



REGULATED ENVIRONMENT

Clarity Software

ENG

Code/Rev.: M132/80D
Date: 4/1/2019

Phone: +420 251 013 400
Fax: +420 251 013 401
clarity@dataapex.com
www.dataapex.com

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

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

1 What is a Regulated Environment	1
1.1 Good Laboratory Practice	1
1.2 CFR 21 Part 11	1
2 How to set Clarity	3
2.1 Computer installation	4
2.2 Installing Clarity	5
2.3 Specific settings	7
2.3.1 21 CFR Part 11 - requirements	7
2.3.1.1 Mandatory	7
2.3.2 GLP – requirements	8
2.3.2.1 Mandatory	8
2.3.2.2 Optional	8
3 Solutions and SOP's	10
3.1 Clarity GLP Options settings	10
3.1.1 SOP - GLP Options settings	10
3.2 Computer User Rights	13
3.2.1 SOP - Setting the user rights in Windows 7	14
3.2.2 SOP - Setting the user rights in Windows 8.1	24
3.2.3 SOP - Setting the user rights in Windows 10	32
3.3 User Accounts in Clarity	43
3.3.1 SOP - User Accounts - setup administrator account	43
3.3.2 SOP - User Accounts - setup user account	44
3.3.3 SOP - User Accounts - setup QA account	45
3.4 Logging of all changes	48
3.4.1 SOP - setup logging in Audit Trail	48
3.5 Logging reasons of changes	48
3.6 Archiving the data	49
3.6.1 SOP - the data archiving	49
3.7 Shared desktop file	52
3.7.1 SOP - shared desktop file	52
3.8 Multistation environment	58
3.9 Electronic signatures	59
3.9.1 Setting certificates	59

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:

Instrument (blue text) marks the name of the window to which the text refers.

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 (when you already are in the topic describing the window).

WORK1 (capitals) indicates the name of the file and/or directory.

ACTIVE (capital italics) marks the state of the station or its part.

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 4.
- Installing **Clarity** - see the chapter "**Installing Clarity**" on pg 5.
- Setting up the respective user accounts with appropriate privileges on the computer operating level - see the chapter "**Computer User Rights**" on pg 13.
- Setting **Clarity** to comply with the specific regulated environment requirements - see the chapter "**Specific settings**" on pg 7. and the chapter "**User Accounts in Clarity**" on pg 43.

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 - Pro, Enterprise*
- Microsoft Windows 8.1 - Pro, Enterprise*
- Microsoft Windows 10 - 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 **Windows 7 Professional, Windows 8.1 Pro** and **Windows 10 Pro**. When using another operating system, it may be necessary to change the sequence of steps.

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.
- Set the user accounts that will be needed on the computer (for more details see the chapter "**Computer User Rights**" on pg 13.).
- Install any other software required on the computer, along with its service packs and updates.
- Install **Clarity** (see the chapter "**Installing Clarity**" on pg 5.).

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 or the HW key 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) and press the *Next* button.
- Set the type of the installation on the next screen (or select the particular installation components in the bottom pane) and press 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.
- Enter the *User code*. This code may be found on the back side of the plastic card provided with **installation USB** or is provided by **DataApex** by e-mail. The installation will continue by the copying of the files to hard drive.

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.

- After the copying is finished, drivers for various hardware will need to be installed or updated. Click the *Next* button.
- When the updating is finished, it is necessary to register all *.DLL files. Click the *Finish* button to do so.
- Click the *Next* button in the next dialog. From the following 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. Print the IQ report, sign it and save it to be checked by the relevant authorities if need arises.

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.

- If you want to insert the internal A/D card, shut down the computer. Otherwise just restart it and skip the following step.
- Insert the internal A/D cards into the computer. After the computer starts, follow the given A/D card installation procedure described in the appropriate hardware manual.
- Insert the HW key into the USB slot and follow the installation procedure described in the **Clarity Getting Started** manual.

Note: If you have the serial (printer port) hardware key instead of the USB HW key, follow the procedure described in the **Clarity Getting Started** for the key type you have.

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 5.
- § 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 49.
- § 11.10 d, § 11.10 g - System access must be limited to authorized individuals - see the chapter "**Computer User Rights**" on pg 13. and the chapter "**User Accounts in Clarity**" on pg 43.
- § 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 48.
- § 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 59. the chapter "**Logging of all changes**" on pg 48.
- § 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 10. and the chapter "**Electronic signatures**" on pg 59. the chapter "**Logging of all changes**" on pg 48.
- § 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 43.

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 13.
- 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 13.
- 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 43.
- Every change in the data must be properly logged - see the chapter "**Logging of all changes**" on pg 48.
 - 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 48.
- All data must be archived for the period specified by appropriate authorities - see the chapter "**Archiving the data**" on pg 49.

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
- 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 52.
- 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 **58**.

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.

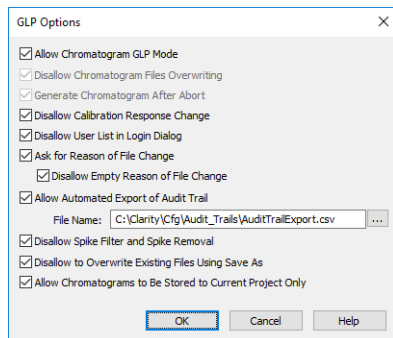


Fig 1: GLP Options

- 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 in 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.

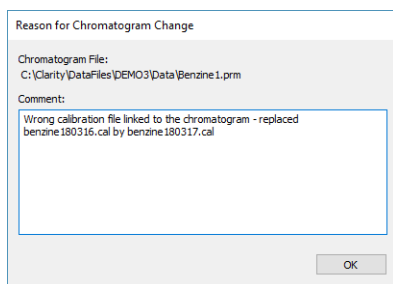


Fig 2: Reason for Chromatogram Change

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* 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 13. Detailed description of this feature is given in [GLP Options](#) topic of **Clarity** Help.

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** and **Windows 10 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** and **DataFiles** 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 7

Note: This SOP was prepared and tested on the computer with **Windows 7 Professional** operating system (English localization), Service Pack 1 and the latest updates (to the 28.7.2014) 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, click on *Windows Start* icon and type "Computer Management" text into search field and select *Computer Management* item. The *Computer Management* window will open. Navigate to item *Users* available under *Local Users and Groups* item.

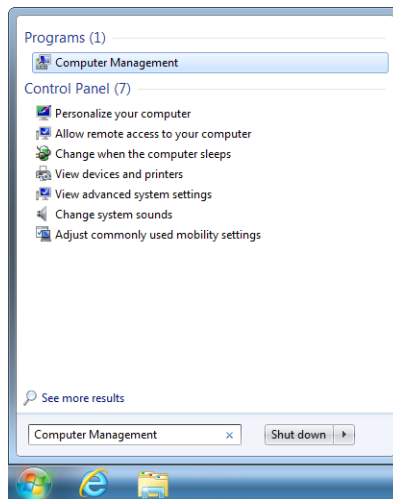
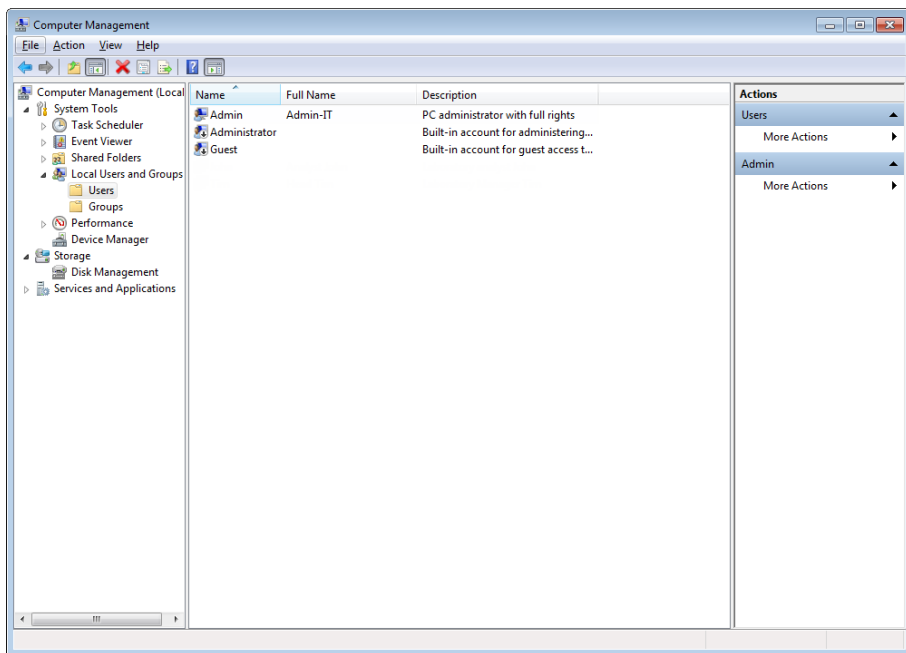


Fig 3: Start - Computer Management



- 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 and set password. Its setting is based on the policy of the organization where **Clarity** is installed and click *Create* button.

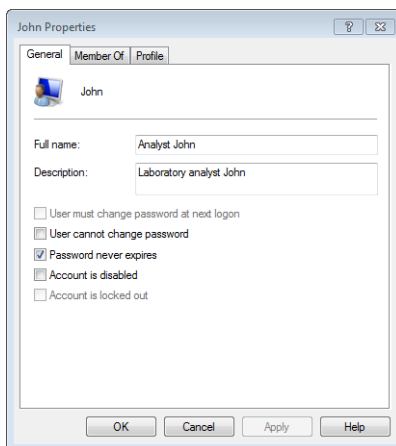


Fig 4: Create New User

- Repeat this procedure for each additional user you want to add.
- Check and assure that all user accounts of the of the users who should run Clarity are members of the *Users* group. To do that click on each created user and through right mouse button invoke context menu and select *Properties* and a new window will pop up. Then click on *Member Of* tab and check membership of the respective user in the user groups.

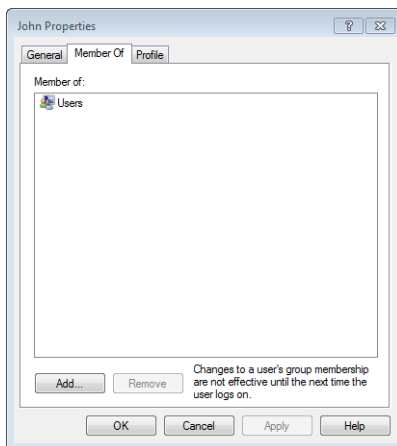


Fig 5: Users Group

- 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 **Cfg** and **DataFiles** 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 e.g. **Windows** explorer.
- Change the privileges for the user accounts you added earlier for the subfolders **Cfg** and **DataFiles** (wherever **DataFiles** subfolder is located):
 - 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.

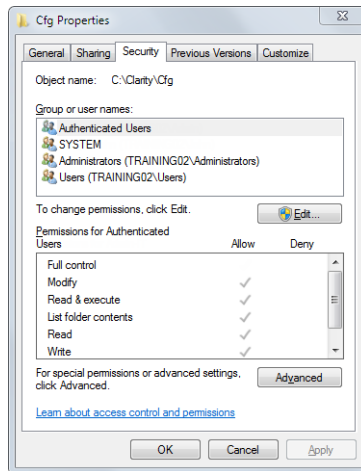


Fig 6: Cfg Folder Security Properties

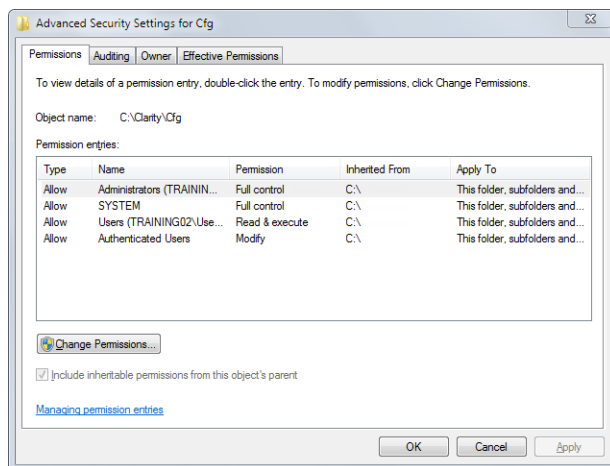


Fig 7: Advanced Security Settings - Initial state

- Click *Change permissions* button which invokes new window for permission settings. In the next dialog uncheck option *Include inheritable permissions from this object* which invokes *Windows Security* window. In this *Windows Security* window click *Remove* button which will result in cleared out Permission entries in *Advanced Security Settings for Cfg* window. Refer to next two screenshots below and the resulting cleared out *Advanced Security Settings* window.

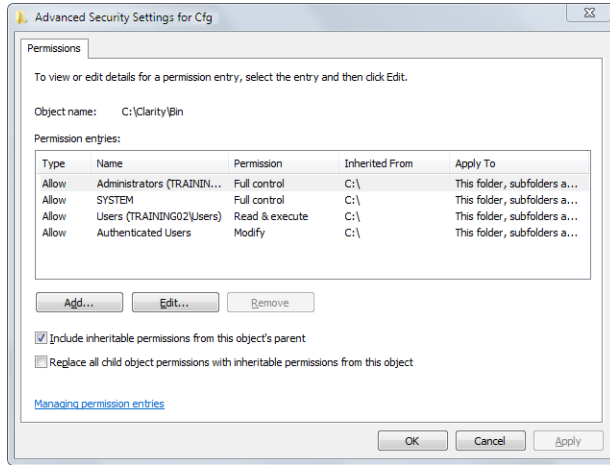


Fig 8: Advanced Security Settings - Intermediate state

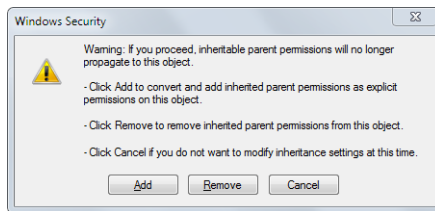


Fig 9: Windows Security

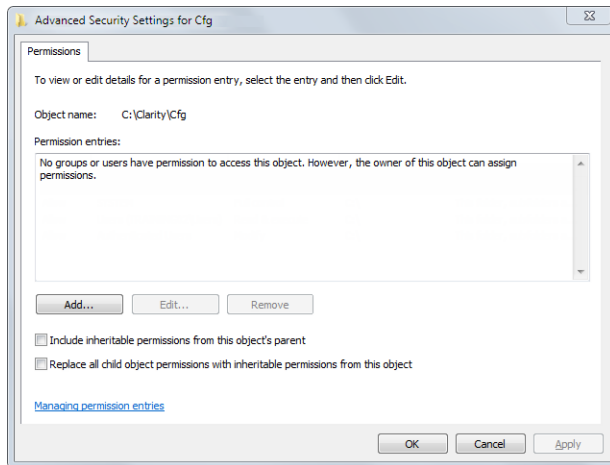


Fig 10: Advanced Security Settings - Cleared out state

- Click the *Add...* button to invoke a new window for selection of user or group. Click *Advanced* button which will invoke *Select User or Group* window. Click *Find Now* button and select a user account of the user who should run **Clarity**.

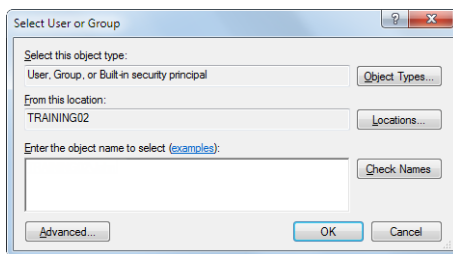


Fig 11: Select User - Initial

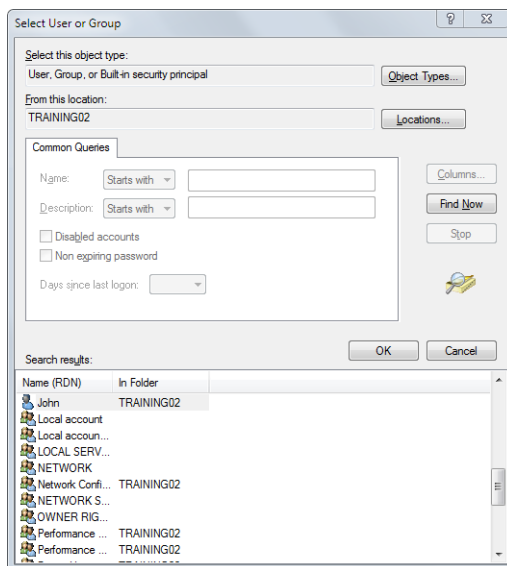


Fig 12: Select User - Intermediate

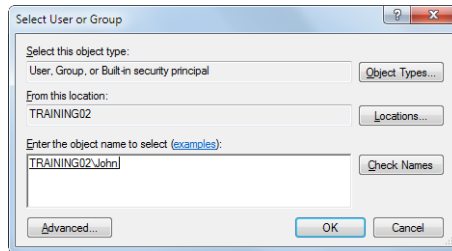


Fig 13: Select User - Final

- Select necessary permissions for user accounts of the users who should run **Clarity** as follows. Check **Full Control** item in the **Allow** column and then uncheck following items: **Delete Subfolders and Files**, **Delete**, **Change Permissions** and **Take Ownership**. Column **Deny** has to remain fully unchecked.

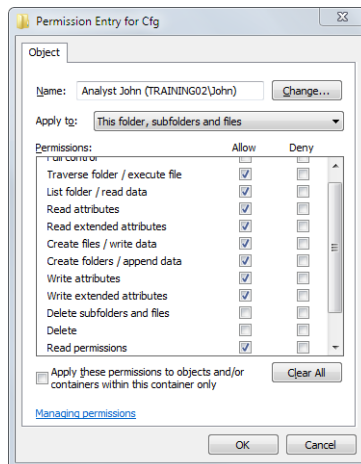


Fig 14: User Permission Entry

- Repeat this procedure for **Cfg** folder for all the user accounts of the users who should run **Clarity** and local **Administrator** user account also. **Administrator** user account should have all privileges listed in the **Allow** column, **Deny** column has to remain fully unchecked.

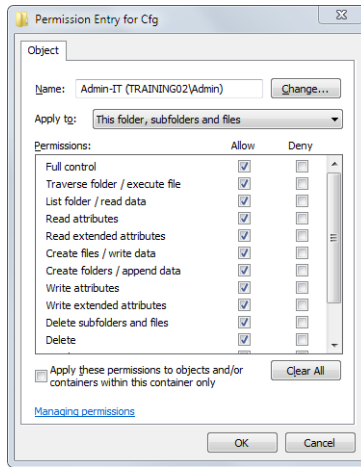


Fig 15: Administrator Permission Entry

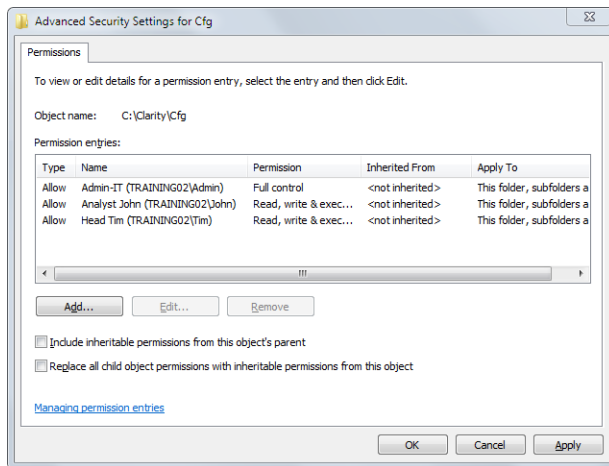


Fig 16: Advanced Security Settings for the Cfg Folder

- If needed, the settings can be reviewed for respective users from the Security tab in Cfg Properties window.

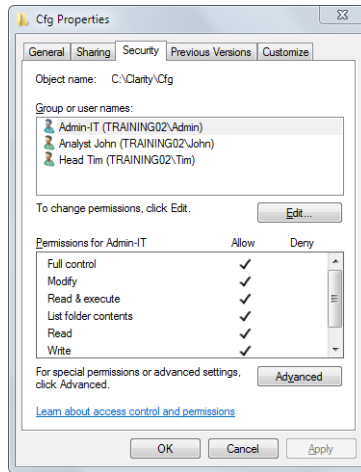


Fig 17: Administrator Cfg Folder Security Properties

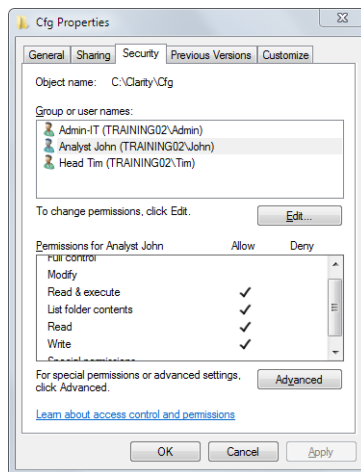


Fig 18: User Cfg Folder Security Properties

- Repeat this procedure for *DataFiles* folder for all the user accounts of the users who should run **Clarity** and the local *Administrator* user account in the same manner.

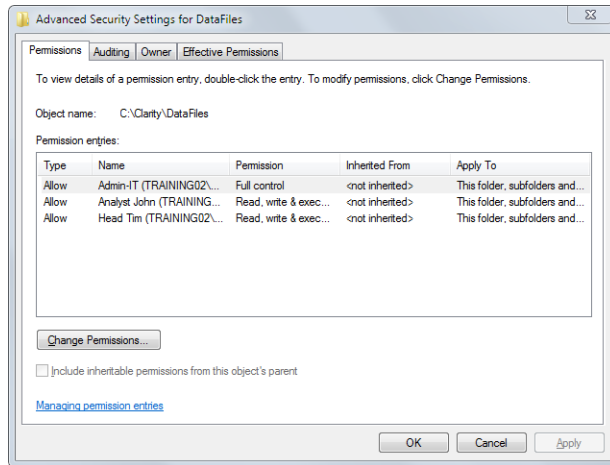


Fig 19: Advanced Security Settings for DataFiles Folder

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

3.2.2 SOP - Setting the user rights in Windows 8.1

Note: This SOP was prepared and tested on the computer with **Windows 8.1 Pro** operating system (English localization), all the latest updates (to the 28.7.2014) 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, right-click on the *Windows Start* icon to invoke context menu and select *Computer Management* item. In the **Computer Management** window, navigate to item *Users* available under *Local Users and Groups* item.

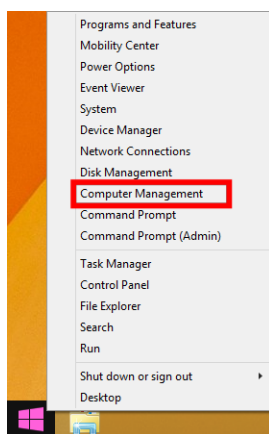


Fig 20: Start - Computer Management

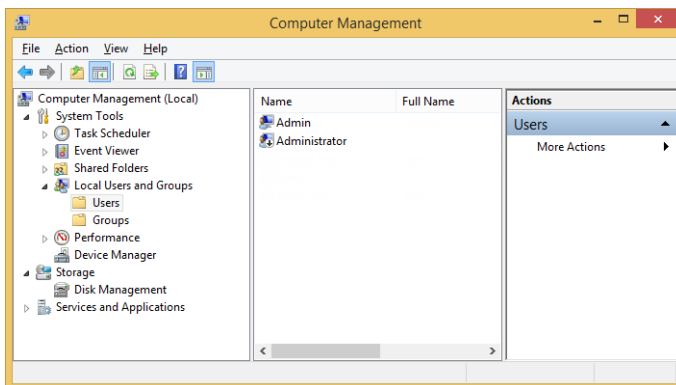


Fig 21: Computer Management

- 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.

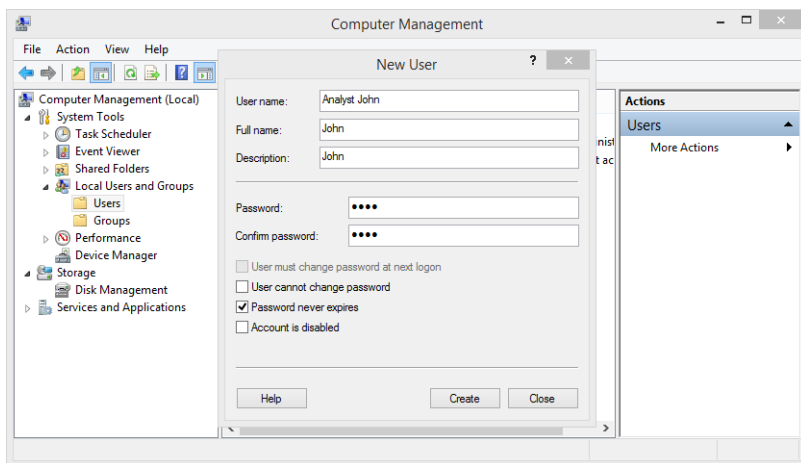


Fig 22: Create New User

- Repeat this procedure for each additional user you want to add.
- Check and assure that all user accounts of the of the users who should run Clarity are members of the *Users* group. To do that click on each created user and through right mouse button invoke context menu and select *Properties* and a new window will pop up. Then click

on *Member Of* tab and check membership of the respective user in the user groups.

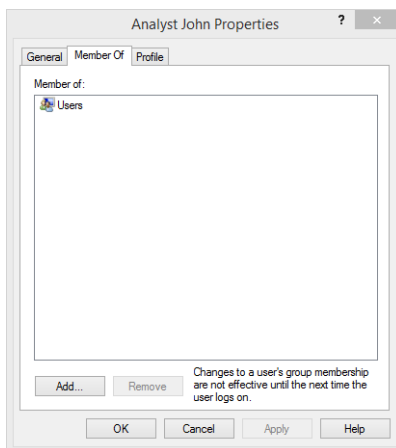


Fig 23: Users Group

- 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 **Cfg** and **DataFiles** 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 e.g. **Windows** explorer.
- Change the privileges for the user accounts you added earlier for the subfolders **Cfg** and **DataFiles** (wherever **DataFiles** subfolder is located):
 - 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.

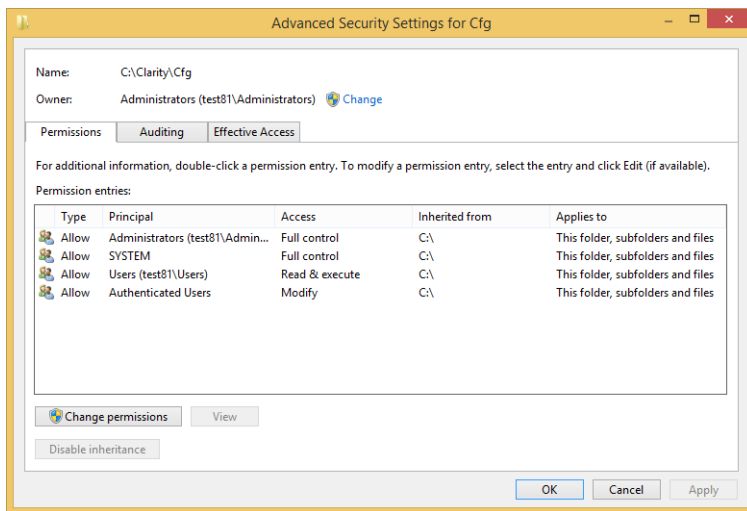


Fig 24: Advanced Security Settings

- Click *Change permissions* button which will invoke new window for settings of the permissions. In the following *Block Inheritance* window click the *Remove all inherited permissions from this object*. *Permissions* tab in *Advanced Security Settings* window should be cleared and without any listed permission entry.

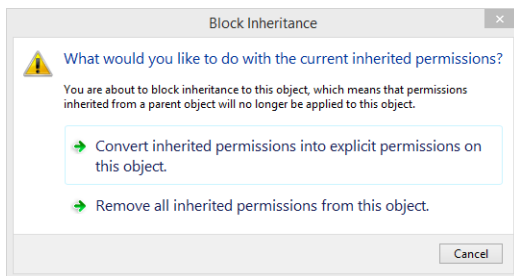


Fig 25: Blocking of permissions inheritance

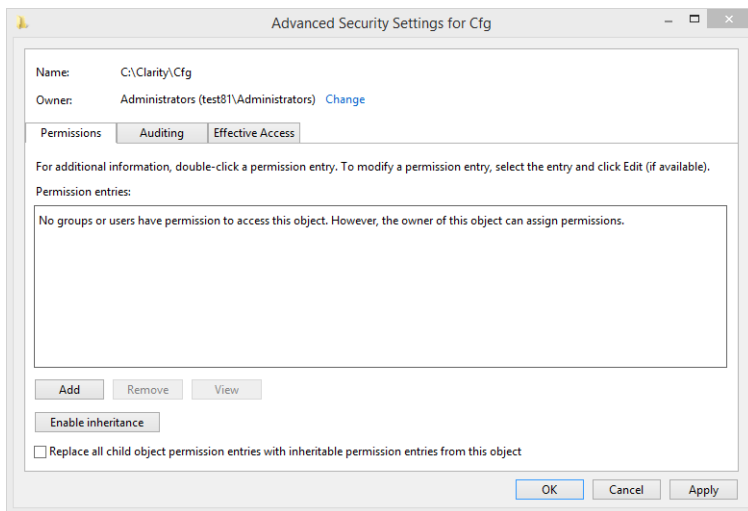
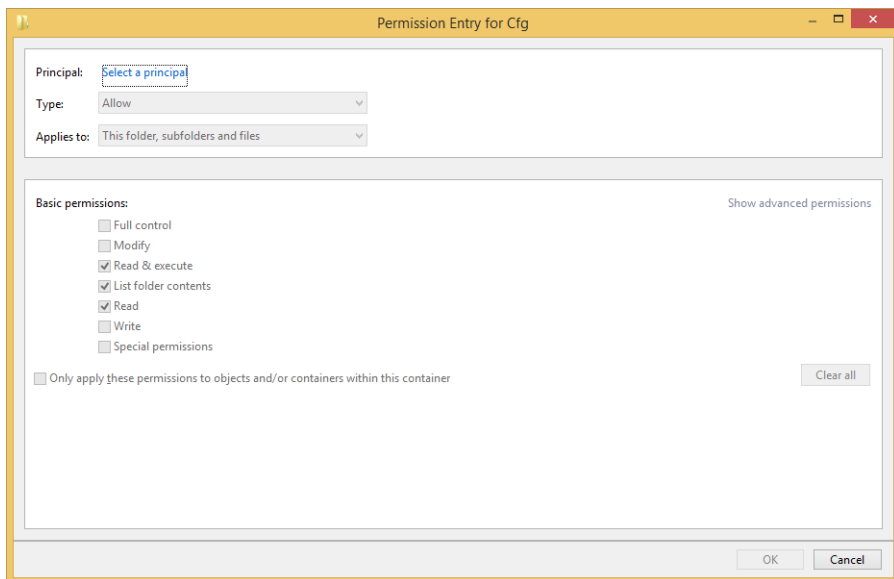


Fig 26: Empty Advanced Security Settings

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



- Using **Advanced** select user account of the user who should run **Clarity**.

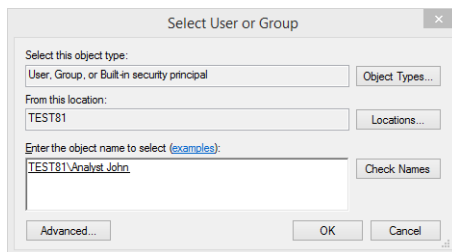


Fig 27: User Select

- Select necessary permissions for user accounts of the users who should run **Clarity** as follows. First of all, click the *Show advanced permissions*, check *Full Control* item and then uncheck following items: *Delete Subfolders and Files*, *Delete*, *Change Permissions* and *Take Ownership*. Perform these settings only for *Allow* item in *Type*: section in the upper part of the window.

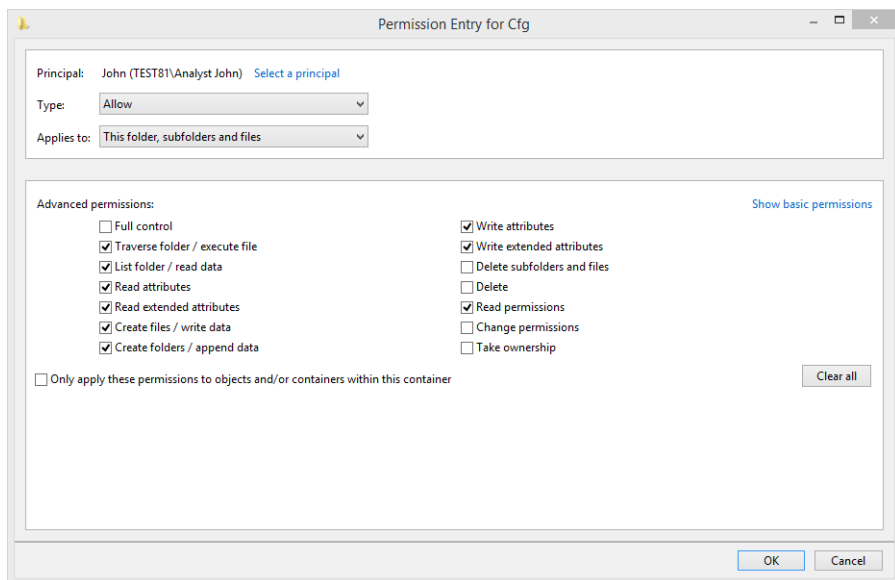


Fig 28: User Permissions

- Repeat this procedure for *Cfg* folder for all the user accounts of the users who should run **Clarity** and local *Administrator* user account also. *Administrator* user account should have all privileges.

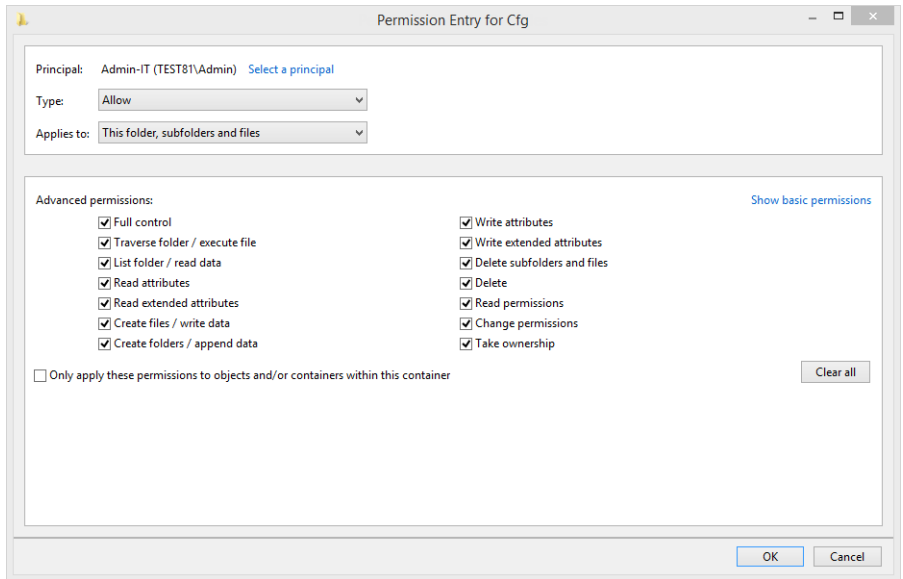


Fig 29: Administrator Permissions

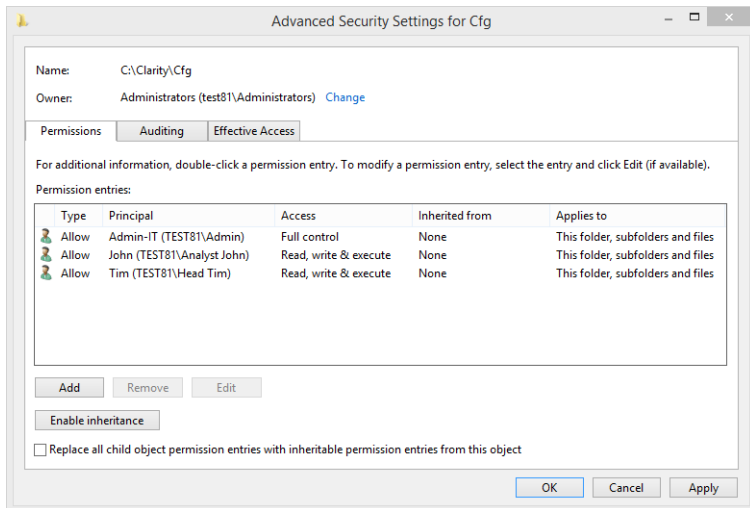


Fig 30: Advanced Security Settings for Cfg Folder

- Repeat this complete procedure for *DataFiles* folder for all the user accounts of the users who should run **Clarity** and local *Administrator* user account in the same manner.

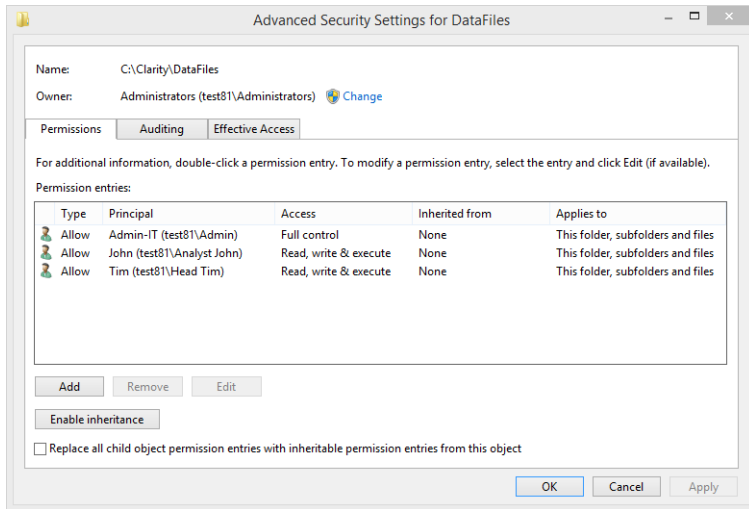


Fig 31: Advanced Security Settings for DataFiles Folder

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

3.2.3 SOP - Setting the user rights in Windows 10

Note: This SOP was prepared and tested on the computer with **Windows 10 Pro** operating system (English localization), all the latest updates (to the 22.6.2016) 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.

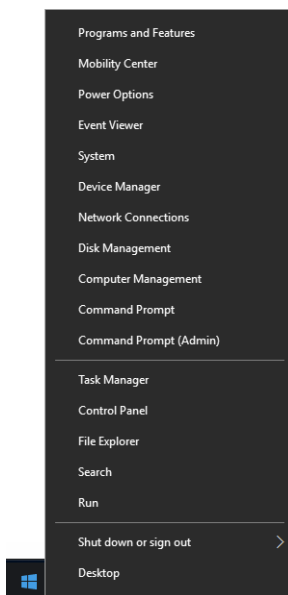


Fig 32: Windows - Computer Management

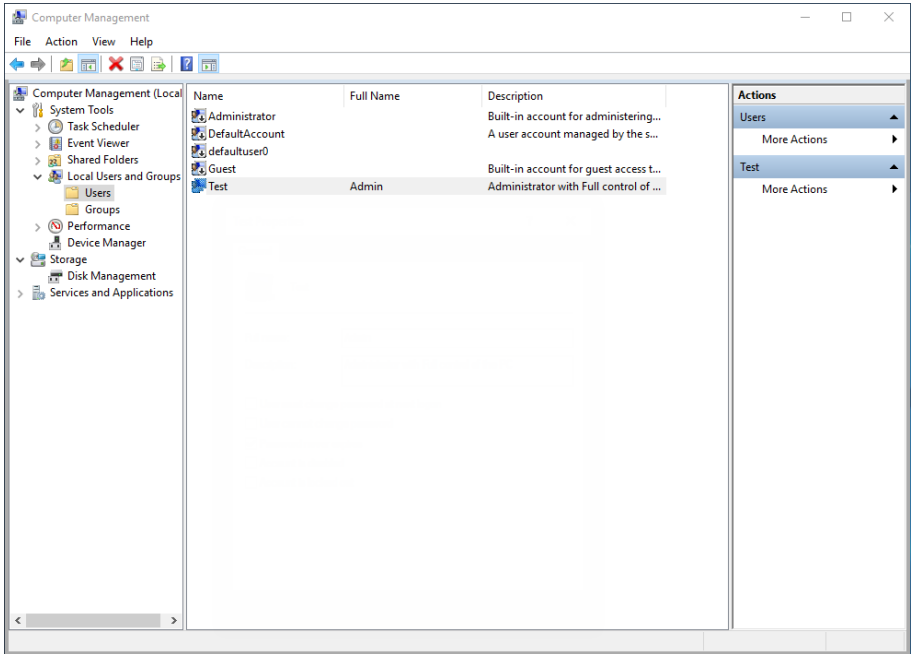


Fig 33: Computer Management

- 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.

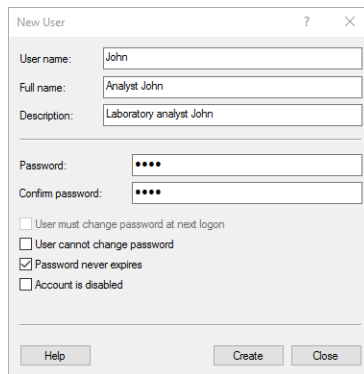


Fig 34: Create New User

- Repeat this procedure for each additional user you want to add.
- Check and assure that all user accounts of the of the users who should run Clarity are members of the *Users* group. To do that click on each created user and through right mouse button invoke context menu and select *Properties* and a new window will pop up. Then click on *Member Of* tab and check membership of the respective user in the user groups.

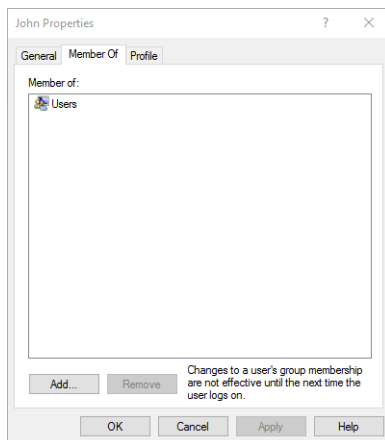


Fig 35: Users Group

- 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 **Cfg** and **DataFiles** 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 e.g. **Windows** explorer.
- Change the privileges for the user accounts you added earlier for the subfolders **Cfg** and **DataFiles** (wherever **DataFiles** subfolder is located):
 - 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.

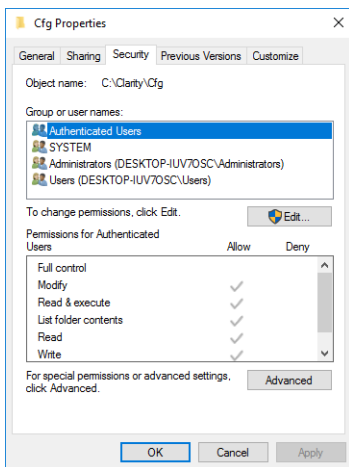


Fig 36: Cfg Folder Security Properties

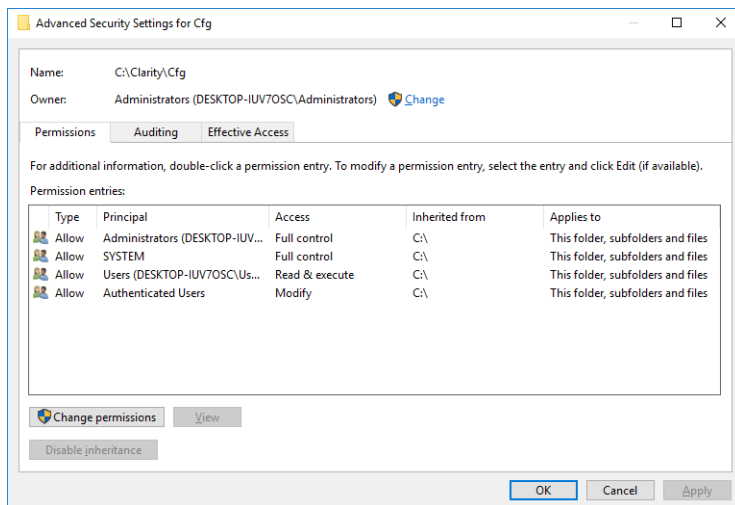


Fig 37: Advanced Security Settings - Initial state

- 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.

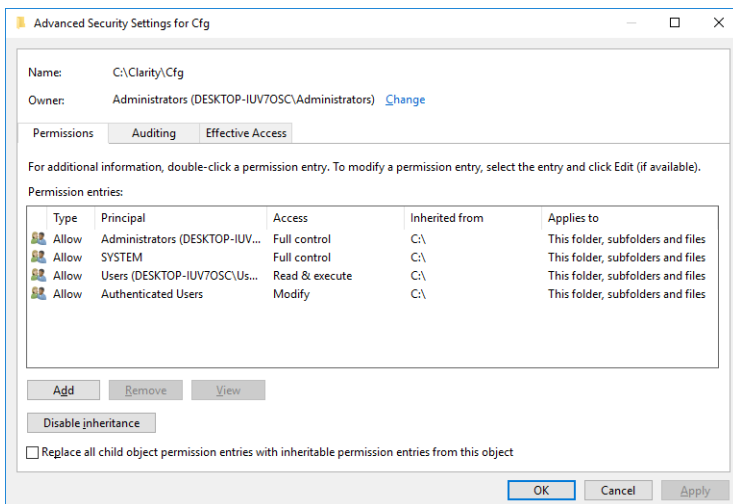


Fig 38: Advanced Security Settings - Intermediate state

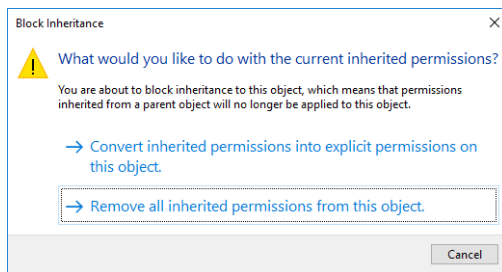


Fig 39: Block inheritance

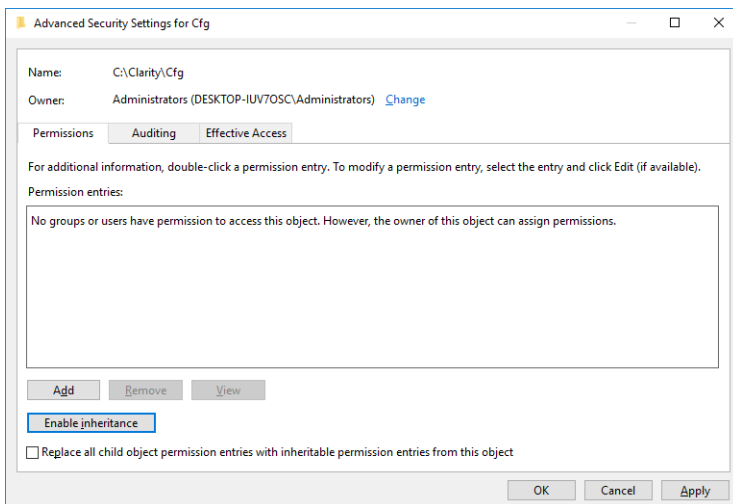
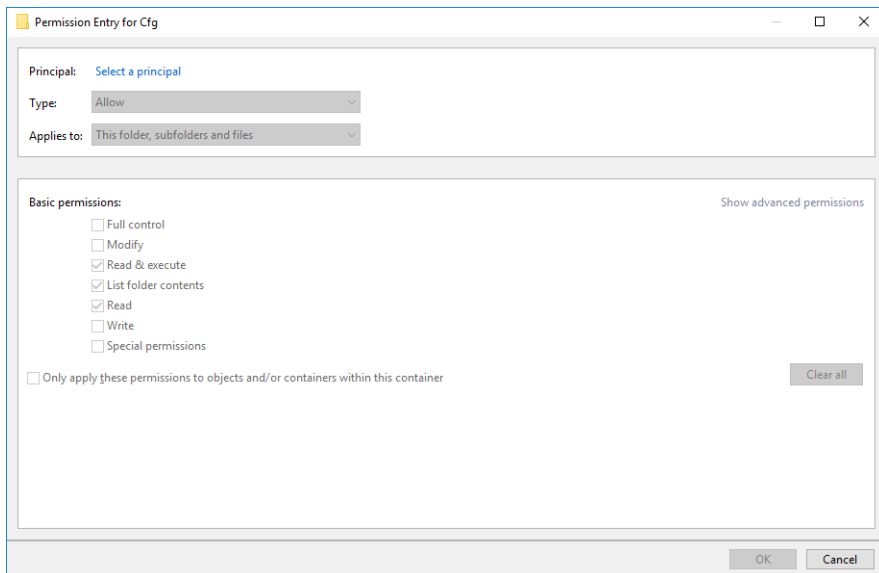


Fig 40: Advanced Security Settings - No Entry

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



- Click the **Advanced...** button to select user who should run **Clarity**.

Fig 41: Permission Entry

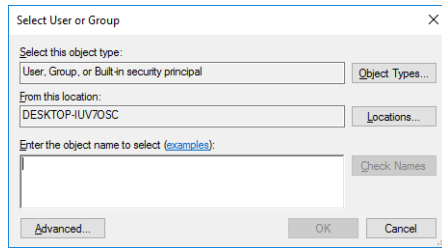


Fig 42: Select User - Initial

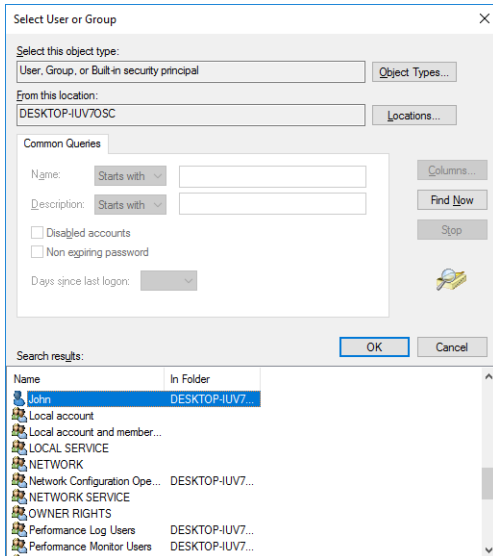


Fig 43: Select User - Intermediate

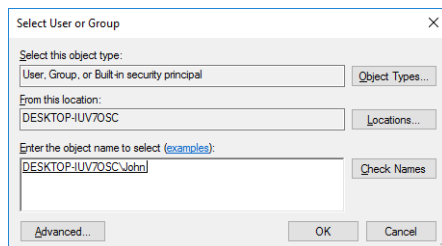


Fig 44: Select User - Final

- Select necessary permissions for user accounts of the users who should run **Clarity** as follows. First of all, click the *Show advanced permissions*, check *Full Control* item and then uncheck following

items: *Delete Subfolders and Files, Delete, Change Permissions and Take Ownership*. Perform these settings only for *Allow* item in *Type*: section in the upper part of the window.

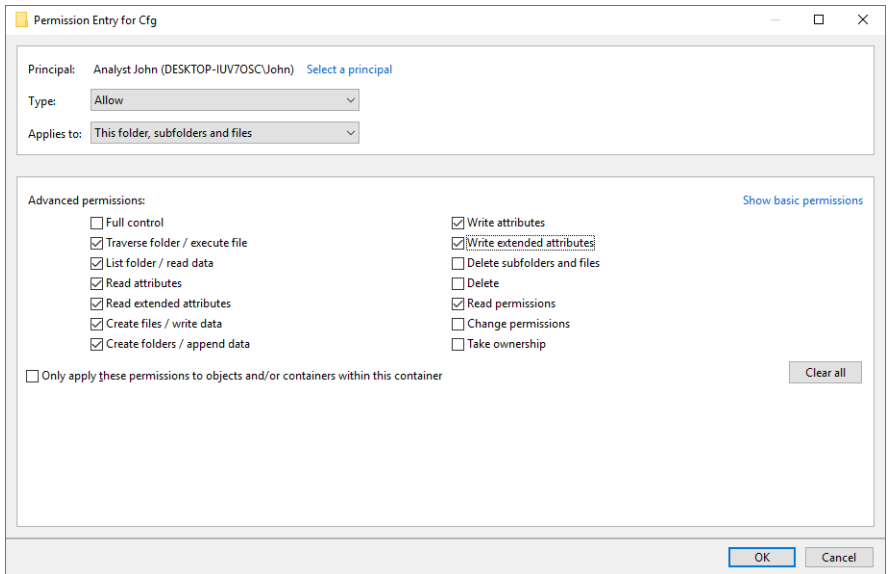


Fig 45: User Permission Entry

- Repeat this procedure for *Cfg* folder for all the user accounts of the users who should run **Clarity** and local *Administrator* user account also. *Administrator* user account should have all privileges.

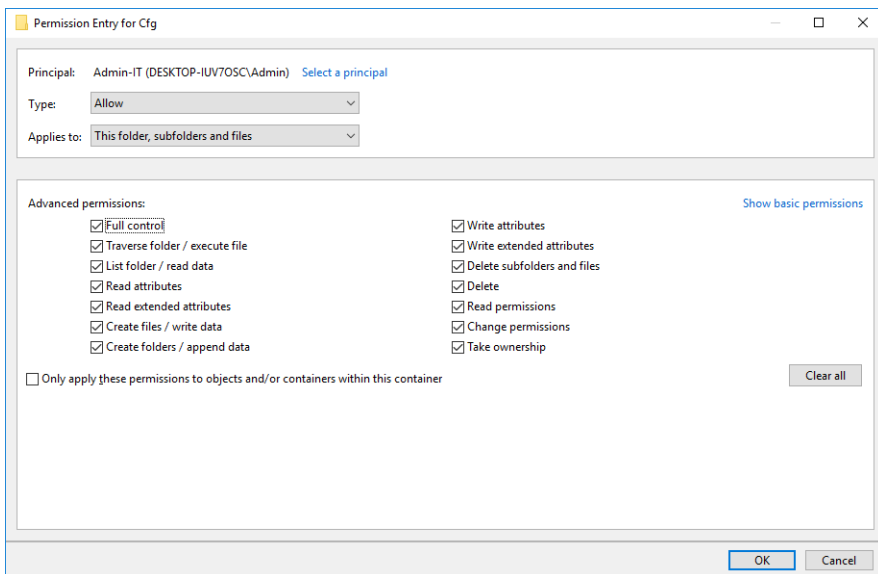


Fig 46: Administrator Permission Entry

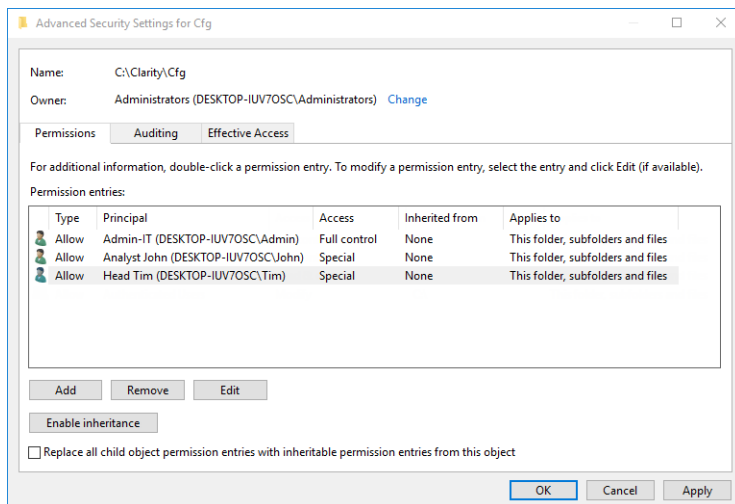


Fig 47: Advanced Security Settings for the Cfg Folder

- If needed the settings can be reviewed for respective users from the *Security* tab in *Cfg Properties* window.

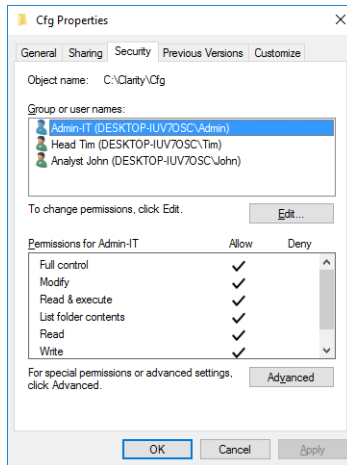


Fig 48: Administrator Cfg Folder Security Properties

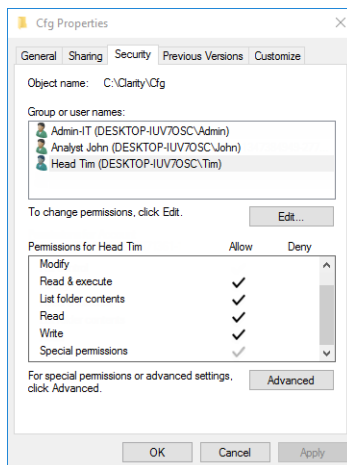


Fig 49: User Cfg Folder Security Properties

- Repeat this complete procedure for *DataFiles* folder for all the user accounts of the users who should run **Clarity** and local *Administrator* user account in completely same manner.

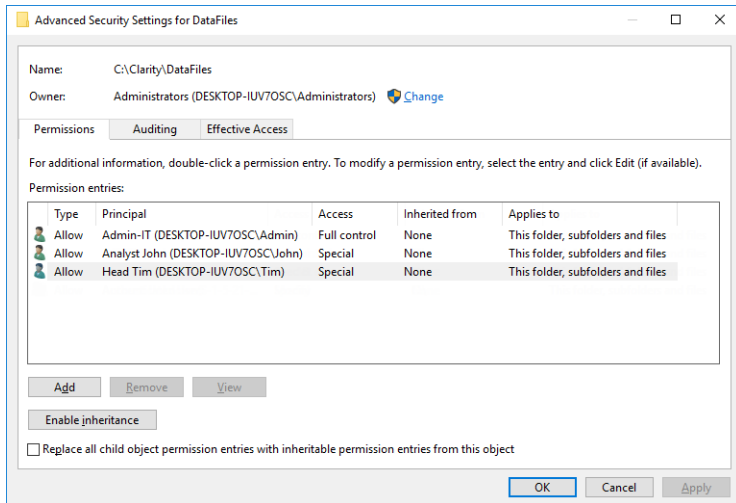


Fig 50: Advanced Security Settings for DataFiles Folder

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

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 account

- 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 *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 *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, other fields are optional.

Note: Set the *Min. Length* to at least 6 characters or according to the rules set in your company. Sample settings are shown in the **Fig 51** on pg **44**.

Fig 51: User Accounts - Setting the Administrator

- Use the *Change Password* button to set the *User Password* for your *Administrator* account. The password must comply with the *Password Restrictions* set in the previous step.
- Set the *User Access Rights* for the *Administrator* account.

Note: The *Administrator* account must have rights for *Open User Accounts* and *Open Configuration* checked to successfully set the **Clarity** station to regulated environment conditions.

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 52.) and the *Description* fields.
 - Set the *User Access Rights* for the user account. The following checkboxes **MUST** be unchecked:

- *Open User Accounts*
- *Open Configuration*
- *Open Audit Trail Settings*
- *Archive / Restore*

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 Administrator**. We recommend leaving the *Archive / Restore* privileges to the **Clarity Administrator** 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:

The screenshot shows the 'User Accounts' dialog box with the following details:

- User List:** A list containing 'Gheorge Ricci' and 'John LeGrace'. A 'New' button is highlighted.
- Password Restrictions - Common for All:**
 - Min. Length: 4 [Chars.]
 - LifeTime: 90 [Days]
 - Expiration Warning: 5 [Days]
 - Password Reuse: 85 [Days]
 - Auto Lock: 10 [min]
- User Details for: Gheorge Ricci**
 - User:**
 - User Name: Gheorge Ricci
 - Desktop File: gricci
 - Description: User -lab 116
 - User Info:**
 - Password: Submitted
 - Password Changed: 05. prosinec 2018
 - Last Login:
 - Change Password...
 - Other Users Can:**
 - Read & Write (selected)
 - Read
 - No Access
 - Access To:**
 - Instrument 1
 - Instrument 2
 - Instrument 3
 - Instrument 4
 - User Access Rights:**
 - Open User Accounts
 - Open Configuration
 - Edit Method
 - Edit Chromatogram
 - Edit Calibration
 - Projects
 - Import Chromatogram
 - Edit Sequence
 - Edit Report Style
 - Select Method
 - Open Audit Trail Settings
 - Archive / Restore
 - Post Run Settings
 - Start Acquisition
 - Certificate:**
 - No certificates assigned to the selected user
 - Select Certificate...
 - Clear Certificate
 - Certificate For Exporting To PDF: C:\MyCcert\mycert.pfx

Fig 52: User Accounts - Setting the User

- Create another user account or leave the **User Accounts** dialog by pressing 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 52.) 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 53** on pg 46.:

The screenshot shows the 'User Accounts' dialog box. The 'User List' contains three users: Gheorge Ricci, John LeGrace, and Stephan Brown. The 'User Details for: Stephan Brown' section is expanded, showing the following fields: User Name (Stephan Brown), Desktop File (sbrown), and Description (Quality Assesment). The 'User Access Rights' section is also expanded, showing the following checkboxes: Open User Accounts, Open Configuration, Edit Method, Edit Chromatogram, Edit Calibration, Projects (checked), Import Chromatogram, Edit Sequence, Edit Report Style, Select Method, Open Audit Trail Settings, Archive / Restore, Post Run Settings, and Start Acquisition. The 'Password Restrictions - Common for All' section is visible at the top right, showing settings for Min. Length (4), LifeTime (90), Expiration Warning (5), Password Reuse (85), and Auto Lock (10). The 'User Info' section shows Password (Blank), Password Changed, and Last Login. The 'Certificate' section shows 'No certificates assigned to the selected user' and a 'Certificate For Exporting To PDF' field with the value 'C:\MyCcert\mycert.pdf'.

Fig 53: User Accounts - setting the QA worker

- Ensure that all other users do not have the *Other Users Can* section ① switched to *No Access* option.
- Leave the [User Accounts](#) dialog by pressing the *OK* button.

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 **10**.

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

To save space during the data archiving, it is possible to use compressed archives of whole projects. To do so:

- 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.

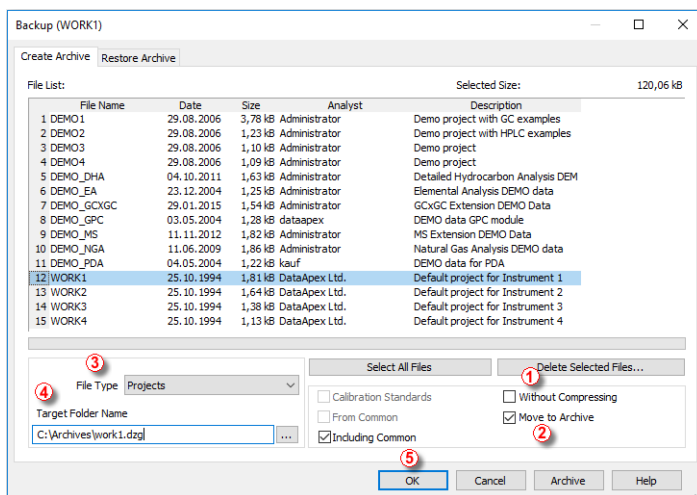


Fig 54: Backup

- Uncheck the **Without Compressing** checkbox ①.
- Check the **Move to Archive** checkbox ②.

Note: If you just want to archive the files, without deleting the source files, do not check the **Move to Archive** checkbox.

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 13. the moving to archive (=deleting of the files) can be done only by the person with *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.
- Choose the path to and the name of the archived file (*.DGZ extension) in the *Target* field ④.

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 it 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 is possible to disable deletion or alteration of created *.DGZ archives. The *Security Settings* for the folder stated in the *Target* field ④ has to be completely the same as described in the chapter "**Computer User Rights**" on pg 13. In this case, it is necessary to follow guidance given in the respective subchapter of the chapter "**Computer User Rights**" on pg 13. based on used *Windows* version.

- 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 its 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 ④. Take care not to overwrite the backed-up project.
- 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.
- 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\BIN 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.

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 be become read-only. This should be only done *Windows* user account with *Administrator* privileges by the same manner as described the chapter "**Computer User Rights**" on pg 13. This setting should be done for all *Windows* user accounts of the **Clarity** users who should use this selected shared desktop file.
- 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 13..
- 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*.

- **Windows 7:**

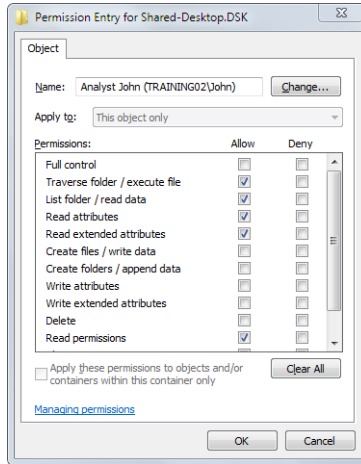


Fig 55: Security Settings for Shared Desktop - User Entry

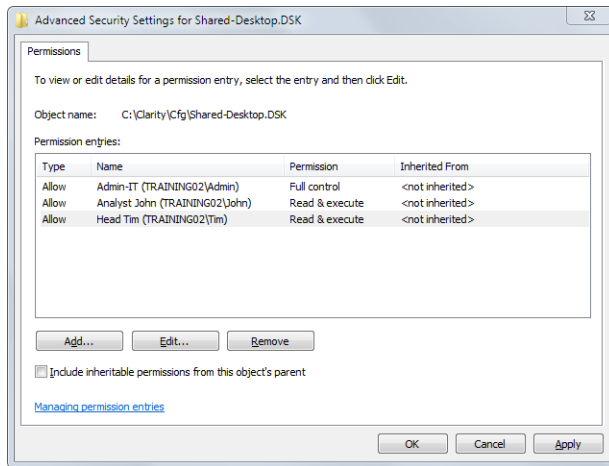


Fig 56: Security Settings for Shared Desktop - Advanced Settings - 1

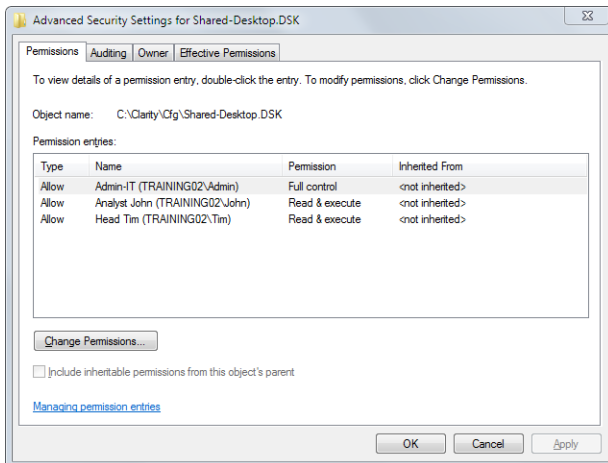


Fig 57: Security Settings for Shared Desktop - Advanced Settings - 2

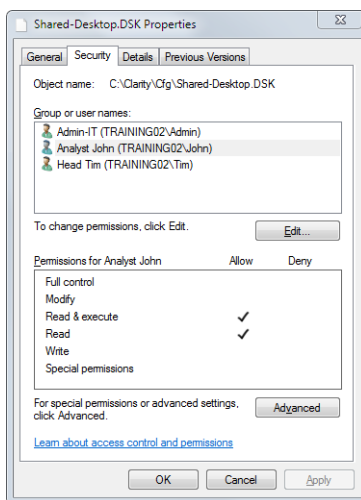


Fig 58: Security Settings for Shared Desktop - Security Overview

- **Windows 8.1:**

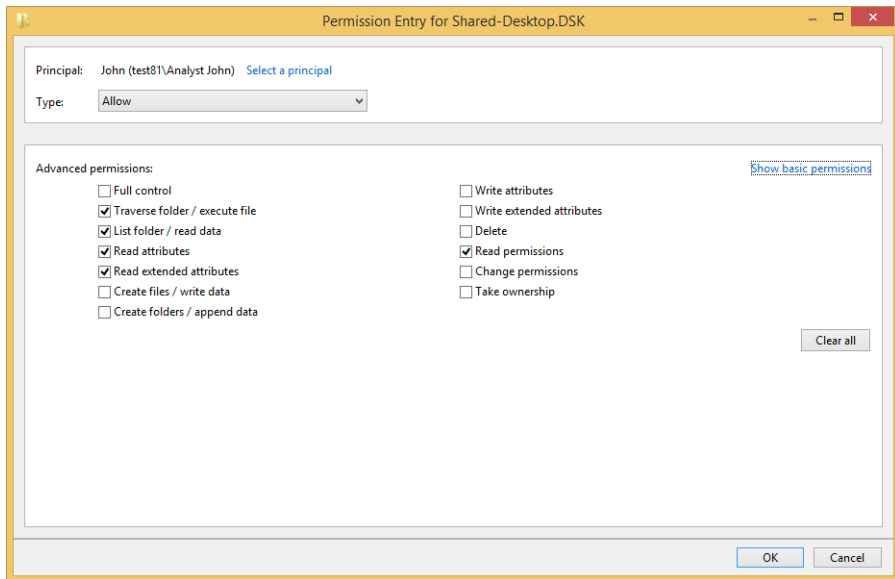


Fig 59: Security Settings for Shared Desktop - User Entry

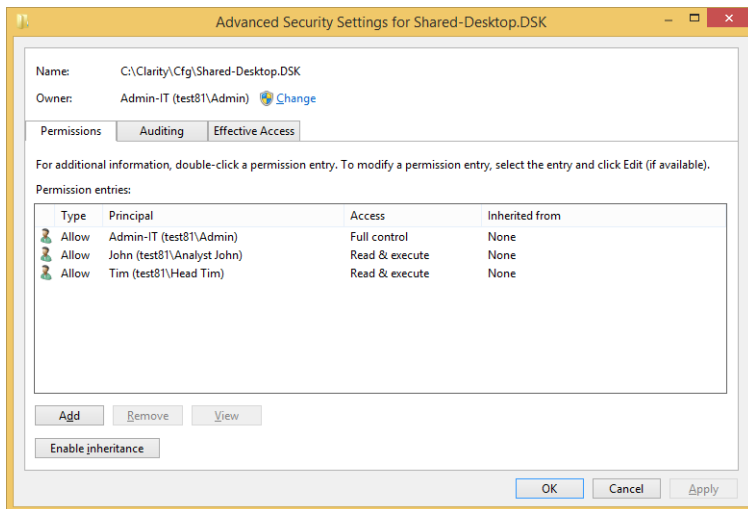


Fig 60: Security Settings for Shared Desktop - Advanced Settings

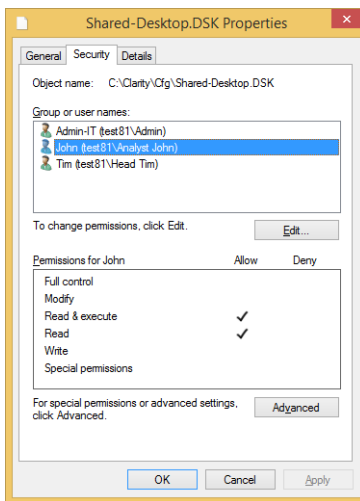


Fig 61: Security Settings for Shared Desktop - Security Overview

• **Windows 10:**

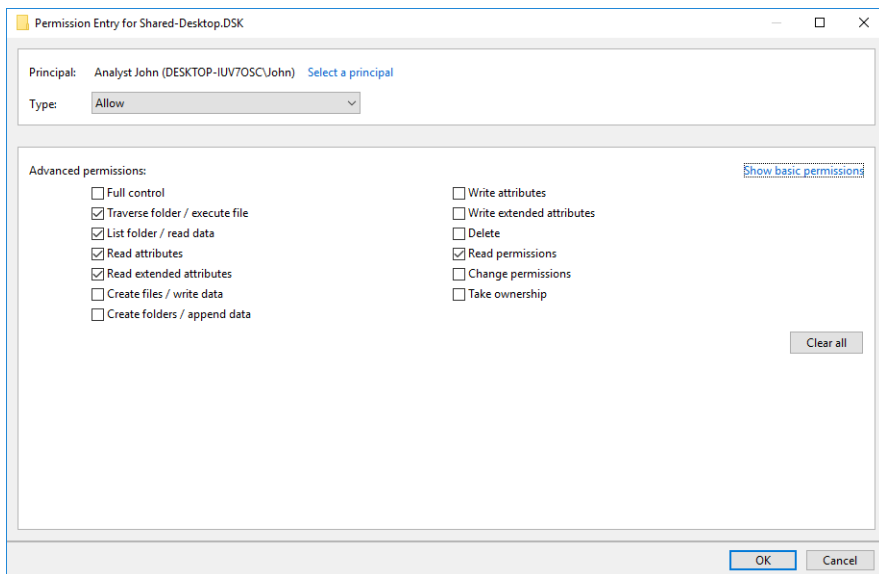


Fig 62: Security Settings for Shared Desktop - User Entry

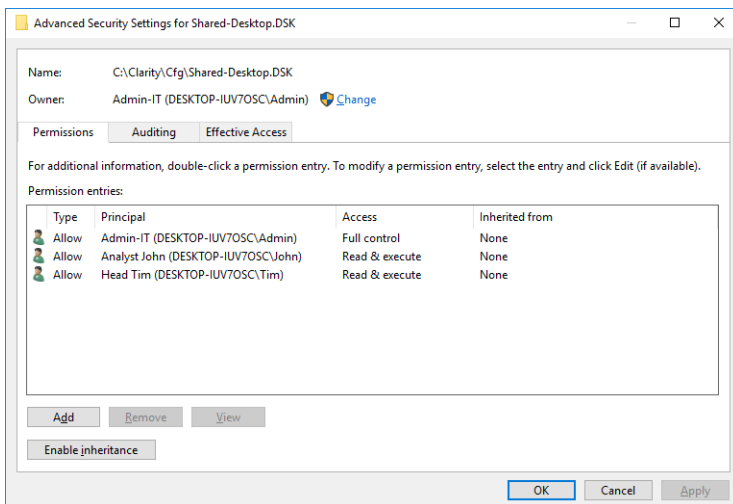


Fig 63: Security Settings for Shared Desktop - Advanced Settings

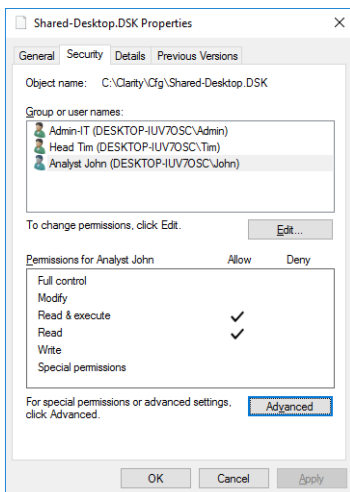


Fig 64: Security Settings for Shared Desktop - Security Overview

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.

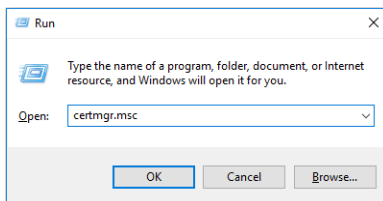
3.9.1 Setting certificates

The certificate issued by any official authority is a file that can be installed on the given computer. Such installation procedure shall be explained

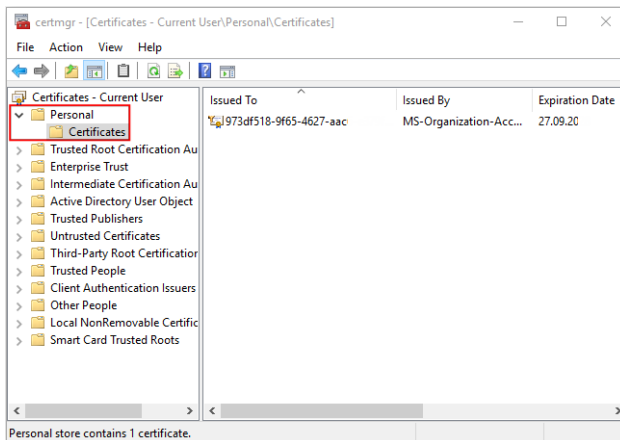
and described in detail by the certification authority by which the certificate was issued.

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.

- Press 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.