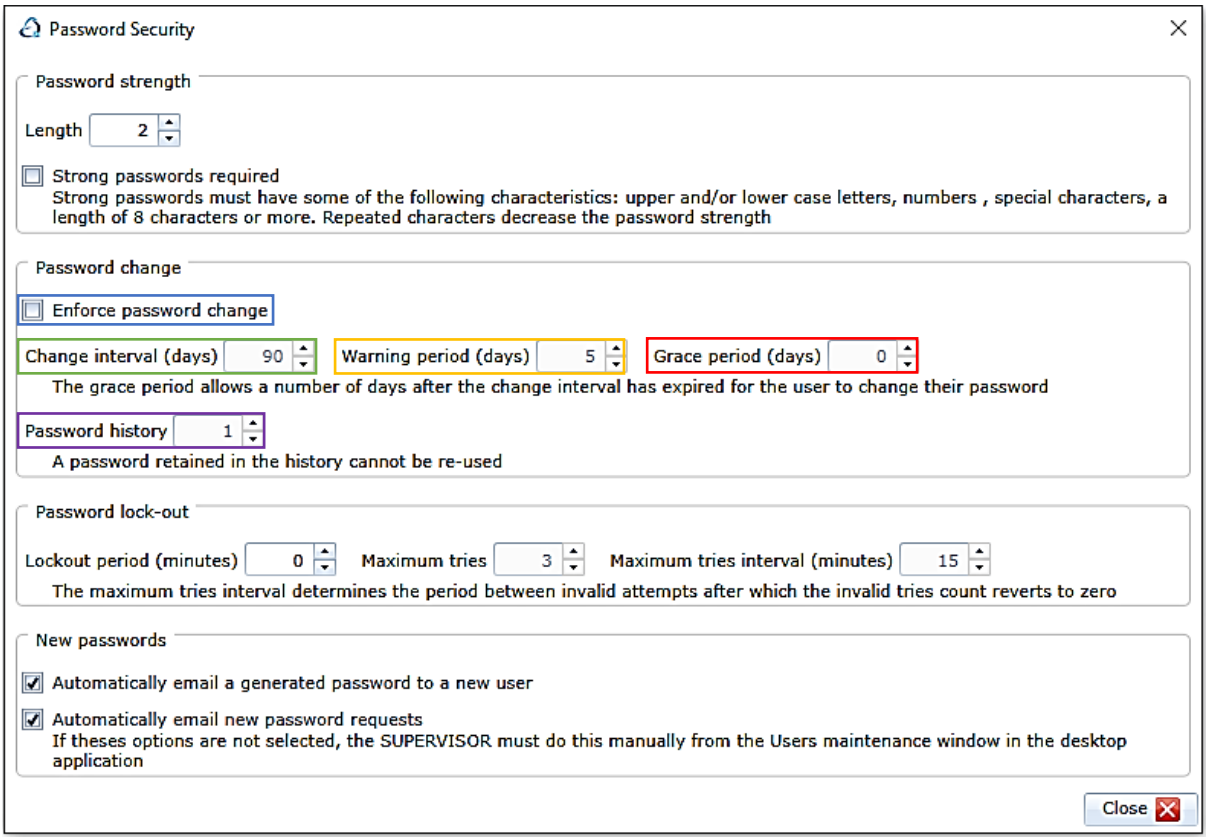
If the *Enforce password change* parameter (highlighted in blue below) is ticked the additional parameters within the *Password change* section come into effect.

The Change interval (days) field highlighted in green denotes how frequently the user will need to change their Clarity password.

The Warning period (days) field highlighted in yellow denotes how many days warning the user will receive before they will need to change their Clarity password.

The Grace period (days) field highlighted in red denotes how many days after the *Change interval* has been breached the user will still be able to login to Clarity using their current password.

The *Password history* field highlighted in purple denotes the number of historic passwords retained that cannot be re-used. *Example – if this value is set to 2 you will be able to re-use the first password entered on the fourth password change interval.*

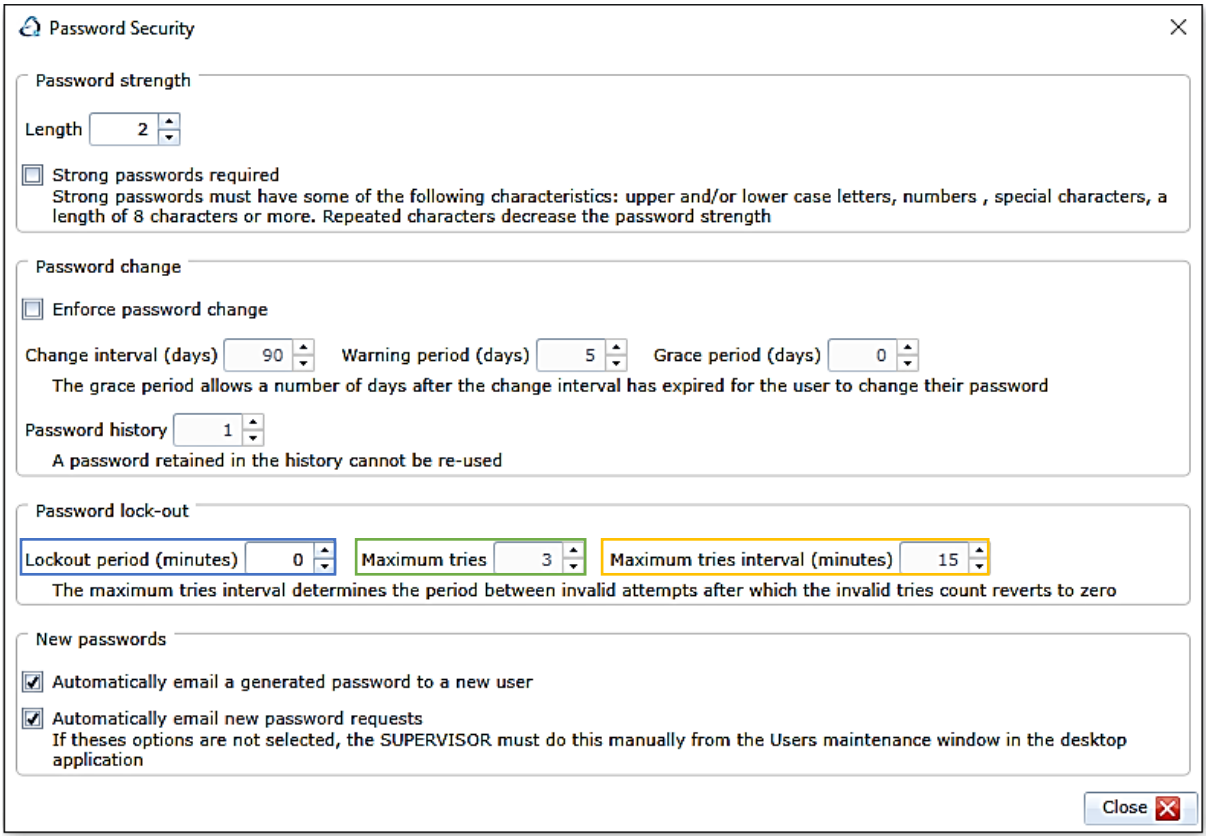


The third section is ***Password lock-out***.

If a value is entered into the *Lockout period (minutes)* field (highlighted in blue below) the user will be locked out of Clarity for that period of time should they exceed the *Maximum tries* value.

The value entered into the *Maximum tries* field (highlighted in green) is the maximum number of times a user can attempt to login unsuccessfully before being locked out.

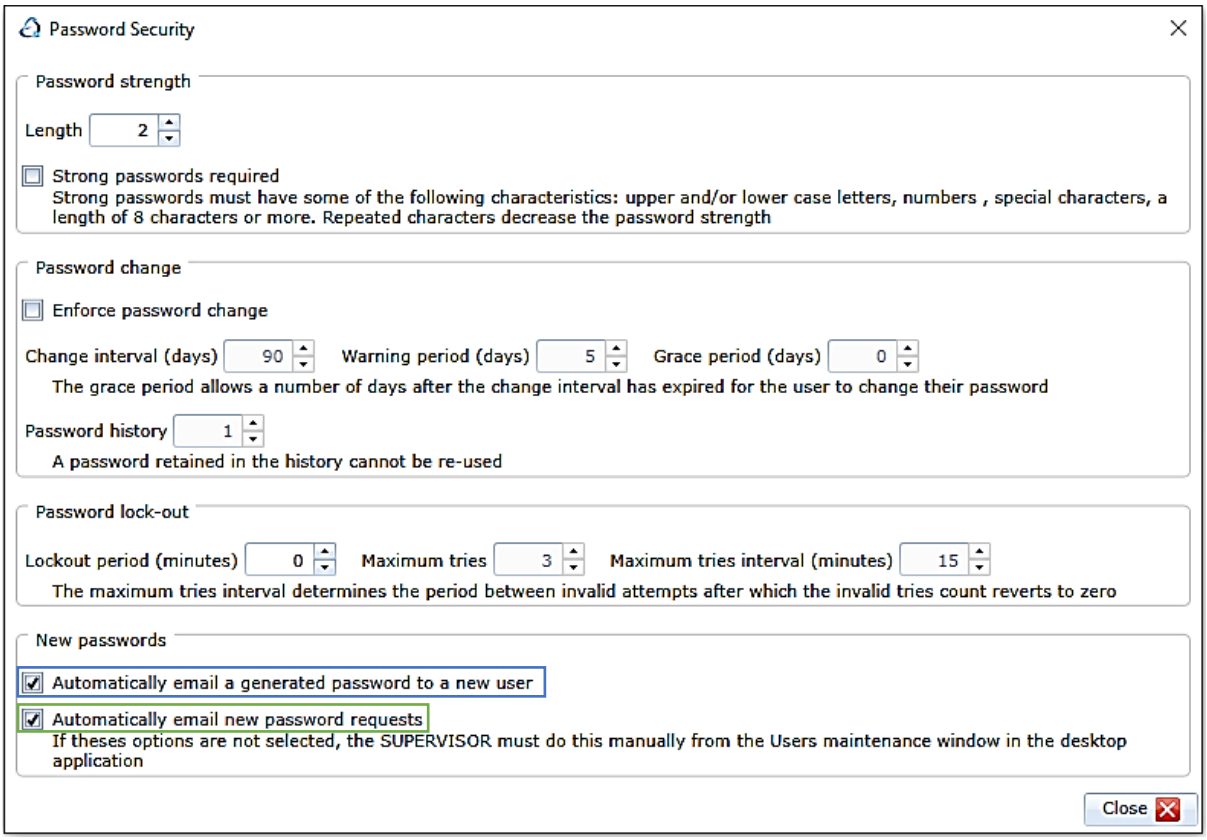
The value entered into the *Maximum tries interval (minutes)* field (highlighted in yellow) is the length of time needed to elapse before a locked out user will be able to reattempt to login.



The final section is ***New passwords***.

If the *Automatically email a generated password to a new user* parameter (highlighted in blue below) is ticked an email containing a temporary password will be sent to the email address defined against that users Clarity profile. Once that new user has logged in for the first time using the emailed temporary password Clarity will prompt the user to change the password.

If the *Automatically email a generated password to a new user* parameter (highlighted in blue below) is not ticked the SUPERVISOR account will need to login into the Dataflow desktop application and reset the password on the users behalf using the Generate New Password button.
By doing so a temporary password will be emailed to the address defined within the user's profile. The user will be prompted to change their password once they have logged in using the emailed temporary password.

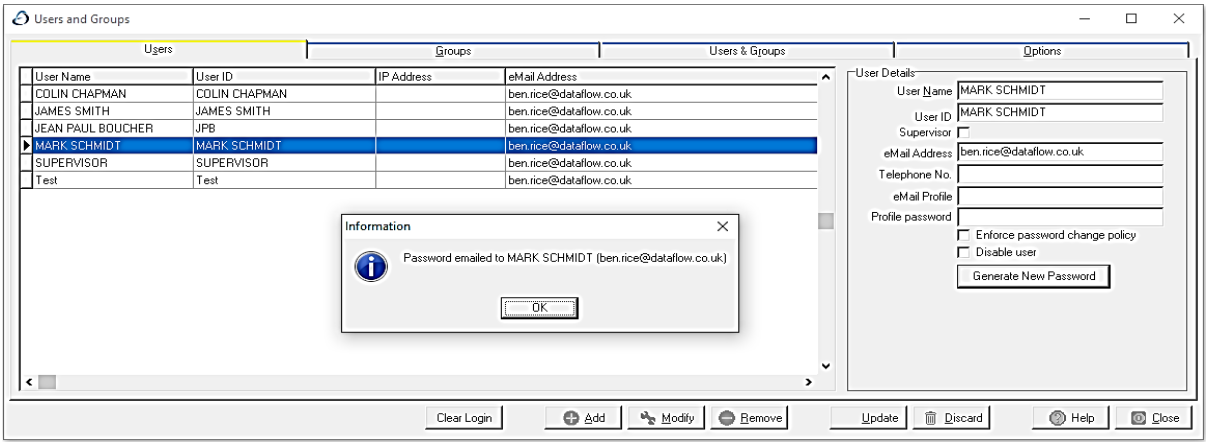


If the *Automatically email new password requests* parameter (highlighted above in green) is ticked an email containing a temporary password will be sent to the email address defined against that users Clarity profile when an existing user has requested a new password. Once that new user has logged in for the first time using the emailed temporary password Clarity will prompt the user to change the password.

If the *Automatically email new password requests* (highlighted above in green) is not ticked the SUPERVISOR account will need to login into the Dataflow desktop application and reset the password on the users behalf using the Generate New Password button.

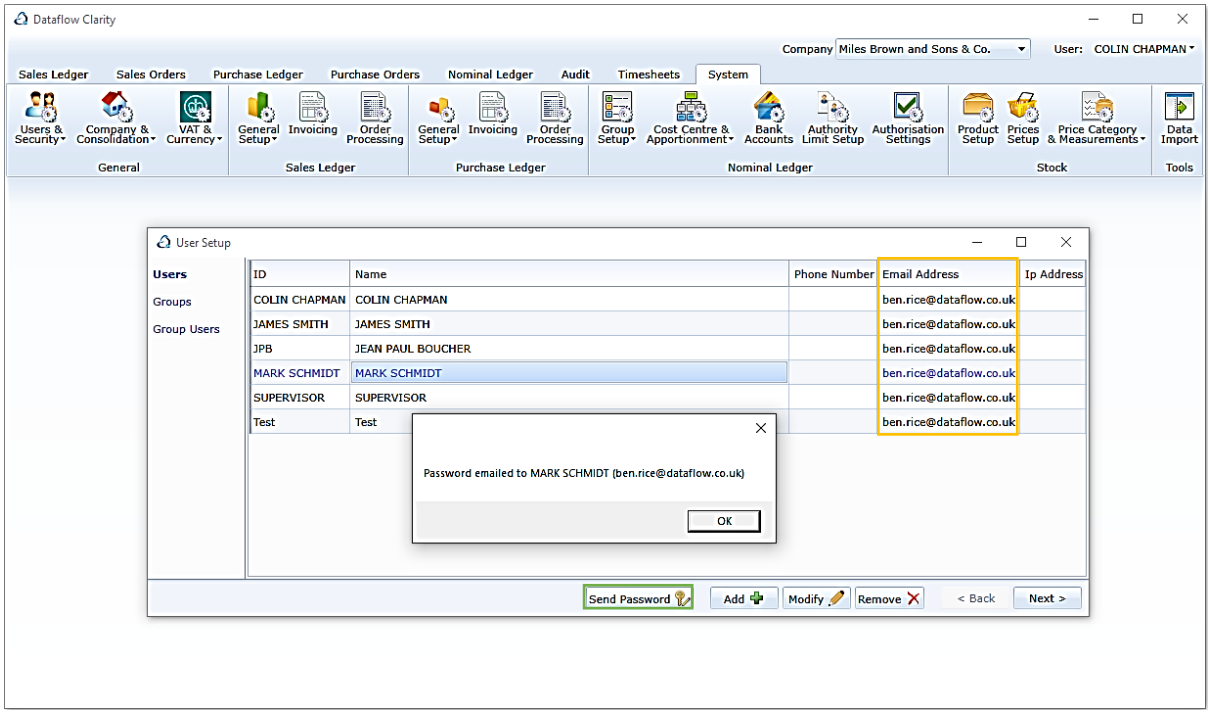
By doing so a temporary password will be emailed to the address defined within the user's profile. The user will be prompted to change their password once they have logged in using the emailed temporary password.

Below is an example image of the Dataflow desktop application *Users and Groups* window containing the *Generate New Password* button.



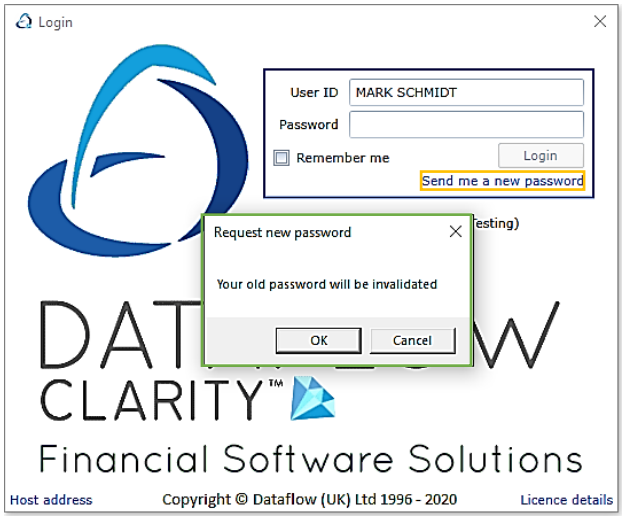
A new password request can be carried out one of two ways. The first is to select that user within the *Users* list and use the Send Password button highlighted green below. Clarity will send a temporary password to the users email address defined within the *Email Address* column (highlighted in yellow below). If the *Automatically email new password requests parameter* is unticked the email will be sent to the email address defined against the SUPERVISOR account.

A confirmation dialogue will be generated when Clarity has sent a new password.

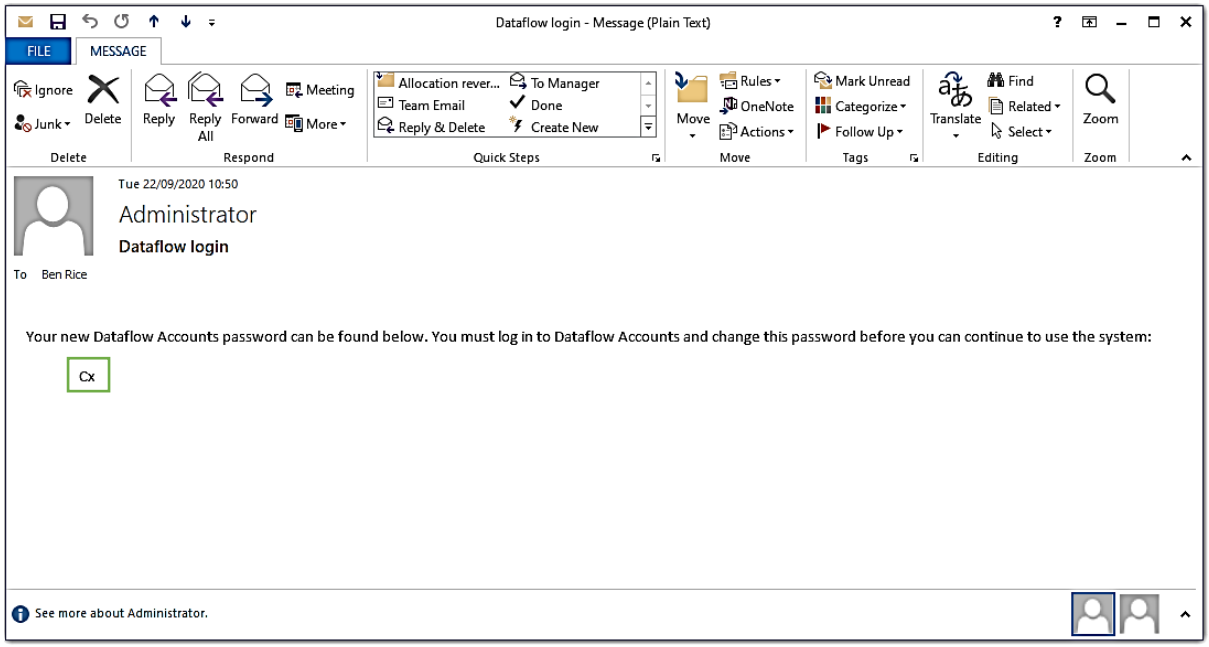


The second option is to use the *Send me a new password* link on the Clarity login window (highlighted in yellow below). As above Clarity will email a temporary password to the users email address defined within the *Email Address* column, unless the *Automatically email new password requests parameter* is unticked, in which case the email will be sent to the email address defined against the SUPERVISOR account.

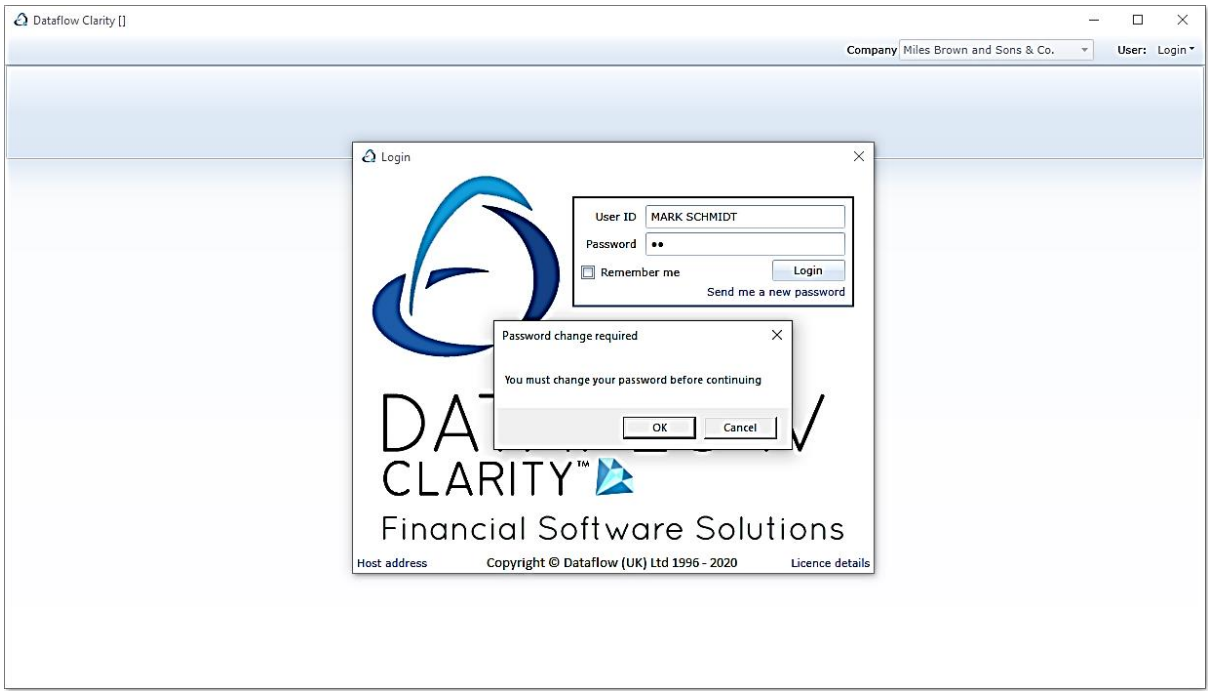
Requesting a new password will invalidate the old password. Clarity will display a confirmation dialogue to that effect (highlighted in green below).



Below is an example of the password request email. The temporary password is highlighted in green below.



The next time Mark Schmidt logs in he'll need to use his user ID and the temporary password that was emailed (highlighted in green above). Once those details have been entered and the Login button clicked Clarity will prompt Mark to change his password.



Clicking OK on the *Password change required* prompt opens a *Change User Password* window.

Enter the emailed temporary password into the *Old password* field (highlighted in green below).
Enter the new password and confirm the password in the field highlighted in blue below.