DataApex
Clarity™
CHROMATOGRAPHY SOFTWARE

REGULATED ENVIRONMENT

Clarity Software ENG

Code/Rev.: M132/100D
Date: 2026-05-21

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

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

Clarity®, DataApex® and ® are trademarks of DataApex Ltd. Microsoft® and Windows™ are trademarks of Microsoft Corporation.
DataApex reserves the right to make changes to manuals without prior notice. Updated manuals can be downloaded from 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 any environment operating under defined control rules and standards that ensure valid and consistently high-quality results or products. Such regulations are usually set by various sources: the company itself, government authorities - such as the American Food and Drug Administration (FDA) - or other organizations responsible for product quality and standardization.

In the context of analytical laboratories, compliance with a regulated environment means that every operation involving data must be reproducible at any time. In Clarity, the following file types are considered data: methods (*.MET), chromatograms (*.PRM), calibrations (*.CAL), and sequences (*.SEQ). Each of these files includes its own *Audit Trail*, and both method and chromatogram files also store their complete history.

This manual is designed to guide Clarity users in configuring and operating the software in accordance with such regulatory requirements.

1.1 Good Laboratory Practice

Good Laboratory Practice (GLP) is a set of principles defined by Organisation for Economic Co-operation and Development (OECD) and implemented by national authorities. It provides a framework for how laboratory studies are planned, performed, monitored, recorded, reported and archived.

These principles ensure that studies producing data for assessing hazards and risks — whether to users, consumers, third parties, or the environment — are carried out in a consistent and reliable manner. GLP applies to areas such as preclinical pharmaceutical testing, agrochemicals, cosmetics, food and feed additives, contaminants, novel foods, biocides, and detergents.

By following GLP, laboratories demonstrate to regulatory authorities that the submitted data accurately reflect the results obtained during the study and can be relied upon for risk or safety assessments.

1.1.1 GLP in Clarity

This section describes how Clarity supports compliance with **GLP** requirements.

Some measures are mandatory for operating Clarity in a regulated environment, while others depend on specific system configurations or company policies.

Each requirement listed below includes a reference to the relevant section or SOP that provides further guidance and setup details.

Mandatory

- The computer on which Clarity is installed must operate under conditions where every user has their own defined rights - see the chapter **"Computer User Rights"** on pg. **6**.

- File overwriting in Clarity must be disabled. Data loss caused by overwriting or similar actions must not be allowed - see the chapter **"Computer User Rights"** on pg. **6**.
- Every user who has access to Clarity must have their own user account with unique password and defined access rights specifying which actions they can perform - see the chapter **"User Accounts in Clarity"** on pg. **19**.
- Every change in the data must be properly logged - see the chapter **"Logging of all changes"** on pg. **24**.
- The reason for each change must be logged, along with the change itself, so that it can be reviewed later - see the chapter **"Logging reasons of changes"** on pg. **25**.
- All data must be archived for the period specified by relevant authorities - see the chapter **"Archiving the data"** on pg. **25**.

Optional

- When Quality Control or Quality Assessment personnel are present – QA staff should have their own access to the Clarity station, without authorization to modify any data - see the chapter **"SOP - User Accounts - QA account setup"** on pg. **23**.
- 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. **27**.
- Multistation environment: each user must have an individual account but use the same credentials and access rights on every Clarity station - see the chapter **"Multistation environment"** on pg. **31**.

1.2 CFR 21 Part 11

CFR 21 Part 11 is a regulation issued by FDA. It defines the conditions under which organizations may submit or store FDA-related documents in electronic form instead of on paper. The regulation focuses on ensuring that electronic records are as reliable and trustworthy as their paper equivalents.

The key requirements include:

- System validation
- Controlled access - records must be accessible only to authorized personnel
- Audit trail - documentation of all modifications to electronic records
- Electronic signatures

Compliance with CFR 21 Part 11 can only be achieved through a combination of the appropriate software functionality, system configuration, and standard operating procedures (SOPs) defined by the organization.

1.2.1 21 CFR Part 11 in Clarity

This section describes how Clarity supports compliance with **CFR 21 Part 11** requirements.

The detailed **21 CFR Part 11** requirements for Clarity can be found in the D019 Clarity 21 CFR Part 11 tools datasheet. For the most of the requirements set by the **21 CFR Part 11**, the necessary conditions must first be defined at the company level.

However, the following articles of **21 CFR Part 11** are supported by Clarity (some fully, some only partially) and the corresponding setup procedures are described in this manual.

Mandatory

- § 11.10 a, § 11.10 i - Clarity software must be validated. This is accomplished by the **DataApex** Quality Assurance system (see the D028 ISO9001:2015 certificate datasheet) and verified and verified by Installation Qualification (IQ) , Operational Qualification (OQ) and Performance Qualification (PQ).
    - IQ verifies that the Clarity software is correctly installed and that all required components are present in the correct versions. The results of IQ are documented in IQ report.
    - OQ verifies that the installed Clarity system operates in accordance with manufacturer's specifications. DataApex considers the OQ to be valid only if it is performed by a person authorized by DataApex. Authorization is granted by a certificate issued by DataApex.
    - PQ verifies that the analytical system is fit for its intended use under actual operating conditions. PQ must be performed based on the SOPs, instruments, and workflows used at the specific site. Therefore, DataApex does not provide pre-prepared PQ procedures but can assist with the PQ of the system if required.
- § 11.10 c - You must ensure that the data are stored and can be retrieved throughout the entire record retention period - see the chapter **"Archiving the data"** on pg. **25**.
- § 11.10 d, § 11.10 g - System access must be limited to authorized individuals - see the chapter **"Computer User Rights"** on pg. **6**. and the chapter **"User Accounts in Clarity"** on pg. **19**.
- § 11.10 e - Every action performed in the Clarity system must be recorded in a secure *Audit Trail* - see the chapter **"Logging of all changes"** on pg. **24**.
- § 11.50, §11.70, § 11.100 - It must be possible to sign electronic data in the Clarity using electronic signatures that are unique to each individual, are not reused or reassigned, and cannot be manipulated - see the chapter **"Electronic signatures"** on pg. **29**.the chapter **"Logging of all changes"** on pg. **24**.
- § 11.200 a - Any access or signature must be performed based on two distinct identification components - see the chapter **"Clarity GLP Options"** on pg. **17**. and the chapter **"Electronic signatures"** on pg. **29**.the chapter **"Logging of all changes"** on pg. **24**.
- § 11.300 - Each security code / password pair must be unique to a single user. Moreover, each password must be periodically verified and updated - see the chapter **"User Accounts in Clarity"** on pg. **19**.

2 How to set up Clarity

Setting up the Clarity chromatography station to operate in a regulated environment involves the following steps:

- Selecting appropriate computer and installing correct operating system - see the chapter **"Computer installation"** on pg. **4**.
- 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. **6**.
- Setting Clarity to comply with the specific regulated environment requirements - see the chapter **"Clarity GLP Options"** on pg. **17**. and the chapter **"User Accounts in Clarity"** on pg. **19**.

2.1 Computer installation

Hardware requirements for the computer system may change with the continuing development of Clarity. Version-specific requirements can be found on the **DataApex website** or in the D016 Clarity Compatibility Table datasheet.

To operate Clarity in regulated environment, the computer must run an operating system that supports file access restrictions based on individual user accounts.

Operating systems that supports regulated environment operations in Clarity include:

- 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 and installation procedures following this note are described for Windows 11 Pro. The procedure is similar for other operating systems, although some minor differences may occur.

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

- Install the operating system on the computer.
- Install the available service packs and updates for the operating system.
- Install Clarity (see the chapter **"Installing Clarity"** on pg. **4**.).
- Set the user accounts that will be needed on the computer (for more details see the chapter **"Computer User Rights"** on pg. **6**.).
- Install any other software required on the computer, along with its service packs and updates.

2.2 Installing Clarity

It is recommended to install Clarity first and create the accounts afterward according to the instructions in the Computer User Rights.

In short, to install Clarity in compliance with regulated environment requirements, follow the steps described below.

For more detailed guide on how to install clarity for the first time, please refer to the *User Guide*.

1. Verify the installation package.

Caution: Do not plug in any hardware yet apart from HW key!

2. Insert the Clarity installation USB into the computer and run INSTALL.EXE.
3. Select the language and confirm the License Agreement.
4. Select installation directories. Set location for your data files. C:\CLARITY\DATAFILES is set by default.
5. Enter the *User Code*.
6. Select the installation type (or specific components in the lower pane).
7. Confirm driver installation.
8. Insert the HW key into the USB slot if not plugged earlier.
9. Connect any other HW.

3 Solutions and SOP's

This chapter describes a set of solutions to specific issues that may occur in regulated environment, along with the corresponding Standard Operation Procedures (SOPs) designed to ensure compliance with the requirements of the given regulated environment platform.

3.1 Computer User Rights

The computer on which Clarity is installed must operate under the conditions where each user has individually defined access rights.

Caution: In order to maintain good Data Integrity, staff operating Clarity (typically laboratory personnel) **must not** have any privileges to change Windows System Time on the computer running Clarity. If this condition is not met, the accuracy and integrity of timestamps *Audit Trail* can be compromised, since they are recorded as current Windows System Time in the moment of any action performed.

These settings may only be set by the system administrator, preferably during the computer installation. This feature, mandated by both **21 CFR Part 11** and **GLP**, has been tested and verified on the following operating systems: **Windows 7 Professional**, **Windows 8.1 Pro**, **Windows 10 Pro** and **Windows 11 Pro**. Here are some general recommendations on the computer system:

- The computer where Clarity will be run must use only user accounts with specifically defined user privileges, as described in the following sections of this chapter. The administrator account should be reserved for IT personnel, who must not be involved in creating electronic records in Clarity, because administrator privileges allow access to data outside of Clarity without *Audit Trail* logging.
- Each Clarity user should have their own individual Windows user account. Windows user accounts can be either local or domain-based (Active Directory). When the computer is part of a domain, domain user accounts may be used instead of local accounts without limitation.

  Caution: It is not possible to switch Windows users while Clarity is running. If taking over a running instrument is required, it is recommended to use one shared Windows user account for all Clarity users (that require this function).

- All Windows user accounts must have defined access rights for the **Cfg**, **DataFiles**, and **Bin** subfolders within the Clarity installation directory. If the DataFiles folder has been renamed or moved outside the Clarity directory (for example, to a regularly backed-up network location), user privileges must be set in the same way as for the default folder. The data storage location can be modified via the *System - Directories...* command in the Clarity main window.
- The data created by Clarity users must not be stored in **Bin** subfolder.

Note: To further protect data integrity, the organization should implement internal measures to prevent accidental or unauthorized data changes by IT staff or other personnel with administrator privileges.

3.1.1 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 31.10.2025) installed.

This process must be performed by a person with Administrator privileges (e.g., an IT specialist). It assumes that the computer is freshly installed with no user accounts other than the administrator one. Clarity is supposed to be already installed.

User accounts setup

User accounts can be either local or domain-based (if the computer is part of a domain).

If the computer is part of a domain, existing domain user accounts can be used directly and it is not necessary to create local user accounts. In such case, include these domain users in a group or assign the required permissions as described below.

If no suitable accounts exist, create local user accounts as described below.

- Open *Computer Management*: Right-click the Start menu and select *Computer Management*. In the left panel, navigate to *Local Users and Groups - Users*.

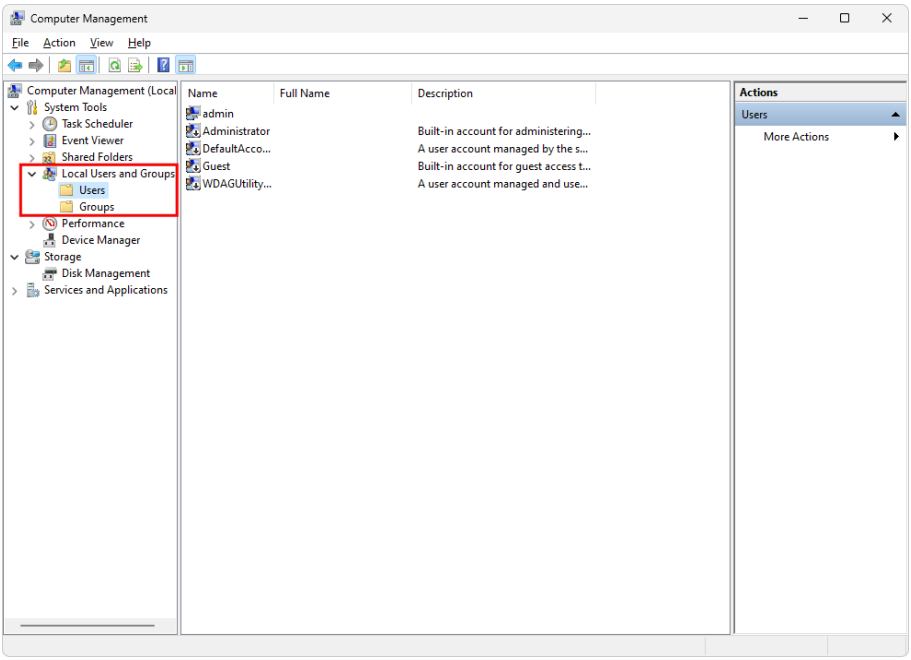


Fig. 1: Computer Management

- Create a new user account: Right-click the *Users* item and select *New User...* from the context menu. Fill in all required fields in the *New User* dialog, set a password according to your organization's policy and click the *Create* button.

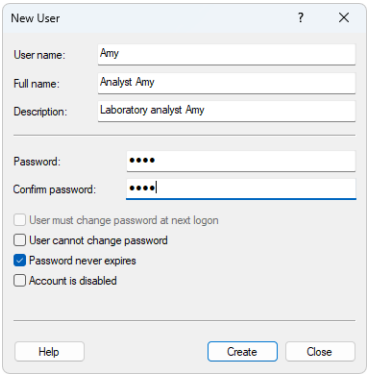


Fig. 2: Create New User

- Repeat this procedure for each additional user you want to add. Close the *New User* dialog by clicking *Close*.

Group configuration and management

Creating a group is recommended when multiple users work with Clarity, as it simplifies permission management. However, it is also possible to assign the required access rights directly to individual user accounts.

If the computer is part of a domain, a domain group may be used instead of a local group. In such case, it is recommended to use a dedicated domain group (e.g., for all Clarity users) and assign permissions to this group.

- In *Computer Management* window, navigate to *Local Users and Groups - Groups* section.
- Right-click the *Group* and select *New Group...* from the context menu and add its description. Then click *Add* to manage members.

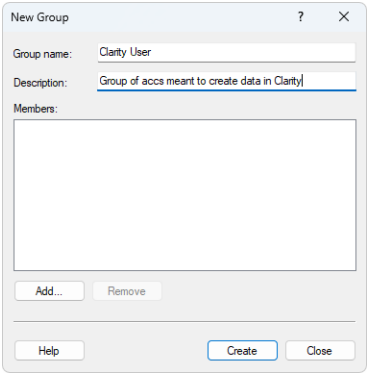


Fig. 3: Users Group

- 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 verify which users are members of the group in the group properties.

Perform the first login

Perform first login for all newly created users. This step is essential — performing it later can compromise the electronic security of Clarity records.

During the first login, the newly created users are automatically added to the *Authenticated User* group. To ensure proper data protection under GLP, this group must not have access to Clarity subfolders. This is achieved by removing inherited permissions as described in the steps below.

Each user may create a shortcut to Clarity on their desktop for convenient access.

Setting the permissions

- Log back in as the local *Administrator*.
- Locate the Clarity installation directory. If the DATAFILES subfolder is elsewhere, verify that it is properly setup using *System Directories* in Clarity.
- Right-click on the subfolder CFG and select the *Properties* from the context menu. Switch to the *Security* tab.

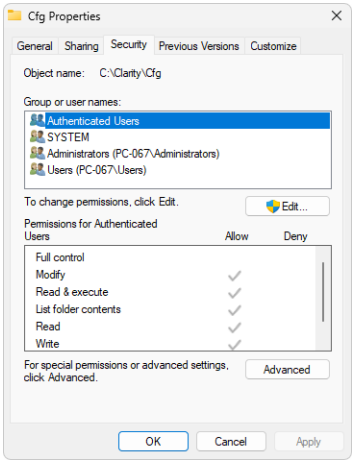


Fig. 4: Cfg Folder Security Properties

- Select *Advanced* and window *Advanced Security Settings for Cfg* opens.

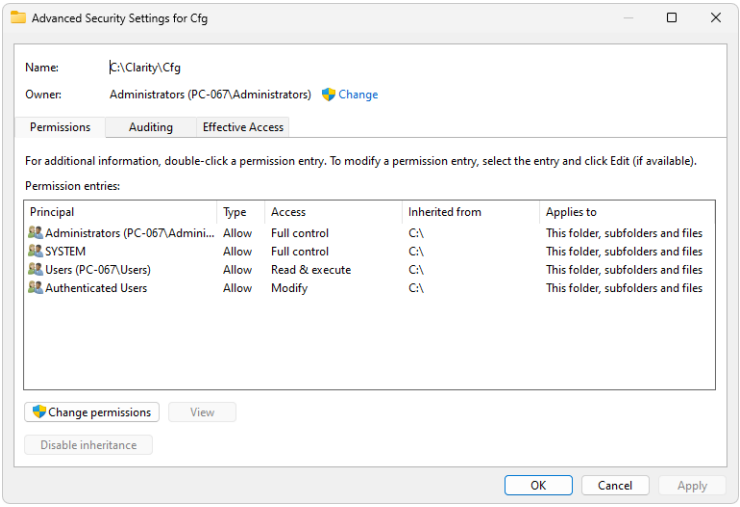


Fig. 5: Advanced Security Settings - Initial state

- 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.

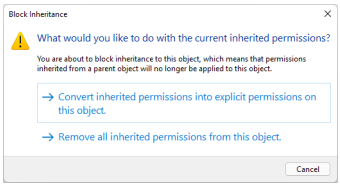


Fig. 6: Block inheritance

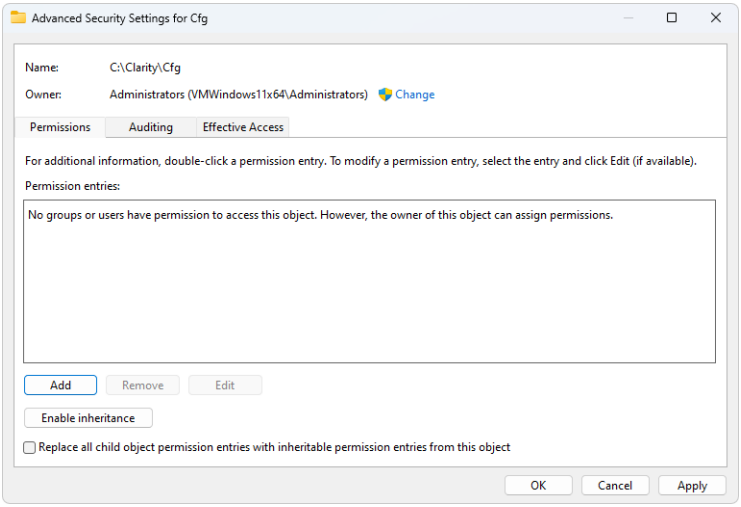


Fig. 7: Advanced Security Settings - No Entry

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

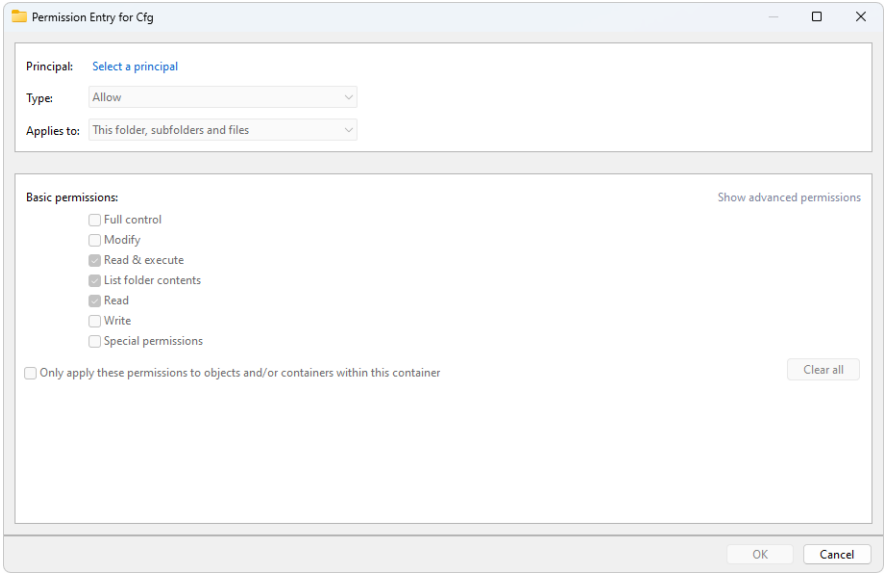


Fig. 8: Permission Entry

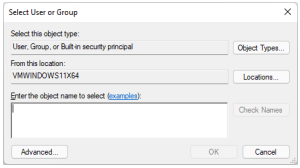


Fig. 9: Select User - Initial

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

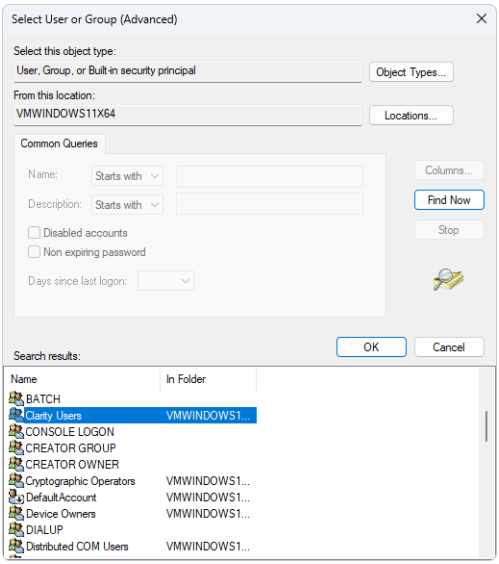


Fig. 10: Select User - Advanced

- 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.

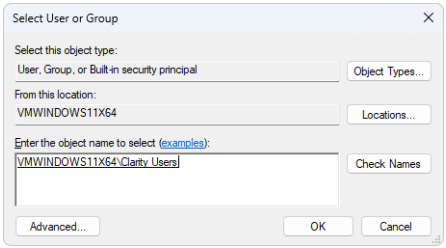


Fig. 11: Select User - Final

- Click *Show advanced permissions*. Select the relevant permissions for the user accounts of those who will run Clarity.

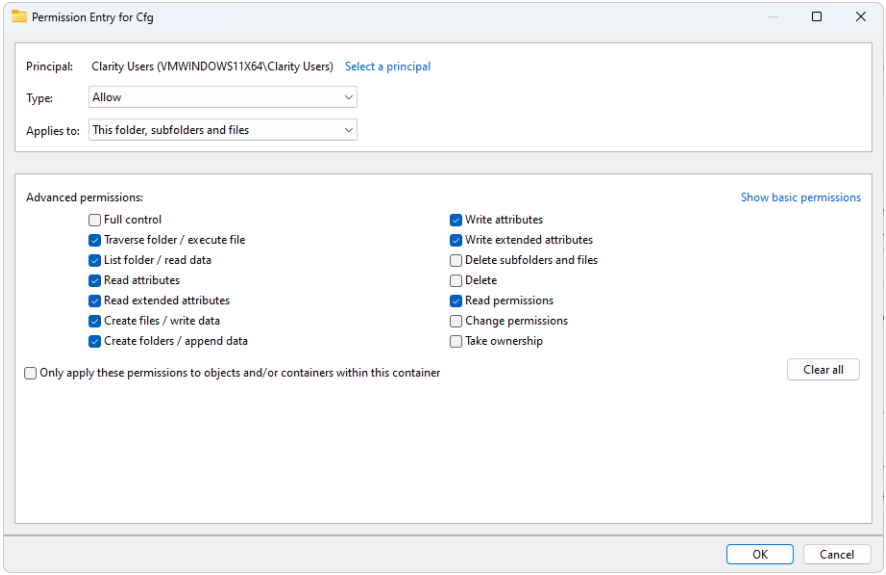


Fig. 12: User Permission Entry

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

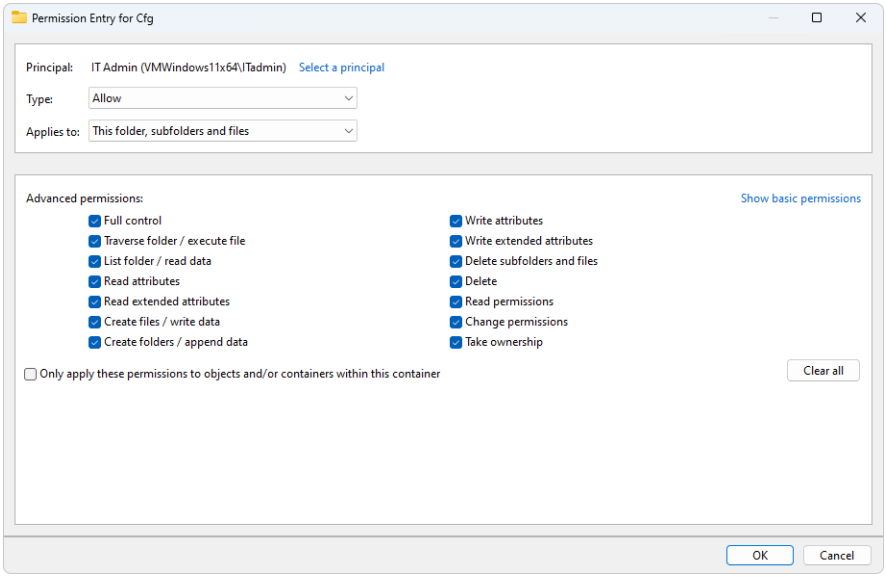


Fig. 13: Administrator Permission Entry

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

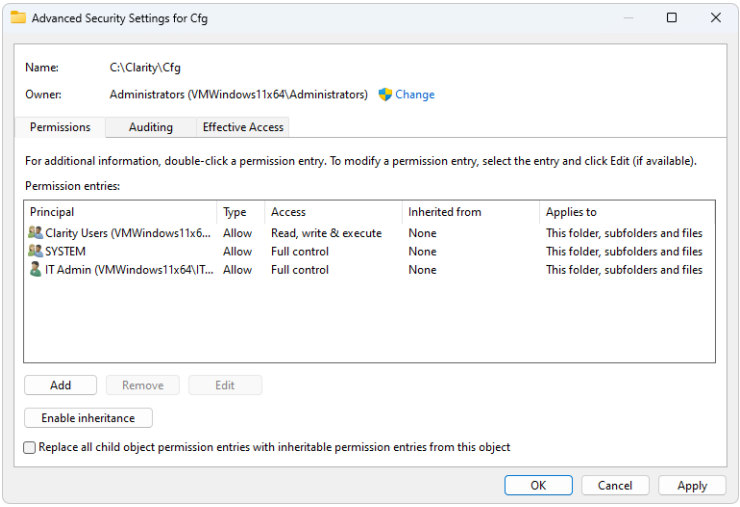


Fig. 14: Advanced Security Settings for the Cfg Folder

- 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 exactly the same manner (*SYSTEM* permissions are not required here).

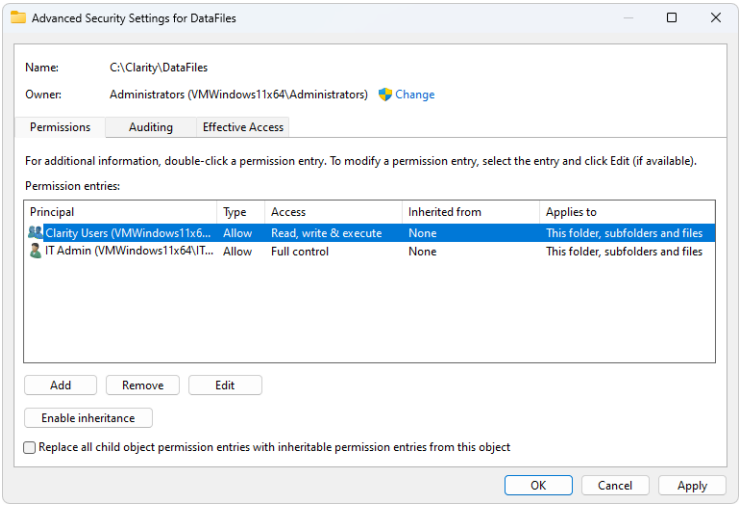


Fig. 15: Advanced Security Settings for DataFiles Folder

- 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 the similar manner. Be careful as permissions setting for users is different (SYSTEM and local administrator both require full control).

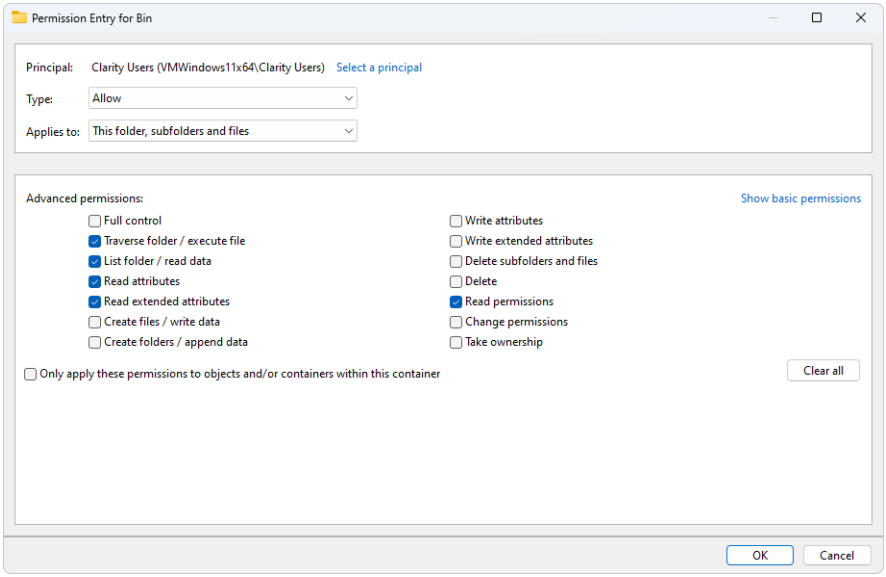


Fig. 16: User Permission Entry for Bin Folder

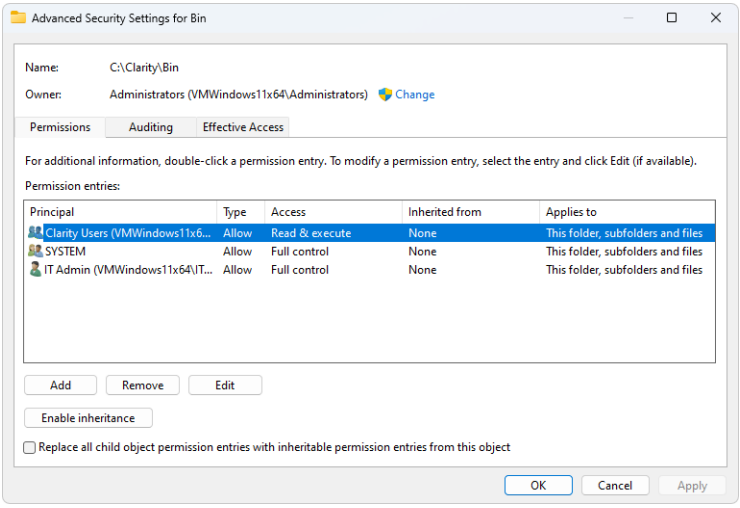


Fig. 17: Advanced Security Settings for Bin Folder

3.2 Clarity GLP Options

This step applies the basic regulated environment settings in Clarity. By default, all regulated environment options in Clarity station are disabled. To ensure **21 CFR Part 11** and GLP compliance, all the options should be enabled. In specific cases, it may be acceptable to disable certain options — provided this is clearly justified by the laboratory's internal policy.

3.2.1 SOP - Setting the GLP Options

To configure Clarity for basis regulated environment conditions, follow these steps:

Note: If the station has already User Accounts set up, only the user with *Administrator* access rights can open the ***GLP Options*** dialog.

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

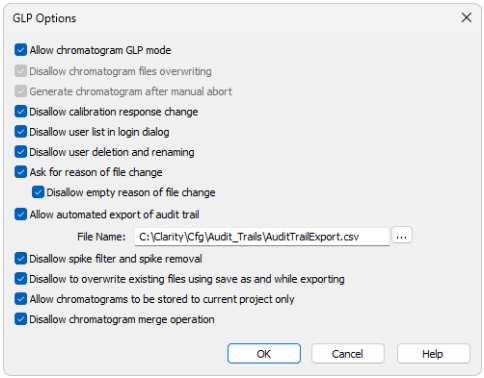


Fig. 18: GLP Options

- To prevent loss of any data from chromatograms, check the *Allow chromatogram GLP mode* checkbox. This option prevents overwriting of existing chromatograms and ensures that a chromatogram is generated even if an analysis is aborted for any reason. Chromatograms created in *GLP Mode* can be edited only on Clarity stations where *GLP Mode* is also enabled; on other stations, they will open as read-only.
- To prevent any manual edits of response values in the ***Calibration*** window, check the *Disallow calibration response change* checkbox. Although manual changes are recorded in the *Calibration Audit Trail*, they break the link between the calibration standard and the calibration itself and can affect the results of chromatograms linked to that calibration file.
- 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.

- To prevent users from being deleted or renamed in the *User Accounts* dialog, check the *Disallow user deletion and renaming* checkbox. This option ensures traceability and maintains integrity of user accounts.
- To require users to provide a reason for file changes, check the *Ask for reason of file change* checkbox. When saving or modifying a chromatogram, method, sequence, calibration or GPC calibration file or other Clarity settings (such as *System Configuration* or *User Accounts*), the *Reason for Chromatogram (Method, Sequence, ...) Change* dialog will appear, allowing the user to enter an explanation for the modification.

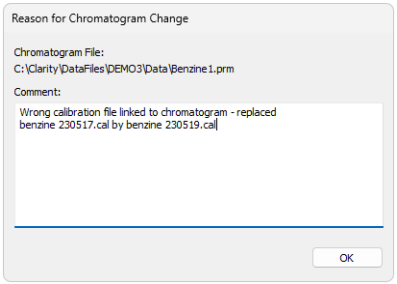


Fig. 19: Reason for Chromatogram Change

To ensure that the field is not left empty, check the *Disallow empty reason of file change* checkbox — only reasons containing text are accepted. The reason is then logged in *Audit Trail* next to the *Save file* information.

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. The exported audit trail file is marked as read-only while Clarity is running and is continuously updated during the session. Although this feature is not required by any regulated environment standard, it can help QA personnel review audit trails without accessing Clarity directly.
- To disallow the use of *Spike Filter* and *Spike Removal* operations, check the *Disallow spike filter and spike removal* checkbox. These functions can significantly alter the signal and potentially remove peaks. Although their use is logged in the *Audit Trail* and visible in the *Integration Table*, disabling them helps protect data integrity.
- To prevent users from overwriting existing files, check the *Disallow to overwrite existing files using save as and while exporting* checkbox. This option applies to all Clarity files. If a user attempts to overwrite an existing file, a warning message appears and the file must be saved under a different name.
- To ensure that new chromatograms are saved only within the current project, check the *Allow chromatograms to be stored to current project only* checkbox. The setting supports data integrity by ensuring that files are created only in locations with controlled access, as described in the chapter **"Computer User**

Rights" on pg. **6**.. A detailed description of this option can be found in *GLP Options of the Clarity main help*.

- To disable the chromatogram merge operation, check the *Disallow chromatogram merge operation* checkbox. This prevents users from combining multiple chromatograms into a single new file.

3.3 User Accounts in Clarity

Every user who has access to Clarity must have their own user account with a unique name and password and defined access rights specifying which actions they are allowed to perform. This requirement is mandated by both **21 CFR Part 11** and **GLP**.

One or more Clarity user should serve as a station administrator and have the *Administrator* rights on the Clarity station.

The *Administrator* is the only person authorized to create new user accounts in Clarity and to modify the access rights of existing users.

It is recommended to have two separate *Administrator* accounts with the same level of privileges, as password recovery is not supported in Clarity.

3.3.1 SOP - User Accounts - Administrator accounts setup

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

3.3.1.1 IT Administrator

The IT Administrator should have access to the Clarity station, but not to the analytical data (chromatograms, methods, etc.) created on that station. IT Administrator's main responsibilities are managing configuration settings, user account management, and maintaining a complete list of system users.

To set an IT Administrator account in Clarity, follow these steps:

- Open the Clarity station.
- In the main *Clarity* window, use the *System – User Accounts...* command to enter the *User Accounts* dialog. Click *New* to create new user account. Fill in the following fields:
  - *User Name*: Enter the desired user name.
  - *Desktop File*: Specify the desktop file name.
  - *Description* (optional)

Note: It is recommended to use the user's full name in the *User Name* field as it is then displayed in the *Audit Trail* and in reports, making it easier to identify who performed each action.

- Set the *Password Restrictions*. Define global password rules for all users. Specify the minimum password length (at least six characters are recommended, or follow your company's policy). Other parameters are optional and depend on applicable regulations.
- Set the password for the *IT Administrator* account. Click *Change Password* and enter a password that complies with the restrictions defined in the previous step.

- For the *IT Administrator* account, enable the following:
  - *Open User Accounts*
  - *Open Configuration*
  - *Open Audit Trail*
  - *Open Audit Trail Settings*
- Enable archiving privileges. To use Clarity *Archive* function, also enable:
  - *Access To* all instruments
  - *Archive / Restore*

Note: If an external tool is used for data backup, these options should remain disabled. Note that when an external tool is used, the changes will not be logged in *Audit Trail*. To comply with GLP requirements, it is necessary to use the *Archive* function.

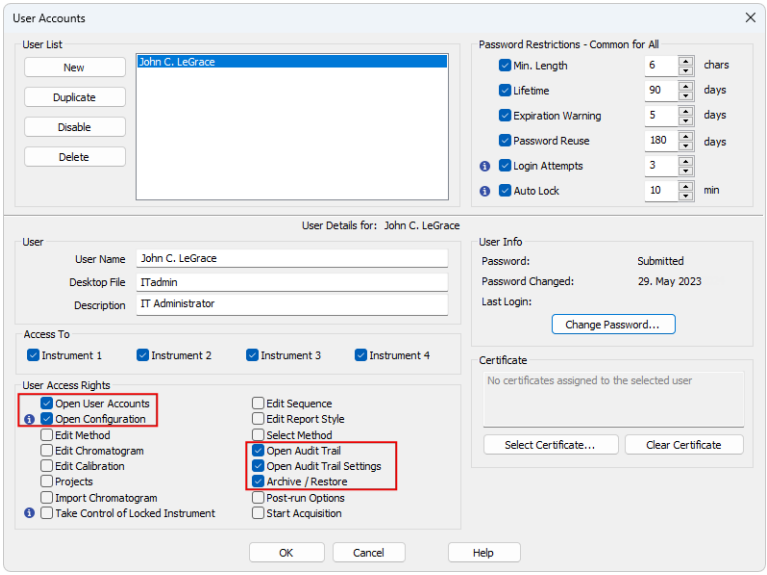


Fig. 20: User Accounts - Setting the IT Administrator account

3.3.1.2 Lab Administrator

Lab Administrator should have access only to data (chromatograms, methods, etc.) created on the Clarity station. *Lab Administrator*'s main responsibilities include allocating Chromatography Data System (CDS) resources to users, creating and maintaining projects, creating and verifying methods, custom calculations and reports, etc.

To set a Lab Administrator account in Clarity, follow these steps:

- Open the Clarity station.

- In the main *Clarity* window, use the *System – User Accounts...* command to enter the *User Accounts* dialog. Click *New* to create new user account. Fill in the following fields:
  - *User Name*: Enter the desired user name.
  - *Desktop File*: Specify the desktop file name.
  - *Description* (optional)

Note: It is recommended to use the user's full name in the *User Name* field as it is then displayed in the *Audit Trail* and in reports, making it easier to identify who performed each action.

- Assign the *User Access Rights*. The *Lab Administrator*'s rights depend on the laboratory's internal policy. The most common set of access rights is displayed in the picture below. However, the *Lab Administrator* should not be allowed to:
  - Modify the Clarity configuration. We recommend doing so, unless internal regulations state otherwise.
  - Change user accounts (except for assigning privileges to already existing users, where *Open User Accounts* access may be justified).
- Optional: Select the *Certificate* to be used for electronic signatures.

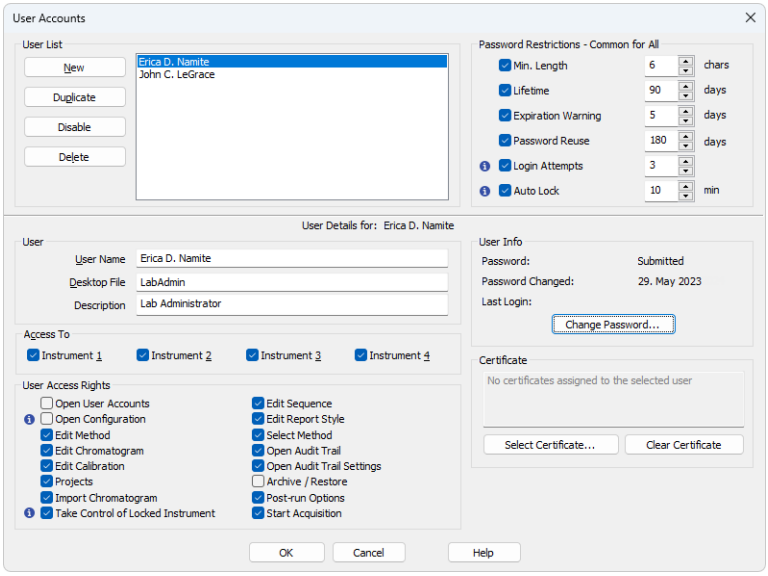


Fig. 21: User Accounts - Setting the Lab Administrator account

3.3.2 SOP - User Accounts - User account setup

To create a standard *User account* in Clarity, follow these steps:

- Open the Clarity station.
- In the main *Clarity* window, use the *System – User Accounts...* command to enter the *User Accounts* dialog. Click *New* to create new user account. Fill in the following fields:
  - *User Name*: Enter the desired user name.
  - *Desktop File*: Specify the desktop file name.
  - *Description* (optional)

Note: It is recommended to use the user's full name in the *User Name* field as it is then displayed in the *Audit Trail* and in reports, making it easier to identify who performed each action.

- Assign the *User Access Rights*. Access rights depend on the user's role and responsibilities. At minimum, the following checkboxes SHOULD NOT be checked for standard users:
  - *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 only to the person responsible for data archiving in the company. All other options listed above should remain restricted to *Administrators*. It is recommended to leave *Archive / Restore* privileges to the *IT Administrators* and/or *QA* personnel.

- The setting of the *User Accounts* dialog for the common user may be seen in the picture below:

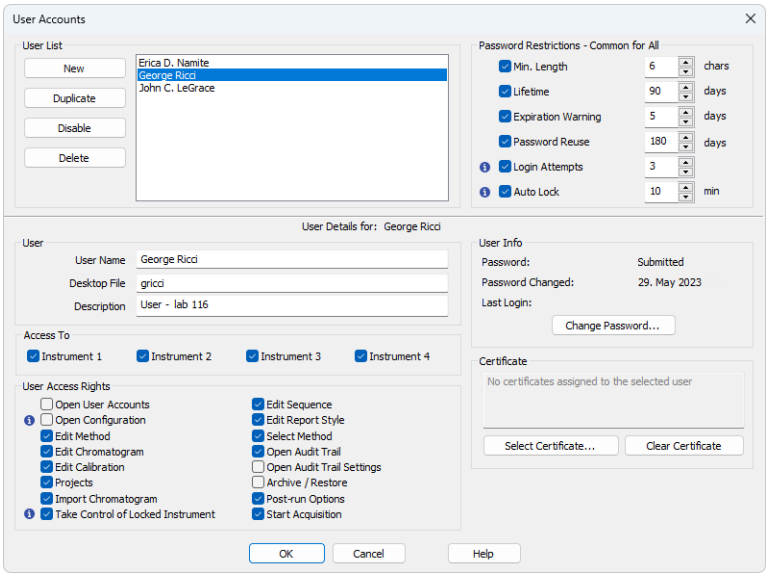


Fig. 22: User Accounts - Setting a User account

- Create all required *User accounts* the same way, then click *OK* to confirm and save the settings. You can also use the *Duplicate* function to create additional accounts more quickly with the same access rights.

3.3.3 SOP - User Accounts - QA account setup

QA personnel must have their own access to the Clarity station, without the authorization to modify any data. To set a QA user account in Clarity, follow these steps:

- Open the Clarity station.
- In the main *Clarity* window, use the *System – User Accounts...* command to enter the *User Accounts* dialog. Click *New* to create new user account. Fill in the following fields:
  - *User Name*: Enter the desired user name.
  - *Desktop File*: Specify the desktop file name.
  - *Description* (optional)

Note: It is recommended to use the user's full name in the *User Name* field as it is then displayed in the *Audit Trail* and in reports, making it easier to identify who performed each action.

- Set the *User Access Rights*. Most of the checkboxes must not be selected. Only the *Projects* and *Open Audit Trail* checkboxes should be enabled. Additional rights (e.g., *Post-run Options* or *Archive/Restore*) may be granted if allowed by company policy or regulatory requirements.

- The setting of the *User Accounts* dialog common for the QA user may be seen in the picture below:

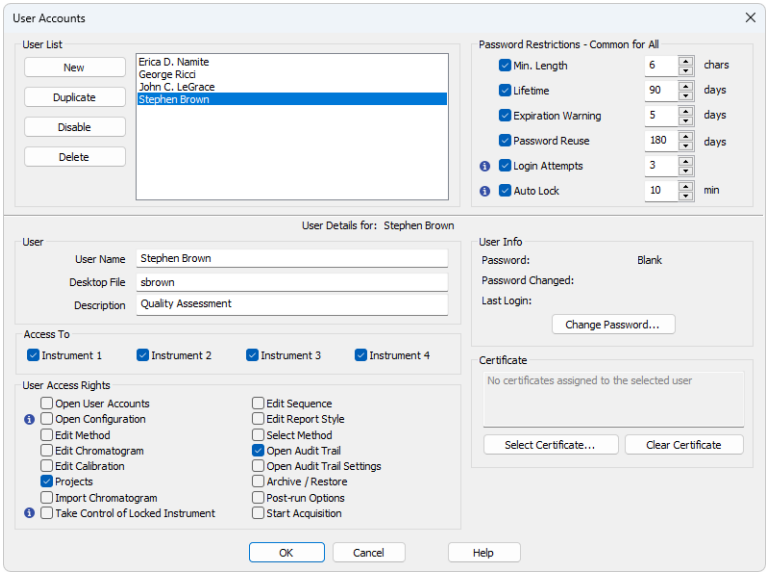


Fig. 23: User Accounts - Setting the QA worker account

3.4 Logging of all changes

All data changes in Clarity must be recorded in a secure *Audit Trail*, together with the reason for each change, as required by **21 CFR Part 11** and **GLP**.

To verify or adjust the logging settings, the user with the *Administrator* rights should perform the following steps:

3.4.1 SOP - setup logging in Audit Trail

Logging of all actions in Clarity's *Audit Trail* should be enabled by default. If these options were previously changed, follow these steps to enable it:

- Use the *System – Audit Trail* command from the *Clarity* main window to open the *Audit Trail* window.
- Log in with *User Name* and password.
- Use the *View - Properties...* command from the *Audit Trail* window to access the *Audit Trail Settings* dialog.
- Check all checkboxes on all tabs to ensure complete logging of system actions.
- Click *OK* to save the changes and close the dialog.

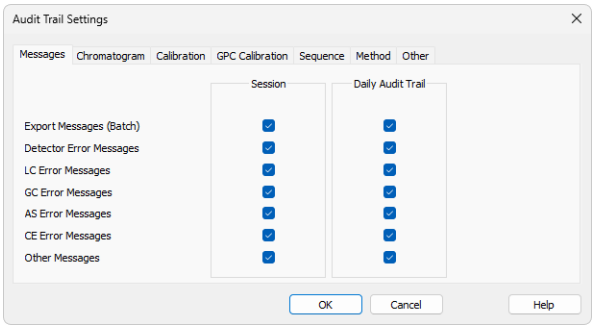


Fig. 24: Audit Trail Settings dialog

3.5 Logging reasons of changes

Each data modification must be accompanied by a recorded reason so that the cause of the change can be reviewed later.

This requirement is managed through the *GLP Options* dialog. For more details see the chapter **"SOP - Setting the GLP Options"** on pg. **17**.

3.6 Archiving the data

All data must be archived for the period specified by the relevant regulatory authorities. This requirement is mandated by **21 CFR Part 11** and **GLP**.

Note: The **FDA**'s version of the **GLP** specifies minimum record retention periods in § 58.195.

From the Clarity perspective, this requirement can be met by using the *Archive...* and *Restore...* commands available from the *Instrument* window. Alternatively, suitable external archiving software may be used.

Note: Archiving and restoring data should be only performed by users with *Administrator* rights.

3.6.1 SOP - the data archiving

It is recommended to use external tool to create regular backup of data and other files. However, entire projects can also be archived directly in Clarity by following these steps:

- A user with *Archive/Restore* privileges (typically an *Administrator* or *QA* personnel) must open Clarity and the *Instrument*.
- Use the *Instrument - Archive...* command on the *Instrument* window to open the *Backup* dialog.

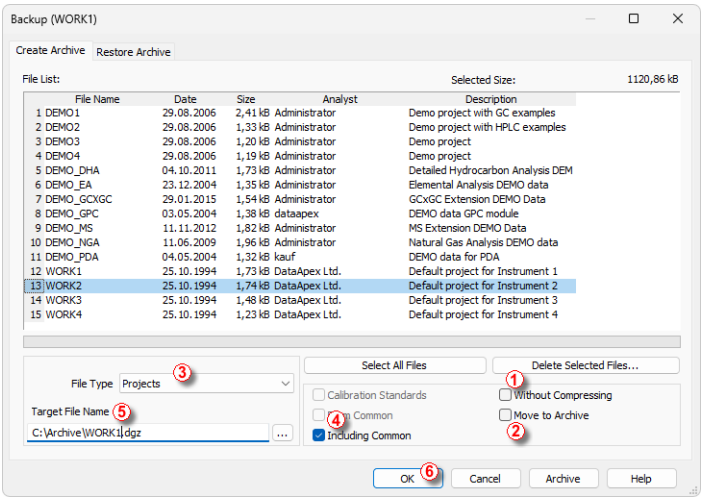


Fig. 25: Backup

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

Caution: If the *Move to Archive* ② option is selected, files will be deleted from their source folder. When the DataFiles folder has restricted permissions (as described in the chapter **"Computer User Rights"** on pg. **6**.), this operation can only be performed by a user with *Full Control* privileges - typically a local IT administrator.

- In the *File Type* field ③ , select *Projects*. The list of available projects will appear in the *File List*. Select the project you want to archive.
- Optionally, check *Include Common* to include any files that are stored in DATAFILES\COMMON ④ .
- In the *Target* field ⑤ , choose the path and the name of the archived file (*.DGZ extension).

Note: Do not save archive files directly to the root directory of the operating system (typically "C:\"). Due to *UAC - User Account Control* restriction in *Windows 7* and newer, it is safer to create and use a dedicated subfolder instead.

Caution: It is possible to disable deletion or alteration of created *.DGZ archives by adjusting the *Security Settings* of the *Target* folder ⑤ . These settings must be configured exactly as described in the chapter **"Computer User Rights"** on pg. **6**..

- Click *OK* ⑥ to archive the project and close the *Backup* dialog. Alternatively, you can use the *Archive* button to perform the operation without closing the dialog.

To ensure that the archived data set is complete, also archive the *Audit Trail* and *Configuration* files.

Note: Each data file in Clarity has its own *Audit Trail* log. Overall events, such as opening the Instruments or actions performed in the *Device Monitor*, are recorded in the *Station Audit Trail*.

Archiving Audit Trail Files

- Open the *Backup* dialog.
- Uncheck the *Without Compressing* checkbox ①. 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 entire Clarity station. If multiple instruments are available, deleting these files might also remove log data from other projects.

- In the *File Type* field ③, select the *Audit Trail Files*, then choose the appropriate files from the *File List*.
- Choose the path and the name of the archived file (*.DGZ extension) in the *Target* field ⑤. Be careful not to overwrite an existing project backup.
- Click *OK* ⑥ to archive and close the dialog, or use *Archive* to perform the operation without closing the window.

Archiving Configuration Files

Archiving the Clarity configuration file cannot be performed from within the Clarity environment. Although the configuration file is not required for processing further records, it is essential for ensuring the repeatability of measurements.

- A person with *Administrator* rights on the computer (not in Clarity - typically a company IT worker or laboratory supervisor) must open the file manager while Clarity is closed.
- Navigate to Clarity installation directory (C:\CLARITY by default).
- Locate the configuration file CLARITY.CFG (in C:\CLARITY\CFG by default).
- Copy this file to the same location as the other archived files.

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

3.7 Shared desktop file

If your laboratory uses special calculations defined via *User Columns*, all users must have these *User Columns* configured identically.

These settings are defined and stored in the desktop (*.dsk file). Since this file also contains user-specific preferences, such as the last opened documents and window layout, it is normally unique for each user.

To ensure consistency across users, it is necessary to use a shared desktop file that contains the common User Column settings and cannot be modified. To configure a shared desktop file, perform the following steps:

3.7.1 SOP - shared desktop file

To set up and secure a shared desktop file, follow these steps:

- 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.
- In the *User List*, select each user who should use the shared desktop. For each user selected, change the desktop file name in the *Desktop File* field to the desired name.

Note: The file name of the shared desktop corresponds to the file created under the account that prepared it. If the *Desktop File* field is left empty, Clarity automatically uses the default file, which has the same name as the user account.

- Click *OK* to confirm the changes and leave the ***User Accounts*** dialog.
- Close Clarity.
- Using the file manager, locate the desktop file in the Clarity installation directory (C:\CLARITY\CFG by default). The file name will match the one specified earlier and will have the .DSK extension.
- Open the file's Properties, then adjust the security settings so that users have only *Read & Execute* permissions. This change must be made using an account with Administrator privileges, in the same way as described in the chapter **"Computer User Rights"** on pg. **6**. Apply these restrictions to all operating system user accounts that should use this shared desktop file.
- Go to *Advanced Security Settings* of the targeted file to change privileges. Use *Disable inheritance* and select *Convert inherited permissions into explicit permissions on this object*. Modify the permissions for the selected groups or users so that they can access this file but cannot modify it, as shown in the image below.
- Ensure that the *Security Settings* for the CFG folder remain identical to those described in the chapter **"Computer User Rights"** on pg. **6**..

Note: Users will be able to modify the shared desktop temporarily while Clarity is open, but they will not be able to save these changes.

- Users that should be able to update the file must keep permissions inherited from the CFG folder.

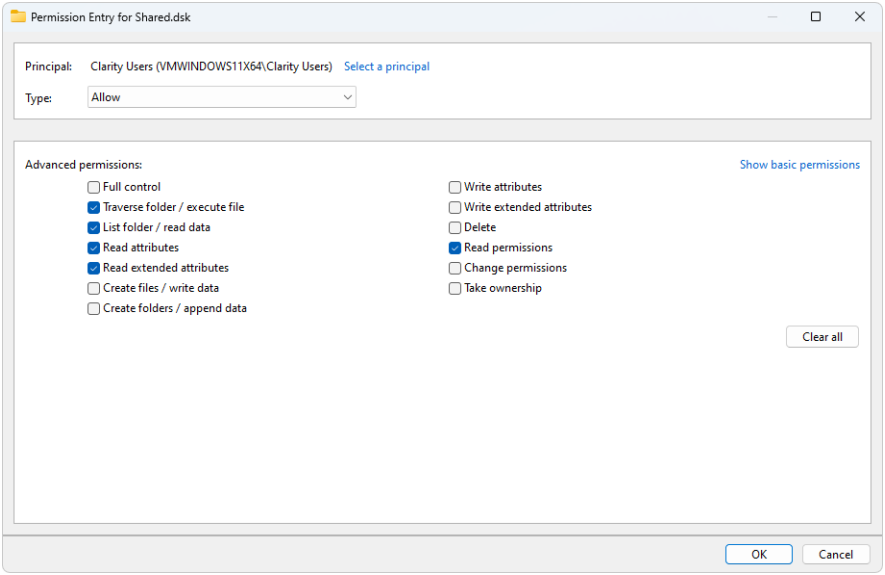


Fig. 26: Security Settings for Shared Desktop - User Entry - Windows 11

3.8 Electronic signatures

Clarity allows electronic data to be signed using electronic signatures that are unique to each individual, cannot be reassigned or reused, and cannot be altered. This feature is required by **21 CFR Part 11**.

Chromatograms in Clarity can be signed either under a Clarity user account or using a certificate. The certificate must include a private key protected by a password known only to the particular user, and the password must be entered each time the certificate is used.

Note: Certificates used for electronic signatures are not part of Clarity installation package. They must be obtained from an authorized certification authority. DataApex does not issue certificates for electronic signatures.

When using third-party certificates, ensure that each Windows user account used on a given computer has its own certificate installed in its Personal store. If multiple certificates for different Clarity users are installed under a single Windows account, there is a risk that chromatograms could be signed using another user's certificate. This is because Windows prompts for the certificate password only the first time a certificate is used during a session; subsequent signatures may reuse the same credentials automatically.

Each Clarity user should therefore use a dedicated Windows account with their own certificate installed in the personal certificate store. This setup is required when Clarity operates in a regulated environment using certificates issued by third- party certification authorities.

As an alternative, Clarity supports signing chromatograms using the credentials defined for each Clarity user through the *Sign as Current User* option in the ***Sign*** dialog.

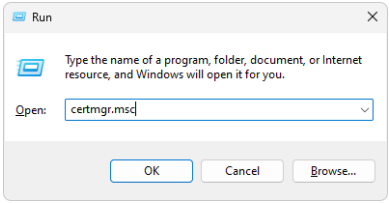
To set the certificate to a particular user, perform the following steps:

3.8.1 Setting certificates

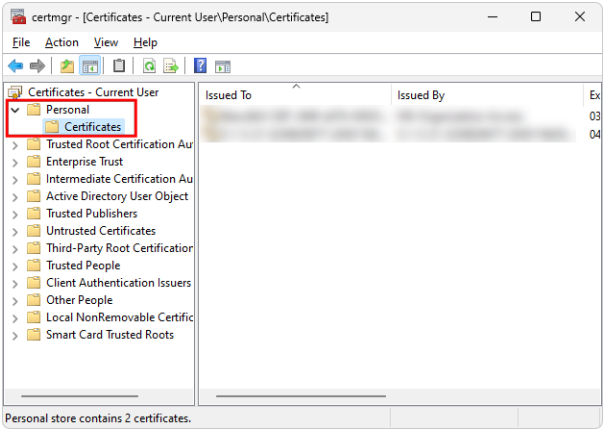
A certificate issued by an official certification authority is a file that can be installed on a given computer. The installation procedure is specific to the issuing authority and should be described in the documentation provided with the certificate.

3.8.1.1 Checking installed certificates:

- System *Administrator* should install the certificate by running the certificate file and following the procedure provided by the issuing certification authority. The exact installation steps may vary depending on the operating system, but the certificate must always be installed into the *Personal* certificate store.
- In Microsoft Windows, press the windows + R to open 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 detected by Clarity, which can be later selected in the *Select certificate* dialog in the ***User Accounts*** window.



3.8.1.2 Setting certificate for signing chromatograms:

- Clarity *Administrator* should start Clarity and open the ***User Accounts*** dialog (using the *System - User Accounts...* command).
- In the *User List* section (upper left corner), select the desired user.
- Click the *Select Certificate* button in the lower right part of the dialog. The ***Select Certificate*** dialog appears.
- Choose the appropriate certificate from the list and click *OK*. The selected certificate will be added to the corresponding user account.
- Set other certificates for other users, if desired, by repeating the aforementioned steps.
- Click *OK* to close the ***User Accounts*** dialog.

3.9 Multistation environment

When one or more users need to work on multiple computers, the user accounts (including passwords) must be identical on all Clarity stations. This can be achieved by copying the CLARITY.PSW file to the CFG directory (C:\CLARITY\CFG by default) on each computer.

Caution: The CLARITY.PSW file needs to be synchronized only after user accounts have been modified in the ***User Accounts*** dialog (for example, when adding users or changing access rights).

Because the Clarity installation directory should not be accessible to standard users, the system *Administrator* is responsible for copying the updated CLARITY.PSW file to all Clarity stations used in a multistation setup.

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

3.9.1 Multistation environment in network

If you want to operate multiple Clarity stations that share projects or data, use the Clarity in Network configuration. This setup allows several computers to work with the same projects or instruments while maintaining centralized data storage and control.

Detailed instructions for network installation and configuration can be found in the ***Clarity in Network*** manual.

When working in a multistation setup, it is important that users do not access or modify the same file (for example, a method, sequence, or chromatogram) from more than one station at the same time.

Clarity in Network can tolerate short network interruptions. If the connection is lost for a longer time or during data saving, an error message appears and Clarity automatically stores the data locally to prevent loss. Once the connection is restored, the next analysis must be started manually.

The files from the last analysis were saved locally during the network outage and can be found in C:\USERS<USERNAME>\APPDATA\LOCAL\TEMP\CLARITY. To

comply with GLP requirements, these files should be transferred back to the network directory using the Archive/Restore command so that the process is properly recorded in the Audit Trail.