



## **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).

		$\wedge$	
Dataflow Clarity		$\sim$	– 🗆 ×
		Company Miles Brown and Sor	ns & Co. • User: COLIN CHAPMAN •
Sales Ledger Sales Orders Pu	urchase Ledger Purchase Orders Nominal Ledger	Audit Timesheets System	
Users & Company & VAT & Security* Consolidation* Currency*	General Invoicing Processing Setupy Invoicing Processing	Order rocessing Setup: Apportionment Accounts Limit Setup Apportionment Accounts Limit Setup	Product Prices Price Category Data Import
General	Sales Ledger Purchase Ledge	per Nominal Ledger	Stock Tools
$\land$			

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).

- co	Company & VAT		oicing Order Processing	General Invoicing	Order	Group Setup* A	Cost Centre &	Bank Auth	ority Authorisation P	roduct Prices	Price Category & Measurements *
	General	Sale	s Ledger	Purchase Le	dger		No	ominal Ledger		s	tock
	🙆 User Setup									X	1
	Users	ID	Name					Phone Number	Email Address	Ip Address	
	Groups	COLIN CHAPMAN	COLIN CHAPMAN						ben.rice@dataflow.co.u	k	
	Group Users	JAMES SMITH	JAMES SMITH						ben.rice@dataflow.co.u	k	
		JPB	JEAN PAUL BOUCHER				ben.rice@dataflow.co.u	k			
		MARK SCHMIDT	MARK SCHMIDT						ben.rice@dataflow.co.u	k	
		SUPERVISOR	SUPERVISOR						ben.rice@dataflow.co.u	k	
		Test	Test						ben.rice@dataflow.co.u	k	
					a 10	. @		Martifa 🥖 Dave	e Raak	Nucl. a	

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

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

👌 User Setup									_		1 ×	
Users	ID		Name		Phone Number	Email Address	Ip Address					
Groups	COLIN CH	APMAN	COLIN CH	IAPMAN		ben.rice@dataflow.co.uk						
Group Users	JAMES SM	👌 Us	er						_		×	
	JPB	C Detai	ils									
	MARK SCH											
	SUPERVIS		User Id									
	Test		Name									
		Phone	number									
		Email	address									
		Emai	ling Profile									
		Pro	file									
		Passwo	ord								-1	
		Secu	nty									
		Ent	torce passv sable user	word change	policy							
									ок ⊘	Can	cel 🕢	
	l				Seliu Passw		ioany 🍠 👔	centove A	- 000	-	TICAL 2	

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 I button.

To modify an existing user click on the user group within the list and use the Modify P button. To remove an existing user click on the user group within the list and use the Remove X button.

🙆 User Setup				_		×
Users	Name					
Groups	ACCOUNTS CLERKS					
Group Users	ACCOUNTS MANAGERS					
	AUTH_HIGH					
	AUTH_LOW					
	AUTH_MEDIUM					
	EVERYBODY					
	STOCK DEPARTMENT					
		Add 🖶 🛛 Modify 🥖 Remove	×	< Back	Nex	d >

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.

🙆 User Setup		-		×
Users Groups Group Users	Selected Group ACCOUNTS CLERKS Available Test SUPERVISOR SUPARVISOR SUPARVISOR SUPERVISOR SUPA			
		< Back	Ne:	xt >



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.

<u>Note</u> – 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.

② User Licence Registration	×
Your installation is licensed for 10 users You have currently registered 4 users All COLIN CHAPMAN JAMES SMITH JEAN PAUL BOUCHER MARK SCHMIDT Test	
Filter	<b>×</b>
Cl	ose 🔀



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.

	×
Password strength	
Length 2 - Strong passwords required Strong passwords must have some of the following characteristics: upper and/or lower case letters, numbers, special characters,	а
length of 8 characters or more. Repeated characters decrease the password strength	
Password change	
Enforce password change	
Change interval (days) 90 📩 Warning period (days) 5 🖨 Grace period (days) 0 📩	
The grace period allows a number of days after the change interval has expired for the user to change their password	
Password history	
A password retained in the history cannot be re-used	
Password lock-out	
Lockout period (minutes) 0 📩 Maximum tries 3 🚖 Maximum tries interval (minutes) 15 🛬	
The maximum tries interval determines the period between invalid attempts after which the invalid tries count reverts to zero	
New passwords	
I Automatically email a generated password to a new user	
Automatically email new password requests If theses options are not selected, the SUPERVISOR must do this manually from the Users maintenance window in the desktop application	
Close	X



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 <u>after</u> 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.* 

∂ Password Security ×
Password strength
Length 2 ×
Strong passwords required Strong passwords must have some of the following characteristics: upper and/or lower case letters, numbers, special characters, a length of 8 characters or more. Repeated characters decrease the password strength
Password change
Enforce password change
Change interval (days) 90 + Warning period (days) 5 + Grace period (days) 0 +
The grace period allows a number of days after the change interval has expired for the user to change their password
Password history 1
A password retained in the history cannot be re-used
Password lock-out
Lockout period (minutes) 0 🔹 Maximum tries 3 🔹 Maximum tries interval (minutes) 15 🛓
The maximum tries interval determines the period between invalid attempts after which the invalid tries count reverts to zero
New passwords
Automatically email a generated password to a new user
Automatically email new password requests If theses options are not selected, the SUPERVISOR must do this manually from the Users maintenance window in the desktop application
Close 🔀



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.

∂ Password Security ×
Password strength
Length 2 ×
Strong passwords required Strong passwords must have some of the following characteristics: upper and/or lower case letters, numbers, special characters, a length of 8 characters or more. Repeated characters decrease the password strength
Password change
Enforce password change
Change interval (days) 90 🔹 Warning period (days) 5 🔹 Grace period (days) 0 🔹
The grace period allows a number of days after the change interval has expired for the user to change their password
Password history
A password retained in the history cannot be re-used
Password lock-out
Lockout period (minutes) 0 🗘 Maximum tries 3 🗘 Maximum tries interval (minutes) 15 🗘
The maximum tries interval determines the period between invalid attempts after which the invalid tries count reverts to zero
New passwords
Automatically email a generated password to a new user
Automatically email new password requests If theses options are not selected, the SUPERVISOR must do this manually from the Users maintenance window in the desktop application
Close 🔀



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 <u>not</u> ticked the SUPERVISOR account will need to login into the <u>Dataflow desktop application</u> and reset the password on the users behalf using the <u>Generate New Password</u> 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.

A Password Security
Password strength
Length 2 ×
Strong passwords required Strong passwords must have some of the following characteristics: upper and/or lower case letters, numbers, special characters, a length of 8 characters or more. Repeated characters decrease the password strength
Password change
Enforce password change
Change interval (days) 90 🔹 Warning period (days) 5 🖕 Grace period (days) 0 🛓
The grace period allows a number of days after the change interval has expired for the user to change their password
Password history
A password retained in the history cannot be re-used
Password lock-out
Lockout period (minutes) 0 🔺 Maximum tries 3 🛧 Maximum tries interval (minutes) 15 💂
The maximum tries interval determines the period between invalid attempts after which the invalid tries count reverts to zero
New passwords
Automatically email a generated password to a new user
Automatically email new password requests If theses options are not selected, the SUPERVISOR must do this manually from the Users maintenance window in the desktop application

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 <u>not</u> ticked the SUPERVISOR account will need to login into the <u>Dataflow desktop application</u> and reset the password on the users behalf using the <u>Generate New Password</u> 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 <u>Dataflow desktop application</u> Users and Groups window containing the Generate New Password button.

🗿 Users and Groups						- 🗆 X
Ugers		<u>G</u> roups		Users & Grou	ips	<u>Options</u>
User Name	User ID	IP Address	eMail Address		^	User Details
COLIN CHAPMAN	COLIN CHAPMAN		ben.rice@dataflo	w.co.uk		User Name MARK SCHMIDT
JAMES SMITH	JAMES SMITH		ben.rice@dataflo	w.co.uk		User ID MARK SCHMIDT
JEAN PAUL BOUCHER	JPB		ben.rice@dataflo	w.co.uk		Supervisor
MARK SCHMIDT	MARK SCHMIDT		ben.rice@dataflo	w.co.uk		eMail Address ben rice@dataflow.co.uk
SUPERVISOR	SUPERVISOR		ben.rice@dataflo	w.co.uk		Telephone Ne
Test	Test		ben.rice@dataflo	w.co.uk		Telephone No.
<		Password emaile	ed to MARK SCHMIDT	X (ben.rice@dataflow.co.uk)	*	Profile password Enforce password change policy Disable user Generate New Password
			1	1. E	_	E E E E E
		Clear Log	in 🕒 🗛	dd 🏻 🗞 Modify 💭 Bemov	/e	Update 🗎 Discard 💿 Help 💿 Close

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 v 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 <u>unticked</u> 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.



Sales Ledo	w Clarity	Orders Pur	chase Ledoer Pur	chase Orde	rs Nominal Ledger Audi	t Timesheets Syste	c	Company Miles E	rown and Sor	ns & Co.	▼ User: 0		× PMAN
Users & Security*	Company 8 Consolidation	VAT & VAT &	General Invoicing	Order Processing	General Invoicing Order Processing	Group Setup Apportionment	Bank	Authority s Limit Setup	Authorisation Settings	Product Pr Setup Se	ices Price C a Measur	ategory rements •	Data Import
	General		Sales Ledge	r	Purchase Ledger	N	lominal Le	dger			Stock		Tools
		O User Setup	1							- (	- ×		
		Users	ID	Name				Phone Number	Email Addre	ss	Ip Address		
		Groups	COLIN CHAPMAN	COLIN CH	IAPMAN				ben.rice@da	taflow.co.uk			
		Group Users	JAMES SMITH	JAMES SM	1ITH				ben.rice@da	taflow.co.uk			
			ЈРВ	JEAN PAU	L BOUCHER				ben.rice@da	taflow.co.uk			
			MARK SCHMIDT	MARK SCI	HMIDT				ben.rice@da	taflow.co.uk			
			SUPERVISOR	SUPERVIS	SOR				ben.rice@da	taflow.co.uk			
				Test	Password emailed to MARK SCHM	AIDT (ben.rice@dataflow.co.u			Denneegen				
						Send Password 论 🛛 Ad	id 🖶	Modify 🥖 Rer	nove 🗙	< Back	Next >		

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 <u>unticked</u>, 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.

	Dataflow login - Message (Plain Text)	? 🗹 – 🗆 🗙
Image: Second Image: Second   Image: Second Image: Second	Allocation rever  G To Manager Team Email Create New Outlet Steps Outlet Steps Outlet Steps	Mark Unread Categorize → Follow Up → Taas 5 Follow Up → Follow Up →
To Ben Rice Your new Dataflow Accounts password can be four	nd below. You must log in to Dataflow Accounts and change this passw	rord before γou can continue to use the system:
See more about Administrator.		

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.

Dataflow Clarity [] □	×
Dataflow Clenty []  Company Miles Brown and Sons & Co.  User: L  Company Miles Brown and Sons & Co.  User: L  User: ID  User: I	×



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.

Dataflow Clarity []	Company Miles Brown and Sons & Co.	*	User:	× Login •
	Login X User ID MARK SCHIIIDT Password • Remember me Login Send me a new password Vid password Vid password View password CLARITY Financial Software Solutions Host address Copyright © Dataflow (UK) Ltd 1996-2020 Licence details			