DataApex
Clarity™
CHROMATOGRAPHY SOFTWARE

REGULATED ENVIRONMENT

Clarity Software ENG

Code/Rev.: M132/90B
Date: 2024-02-14

DataApex Ltd.
Petrzilkova 2583/13
158 00 Prague 5
Czech Republic

Phone: +420 251 013 400
clarity@dataapex.com
www.dataapex.com

Author: JaKa

Contents

To facilitate the orientation in the **Regulated Environment** manual and **Clarity** chromatography station, different fonts are used throughout the manual. Meanings of these fonts are:

Open File (italics) describes the commands and names of fields in **Clarity**, parameters that can be entered into them or a window or dialog name.
WORK1 (capitals) indicates the name of the file and/or directory.
ACTIVE (capital italics) marks the state of the station or its part.
Chromatogram (blue underlined) marks clickable links referring to related chapters.

The bold text is sometimes also used for important parts of the text and the name of the **Clarity** station. Moreover, some sections are written in format other than normal text. These sections are formatted as follows:

Note: Notifies the reader of relevant information.

Caution: Warns the user of possibly dangerous or very important information.

Marks the problem statement or trouble question.

Description: Presents more detailed information on the problem, describes its causes, etc.

Solution: Marks the response to the question, presents a procedure how to remove it.

1 What is a Regulated Environment

A regulated environment is basically any controlled environment. Rules state which conditions must be met by a company to produce valid results or goods of a guaranteed level of quality.

Note: In other words, to comply with any regulated environment means to ensure that any operation with the data can be later reproduced. **Clarity** regards the following types of documents as data: chromatograms (*.PRM), calibrations (*.CAL) and sequences (*.SEQ). Thus, in **Clarity**, these files include their own audit trail log and, moreover, the chromatogram files are saved with their history.

The regulations set for the working environment may come from several sources, for example the company itself, government agencies and institutions (like the American FDA) or regulatory bodies and other groups with an interest in ensuring product standardization. When a company is to produce results or goods for the public which are going to be generally credible or of guaranteed quality, it should abide by the rules set on such processes by the given country's authorities.

This manual was established to help the users of **Clarity** software to achieve compliance with those rules, which are issued for selected type of regulated environment.

1.1 Good Laboratory Practice

Good Laboratory Practice (GLP) embodies a set of principles defined by OECD and implemented by national authorities that provides a framework within which laboratory studies are planned, performed, monitored, recorded, reported and archived. These studies are undertaken to generate data by which the hazards and risks to users, consumers and third parties or the environment, can be assessed for pharmaceuticals (only preclinical studies), agrochemicals, cosmetics, food additives, feed additives and contaminants, novel foods, biocides, detergents, etc. GLP helps assure regulatory authorities that the data submitted are a true reflection of the results obtained during the study and can therefore be relied on when making risk or safety assessments.

1.2 CFR 21 Part 11

CFR 21 Part 11 is the directive issued by the United States of America Federal Drug Administration agency (FDA). It specifies conditions which must be met when an organization intends to submit or store documents required by the FDA in the form of electronic records, instead in the traditional paper form. The major concerns of this code are related to the nature of electronic records, with respect to their reliability compared to paper form documents.

The major issues are:

- System Validation
- Access to the records limited to authorized personnel only

- Documentation (Audit trail) of all modifications of the records
- Electronic signatures

A compliance with the directive can be achieved only by combination of the respective software capabilities, overall system settings and use of standard operational procedures as defined by the organization.

2 How to set Clarity

The process of setting the **Clarity** chromatography station to regulated environment conditions involves following steps:

- Selecting correct computer and installing correct operating system - see the chapter **"Computer installation"** on pg. **3**.
- Installing **Clarity** - see the chapter **"Installing Clarity"** on pg. **4**.
- Setting up the respective user accounts with appropriate privileges on the computer operating level - see the chapter **"Computer User Rights"** on pg. **11**.
- Setting **Clarity** to comply with the specific regulated environment requirements - see the chapter **"Specific settings"** on pg. **5**. and the chapter **"User Accounts in Clarity"** on pg. **23**.

2.1 Computer installation

The requirements in the hardware configuration of the computer system change with the continuing development of **Clarity**. The version specific requirements may be found in the **D016-Clarity-Compatibility-Table** datasheet (which is saved on the **Clarity** installation USB) or are available on the **DataApex website** .

To be able to work in a regulated environment, an operating system which supports file access restrictions based on individual user accounts is also needed. Take care in selecting the system, as some modifications of various operating systems don't support this function; for example **Microsoft Windows 7 Home** doesn't allow personalized file access restrictions, while **Microsoft Windows 7 Professional** does. Operating systems supporting the regulated environment in **Clarity** are:

- Microsoft Windows 7 - Professional, Ultimate*
- Microsoft Windows 8.1 - Pro, Enterprise*
- Microsoft Windows 10 - Pro, Enterprise*
- Microsoft Windows 11 - Pro, Enterprise*

** the systems marked with an asterisk support personalized file access, but have not been tested with **Clarity***

Note: All setup/installation procedures following this note are described for **Window 11 Pro**. Procedure is similar on other operating systems, but there might be slight differences.

During the computer installation, follow the these steps (if possible):

- Install the operating system on the computer.
- Install the available service packs and updates for the operating system.
- Set the user accounts that will be needed on the computer (for more details see the chapter **"Computer User Rights"** on pg. **11**.).
- Install any other software required on the computer, along with its service

packs and updates.

- Install **Clarity** (see the chapter **"Installing Clarity"** on pg. **4**.).

2.2 Installing Clarity

Note: If you want to update to a newer version, it is recommended to first uninstall the current version of **Clarity** on your PC. The uninstallation is offered automatically upon the start of new version's installation.

The process of installing **Clarity** to comply with regulated environment rules is as follows:

- Check whether the package for the **Clarity** installation is complete, eg. its content matches the packing list.

Caution: Do not plug in any hardware yet!

- Plug in the **Clarity** installation USB into the computer. Search for removable disc in the file explorer (e.g. My Computer in windows) and run the INSTALL.EXE file located in the root directory.
- On the first screen, select the directory for the installation (C:\CLARITY by default), click the *Next* button, select the directory for data location and click the *Next* button again.
- Enter the *User code*. This code may be found on the back side of the card provided with **installation USB** or is provided by **DataApex** by e-mail, click the *Next* button to continue.
- Set the type of the installation on the next screen (or select the particular installation components in the bottom pane) and click the *Next* button.
- Select the name of the folder in the **Windows** *Start* menu where various **Clarity** shortcuts will be placed. Alternatively, it is possible to prevent the creation of the folder in the *Start* menu. Then press the *Install* button.

Caution: In case **Clarity** wasn't supplied with a user code, it can be run in the Trial mode. In that case, do not enter anything in the *User code* field.

- If this is the first installation on given PC, installation of drivers for various hardware needs to be confirmed.
- Click the *Next* button in the next dialog. From the listed options, check the *Make IQ Report now* checkbox and press the *Finish* button.
- The IQ report will emerge. If it is marked as passed (green label below the first table in the report), it means that **Clarity** was successfully installed.

Caution: It is recommended to run **Clarity** before printing the final form of IQ since some information is only loaded after the first start.

Note: Sometimes, the IQ report will fail. This happens mainly when older versions of **Clarity** are installed in other directories on the computer. When this situation arises, we recommend uninstalling the **Clarity**, deleting the directory it was installed to (take care to save the data prior to the deletion if you are only re-installing) and installing the **Clarity** again. If the IQ report fails again, please report the problem to your local distributor.

- Insert the HW key into the USB slot.
- Connect any other HW.

2.3 Specific settings

Each regulated environment has its own set of rules which have to be abided by, but in most cases these rules are very similar to rules in any other system. This chapter lists the requirements for particular regulated environment systems with references to Standard Operation Procedures (SOP's) that should be followed to fulfill the mentioned requirement.

2.3.1 21 CFR Part 11 - requirements

The commented **21 CFR Part 11** requirements for **Clarity** may be found in the D019-CLARITY-21CFR11.PDF datasheet available on the **DataApex** website. For the majority of requirements set by the **21 CFR Part 11** regulation the conditions must first be set at the company level. However, the following list of articles belonging to the **21 CFR Part 11** regulation is supplied by **Clarity** (some fully, some only in part) and necessary setup is fully described in this manual.

2.3.1.1 Mandatory

- § 11.10 a, § 11.10 i - **Clarity** software must be validated. This is accomplished by the **DataApex** Quality Assurance system, see the D028-ISO9001-DATAAPEX-CERT.PDF datasheet available on the **DataApex** website, and the verification that the software was successfully installed provided by the IQ report, see the chapter **"Installing Clarity"** on pg. **4**.
- § 11.10 c - You must ensure that the data is stored and can be retrieved during the whole records retention period - see the chapter **"Archiving the data"** on pg. **30**.
- § 11.10 d, § 11.10 g - System access must be limited to authorized individuals - see the chapter **"Computer User Rights"** on pg. **11**. and the chapter **"User Accounts in Clarity"** on pg. **23**.
- § 11.10 e - Any action performed in the **Clarity** system must be recorded in secure Audit trail - see the chapter **"Logging of all changes"** on pg. **29**.
- § 11.50, §11.70, § 11.100 - It must be possible to sign electronic data in the **Clarity** with electronic signatures that are unique to each individual, will not be reused by, or reassigned to, anyone else and cannot be manipulated - see the chapter **"Electronic signatures"** on pg. **36**.the chapter **"Logging of all changes"** on pg. **29**.

- § 11.200 a - Any access or signature must be performed based on two distinct identification components - see the chapter **"Clarity GLP Options settings"** on pg. **8**. and the chapter **"Electronic signatures"** on pg. **36**.the chapter **"Logging of all changes"** on pg. **29**.
- § 11.300 - Any security code / password pair must be unique to a single user. Moreover, each password must be periodically checked and revised - see the chapter **"User Accounts in Clarity"** on pg. **23**.

2.3.2 GLP – requirements

Some of these requirements are mandatory in order to comply with the **GLP**, others are required only when some special features in **Clarity** or special conditions in the company should be satisfied. The steps in the following list are divided into mandatory and optional. Each requirement then links to a corresponding section in the next chapter that includes the general guide for solving the requirement and particular SOP.

2.3.2.1 Mandatory

- The computer in which **Clarity** is installed must operate under the conditions where every user has their own defined rights - see the chapter **"Computer User Rights"** on pg. **11**.
- File overwriting in **Clarity** must be disabled. Data loss caused by this or any similar reason can not be allowed - see *Note* section in the chapter **"Computer User Rights"** on pg. **11**.
- Every user who has access to **Clarity** must have their own user account with his/her own secret password and access rights defining which actions he/she can perform - see the chapter **"User Accounts in Clarity"** on pg. **23**.
- Every change in the data must be properly logged - see the chapter **"Logging of all changes"** on pg. **29**.
  - The reason for the change must be logged, along with the change itself, so that the reason for the change can be found later - see the chapter **"Logging reasons of changes"** on pg. **29**.
- All data must be archived for the period specified by appropriate authorities - see the chapter **"Archiving the data"** on pg. **30**.

Caution: In order to maintain good Data Integrity the staff who runs **Clarity** (typically laboratory staff) **mustn't** have any privileges to change Windows System Time on the computer where **Clarity** is operated. If this condition is not fulfilled it can easily jeopardize correctness and integrity of the timestamps in *Audit Trail* because they are recorded as current Windows System Time in the moment of any action performed.

2.3.2.2 Optional

- When Quality Control/Quality Assessment workers are present – Quality Assurance Personnel should have their own access to the **Clarity** station, without the authorization to change any data - see the chapter **"SOP - User**

Accounts - setup QA account" on pg. **27**.

- When user calculations are used – all users must have the same settings in the user calculation columns - see the chapter **"Shared desktop file"** on pg. **33**.
- Multistation environment – when the user (or several users) is supposed to work on several computers, the user accounts for all users (along with stored passwords) should be the same for all users everywhere - see the chapter **"Multistation environment"** on pg. **35**.

3 Solutions and SOP's

This chapter lists a set of solutions for particular regulated environment problems and Standard Operation Procedures (SOP) which should lead to meeting the requirements of the given regulated environment platform. The SOP's should be abided to the letter and fulfilled in the order recommended by the given platform's section in the chapter **"How to set Clarity"** on pg. **3**.

3.1 Clarity GLP Options settings

This step is taken to apply the basic regulated environment settings to **Clarity**. By default, all regulated environment options in the **Clarity** station are disabled. The selections for compliance are voluntary because some users might not need the regulated environment as a whole and setting the station to the regulated environment conditions would only complicate and slow down their work.

3.1.1 SOP - GLP Options settings

To set **Clarity** to the regulated environment basic conditions, perform the following steps:

Note: If the station is already set to the user account mode, only the user with *Administrator* access can open the *GLP Options* dialog.

- Open the **Clarity** station. In the main *Clarity* window, use the *System – GLP Options...* command to enter the *GLP Options* dialog.

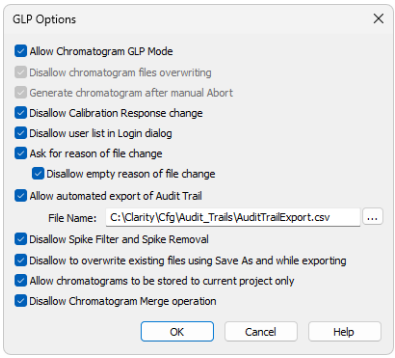


Fig. 1: GLP Options

- To prevent the loss of any data from chromatograms, check the *Allow Chromatogram GLP Mode* checkbox. This will both cancel the possibility of overwriting a chromatogram if a file with the same name already exists in the selected directory (a 6-digit number is added at the end of the new filename) and will cause the generation of the chromatogram if the analysis is aborted for any reason. This feature is required by **21 CFR Part 11** and **GLP**,

therefore files overwriting must be disabled and possible data loss caused by this or any similar reason is disabled.

Note: If you open a chromatogram created in *GLP Mode* in *Clarity* without enabled *GLP Mode*, it will be always opened as read-only.

- To prevent any manual changes in the response in the *Calibration* window use the *Disallow Calibration Response Change* checkbox. The manual change is marked in the *Calibration Audit Trail*, but it breaks the link between the calibration standard and the calibration itself and is not recognizable in the chromatogram linked to the calibration file. This feature is required by **21 CFR Part 11** and **GLP**.
- To disable the display of all available **User Names** in the *Login* dialog, check the *Disallow User List in Login Dialog* checkbox. The user is then required to enter two unique identification components to successfully log in. This feature is required by **21 CFR Part 11**.
- To set **Clarity** to prompt users to fill in the reason for a change, check the *Ask for Reason of File Change* checkbox. When saving or modifying a chromatogram, method, sequence, calibration or GPC calibration file or another **Clarity** settings such as (*System Configuration* or *User Accounts*), the *Reason for Chromatogram (Method, Sequence, ...) Change* dialog will appear. The user can fill in the reason for the change.

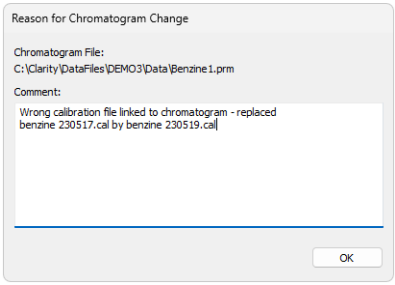


Fig. 2: Reason for Chromatogram Change

GLP requires the reason for a change to be filled in for each change. To ensure that the reason field is not left empty, check the *Disallow Empty Reason of File Change* checkbox in the *GLP Options* dialog. Only reasons with some text in them are now valid. This feature is required by **21 CFR Part 11** and **GLP**.

Note: The reasons for changes are displayed in the **Audit Trails**, separated by a dash from the „file has been saved“ event.

- To automatically export the audit trail, check the *Allow Automated Export of Audit Trail* checkbox. Exported file will be marked as read-only for as long as **Clarity** is open. Changes to this export file will be made continuously. This feature is not required by any regulated environment platform, but may help

QA personnel representatives to check the audit trails without the need to give them access to **Clarity** itself.

- To disallow *Spike Filter* and *Spike Removal* operations, which can significantly change the signal line, check the *Disallow Spike Filter and Spike Removal* checkbox. The usage of these parameters is of course logged into the audit trail and also visible from the Integration table, but as these change the signal (possibly removing peaks in the chromatogram), it might be better to disallow them.
- To prohibit users from overwriting existing files, check the *Disallow to overwrite existing files using Save As and while exporting* checkbox. This feature applies to any file (methods, calibrations, chromatograms, etc.) created by **Clarity**. Warning message pops up and the user must save it under a different filename.
- Option *Allow Chromatograms to Be Stored to Current Project Only* is tool which disables to store any newly generated chromatogram outside of working subfolders (typically *Data* or *Calib*) of current *Project*. This option disables storing any newly generated chromatogram directly into root of current project. It also disables automated creating of new subfolders directly in root of current project. It will allow to store any newly generated chromatogram within one of working subfolders (typically *Data* or *Calib*) of current project. This feature is intended as support of data integrity because it will disallow creating data in destinations where might not be applied measures described in the chapter **"Computer User Rights"** on pg. **11**. Detailed description of this feature is given in *GLP Options* topic of **Clarity** Help.
- *Disallow Chromatogram Merge operation* disables *Merge* fuction which can normally be used to merge multiple chromatograms into a new single file.

3.2 Computer User Rights

The computer on which **Clarity** is installed must operate under the conditions where every user has their own defined rights.

These settings may only be set by the system administrator, preferably during the installation of the computer. This feature is required by **21 CFR Part 11** and **GLP**. Here are some general recommendations on the computer system:

Note: These are not given in the way of comprehensive SOP applicable on every computer, as the computer system and general company conditions on this field may differ widely. However, the SOP provided was tested to work on four selected computer operation systems - **Windows 7 Professional**, **Windows 8.1 Pro**, **Windows 10 Pro** and **Windows 11 Pro**.

- The computer where **Clarity** will be run must use only user accounts with specifically set user privileges that is described in the following subheads of this chapter. The user account with administrator privileges should be reserved for the company IT personnel who mustn't be involved in creation of electronic records by **Clarity**. The reasoning of these specific settings is described in the *Note* below this section.
- Each **Clarity** user must have it's own user account on the operating system.
- All of these user accounts for **Clarity** users must have set privileges for **Cfg**, **DataFiles**, and **Bin** subfolders in **Clarity** folder. If default name of the subfolder **DataFiles** in **Clarity** folder is changed or the this folder is located outside **Clarity** folder (for example on a regularly backed up network drive), the user privileges have to be set in the same manner as in case of default name or location of this subfolder. The modification of the location of **DataFiles** folder, where the data created by **Clarity** will be stored, can be set from *Directories...* item in the *System* Menu, which is accessible from the **Clarity** *Main window*.
- The data created by users of **Clarity** must not be stored in **Bin** subfolder.

Note: This whole process will ensure that the computer user or users will not be able to alter or delete any data created by **Clarity** outside **Clarity** environment. The only way how to modify the data is doing that from the **Clarity** environment, where operations are logged. As local IT personnel must have Administrator privileges they still have privileges to modify or delete data outside **Clarity** environment and without any logging by **Clarity** audit trails therefore there must be established different kind of protection to prevent any potential mistakes or missuses of local IT personnel. Local IT department and all other personnel and management (such as QC, QA etc.) must be aware of this fact.

3.2.1 SOP - Setting the user rights in Windows 11

Note: This SOP was prepared and tested on the computer with **Windows 11 Pro** operating system (English localization), with the latest updates (as of 16.12.2022) installed.

The whole process described in this walk through has to be performed by a person who has the system *Administrator* rights (for example a company IT worker). It assumes that the computer is freshly installed with no user accounts other than the administrator one. **Clarity** is supposed to be already installed. In case that user accounts are already present, (for example computer is connected to domain with domain user accounts), the IT worker performing following steps needs to apply following procedure to already existing user accounts.

- Open the *Computer Management* window, navigate mouse cursor over the *Windows* icon of the *Windows Start Menu* and click right mouse button to invoke context menu and select *Computer Management* item. The *Computer Management* window will open. Navigate to item *Users* available under *Local Users and Groups* item.

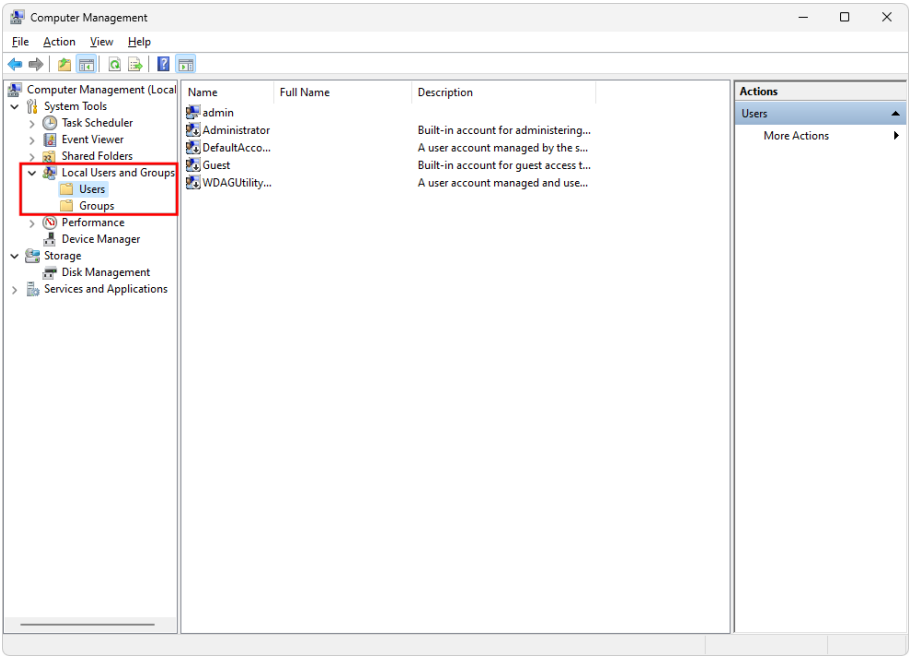


Fig. 3: Computer Management

- Create a new computer user:

- Click on *Action* command (or invoke context menu using right mouse button) and select *New User...*. Fill in all empty fields in the *New User* dialog set password and its setting based on policy of the organization where **Clarity** is installed and click *Create* button.

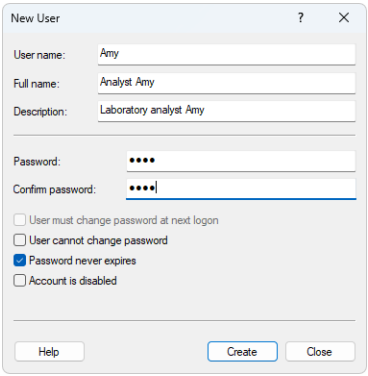


Fig. 4: Create New User

- Repeat this procedure for each additional user you want to add.

- Create a group for all user accounts that will use Clarity

Note: It is not necessary to create a group for the users. It is recommended to do so if there are multiple users that are going to work with Clarity, but it is always possible to set necessary access rights directly for user accounts.

- Creating group is similar to user creation. Navigate to *Groups* available under *Local Users and Groups* section.
- Use *Action - New Group* name it and add description. Then click *Add* to manage members.

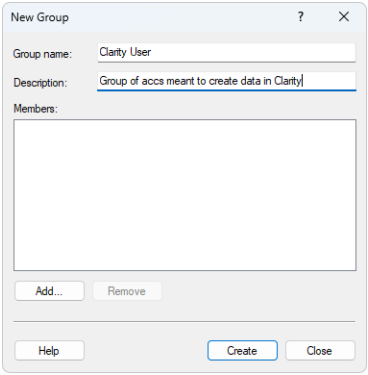


Fig. 5: Users Group

- Click *Advanced* in *Select Users* dialog. *Select User (Advanced)* dialog is opened.
- Click *Find Now* and select all users you want to add from *Search results:* list at the bottom of the dialog.
- You can check which users are members of the group in the group properties.

- Then it is necessary, to perform first login for all newly created users. This step is compulsory and must be performed in this stage and not later. Performing the logging later may compromise all settings performed later and threaten the "electronic" security of all records created by Clarity.

Note: During the first login, the newly created users are automatically added to the *Authenticated User* group which is done by the operating system by default. In order for Clarity to function under GLP, the *Authenticated User* must not have access to Clarity subfolders and thus this group must be deleted (which is explained in the steps below).

- Then local *Administrator* with administrator privileges has to login on the operating system and continue with following steps.
- Find the directory where **Clarity** is installed using. If **DataFiles** subfolder is meant to be located outside of its default place, check that the it is properly setup by using *System Directories* in Clarity.
- Change the privileges for the user accounts you added earlier for the subfolders **Cfg**, **DataFiles** (wherever **DataFiles** subfolder is located) and **Bin**:
  - Right-click on the subfolder **Cfg** and select the *Properties* command from the context menu.
  - Switch to the *Security* tab.
  - Select *Advanced* and window *Advanced Security Settings for Cfg* opens.

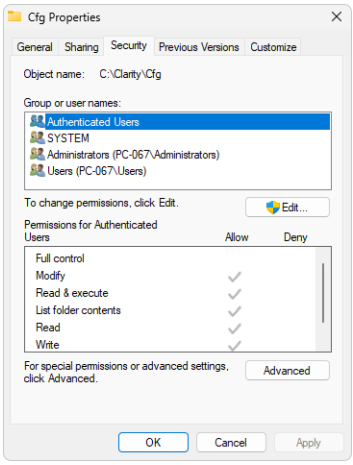


Fig. 6: Cfg Folder Security Properties

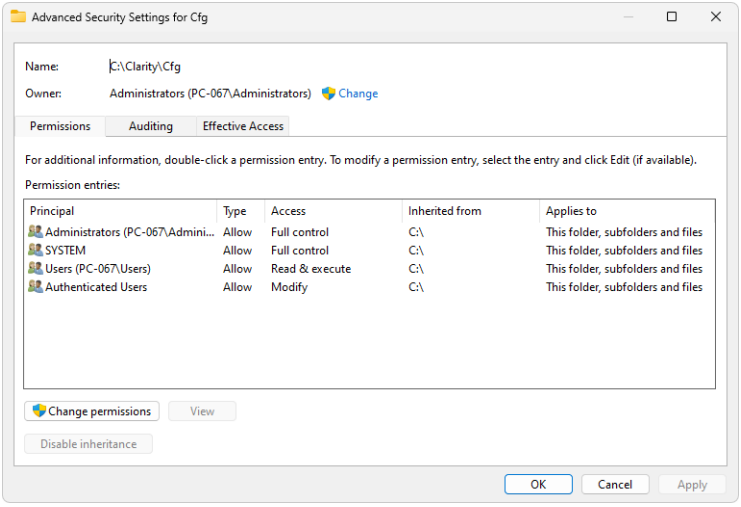


Fig. 7: Advanced Security Settings - Initial state

- Click *Change permissions* button which will invoke new window for settings of permissions. Click *Disable inheritance* button and new *Block inheritance* window will be invoked. Click *Remove all inherited permissions from this object* option which will result in cleared out Permission entry in *Advanced Security Settings for Cfg* window.

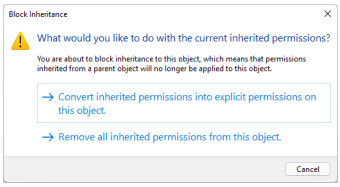


Fig. 8: Block inheritance

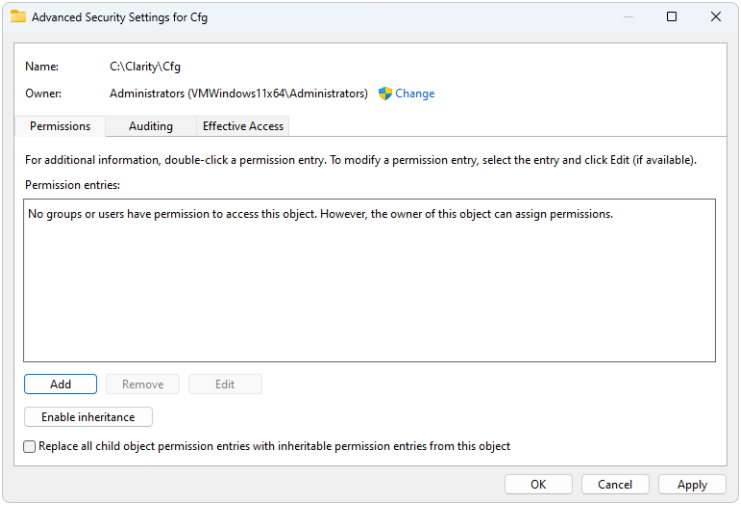


Fig. 9: Advanced Security Settings - No Entry

- Click the *Add* button which will invoke new window for settings of the permissions. Ćlick *Select a principal* to open *Select User or Group* dialog.

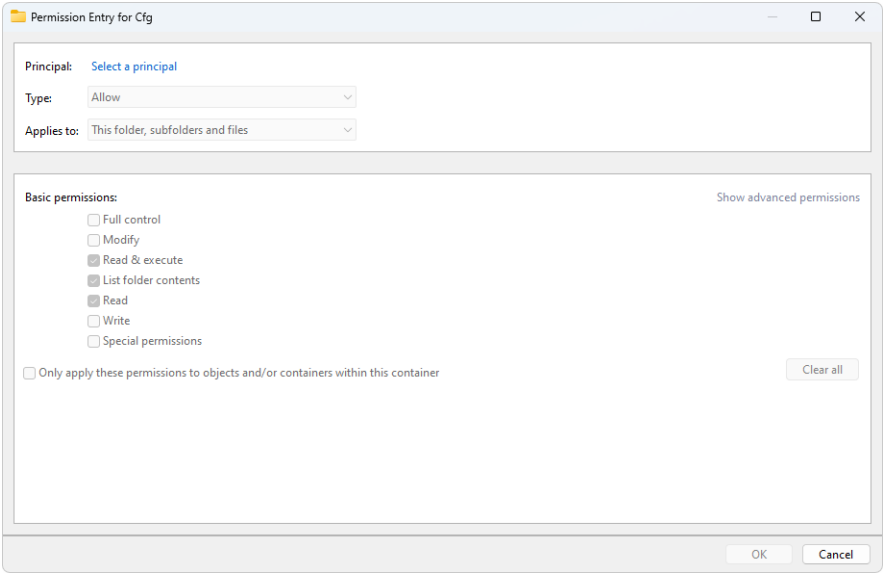


Fig. 10: Permission Entry

- Click the *Advanced...* to open advanced dialog view.

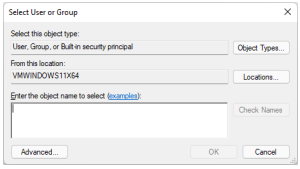


Fig. 11: Select User - Initial

- Click *Find Now* and select the group you created for Clarity users. If you didn't create any select individual accounts.
- Click *OK* in the *Select User of Group (Advanced)* and *Select User of Group* dialogs.

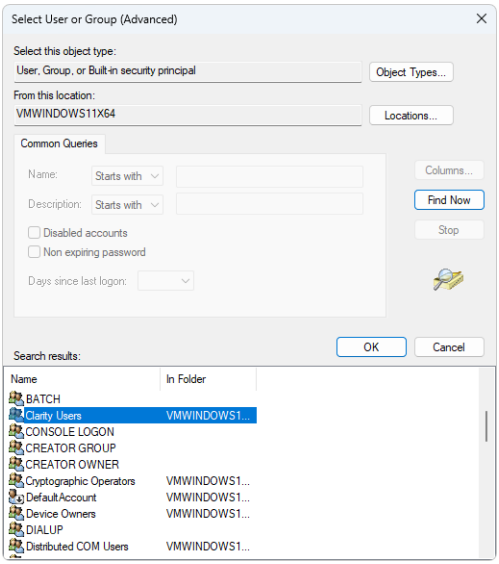


Fig. 12: Select User - Advanced

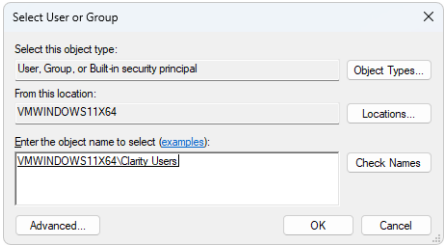


Fig. 13: Select User - Final

- Select necessary permissions for user accounts of the users who should run **Clarity** according to the image below.

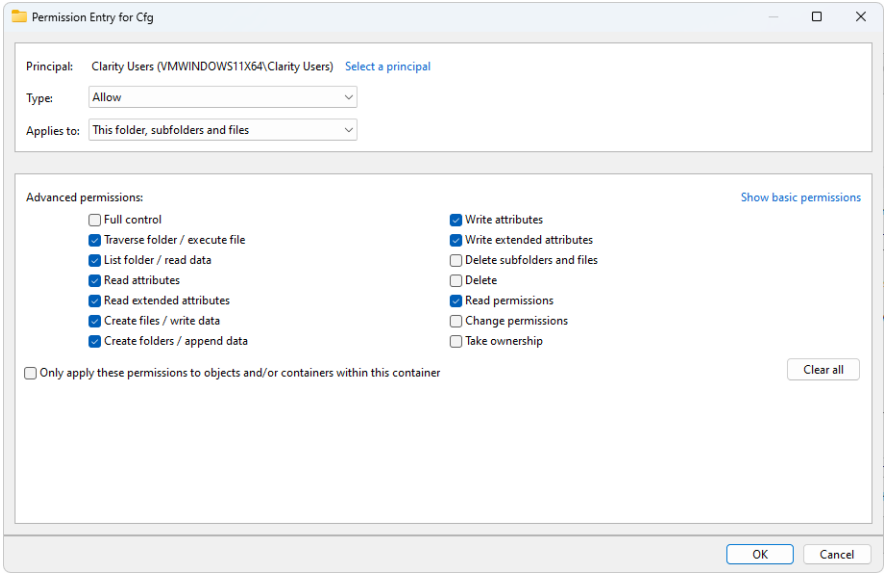


Fig. 14: User Permission Entry

- Repeat this procedure for *Administrator* user account and *SYSTEM*. Both should have all privileges.

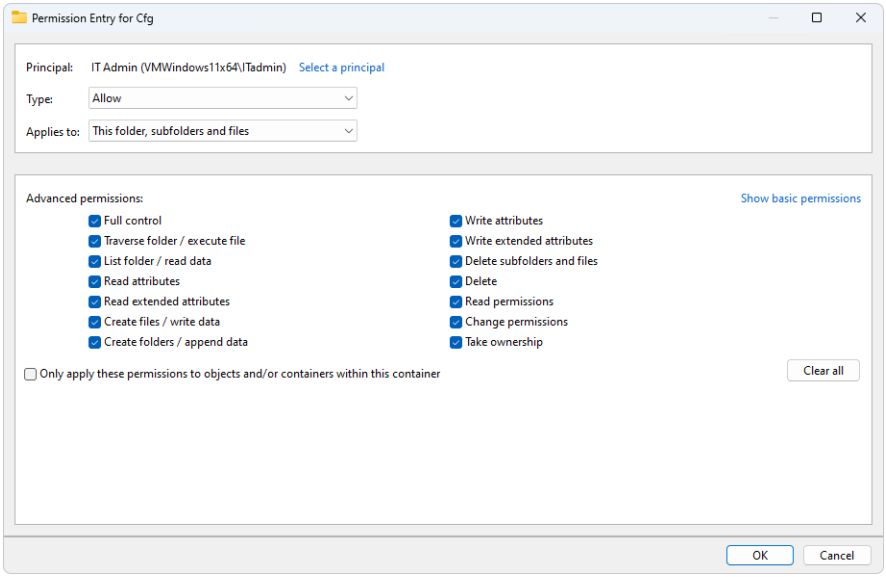


Fig. 15: Administrator Permission Entry

- Final security settings for CFG is displayed in image below.

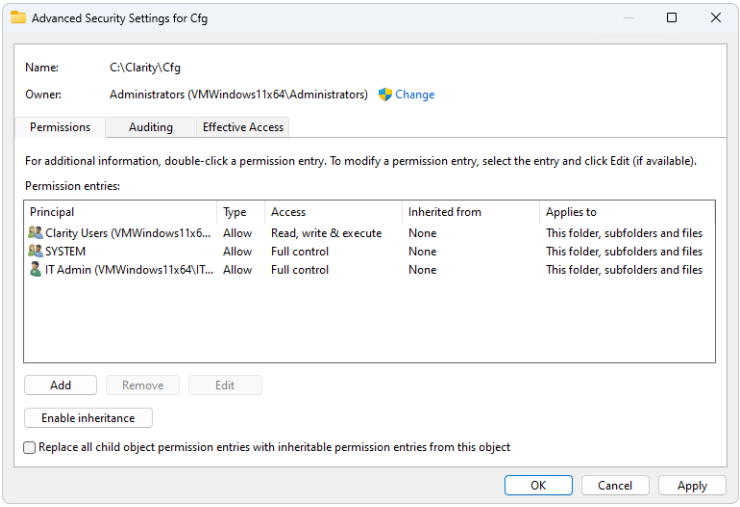


Fig. 16: Advanced Security Settings for the Cfg Folder

- If needed the settings can be reviewed for respective users/group from the *Security* tab in *Cfg Properties* window.
- Repeat this complete procedure for *DataFiles* folder for user group (all user accounts of users who should run **Clarity**) and local *Administrator* user account in completely same manner. (*SYSTEM* permissions are not required here.)

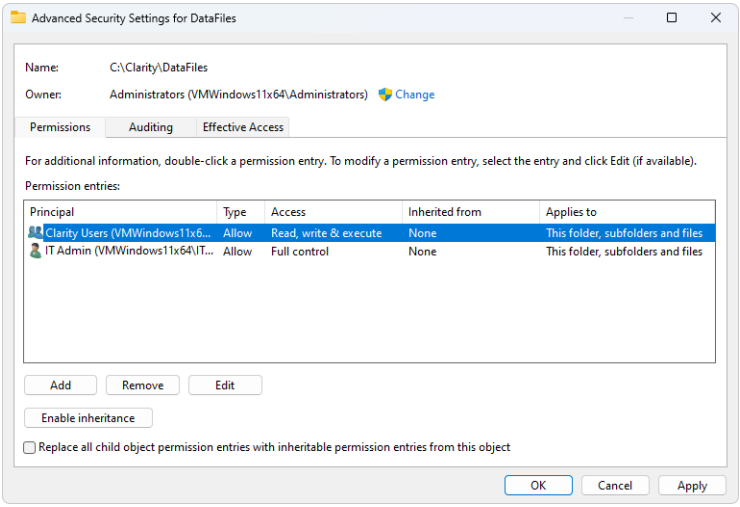


Fig. 17: Advanced Security Settings for DataFiles Folder

- Repeat this complete procedure for *Bin* folder for user group (all user accounts of users who should run **Clarity**), local *Administrator* user account, and *SYSTEM* in similar manner. Be careful as permissions setting for users is different (SYSTEM and local administrator both require full control).

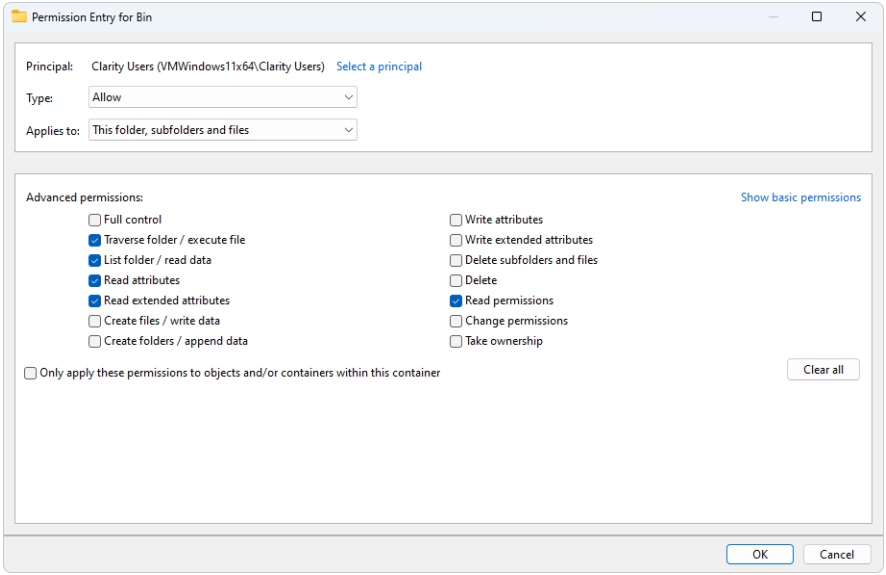


Fig. 18: User Permission Entry for Bin Folder

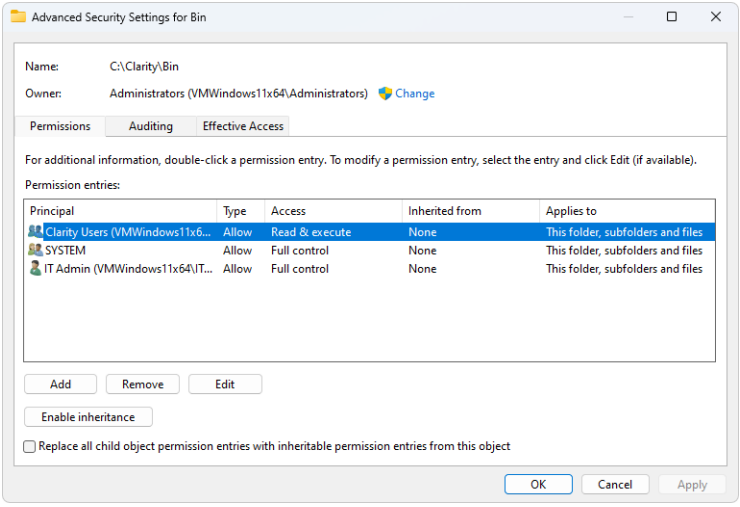


Fig. 19: Advanced Security Settings for Bin Folder

- All user accounts of users who should run **Clarity** can create shortcut of **Clarity** on the their respective *Desktop*.

3.3 User Accounts in Clarity

Every user who has access to **Clarity** must have their own user account with his/her own secret password and access rights defining which actions he/she can perform. This feature is required by **21 CFR Part 11** and **GLP**.

One of the **Clarity** users should serve as a station administrator and have the *Administrator* rights on the **Clarity** station.

Note: These rights may be assigned for example to the laboratory supervisor.

The *Administrator* must be the only one who can create new user accounts in **Clarity** and change the user rights for the existing accounts. Be aware there has to be more than one individual in the organization knowing *Administrator* account login credentials for cases unforeseen circumstances (such as long term absence of the local *Administrator* due illness or injury and so on).

3.3.1 SOP - User Accounts - setup administrator accounts

To comply with regulated environment, two administrators should be created: IT Administrator and Lab Administrator.

IT Administrator

IT Administrator should have access to the station, but not to the data (chromatograms, methods, etc.) created by such station. IT Administrator's main responsibilities are managing configuration settings, user account management, maintaining a list of cumulative users of the system and implementing change control.

So for **Clarity** side, the following needs to be done:

- Open the **Clarity** station.
- In the main *Clarity* window, use the *System – User Accounts...* command to enter the *User Accounts* dialog.
- Create the user account with the *IT Administrator* rights:
  - Use the *New* button.
  - Fill in the *User Name* field with the desired user name.
  - Fill in the *Desktop File* field with the desktop file name and possibly the *Description* field with specification of the account (e.g. the IT Administrator description or the name of the person who should be contacted in case the change of settings should be needed).

Note: Use full names of the users in the *User Name* field. These names will be displayed in the Audit trail records and in all reports. This will make it easier to identify the person who caused a change.

- Set the *Password Restrictions* (this will apply to all users). The minimal length (*Min. Length*) of the password must be specified (at least 6

characters are recommended or according to your company's policy), other fields are optional/dependent on regulations related to you.

- Use the *Change Password* button to set the *User Password* for your *IT Administrator* account. The password must comply with the *Password Restrictions* set in the previous step.
- Set the *User Access Rights* for the *IT Administrator* account: *Open User Accounts* and *Open Configuration*.
- To use Clarity *Archive* function it is necessary to enable *Access To* all instruments and *Archive / Restore* option. When external tool is used for backup these options should not be enabled.

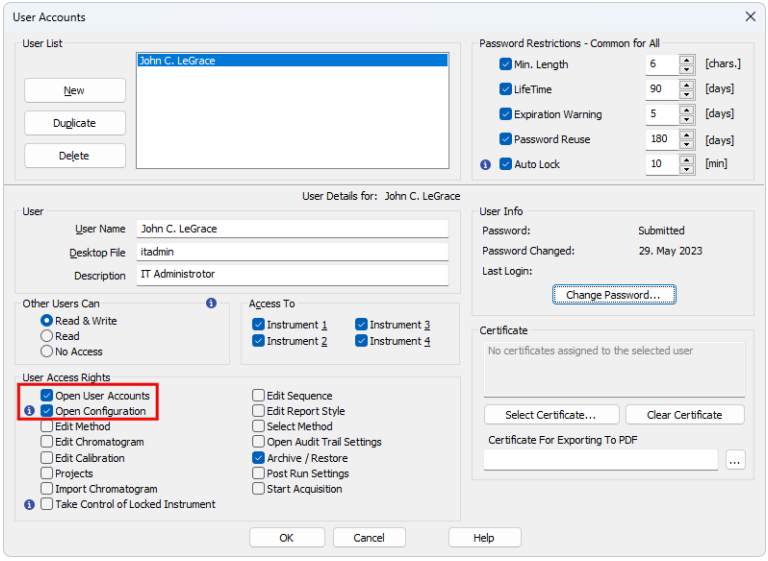


Fig. 20: User Accounts - Setting the IT Administrator

Lab Administrator

Lab Administrator should have access only to the data (chromatograms, methods, etc.) created by such station. Lab Administrator's main responsibilities are allocating CDS resources to users, creating and maintaining projects, creating and verifying methods, custom calculations and reports, etc.

So for **Clarity** side, the following needs to be done:

- Open the **Clarity** station.
- In the main *Clarity* window, use the *System – User Accounts...* command to enter the *User Accounts* dialog.
- Create the user account with the *Lab Administrator* rights:
  - Use the *New* button.
  - Fill in the *User Name* field with the desired user name.

- Fill in the *Desktop File* field with the desktop file name and possibly the *Description* field with specification of the account (e.g. the Lab Administrator description or the name of the person who should be contacted in case the change of settings should be needed).

Note: Use full names of the users in the *User Name* field. These names will be displayed in the Audit trail records and in all reports. This will make it easier to identify the person who caused a change.

- Set the *User Access Rights* for the *Lab Administrator* account. It is up to every laboratory own rules what Lab Administrator's responsibilities are, but Lab Administrator should never be able to modify configuration and do changes in User Accounts (except for allocating privileges to already created users, meaning access to*Open User Accounts* is sometimes justifiable/necessary). Most common set of access rights is displayed in the image below.

- Optional: Select *Certificate* to be used for electronic signatures.

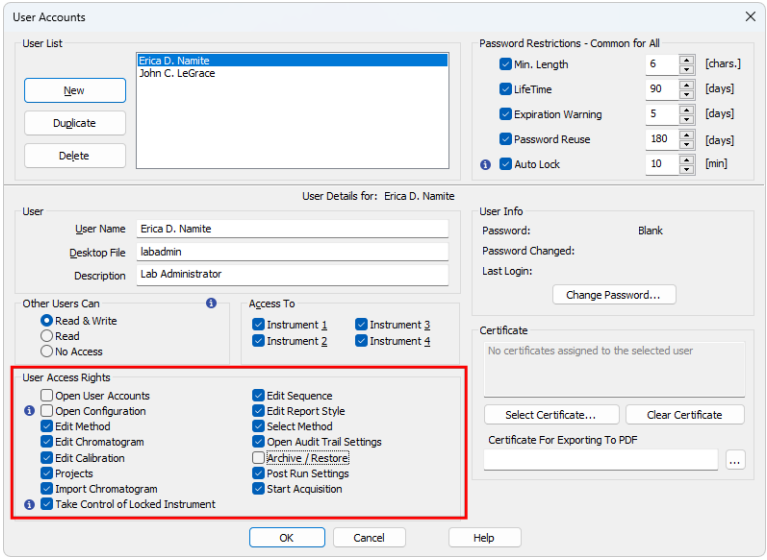


Fig. 21: User Accounts - Setting the Lab Administrator

3.3.2 SOP - User Accounts - setup user account

- Open the **Clarity** station.
- In the main ***Clarity*** window, the user with the *Administrator* rights must use the *System – User Accounts...* command to enter the ***User Accounts*** dialog.
- Create the user account with the *User* rights.
  - Use the *New* button.

- Fill in the *User Name* (again, full names are recommended), *Desktop File* (if you need to share user columns see the chapter **"Shared desktop file"** on pg. **33**.) and the *Description* fields.
- Set the *User Access Rights* for the user account. Rights of each user can vary depending on their position and duties. At minimum the following checkboxes MUST be unchecked:

- *Open User Accounts*
- *Open Configuration*
- *Open Audit Trail Settings*
- *Archive / Restore*
  - Optional: Set the *Certificate* to be used for electronic signatures.

Note: The *Archive / Restore* rights may be set to one user who will be appointed to archiving the data in the company. However, other previously mentioned options should still be assigned only to **Clarity** *Administrators*. We recommend leaving the *Archive / Restore* privileges to the **Clarity** *IT Administrators* and/or *QA* worker.

- Do not change the password settings as this part of the ***User Accounts*** dialog is common for all users of the given **Clarity** station. The setting of the ***User Accounts*** dialog for the common user may be seen in the picture:

Caution: Make sure that *Other Users Can* is **NOT** set to *No Access*. Otherwise data can be only accessed by user that created them.

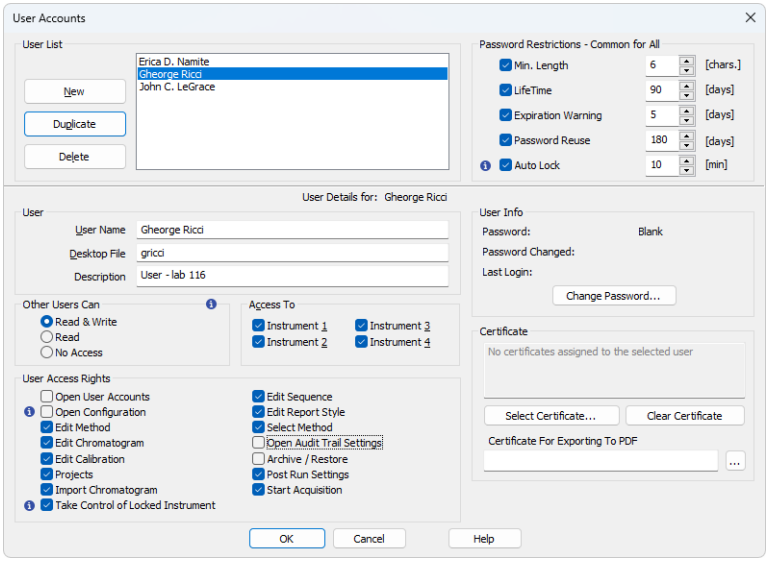


Fig. 22: User Accounts - Setting the User

- Create another user account or leave the *User Accounts* dialog by clicking the *OK* button.

3.3.3 SOP - User Accounts - setup QA account

QA personnel must have their own access to the **Clarity** station, without authorization to change any data.

It is necessary to set the user account for the QA worker in **Clarity** without the right to change any data. To achieve this follow the following procedure.

- Open the **Clarity** station.
- In the main *Clarity* window, the user with the *Administrator* rights must use the *System – User Accounts...* command to enter the *User Accounts* dialog.
- Create the user account with the *QA personnel* rights.
  - Use the *New* button.
  - Fill in the *User Name* (again, full names are recommended), *Desktop File* (if you need to share user columns see the chapter **"Shared desktop file"** on pg. **33**.) and the *Description* fields.
  - Set the *User Access Rights* for the user account. The majority of the checkboxes MUST be unchecked, only the *Projects* checkbox should be enabled. Some other checkboxes might be enabled too, based on the access rights and regulations of the company itself. This specifically targets the *PostRun Settings* and the *Archive / Restore* options.
  - Do not change the password settings as this part of the *User Accounts* dialog is common for all users of the given **Clarity** station. The setting of the *User Accounts* dialog for the common user may be seen in the **Fig. 23** on pg. **28**.:

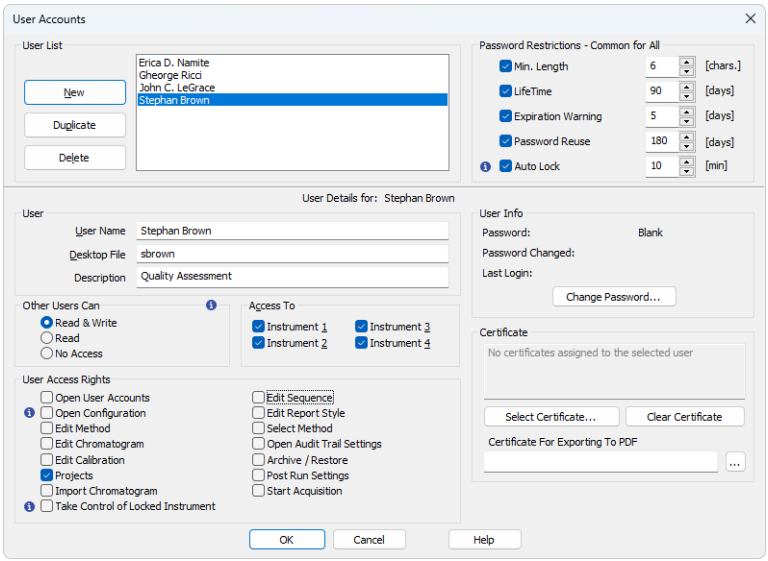


Fig. 23: User Accounts - Setting the QA worker

3.4 Logging of all changes

Every change in the data must be properly logged, along with the reason for the change, so that the reason of the change can be later found. This feature is required by **21 CFR Part 11** and **GLP**.

Overall, the best way to ensure that every important change is recorded is to log every operation **Clarity** performs. This is the default setting in the **Clarity** version 2.7 and later. To check that this is the case, or to set this feature, the **Clarity** user with the *Administrator* rights should perform the following steps:

3.4.1 SOP - setup logging in Audit Trail

- Use the *System – Audit Trail* command from the *Clarity* main window to open the *Audit Trail* window.
- Use the *View - Properties...* command from the *Audit Trail* window to access the *Audit Trail Settings* dialog.

Note: You will be asked for the correct **Clarity** *User Name* and password.

- Check all of the checkboxes on all tabs there and verify that they are all enabled; if some of them are not, check them.
- Use the *OK* button to exit the dialog.

3.5 Logging reasons of changes

The reason for the change must be logged along with the change itself so that the reason for the change can be found later.

This issue may be solved, along with other issues, from the *GLP Options* dialog. For more details see the chapter **"SOP - GLP Options settings"** on pg. **8**.

3.6 Archiving the data

All data must be archived for the period specified by the appropriate authorities. This feature is required by **21 CFR Part 11** and **GLP**.

Note: The **FDA**'s (American) version of the **GLP** already includes the minimum records retention periods in the § 58.195.

This requirement may be fulfilled (from the **Clarity** standpoint) by the *Archive...* and *Restore...* commands from the ***Instrument*** window. Some external archiving software may also be appropriate.

Note: Archiving and restoring data should be left to people with the administrator account.

3.6.1 SOP - the data archiving

It is recommended to use external tool to create regular backup of data and other files. But it is possible to compress whole projects to archives in Clarity:

- A person with the *Archive/Restore* privilege (**Clarity** *Administrator* or *QA* worker) must open **Clarity** and the given Instrument.
- Use the *File - Archive...* command to open the ***Backup*** dialog.

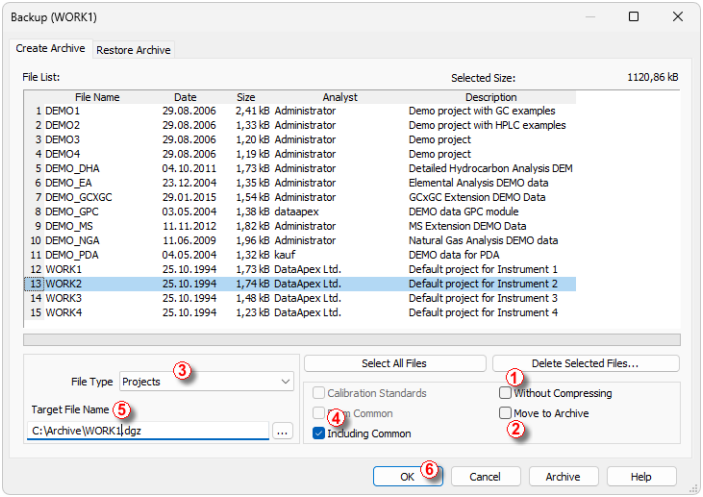


Fig. 24: Backup

- Uncheck the *Without Compressing* checkbox ① .
- If you want to delete files from the original location and move them to archive check the *Move to Archive* checkbox ② .

Caution: If you want to archive the files with deleting the source files (chromatograms, sequences etc.) check ② *Move to Archive* option. Be aware that if the *Security Settings* for *DataFiles* folder are set according to the chapter **"Computer User Rights"** on pg. **11**. the moving to archive (=deleting of the files) can be done only by the person will *Full Control* privileges for *DataFiles* folder, typically local IT worker.

- Select *Projects* from the drop down menu in the *File Type* field ③ . The list of available projects will emerge in the *File List*. Select the project you want to archive there.
- Check *Include Common* to archive any files that are stored in DATAFILES\COMMON ④ .
- Choose the path to and the name of the archived file (*.DGZ extension) in the *Target* field ⑤ .

Note: Be aware it is not allowed to save files to root folder of operating system (typically "C:\") usually because of commonly predefined *UAC - User Account Control* settings in *Windows 7* and newer. In this case is necessary to select other location for storing of resulting *.DGZ archive than *Windows* root folder. It is sufficient to create some other folder in *Windows* root folder usually.

Caution: It possible to disable deletion or alteration of created *.DGZ archives. The *Security Settings* for the folder stated in the *Target* field ⑤ has to be completely the same as described in the chapter **"Computer User Rights"** on pg. **11**. in this case. It is necessary to follow guidance given in the respective subchapter of the the chapter **"Computer User Rights"** on pg. **11**..

- Press the *OK* button ⑤ to archive the project and close the ***Backup*** dialog. Archiving without leaving the dialog can be performed by using the *Archive* button instead.
- For the data to be complete and valid, two more file types must be archived - audit trail and the configuration files. To archive audit trail files:

Note: Each data file produced by **Clarity** has it's own audit trail log, but these separate log's do not hold information on the global events like opening the Instruments in **Clarity**, changing the method files and so on. All of these events are recorded in the station audit trail.

- Uncheck the *Without Compressing* checkbox ① in the opened ***Backup*** dialog. Unlike the whole projects archiving, the *Move to Archive* checkbox ② should stay unchecked.

Note: The daily and station audit trails are common for the whole **Clarity** station. Thus, in case more than one Instrument is available to users, removing the audit trail files might also remove the log data from other **Clarity** projects.

- Select the *Audit Trail Files* option in the *File Type* field ③ and choose the valid files in the *File List*.
- Choose the path to and the name of the archived file (*.DGZ extension) in the *Target* field ⑤ . Take care not to overwrite the backed-up project.
- Press the *OK* button ⑥ to archive the project and close the ***Backup*** dialog. Archiving without leaving the dialog can be performed by using the *Archive* button instead.

- To archive the configuration file, do the following:

Note: The process of **Clarity** configuration file archiving cannot be performed from the **Clarity** environment. The configuration file is not needed for further file records, it is just a necessary part which has to be saved for the repeatability of the measurement.

- A person with the *Administrator* rights on the computer (not in **Clarity** - typically a company IT worker or laboratory supervisor) must open the file manager while **Clarity** is off and enter the **Clarity** installation directory (C:\CLARITY by default).
- This *Administrator* should locate the CLARITY.CFG file (C:\CLARITY\CFG by default) and copy it to the location with the other archived files.

Note: It is recommended to backup any used *.DSK files and clarity.psw in the same manner as the configuration file.

3.7 Shared desktop file

All users must have the same settings in the user calculation columns.

These settings are defined in the user desktop, which, by default, are not common for all users as the desktop file also saves data on the last opened documents, user settings and so on. When all users have to use the User calculations in tables or other features saved in the user settings, it is necessary to ensure that all users use the same desktop file, which is not modifiable. To set that, perform the following steps:

3.7.1 SOP - shared desktop file

- Prepare the desktop file so that it meets your requirements for the settings.
- Use the account with *Administrator* rights to enter the *User Accounts* dialog.
- One at a time, select users who should use the same desktop in the *User List*. For each user selected, change the desktop file name in the *Desktop File* field to the desired name.

Note: The file name of the desired desktop is the one set for the account who prepared it. If the *Desktop File* field there is empty, than the default desktop file name is used, which is the same as the given User Name.

- Leave the *User Accounts* dialog by pressing the *OK* button.
- Close **Clarity**.
- Find the desktop file on your computer in a file manager program. The file will be located in the **Clarity** main directory (C:\CLARITY\CFG by default) and will have the given file name and the *.DSK extension.
- Change the properties of the file to *Read & execute* . This should be only done by *Windows* user account with *Administrator* privileges in the same manner as described the chapter **"Computer User Rights"** on pg. **11**. This setting should be done for all *Windows* user accounts of the **Clarity** users who should use this selected shared desktop file.
- To change privileges go to *Advanced Security Settings* of targeted file. Use *Disable inheritance* and select *Convert inherited permissions into explicit permissions on this object*. Then change the permissions for group/users that will use this file and should not modify it according to the image below.
- When changing Security properties to the selected shared desktop file assure that Security Setting for CFG folder remains exactly the same as described the chapter **"Computer User Rights"** on pg. **11**..
- Be aware that users will be able to modify current shared desktop file in **Clarity** but they won't be able to store the modifications, as an error message *Desktop file write error* will be displayed when closing *Instrument Window*.
- Users that should be able to change the file must keep permissions inherited from CFG folder.

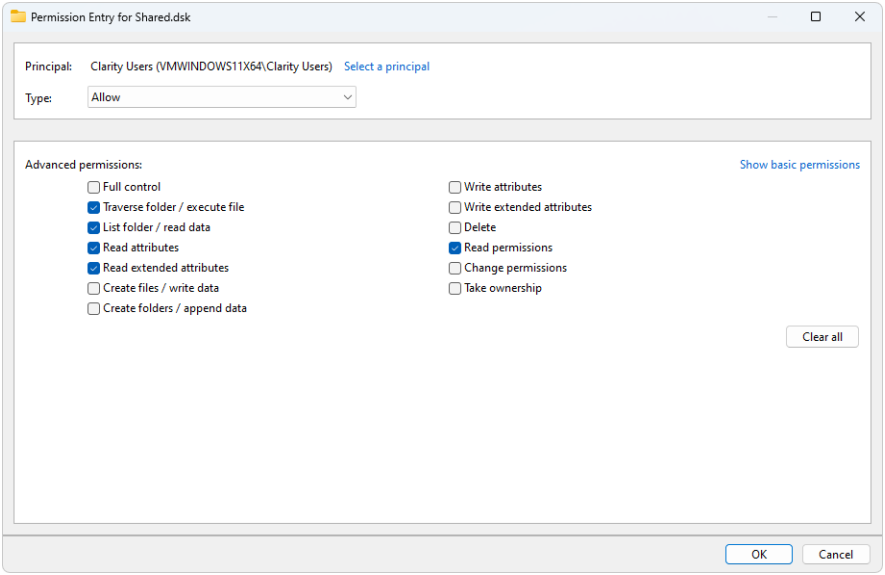


Fig. 25: Security Settings for Shared Desktop - User Entry - Windows 11

3.8 Multistation environment

When the user (or several users) is supposed to work on several computers, the user accounts for all users (along with stored passwords) should be the same for all users everywhere. This can be achieved by having the same CLARITY.PSW file in the CFG directory of the **Clarity** station (C:\CLARITY\CFG by default) on all computers.

The CLARITY.PSW file changes only in two cases - either when a new user is added to the user list or when the current user changes his/her password.

Caution: It is only necessary to ensure that the user accounts used are the same on all computers, in other words do so only after a change was made in the ***User Accounts*** dialog (adding user, modifying user's rights, ...). Ensuring that the file is the same after the password change may help the comfort of the users, but is not required.

As the whole **Clarity** installation directory should be inaccessible to normal users, the system *Administrator* should be supposed to copy this CLARITY.PSW file to all other computers with **Clarity** in multistation environment.

Note: The CLARITY.PSW file is saved and modified when the **Clarity** station is closed. Therefore it is necessary to copy the file into the root directory only when **Clarity** is not running.

3.9 Electronic signatures

It must be possible to sign electronic data in the **Clarity** with electronic signatures that are unique to each individual, will not be reused by, or reassigned to, anyone else and cannot be manipulated. This feature is required by **21 CFR Part 11**.

Note: Certificates used for electronic signatures are not part of **Clarity** installation and such certificates are to be provided by certification authorities. DataApex does not issue any certificates for electronic signatures.

The certificate that is to be used with **Clarity** must include the private key part with the password known only to the particular user and require entering the password at each use. To set the certificate to a particular user, perform the following steps:

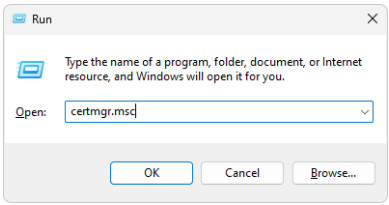
Cautions It is necessary to bear in mind that in case of signing chromatograms with 3rd party certificate it is absolutely necessary to have the certificate of each Windows user account installed in the Personal storage of every Windows user account used on the PC where Clarity is operated. If there would be installed more certificates for more Clarity user accounts under single Windows user account it could easily happen that various Clarity users (defined through *User Accounts* dialog) could sign chromatograms with someone's else certificate. This situation can occur because it is standard behavior of the certificates in Windows environment to ask currently logged Windows user for password to his/her certificate only for the first usage of the certificate during individual Windows user account login session. Every other request to sign any chromatogram with already used certificate won't invoke any other request for repeated password insertion and the selected chromatogram could be signed using any available certificate for which its correct password was entered during current session of the logged in Windows user. To avoid that, in case of wish or necessity to use 3rd party certificates, it is necessary to have for each Clarity user account its separate Windows user account with unique credentials and 3rd party certificate installed in Private storage of this Windows user account. This condition has to be handled when Clarity should be deployed in regulated environment and there should be used certificates issued by 3rd certification authorities. There is still option to avoid this complication by signing of chromatograms by credentials defined for each Clarity user through option *Sign As Current User* in the *Sign* dialog.

3.9.1 Setting certificates

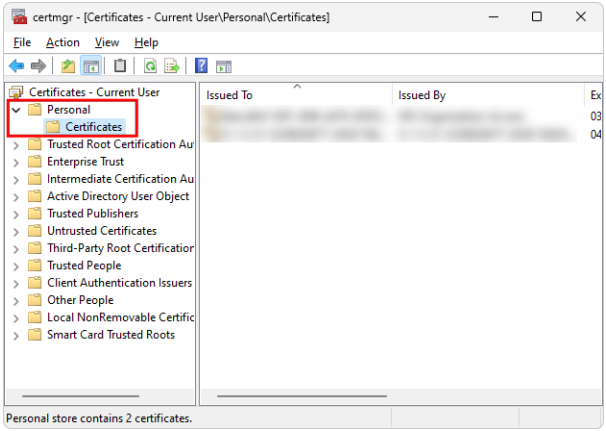
The certificate issued by any official authority is a file that can be installed on the given computer. Such installation procedure shall be explained and described in detail by the certification authority by which the certificate was issued.

Checking installed certificates:

- System *Administrator* should run the certificate file and install it according to the process described by the issuer. Its installation may differ in various operating systems, but the file should be installed to the *Personal* certificate store.
- In the Microsoft Windows press windows key together with the "R" key on your keyboard to invoke the *Run* dialog. Type "certmgr.msc" in the dialog and click *OK*.



- In the following window, navigate to *Personal* folder. Such folder contains certificates that are shown by **Clarity** and can be selected in the *Select certificate* dialog in the ***User Accounts*** window.



Setting certificate for signing chromatograms:

- **Clarity** *Administrator* should run **Clarity** and open the ***User Accounts*** dialog (by using the *System - User Accounts...* command).

- Select the particular user name in the *User List* section in the upper left part of the dialog.
- Click the *Select Certificate* button in the lower right part of the dialog. The *Select Certificate* dialog appears.
- Select the certificate from the list of available certificates in the dialog and press the *OK* button. The selected certificate will be added to the user's user account.
- Set other certificates for other users, if desired, by repeating the above mentioned steps.
- Close the *User Accounts* dialog by pressing the *OK* button.

Setting the certificate for signing PDF documents:

- **Clarity** *Administrator* should run **Clarity** and open the *User Accounts* dialog (by using the *System - User Accounts...* command).
- Click the ... button to invoke the *Open* dialog and select the PKCS#12 type certificate.
- Set other certificates for other users, if desired, by repeating the above mentioned steps.
- Close the *User Accounts* dialog by pressing the *OK* button.